HI-TECH CRIME TRENDS 2019/2020

Cyberwar | Cyberweapons | State-sponsored | 2019/2020

Hacking back | Supply Chain | BGP hijacking | DNS hijacking

SWIFT | ATM Switch | SS7-threats | JS-sniffers | 5G

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

и топ-10 тенденций

КОНЕЦ ЭРЫ СТАБИЛЬНОСТИ КИБЕРПРОСТРАНСТВА

За последнее десятилетие число и уровень сложности кибератак со стороны как прогосударственных хакерских групп, так и финансово мотивированных киберпреступников значительно возросли. Люди, компании и государственные организации больше не могут быть уверены в безопасности киберпространства, а также в целостности и защищенности своих данных.

Интернет стал кровеносной системой нашей цивилизации. Однако свобода коммуникаций и глобальные возможности, которые дает Интернет, все чаще оказываются под угрозой: сливы и утечки данных, кибератаки со стороны враждующих государств – это реалии, в которых живет каждый из нас сегодня.

Свобода коммуникаций и глобальные возможности, которые дает Интернет, оказываются под угрозой

Уже более 16 лет эксперты Group-IB расследуют киберинциденты, анализируя инструменты и инфраструктуру атакующих. Каждая новая кибератака, направленная на компанию, политическую партию или объект критической инфраструктуры, дает нам возможность увидеть эволюцию тактик и инструментов их совершения.

Мы глубоко убеждены в том, что государственные организации и частные субъекты, которые борются против киберпреступности, должны обмениваться данными и публиковать свои исследования. Именно поэтому 6 лет назад мы выпустили первый отчет "High-Tech Crime Trends". Тогда это было единственное исследование тенденций киберпреступлений в России и одно из первых в мире.

Как и прежде, ежегодный отчет Group-IB показывает произошедшие за год изменения, являясь единым и максимально полным источником стратегических и тактических данных об актуальных киберугрозах в мире. Исследование покрывает период H2 2018 — H1 2019 по сравнению с H2 2017 — H1 2018.

Благодаря применению уникальных инструментов слежения за инфраструктурой киберпреступников, а также тщательному изучению исследований других команд, занимающихся кибербезопасностью в разных странах, мы находим и подтверждаем общие паттерны, формирующие целостную картину развития киберугроз. На этой основе мы формулируем прогнозы, которые сбываются каждый год в течение всего времени существования отчета.

Отчет Group-IB – единый и полный источник стратегических данных о киберугрозах и надежных прогнозов их развития

Ведущим и самым пугающим трендом 2019 года мы считаем использование кибероружия в открытых военных операциях. Конфликт между государствами приобрел новые формы, и кибер-активность играет ведущую роль в этом деструктивном диалоге. Атаки на критическую инфраструктуру и целенаправленная дестабилизация сети Интернет в отдельных странах открывают новую эпоху проведения кибератак. Мы уверены, что мирное существование больше невозможно в отрыве от кибербезопасности: этот фактор не может игнорировать ни одно государство, ни одна корпорация, ни один человек.

Целенаправленная дестабилизация сети Интернет в отдельных странах открывает новую эпоху проведения кибератак

Group-IB поддерживает инициативы Глобальной комиссии по стабильности киберпространства (The Global Commission on the Stability of Cyberspace, GCSC), созданной для выработки рекомендаций по продвижению киберстабильности в мире.

ТОП-10 ТЕНДЕНЦИЙ

Проведение открытых военных операций с использованием кибероружия

3 открытые военные

операции были проведены за первую половину 2019 года

За первые 6 месяцев 2019 года стало известно о трех открытых военных операциях: в марте в результате атаки на ГЭС Венесуэлы большая часть страны осталась без электричества на несколько дней, в мае в ответ на кибератаку армия Израиля произвела ракетный удар по хакерам группировки «Хамас», а в июне США использовали кибероружие против иранских систем контроля за запуском ракет в ответ на сбитый американский беспилотник.

Инструменты атакующих не установлены, при этом в последнем случае кибератака произошла всего через несколько дней после инцидента с беспилотником. Это подтверждает предположение о том, что критические инфраструктуры многих стран уже скомпрометированы, и атакующие просто остаются незамеченными до нужного момента.

Нарушение стабильности интернета на государственном уровне

Все уровни

инфраструктуры связи могут быть скомпрометированы

В современном мире максимальный социальный и экономический ущерб может быть нанесен за счет отключения людей и бизнеса от связи. При этом страны, выстраивающие централизованный контроль доступа в Интернет, становятся более уязвимыми и могут стать первой мишенью.

За последние годы были опробованы атаки на разные уровни инфраструктуры коммуникаций, и к 2019 году известны успешные случаи атак на маршрутизацию сети Интернет и BGP hijacking, на регистраторов доменных имен, администраторов корневых DNS-серверов, администраторов национальных доменов и DNS hijacking, на локальные системы фильтрации и блокировки трафика.

Новые угрозы, связанные с повсеместным внедрением 5G

Распространение 5G

станет новым драйвером угроз

Переход на технологии 5G только усугубит ситуацию с угрозами для телекоммуникационной отрасли. Первой причиной являются архитектурные особенности, которые открывают возможности для новых типов атак на сети операторов. Вторая причина — конкурентная борьба за новый рынок, которая может привести к демонстрации возможностей по взлому отдельных вендоров и появлению большого количества анонимных исследований об уязвимостях определенных технологических решений.

Скрытые угрозы со стороны проправительственных группировок

38 групп

спонсируемых государствами, были активны за исследуемый период, из них 7 — новые

Несмотря на то, что за последний период было опубликовано относительно большое количество исследований о новых проправительственных группировках, эта сфера остается малоизученной. Была замечена активность 38 групп (7 – новые, целью которых является шпионаж), однако это не значит, что другие известные группы прекратили свою деятельность — скорее всего, их кампании просто остались ниже радаров аналитиков.

К примеру, в сфере энергетики известно лишь два фреймворка — Industroyer и Triton (Trisis) — и оба были найдены в результате ошибки их операторов. Наиболее вероятно, что существует значительное количество подобных, еще не обнаруженных угроз, и это бомба замедленного действия.

Также стоит отметить, что известные в публичном пространстве проправительственные группировки в основном из развивающихся стран, однако информация об атаках и инструментах подобных групп из развитых стран по-прежнему не публикуется.

Обратный взлом: противостояние проправительственных группировок

Иран, Китай, Россия

были атакованы, и часть полученных данных выложены в открытый доступ от имени хактивситов

В 2019 году участились случаи появления в открытом доступе информации об инструментах атакующих от имени якобы хактивистов или бывших участников группировки. Чаще всего, это примеры обратного взлома, когда злоумышленники сами становятся жертвами. В настоящее время частные компании не имеют права проводить подобные операции, и такие полномочия официально есть только у специальных государственных служб.

Целенаправленные атаки на иностранные банки со стороны русскоязычных групп

5 групп

проводят целенаправленные атаки и представляют реальную опасность для банков

Всего 5 групп представляют сейчас реальную угрозу финансовому сектору: Cobalt, Silence, MoneyTaker — Россия, Lazarus — Северная Корея, SilentCards — новая группа из Кении.

В России ущерб от целенаправленных атак на банки со стороны финансово-мотивированных группировок за исследуемый период сократился почти в 14 раз. Это связано в том числе с переключением фокуса русскоязычных финансово-мотивированных групп на иностранные банки.

Постепенное исчезновение троянов для ПК и Android

22 трояна

для ПК и Android вышли из употребления, на смену им пришло всего 7 новых

Тенденция исчезновения троянов для ПК с ландшафта киберугроз продолжается: в России — на «родине» этого типа вредоносных программ — их перестали писать. Единственной страной, активно создающей трояны, стала Бразилия, но их использование носит исключительно локальный характер. Только Trickbot значительно эволюционировал за последний год и теперь может использоваться как для целенаправленных атак на банки, так и для шпионажа за государственными учреждениями, как это было с трояном Zeus.

Трояны для Android исчезают медленнее, чем для ПК, однако в любом случае количество новых в разы меньше вышедших из употребления. Новые программы эволюционируют от перехвата SMS к автоматическому переводу средств через банковские мобильные приложения — автозаливу.

Количество активных троянов продолжит снижаться за счет внедрения средств защиты и резкого сокращения экономической выгоды для атакующих.

Эволюция способов социальной инженерии без использования вредоносного кода

Программы удаленного доступа

относительно новый вектор социальной инженерии

На фоне падения троянов растет угроза социальной инженерии без использования вредоносного кода. Злоумышленники продолжают использовать поддельные аккаунты в соцсетях, совершают звонки с надежных номеров по хорошо продуманным скриптам, покупают для надежности базы паспортных данных и т.д. К относительно новым методам социальной инженерии можно отнести управление телефоном с помощью программ удаленного доступа, которые жертвы устанавливают на свои устройства под руководством телефонных мошенников.

Рост рынка кардинга за счет JS-сниффероов

$229 млн

составил штраф British Airways за компрометацию данных

При падении финансовой отдачи от использования банковских троянов для ПК и Android злоумышленники стали применять более эффективный способ заработка — JS-сниффферы. Уже сейчас их количество превышает количество троянов, а общее количество скомпрометированных с их помощью карт выросло на 38%. JS-сниффферы станут наиболее динамично развивающейся угрозой, особенно для стран, где не распространена система 3D Secure.

Новые атаки на страховые, консалтинговые и строительные компании

RedCurl

название новой группы, обнаруженной экспертами Group-IB

В 2019 году специалисты Group-IB зафиксировали атаки новой группы, получившей имя RedCurl. Основные цели группы — шпионаж и финансовая выгода. После выгрузки значимой документации злоумышленники устанавливают майнеры в инфраструктуру скомпрометированной компании.

Особенностью этой группы можно назвать очень высокое качество фишинговых атак — под каждую компанию злоумышленники создают отдельное письмо. RedCurl использует уникальный самописный троян, осуществляющий коммуникацию с управляющим сервером через легитимные сервисы, что сильно затрудняет обнаружение вредоносной активности в инфраструктуре.

КЛЮЧЕВЫЕ ВЫВОДЫ

и прогнозы

ПРОПРАВИТЕЛЬСТВЕННЫЕ ГРУППИРОВКИ, КИБЕРОРУЖИЕ И КИБЕРВОЙНЫ

СУЩЕСТВУЮЩИЕ УГРОЗЫ

Впервые в истории в ответ на кибератаку был нанесен реальный ракетный удар. В результате здание, в котором предположительно находился командный пункт атакующих, было разрушено. Данный удар нанес Израиль, однако законы других стран также не исключают применение реального оружия в ответ на кибератаку, и такой прецедент является крайне опасным.

Первые лица стран заявляют о возможности использования кибероружия для выведения из строя оборонной инфраструктуры противников. В случае исполнения это фактически будет проведением военной операции на территории другой страны.

Отчасти в результате кибератаки на Венесуэлу большая часть страны на протяжении нескольких дней оставалась без электроэнергии. Считается, что эта атака была произведена оппозицией с целью дестабилизации ситуации в стране.

Растет интерес прогосударственных атакующих к телекоммуникационной инфраструктуре. Их целями становятся операторы, регистраторы доменов, организации, отвечающие за национальные домены и корневые ДНС.

Некоторые проправительственные группы находятся в противостоянии друг с другом и под видом хактивистов выкладывают в открытый доступ инструменты своих соперников и материалы о них. С одной стороны, это помогает в уголовном преследовании разоблаченных лиц, с другой — позволяет другим атакующим более эффективно маскироваться под активность преследуемых групп.

Были проведены успешные атаки на производителей компьютерной техники с целью доставки вредоносного кода на их оборудование. Это указывает на то, что многие из них не готовы противостоять целенаправленным атакам, а значит “supply chain”-угрозы

38 групп

прогосударственных атакующих были активны в исследуемый период

7 новых групп

основной целью которых является шпионаж, было открыто за этот год

Аналитика

проводится в отношении групп из следующих стран — Россия, Северная Корея, Пакистан, Китай, Вьетнам, Иран, США, ОАЭ, Индия, Турция и страны Южной Америки

Информация

об исследованиях кибератак со стороны ведущих мировых держав по-прежнему не публикуется

ПРОГНОЗ: СТАБИЛЬНОСТЬ ИНТЕРНЕТА В НЕКОТОРЫХ СТРАНАХ БУДЕТ ПОД УГРОЗОЙ

Ранее казавшиеся нереалистичными сценарии отключения страны от Интернета становятся все более вероятными. Для проведения атаки, способной нарушить стабильность работы глобальной сети в отдельно взятой стране, требуется длительная подготовка, однако технически это возможно. Неутихающая военная риторика и агрессия могут привести к тому, что мы станем свидетелями демонстрации таких возможностей. Государствам и частным компаниям стоит позаботиться об отказоустойчивости предоставляемых сервисов в случае возникновения таких ситуаций.

Регистраторы доменных имен — это часть критической инфраструктуры страны. Так как нарушение их работы влияет на функционирование глобальной сети, они являются объектом атак со стороны проправительственных атакующих. В следующем году высок риск большого количества успешных атак, часть из которых будет проведена с целью саботажа.

Система централизованного контроля доступа в Интернет, выстраиваемая в некоторых странах, противоречит концепции отказоустойчивой глобальной сети. Поэтому для них риск проведения успешных атак с целью отключения от Интернета выше, а последствия будут иметь больший ущерб. Вероятно, что для подобных атак и демонстрации своих возможностей атакующие выберут именно эти страны.

ГЕОГРАФИЯ АТАК ПРОПРАВИТЕЛЬСТВЕННЫХ ГРУППИРОВОК

США	Европа	Азиатско-Тихоокеанский регион	Ближний Восток и Африка	Россия и СНГ
APT28 — Россия	APT28 — Россия	DarkHotel — Северная Корея	OilRig — Иран	Equation Group - США
Turla — Россия	Gorgon Group — Пакистан	APT37 — Северная Корея	APT37 — Северная Корея	PowerPool
Charming Kitten — Иран	PowerPool	Kimsuky — Северная Корея	**Windshift**	Gorgon Group — Пакистан
Gorgon Group — Пакистан	DarkHotel — Северная Корея	Sidewinder — Индия	Gaza Cybergang - Газа	MuddyWater - Иран
APT29 - Россия	APT29 — Россия	Chafer — Иран	Bahamut - Ближний Восток	APT37 — Северная Корея
APT33 - Иран	MuddyWater - Иран	APT-C-35	MuddyWater - Иран	Winnti - Китай
APT-C-36 - Южная Америка	APT10 - Китай	**BlueMushroom**	APT33 - Иран	Lazarus - Северная Корея
Kimsuky — Северная Корея	APT33 - Иран	APT10 - Китай	**Gallmaker**	**Whitefly**
Xenotime — Россия	Gamaredon Group - Росия	APT29 - Россия	APT-C-27 - Ближний Восток	Gamaredon Group - Россия
Lazarus — Северная Корея	**Gallmaker**	OceanLotus - Вьетнам	Lazarus - Северная Корея	Buhtrap - Россия
APT40 — Китай	Inception	OilRig - Иран	FruityArmor - ОАЭ	APT28 - Россия
STOLEN PENCIL — Северная Корея	Turla - Россия	**Whitefly**	Emissary Panda - Китай	**HEXANE — Ближний Восток**
	LEAD - Китай	Winnti - Китай	APT-C-38	
	OceanLotus - Вьетнам	BITTER - Индия	Domestic Kitten - Иран	
	Lazarus - Северная Корея	Turla - Россия	Chafer - Иран	
	APT40 — Китай	Xenotime - Россия	StrongPity - Турция	
		Lazarus - Северная Корея	**HEXANE — Ближний Восток**	
		APT40 - Китай		
		Неизвестная группа, фреймворк TajMahal		

*** новые группы**

ОБЩАЯ ОЦЕНКА РЫНКА ВЫСОКОТЕХНОЛОГИЧНЫХ ПРЕСТУПЛЕНИЙ В ФИНАНСОВОЙ ОТРАСЛИ РОССИИ

За исследуемый период сократился ущерб сразу от всех видов мошенничества с использованием вредоносного кода, направленных как напрямую на банки, так и на их клиентов. Самой растущей угрозой стала социальная инженерия без использования вредоносного кода - поддельные аккаунты в соцсетях, звонки мошенников по хорошо продуманным скриптам и т.д.

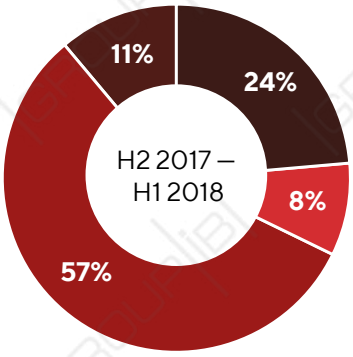
Почти в 14 раз сократился ущерб от целенаправленных атак на банки со стороны финансово-мотивированных группировок. Это связано в том числе с переключением их фокуса на иностранные банки.

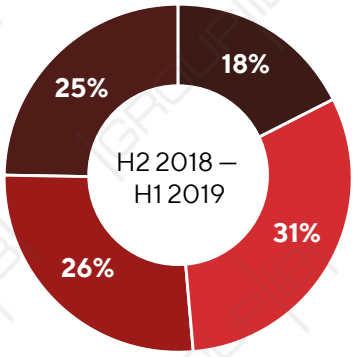
Оценивая рынок высокотехнологичных преступлений в России, эксперты Group-IB выделяют несколько сегментов:

- Хищения с помощью троянов для ПК — ущерб сократился на 89% и составил 62 миллиона рублей. Групп, использующих этот метод, осталось только две (из трех в прошлом периоде), при этом только одна из них (с трояном RTM) проявляет постоянную активность.
- Хищения с помощью троянов для Android также находятся на спаде. Общий объем хищений упал на 43% и составил 110 млн. рублей. Количество групп, использующих Android-трояны в России, сократилось с 8 до 5, при этом со сцены ушли трояны с наибольшим количеством мошеннических транзакций. Оставшиеся группы больше не используют СМС-канал для хищений, его заменил метод перевода с карты на карту, что привело к увеличению среднего размера хищения с 7 до 11 тысяч рублей.
- Ущерб от финансового фишинга сократился на 65% до уровня 87 миллионов рублей. На общую цифру повлияло как снижение количества активных групп, так и уменьшение «среднего чека» атаки. Из-за низкой экономической эффективности фишинговых атак в этом сегменте осталось всего 11 активных групп из 26 в прошлом периоде.

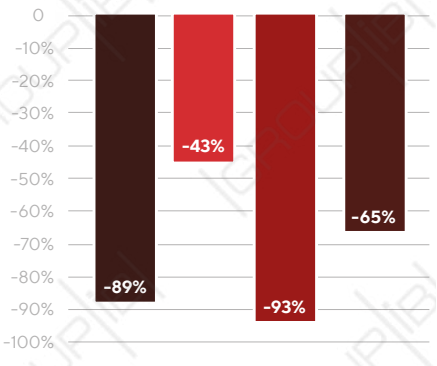
Сегмент рынка в России	Кол-во групп	Общее число успешных атак в день	Средняя сумма одного хищения	Средняя сумма хищения в день*	H2 2018- H1 2019 (в RUR)	H2 2018- H1 2019 (в USD)	Рост к прошлому периоду
Хищения у юридических лиц с троянами для ПК	2	0,5	500 000 ₽	250 000 ₽	62 250 000 ₽	$957 692	-89%
Хищения у физических лиц с Android-троянами	5	40	11 000 ₽	440 000 ₽	109 560 000 ₽	$1 685 538	-43%
Целевые атаки на банки	3	—	31 000 000 ₽	—	93 000 000 ₽	$1 430 769	-93%
Фишинг	11	435	800 ₽	348 000 ₽	86 652 000 ₽	$1 333 108	-65%
Обналичивание похищаемых средств	—	—	—	467 100 ₽	158 157 900 ₽	$2 433 198	-85%
Итого	—	—	—	**1 038 000**	**509 619 900 ₽**	**$7 840 306**	**-85%**

* учтены только рабочие дни





Изменение к прошлому периоду



ТЕНДЕНЦИИ И ПРОГНОЗЫ ПО ИНДУСТРИЯМ

Угрозы для телекоммуникационного сектора

СУЩЕСТВУЮЩИЕ УГРОЗЫ

Значительную угрозу для телекоммуникационного сектора представляет BGP hijacking, который приводит к нарушению доступности сетей и множества опирающихся на них сервисов. Как правило, восстановление доступности в результате такой атаки происходит за несколько часов.

Распространение 5G, как и любой технологии следующего поколения, открывает новые возможности для атакующих. Из-за архитектурных особенностей 5G становятся возможными новые типы атак на сети операторов.

Массовую угрозу для телеком-сектора представляют уязвимые роутеры, которые сдаются в аренду физическим и юридическим лицам. Небезопасные настройки и невозможность обновления этого оборудования приводят к деградации сервиса и росту вредоносного трафика. Таким образом, злоумышленники могут проводить разные типы атак, опираясь на инфраструктуру оператора.

9 групп

представляли угрозу для телекоммуникационного сектора в исследуемый период — это больше, чем для финансового сектора

Шпионаж, “supply chain”–атаки

являются основными целями этих групп, поэтому их активность дольше остается незамеченной

ПРОГНОЗ: РАСПРОСТРАНЕНИЕ 5G СТАНЕТ ПРИЧИНОЙ НОВЫХ УГРОЗ

На распределение долей рынка 5G между игроками будет влиять в том числе уровень их кибербезопасности. Недостатки в системе защиты у одного производителя 5G платформ будут создавать конкурентные преимущества для другого.

Демонстрация возможностей эксплуатации и нарушения работоспособности оборудования отдельных производителей 5G будут использоваться как один из методов конкурентной борьбы за новый рынок. Успешные атаки могут нанести производителям значительный репутационный ущерб.

Более широкое внедрение 5G значительно увеличит возможности обычных киберпреступников по проведению DDoS-атак, манипуляции трафиком, распространению вредоносных программ.

Через несколько лет телеком-операторы столкнутся с проблемой выявления аппаратных и firmware закладок в оборудовании, которое сейчас используется для инфраструктуры 5G.

Многие телеком-операторы относятся к классу Managed Service Provider и оказывают услуги по обеспечению безопасности государственных и коммерческих предприятий. Их будут атаковать с целью проникновения в защищаемые ими сети.

Угрозы для энергетического сектора

СУЩЕСТВУЮЩИЕ УГРОЗЫ

Основным вектором проникновения в изолированный сегмент OT-сети является компрометация ИТ-сетей с помощью традиционных вредоносных программ и техник, включая "living off the land".

За последние годы выявлено только два фреймворка, которые способны влиять на технологические процессы, — Industroyer и Triton (Trisis). Эксперты по безопасности связывают их с Россией.

Оба фреймворка были обнаружены в результате ошибки их операторов. Очевидно, что существует значительное количество еще не обнаруженных угроз, и это бомба замедленного действия.

В 2019 году Lazarus атаковал энергетическую ядерную корпорацию в Индии. Выбор жертвы нетипичен для этой прогосударственной группы и может свидетельствовать о растущем интересе к таким атакам со стороны военных ведомств.

7 групп

представляли угрозу для энергетического сектора в исследуемый период

Иран, Россия и Северная Корея

страны, с которыми связывают активность этих групп

ПРОГНОЗ: ОСНОВНЫМ ВЕКТОРОМ ПРОНИКНОВЕНИЯ БУДУТ ИТ-СЕТИ И “SUPPLY CHAIN”-АТАКИ

Основным вектором для атакующих останутся ИТ-сети, доступ к которым необходим для шпионажа и сбора информации о том, как атаковать конкретную энергетическую компанию с целью саботажа.

Компрометация OT-сетей — это следующий шаг после успешного проникновения в ИТ-сегмент сети. Выявить компрометацию OT-сети возможно только в двух случаях: если атака готовилась с целью саботажа или если оператор вредоносной программы допустил ошибку. Поэтому чаще всего атакующие максимально скрывают свое присутствие до крайнего момента, когда понадобится провести массовую атаку.

Большую проблему для энергетического сектора будут составлять “supply chain”-атаки со стороны поставщиков программного и аппаратного обеспечения. Прежде всего будут атакованы управляющие компании, и уже через них пойдет развитие атак на сети энергетических компаний.

Наибольшую опасность следует ожидать со стороны развитых стран. При том что они обладают более совершенным арсеналом для проведения атак, их активность менее заметна и изучена.

Угрозы для финансовой отрасли

Целенаправленные атаки на финансовый сектор

СУЩЕСТВУЮЩИЕ УГРОЗЫ

SilentCards — новая группа, которая проводит целенаправленные атаки на банки в Африке. Несмотря на слабую техническую подготовку по сравнению с другими группами, они успешно совершают хищения в своем регионе.

FastCash — новый метод хищения, который стал известен в конце 2018 года, хотя был использован впервые в Азии еще в 2016 году. За всеми атаками этого типа стоит группа Lazarus.

Эксперты наблюдали следующие тенденции в используемых схемах атак: через банкоматы атаковал только Silence, через карточный процессинг - Silence и SilentCards, через SWIFT - Lazarus (2 успешных хищения: в Индии и на Мальте на общую сумму $16 миллионов).

Участники Silence перестали заниматься рассылками и вместо этого начали покупать их у других хакерских групп (в частности, у TA505).

В России каждая из русскоязычных групп провела по одной атаке за исследуемый период. Cobalt попытался ограбить одну из компаний дважды, но хищения не нанесли большого финансового ущерба. По сравнению с прошлым периодом, средняя сумма хищения в России упала со 118 до 31 миллиона рублей, а общий объем хищений составил 93 миллиона рублей, что на 93% ниже аналогичного показателя прошлого периода.

5 групп

представляли реальную угрозу финансовому сектору в исследуемый период — Cobalt, Silence, MoneyTaker, Lazarus, SilentCards

3 из 5 групп

являются русскоговорящими (Cobalt, Silence, MoneyTaker), и только они обладают троянами, которые позволяют управлять диспенсером банкомата

2 из 3 групп

русскоязычных групп (Cobalt и Silence) стали атаковать банки преимущественно за пределами России

ПРОГНОЗ: РАСШИРЕНИЕ ГЕОГРАФИИ АКТИВНОСТИ РУССКОЯЗЫЧНЫХ ГРУПП

Русскоязычные группы Silence, MoneyTaker, Cobalt вероятнее всего продолжат географическую экспансию, увеличивая количество атак за пределами России. Для вывода денег они будут использовать атаки на систему карточного процессинга и трояны для банкоматов. SWIFT будет намного реже попадать в фокус этих групп.

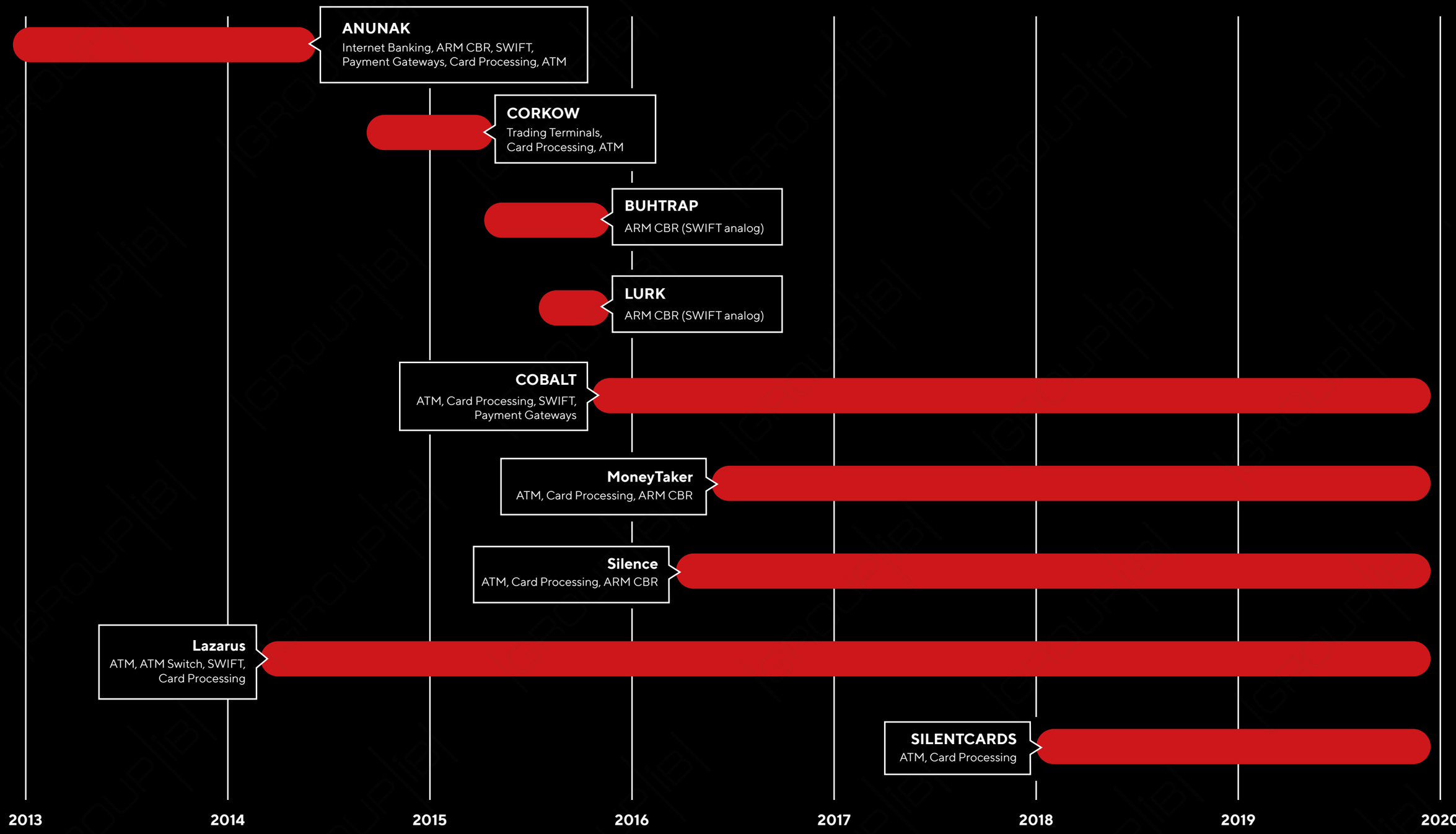
Lazarus останется единственной группой, которая будет совершать хищения через SWIFT и ATM Switch. Успешные атаки через ATM Switch были проведены в банках, использующих программное обеспечение под операционной системой IBM AIX. Поэтому банки, использующие это программное обеспечение, первыми попадут на радар группы.

Успешные атаки на банки будут завершаться выводом инфраструктуры из строя для сокрытия следов.

Предположительно SilentCards пока останется локальной группой и будет атаковать банки в Африке. Скорее всего, она расширит список целей за счет других отраслей, где основным вектором будет вымогательство после применения программ-шифровальщиков.

Троян Trickbot значительно эволюционировал (см. пункт ниже «Банковские трояны для ПК»), и теперь может использоваться для целенаправленных атак на банки и шпионажа за государственными учреждениями, как это было с трояном Zeus.

ЦЕЛЕНАПРАВЛЕННЫЕ АТАКИ НА ФИНАНСОВЫЙ СЕКТОР



Нецелевые атаки и угрозы для клиентов банков

Рост кардинга за счет распространения JS-сниффферов

Дампы по-прежнему составляют основную долю рынка кардинга, их количество в продаже выросло на 46%. Продажа текстовых данных (номер, CVV, срок действия) тоже на подъёме, их рост составил 19%.

Самые массовые утечки данных банковских карт связаны с компрометацией ритейла в США. По количеству скомпрометированных карт США занимает первое место с большим отрывом — 93%.

Страны Ближнего Востока (Кувейт, Пакистан, ОАЭ, Катар) занимают следующие позиции антирейтинга, суммарно на них приходится 2.38%. Предположительно, причиной роста количества скомпрометированных карт в этом регионе стали атаки группы Lazarus в конце 2018 и начале 2019 года.

Одной из точек роста объема текстовых данных стали JS-сниффферы. В этом году эксперты Group-IB выявили минимум 38 разных семейств JS-сниффферов, и их количество превышает число банковских троянов.

В случаях с компрометацией с помощью JS-сниффферов первую позицию также занимает США, а вторую — английские банки. Это прежде всего связано с успешной атакой на British Airways в конце 2018 года, в результате которой были скомпрометированы более 300 тысяч банковских карт.

на 38% выросло

общее количество скомпрометированных карт

$229 миллионов

составил штраф British Airways за компрометацию данных

ПРОГНОЗ: РОСТ КАРДИНГА ЗА СЧЕТ РАСПРОСТРАНЕНИЯ JS-СНИФФЕРОВ

Разработчики фишинг-китов стали больше внимания уделять самозащите: они используют блокировку подсетей вендоров по безопасности, хостинг компаний, отдают фишинговый контент только с IP-адресов региона, где находятся их жертвы, перенаправляют на легитимные сайты, проверяют аномальные user-agent.

В борьбе за клиента разработчики фишинговых наборов стали снабжать их удобными системами управления. Теперь вместо работы с логами в почте покупатели могут удобно управлять данными через простые веб-панели.

При финансовом фишинге атакующие начали использовать панели для управления веб-инжектами и автозаливом, которые раньше использовались банковскими троянами.

SMS-трафик в некоторых странах становится популярным инструментом распространения ссылок на фишинговые сайты. В связи с этим набирают популярность утечки баз данных с телефонами, а также доступы к личным кабинетам мобильных операторов, через которые можно отправлять SMS.

Новые изощренные методы социальной инженерии

Значительное сокращение активности банковских троянов для ПК и Android, а также сокращение фишинговых атак вывели мошенничество с использованием приемов социальной инженерии на первое место по степени распространения угрозы.

Социальная инженерия может иметь множество форм. Широко известны схемы, при которых жертв вынуждают раскрывать логины, пароли, данные банковских карт, осуществлять переводы через банкоматы и мобильные приложения. При этом злоумышленники используют различные каналы, чтобы связаться с жертвой: телефонные звонки, мессенджеры, социальные сети.

Развиваются и новые формы: например, набирает популярность схема, когда мошенники просят пользователя установить на мобильный телефон средство удаленного управления и таким образом получают доступ к любым приложениям и данным на устройстве.

Уменьшение количества банковских троянов для ПК

Русскоязычные хакеры перестали создавать банковские трояны для ПК. Новым источником такого вредоносного ПО стала Бразилия, однако пока с его помощью атакуют только местное население.

Владельцы старых бот-сетей не расширяют свою географию и, как правило, атакуют клиентов банков в 2-3 странах, где им проще осуществлять отмывание похищенных средств.

Осталось всего две группы, которые похищают деньги в России с помощью троянов для ПК — RTM и Buhtrap2. Активность проявляет только первая из них.

7 троянов для ПК

вышли из эксплуатации, ни одного нового не было создано русскоязычными хакерами за исследуемый период

Trickbot — единственный троян, который значительно эволюционировал за последний год:

- новый модуль для сбора паролей из установленных приложений
- возможность красть конфигурационные файлы из директорий SYSVOL на контроллере домена, а также данные RDP, VNC и PuTTY
- использование Mimikatz и проведение Fileless-атак
- отсутствие загрузки модулей и конфигурационного файла на диск (ОС Windows 10)
- рассылка письма со скомпрометированных компьютеров
- новый cookie stealer

Некоторые исследователи выделяют отдельную группировку Grim Spider, которая использует Trickbot для изучения сети. Далее они загружают шифровальщик Ryuk и требуют от $100,000 за расшифровку данных.

Автозалив и подмена push-уведомлений в банковских троянах под Android

Раньше для хищений денег с банковских счетов в основном использовался метод демонстрации поддельных окон, куда требовалось ввести данные карты или логин и пароль. При этом для получения кодов подтверждения транзакций перехватывались SMS. В 2019 году появились трояны, способные автоматически переводить средства через банковские мобильные приложения — автозалив.

Push-уведомления считались надежным методом доставки одноразовых кодов, однако теперь, используя Accessibility Service — службы специальных возможностей — трояны получают возможность манипулировать PUSH-уведомлениями, копировать их текст, нажимать на определенные области.

США добились того, что авторы троянов под Android начинают запрещать использование их программ не только в России и СНГ, но и в Америке.

Наиболее совершенные трояны под Android появились в 2019 году. Они были разработаны для сдачи в аренду, цена в месяц варьируется от $800 до $2,000.

Владельцы банковских бот-сетей стали уделять больше внимания самозащите, способам обнаружения и обхода песочниц.

15 троянов

вышли из эксплуатации, код 7 троянов адаптировали под работу современной ОС Android, 5 новых троянов появились на рынке

ПРОГНОЗ: ВЫТЕСНЕНИЕ ТРОЯНОВ JS-СНИФФЕРАМИ, МОДИФИКАЦИЯ МЕТОДОВ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ И РАСПРОСТРАНЕНИЯ ФИШИНГА

Основной угрозой для клиентов банков останутся фишинг и социальная инженерия. При этом канал распространения фишинговых ссылок может сместиться с почты на SMS-трафик.

Владельцы DDoS-бот-сетей, построенных на большом количестве зараженных роутеров, могут начать сдавать их в аренду злоумышленникам, занимающимся фишингом. Это позволит им зарабатывать больше, чем на проведении DDoS-атак.

Схема с оказанием дистанционной поддержки через средства удаленного дистанционного управления сместится с ПК на мобильные устройства. Это преследует две цели: получить от клиента данные банковских карт или требовать от него оплату за «фиктивные услуги» (например, проверка на безопасность, очистка устройства от вредоносного ПО и т.п.)

Количество активных банковских троянов для ПК сократится повсеместно за исключением Бразилии, где их локальное использование наоборот развивается. Будет сокращаться как количество активных троянов, так и география их распространения за счет внедрения средств защиты и резкого сокращения экономической выгоды для атакующих.

Сейчас автозалив на Android-троянах реализуется самостоятельно каждым вирусописателем. Если кто-то сделает общее универсальное решение (как это было с Zeus), то популярность такой атаки резко вырастет. Однако в течение одного года этого эффекта вряд ли удастся достичь.

Наиболее динамично развивающейся угрозой будут JS-сниффферы, которые позволяют атакующим зарабатывать больше, чем на банковских троянах. Их количество уже превышает количество банковских троянов для ПК и Android. Угроза будет актуальна в первую очередь для стран, где не распространена система 3D Secure.

POS-трояны не претерпят серьезных изменений и будут по-прежнему использоваться для атак прежде всего на ритейл в США и в меньшей степени — в испаноговорящих странах.

НОВЫЙ ЭТАП КИБЕРВОЙНЫ:
нарушение работоспособности сети Интернет

Основные тенденции киберугроз по годам

2017

эпидемии шифровальщиков WannaCry, NotPetya, BadRabbit

2018

“side-channel”-атаки и новые уязвимости в микропроцессорах

2019

открытые военные операции в киберпространстве

В 2019 году тема кибербезопасности вышла на первый план в политике, а действия киберармий и публичная риторика политических деятелей вокруг кибератак продолжают набирать обороты.

Март 2019, Венесуэла. В результате саботажа на ГЭС имени Симона Боливара («Гури») в Венесуэле произошло массовое отключение электроэнергии в Каракасе и 22 штатах страны из 23. По данным министра связи и информации, «была совершена кибератака, направленная на автоматическую систему контроля гидроэлектростанции «Гури». В итоге на атаку работа ГЭС была остановлена, что привело к прекращению энергоснабжения». В отличие от других известных атак на энергетические компании, это первый случай, когда большая часть страны оставалась без электричества несколько дней.

5 мая 2019, Палестина. По данным Израиля, 4 мая 2019 хакеры группировки «Хамас» попытались провести кибератаку. Подробности обнаруженного инцидента Израиль отказался раскрывать. Для предотвращения атаки армия обороны нанесла ракетный удар по зданию в секторе Газа, где предположительно находился штаб хакеров.

Этот инцидент в очередной раз подтверждает предположение о том, что критические инфраструктуры многих стран уже скомпрометированы, но атакующие остаются незамеченными до нужного момента.

Июнь 2019, Иран. 20 июня 2019 корпус стражей Исламской революции сбил американский беспилотник. В ответ на это через несколько дней США провели кибератаку на ракетные системы Ирана. Для осуществления такой операции требуются месяцы подготовки, поэтому очевидно, что системы были скомпрометированы заранее.

Все эти примеры демонстрируют, как киберпространство превращается в поле боевых действий. Развитие такой тенденции может привести к новым кибератакам на военные и государственные системы с целью вывода их из строя, нанесения социального и экономического ущерба, дестабилизации ситуации в стране.

Опасным вектором становится нарушение работоспособности инфраструктуры сети Интернет, от которой сейчас зависят почти все государственные и частные компании. В следующих разделах мы рассмотрим сценарии операций, которые уже были опробованы и могут использоваться в более серьезных масштабах на государственном уровне в следующем году.

АТАКИ НА РЕГИСТРАТОРОВ ДОМЕННЫХ ИМЕН И DNS HIJACKING

Протокол DNS лежит в основе работоспособности глобальной сети, и получение контроля над ним может быть крайне опасно. При этом для проведения операций с использованием этого протокола не обязательно иметь доступ к DNS-серверам.

При покупке доменного имени возможно два варианта событий:

- регистратор доменного имени предоставляет услуги DNS-сервера;
- регистратор предоставляет только доменное имя, а DNS-серверы находятся у другого провайдера.

В любом из сценариев каждый из клиентов может в своем личном кабинете на сайте регистратора доменных имен указать:

- какие DNS-серверы будут отвечать за конкретное доменное имя;
- на какие IP-адреса будет отправляться трафик в случае запросов ресурсов, связанных с этим доменным именем.

Это значит, что, скомпрометировав определенного регистратора доменных имен, атакующий может манипулировать всеми доменами, зарегистрированными через этого доменного регистратора. Ситуация усугубляется тем, что в каждой стране, как правило, существует лишь несколько крупных регистраторов, услугами которых пользуются и государственные, и частные компании.

Одновременный взлом нескольких основных регистраторов в таком случае приведет к остановке работы веб-сайтов, почтовых серверов, DNS-серверов и всех связанных с ними служб для большей части страны. Если такая атака будет проводиться в комбинации с саботажем, то оперативно восстановить работоспособность регистратора и вернуть нормальные настройки будет невозможно, и это нанесет ущерб всем отраслям без исключения.

Кроме отдельных регистраторов целью атакующих могут также стать организации, управляющие национальными доменными зонами. Такая организация есть практически в любой стране — например, за доменную зону Сингапура .sg отвечает Singapore Network Information Centre (SGNIC) Pte Ltd.

Таким образом, регистраторы доменных имен и организации, отвечающие за корневые доменные сервисы, стали новой приоритетной целью атакующих. В 2019 году экспертами по информационной безопасности было раскрыто несколько подобных инцидентов.

Инфраструктура DNS может быть успешно атакована на всех уровнях

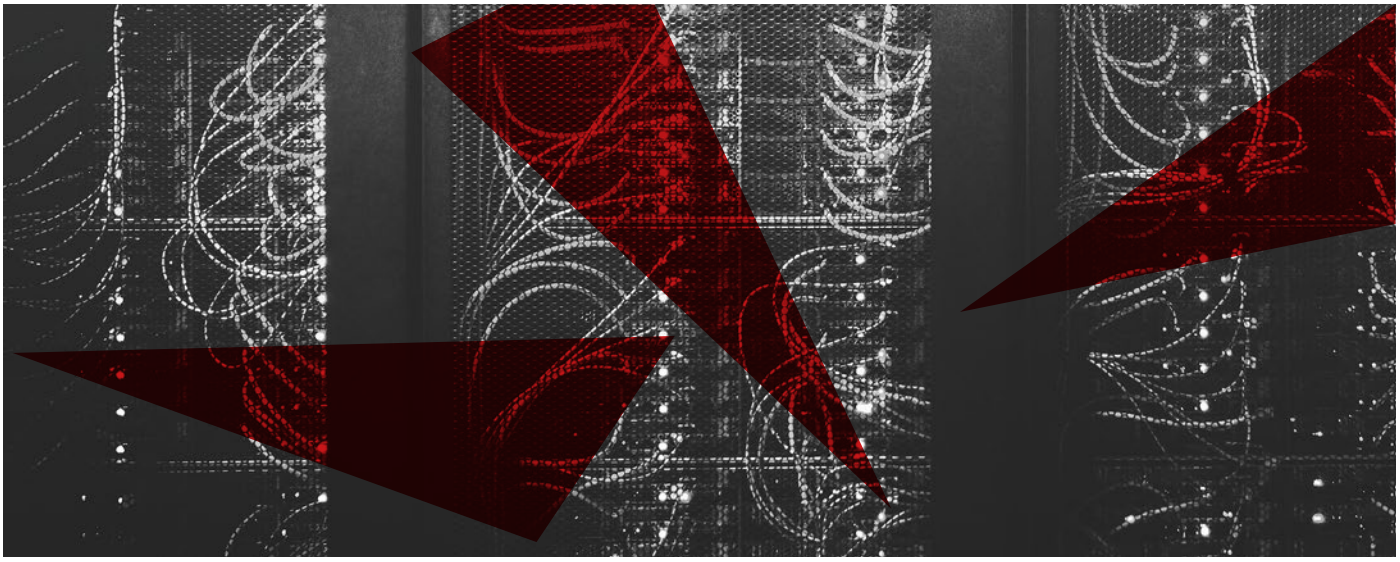
12.14.2018 – 1.2.2019

атакам подвергалась шведская компания Netnod — одна из 12 организаций в мире, управляющих корневыми DNS-серверами. Атакующие могли манипулировать DNS-записями для MITM-атак, нацеленных на выбранных клиентов.[1]

АПРЕЛЬ 2019

владельцы доменов .gr и .ελ получили уведомление, что Институт компьютерных наук Фонда исследований и технологий (FORTH-IC), отвечающий за техническую поддержку и эксплуатацию доменов в этих зонах, был подвергнут атаке. В связи с этим пользователей просили срочно сменить пароли для авторизации.[2]

Описанные атаки были успешными, и их целями являлись отдельные компании государственного и частного сектора. Если атакующие поставят перед собой задачу нарушения работоспособности инфраструктуры в стране, то такие атаки могут иметь намного более масштабные последствия.



[1] https://www.netnod.se/news/statement-on-man-in-the-middle-attack-against-netnod
[2] https://www.zdnet.com/article/hackers-breached-greeces-top-level-domain-registrar

АТАКИ НА МАРШРУТИЗАЦИЮ СЕТИ ИНТЕРНЕТ И BGP HIJACKING

Другим основополагающим протоколом маршрутизации для глобальной сети является BGP (Border Gateway Protocol). Суть BGP hijacking или перехвата маршрута заключается в перенаправлении сетевого трафика отдельных префиксов автономной системы (пулов IP-адресов) через свое оборудование. Самый распространенный способ использования этого сценария – шпионаж.

Однако подобная манипуляция сетевыми маршрутами может быть также использована для нарушения работоспособности крупных телекоммуникационных компаний. Публично известно о нескольких масштабных инцидентах (правда они были результатом ошибки человека и неправильных настроек, а не целенаправленными атаками).

25 НОЯБРЯ 2018

небольшой российский оператор Krek Ltd допустил ошибку в конфигурации BGP, в результате которой от 10 до 20% пользователей интернета в России потеряли доступ к тысячам сервисов. Сбой продолжался более часа и затронул такие известные компании, как Amazon, YouTube, ВКонтакте, онлайн-кинотеатр ivi и многие другие.[1]

НОЯБРЬ 2018

из-за ошибки конфигурации нигерийский интернет-провайдер MainOne изменил маршруты так, что трафик к сервисам Google начал идти через Китай, где и обрывался. Всего утекло 180 префиксов Google. С момента обнаружения проблемы до ее решения прошло 74 минуты, в течение которых некоторые пользователи Google испытывали проблемы с доступом.[2]

6 ИЮНЯ 2019

швейцарская компания Safe Host (AS21217) стала причиной утечки 70 000 маршрутов в Китай Telecom (AS4134). Среди наиболее пострадавших сетей оказались швейцарская компания Swisscom (AS3303), голландская KPN (AS1136) и французские Bouygues Telecom (AS5410) и Numericable-SFR (AS21502). Данный инцидент продлился 2 часа.[3]

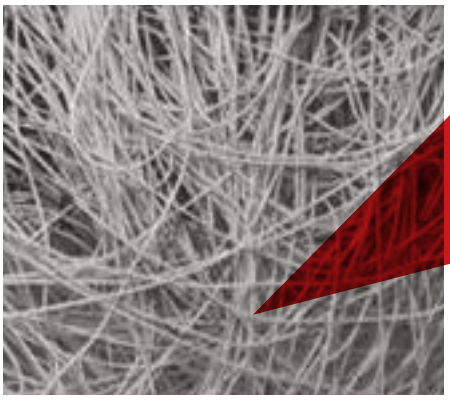
Еще одним интересным примером является эксперимент, проведенный в январе 2019 года с целью изучения новых функций безопасности протокола BGP. Он привел к выводу из строя маршрутизаторов интернет-провайдеров в Азии и Австралии.

BGP ROV

Наряду с BGP Resource Public Key Infrastructure (RPKI) и BGP Path Validation (BGPsec) новый стандарт BGP Route Origin Validation (ROV) стал частью пакета безопасности для протокола BGP. BGP ROV позволяет маршрутизаторам использовать информацию BGP RPKI для фильтрации неавторизованных объявлений маршрутов и предотвращения перехвата BGP злоумышленниками. Таким образом трафик может быть перенаправлен с легитимных серверов на вредоносные. По словам исследователей, проблема заключалась в том, что используемый ими атрибут BGP вызвал сбой в работе программного обеспечения маршрутизаторов, работающих на базе FRRouting (FRR) – набора IP-протоколов для Linux и Unix.

Описанные выше кейсы демонстрируют, что для манипуляции трафиком не обязательно иметь доступ к сетевому оборудованию атакуемой компании. Чтобы менять настройки BGP, достаточно доступа к пограничному маршрутизатору.

Пока эффект от BGP hijacking носит массовый, но непродолжительный характер. Для продолжительного саботажа злоумышленникам понадобится доступ к сетевым маршрутизаторам нескольких операторов и заранее спланированные сценарии по манипуляции трафиком. В таком случае BGP hijacking сможет вызвать значительные перегрузки в сетях определенных стран (по аналогии с тем, как это происходит в сетях энергокомпаний).



[1] https://qrator.net/ru/company/news/perekhvat-trafika-privel-k-sboiu-v-rossiiskom-segmente-interneta
[2] https://blog.cloudflare.com/how-a-nigerian-isp-knocked-google-offline/
[3] https://www.zdnet.com/article/for-two-hours-a-large-chunk-of-european-mobile-traffic-was-rerouted-through-china/

АТАКИ НА ЛОКАЛЬНЫЕ СИСТЕМЫ ФИЛЬТРАЦИИ И БЛОКИРОВКИ ТРАФИКА

Некоторые страны уже внедрили или создают системы фильтрации, анализирующие и блокирующие определенный трафик пользователей. Подобные технологические решения расширяют для злоумышленников возможности атак по блокировке работы сети в определенной стране. Ниже описаны примеры, которые уже опробованы и могут быть масштабированы.

Списки запрещённых ресурсов

Для ограничения доступа к запрещенным ресурсам (террористические, вредоносные, наркотические и т.п.) интернет-провайдеры получают списки этих ресурсов и осуществляют блокировку. Списки состоят из доменов, IP-адресов, ссылок и постоянно обновляются, чтобы владельцы запрещенных ресурсов не могли обойти блокировку.

Однако операторы не могут везде развернуть DPI-решения для фильтрации, поэтому по-прежнему вынуждены осуществлять блокировку по IP-адресам. Зная это, атакующие используют домены из черного списка для блокировки легитимных ресурсов. Для этого они меняют у доменов из черных списков IP-адрес своего сервера на IP-адрес легитимного ресурса. Таким образом, в результате обновлений черного списка или автоматического разрешения домена в IP на стороне конкретного оператора трафик к легитимному ресурсу блокируется.

Так в России, начиная с 2017 года, атакующие блокировали доступ к Wikipedia, некоторым банковским и государственным ресурсам. В марте 2019 года такая же атака была проведена и на пользователей российской поисковой системы.[1]

Это простой и дешевый способ проведения подобной атаки. От нее можно защититься введением белого списка критичных ресурсов, которые никогда не должны блокироваться. Однако черные списки распространяются централизовано, и если атакующий получит доступ к серверу, осуществляющему распространение этих списков, он может добавить в него любые подсети.

Расшифровка трафика

Большая часть контента передается в зашифрованном виде, поэтому некоторые страны требуют от граждан устанавливать выпущенные ими сертификаты, чтобы иметь возможность расшифровывать содержимое трафика.

Такие сертификаты выпускают определенные центры, и если производители ОС или браузеров принудительно перестанут им доверять, то это затронет всех пользователей, у которых установлены эти сертификаты.

Именно это случилось с компанией DarkMatter из ОАЭ, когда Google заявила о решении запретить в браузере Google Chrome и операционной системе Android корневые сертификаты, принадлежащие этой компании, а позднее то же самое сделала Mozilla. В августе 2019 года Google и Mozilla заблокировали национальный сертификат Казахстана, используемый для прослушки трафика.

[1] https://www.netnod.se/news/statement-on-man-in-the-middle-attack-against-netnod

ЭВОЛЮЦИЯ ГРУППИРОВОК

спонсируемых государствами

ГЕОГРАФИЧЕСКИЙ ЛАНДШАФТ И ПОЯВЛЕНИЕ НОВЫХ ГРУПП

Всего известно об активности 38 групп, кампании которых затрагивают все регионы мира. Аналитики изучают в основном группы из России, Северной Кореи, Пакистана, Китая, Вьетнама, Ирана, США, ОАЭ, Индии, Турции, региона Южной Америки.

Примечательно, что в публичном пространстве по-прежнему отсутствуют сведения об атаках со стороны развитых стран. Это подтверждает предположение о том, что активность хорошо подготовленных атакующих сложно обнаружить или связать с конкретной группой или страной.

1. АТАКИ НА АМЕРИКУ

Россия: APT28, Turla, APT29, Xenotime
Пакистан: Gorgon Group
Иран: APT33, Charming Kitten
Северная Корея: Kimsuky, Lazarus, STOLEN PENCIL
Китай: APT40
Южная Америка: APT-C-36*

2. АТАКИ НА ЕВРОПУ

Россия: APT28, Turla, Gamaredon Group, APT29
Пакистан: Gorgon Group
Иран: APT33, MuddyWater
Северная Корея: DarkHotel, Lazarus
Китай: APT40, LEAD, APT10
Вьетнам: OceanLotus
Неизвестно: PowerPool, Inception, Gallmaker*

3. АТАКИ НА АЗИАТСКО-ТИХООКЕАНСКИЙ РЕГИОН

Северная Корея: APT37, Kimsuky, Lazarus, DarkHotel
Индия: Sidewinder, BITTER
Иран: Chafer, OilRig
Китай: APT10, Winnti, APT40
Россия: APT29, Turla, Xenotime
Вьетнам: OceanLotus
Неизвестно: APT-C-35 , BlueMushroom*, Whitefly*, Неизвестная группа, TajMahal framework

4. АТАКИ НА БЛИЖНИЙ ВОСТОК И АФРИКУ

Ближний Восток: Bahamut, APT-C-27, HEXANE*
Турция: StrongPity
Газа: Gaza Cybergang
ОАЭ: FruityArmor
Иран: OilRig, MuddyWater, APT 33, Domestic Kitten, Chafer
Северная Корея: APT37, Lazarus
Китай: Emissary Panda
Неизвестно: APT-C-38, Windshift*, Gallmaker*

5. АТАКИ НА РОССИЮ И СНГ

Ближний Восток: HEXANE*
США: Equation Group
Пакистан: Gorgon Group
Иран: MuddyWater
Северная Корея: APT37, Lazarus
Россия: Gamaredon Group, Buthtrap, APT28
Китай: Winnti
Неизвестно: PowerPool, Whitefly*

* новые группы

За вторую половину 2018 и первую половину 2019 года эксперты по информационной безопасности обнаружили большое количество ранее неизвестных групп, спонсируемых государствами. Многие из них ведут операции уже несколько лет, хотя долго время оставались незамеченными. Некоторые группы атакуют похожие цели, что приводит к конкуренции между ними и более быстрому обнаружению их действий.

Windshift

География
Ближний Восток

Вектор проникновения
Социальная инженерия
Целевой фишинг
Drive-by атаки

Инструменты
WindTail
WindTape

Группа WindShift в течение нескольких лет занималась кибершпионажем, оставаясь незамеченной. Ее отличительной чертой является тщательная подготовка к атакам.

Злоумышленники создавали фейковые страницы пользователей в соцсетях (LinkedIn, Facebook, Twitter, Instagram, Google Plus) и налаживали дружеское общение с потенциальными жертвами. Такое общение длилось от 6 месяцев до года, в течение этого периода атакующие выманивали полезную информацию.

Целями группы стали сотрудники государственных учреждений и объектов критической инфраструктуры в странах Ближнего Востока. Жертвы использовали macOS системы, под которые злоумышленники специально разработали вредоносные программы — OSX. WindTail.A, OSX.WindTail.B и OSX.WindTape.

Blue Mushroom

(aka Sapphire Mushroom, APT-C-12)

География
Китай

Вектор проникновения
Целевой фишинг

Инструменты
SinaAppEngine
ps_backdoor

Злоумышленники группы Blue Mushroom (aka Sapphire Mushroom, APT-C-12) ведут свою деятельность с 2011 года, однако стали известны лишь в середине 2018 года.

Они используют в атаках облачную инфраструктуру: например, для эксфильтрации конфиденциальной информации пользователя группа применяет Amazon AWS S3 и протоколы связи облачной инфраструктуры.

Позже злоумышленники начали использовать облачную службу Digital Ocean в качестве C&C, а также сервис SinaAppEngine (SAE) для создания собственной инфраструктуры управления C&C.

Gallmaker

География
Ближний Восток
Восточная Европа

Вектор проникновения
Целевой фишинг

Инструменты
Metasploit

Gallmaker осуществляют свои операции как минимум с декабря 2017 года, однако были обнаружены только в 2018 году. Для компрометации систем злоумышленники эксплуатируют функцию Dynamic Data Exchange (DDE) в приложении Word. Протокол DDE применяется для обмена информацией между программами пакета Office, использующими общие данные или общую память.

APT-C-36

(aka Blind Eagle)

География
Колумбия

Вектор проникновения
Целевой фишинг

Инструменты
Imminent Monitor RAT

APT-C-36 (aka Blind Eagle) — группа из Южной Америки, которая также стала известна в конце 2018 года. Цель злоумышленников — коммерческие тайны крупных компаний и правительственных учреждений, а основной вектор проникновения — вредоносные письма. Для сокрытия IP-адреса отправителя письма они использовали прокси и VPN-сервисы.

Whitefly

География
Юго-Восточная Азия
Россия

Вектор проникновения
Целевой фишинг

Инструменты
Mimikatz
Trojan.Vcrodat
Termite
Nibatad

В 2018 году стало известно об атаке на SingHealth, крупнейшую в Сингапуре организацию общественного здравоохранения, в результате которой было похищено 1,5 миллиона записей о пациентах. За инцидентом стояла группа Whitefly, остававшаяся незамеченной с 2017 года. Основными целями этой группы являются компании, расположенные в Сингапуре.

HEXANE

(aka LYCEUM)

География
Ближний Восток
Центральная Азия
Африка

Вектор проникновения
Атаки через поставщиков
Целевой фишинг
Подбор паролей
Брутфорс

Инструменты
DanBot
PoshC2
PowerShell Empire

HEXANE — новая группа среди атакующих, нацеленных на промышленные предприятия. Злоумышленники активны с середины 2018 года и акцентируют своё внимание на Ближнем Востоке, Центральной Азии и Африке.

Неизвестная группа

География
Центральная Азия

Вектор проникновения
—

Инструменты
TajMahal

Осенью 2018 года была опубликована новость об APT-фреймворке TajMahal. Он используется не менее 5 лет, однако до сих пор остается неясным, к какой конкретной группе относится этот инструмент. Фреймворк состоит из двух наборов («Tokyo» и «Yokohama») и содержит около 80 различных вредоносных модулей. Инструмент предназначен для шпионажа, но в списке подтвержденных жертв лишь одна дипломатическая миссия в Центральной Азии.

АТАКИ ЧЕРЕЗ ПОСТАВЩИКОВ (SUPPLY CHAIN)

В прошлогоднем отчете Group-IB атаки на BIOS/UEFI были названы одним из важнейших трендов. Эксперты прогнозировали, что основными целями могут стать разработчики прошивок и материнских плат прежде всего в регионе APAC, где крупные компании держат свои производства.

Атаки Winnti на производителей техники и разработчиков игр

Всего через несколько месяцев после выпуска отчета прогноз подтвердился новостью об операции под названием ShadowHammer.[1] Для доставки вредоносного кода применялась легитимная утилита ASUS Live Update, используемая для автоматического обновления BIOS, UEFI, драйверов и системных приложений.

Модифицированная утилита была подписана легитимным сертификатом "ASUSTeK Computer Inc." и размещалась на сервере компании ASUS. Аналогичные техники доставки вредоносной программы использовались и для заражения программ трех других производителей, чьи названия не разглашаются. Эти атаки связывают с китайской группой Winnti. Основной целью злоумышленников был шпионаж.

Кроме производителей техники эта же группа успешно атакует игровую индустрию: всего были заражены две игры и одна игровая платформа. Одним из производителей зараженных игр является тайская компания.

Группа Plead: фокус на Тайване

В этом же регионе был скомпрометирован сертификат корпорации D-Link, с помощью которого в 2018 году подписывали вредоносные программы, получившие название Plead. Группа, использующая бэкдор Plead, известна давно и действует преимущественно на Тайване. Чуть позже стало известно, что тот же бэкдор продолжили распространять, но уже от имени легитимного процесса AsusWSPanel.exe с цифровой подписью от "ASUS Cloud Corporation".

Неудачная атака на вендора ПО для разработчиков

В 2019 году была обнаружена атака на международную компанию, которая является вендором инструментов для разработки на различных языках программирования. Атакующим удалось скомпрометировать инфраструктуру компании и добраться до Docker-контейнеров, используемых для сборки программного обеспечения, после чего злоумышленники были обнаружены. Предположительно атакующие планировали внедрять вредоносный код в легитимные программы на этапе их сборки.

Атаки китайской группировки через Hewlett Packard (HP) и IBM

В декабре 2018 года стало известно об операции Cloudhopper, в рамках которой китайские атакующие получили доступ в сети HP и IBM. Затем этот доступ был использован для проникновения в сети клиентов, обслуживающихся у этих компаний.

Жертвами стали предприятия из 12 стран (включая Бразилию, Германию, Индию, Японию, Объединенные Арабские Эмираты, Великобританию и Соединенные Штаты) в следующих отраслях: финансы, электроника, медицинское оборудование, биотехнологии, автомобилестроение, добыча полезных ископаемых и разведка нефти и газа.

[1] https://securelist.com/operation-shadowhammer/89992/

ОБРАТНЫЙ ВЗЛОМ (HACKING BACK)

Одной из мер активного противостояния атакующим является обратный взлом, когда злоумышленники сами становятся жертвами. Вопрос о том, могут ли частные компании проводить подобные операции, обсуждается давно, и на текущий момент обратный взлом разрешен только специальным государственным службам. В 2019 году участились случаи, когда в результате ответных атак информация об инструментах атакующих стала появляться в открытом доступе.

В марте 2019 года в Telegram-канале "Lab Dookhtegan" была опубликована информация об иранской группе OilRig (APT34): исходный код инструментов, жертвы хакеров, имена, фамилии, ссылки на соцсети и досье на якобы действующих участников группы, включая руководителей. Пользователь под ником "Lab Dookhtegan" утверждает, что он является бывшим участником OilRig и имеет отношение к разработке “DNSpionage”.

Среди опубликованных инструментов присутствуют:

- Glimpse (новая версия PowerShell-трояна, который эксперты Palo Alto Networks называют BondUpdater);
- PoisonFrog (старая версия BondUpdater);
- HyperShell (веб-шелл, известный Palo Alto Networks как TwoFace);
- HighShell (еще один веб-шелл);
- Fox Panel (фишинговый набор);
- Webmask (основной инструмент, использованный в кампании DNSpionage).

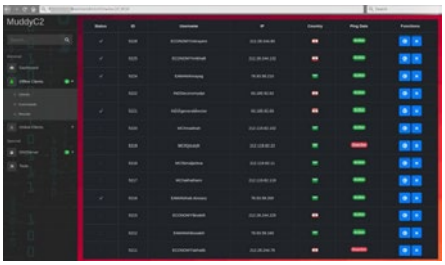
Опубликованные данные о 66 жертвах APT34 были взяты с C&C-серверов группы и содержали в том числе учетные данные от внутренних серверов и IP-адреса пользователей. В основном в этот список вошли компании и организации из стран Ближнего Востока, Африки, Восточной Азии и Европы.

Также Lab Dookhtegan опубликовал информацию о прошлых операциях, включая списки IP-адресов и доменов, где группировка ранее хостила веб-шеллы и другие оперативные данные. На 18 апреля 2019 года было известно о 125 веб-шеллах.

В июне была опубликована информация об атаке, проводимой группой Turla против ближневосточной организации с января 2018 года. В ходе атаки злоумышленники использовали инфраструктуру OilRig для загрузки на машину жертвы модифицированной версии Mimikatz, которая является уникальной для группы Turla.

По аналогии с кейсом OilRig (APT34) через Telegram началось распространение информации о другой группе, которую связывают с Ираном — MuddyWater. Были опубликованы исходный код инструмента, написанного на языке Python, и его система управления.

Данный инструмент позволяет сгенерировать полезную нагрузку, которую можно внедрить в макрос. При выполнении этого макроса жертва будет подключаться к удалённому серверу для загрузки дополнительных модулей. Также этот инструмент позволяет доставить полезную нагрузку второго этапа — например, .sct, .hta и PowerShell.



В июне 2018 года США ввели санкции против российского НИИ «Квант», а в декабре от имени группы Digital Revolution в публичный доступ были выложены сведения и документы, подтверждающие успешную компрометацию инфраструктуры НИИ «Квант». В июле 2019 года аналогичная ситуация случилась с другим подрядчиком ФСБ: от имени той же группы были выложены некоторые похищенные документы и снимки экрана, подтверждающие компрометацию инфраструктуры «Сайтэк».

В июле 2019 года группа Intrusion Truth выложила сведения о китайских правительственных хакерах, которые входят в группу APT17. В августе 2018 года та же группа обнародовала данные трех граждан КНР, которые якобы являлись участниками APT10.

В августе 2019 года на конференции BlackHat компания FireEye представила результаты исследования, где они подробно описали действия группы APT41. Эта группа имеет много пересечений с APT17, из-за чего многие эксперты рассматривали эти группы как одну (под названием Winnti или BARIUM).

ПЕРЕСЕЧЕНИЯ ИНСТРУМЕНТОВ КИТАЙСКИХ ПРОПРАВИТЕЛЬСТВЕННХ ГРУППИРОВОК[1]

Вредоносное ПО	APT1	APT3	APT10	APT17	APT18	APT19	APT40	APT41
BLACKCOFFEE				●			●	●
CHINA CHOPPER				●			●	●
COLDJAVA								●
HIGHNOON				●				●
HIGHNOON.BIN				●				●
HIGHNOON.LITE								●
HOMEUNIX	●		●	●	●			●
JUMPALL				●				●

[1] https://content.fireeye.com/apt-41/rpt-apt41

ТЕЛЕКОММУНИКАЦИИ

угрозы для отрасли

ГРУППЫ, АТАКУЮЩИЕ ТЕЛЕКОММУНИКАЦИОННЫЙ СЕКТОР

Телекоммуникационный сектор является одним из приоритетных для прогосударственных атакующих. Скомпрометировав телекоммуникационную компанию, злоумышленники получают возможность развивать атаки на её клиентов с целью шпионажа или саботажа.

APT10

Одной из самых крупномасштабных операций за рассматриваемый период стала кампания "Operation Soft Cell", предположительно проводившаяся китайской проправительственной группировкой APT10. Кампания ведется по меньшей мере с 2012 года.

Целью злоумышленников было получение CDR-записей (от англ. Call Detail Record — подробная запись о вызове) крупных телекоммуникационных провайдеров. Им удалось скомпрометировать имена и пароли пользователей, а также данные выставления счетов, подробные записи о вызовах, учетные данные, почтовые серверы, геолокацию пользователей и др.

Для получения доступа к сетям телекоммуникационных компаний использовалась модифицированная версия веб-оболочки China Chopper. Сам взлом сетей производился через процесс ОС Windows w3wp.exe, запускающий веб-приложения и отвечающий за обработку запросов, отправленных на веб-сервер.

Злоумышленники использовали украденные учетные данные для создания мошеннических учетных записей пользователей домена с высоким уровнем привилегий. Далее они использовали эти учетные записи либо разворачивали Poison Ivy RAT для поддержания доступа к скомпрометированным ресурсам.

MuddyWater

Проправительственные хакеры из MuddyWater получили доступ к локальной сети Korek Telecom — оператора мобильной связи в Эрбиле (Ирак). Компрометация оператора была промежуточным этапом атаки на нефтегазовую компанию Missan Oil Company, которая предположительно является клиентом Korek Telecom.

APT33 (aka Elfin, Magnallium)

В конце 2018 года APT33 (aka Elfin, Magnallium) снова начали проводить атаки с обновленным инструментом Shamoon (первая версия трояна была обнаружена ещё в 2012 году, а вторая версия и волна атак с ней в 2017 году). Shamoon-3 позволяет перезаписывать MBR, разделы и файлы в системе случайно сгенерированными данными.

Первой жертвой стала нефтегазовая компания Saipem SpA, однако випер трояна также был обнаружен в атаках на нефтяные, газовые, телекоммуникационные, энергетические и правительственные организации на Ближнем Востоке и в Южной Европе.

Chafer (aka APT39)

Цель группы Chafer (aka APT39) — сбор персональных данных для проведения дальнейших операций по мониторингу и отслеживанию пользователей в интересах иранского правительства. Кроме того, собранные данные могут быть использованы как вектор для будущих атак.

Для проникновения в сеть группа использует фишинговые письма с вредоносными ссылками или вложениями, открытие которых приводит к установке бэкдора POWBAT. Также злоумышленники компрометируют целевые веб-серверы и устанавливают на них веб-шеллы, такие как ANTAK и ASPXPY. Еще один вектор — использование украденных учётных записей для компрометации Outlook Web Access.

HEXANE

Недавно обнаруженная группа HEXANE атакует телекоммуникационные компании на Ближнем Востоке, в Центральной Азии и Африке как промежуточное звено в “supply chain”-атаке. Таким образом они пытаются добраться до критической инфраструктуры организаций, являющихся клиентами этих телеком-компаний.

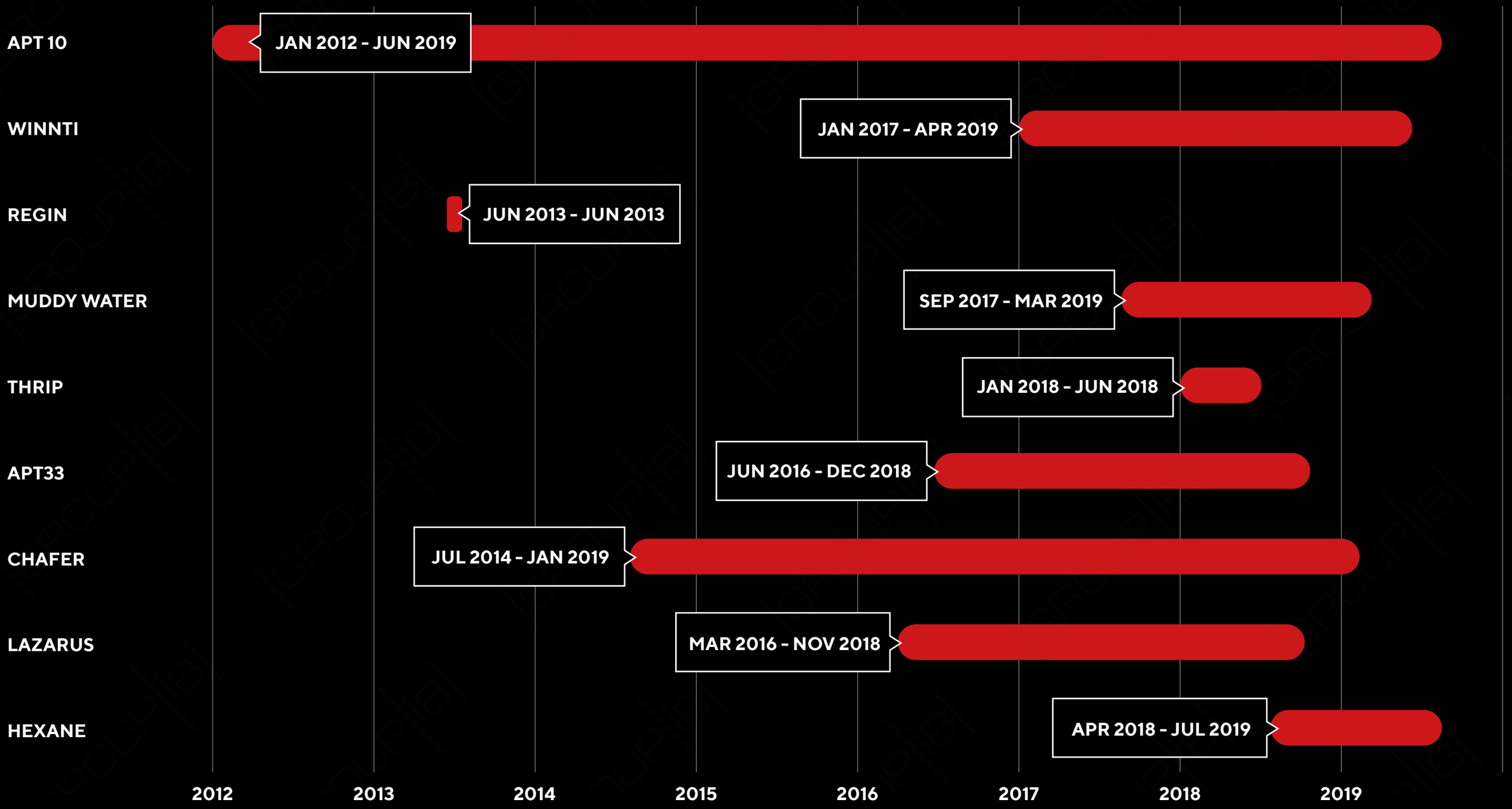
Lazarus

Группа Lazarus также занимается шпионажем в телекоммуникационной отрасли с использованием нового бэкдора Rising Sun. Он собирает и передает на управляющий сервер данные о зараженной машине: IP-адреса, информацию о сетевых устройствах, название и версию ОС, данные о системе, имя пользователя и т.д. Вероятно, распространение этого бэкдора является первой стадией атаки, за которой может следовать догрузка дополнительных вредоносных программ.

Thrip

Китайская хакерская группа Thrip известна атаками с целью шпионажа и саботажа. В телекоммуникационной отрасли их целями стали компании-разработчики технологий спутниковых коммуникаций. Злоумышленники применяют технику "living off the land" — использование легитимных локальных приложений (PsExec, Mimikatz, WinSCP и LogMeIn) во вредоносных целях для установки троянов.

ГРУППЫ, АТАКУЮЩИЕ ТЕЛЕКОММУНИКАЦИОННЫЙ СЕКТОР



ВЫЗОВЫ, СВЯЗАННЫЕ С ПОВСЕМЕСТНЫМ РАСПРОСТРАНЕНИЕМ 5G

Планируется, что стандартизация 5G завершится к 2021 году, но первые сети уже построены. Более того, сейчас идет активная конкурентная борьба не только между технологическими гигантами, но и между странами (лидируют США и Китай).

Первопроходцы установят стандарты и практики, которые будут внедряться игроками, идущими следом. Странам-лидерам это принесет миллиардные доходы, создание новых рабочих мест и лидерство в технологических инновациях по аналогии с тем, как это было с 2/3/4G сетями.

Угрозы, связанные с архитектурными особенностями 5G

Основная особенность 5G (в отличие от 1/2/3/4G) заключается в том, что это больше программная, чем аппаратная платформа. Оборудование традиционных сетей мобильной связи заменяется на программные сущности, работающие в дата-центрах на стандартных серверах и виртуальных машинах. Кроме виртуальных машин для реализации программных функций будут использоваться программные контейнеры, а также программная архитектура микросервисов. Именно эти архитектурные особенности беспокоят специалистов по безопасности: теперь все угрозы для серверных и программных решений становятся актуальными и для операторов 5G сетей.

Увеличение поверхности атаки при компрометации инфраструктуры

Network Slicing — это технология внутри 5G сетей, которая позволяет на базе единого пула сетевых ресурсов производить логическое разделение сетей. Этот подход используется для оказания различных типов услуг 5G: передачи веб- или голосового трафика, трафика для приложений дополненной реальности и т.д.

Доступ к таким «слайсам» получают разные компании, которые хотят оказывать услуги на базе 5G. Несмотря на то что пул адресов логически изолирован, доступ к нему значительно увеличивает поверхность атаки, что может привести к компрометации всей инфраструктуры.

Потенциально Network Slicing открывает для APT-групп возможность проведения атак, связанных с BIOS/UEFI, side channel, supply chain. Целями прогосударственных хакеров могут быть шпионаж или саботаж для подрыва доверия к конкурентному решению.

Опубликованные исследования об уязвимостях 5G

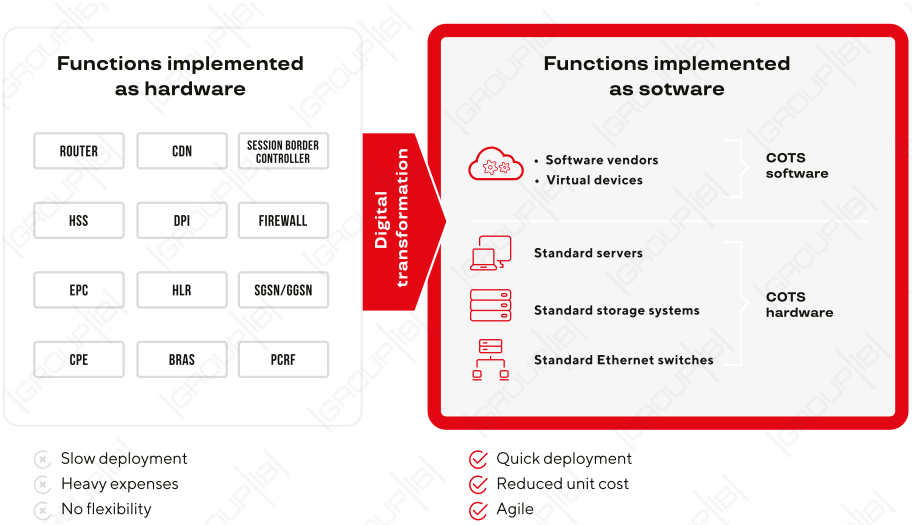
Новые вызовы и проблемы безопасности 5G сетей волнуют экспертов во всем мире. За последний год было опубликовано несколько исследований на эту тему:

- В ноябре 2018 года команда исследователей из Швейцарии, Франции и Великобритании выявила проблемы с протоколом безопасности 5G, известным как Authentication and Key Agreement (AKA).
- В феврале 2019 года группа университетских исследователей обнаружила уязвимости сотовой сети, которые влияют на протоколы LTE (как 4G, так и 5G). Согласно статье, удаленный атакующий может обойти защитные механизмы этих протоколов и снова включить устройства перехвата IMSI (такие как Stingrays) для перехвата телефонных звонков пользователей и отслеживания их местоположения.
- ToRPEDO ("TRacking via Paging mEssage DistributiOn) — это наиболее опасная атака, использующая протокол пейджинга. Она позволяет удаленным атакующим проверять местоположение устройства жертвы, вводить поддельные пейджинговые сообщения и проводить атаки типа «отказ в обслуживании» (DoS). ToRPEDO затрагивает как 4G, так и текущую версию протокола 5G LTE. Исследователи заявили, что проверили ToRPEDO против 3 канадских поставщиков услуг и всех поставщиков услуг США.
- PIERCER (Persistent Information ExposuRe by the CorE networRk) атака позволяет злоумышленнику связать уникальный IMSI устройства жертвы с его номером телефона.

Новый масштаб «традиционных» угроз

Более широкое внедрение 5G значительно увеличит количество традиционных атак, с которыми провайдеры сталкиваются в последние годы:

- DDoS-атаки — мощность и частота таких атак значительно вырастут благодаря большому количеству небезопасных устройств и широкой полосе пропускания.
- Проксирование — еще один популярный метод мошенничества. Превращая скомпрометированные устройства в прокси-серверы, злоумышленники могут совершать действия с большого пула IP-адресов. Это позволяет обходить ограничения систем безопасности для скрэпинга, автоматизированного мошенничества, накрутки разного рода трафика. Подключение IoT-устройств к сетям 5G значительно увеличит количество небезопасных устройств, которые могут быть использованы для проксирования.
- Распространение вредоносных программ через взломанные устройства — популярная практика, и она будет только масштабироваться с развитием 5G сетей.



BGP HIJACKING И SS7-УГРОЗЫ

Об использовании уязвимостей SS7 в целях шпионажа и мошенничества известно уже давно, однако атаки этого типа продолжаются. Так, в январе 2019 года клиенты британского Metro Bank стали жертвой обхода 2FA. Использовав уязвимости протокола SS7, киберпреступники могли перехватывать текстовые сообщения, которые банк отправлял клиентам для авторизации транзакций. Metro Bank немедленно проинформировал власти об инциденте, однако другие банки этого не сделали.

В начале этого отчета мы уже приводили несколько примеров с BGP hijacking, однако таких инцидентов было значительно больше.

Прекращение работы португальского провайдера Bitcanal

25 июня 2018 года независимый специалист по безопасности Ronald Guilmette обнаружил подозрительную активность, связанную с множественными случаями перехвата Интернет-трафика средствами BGP. Перехват осуществлял португальский провайдер Bitcanal, в результате чего транзитные провайдеры прекратили работу с ним, лишив его международного транзита.

В ходе одного из перехватов Bitcanal анонсировал подсети, принадлежащие Beijing Jingdong 360 Degree E-commerce. Отключение Bitcanal повлекло за собой отключение от транзита провайдера Routed Solutions (AS39536), который, предположительно, являлся клиентом или дочерней организацией Bitcanal.

Перехват трафика для атаки на серверы WorldPay, Datawire и Vantiv

6 июля 2018 года провайдер "Digital Wireless Indonesia" (AS38146) анонсировал следующие префиксы в течение 30 минут:

64.243.142.0/24 – "Savvis", 64.57.150.0/24 – "Vantiv, LLC", 64.57.154.0/24 – "Vantiv, LLC", 69.46.100.0/24 – "Q9 Networks Inc.", 216.220.36.0/24 – "Q9 Networks Inc."

Затем эти же пять префиксов были анонсированы 10 июля 2018 года в течение 30 минут провайдером Malaysian operator Extreme Broadband (AS38182), а затем повторно спустя час, но уже в течение 15 минут.

11 июля 2018 года "Malaysian operator Extreme Broadband" (AS38182) начал анонс нового набора префиксов:

209.235.25.0/24 – "Mercury Payment Systems", 63.111.40.0/24 – "Mercury Payment Systems", 8.25.204.0/24 – "Level 3", 12.130.236.0/24 – "CERFnet"

12 июля "Malaysian operator Extreme Broadband" (AS38182) начал анонс тех же пяти префиксов, что были анонсированы в первом зафиксированном инциденте:

64.243.142.0/24 – "Savvis", 64.57.150.0/24 – "Vantiv, LLC", 64.57.154.0/24 – "Vantiv, LLC", 69.46.100.0/24 – "Q9 Networks Inc.", 216.220.36.0/24 – "Q9 Networks Inc."

Однако в данном случае перехват длился значительно дольше: почти три часа провайдер анонсировал эти префиксы для перехвата трафика.

Затем спустя час тот же провайдер анонсировал следующие блоки в течение 10 минут:

199.7.68.0/24–"UltraDNS Corporation", 199.7.69.0/24–"UltraDNS Corporation", 204.74.108.0/24 – "UltraDNS Corp", 204.74.109.0/24 – "Internet Media Network", 204.74.114.0/24 – "Internet Media Network", 204.74.115.0/24 – "Internet Media Network", 65.118.49.0/24 – "CenturyLink"

Перехваченный трафик был предназначен для финансовых компаний и компаний, занимающихся обработкой платежей: скорее всего, злоумышленников интересовала платежная информация.
Passive DNS показал, что между 10 и 13 июля поддомены datawire.net соответствовали IP-адресу 45.227.252.17 (AS58271, "VSERVER-AS", Panama).

Многочисленные случаи перехвата трафика компанией China Telecom

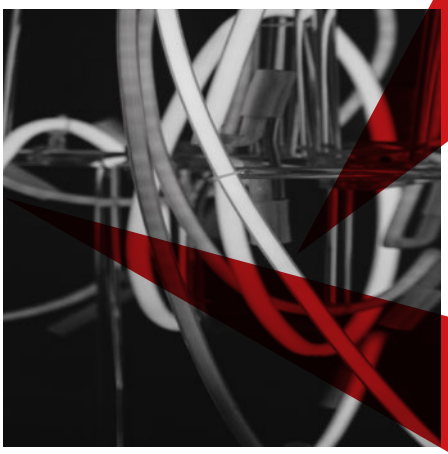
Специалисты Военно-морского колледжа США и Тель-Авивского университета (Израиль) опубликовали доклад, согласно которому китайская телекоммуникационная компания China Telecom осуществляла перехват трафика средствами BGP в течение нескольких лет.

К примеру, в 2016 году компания перенаправила трафик правительственных сетей Канады и Южной Кореи на свои точки присутствия (Point of presence, POP) в Торонто (Канада). Затем трафик был перенаправлен на точки присутствия China Telecom на Западном побережье США, а затем – в Китай и Южную Корею.

В 2017 году компания перехватила трафик между Японией и Скандинавией, проходящий через территорию США, и отправила его на почтовый сервер, принадлежащий крупной тайваньской финансовой организации. Согласно докладу, после перехвата трафика, его расшифровки и изучения China Telecom отправляет трафик в сети назначения с небольшой задержкой.

Атака на публичные DNS-серверы Тайваня

15 мая 2019 года исследователи сообщили о том, что была зафиксирована утечка маршрутов BGP. Она была нацелена на перехват трафика, предназначенного для DNS-сервиса и управляемого Taiwan Network Information Center (TWNIC). 8 мая 2019 года трафик был перенаправлен в сети бразильского провайдера "Fibra Plus Telecomunicacoes LTDA" (AS268869), инцидент продолжался три с половиной минуты.
8 мая "Fibra Plus Telecomunicacoes LTDA" (AS268869) начал анонс префикса 101.101.101.0/24, который им не принадлежит. Это была попытка перехвата трафика, предназначенного для префикса DNS-сервиса Quad101, управляемого TWNIC.



ЭНЕРГЕТИЧЕСКИЙ СЕКТОР

угрозы для отрасли

В случае с энергетическим сектором целью злоумышленников обычно является шпионаж, однако некоторые атаки приводили к отключению объекта критической инфраструктуры.

3 страны	Незаметные игроки	Ближний Восток
Исследователи связывают атаки на энергообъекты, в основном, с Ираном, Россией и Северной Кореей.	Stuxnet, Dugu, Flame и атака на Венесуэлу подтвержают, что наиболее опасные угрозы еще не выявлены.	Полигон для испытаний инструментов атак на энергетику со времен Stuxnet и до настоящего времени.

ГРУППЫ, АТАКУЮЩИЕ ЭНЕРГЕТИЧЕСКИЙ СЕКТОР

HEXANE

В 2018 году стало известно о новой группе HEXANE, участники которой фокусируются на системах промышленного контроля и атакуют предприятия нефтегазовой отрасли на Ближнем Востоке (в основном, в Кувейте). Преступники обходят защиту через доверенных поставщиков, компрометируя устройства, программное обеспечение и телекоммуникационные сети, используемые целевыми объектами.

LeafMiner

Хакеры из LeafMiner, предположительно базирующиеся в Иране, используют в своих атаках как общеизвестные инструменты (например, Inception Framework), так и программы собственной разработки (Trojan.Imecab и Backdoor.Sorgu по классификации Symantec). Основные цели группировки находятся на Ближнем Востоке.

Для проникновения в целевую организацию LeafMiner используют атаки типа watering hole: встраивают вредоносные ссылки в скомпрометированные сайты, чтобы открыть соединение по SMB-каналу и похитить учетные данные пользователей Windows. LeafMiner не были замечены за нарушением работы ICS, пока они получали только первичный доступ к учетным данным организации.

Xenotime

Хакерская группа Xenotime в 2018 году также переключилась на энергосети. Она получила известность благодаря своей вредоносной программе Triton (он же Trisis), который используется для атак на контроллеры систем инструментальной безопасности Triconex (Triconex Safety Instrumented System, SIS) производства Schneider Electric.

Позже стало известно, что Xenotime доработали свою вредоносную программу, и новая версия способна атаковать целый ряд систем противоаварийной защиты (ПАЗ). Это отдельные средства защиты, которые подключаются к управлению производственными процессами в случаях, когда условия становятся небезопасными (например, избыточное давление, превышение скорости или перегрев).

Lazarus

23 сентября была опубликована информация о появлении нового набора инструментов у хакерской группы Lazarus. Они были использованы в атаках на индийские компании в период с конца 2018 по весну 2019. Злоумышленники успешно скомпрометировали учетную запись одного из руководителей в головном офисе ядерной корпорации в APAC.

Перечисленные выше группы стали открытием, однако не стоит забывать о двух уже известных — "BlackEnergy" и "Dragonfly". Затишье с их стороны может быть связано с тем, что хакеры перерабатывают свои инструменты и техники для совершения новых атак.

BlackEnergy

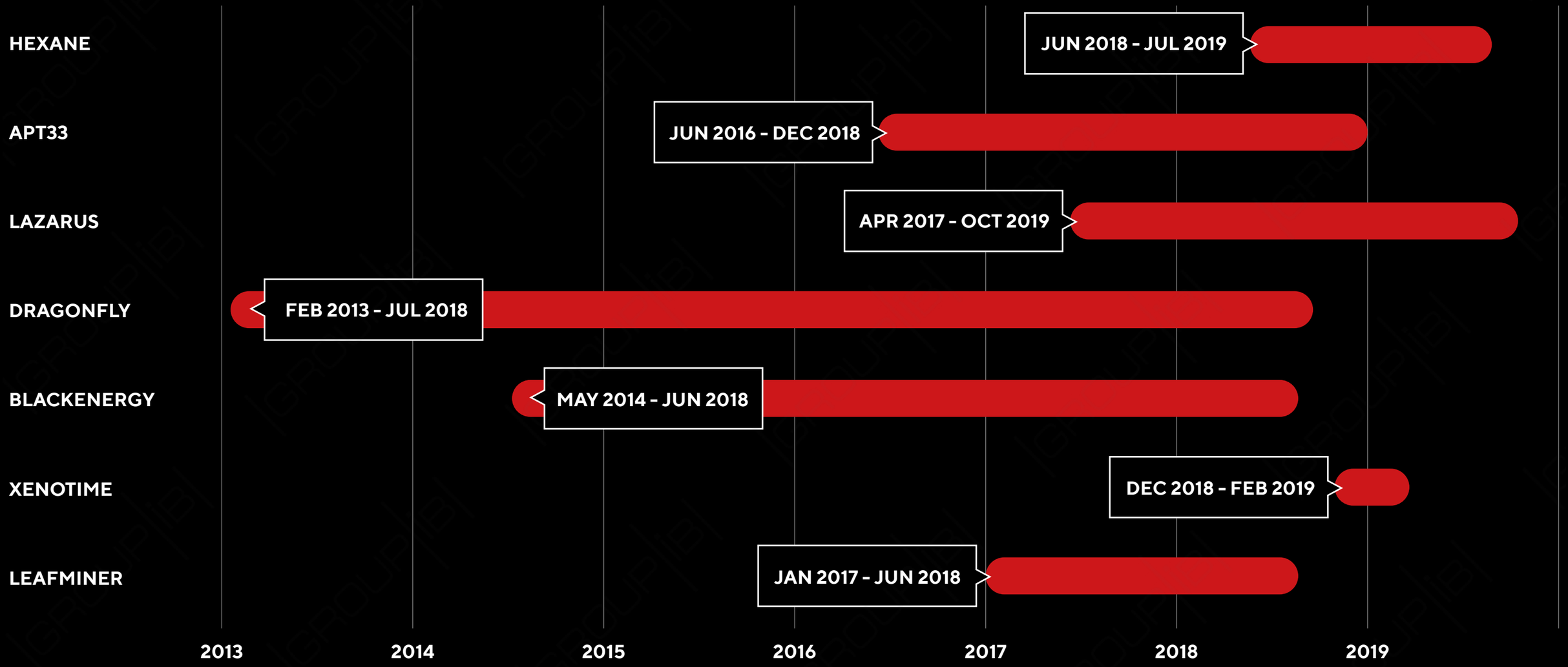
Одна из самых «подкованных» групп, атакующих энергетический сектор, это BlackEnergy. Они не раз нарушали работу предприятий электроэнергетики. Группа ориентируется на ICS/SCADA системы по всему миру, но главное отключение произошло в конце 2015 года, когда атака нарушила подачу электричества в Ивано-Франковской области (Украина).

Основным инструментом в руках этих хакеров остается Industroyer или CRASHOVERRIDE, который предоставляет возможность удаленного управления remote terminal units (RTU), которые отвечают за физическое размыкание/замыкание сети. Однако в 2017 и 2018 году арсенал группы пополнился вредоносными программами BadRabbit и VPNFilter соответственно. Последняя заточена под атаку на роутеры и содержит модуль для обнаружения SCADA-систем.

Dragonfly

Группа Dragonfly, которую специалисты причисляют к спонсируемым Россией, сосредоточена на сборе данных с энергетических и промышленных объектов. Злоумышленники используют фишинговые письма при атаках на отдельных сотрудников, а также watering hole атаки для более массовой кражи корпоративных учетных данных. В арсенале Dragonfly также присутствуют такие инструменты как Goodor, DorShel и Karagany.

ГРУППЫ, АТАКУЮЩИЕ ЭНЕРГЕТИЧЕСКИЙ СЕКТОР



ФИНАНСОВЫЙ СЕКТОР

угрозы для отрасли

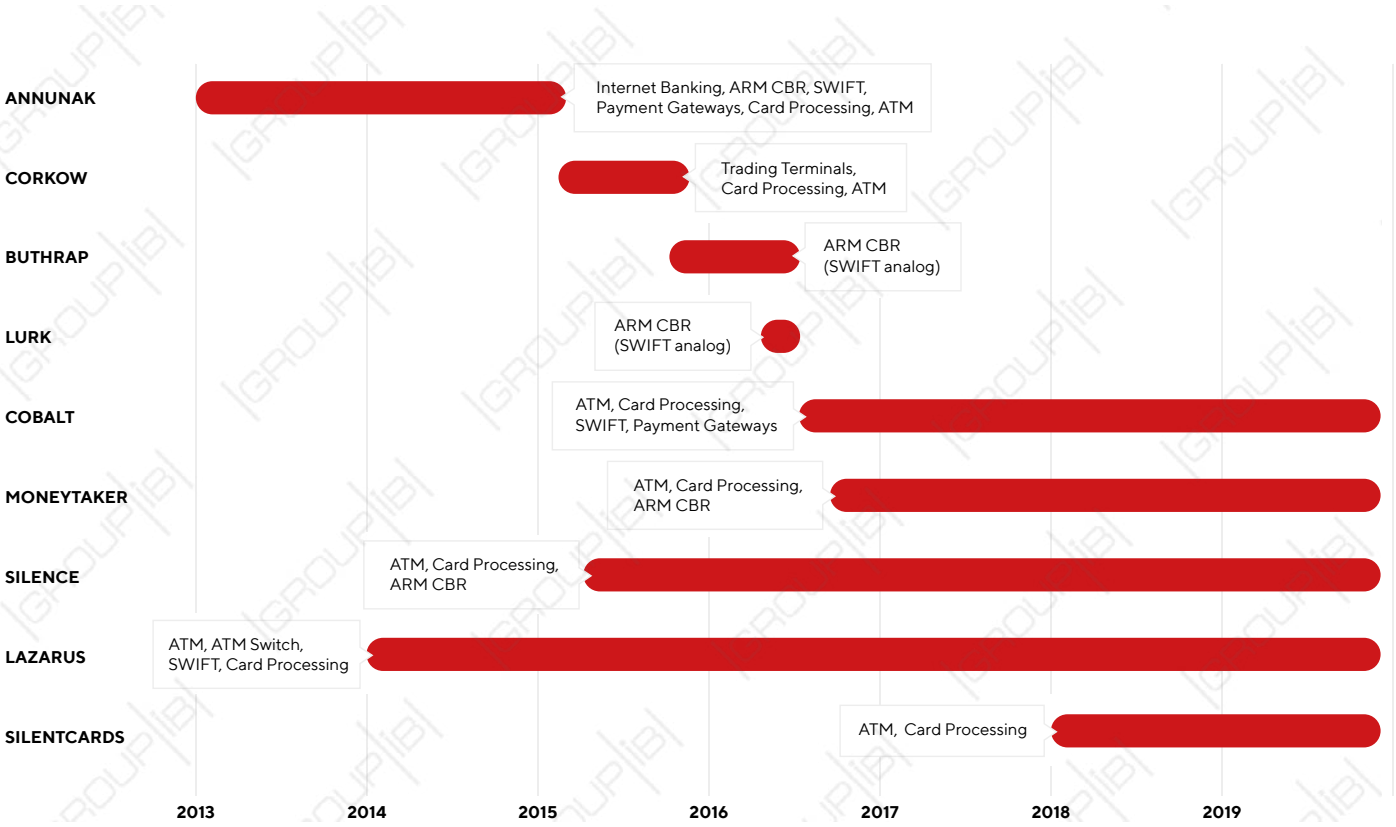
ЭВОЛЮЦИЯ ГРУППИРОВОК И ПОЯВЛЕНИЕ НОВОГО ИГРОКА

5 групп из 3 стран	**3 из 5 групп**	**Lazarus**
проводят целенаправленные атаки на финансовые учереждения	являются русскоговорящими и действуют в разных регионах	применяет наиболее интересные методы проникновения и хищения

На текущий момент существует 5 групп, представляющих реальную опасность для банков в разных регионах мира – они используют разные векторы атак, способны проникнуть в изолированные системы и вывести деньги. Практически каждая из них имеет богатую историю, и некоторые антивирусные и консалтинговые компании придумывают им новые названия, однако это не влияет на общее количество групп. На таймлайне отмечена история активности этих хакеров в банковской индустрии, атаки с целью саботажа или шпионажа здесь не отображены.

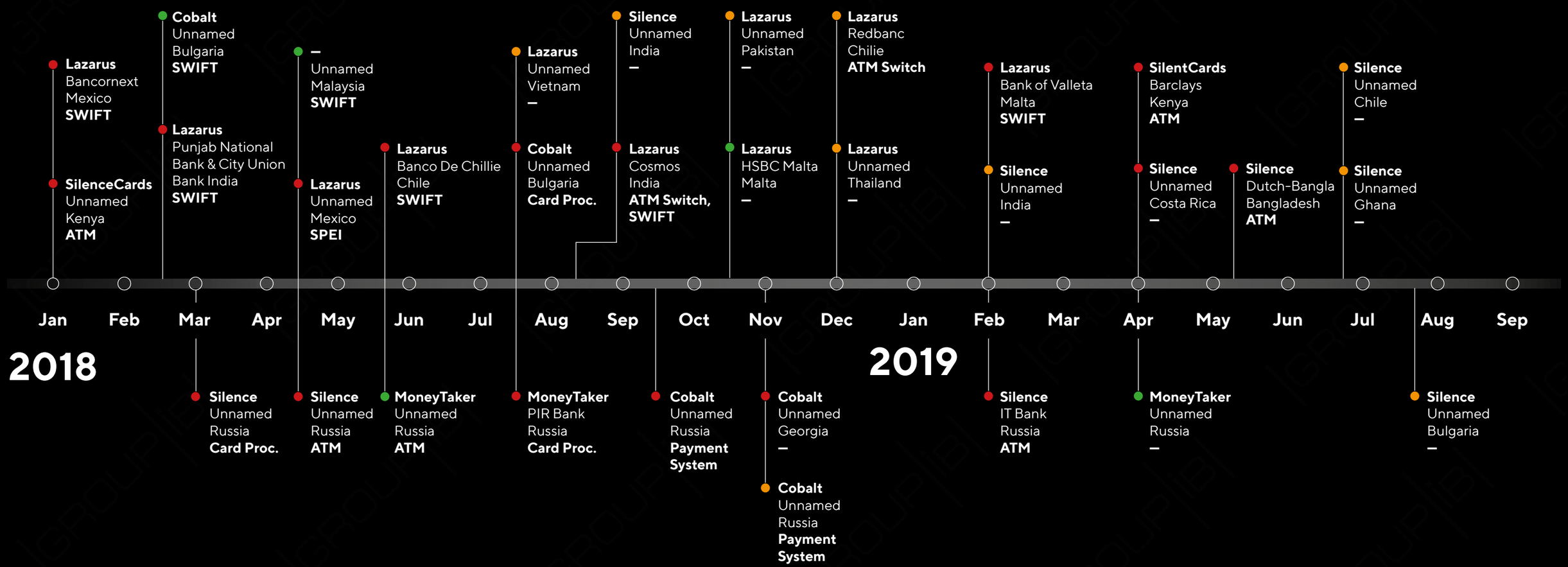
«Большая тройка» хакерских групп — Cobalt, MoneyTaker, Silence – без исключения является русскоговорящей. Группа SilentCards из Кении попала в поле зрение аналитиков только в 2018 году, а Lazarus принято считать группировкой, спонсируемой Северной Кореей.

До 2018 года русскоязычные группы чаще атаковали банки в России и СНГ, однако за последний год этот тренд кардинально изменился. Теперь злоумышленники фокусируются в основном на иностранных банках и организациях



ТАЙМЛАЙН И ГЕОГРАФИЯ ЦЕЛЕНАПРАВЛЕННЫХ АТАК НА БАНКИ ЗА 2018-2019 гг

- Названия финансовых учреждений указаны только в случаях, когда они были раскрыты публично. Указание названий других жертв мы считаем неэтичным.
- В случае с группой Lazarus по некоторым атакам атрибуция может быть неточной в связи с отсутствием технических деталей об инциденте.



- Ограблен
- Неизвестно
- Предотвращено

Silence

География

Россия
СНГ
Азиатско-Тихоокеанский регион
Ближний Восток
Восточная Европа
Африка
Латинская Америка

Метод хищения

АТМ-троян (xfs-disp)
Карточный процессинг
АРМ КБР

Вектор проникновения

Фишинг

Инструменты

Silence Trojan
Silence Proxybot
Atmosphere
xfs-disp.exe
Ivoke
EDA — EmpireDNSAgent (Empire+dnscat2)
PowerMTA
Farse
Cleaner
Metasploit
Mimikatz
winexe
RAdmin

Подробнее о Silence в полном техническом исследовании Group-IB

География

Silence – одна из самых быстроразвивающихся группировок. В начале своей деятельности злоумышленники использовали Россию как тестовый полигон, чтобы подготовиться к международной экспансии:

- Первая половина 2018 года – основная активность и первые успешные атаки в России.
- Осень 2018 года – первые массовые атаки в других странах, в основном на Ближнем Востоке и в Юго-Восточной Азии.
- Февраль 2019 года – активность в России резко снизилась, и внимание Silence полностью переключилось на финансовый сектор в Болгарии, Индии, Бангладеш, Чили, Коста-Рике, Гане.
- Прогноз на вторую половину 2019 и 2020 год – география атак может быть сильно расширена за счет коллаборации с другими атакующими. В частности, как показали реагирования Group-IB в ряде банков, Silence уже начала приобретать установки своего трояна в банки через другую группу – TA505.

Метод хищения

Целями Silence в последних инцидентах были банкоматы — они устанавливали на них новую версию АТМ-трояна и получали возможность удаленного управления диспенсером.

Однако, стоит отметить, что у этой группы есть опыт совершения хищений через систему управления банковскими картами, который мог быть успешно применен в атаке на Dutch-Bangla банк и ранее на банки в РФ.

Метод проникновения

Эта группа использует только один способ проникновения в банк – хорошо подготовленные, но не целенаправленные фишинговые письма. Особенность подготовительного этапа атаки Silence — рассылка «тестовых» писем, не содержащих вредоносного контента. Это позволяет актуализировать базу и понять, какие решения по кибербезопасности используются в организации. Фишинговые письма с вредоносной нагрузкой рассылаются уже по проверенной и актуальной базе.

В середине 2019 года Silence приобрели доступ в целевые банки у группы TA505, это было подтверждено экспертами Group-IB в рамках реагирования на инцидент в болгарском банке. Вероятнее всего, Silence откажется от собственных рассылок и продолжит пользоваться услугами сторонних групп.

Инструментарий

Основным инструментом группы является их собственная разработка — одноименный фреймворк Silence. В конце 2018 года они значительно модернизировали его загрузчик Ivoke:

- стал бесфайловым (написан на Powershell);
- научился более эффективно обходить средства обнаружения;
- начал более активно собирать данные о целевой системе для принятия решения о целесообразности развития атаки;
- были удалены команды, указывающие на русскоязычные слова;
- добавилась возможность передачи файлов с зараженной системы на сервер управления;
- изменился протокол взаимодействия с сервером управления.

Для проксирования трафика группа продолжает использовать Silence.Proxy, однако вместе с ним применяет и другие средства удаленного управления: DarkVNC и модифицированную версию AmmyAdmin, получившую название FlawedAmmyy. Это полнофункциональной RAT, позволяющий получить административный контроль над зараженным устройством для мониторинга активности пользователей, профилирования системы и кражи учетных данных. FlawedAmmyy используется не только группой Silence — в частности, в последних кампаниях его применяют хакеры TA505.

Также в 2019 году для создания скрытых каналов группа начала использовать троян, основанный на проектах DNScat2 и Empire. Он был выявлен экспертами Group-IB в ходе реагирований на инциденты и получил название EmpireDNSAgent или просто EDA. В атаках на банки Чили, Коста-Рики, Ганы и Болгарии он догружался вместе с основным трояном Silence. Main.

Ранее для атак на банкоматы Silence использовали исключительно свой уникальный троян Atmosphere, однако в 2019 году они перешли на новую программу. После успешного тестирования в России на «ИТ-банке» (Омск) новый инструмент предположительно применялся для хищений в бангладешском банке Dutch-Bangla.

Cobalt

География

Россия
Казахстан
Грузия
Европа
Индия
Греция

Метод хищения

ATM-троян
Карточный процессинг
Платежные шлюзы
SWIFT
Локальные внутрибанковские системы

Вектор проникновения

Фишинг
Атаки через поставщиков
Скрытая загрузка (driveby)

Инструменты

CobInt
JS-backdoor
SSH-backdoor
Cobalt Strike
alexusMailer
SoftPerfect Network Scanner
Eternal Blues
EternalPunch
Radmin
AmmyAdmin
TeamViewer
RPIVOT
Mimikatz
PetrWrap
InfoStealer v. 0.2

Подробнее о Cobalt в полном техническом исследовании Group-IB

География

Последнее успешное хищение группы Cobalt в России было зафиксировано в ноябре 2018 года, и только в июле 2019 года они снова начали предпринимать попытки проникнуть в российские банки. Во время этого перерыва злоумышленники сфокусировались на других странах, рассылая фишинговые письма от имени European Banking Federation, Diebold Nixdorf, Interkassa e-payment system, SEPA Europe, SWIFT.

Отдельно стоит отметить рассылки от имени некоторых банков в Европе, Греции, Индии, Казахстане: они велись с почтовых серверов этих компаний, что свидетельствует об успешной компрометации самих банков или адресов электронной почты их сотрудников.

Несмотря на рассылки и другие следы активности, в публичном пространстве ничего не известно об успешных хищениях этой группы за пределами России. Однако это свидетельствует скорее об отсутствии процедур информирования в атакуемых регионах, чем об отсутствии атак.

Метод хищения

В 2018 году группа использовала разные методы хищений: SWIFT, локальные системы межбанковских переводов, карточный процессинг и платежные шлюзы систем моментальных денежных переводов. При этом опыт хищений через платежные шлюзы есть только у Cobalt, и применяли они его только в России.

Метод проникновения

Для проникновения в инфраструктуру группа Cobalt использует фишинг от имени банков, финансовых организаций и их партнеров. Иногда уже после успешной атаки на банк они продолжают использовать полученные доступы, рассылая фишинговые письма от имени жертвы и с ее почтовых серверов.

В октябре 2018 года эксперты Group-IB зафиксировали атаку с поддоменов российского государственного портала — происходили редиректы на серверы с RIG Exploit Kit, и на компьютеры жертв загружался CobaltStrike Beacon. Как было установлено впоследствии, в результате этой атаки был ограблен один из банков в СНГ.

С января 2019 года Cobalt начали использовать новую схему распространения вредоносного кода. Они стали рассылать письма от имени людей, хорошо известных в финансовых кругах, используя адреса на бесплатных почтовых сервисах.

Другим важным изменением в письмах стало улучшение их качества. Если раньше это был плохо оформленный текст без документов-приманок, то в последних атаках письма стали выглядеть лучше, а вредоносные вложения сопровождаются качественными приманками.

Инструментарий

Первым в атакуемую компанию попадает модульный бэкдор CobInt. Он запускает модули, отвечающие за сбор информации о системе, а также загрузку и запуск основного инструмента для развития атаки. Основным инструментом остается Cobalt Strike, который группа использует с начала своей активности.

Другой используемый инструмент — это JS-бэкдор, который позволяет загружать и запускать PE-файлы, а также выполнять скрипты. Трояны для Windows, Linux и банкоматов, которыми располагает Cobalt, в анализируемый период не использовались.

MoneyTaker

География

Россия

Метод хищения

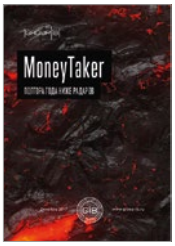
ATM-трояны
APM КБР

Вектор проникновения

Фишинг
Атаки через поставщиков
Сетевые уязвимости

Инструменты

Metasploit
ATM trojan
MTHole.VBE
VNC
Mimikatz
MBR Killer



Подробнее о MoneyTaker в полном техническом исследовании Group-IB

География

Активность группы MoneyTaker в 2018 и 2019 замечена только в России, однако изначально она была выявлена из-за атак в США. Тогда группа оставалась незамеченной на протяжении нескольких лет.

Метод проникновения

MoneyTaker использует три основных метода проникновения в сеть жертвы:

1. Уязвимое сетевое оборудование, получив доступ к которому, злоумышленники через VPN добавляют свой сервер в локальную сеть банка и уже с него развивают атаку. Такой вектор сложно выявить, из-за чего экспертам долгое время не удавалось установить, как именно MoneyTaker проникает в сеть.
2. Доступ из сети доверенного партнера через подбор паролей локальных администраторов с дальнейшим развитием атаки.
3. Фишинговые письма от имени банков и финансовых регуляторов.

Метод хищения

Хищения происходят через российскую систему межбанковских переводов или через банкоматы с использованием собственного уникального ATM-трояна для удаленного управления диспенсером, созданного в 2018 году. При использовании первого метода злоумышленники стали осторожней и проводят транзакции вручную, отказавшись от использования средств автоматизации.

Инструментарий

Основным инструментом MoneyTaker остается Metasploit, который группа использует с начала своей активности. Также они применяют другой популярный фреймворк — PowerSploit, для удаленного управления — Radmin, а для хищений из банкоматов — самописный ATM-троян.

SilentCards

География

Кения

Метод хищения

Карточный процессинг

Вектор проникновения

–

Инструменты

Metasploit
Battlefield
Mimikatz
Pylogger
Kitho Backdoor
MTReverseTCP Stager

География

SilentCards — новая локальная группа из Кении, которая пока проводит атаки только в своей стране. Известно о двух успешных хищениях с участием этой группы.

Метод проникновения

Мы не владеем точной информацией о способах и векторах атак, которые применяет группа для проникновения в сеть. Каких-либо фишинговых писем или вредоносных документов, которые могли бы быть использованы для доставки нагрузки, найдено также не было. Однако, некоторые экземпляры вредоносных файлов были настроены на работу с серверами управления в локальной сети. Исходя из этого, можно предположить, что для атаки на корпоративную сеть у хакеров уже имеется подконтрольное устройство внутри организации. Это может быть как корпоративный компьютер, так и устройство, принесенное извне.

Метод хищения

Злоумышленники выводят деньги через карточный процессинг: получив доступ к системам управления банковскими картами, они изменяют лимиты и снимают с заранее полученных карт наличные в банкоматах.

Инструментарий

SilentCards использует как самописные инструменты, так и Metasploit и различные PowerShell-скрипты для автоматизации некоторых задач в ходе атаки. Среди собственных разработок группы:

- keylogger, который отправляет результаты работы на FTP-сервер или адрес электронной почты;
- battlefield — шелл, написанный на python и упакованный в ".exe" при помощи программы py2exe. В его возможности входят удаленная командная оболочка, создание и сохранение снимков экрана на локальный диск, загрузка файла по произвольному URL.

Lazarus

География

Европа
Азиатско-Тихоокеанский регион
Ближний Восток
Латинская Америка

Метод хищения

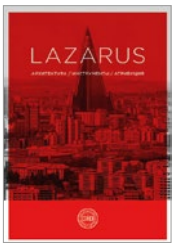
SWIFT
Локальные внутрибанковские системы
ATM Switch

Вектор проникновения

Целевой фишинг
Социальные сети
Атаки типа watering hole

Инструменты

Ratankba
PowerRatankba
ClientRAT (aka FALLCHILL aka Manuscrypt)
ClientTraficForwarder (Proxy)
AppleJeus
PowerTask
PowershellRAT
Banswift/BBSwift
FastCash
RatankbaPOS
Mimikatz
Metasploit
Cobalt Strike
Dtrack



Подробнее о Lazarus в полном техническом исследовании Group-IB

География

Основным фокусом группы Lazarus всегда был Азиатско-Тихоокеанский регион. Атака 2017 года, когда их жертвами стали банки в Польше, выглядела скорее исключением.

Однако в октябре 2018 года HSBC зафиксировал атаку на свое подразделение на Мальте от неизвестного атакующего, который получил название EmpireMonkey, а в феврале 2019 года из мальтийского банка Bank of Valetta было похищено 13 миллионов евро.

Эксперты Group-IB связывают атаку на мальтийские банки с группой Lazarus, что может свидетельствовать о возрождении интереса группы к европейским компаниям.

Метод проникновения

Lazarus использует различные векторы и изощренные инструменты для проникновения в банки:

- Целевой фишинг, который отправляется очень узкому кругу получателей.
- Watering hole — получая доступ к сайтам финансовых регуляторов, Lazarus атакует посетителей этих сайтов. При этом вредоносный код будет загружаться, только если пользователь пришел с определенного пула IP-адресов.
- Социальная инженерия через соцсети, где злоумышленники находят наиболее подходящего по профилю сотрудника, делают ему предложение о работе и в ходе общения вынуждают загрузить и запустить вредоносную программу на рабочем месте.

Метод хищения

При атаках на финансовые учреждения основным способом вывода денег, используемым Lazarus, является SWIFT. Предположительно с 2016 года группа также использует для вывода денег ATM Switch — в 2018 году стало известно о двух таких ограблениях в Индии и Чили.

Инструментарий

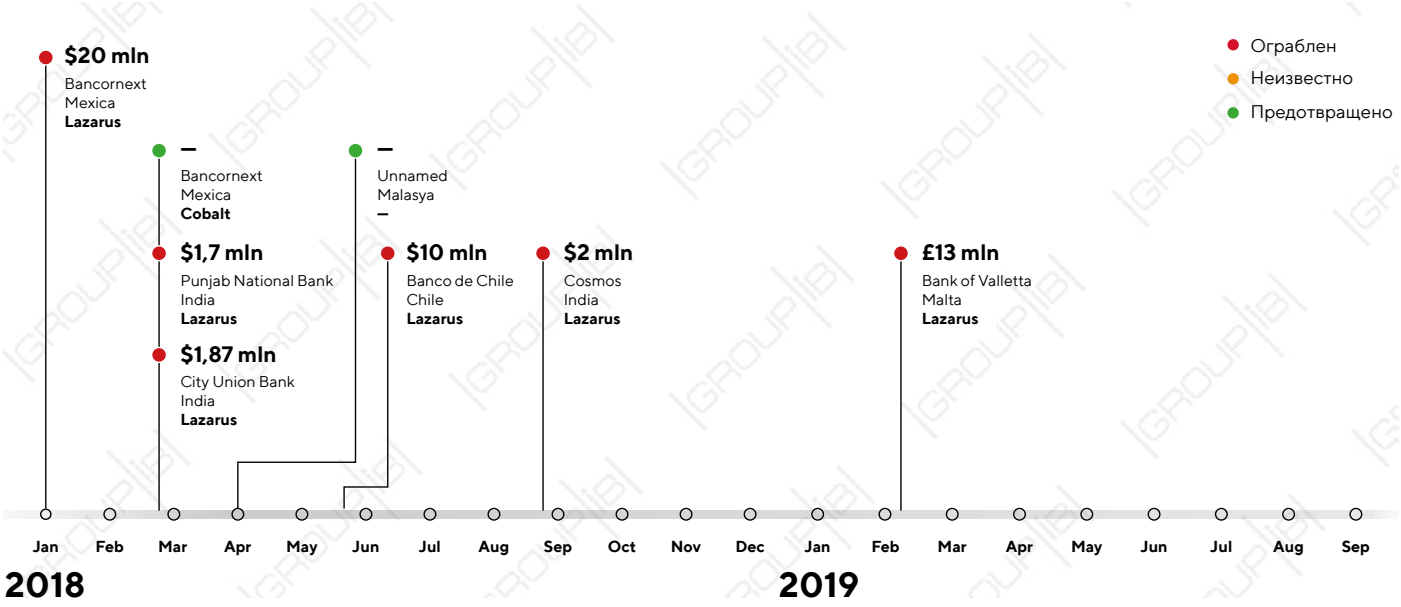
На самом начальном этапе развития атаки группа по-прежнему использует свой загрузчик, известный как Ratankba. В 2017 году была выпущена первая модификация этого загрузчика на PowerShell, а в 2019 году эксперты обнаружили его модернизированную версию. Для атак на пользователей Apple Lazarus создали загрузчик, который получил название AppleJeus.

Основной троян ClientRAT (aka FALLCHILL, Manuscrypt) также был переписан на PowerShell с конца 2018 года. По функциональности он копирует прошлую версию, но намного более сложен для обнаружения.

Для проксирования трафика группа использует свой прокси-бот ClientTraficForwarder, а во время атак — хорошо известные фреймворки Metasploit и Cobalt Strike, что усложняет процесс атрибуции.

Хищения через ATM Switch осуществляются с помощью их собственной уникальной вредоносной программы Fastcash.

ХИЩЕНИЯ ЧЕРЕЗ SWIFT



СУЩЕСТВУЮЩИЕ УГРОЗЫ

Основная масса хищений через SWIFT пришлась на вторую половину 2017 и первую половину 2018 года, после чего наступило затишье, и за отчетный период атакующим удалось совершить лишь два успешных хищения в банках Индии и Мальты на общую сумму $16 миллионов.

Опыт успешного вывода денег через SWIFT есть только у двух групп — Lazarus и Cobalt. Поэтому когда произошедший на Мальте инцидент не смогли связать ни с одной из них, некоторые специалисты объявили о появлении «новой группы» EmpireMonkey. Второй инцидент, приписанный этой группе — атака на мальтийское подразделение HSBC, которая была успешно остановлена. Однако, по данным Group-IB, за этими атаками все же стоит Lazarus.

В 2017 году Lazarus уже пыталась атаковать банки в Европе, и методом проникновения был Watering hole. Кроме Польши были скомпрометированы сайты финансовых регуляторов в Мексике и Республике Уругвай. Тогда удалось найти конфигурационный файл, в котором были указаны подсети банков, представлявших интерес для группы Lazarus. В нем были перечислены подсети мексиканских банков, Banco de Chile, турецкий Akbank, которые через год были успешно ограблены, а также атакованные якобы "EmpireMonkey" подсети и банка HSBC.

Таким образом, несмотря на общее снижение количества инцидентов с хищениями через SWIFT, этот вектор все еще остается актуальным. Более того, возможно появление новых инструментов для совершения таких атак.

ПРОГНОЗ: ПОЯВЛЕНИЕ BANSWIFT/BBSWIFT НА POWERSHELL

В 2016 году при известной атаке на центральный банк Бангладеша Lazarus использовал специальную программу Banswift/BBSwift. Она позволила отслеживать нужные операции, модифицировать данные в базе и блокировать печать документов из SWIFT на принтере.

Во всех следующих инцидентах подобные средства автоматизации не использовались, и хищения совершались в ручном режиме. Атакующие компрометировали места операторов с легитимным доступом к интерфейсу SWIFT, а для вывода денег использовали тип сообщений MT103 Serial или MT103 Cover.

Однако за последний год группа Lazarus значительно усовершенствовала свои инструменты, прежде всего, за счет их перевода на Powershell. Возможно, в следующих хищениях они будут использовать аналог Banswift/BBSwift, написанный на Powershell.

ХИЩЕНИЯ ЧЕРЕЗ ATM SWITCH

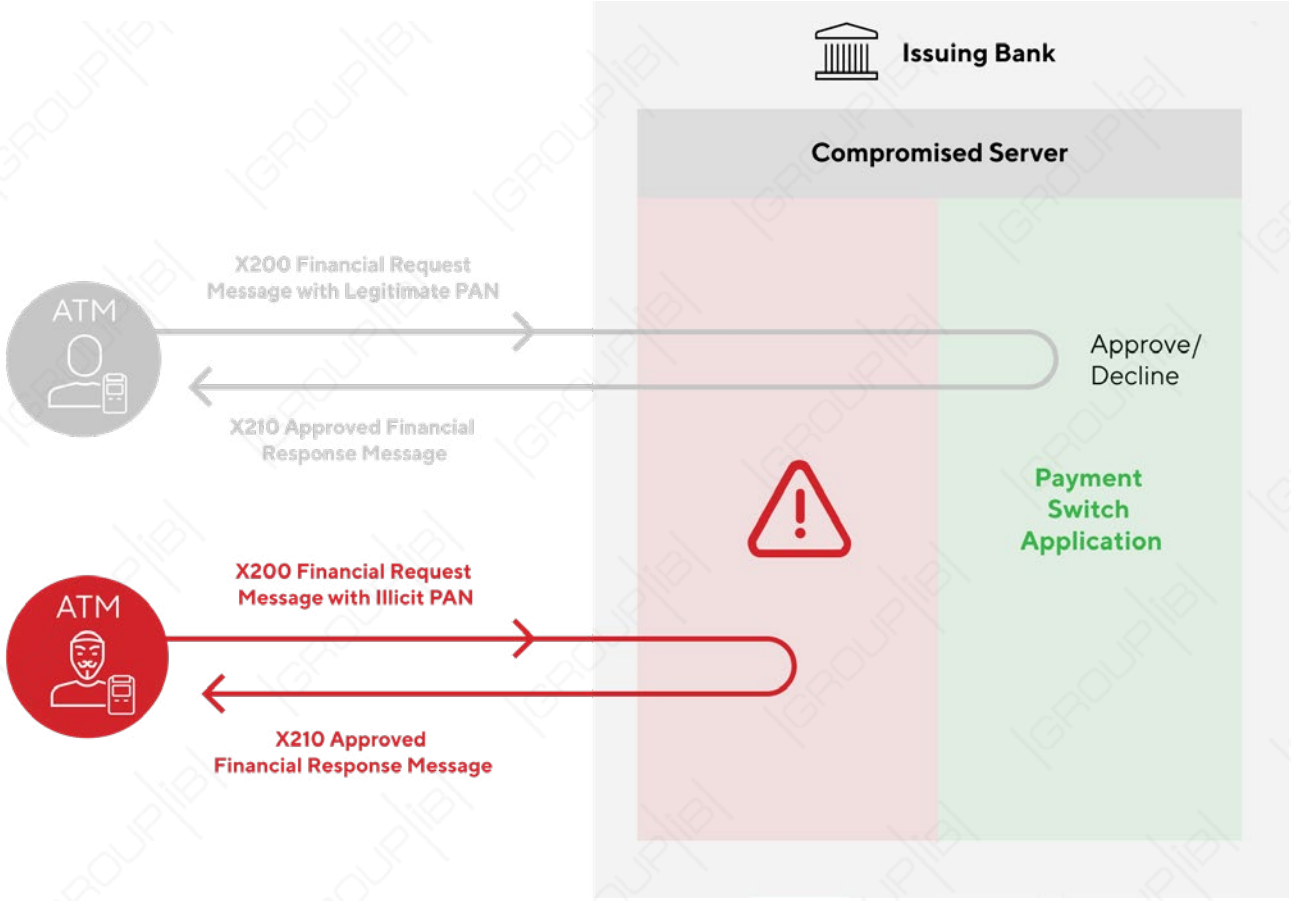
Произошедшая в 2018 году атака Lazarus на индийский Cosmos bank завершилась выводом денег в два этапа:

- 11 миллионов долларов были сняты через подставных лиц со счетов клиентов банка по поддельным банковским картам в банкоматах. В течение 7 часов было осуществлено почти 15 тысяч таких транзакций в 28 странах мира. Еще около 400 тысяч долларов были сняты в банкоматах по фальшивым картам в самой Индии.
- 2 миллиона долларов были выведены уже на следующий день через систему SWIFT со счетов банка на подставные счета в Гонконге.

Метод, используемый на первом этапе, получил название FastCash. Схема его реализации кажется простой, но имеет много сложностей в исполнени:

- Получить доступ в сеть банка.
- Найти в сети банка сервер приложений, отвечающий за процессинг транзакций с банкоматов — ATM Switch, работающий на операционной системе AIX – подобная UNIX операционная система компании IBM.
- Получив доступ к этому серверу, загрузить консольную утилиту для добавления своей вредоносной библиотеки в уже запущенный процесс.

В обычной схеме запросы от банкомата приходят на этот сервер приложений, который проверяет в банковских системах, подтверждать ли операцию выдачи денег. Загруженный вредоносный код перехватывал такие запросы и подменял ответы для нужных карт, подтверждая выдачу средств.



Описанная атака была далеко не первой

- некоторые вредоносные файлы, связанные с инцидентом в Cosmos Bank, были скомпилированы в 2016 году;
- после инцидента один из клиентов также сообщил Group-IB, что их банк в Азии был атакован таким же образом еще в 2016 году;
- в 2017 US-CERT указывал, что аналогичным образом были похищены средства через банкоматы в 30 странах. Предположительно, это оповещение было связано с инцидентом 2015 года, когда Lazarus атаковал оператора банкоматов в Южной Корее и до февраля 2017 года имел доступ в их сеть и банкоматы;
- кроме Cosmos Bank в 2018 году аналогичным методом были похищены деньги через чилийскую межбанковскую сеть Redbanc.

ЛОГИЧЕСКИЕ АТАКИ НА БАНКОМАТЫ

Как было отмечено ранее, из 5 активных групп 3 имеют в своем арсенале ATM-троян — это Cobalt, Silence, MoneyTaker. Однако за исследуемый период только Silence проводила успешные атаки на банкоматы.

Ранее группа использовала собственный троян Atmosphere, однако в феврале 2019 года была проведена атака в России с помощью нового трояна. При этом в коде программы присутствовали признаки того, что она нацелена на хищение валюты в долларах.

Спустя три месяца Silence успешно ограбила Dutch Bangla Bank Limited (DBBL), предположительно используя протестированный в России новый троян. Вскоре после хищения 6 украинцев, собиравших деньги из банкоматов, были задержаны.

```
qmemcpy(v141, "USD BUSD", 8);
v143 = 5;
v144 = 1000;
v145 = 1000;
v158 = &WindowName;
strcpy(v159, "USD CUSD\n");
v161 = 1000;
v162 = 1000;
v175 = &WindowName;
qmemcpy(v176, "USD DUSD", 8);
v178 = 20;
v179 = 1000;
v180 = 1000;
snprintf(&s[1], 3u, "USD");
snprintf(v123, 5u, "USD A");
snprintf(&v142[1], 3u, "USD");
snprintf(v141, 5u, "USD B");
snprintf(&v160[1], 3u, "USD");
snprintf(v159, 5u, "USD C");
snprintf(&v177[1], 3u, "USD");
snprintf(v176, 5u, "USD D");
v6 = &v84;
v7 = &v102;
v8 = &v120;
v9 = &v138;
v10 = &v156;
v11 = &v173;
v198 = '\x06\0\0';
v199 = (int *)&v6;
v3 = WFSExecute(v1, 312, &v198, 60000, &v206);// WFS_CMD_CDM_END_EXCHANGE
```

Кроме подтвержденной атаки на DBBL, Silence предпринимали попытки хищений еще в двух банках (NCC Bank и Prime Bank), однако по заявлениям последних финансовые потери удалось предотвратить.

Новый троян Silence перебирает все активные процессы, и если в них подгружена dll msxfs.dll, то выполняет инжект кода в этот процесс. Внедренный код перечисляет все потоки приложения и замораживает определенные, вероятно принадлежащие модулю msxfs.dll. Выгрузку средств выполняют не с помощью обычных API XFS с кодами WFS_CMD_CDM_DENOMINATE и WFS_CMD_CDM_DISPENSE, а последовательно с помощью WFS_CMD_CDM_START_EXCHANGE и WFS_CMD_CDM_END_EXCHANGE.

В мае 2018 MoneyTaker также успешно протестировала свой уникальный троян для банкоматов на российском банке, однако других инцидентов не последовало. В отличие от Silence, ATM-троян группы MoneyTaker позволяет взаимодействовать с диспенсером именно через XFS API.

ХИЩЕНИЯ ЧЕРЕЗ КАРТОЧНЫЙ ПРОЦЕССИНГ

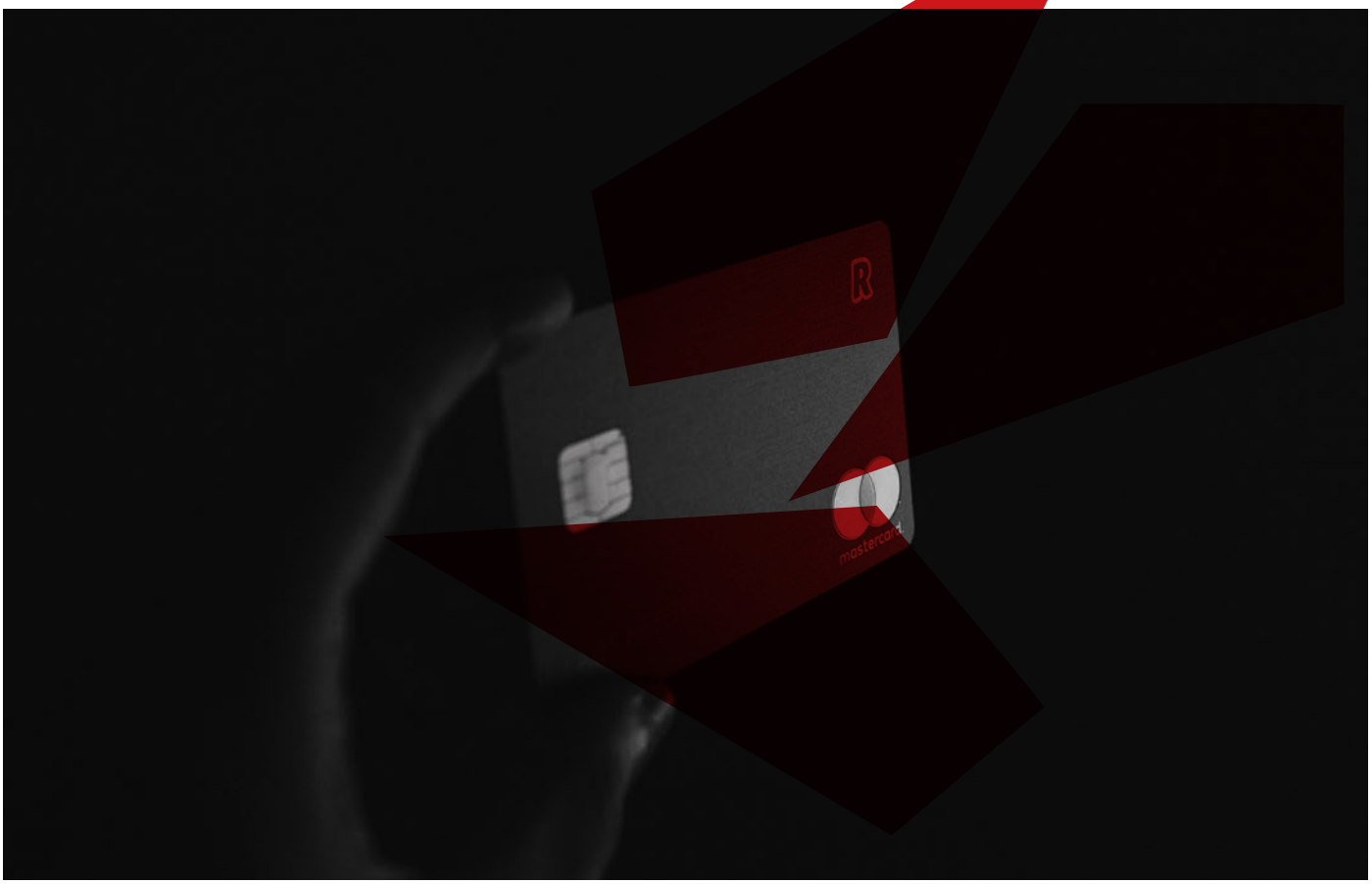
Этапы атаки через карточный процессинг

- получение контроля над банковской сетью;
- проверка возможности подключаться к системе управления карточным процессингом;
- открытие или покупка карт банка, к которому был получен доступ;
- подготовка «мулов», которые с этими картами выезжают в другую страну;
- отключение или увеличение лимита на снятие наличных для этих карт;
- отключение овердрафт-лимитов, чтобы можно было уйти в минус даже по дебетовым картам;
- снятие наличных «мулами» по команде в разных банкоматах.

На разных этапах своего развития атаки на карточный процессинг осуществляли группы Cobalt, MoneyTaker, Silence. За исследуемый период из этого списка только Silence продолжила использовать этот метод, однако к «Большой тройке» добавилась новая группа с созвучным названием SilentCards.

Группа Silence провела свою первую атаку на карточный процессинг в марте 2018 года и сразу успешно похитила 35 млн. рублей в одном из банков в России. При анализе публичной информации об инцидентах в Индии с Dutch Bangla Bank Limited, NCC Bank и Prime Bank установлено, что денежные средства снимались с банкоматов в России, на Украине и на Кипре. Такая схема возможна только, если атакующие получили доступ к системе управления карточным процессингом и имели на руках несколько карт, выпущенных этими банками. Такой подход максимально безопасен для «мулов», которые, находясь в другой стране, могут снимать деньги до тех пор, пока карты не будут заблокированы, или не закончатся банкоматы с деньгами.

В 2018 году произошел случай, который связывают с этой группой, когда в результате получения доступа к карточному процессингу было успешно переведено 400 миллионов кенийских шиллингов. Злоумышленники проникли за периметр корпоративной сети и захватили ключевые серверы, которые отвечают за денежные переводы.



НЕЦЕЛЕВЫЕ АТАКИ

и угрозы для клиентов банков

Уже несколько лет подряд сложные банковские трояны постепенно выводятся из эксплуатации, атаки на клиентов банков становятся все более простыми с технической точки зрения, а каждое отдельное прямое хищение наносит меньший ущерб.

Однако из-за простоты реализации значительно выросло количество случаев компрометации финансовых данных. Благодаря развитию JS-снифферов в 2019 году кардинг стал самым быстрорастущим сегментом в области угроз на клиентов банков.

ОБЩИЕ ТЕНДЕНЦИИ В КАРДИНГЕ

Рынок сбора данных банковских карт продолжает расти на протяжении нескольких лет. Его можно условно разделить на два сегмента: текстовые данные (номер, дата истечения, имя держателя, адрес, CVV) и дампы (содержимое магнитных полос карт).

Сбор дампов происходит с помощью скимминговых устройств и троянов для компьютеров с подключенными POS-терминалами. Для получения текстовых данных используют фишинговые сайты, банковские трояны для ПК, Android и банкоматов, а также JS-снифферы (вредоносный код, внедренный на сайты онлайн-магазинов или других порталов, где пользователи вводят данные своих карт). Именно JS-снифферы стали главным открытием этого года, и эксперты отмечают заметный тренд в их популяризации.

За исследуемый период количество скомпрометированных карт выросло с 27,1 до 43,8 млн, и средняя цена на текстовые данные — с 9 до 14 долларов, при этом снизилась средняя цена дампа — с 33 до 22 долларов.

Год	2019			2018		
	Текстовые данные	Дампы	Всего	Текстовые данные	Дампы	Всего
Общее количество	12 540 190	31 213 941	43 754 131	10 218 489	16 927 777	27 146 266
Размер рынка	$ 179 159 552	$ 700 520 520	$879 680 072	$95 590 424	$567 791 443	$663 381 867
Минимальная цена	$0.7	$0.5		$0.75	$0.5	
Максимальная цена	$150	$500		$99.99	$295	
Средняя цена	$14,29	$22,44		$9.35	$33.54	

РАЗВИТИЕ POS-УГРОЗ

Дампы банковских карт занимают около 80% рынка кардинга, и за исследуемый период было обнаружено 31,2 миллиона дампов, выставленных на продажу (на 46% больше, чем в прошлом году).

Основным способом компрометации данных магнитной полосы является заражение компьютеров с подключенными POS-терминалами специальными троянами, которые собирают информацию о банковских картах из оперативной памяти.

За последний год было выявлено 4 новых POS-трояна, которые ранее оставались неизвестными и активно использовались в атаках. Исходные коды большей части известных ранее программ (Alina, MajikPos, FrameworkPOS) уже давно распространяются на хакерских форумах и могут использоваться кем угодно.

Новые трояны
DMSniff
Glitch
Badhatch
RtPOS

Старые и еще активные
FrameworkPOS
MajikPos
TinyPOS
UdPOS
Alina

Всего с марта 2018 по июнь 2019 года произошло 17 массовых утечек, 14 из них были идентифицированы, 3 не удалось связать с конкретной компанией. В описании баз на кардшопах указывается, что скомпрометировано гораздо больше данных, чем представлено для продажи. При оценке объема рынка эксперты Group-IB учитывали только действительно выложенные данные, а значит реальный объем дампов может быть даже больше. Всего таких карт 3,6 миллиона, что составляет 11% от общего количества, остальные данные выкладываются небольшими порциями, поэтому связывать их со значимыми утечками тяжелее.

Дата	Скомпрометированная компания	Названия баз на кардшопах	Кол-во карт	Группа
Март 2018	Applebees in Ohio	BOSSA, NAIFESI, HYTIRI, EXCIRA, PEGASUS, GAZZE, ZYLLA, COSMOS, TRENZO, SABBIA, WYREX, GIRLIX, FANTASI, MCUSTA, FURRI, SIMINDI, TEGRITY, GAZZAK, VELTEX, FIERCE, HISAIS, BAVATA, HAXTI, BAZO, ZERCO, TIGGI, LYZYN, MUAZA, FIREFEX, SERPENTA, SECARMA	121 987	-
Март 2018	Zippy's Restaurants	-	-	-
Апрель 2018	Saks Fifth Avenue and Lord & Taylor Stores	BIGBADABOOM-02	1 094 232	Fin7
Май 2018	Chilis	ZIPPO	1 582 565	Fin7
Июнь 2018	PDQ	-	-	-
Июль 2018	-	ARABIAN-NIGHTS	603 828	-
Август 2018	Cheddar's Scratch Kitchen	-	567 000	-
Август 2018	Burgerville	-	-	Fin7
Сентябрь 2018	-	FIERYRAIN	1 225 311	-
Октябрь 2018	Taco Bueno	-	-	-
Ноябрь 2018	Caribou Coffee	-	-	-
Декабрь 2018	-	BADASS-SANTA	184 927	-
Январь 2019	Huddle House	-	-	-
Январь 2019	N₹rth Country (NCBP)	-	-	-
Март 2019	Earl Enterprise (Buca di Beppo, Earl of Sandwich, Planet Hollywood)	DAVINCI	883 290	-
Май 2019	Checkers and Rally's	-	-	-
Июнь 2019	Cotton Patch Cafe	BLACKSPIDER, BENEDICT, INTUITION, PERMANENT, ROOTDIRECTORY, VITAMIN	113 500	-

Сложности атрибуции массовых утечек

При обнаружении дампов практически отсутствуют технические детали, что усложняет процесс атрибуции и позволяет делать только предположения о том, кто был причастен к утечке.

В случае с Fin7 атакующих удавалось установить либо когда сама атакованная компания заявляла об этой группе, либо когда названия компаний были опубликованы в обвинительных документах из расследований.

При массовых утечках мы можем только догадываться о взаимосвязи между реагированием на конкретный инцидент и публикацией технического описания новых троянов, но уже без указания конкретных компаний, например:

- В августе 2018 года стало известно об утечке Cheddar's Scratch Kitchen, чуть позже в этом же месяце впервые была опубликована информация о трояне RtPOS.
- В марте 2019 начинается реагирование на инцидент в Earl Enterprise (Buca di Beppo, Earl of Sandwich, Planet Hollywood), и в этом же месяце появляется информация сразу о двух новых POS троянах — GlitchPOS и DMSniff.
- В июне 2019 через месяц после реагирования на инцидент в Cotton Patch Cafe вышла новость о трояне Badhatch, который связали с группой Fin8.

География источников дампов

Основной целью атакующих являются сети ресторанов быстрого обслуживания в США, эта страна занимает первое место по количеству скомпрометированных карт — около 93% всего объема дампов. На следующие места антирейтинга в этом году вышли страны Ближнего Востока (Кувейт, Пакистан, ОАЭ, Катар), суммарно на них приходится 2.38%.

Страна	Количество дампов	Процент (%)
США	29 121 383	93,30
Кувейт	359 037	1,15
Пакистан	261 901	0,76
Великобритания	238 186	0,47
Канада	145 366	0,47
Китай	119 807	0,38
Бразилия	95 344	0,31
ОАЭ	87 447	0,28
Республика Корея	64 946	0,21
Катар	59 364	0,19
Другие страны	661 178	2,12

Возможные причины ближневосточной аномалии

Благодаря собственной инфраструктуре мониторинга подпольных форумов и кардшопов, аналитики Group-IB видят полную картину рынка кардинга и выявляют аномалии. В этом периоде наблюдался необычный всплеск количества скомпрометированных банковских карт Пакистана, которые до октября 2018 года практически никто не продавал.

26 октября на продажу была выставлена база из 10 467 дампов, 8 704 из них относились пакистанским банкам, включая Banklislami. Через 2 дня банк Banklislami опубликовал сообщение, что 27 октября атакующим удалось вывести со счетов около $2.6 миллионов.

После этой публикации на кардшопах было опубликовано еще две базы, содержащие данные пакистанских банков:

- 31 октября 2018 года — 11 795 дампов;
- 13 ноября года — 177 878 дампов.

В общей сложности было выложено 150 632 дампа пакистанских карт, однако это была лишь первая волна.

24 января в продаже появилась небольшая база с 1 535 дампами, 96% карт которой были выпущены пакистанским банком Meezan Bank Ltd, а 30 января — крупная база с 67 654 дампами.

Отличительной особенностью этой базы от всех предыдущих было наличие пин-кода. Чтобы получить дампы с пин-кодом, обычно необходимо аппаратное скимминговое оборудование, но объемы скомпрометированных таким образом карт всегда небольшие. Другой вариант их получения — компрометация банка, который не следует международным требованиям безопасности и хранит у себя информацию о пин-коде.

16 января на VirusTotal из Пакистана был загружен файл с именем ApplicationPDF.exe — вредоносная программа группы Lazarus, которая используется злоумышленниками для отправки сотрудникам банков после знакомства в социальных сетях. Аналогичная программа использовалась для получения доступа в атаке на чилийскую межбанковскую сеть Redbanc. Загруженный на VirusTotal файл был скомпилирован 31 октября 2018 года — он не может иметь отношение к утечкам 2018 года, но может объяснить инциденты 2019 года.

НОВЫЙ ТРЕНД — JS-СНИФФЕРЫ

Одним из наиболее эффективных способов компрометации банковских карт является внедрение JS-сниффероов. Сниффер — тип вредоносного кода, внедряемого злоумышленниками в сайт жертвы для перехвата вводимых пользователем данных: номеров банковских карт, имен, адресов, логинов, паролей и т. д. Полученные платежные данные злоумышленники перепродают или используют сами для покупки ценных товаров.

Аналитики RiskIQ были первыми, кто в партнерстве с компанией Flashpoint проанализировал деятельность злоумышленников, использующих снифферы. Они выделили 12 групп под общим названием MageCart. Эксперты Group-IB изучили обнаруженные снифферы и, применив собственные аналитические системы, смогли вскрыть всю инфраструктуру и получить доступ к исходникам и инструментам злоумышленников. Такой подход к весне 2019 года позволил выявить как минимум 38 разных семейств. На момент выхода этого отчета семейств уже было больше.

Каждое семейство обладает уникальными признаками и, скорее всего, управляется разными людьми. Так как все снифферы имеют схожий функционал, создание двух сниффероов одной группой злоумышленников нецелесообразно.

Список семейств JS-sniffer, проанализированных в этом очете: 15 из 38, обнаруженных командой Group-IB

TokenLogin	Март 2016	Illum	Конец 2016	MagentoName	Декабрь 2017
TokenMSN	Середина 2016	WebRank	Конец 2016	ImageID	Конец 2017
G-Analytics	Сентябрь 2016	ReactGet	Июнь 2017	GetBilling	Начало 2018
PreMage	Ноябрь 2016	PostEval	Середина 2017	Qoogle	Апрель 2018
FakeCDN	Ноябрь 2016	CoffeMokko	Сентябрь 2017	GMO	Май 2018

Как работают снифферы

1 шаг: получение доступа к сайту

- Вариант 1 — получение доступа к административной панели с использованием вредоносных программ, крадущих пароли;
- Вариант 2 — поиск уязвимых сайтов (эксплоиты популярных CMS, известные уязвимости поставщиков услуг). Используя эксплоиты, злоумышленник загружает веб-шелл и получает доступ к изменению файлов сайта;
- Вариант 3 — покупка доступа к сайту у другой группы злоумышленников.

2 шаг: получение сниффера

- Вариант 1 — собственная разработка;
- Вариант 2 — покупка/аренда готового варианта на андеграундном форуме.

3 шаг: установка сниффера

Установленный через панель управления или веб-шелл сниффер собирает информацию и отправляет ее на хост, управляемый злоумышленником. Некоторые снифферы используют техники, позволяющие оставаться незамеченными при ручной проверке:

- добавление в легитимную библиотеку скриптов;
- механизм приостановки активности сниффера в момент использования консоли разработчика (например, Chrome DevTools или Firefox Browser Toolbox).

4 шаг: монетизация

- Вариант 1 — продажа данных кардерам и получение от $1 до $5 с каждой карты. Этот способ самый простой — для его реализации достаточно иметь контакты проверенных скупщиков;
- Вариант 2 — оплата чужими банковскими картами товаров, которые легко перепродать: гаджетов, электроники, бытовой техники, предметов интерьера, одежды и обуви.

Собранные платежные данные и персональная информация жертвы отправляется на сервер злоумышленников — гейт. Для усложнения обнаружения конечного сервера злоумышленников в цепочке передачи данных со сниффера может быть использовано несколько уровней гейтов, расположенных на разных серверах или взломанных сайтах. Однако в некоторых случаях административная панель расположена на том же хосте, что и гейт для сбора украденных данных.

Конечный сервер злоумышленников, предназначенный для отслеживания активности снифферов и экспорта украденных данных, может представлять собой как полноценную административную панель, так и сервер для размещения инструментов администрирования баз данных. К примеру, функции административной панели могут выполнять такие инструменты, как Adminer или phpMyAdmin.

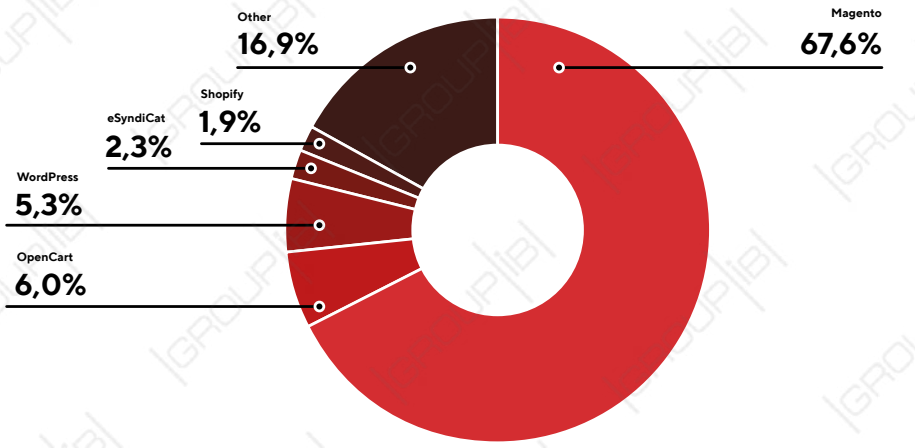
Способы заражения

Злоумышленники могут заражать сайты и внедрять вредоносный код разными способами.

Эксплуатация уязвимостей CMS

Вредоносный код может внедряться в код сайтов онлайн-магазинов при помощи уязвимостей CMS, разработанных специально для онлайн-магазинов, — Magento, OpenCart и др.

- загрузка веб-шелла на сайт при помощи эксплуатации уязвимости с последующей модификацией файлов сайта;
- внедрение кода сниффера при помощи эксплуатации уязвимости, позволяющей добавить код злоумышленника в один из блоков кода сайта, к примеру, в футер.



Взлом административной панели сайта

Сниффер может быть установлен путем получения доступа в административную панель сайта с возможностью редактирования файлов. Компрометация логина и пароля может осуществляться несколькими методами:

- использование стилеров — программ, позволяющих извлекать пароли, сохраненные в браузере;
- использование вредоносных программ для перехвата вводимых данных (в том числе логина и пароля);
- брутфорс — метод перебора паролей.

Взлом сторонних сервисов

Сниффер может попасть на сайт через взлом сторонних сервисов, скрипты которых работают на целевом сайте:

- внедрение вредоносного кода через код скриптов сайтов, предоставляющих услуги онлайн-магазинам (чаты клиентской поддержки, системы аналитики и статистики);
- взлом аккаунтов CDN-сервисов с возможностью модификации скриптов, подгружающихся из CDN на целевые сайты.

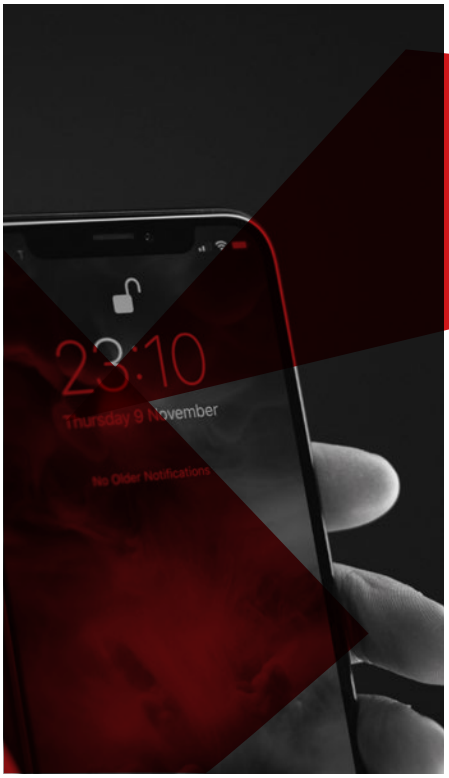
Атаки через поставщиков

Преступная группа, стоящая за использованием семейства снифферов WebRank, зачастую осуществляла атаки через поставщиков услуг. К примеру, взломав систему веб-аналитики, злоумышленники внедряли код сниффера в их скрипт. Данный скрипт, подгружаемый многими сайтами, вместе с собой подгружал и сниффер банковских карт.

Такая техника доставки также делает возможным вытеснение конкурирующих семейств снифферов. Так в ходе одной из волн заражений операторы сниффера WebRank получили доступ к коду сниффера MagentoName и добавили к нему в сайт свой вредоносный код.

Другой пример — атака на Feedify, сервис для push-уведомлений в режиме реального времени. Внедрив код сниффера в код файла, преступная группа автоматически подгрузила сниффер всем клиентам компании Feedify, на сайты которых подгружался скрипт feedbackembad-min-1.0.js. Сниффер был впервые добавлен в код Feedify 17 августа, а 11 сентября обнаружен и удален. Однако злоумышленники вновь провели заражение 12 сентября.

Атаки через сторонних поставщиков доказали свою эффективность: более 60% из трех сотен сайтов, подгружающих скрипт Feedify, относятся к eCommerce-сайтам, а значит, служат целями для сниффера семейства WebRank.



Целевые платежные системы

С точки зрения архитектуры каждый сниффер имеет клиентскую и серверную часть.

Клиентская часть сниффера отвечает за первоначальный сбор данных, осуществляемый разными способами:

- по жестко записанному списку имен полей платежных форм;
- по списку регулярных выражений, определяющему интересные снифферу поля;
- по списку базовых HTML-элементов, используемых в платежной форме.

Серверная часть сниффера — приложение, с которым работает оператор сниффера.

Выполняемые серверной частью функции зависят от того, насколько точно клиентская часть сниффера определяет тип украденных данных. Если данные передаются в необработанном виде, значит определение номера карты, CVV, телефона, электронной почты и имени владельца к единому виду происходит уже в административной панели.

Обработка данных в административной панели — более удобный вариант, так как внести изменения в код административной панели легче, чем изменить код сниффера, уже внедренного на сайт онлайн-магазина.

Тем не менее многие семейства снифферов используют уникальные варианты для каждой отдельной платежной системы, что требует модификации и тестирования скрипта перед каждым заражением.

Универсальные снифферы

К универсальным снифферам можно отнести те семейства, которые настроены на кражу данных из разных платежных систем и не требуют доработки под определенную платежную систему. Снифферы семейств G-Analitycs и WebRank настроены похищать все содержимое элементов HTML определенного типа. Это означает, что парсинг украденных данных происходит в административной панели этих снифферов, то есть на стороне сервера.

- Снифферы семейства WebRank обращаются ко всем объектам типа “text”, “a”, “button”, “input”, “submit” и “form” и добавляют специальные обработчики событий, связанных с этими элементами.
- Снифферы семейства G-Analytics осуществляют поиск всех элементов следующих типов на странице оплаты: "input", "select", "textarea", "checkbox". Если в результате этого поиска обнаруживаются данные, похожие на номер кредитной карты, сниффер отправляет эти данные на сервер злоумышленников.

Снифферы для определенных CMS

Большая часть обнаруженных снифферов нацелена на платежные формы определенных CMS, то есть сниффер осуществляет поиск определенных полей, содержащих платежную информацию, и список таких полей жестко записан в коде сниффера.

Следующие снифферы осуществляют поиск стандартных полей платежной формы CMS Magento:

- PreMage;
- MagentoName;
- FakeCDN;
- Qoogle.

Сниффер GetBilling также нацелен на платежную форму CMS Magento, но вместо поиска по списку полей он осуществляет поиск форм по их имени. Сниффер семейства PostEval нацелен на платежные формы сайтов, работающих под управлением CMS OpenCart, для поиска данных сниффер использует жестко закодированные имена полей.

Сниффер как сервис

Каждое семейство снифферов может представлять разные типы сервисов. При анализе подпольных форумов, предназначенных для общения киберпреступников, было обнаружено большое количество сервисов, предлагающих своим клиентам полностью готовое решение, в которое входит:

- сниффер или утилита для генерации снифферов;
- административная панель для обработки данных и отслеживания активности снифферов;
- мануалы по заражению сайтов онлайн-магазинов;
- готовые эксплоиты для заражения сайтов;
- вспомогательные утилиты для поиска уязвимостей и массовых заражений сайтов.

При анализе обнаруженных семейств снифферов было установлено, что в некоторых случаях домены, использованные для хранения кода сниффера или для сбора украденной информации, были зарегистрированы разными пользователями. Код был модифицирован, применялись разные способы обфускации и техники сокрытия вредоносной активности. Эти факторы указывают на то, что семейство снифферов используется разными преступными группами, то есть поставляется как сервис.

В других случаях прослеживалась четкая специфика деятельности определенной преступной группы, что может означать независимость от сторонних разработчиков и использование только собственного кода. Таким образом, эти преступные группы должны иметь как минимум одного человека, имеющего навык веб-разработки и знакомого с такими языками, как HTML, JavaScript и PHP.

Сколько стоит использование сниффера

Стоимость снифферов составляет от $250 до $5000. Некоторые сервисы дают возможность работать в партнерстве: клиент предоставляет доступ к скомпрометированному онлайн-магазину и получает 80% от дохода, а создатель сниффера отвечает за серверы для хостинга, техподдержку и административную панель для клиента.

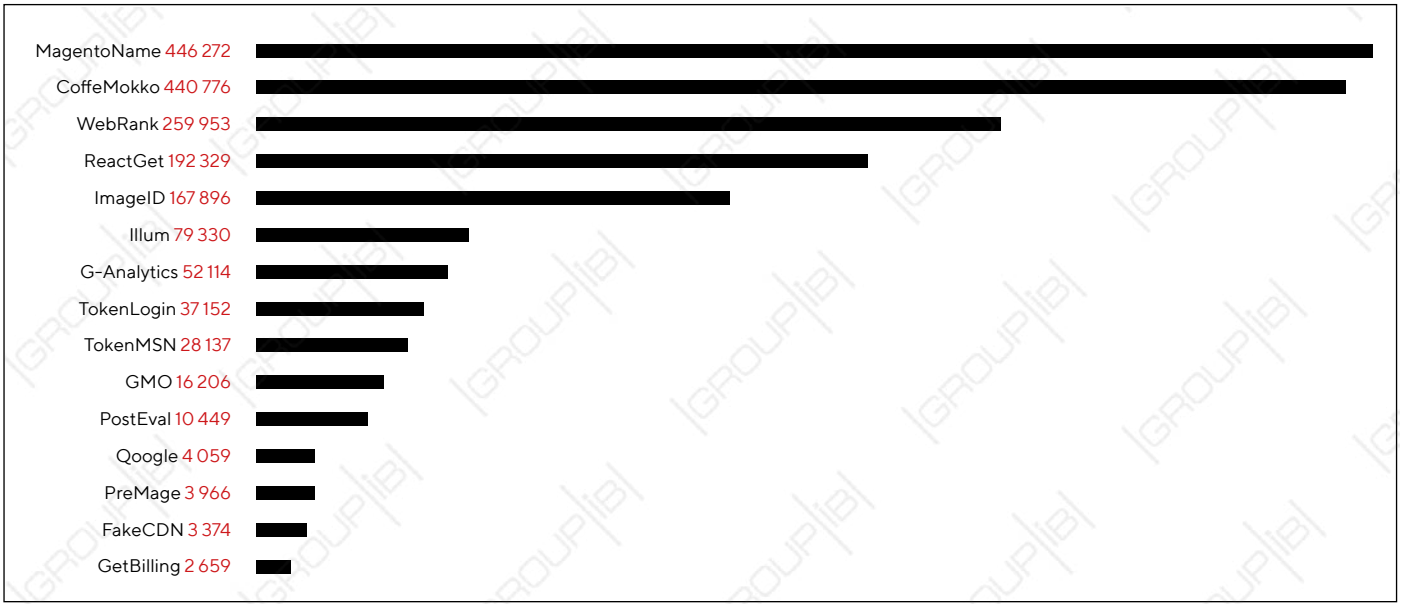
Масштабы заражений и жертвы

Обнаруженные семейства снифферов были использованы для заражения как минимум 2440 онлайн-магазинов, принимающих к оплате банковские карты. Суммарное суточное количество посетителей всех зараженных сайтов — более полутора миллионов человек.

Анализ среднего значения посещаемости каждого зараженного магазина по отдельности показывает, что некоторые снифферы специализируются на более популярных онлайн-магазинах, а другие — на мелких игроках. Так средняя посещаемость сайтов, зараженных снифферами Illum, G-Analytics и TokenMSN, составляет около 3000 человек в сутки на сайт, в то время как этот же показатель для MagentoName составляет около 500 человек в сутки на сайт.

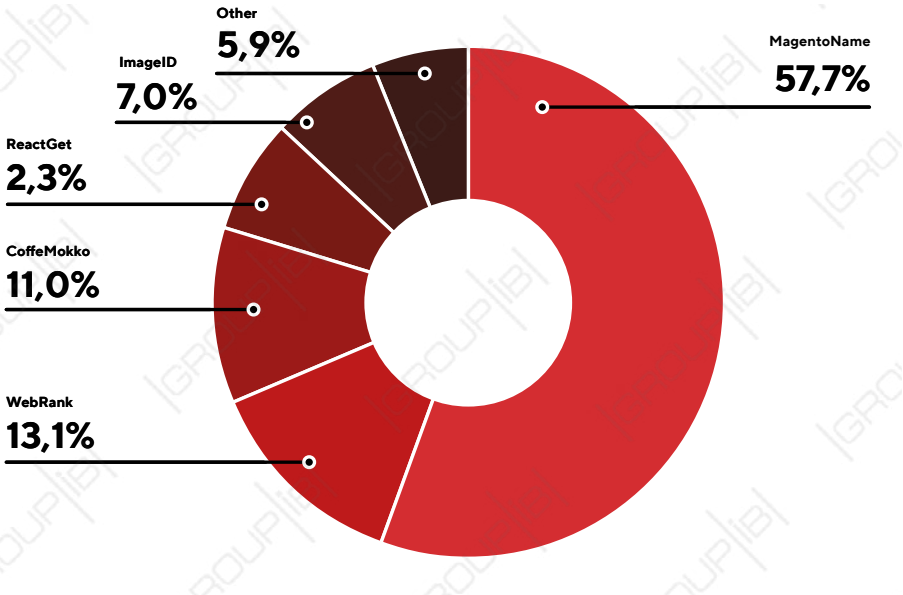
Сниферы, совершающие самые масштабные атаки

Благодаря массовым заражениям, самые большие показатели суммарной посещаемости зараженных сайтов у снифферов семейств MagnetoName и CoffeMokko. Ресурсы, зараженные этими снифферами, посещает более **440 000** человек ежедневно. Третьим по посещаемости является семейство снифферов WebRank — **250 000** человек.



Более половины зараженных сайтов были атакованы сниффером семейства MagentoName, операторы которого используют уязвимости устаревших версий CMS Magento для внедрения вредоносного кода в код сайтов, работающих под управлением этой CMS. Более 13% заражений приходится на долю снифферов семейства WebRank, использующего схему атаки на сторонние сервисы для внедрения вредоносного кода на целевые сайты. 11% приходится на заражения снифферами семейства CoffeMokko, операторы которого используют обфусцированные скрипты, нацеленные на кражу данных из форм оплаты определенных платежных систем, названия полей которых жестко записываются в коде сниффера.

Исходя из анализа списка TLD (top-level domain) зараженных онлайн-магазинов, можно сделать вывод, что атакующие в целом заинтересованы в заражении сайтов, относящихся к крупным развитым странам: США, Великобритании, Германии и т.д.



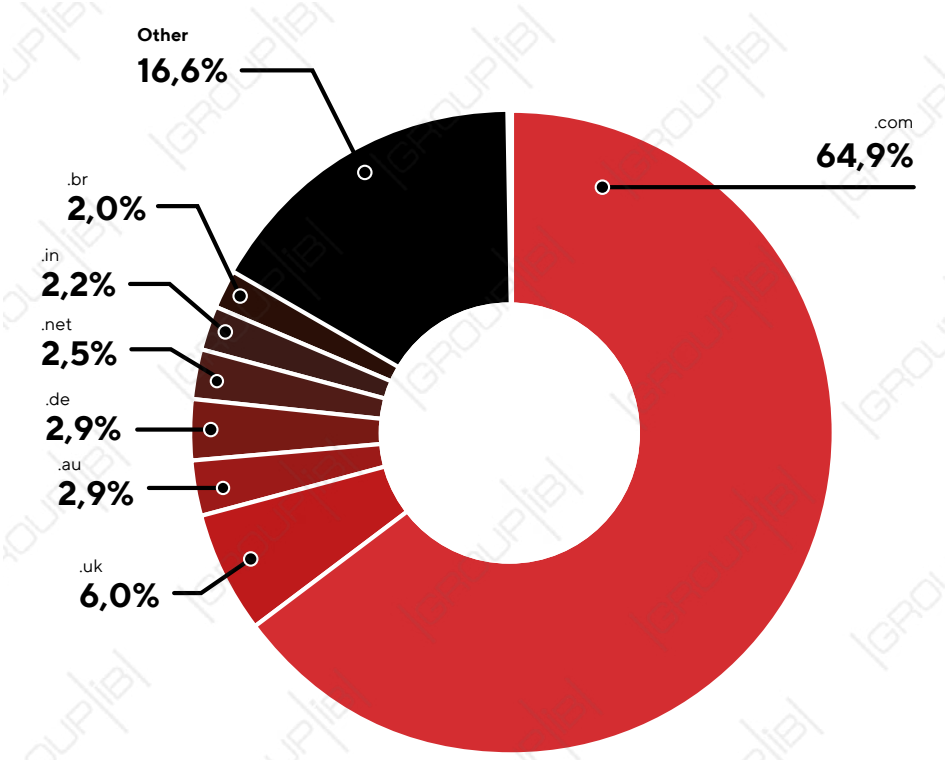
Как и в случае с атаками на POS-терминалы, основной целью атакующих являются клиенты банков США. Вторую позицию занимают английские банки, но это прежде всего связано с успешной атакой на British Airways и внедрением JS-скрипта на раздел с оплатой в конце 2018. В результате было скомпрометировано более 300 тысяч банковских карт, а компания была оштрафована на $229 миллионов.

Анализ атак на пользователей азиатских сайтов, показывает, что есть 11 семейств снифферов, которые стоят за атаками на сайты азиатских стран:

- MagentoName
- Inter
- addtoev Group
- Qoogle
- Illum
- CoffeMokko
- EUTag
- WebRank
- ImageID
- TokenLogin
- OnlineStatus

Прежде всего атакующих интересовали сайты сингапурских, китайских и малазийских компаний.

Страна	Количество сайтов
Сингапур	24
Китай	17
Малайзия	15
Индонезия	6
Вьетнам	4
Таиланд	4
Филиппины	4



ВЕБ-ФИШИНГ И СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

Веб-фишинг — один из самых старых и простых видов мошенничества, который часто используют разные злоумышленники. Постепенно он заменяет собой сложные атаки с использованием дорогостоящих троянов или инструментов для взлома.

Одна из причин популярности фишинга — простота реализации, однако он тоже эволюционирует. Проанализировав за год более 3 миллионов ссылок и 27 тысяч уникальных фишинговых наборов, эксперты Group-IB выявили основные тенденции технологического развития этого типа угроз.

Защита от обнаружения

Все больше компаний предоставляют услуги по блокировке фишинговых сайтов, поэтому все разработчики фишинговых наборов продают их со встроенными механизмами, снижающими вероятность обнаружения:

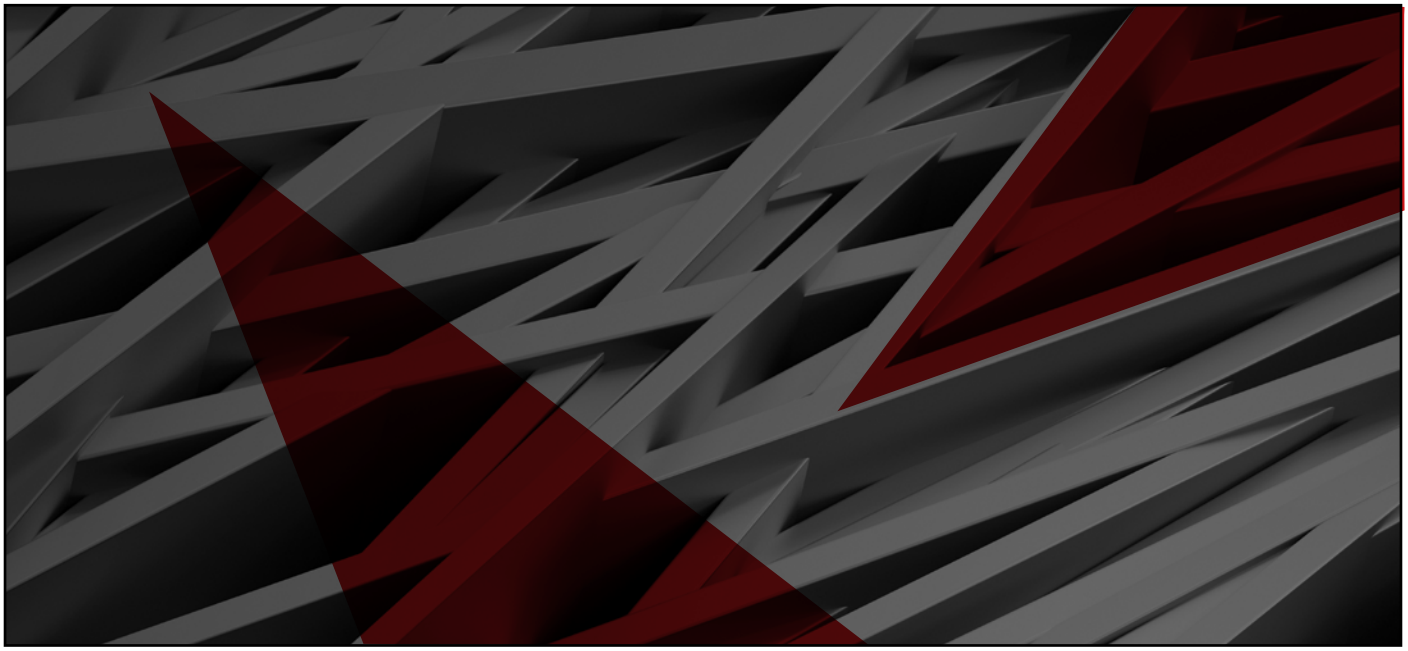
- Блокировка по подсетям — если запрос на страницу приходит из подсетей компаний, оказывающих услуги обнаружения фишинговых страниц, то фишинговый контент не будет отдаваться.
- Блокировка по user agent — атакующие анализируют user agent, пытаясь понять, реальный ли это пользователь. Например, если атака нацелена на владельцев мобильных устройств, то посетители с браузером для ПК не получат фишинговую страницу. Обычно в скриптах фишинговых наборов зашит список ключевых слов, которые проверяются в поле user agent.
- Блокировка по регионам — базы GeoIP активно используются разными злоумышленниками, и если пользователь находится не в атакуемом регионе, то он также не попадет на фишинговую страницу.
- Редиректы на официальные сайты — механизмы специальных проверок позволяют атакующим выявлять подозрительных пользователей и вместо выдачи фишингового контента перенаправлять их на официальный сайт атакуемого бренда или сайт другого легального сервиса.

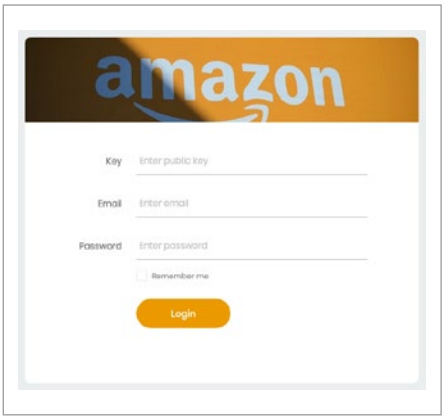
DNS hijacking

В прошлогоднем отчете мы писали, что DNS hijacking будет активно развиваться и позволит атакующим проводить фишинговые атаки еще более эффективно. Напомним, в чем заключается суть этого метода.

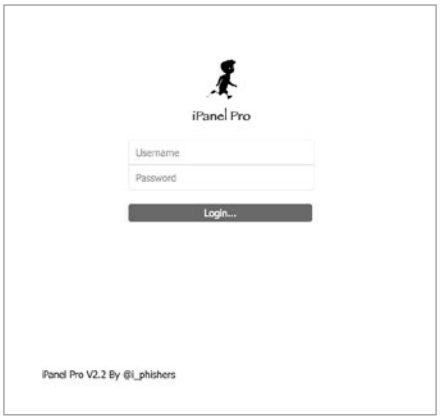
1. Получение доступа к роутеру одним из двух способов:
   - перебор паролей — провайдеры, которые предоставляют роутеры в аренду, мало заботятся об их безопасной настройке, пароли ставят по умолчанию, а интерфейсы управления доступны через интернет.
   - эксплуатация известной уязвимости — обновление домашних роутеров непростая задача. Цикл поддержки таких устройств очень короткий, обновления часто оказываются недоступны, но даже в случаях когда они есть, очень малый процент пользователей занимается обновлением.
2. Изменение настроек DNS-серверов, которые получают устройства, подключенные к Wi-Fi сети этого роутера.
3. Подмена IP-адреса — при запросе определенных доменных имен вредоносные DNS-серверы возвращают мошеннические IP-адреса. Таким образом, когда пользователь вводит в строке браузера название сайта (например, банка), то вместо IP-адреса банка ему возвращается IP-адрес мошенника.

Такая массовая кампания была обнаружена Qihoo 360 в сентябре 2018 года — за 1 неделю они обнаружили более 100.000 скомпрометированных роутеров, большая часть которых была расположена в Бразилии. Угроза получила название GhostDNS и была актуальна минимум до мая 2019 года. Основной целью атакующих были клиенты бразильских банков, а также сервиса Netflix.





Панель для управления фишингом под Amazon



Панель для управления фишингом под Apple

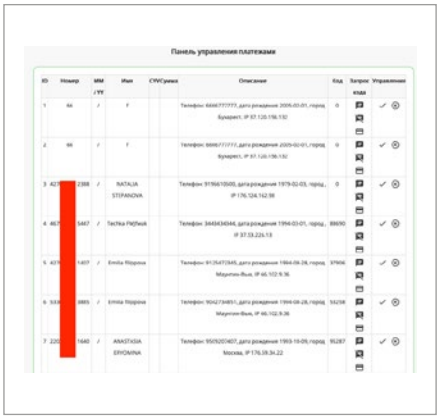
Системы управления фишингом

Чтобы работать с собранными благодаря фишингу данными жертв, атакующие обычно используют один из этих методов:

- отправка данных по электронной почте (по-прежнему самый популярный метод);
- сохранение данных в локальный текстовый файл, который мошенник может забирать с удаленного сервера разными способами;
- загрузка логов на удаленный FTP-сервер (встречается редко).

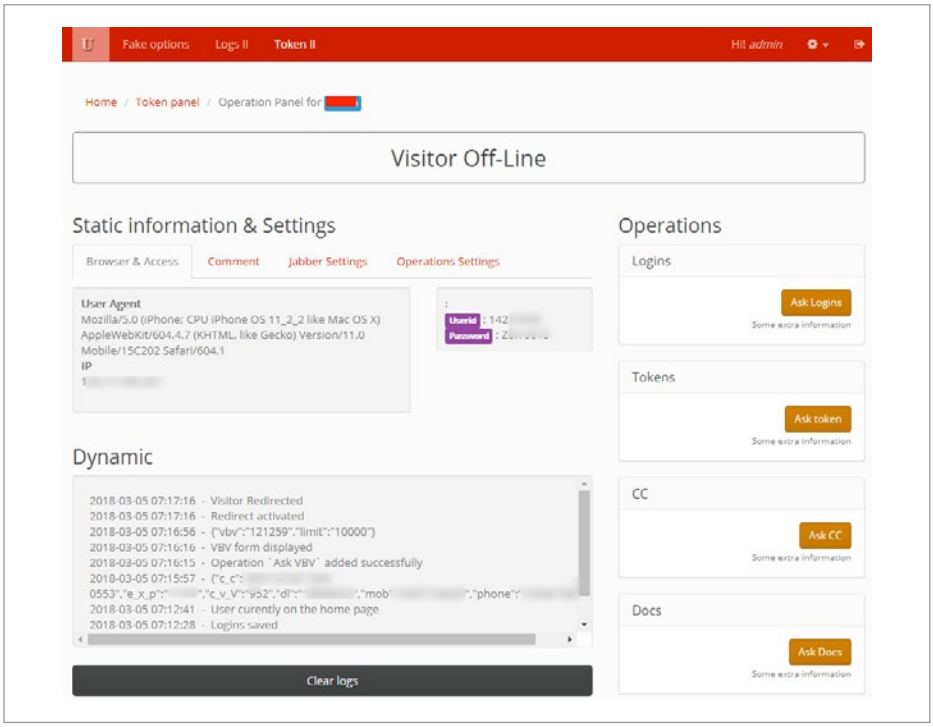
Однако с развитием систем безопасности появилась необходимость работать с данными в режиме реального времени. Кроме того, на андеграундном рынке существует конкуренция, и некоторые поставщики фишинга как услуги начали бороться за клиентов, предлагая им удобные интерфейсы управления скомпрометированными данными.

Панель управления банковским фишингом



Панель управления фишингом под российские банки

Мошенники, занимающиеся фишингом против клиентов банков, начали более активно использовать панели управления веб-инжектами для управления фишинговыми страницами. Это позволяет им проводить атаки в реальном времени, получать от жертв одноразовые пароли и выполнять дополнительные действия, необходимые для подтверждения финансовых операций. Одной из наиболее популярных панелей стала U-Admin.

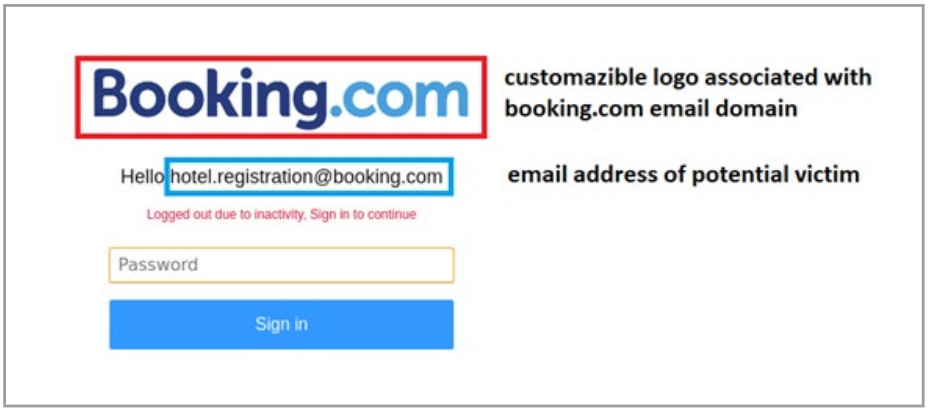


Фреймворк для автоматизированной кастомизации фишинга

Фреймворк для автоматизированной кастомизации фишинга

Интересным примером стала фишинговая кампания, направленная на более чем 200 целей (банки, университеты, коммерческие компании) для сбора адресов электронной почты и паролей пользователей. Ее особенность заключалась в том, что используемый фреймворк автоматически адаптировался под каждую жертву в отдельности.

1. Ссылки на фишинговую страницу рассылались по электронной почте.
2. Если жертва кликала по ссылке из почтового ящика, то в качестве параметра передавались сведения об адресе электронной почты, с которго был осуществлен переход по ссылке.



3. Скрипты на фишинговой странице проверяли домен из адреса электронной почты и делали API запрос к серверу, чтобы получить данные для отображения на фишинговой странице.
4. По домену сервер определял, представляет ли этот пользователь дополнительный интерес, и какой логотип нужно использовать на фишинговой странице.
5. Если пользователь представлял интерес, то после ввода логина и пароля на фишинговой странице он перенаправлялся на следующие этапы.

Рост социальной инженерии без использования вредоносного кода

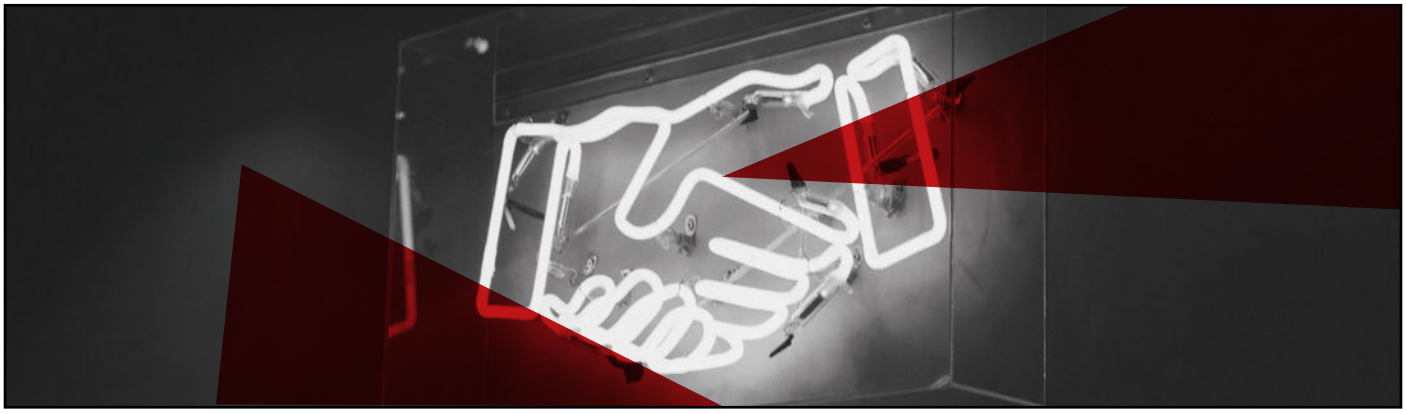
Социальная инженерия без использования вредоносных программ или фишинговых сайтов остается одной из самых массовых и популярных схем. Основными каналами взаимодействия с жертвами всегда были телефонные звонки, SMS, социальные сети. В результате общения жертва сама сообщала мошеннику всю необходимую информацию либо по указанию мошенника устанавливала программы удаленного доступа на ПК, и атакующий мог сам выполнять необходимые операции. Новая схема, появившаяся в этом году, заключается в том, что жертву просят установить средства удаленного управления не на компьютер, а на мобильное устройство.

Типовой сценарий мошенничества выглядит так:

- злоумышленник звонит от имени банка и сообщает клиенту, что зафиксирована попытка взлома личного кабинета или вывода средств;
- службе безопасности банка якобы требуется помощь, чтобы решить техническую проблему для противодействия мошенничеству;
- жертву просят срочно установить программу для удаленного управления смартфоном, чтобы обезопасить пользователя;
- получив инструмент управления приложениями от имени пользователя, мошенник заходит в приложение мобильного банкинга и выводит средства со счета.

Чтобы во время звонка вызвать доверие у жертвы, злоумышленники используют различные приемы, включая самые убедительные:

- звонят с банковских номеров, используя IP-телефонию, подменяя номер телефона через специальные программы;
- сообщают историю транзакций, полную информацию о клиенте, например, где он проживает (базы с такой информацией продаются на форумах в даркнете).



ТРОЯНЫ ДЛЯ БАНКОМАТОВ

Основной и наиболее опасной угрозой для банкоматов являются логические атаки — финальный этап целенаправленных кампаний, в результате которых злоумышленники получают доступ к удаленному управлению банкоматами. Однако такие схемы доступны только продвинутым атакующим.

Для людей без глубоких технических знаний остаются методы, требующие физического доступа к банкомату. Основным ограничением является возможность атаковать только один банкомат, и, как следствие, потенциальный ущерб от таких угроз значительно ниже.

Загрузка на конкретный банкомат вредоносной программы осуществляется с помощью CD, USB носителей или устройств Raspberry Pi. Такие атаки называют "jackpotting", и для их реализации необходимо три уровня злоумышленников — организатор / заказчик, разработчик ПО, дропы.

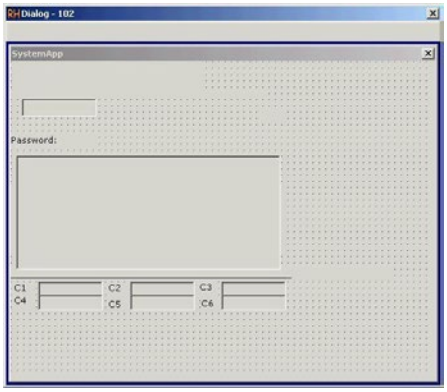
По сравнению с логическими атаками ландшафт таких угроз значительно меньше, но при этом продолжает активно развиваться.

Появление новых угроз

Неименованный троян из Африки

В апреле 2019 года эксперты Group-IB обнаружили интересный экземпляр ATM-трояна из Африки. Программа позволяет управлять банкоматом через pinpad: при вводе правильного PIN-кода напрямую взаимодействовать с диспенсером, а при использовании банковской карты с определенным номером забрать из банкомата все наличные деньги.

Для обхода белых списков атакующие использовали файл cmd.dll — аналог системного инструмента cmd.exe, реализованный разработчиками ReactOS.



HelloWorld

В январе 2019 на андеграундном форуме exploit.in пользователь с псевдонимом “gookee” опубликовал объявление о продаже вредоносной программы. Название “HelloWorld” было упомянуто в теме о продаже ее старой, недоработанной версии. Программа предлагалась в следующих вариантах:

- работающий по принципу “Cutlet Maker” исполняемый файл с кейгеном или без него;
- образ IMG для записи на флеш-накопитель;
- образ на CD;
- образ на дискету;
- образ ISO для загрузки через PXE (в процессе разработки).

Троян работает на всех моделях Wincor/Diebold Nixdorf после 2001 года, у которых есть MXFS/CSCW DLL-файлы, а его стоимость составляет 2000 долларов за EXE-файл или образ, 3000 — за все варианты и 10000 — за исходные коды.

JavaDispCash

Этот троян был загружен на VirusTotal сначала из Колумбии, а потом из Мексики. В отличие от аналогичных инструментов, вместо использования CNG, XFS, JXFS он внедряется в приложение банкомата через JAVA Attach API. Подход к управлению этой программой также является необычным: на банкомате запускается HTTP сервер, который принимает команды по определенным путям.

Путь	Описание команды
/d	Выдача банкнот
/eva	Проверка переданного кода на банкомате
/mgr	Для менеджера, который дает злоумышленникам доступ к списку всех запущенных классов, для подключенной виртуальной машины Java, чтобы они могли вызывать любую функцию по своему усмотрению, предоставляя при необходимости аргументы
/core	Позволяет загрузить .jar файл с файловой системы жертвы
/root	Принимает POST-запрос и передает его содержимое в cmd.exe на исполнение

Эволюция существующих ATM-троянов

Cutlet Maker

Один из самых популярных ATM-троянов, который можно найти и использовать бесплатно. Он используется с середины 2017 года, и за это время на разных хакерских форумах было опубликовано большое количество различных версий.

В декабре 2018 года очередная версия была выложена на русскоязычном хакерском форуме. Cutlet успешно использовали прежде всего в Европе, России и СНГ.

WinPot (Cutlet V2)

В мае 2018 года пользователь с псевдонимом “sl111” опубликовал на андеграундном форуме объявление о продаже ATM-трояна Wincor под названием «Котлета v2» (известного также как WinPot). В комплекте с трояном идут его исходные коды, а цена варьируется от 500 до 1000 долларов. Как и его предшественник, троян использовался для атак на банкоматы европейских стран.

Ploutus

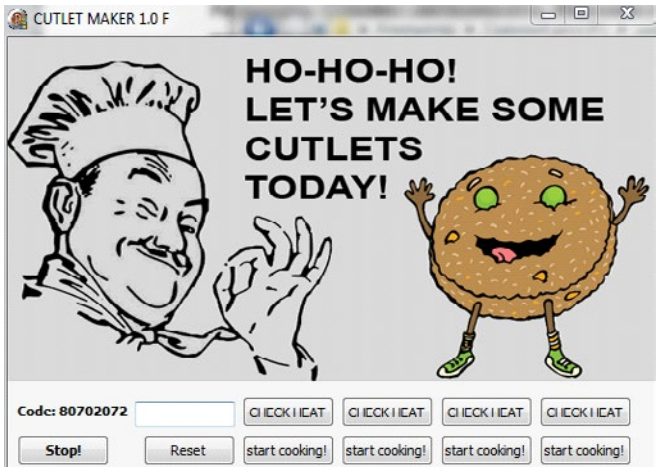
Эту вредоносную программу начали продавать еще в 2016 году, долгое время она использовалась в Мексике, а в 2018 году и в США. Несмотря на свой возраст, Ploutus по-прежнему актуален, и с февраля 2019 года на хакерских форумах снова начали появляться объявления о его продаже.

ATMii

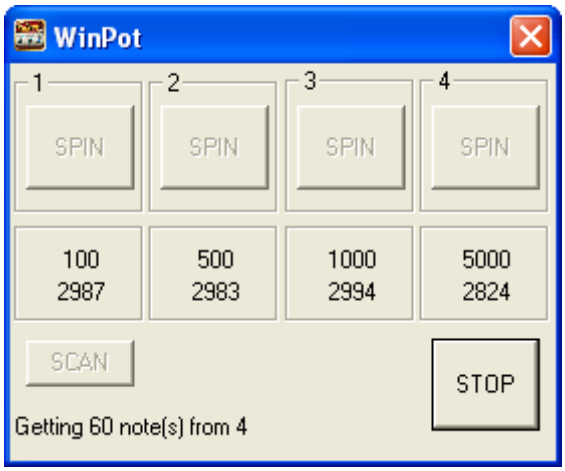
ATMii был обнаружен впервые в апреле 2017 года, и его особенностью является выбор определенных операционных систем. Троян мог работать на Windows 7 и Windows Vista при том, что наиболее популярной операционной системой в банкоматах на тот момент была Windows XP. В декабре 2018 года ATMii также был выложен на русскоязычном хакерском форуме.

Alice

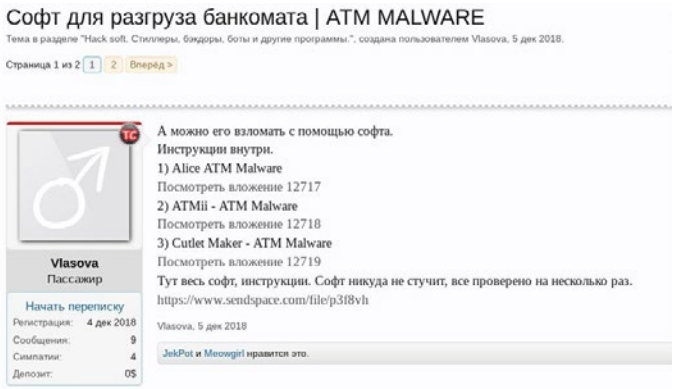
Как и в случае с ATMii, этот троян был снова выложен на форумах в декабре 2018 года, хотя известен он с ноября 2016. По сравнению с бесплатной Cutlet Maker, Alice менее удобен в использовании, и за прошедший период он не был замечен в активных атаках.



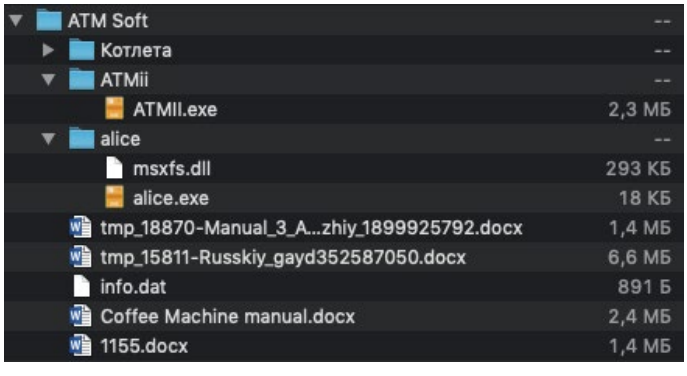
Cutlet Maker



WinPot (Cutlet V2)



ATMii



Alice

ТРОЯНЫ ДЛЯ ПК

Тренд на снижение активности банковских троянов для компьютеров только усугубился, а новые техники хищений перестали разрабатываться. Единственной страной, где эти трояны развиваются, остается Бразилия.

Список атакуемых не изменился, владельцев банковских бот-сетей в основном интересуют эти 18 стран: Австралия, Австрия, Болгария, Бразилия, Великобритания, Германия, Испания, Италия, Канада, Нидерланды, Норвегия, Польша, Россия, США, Украина, Франция, Швейцария, Япония. Большая часть активных троянов остается очень локальными и атакует пользователей 2-3 стран.

Старые

BackSwap, IcedID, Qbot, Gozi (ISFB, Ursnif), Trickbot, TinyNuke (aka NukeBot), Gootkit, Buhtrap, Dridex, Ramnit, Panda Banker, Retefe, Danabot, Osiris, Loki PWS

Новые

BANKER.THBAIAI, CamuBot

Исчезнувшие

Zeus, ZeusVM, Atmos, Corebot, UrlZone, Xbot, Toplel

	Польша	Испания	США	Канада	Великобритания	Нидерланды	Германия	Болгария	Австралия	Австрия	Франция	СНГ	Россия	Япония	Швейцария	Норвегия	Украина	Бразилия	Тайвань	Италия
BackSwap	■	■																		
IcedID			■	■	■															
Qbot		■	■	■		■														
Gozi (ISFB, Ursnif)				■					■					■						■
Trickbot		■	■	■	■	■	■	■	■	■										■
TinyNuke (aka NukeBot)	■										■									
Gootkit		■		■	■	■	■		■	■										■
RTM												■	■							
Buthrap													■							
Dridex 🌐	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
LokiPWS 🌐	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Ramnit			■	■	■								■	■						■
Panda Banker			■	■										■						
Retefe										■					■	■				
DanaBot	■		■				■		■	■							■			■
Osiris	■						■							■						
BANKER.THBAIAI																		■	■	
CamuBot																				■

🌐 глобально

США и Канада

В США ландшафт угроз, связанных с банковскими троянами для ПК, практически не изменился: основные атаки приходятся на IcedID, Trickbot, Dridex и в меньшей степени на Qbot, Ramnit, Panda Banker, Danabot. Ситуация в Канаде всегда была идентичной, и только владельцы одного из форков Gozi избрано нацелены на клиентов банков этой страны. IcedID по-прежнему продолжает использовать веб-инжекты и, в отличие от многих других банковских троянов, применяет автозалив для автоматического хищения денег с банковских счетов.

Из этого списка троянов стоит отметить Trickbot, который за последний год получил новый модуль для сбора паролей из установленных приложений, научился красть конфигурационные файлы из директорий SYSVOL на контроллере домена, начал использовать Mimikatz, проводить Fileless атаки и активно рассылать письма со скомпрометированных компьютеров. Новая версия трояна позволяет проводить целенаправленные атаки на крупные организации, и в скором будущем возможно появление новой группы, которая будет использовать Trickbot в целевых атаках на сами банки, а не на их клиентов.

Европа

Клиентам европейских банков по-прежнему угрожают BackSwap, Gootkit, Danabot, Osiris, TinyNuke, а простой банковский троян Retefe представляет основную угрозу для северных европейских стран.

Все эти трояны хорошо известны, относительно новым является BackSwap, который в прошлом году начал атаковать клиентов банков — сначала польских, а потом и испанских. В целом, Польша — единственная европейская страна, в которой заметен рост интереса атакующих.

Россия и СНГ

В России, «родине» большинства банковских троянов, остался только один активный банковский троян – RTM, но его жертвами становятся в основном клиенты слабо защищенных банков. Банковская бот-сеть Toplel прекратила свою активность, и новых хищений не происходит.

Владельцы бот-сети Buhtrap2 ранее использовали автозалив через российскую ERP систему 1С, однако такая схема позволяла детектировать зараженные устройства, поэтому хищения проводить не удавалось. В феврале 2019 года злоумышленники попытались оживить свою бот-сеть, но не получив экономического эффекта, они прекратили попытки.

Азиатско-тихоокеанский регион

Наиболее привлекательной страной для атакующих в этом регионе является Австралия, на нее нацелены Gozi, Trickbot, Gootkit, Ramnit, Danabot. Второй по популярности является Япония, список активных троянов здесь включает Gozi, Ramnit, Panda banker и Osiris. Несмотря на высокую численность населения и развитые банковские услуги, другие страны региона практически не интересуют атакующих.

Латинская Америка

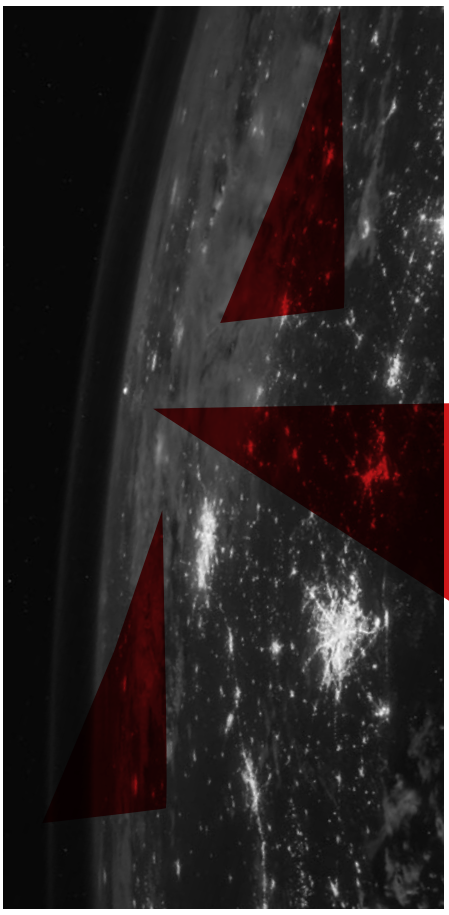
Как уже было отмечено, Бразилия становится основным источником новых банковских троянов, однако они используются только локально и разрабатываются скорее всего местными хакерами. Особенностью троянов из этого региона является демонстрация перекрывающих окон, эмулирующих работу банковского приложения.

MnuBot, обнаруженный в первой половине 2018 года, примечателен тем, что его составляющей является RAT-троян, который получает команды с сервера базы данных Microsoft SQL Server. С сервера управления также приходит конфигурационный файл со списком интересующих хакеров банков.

CamuBot начали использовать для атак в августе 2018 года, и нестандартным стал в первую очередь подход к его распространению. Вместо массовой дистрибуции, злоумышленники звонили жертве от имени банка и просили перейти на фишинговый сайт банка для загрузки «модуля безопасности». Загруженный в систему пользователя, CamuBot открывал туннель для компьютера жертвы и поддельный сайт банка, где пользователю предлагалось ввести логин и пароль от своего аккаунта.

Другой банковских троян был обнаружен в марте 2019, он не получил красивого названия и детектируется как BANKER.THBAIAI. Ниже описан весь набор инструментов, который мошенники используют для проведения атаки с его помощью.

1. Первый модуль заражает компьютер, загружает и выполняет PowerShell скрипты, которые записывают файлы .LNK в папку «автозагрузка» и вынуждают компьютер перезагружаться. После перезагрузки пользователю показывается поддельный экран входа в систему для перехвата логина и пароля.
2. Затем запускается второй троян, который пытается открыть Microsoft Outlook и получить все сохраненные в нем адреса электронной почты. Если Outlook отсутствует на компьютере, то этот шаг будет пропущен.
3. Дополнительно в систему устанавливается "RADMIN".
4. Последним устанавливается бестелесный банковский троян, который нацелен на данные клиентов бразильских банков Banco Bradesco, Banco do Brasil и Sicredi.



ТРОЯНЫ ДЛЯ ANDROID

Хищение денег с помощью банковских Android-троянов основано на одной из трех основных техник:

- денежные переводы по SMS;
- поддельное банковское мобильное приложение;
- сбор данных карт, логинов и паролей путем демонстрации поддельных окон.

Первые два способа имеют серьезные ограничения по масштабу хищений. Услуга перевода денег по SMS предоставляется малым количеством банков, а лимиты на перевод очень низкие. Распространение поддельных банковских мобильных приложений требует больших инвестиций и усилий для их рекламы и продвижения. Поэтому самым эффективным способом было и остаётся использование поддельных окон. Они показываются трояном поверх остальных окон и требуют от пользователя ввода нужных данных.

Когда в обновленных версиях Android ужесточилась политика безопасности, и приложения потеряли возможность показывать произвольные окна, схема с демонстрацией окон перестала работать. Большинство разработчиков Android-троянов не смогли адаптироваться под обновления, и множество эффективных троянов под Android перестали работать. Некоторые проекты закрылись, разработчики ушли, развитие этих троянов заметно замедлилось; снизился и ущерб от их действий.

Изначально коды для подтверждения банковских операций банки отправляли через SMS, однако с распространением мобильных приложений SMS заменили PUSH-уведомления. Они дешевле для банка и к тому же безопаснее, поскольку все банковские трояны под Android уже умеют перехватывать SMS. Это стало еще одной причиной снижения активности этих троянов.

Обойти ограничения безопасности возможно с помощью Accessibility Service — службы специальных возможностей, призванной облегчить работу с устройствами людям с ограниченными возможностями. Получив разрешение на использование Accessibility Service, вредоносное приложение фактически получает возможность перекрывать окна других приложений, управлять устройством голосовыми командами, прослушивать, а не просматривать контент, управлять PUSH-уведомлениями, тайно разблокировать устройство и выполнять произвольные действия, при этом держа экран отключенным.

Старые	Новые	Исчезнувшие
Red Alert, Anubis, Asacub, Loki v2, TarkBot (Rotexy), Flexnet, Riltok	Gustuff, Cerberus, CometBot, Exobot Compact, BasBanke	Agent.sx, Granzy, Agent.BID, LimeBot, Sagawa, Maza-in, Alienbot, Rello, Easy, CryEye, Cannabis, Fmif, AndyBot, Nero banker, Exobot

Автозалив на Android от Gustuff

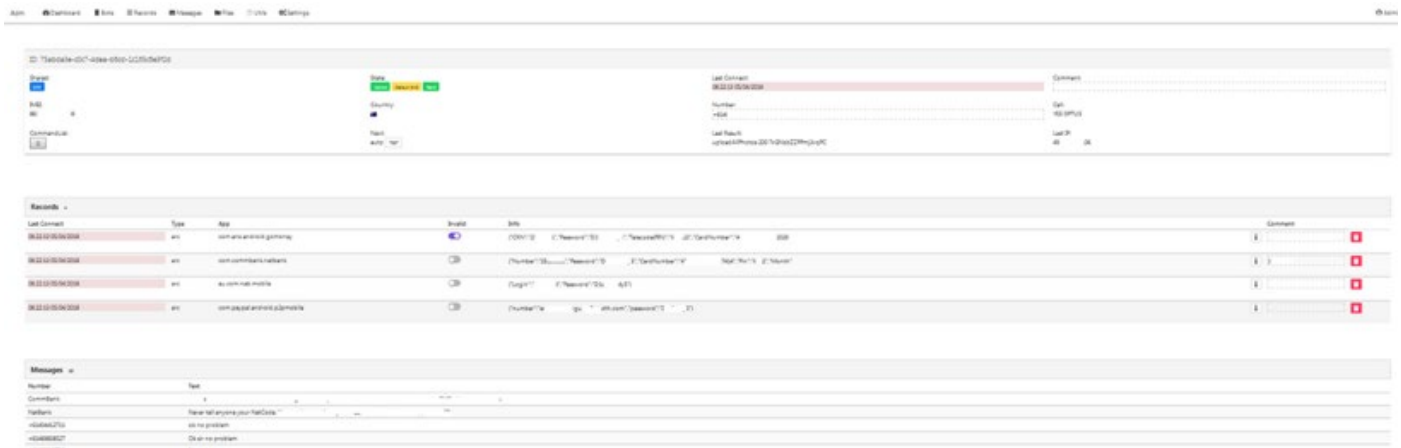
Gustuff является продолжением развития трояна AndyBot, принадлежит тому же автору и может выполнять следующие функции:

- отправлять на сервер информацию о заражённом устройстве;
- читать / отправлять SMS;
- отправлять USSD-запросы;
- запускать SOCKS5 Proxy;
- переходить по ссылке;
- демонстрировать push-уведомления;
- отправлять файлы (в том числе фотографии) на сервер;
- демонстрировать WEB-фейки;
- сбрасывать настройки устройства до заводских.

Троян использует Accessibility Service для взаимодействия с элементами окон приложений и может выполнять следующие действия: сфокусироваться на объекте, кликнуть на объект, изменить содержимое текста объекта. Таким образом, по команде сервера Gustuff может изменять значения полей в банковских приложениях.

Однако самым важным отличием Gustuff от других Android-троянов является возможность осуществления автозалива следующим образом:

- троян отправляет PUSH-уведомление пользователю с иконкой банковского приложения;
- пользователь нажимает на PUSH-уведомление;
- открывается банковское приложение;
- пользователь авторизуется в приложении;
- по команде сервера Gustuff осуществляет автозалив;
- Стоимость аренды составляет 800 долларов в месяц, при этом автор заботится о собственной безопасности и при продаже сообщает, что бот не работает в России, СНГ и США.

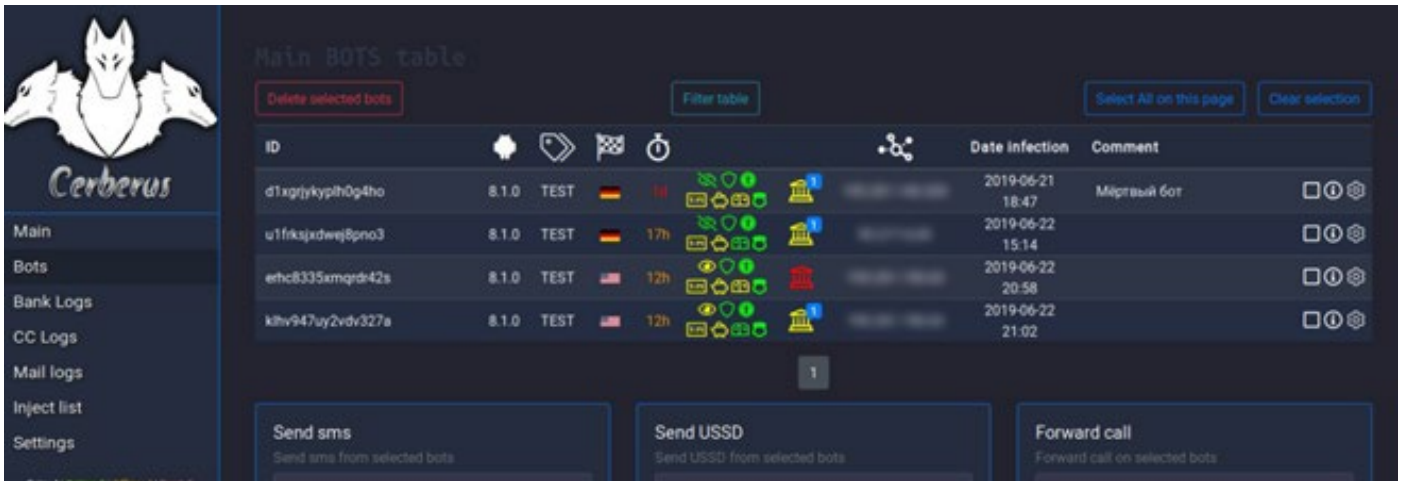


Новые адаптированные трояны без автозалива

Cerberus появился в продаже в июне 2019 года, по возможностям он напоминает Gustuff и тоже умеет работать с PUSH-уведомлениями от банков. Однако в трояне Cerberus реализованы следующие методы самозащиты:

- выключение Google Play Protect и отключение по истечении времени, установленного в панели администратора;
- блокировка удаления бота, блокировка отключения прав администратора, блокировка отключения Accessibility Service;
- определение запуска в песочнице благодаря анализу акселерометра.

Стоимость аренды составляет 2000 долларов в месяц, и по аналогии с Gustuff автор Cerberus также запрещает использовать троян на территории России и СНГ.



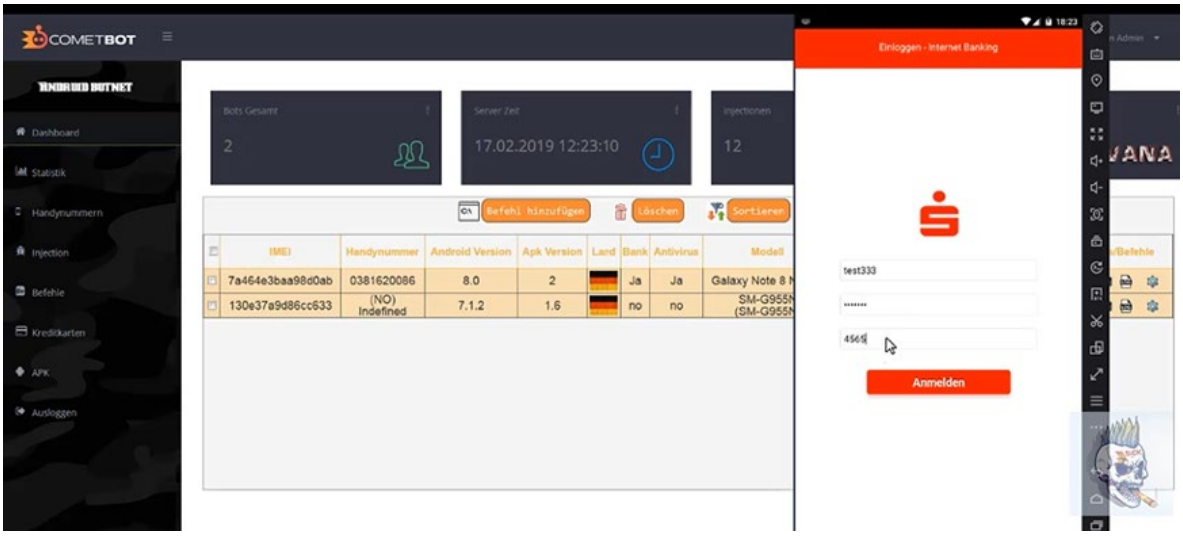
CometBot появился на хакерских форумах в феврале 2019 года, когда пользователь с псевдонимом "SickHavana" опубликовал объявление о сдаче его в аренду.

Этот троян сильно уступает по возможностям описанным выше, однако тоже поддерживает работу на последних версиях Android. Предложение включало готовые веб-фейки только под немецкие и один испанский банк с возможностью простого расширения для поддержки банков других регионов. Аренда **CometBot стоит 850 долларов в месяц.**

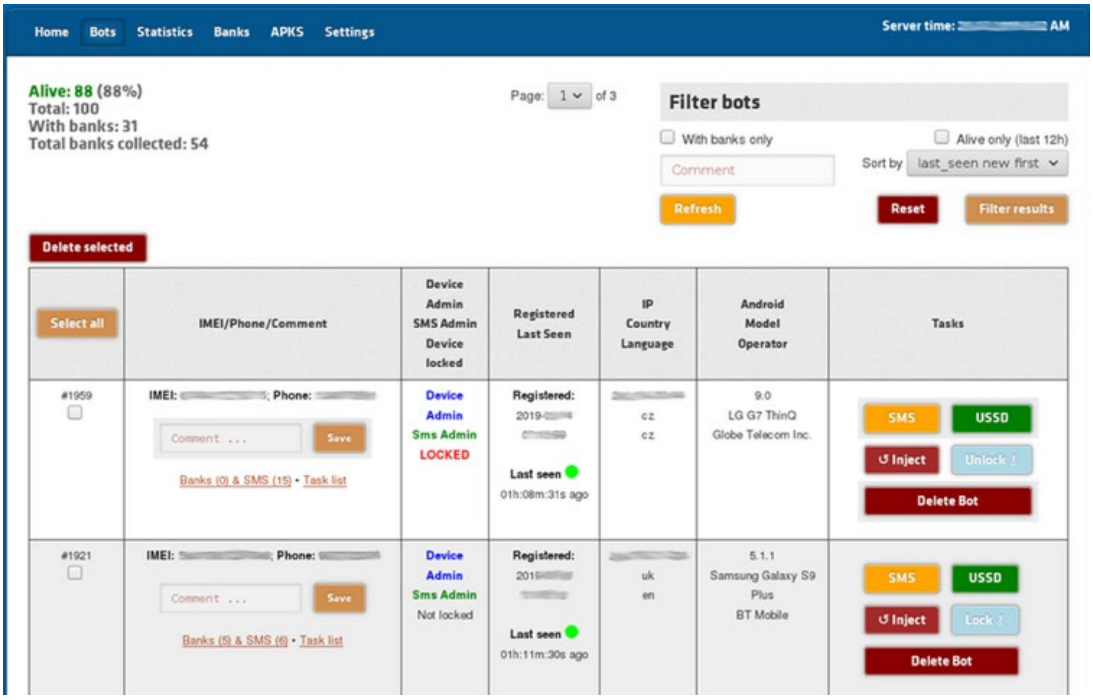
Exobot Compact начал продаваться в марте 2019 и является третьей версией хорошо известного и зарекомендовавшего себя трояна Exobot. В мае 2018 года исходные коды Exobot второй версии были выложены в открытый доступ, и новая версия была полностью переписана и оптимизирована. Exobot Compact может работать на современных версиях Android вплоть до Android 9.

Аналогично случаю с Gustuff автор запрещает работать в России, СНГ и США, но при этом поддельные страницы под американские банки у него есть. **Стоимость аренды составляет 1500 долларов в месяц.**

BasBanke — новый Android троян, нацеленный на пользователей бразильских банков. Функциональные возможности BasBanke достаточно простые, однако его владельцы сумели разместить его в Google Play, в результате чего он был загружен более 10 000 раз. Троян обладает функциями кейлогера, может делать запись с экрана и перехватывать SMS.

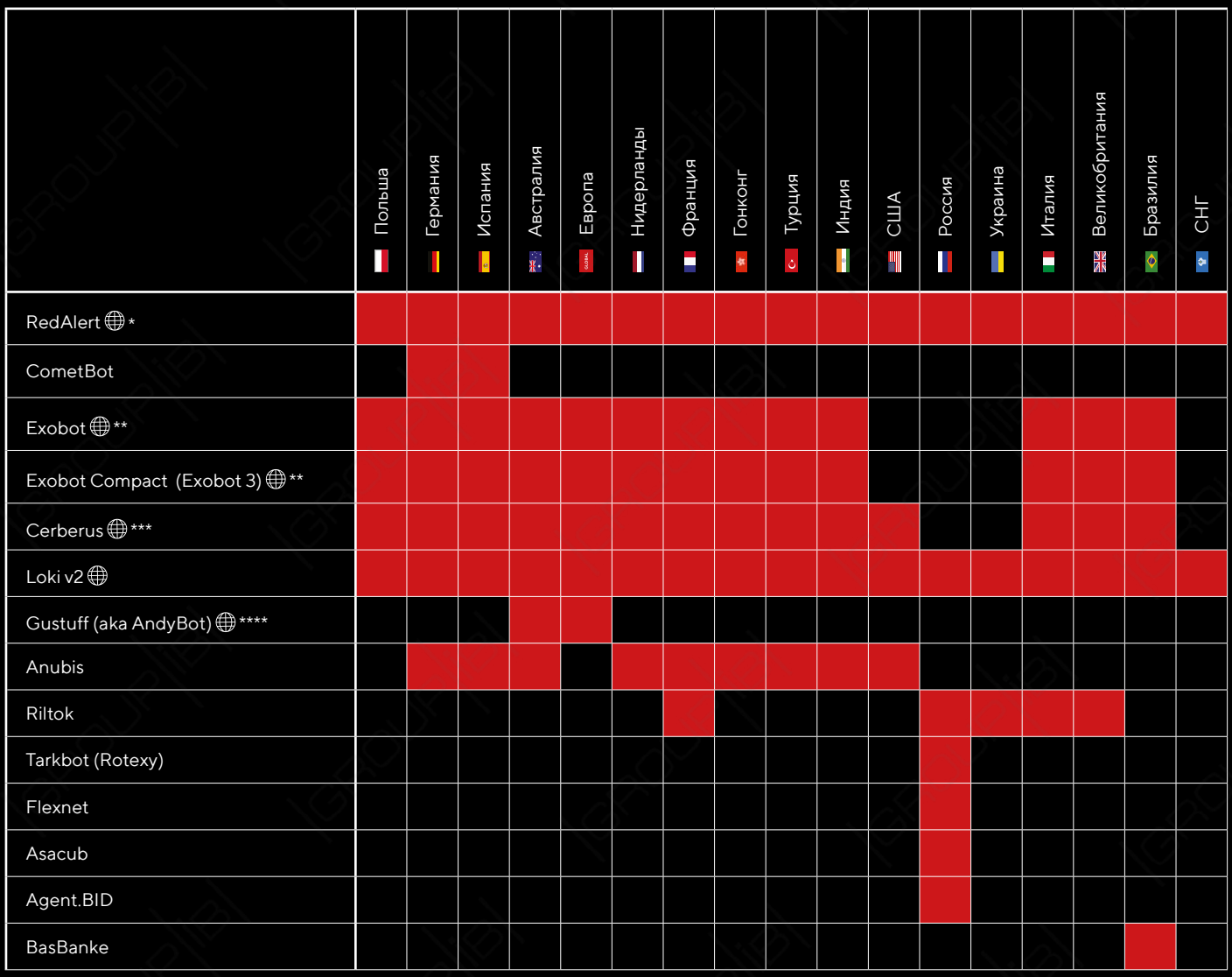


CometBot



Exobot Compact

ТРОЯНЫ ДЛЯ ANDROID



глобально

* более 200 целей в разных странах

** кроме СНГ и США

*** кроме СНГ

**** Запрещено использовать в СНГ и США

О GROUP-IB

Group-IB — один из ведущих мировых разработчиков решений для детектирования и предотвращения кибератак, выявления мошенничества и защиты интеллектуальной собственности в сети.

16 лет практического опыта	**60 000+** часов опыта реагирования	**1 000+** расследований по всему миру	**360+** специалистов и разработчиков

НАМ ДОВЕРЯЮТ

Клиентами Group-IB являются крупнейшие банки и финансовые организации, FMCG-бренды и промышленные корпорации, телеком-провайдеры, финтех и блокчейн-стартапы. Нас особенно ценят компании, которые заинтересованы в глубоком понимании и отражении киберугроз.

400+
enterprise-клиентов

60
стран

Эксперты Group-IB проводили тренинги по кибербезопасности:

- Для специалистов Europol, INTERPOL
- Правоохранительных органов
- Преподавателей университетов в Германии, Нидерландах, Бельгии, Франции, Таиланде, Бахрейне, Ливане и Великобритании

Мы охотимся за реальными киберпреступниками, препятствуя им в нанесении ущерба вашему бизнесу, и собираем безупречную доказательную базу. Этому мы обучаем профессионалов по всему миру.

OSCE

Рекомендована Организацией по безопасности и сотрудничеству в Европе

INTERPOL **EUROPOL**

Официальный партнер

SWIFT

Рекомендованный провайдер решений кибербезопасности

ПРОАКТИВНАЯ ЗАЩИТА И РЕАГИРОВАНИЕ

Укрепите кибербезопасность с помощью специалистов с практическим опытом реагирования и расследования сложных атак, использующих одну из самых продвинутых систем слежения за киберугрозами в мире.

АУДИТ И ОЦЕНКА РИСКОВ	THREAT HUNTING И РЕАГИРОВАНИЕ	КРИМИНАЛИСТИКА И РЕАГИРОВАНИЕ	ОБУЧАЮЩИЕ ПРОГРАММЫ
• Тестирование на проникновение • Анализ исходного кода • Выявление следов компрометации сети • Киберучения в формате Red Teaming • Проверка готовности к реагированию на инциденты • Оценка соответствия	• 24/7 Центр реагирования CERT-GIB • Проактивный хантинг угроз • Выездное реагирование на сложные кибератаки • Реагирование на инциденты «по подписке»	• Компьютерная криминалистика • Расследование финансовых и корпоративных киберпреступлений, атак на объекты КИИ	• Реагирование на инциденты • Анализ вредоносного кода • Проактивный поиск угроз

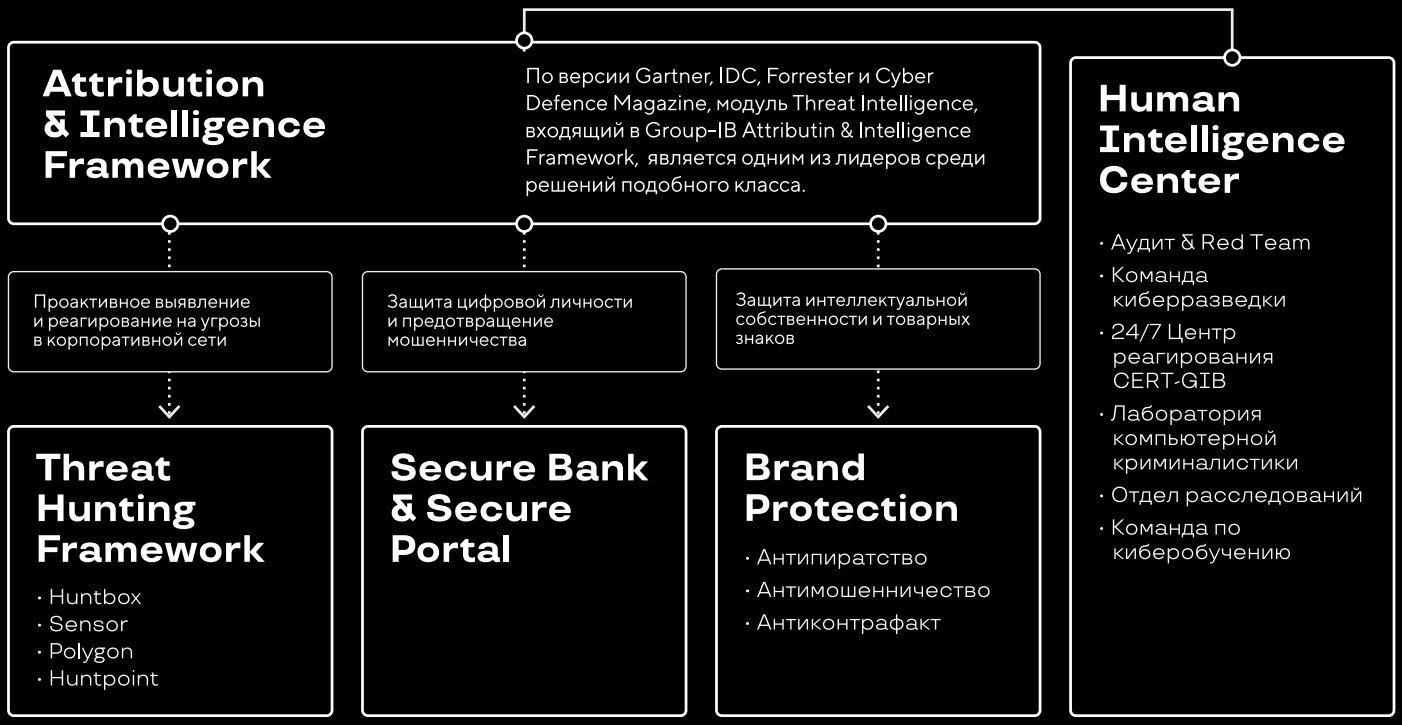
РЕАГИРОВАНИЕ 24/7

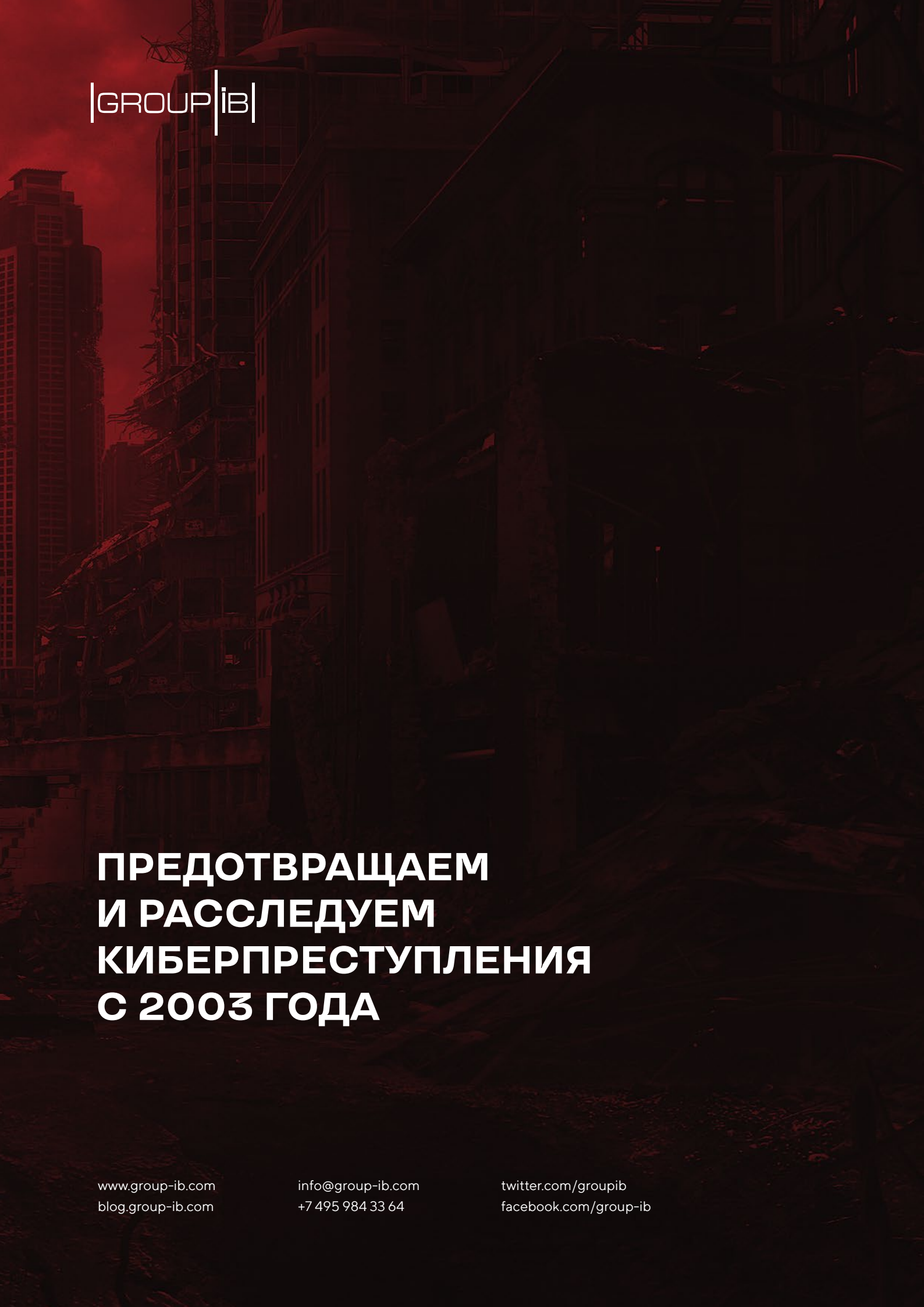
Центр реагирования CERT-GIB — аккредитованный член глобальных профессиональных сообществ FIRST и Trusted Introducer — активно сотрудничает с другими CERT, регистраторами доменных имен и хостинг-провайдерами для обеспечения оперативной блокировки опасных хостов и вредоносных сайтов по всему миру.

КРИМИНАЛИСТИКА И РАССЛЕДОВАНИЯ

Мы успешно расследовали APT и DDoS-атаки, мошенничества и хищения, атаки на объекты критической инфраструктуры, раскрывали сети онлайн-дистрибуции контрафакта и кампании по шпионажу. Наши знания, технологии и опыт позволяют находить злоумышленников, устанавливать их личности и добиваться для них обвинительных приговоров.

Экосистема решений Group-IB для мониторинга, выявления и предотвращения киберугроз





ПРЕДОТВРАЩАЕМ И РАССЛЕДУЕМ КИБЕРПРЕСТУПЛЕНИЯ С 2003 ГОДА

www.group-ib.com
blog.group-ib.com

info@group-ib.com
+7 495 984 33 64

twitter.com/groupib
facebook.com/group-ib