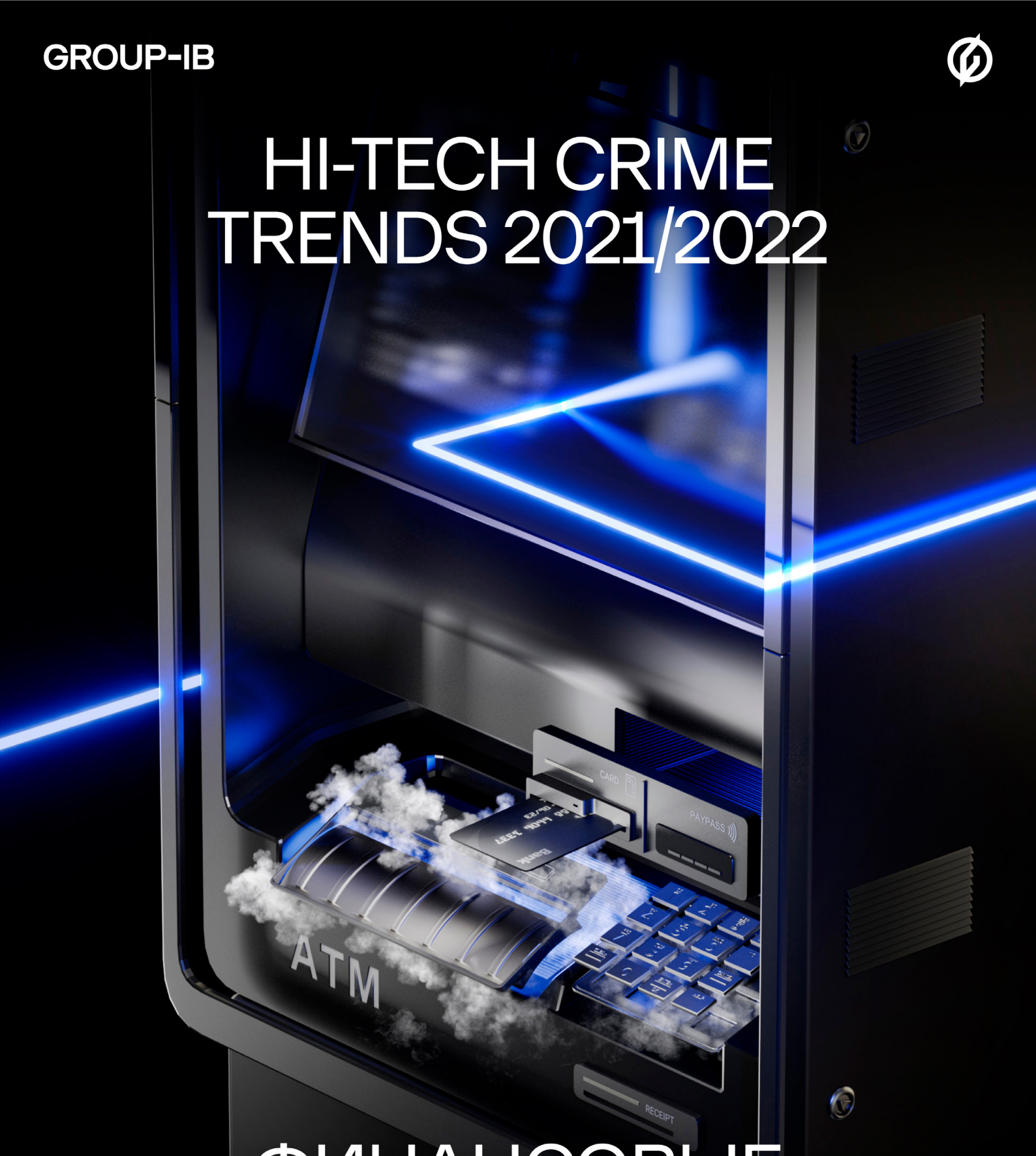
GROUP-IB

HI-TECH CRIME TRENDS 2021/2022



ФИНАНСОВЫЕ КИБЕРУГРОЗЫ

ДИСКЛЕЙМЕР

1. Отчет подготовлен специалистами Group-IB без какого-либо финансирования третьими лицами.
2. Целью отчета является предоставление сведений о тактике, инструментах и особенностях инфраструктуры различных групп для минимизации риска дальнейшего совершения таких противоправных деяний, их своевременного пресечения и формирования у читателей должного уровня правосознания. В отчете приведены рекомендации от экспертов Group-IB по превентивным мерам защиты от атак групп. Описание деталей угроз в отчете приведено исключительно для ознакомления с ними специалистов по информационной безопасности с целью предотвращения возникновения подобных инцидентов в дальнейшем и минимизации возможного ущерба. Опубликованная в отчете информация об угрозах не является пропагандой мошенничества и/или иной противоправной деятельности в сфере высоких технологий и/или иных сферах.
3. Отчет подготовлен в информационных и ознакомительных целях, ограничен в распространении и не может использоваться читателем в коммерческих и иных, не связанных с образованием или личным некоммерческим использованием целях. Group-IB предоставляет читателям право использовать отчет на территории всего мира путем скачивания, ознакомления с отчетом, цитирования отчета в объеме, оправданном правомерной целью цитирования, при условии, что сам отчет, включая ссылку на сайт правообладателя, на котором он размещен, будет указан как источник цитаты.
4. Отчет и все его части являются объектами авторского права и охраняются нормами права в области интеллектуальной собственности. Запрещается его копирование, распространение полностью или в части, в том числе путем копирования на другие сайты и ресурсы в сети Интернет, или любое иное использование информации из отчета без предварительного письменного согласия правообладателя. В случае нарушения авторских прав на отчет Group-IB вправе обратиться за защитой своих прав и интересов в суд и иные государственные органы с применением к нарушителю предусмотренных законодательством мер ответственности, включая взыскание компенсации.

HI-TECH CRIME TRENDS 2021/2022

Большой куш: угрозы для финансовых организаций

ГЛАВА 3

Ландшафт киберугроз: атаки шифровальщиков, кардинг, продажа доступов, фишинг и скам

ОГЛАВЛЕНИЕ

ПОЧЕМУ HI-TECH CRIME TRENDS?

00

Hi-Tech Crime Trends исследует разные аспекты функционирования киберкриминальной индустрии, анализирует атаки и прогнозирует изменение ландшафта угроз для различных отраслей мировой экономики. Отчет выпускается с 2012 года и интегрирует данные собственных исследований компании, реагирований на киберинциденты по всему миру.

Применяя уникальные инструменты слежения за инфраструктурой киберпреступников и тщательно изучая исследования специалистов из разных стран, эксперты Group-IB ежегодно находят и подтверждают общие паттерны глобального развития киберугроз. На основе этого формулируются прогнозы, которые сбываются каждый год с момента первой публикации отчета Hi-Tech Crime Trends. Они помогают компаниям во всем мире выстраивать эффективные стратегии кибербезопасности с учетом релевантных угроз.

Hi-Tech Crime Trends открывает доступ к максимально полному набору стратегических данных и подробной информации об актуальных киберугрозах в мире, как организациям, которые борются с киберпреступностью, так и потенциальным жертвам.

Hi-Tech Crime Trends предназначен для ИТ-директоров, руководителей команд кибербезопасности, SOC-аналитиков, специалистов по реагированию на инциденты, для которых отчет является практическим руководством стратегического и тактического планирования.

Прогнозы и рекомендации Hi-Tech Crime Trends направлены на сокращение финансовых потерь и простоев инфраструктуры, а также на принятие превентивных мер по противодействию целевым атакам, шпионажу и кибертеррористическим операциям.

Команда Group-IB убеждена в том, что постоянный обмен данными, создание и развитие партнерских отношений между частными компаниями и международными правоохранительными органами – эффективный путь борьбы с киберпреступностью. Осознанное отношение к кибербезопасности поможет сохранить и защитить глобальные возможности цифрового пространства и свободу коммуникаций.

ВВЕДЕНИЕ 01

Оценивая киберугрозы, которые нанесли наибольший ущерб организациям финансового сектора и их клиентам за второе полугодие 2020 по первое полугодие 2021, специалисты Group-IB выделили и проанализировали наиболее серьезную проблему для бизнеса, киберугрозу №1 — программы-вымогатели. Суммы выкупов, которые требовали операторы шифровальщиков от своих жертв, огромны — некоторые доходили до $50-70 млн, а последствия атак — беспрецедентны.

Феноменальный рост программ-вымогателей неразрывно связан с другим трендом — увеличением количества продавцов доступов в скомпрометированные сети. Подобные доступы могут использоваться как для проведения целевых атак, так и для распространения шифровальщиков и прочего вредоносного программного обеспечения. За отчетный период со второго полугодия 2020 по первое полугодие 2021 года специалистами **Group-IB Threat Intelligence** было выявлено **95** фактов продажи доступов в компании финансового сектора. Компании, к которым продавали доступ, расположены в следующих странах: Австралия, Бразилия, Великобритания, Вьетнам, Германия, Египет, Индия, Иран, Испания, Италия, Канада, Китай, Мексика, Нигерия, ОАЭ, Парагвай, Португалия, Россия, Саудовская Аравия, Сингапур, США, Таиланд, Филиппины, Франция, Чили, Япония. Чаще всего доступ предлагали в американские банки и финансовые организации.

Специалисты Group-IB также исследовали рынок фишинговых и мошеннических партнерских программ. Несмотря на то, что данное направление существует в андеграунде с 2017 года, в настоящее время количество «партнерок» достигло своего исторического максимума.

Другая опасность — распространение подложных платежных страниц, с которых деньги покупателей через легальные транзакции в банке уходят напрямую злоумышленникам.

После трехлетнего перерыва в России вновь стали актуальны атаки на АРМ КБР — автоматизированное рабочее место клиента Банка России. В начале 2021 года, предположительно, группа **MoneyTaker** совершила хищение в одном из российских банков.

Среди других финансово мотивированных хакерских групп специалисты Group-IB выделяют **OPERA1ER** (aka DESKTOP-GROUP, Common Raven, NXSMS), которая атаковала банки, финансовые организации и телекоммуникационные компании в Африке, Азии и Латинской Америке. В будущем OPERA1ER могут масштабировать свои атаки на другие регионы.

95

случаев продажи доступов в финансовые организации было выявлено за H2 2020-H1 2021

Доступы финансовых организаций 26 стран

были скомпрометированы

Эксперты Group-IB оценили текущую ситуацию на рынке кардинга, проанализировав основные кардшопы — площадки, где продаются данные скомпрометированных банковских карт. Этот рынок несколько просел из-за закрытия крупнейшего кардшопа Joker's Stash.

Традиционно была исследована активность банковских троянов для ПК и Android. Большая часть банкеров, которые были активны в период период со второго полугодия 2020 по первое полугодие 2021 года, разработана русскоговорящими злоумышленниками. Еще часть – латиноамериканскими. Именно в Латинской Америке динамично развивается рынок банкеров.

Специалисты Group-IB исследовали 11 наиболее опасных фишинг-китов. Многие из выявленных фишинговых китов были основаны на исходных кодах фреймворка **U-Admin**.

За отчетный период количество обнаруженных семейств JS-сниффероов выросло до 98, из них активными были **42** семейства. Наибольшую опасность JS-сниффероы представляют для компаний сферы онлайн-торговли: за прошедший год с их помощью было скомпрометировано более **80 000** банковских карт клиентов онлайн-магазинов.

80 000

банковских карт были скомпрометированы с помощью JS-сниффероов

КЛЮЧЕВЫЕ ТРЕНДЫ

02

БАНКОВСКИЕ ТРОЯНЫ ДЛЯ ПК ПОСТЕПЕННО ИСЧЕЗАЮТ

Латинская Америка остается единственным регионом, где банковские трояны представляют серьезную опасность. Но и там за отчетный период появилось только два новых банкера.

БАНКЕРЫ ДЛЯ ANDROID ПОКА ЕЩЕ АКТИВНЫ

Рынок банковских Android-троянов остался без существенных изменений. Однако появились три новых трояна — Ghimob, активный в основном в Латинской Америке, FluBot — в Европе, и TeaBot (Anatsa), активный в Европе и в России. FluBot и TeaBot стали представлять существенную угрозу. Их создатели строят свою работу по модели партнерской программы, привлекая в разных регионах большое количество людей с опытом распространения и совершения хищений с помощью Android-троянов.

ЗЛОУМЫШЛЕННИКИ ОСВАИВАЮТ TELEGRAM-БОТЫ И ПОКУПАЮТ ФИШИНГОВЫЕ ФРЕЙМВОРКИ

Злоумышленники, которые используют фишинговые фреймворки для атак, как правило, не разрабатывают их с нуля, а покупают уже готовый продукт. Многие популярные сейчас фишинговые фреймворки основаны на исходном коде старых и уже известных моделей, например U-Admin и Kr3pto. Другая тенденция — злоумышленники получают данные жертв с помощью Telegram-ботов. Ранее для этого использовалась электронная почта. Еще одна любопытная черта заключается в том, что злоумышленники атакуют банки и их клиентов в том же регионе, где живут. Такую тенденцию эксперты обнаружили в Нидерландах и Испании.

САМЫЙ ПОПУЛЯРНЫЙ СНИФФЕР — INTER

Им пользуется несколько десятков злоумышленников для кражи банковских карт.

РАСТЕТ КОЛИЧЕСТВО АТАК ПРОГРАММ-ВЫМОГАТЕЛЕЙ НА ФИНАНСОВЫЕ КОМПАНИИ

В отчетном периоде было выявлено 127 атак шифровальщиков, хотя в предыдущем их было менее 50.

РЫНОК ПРОДАЖИ ДОСТУПОВ РАСТЕТ

По сравнению с предыдущим периодом количество продавцов выросло с 18 до 47, а количество фактов продажи — с 31 до 95.

РЫНОК ПРОДАЖИ ДАННЫХ БАНКОВСКИХ КАРТ СОКРАЩАЕТСЯ

Количество данных банковских карт, выставленных на продажу, сильно сократилось в 2021 году, например по кредитным картам — вдвое. Одна из главных причин: в январе 2021 года был закрыт крупнейший кардшоп для продажи скомпрометированных данных банковских карт — Joker's Stash, занимавший до 40% всего рынка кардинга в мире. Кроме Joker's Stash, в 2021 году закрылись еще более 10 более мелких кардшопов. Несмотря на это, доля дампов банковских карт, выставленных на продажу остальными кардшопами, осталась прежней.

РАЗВИВАЕТСЯ РЫНОК ПОДЛОЖНЫХ ПЛАТЕЖНЫХ СТРАНИЦ

Финансовый ущерб от подобных атак только в России составил около 3,15 млрд. рублей за отчетный период. За исследуемый период более 40 млн. запросов на подтверждение операций по картам были проведены на фишинговых ресурсах.

ФИШИНГОВЫЕ ПАРТНЕРКИ СТАНОВЯТСЯ ВСЕ БОЛЕЕ ПОПУЛЯРНЫМИ

По оценкам экспертов Group-IB, на данный момент существует более 70 «партнерок». За отчетный период их общая прибыль составила как минимум $10 000 000.

ПОЯВЛЯЮТСЯ НОВЫЕ СПОСОБЫ ОБФУСКАЦИИ JS-СНИФФЕРОВ

Это происходит из-за того, что прошлые методы уже не позволяют в течение долгого времени сохранять код невидимым для антивирусных средств.

ПРОГНОЗЫ 03

ФИШИНГОВЫЕ ФРЕЙМВОРКИ РАСПРОСТРАНЯТСЯ НА ДРУГИЕ РЕГИОНЫ

Если раньше фишинговые фреймворки в основном были нацелены на европейские банки, то уже в ближайшем будущем подобная угроза будет актуальна для банков Азиатско-Тихоокеанского региона и Северной Америки.

TELEGRAM — САМЫЙ ПОПУЛЯРНЫЙ ИНСТРУМЕНТ ЗЛОУМЫШЛЕННИКОВ

Telegram станет самым популярным способом для получения злоумышленниками скомпрометированных данных с фишинговых сайтов.

ГРУППА MONEYTAKER ПРОДОЛЖИТ АТАКОВАТЬ РОССИЮ

После долгого затишья группа MoneyTaker успешно атаковала российский банк. Очевидно, что злоумышленники на этом не остановятся и будут продолжать атаковать АРМ КБР.

УВЕЛИЧИТСЯ КОЛИЧЕСТВО ПРОДАВАЕМЫХ ДОСТУПОВ В ФИНАНСОВЫЕ КОМПАНИИ

Это произойдет из-за роста рынка продажи доступов. В результате увеличится число атак программ-вымогателей на банки и финансовые компании.

ВЫРАСТЕТ КОЛИЧЕСТВО ФИШИНГОВЫХ И МОШЕННИЧЕСКИХ ПАРТНЕРСКИХ ПРОГРАММ

На данный момент они в основном имитируют сервисы доставки и маркетплейсы. В будущем злоумышленники будут активнее развивать фишинговые партнерки под финансовый сектор. Такой вид мошенничества может стать более высокотехнологичной заменой звонков от фейковых колл-центров.

КРИПТОВАЛЮТА В ОПАСНОСТИ

Увеличится количество фишинговых атак, направленных на кражу криптовалюты.

КАРДИНГ СТАНЕТ МЕНЕЕ ПРИВЛЕКАТЕЛЬНЫМ ДЛЯ КИБЕРПРЕСТУПНИКОВ

После закрытия множества кардшопов мы ожидаем, что количество продаж банковских карт будет постепенно снижаться. Прежде всего это коснется продаж дампов.

ВЫРАСТЕТ КОЛИЧЕСТВО ФИШИНГОВЫХ ФРЕЙМВОРКОВ

Это произойдет в том числе потому, что банки все чаще внедряют многофакторную аутентификацию.

УСЛУГИ В ФОРМАТЕ PHISHING-AS-A-SERVICE БУДУТ РАЗВИВАТЬСЯ ДАЛЬШЕ

Это позволит проводить атаки даже тем злоумышленникам, которые не умеют сами создавать вредоносное ПО. Будут появляться злоумышленники, предлагающие арендовать фишинговую инфраструктуру на неделю или месяц. Такая бизнес-модель уже используется в Нидерландах, и она может распространиться на другие регионы.

ОСНОВНАЯ УГРОЗА ДЛЯ ОНЛАЙН-РИТЕЙЛА – JS-СНИФФЕРЫ

Особенно это коснется небольших американских бизнесов, работающих под управлением CMS Magento, OpenCart. При этом основные риски будут связаны со штрафами за нарушение безопасности, а не с возмещением ущерба клиентам или репутационными потерями.

ПРОДОЛЖАТСЯ ЭКСПЕРИМЕНТЫ С JS-СНИФФЕРАМИ

Операторы JS-сниффероов продолжат экспериментировать со способами доставки кода и передачей украденных данных, а также с разработкой автоматических средств обфускации кода. Семейство сниффероов Inter останется самым распространенным.

ПРОДАЖА ДОСТУПОВ В ФИНАНСОВЫЕ ОРГАНИЗАЦИИ

04

Одной из наиболее явных тенденций на андеграундных форумах последних четырех лет является резкое увеличение количества предлагаемых на продажу доступов к скомпрометированным корпоративным сетям компаний.

Доступ к корпоративной сети может осуществляться через данные учетных записей RDP, VPN, Citrix Gateway (далее просто Citrix), панели управления, веб-шелл, обратный шелл, сессию Cobalt Strike и др. Независимо от типа, доступ дает злоумышленнику возможность проникнуть в сеть и получить права ее легитимного пользователя или администратора.

Рынок доступов отличается низким порогом входа. Злоумышленник может получить доступ с помощью инфостиллера, в результате брутфорса или целенаправленной атаки на жертву. Если в последнем случае требуются глубокие знания и навыки, то в первых двух злоумышленник не способен развить атаку до получения прибыли, самостоятельно используя доступ. В сценарии с использованием инфостилера даже не нужно думать о способе доставки этого вредоносного ПО на компьютеры жертв — результаты работы инфостилеров продаются на андеграундных форумах в виде архивов, содержащих различные скомпрометированные учетные записи: как личные, так и рабочие. От злоумышленника требуется лишь отыскать среди такого набора действующие аккаунты корпоративных ресурсов. Сценарий с брутфорсом также не требует серьезных знаний — готовые программы для подбора паролей есть в открытом доступе. Атакующему нужно лишь выбрать жертву.

Доступность необходимых средств для проведения полноценной атаки на корпоративную сеть стало для многих представителей андеграунда источником легкой прибыли. Так рынок продаж доступов наводнило большое количество низкоквалифицировнных злоумышленников, которые слабо ориентируются в технической части, но при этом представляют большую угрозу для компаний.

На рынке доступов представлены разные частные и государственные компании разных отраслей. В данном отчете мы фокусируемся на банках и финансовых компаниях. Чтобы узнать больше о рынке доступов к скомпрометированным ресурсам компаний, смотрите отчет «**Незваные гости: продажа доступов в сети компаний**».

206%

на столько увеличилось количество продавцов доступов за прошедший год

Незваные гости: продажа доступов в сети компаний

За последний год количество продаваемых доступов в банки и финансовые организации выросло почти на **206%** — с 31 (H2 2019 – H1 2020) до 95 (H2 2020 – H1 2021). Количество продавцов также увеличилось с 18 до 47.

За период H2 2020 – H1 2021 прибыль продавцов доступов в компании финансового сектора составила, как минимум, $530 000. Чаще всего их жертвами становились банки и финансовые организации США (22 факта продажи за последний год).

Дата публикации объявления	Псевдоним продавца	Регион компании-жертвы	Цена продажи доступа, USD	Выручка компании, млн. USD
01.07.2020	vasyldn	Великобритания	1500	
06.07.2020	drumrlu	Таиланд		
13.07.2020	pshmm	Португалия	2500	
13.07.2020	pshmm	Канада	2500	
15.07.2020	drumrlu	Саудовская Аравия	3000	
27.07.2020	vasyldn	Великобритания	5000	
27.07.2020	vasyldn	Мексика	500	
29.07.2020	EronM	Сингапур	12000	3000
04.08.2020	EronM	США	6500	3200
04.08.2020	vasyldn	Великобритания	5800	
04.08.2020	vasyldn	Мексика	600	
12.08.2020	bc.monster	Бразилия	2000	
21.08.2020	r41s3r	Парагвай	3000	
25.08.2020	itrade4living	Австралия	2500	5460
25.08.2020	Nikolay (aka Marlon_Brando aka LinuxW)	США	20000	
26.08.2020	EronM	Франция	5000	22000
04.09.2020	davidarnold0151	Япония		
05.09.2020	r0t	Австралия	10000	
12.09.2020	pshmm	США	1500	6
13.09.2020	petervodz (aka johnakamai)	Канада	400	10
13.09.2020	petervodz (aka johnakamai)	Канада	800	25
15.09.2020	pshmm	Великобритания	1750	232
17.09.2020	drumrlu	Таиланд	2000	
19.09.2020	drumrlu	Вьетнам	3000	
19.09.2020	pshmm		2000	17
21.09.2020	NetNet	США	700	35
23.09.2020	NetNet	США	700	35
25.09.2020	vasyldn	Мексика	5000	

Дата публикации объявления	Псевдоним продавца	Регион компании-жертвы	Цена продажи доступа, USD	Выручка компании, млн. USD
27.09.2020	Andreich_kms	Франция	100	1
27.09.2020	Andreich_kms	Испания	100	2
27.09.2020	Andreich_kms		100	10
27.09.2020	drumrlu	Таиланд	1000	140
03.10.2020	Zorbon	Иран	12000	
08.10.2020	magicman1337	Россия		
11.10.2020	3073a (aka DarkGod3)	Китай	4000	49
11.10.2020	magicman1337			100000
12.10.2020	Medusa23	Нигерия	4000	9000
17.10.2020	bryanross		11500	1000
24.10.2020	iannker	США	10000	
26.10.2020	artur11	Филиппины		
30.10.2020	3073a (aka DarkGod3)	Италия	3000	2
06.11.2020	pshmm	США	1500	6
07.11.2020	LORD1			50000
08.11.2020	artur11	Филиппины	2400	
11.11.2020	drumrlu	ОАЭ	2000	800
11.11.2020	drumrlu	Саудовская Аравия	2000	15
23.11.2020	Cipher-Strike	ОАЭ		
02.12.2020	zanko	Индия	20000	
02.12.2020	JxB1990	США	600	5
02.12.2020	pshmm	США	2000	
07.12.2020	realname	США	4999	
09.12.2020	Medusa23	ОАЭ		
12.12.2020	zanko	Индия	4000	49
13.12.2020	SHERIFF		23500	1000
13.12.2020	SHERIFF		23500	1000
13.12.2020	SHERIFF		23500	1000
13.12.2020	SHERIFF		23500	1000
13.12.2020	SHERIFF		23500	
13.12.2020	SHERIFF		23500	
13.12.2020	SHERIFF		23500	
13.12.2020	SHERIFF		23500	
17.12.2020	JPDeadly	Германия		400
24.12.2020	maroder	Чили	7000	1000
25.12.2020	barf	США	100	1
04.01.2021	x_04X		1500	

Дата публикации объявления	Псевдоним продавца	Регион компании-жертвы	Цена продажи доступа, USD	Выручка компании, млн. USD
05.01.2021	EvilKitten	Иран	7000	100
27.01.2021	7h0rf1nn	Франция	1000	
29.01.2021	zanko	Индия	500	5
09.02.2021	Expl0i7	США	5000	
24.02.2021	cc2btc		10000	79000
28.02.2021	barf	Иран	1500	1700
01.03.2021	pshmm	Канада	500	
02.03.2021	Aristokrat	Таиланд		
08.03.2021	Nei	США	300	5
14.03.2021	drumrlu	США	1000	19
15.03.2021	vasyldn	США	5000	
16.03.2021	vasyldn	США	2000	
16.03.2021	vasyldn	США	10000	
19.03.2021	vasyldn	США	20000	
22.03.2021	babam	Мексика	150	4
29.03.2021	drumrlu	Индия	1500	41
14.04.2021	groupby	США	2500	18
19.04.2021	novichok2021	Италия	100	2
23.04.2021	gospoda		5000	
26.04.2021	babam	ОАЭ	1000	2000
27.04.2021	NaMneCash	Египет		
07.05.2021	fab1us	Египет		2000
08.05.2021	zanko	Индия	5000	
08.05.2021	Suraj	Индия	3000	3400
10.05.2021	scredou	ОАЭ	10000	1000
18.05.2021	Novelli	США	300	1
28.05.2021	vasyldn	США	50000	1000
29.05.2021	Alexlogin	Австралия	1000	
26.06.2021	babam	Великобритания	5000	
28.06.2021	T3atral	США	500	

Одним из главных факторов роста рынка продажи доступов стало резкое увеличение числа атак с использованием программ-шифровальщиков. Деятельность продавцов доступов избавляет операторов шифровальщиков от усилий по взлому и проникновению в сеть компаний на первом этапе атаки.

АТАКИ ШИФРОВАЛЬЩИКОВ НА ФИНАНСОВЫЕ ОРГАНИЗАЦИИ

05

Специалисты Group-IB Threat Intelligence фиксируют значительный рост количества с использованием программ-шифровальщиков на финансовые организации. За отчетный период (H2 2020 — H1 2021) было выявлено **127** таких атак. За прошлый аналогичный период (H2 2019 — H1 2020) — менее 50.

В Group-IB зафиксировали активность **24 групп**, атакующих финансовый сектор. Чаще всего атаки проводили группы **REvil**, **Conti** и **Avaddon**. Большинство пострадавших компаний расположены в США **(66)**, второе место делят Канада и Великобритания **(12)**. На третьем месте — Франция **(8)**.

Данные представлены в таблице:

Дата атаки	Индустрия	Страна штаб-квартиры	Группа шифровальщиков
13.07.2020	Финансовые услуги	США	DoppelPaymer
08.08.2020	Финансовые услуги	США	Darkside
18.08.2020	Финансовые услуги: бухгалтерия	США	REvil
18.08.2020	Финансовые услуги	США	REvil
18.08.2020	Финансовые услуги: страхование	США	REvil
19.08.2020	Финансовые услуги: бухгалтерия	США	NetWalker
20.08.2020	Финансовые услуги	США	REvil
20.08.2020	Финансовые услуги: бухгалтерия	Канада	REvil
20.08.2020	Финансовые услуги	Индия	Clop
20.08.2020	Финансовые услуги: бухгалтерия	Великобритания	REvil
24.08.2020	Финансовые услуги	Гонконг	REvil
30.08.2020	Финансовые услуги	США	NetWalker
02.09.2020	Финансовые услуги: страхование	США	DoppelPaymer
14.09.2020	Финансовые услуги: страхование	США	Conti
25.09.2020	Финансовые услуги: страхование	США	Egregor
25.09.2020	Финансовые услуги: страхование	США	Conti
28.09.2020	Финансовые услуги: бухгалтерия	США	MAZE

Дата атаки	Индустрия	Страна штаб-квартиры	Группа шифровальщиков
08.10.2020	Финансовые услуги	Канада	NetWalker
14.10.2020	Финансовые услуги: бухгалтерия	Тринидад и Тобаго	REvil
20.10.2020	Финансовые услуги: бухгалтерия	США	Conti
20.10.2020	Финансовые услуги: страхование	США	Egregor
20.10.2020	Финансовые услуги: бухгалтерия	Франция	Egregor
20.10.2020	Финансовые услуги: страхование	США	Egregor
20.10.2020	Финансовые услуги: страхование	США	Egregor
22.10.2020	Финансовые услуги: страхование	США	REvil
26.10.2020	Финансовые услуги: страхование	США	Darkside
01.11.2020	Финансовые услуги	Канада	Pysa
06.11.2020	Финансовые услуги	США	Egregor
14.11.2020	Финансовые услуги: банкинг	США	Avaddon
18.11.2020	Финансовые услуги: страхование	США	Egregor
20.11.2020	Финансовые услуги: бухгалтерия	США	Egregor
21.11.2020	Финансовые услуги: страхование	Великобритания	Egregor
23.11.2020	Финансовые услуги	Италия	Pysa
25.11.2020	Финансовые услуги	Испания	NetWalker
26.11.2020	Финансовые услуги	Зимбабве	Egregor
27.11.2020	Финансовые услуги: бухгалтерия	Канада	NetWalker
28.11.2020	Финансовые услуги: бухгалтерия	Великобритания	NetWalker
02.12.2020	Финансовые услуги: банкинг	США	Egregor
03.12.2020	Финансовые услуги: банкинг	Индия	Everest
09.12.2020	Финансовые услуги: бухгалтерия	Канада	Conti
11.12.2020	Финансовые услуги	Индия	Egregor
11.12.2020	Финансовые услуги	Новая Зеландия	NetWalker
18.12.2020	Финансовые услуги	США	Egregor
19.12.2020	Финансовые услуги: страхование	США	Conti
28.12.2020	Финансовые услуги: бухгалтерия	США	Ragnarok
30.12.2020	Финансовые услуги	Бельгия	Avaddon
08.01.2021	Финансовые услуги: страхование	Канада	DoppelPaymer
11.01.2021	Финансовые услуги	США	Conti
14.01.2021	Финансовые услуги	США	NetWalker
20.01.2021	Финансовые услуги	США	Darkside
25.01.2021	Финансовые услуги: бухгалтерия	США	NetWalker
25.01.2021	Финансовые услуги	Люксембург	DoppelPaymer
28.01.2021	Финансовые услуги	Гонконг	RansomEXX
30.01.2021	Финансовые услуги: бухгалтерия	Италия	Pysa
01.02.2021	Финансовые услуги: страхование	Индонезия	Avaddon

Дата атаки	Индустрия	Страна штаб-квартиры	Группа шифровальщиков
03.02.2021	Финансовые услуги: страхование	Франция	Avaddon
04.02.2021	Финансовые услуги: банкинг	США	Darkside
08.02.2021	Финансовые услуги: страхование	США	REvil
11.02.2021	Финансовые услуги	США	Pysa
15.02.2021	Финансовые услуги: бухгалтерия	США	Avaddon
18.02.2021	Финансовые услуги	США	Cuba
22.02.2021	Финансовые услуги: бухгалтерия	США	Everest
22.02.2021	Финансовые услуги: страхование	Мексика	Nefilim
22.02.2021	Финансовые услуги	Канада	DoppelPaymer
26.02.2021	Финансовые услуги: банкинг	Нигерия	REvil
27.02.2021	Финансовые услуги: банкинг	Мексика	REvil
28.02.2021	Финансовые услуги: бухгалтерия	США	Lorenz
28.02.2021	Финансовые услуги	Ямайка	Darkside
02.03.2021	Финансовые услуги: банкинг	Индонезия	Darkside
02.03.2021	Финансовые услуги: страхование	США	REvil
06.03.2021	Финансовые услуги: страхование	США	REvil
08.03.2021	Финансовые услуги: банкинг	США	Clop
09.03.2021	Финансовые услуги: страхование	США	REvil
09.03.2021	Финансовые услуги: банкинг	США	Ragnar Locker
09.03.2021	Финансовые услуги: банкинг	США	Ragnar Locker
11.03.2021	Финансовые услуги: страхование	США	Babuk v.1
12.03.2021	Финансовые услуги: бухгалтерия	США	DoppelPaymer
13.03.2021	Финансовые услуги: страхование	США	Darkside
14.03.2021	Финансовые услуги: бухгалтерия	США	LV v.1
14.03.2021	Финансовые услуги: бухгалтерия	США	LV v.2
16.03.2021	Финансовые услуги	США	Conti
17.03.2021	Финансовые услуги	Канада	Conti
20.03.2021	Финансовые услуги: страхование	США	Darkside
23.03.2021	Финансовые услуги: бухгалтерия	США	Clop
23.03.2021	Финансовые услуги: банкинг	США	REvil
23.03.2021	Финансовые услуги: банкинг	США	REvil
28.03.2021	Финансовые услуги	Испания	Ragnarok
28.03.2021	Финансовые услуги: страхование	США	DoppelPaymer
04.04.2021	Финансовые услуги	США	REvil
09.04.2021	Финансовые услуги: бухгалтерия	США	Avaddon
13.04.2021	Финансовые услуги	США	Marketo
17.04.2021	Финансовые услуги	США	REvil
18.04.2021	Финансовые услуги	Германия	REvil

Дата атаки	Индустрия	Страна штаб-квартиры	Группа шифровальщиков
19.04.2021	Финансовые услуги	Испания	Avaddon
22.04.2021	Финансовые услуги	Великобритания	Conti
22.04.2021	Финансовые услуги: бухгалтерия	Великобритания	Conti
01.05.2021	Финансовые услуги	Канада	REvil
10.05.2021	Финансовые услуги	Сальвадор	Prometheus
12.05.2021	Финансовые услуги	Франция	Avaddon
13.05.2021	Финансовые услуги	Италия	Babuk v.1
13.05.2021	Финансовые услуги	Великобритания	Avaddon
15.05.2021	Финансовые услуги: страхование	Франция	Avaddon
18.05.2021	Финансовые услуги: страхование	США	Conti
20.05.2021	Финансовые услуги	Франция	Prometheus
20.05.2021	Финансовые услуги: бухгалтерия	Великобритания	Conti
20.05.2021	Финансовые услуги	Великобритания	Conti
20.05.2021	Финансовые услуги	Великобритания	Avaddon
20.05.2021	Финансовые услуги: бухгалтерия	Кипр	Avaddon
28.05.2021	Финансовые услуги	Ямайка	Avaddon
28.05.2021	Финансовые услуги: бухгалтерия	Великобритания	REvil
31.05.2021	Финансовые услуги	Франция	Everest
01.06.2021	Финансовые услуги	Канада	Grief
03.06.2021	Финансовые услуги: страхование	США	Vice Society
05.06.2021	Финансовые услуги: бухгалтерия	Великобритания	Conti
08.06.2021	Финансовые услуги: банкинг	США	Avaddon
12.06.2021	Финансовые услуги: страхование	США	REvil
14.06.2021	Финансовые услуги: бухгалтерия	США	REvil
14.06.2021	Финансовые услуги	Канада	REvil
15.06.2021	Финансовые услуги	Бразилия	Prometheus
16.06.2021	Финансовые услуги	США	Conti
19.06.2021	Финансовые услуги: бухгалтерия	ЮАР	REvil
19.06.2021	Финансовые услуги: бухгалтерия	Великобритания	REvil
21.06.2021	Финансовые услуги	Франция	Everest
21.06.2021	Финансовые услуги	Мексика	LV v.1
23.06.2021	Финансовые услуги: бухгалтерия	Франция	Conti
25.06.2021	Финансовые услуги: страхование	Канада	Conti
25.06.2021	Финансовые услуги: страхование	США	Conti

ФИШИНГОВЫЕ И МОШЕННИЧЕСКИЕ ПАРТНЕРСКИЕ ПРОГРАММЫ

06

В последние годы широкое распространение получили фишинговые и мошеннические партнерские программы. По оценкам экспертов Group-IB, существует около 70 фишинговых и мошеннических партнерских программ. Цель участников фишинговых и мошеннических партнерских программ — кража денег, персональных и платежных данных. Их общая прибыль составила как минимум $10 000 000 за отчетный период. Средняя сумма хищений участниками партнерок составляет $83. В «партнерках» задействовано большое количество участников, есть строгая иерархия и сложная техническая инфраструктура для автоматизации мошенничества. Это позволяет масштабировать фишинговые кампании как под банки, так и под популярные почтовые сервисы, маркетплейсы, логистические и другие компании.

Распределение атакуемых брендов по отраслям

Название	%
Маркетплейсы	**69,6%**
Сервисы доставки	**17,2%**
Сервисы совместного использования автомобилей	**12,8%**
Банковские услуги	**0,4%**

Отработав схему с обманом пользователей в России и СНГ, партнерки начали онлайн-миграцию в страны Европы, Америки, Азии, Ближнего Востока. Одним из таких примеров является **Classiscam** — мошенническая схема, популярная среди скам-партнерок. На данный момент участники «партнерок» атакуют пользователей в следующих странах:

Атаки Classiscam по странам

Россия, Казахстан, Беларусь, Румыния, Польша, Украина, Чехия, Болгария, Узбекистан, Франция, Азербайджан, Киргизия, Молдова, Италия, Испания, Эстония, Швеция, Катар, Остальные страны Европейского союза, Финляндия, Австралия, Мексика, Филипинны, Словакия, Латвия, Литва, США, Грузия, Норвегия, Ирландия, Дания, Венгрия, Кипр, Хорватия, Австрия, ОАЭ, Македония

31 страна
была подвержена атакам Classiscam

Первые фишинг-партнерки появились в 2017 году, и с тех пор их количество растет с каждым годом:

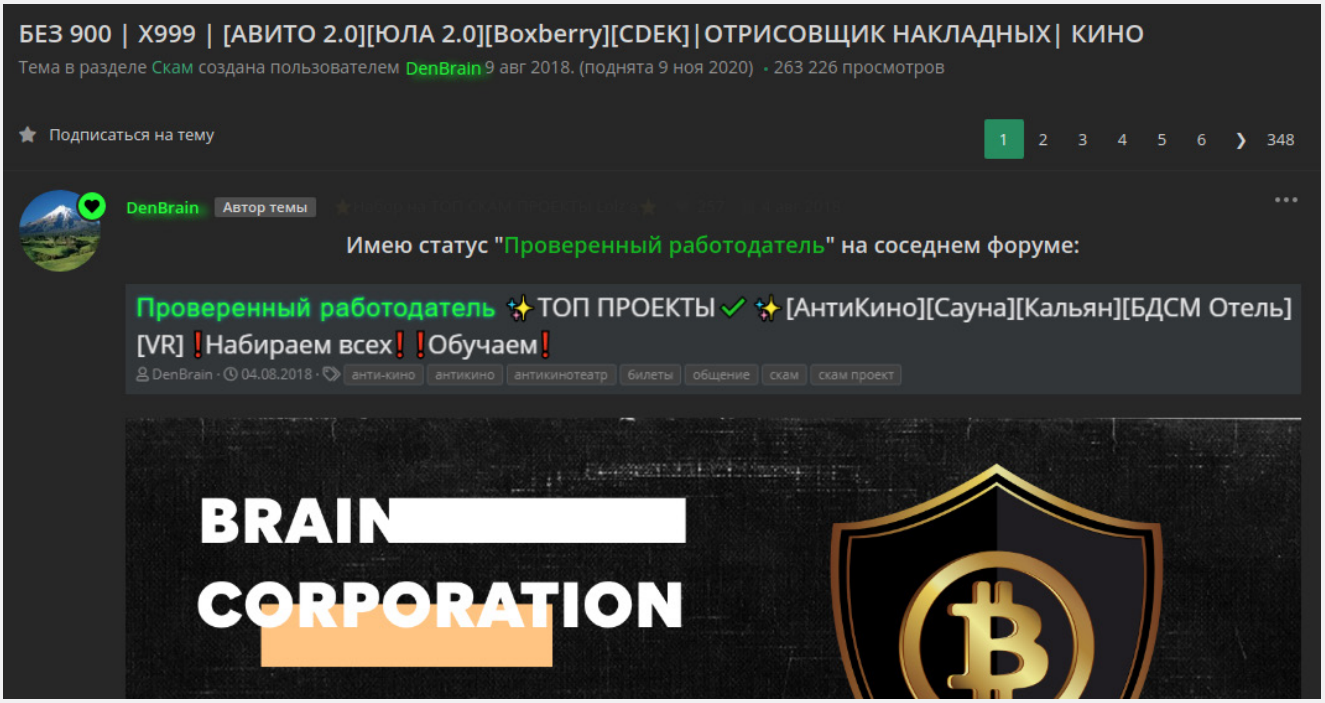
Специалисты Group-IB отмечают, что с 2017 до 2021 произошли серьезные изменения в данной схеме. В частности, злоумышленники стали активно использовать Telegram в работе. У «партнерок» появилось огромное количество ручного трафика, получаемого через целенаправленную работу с жертвой.

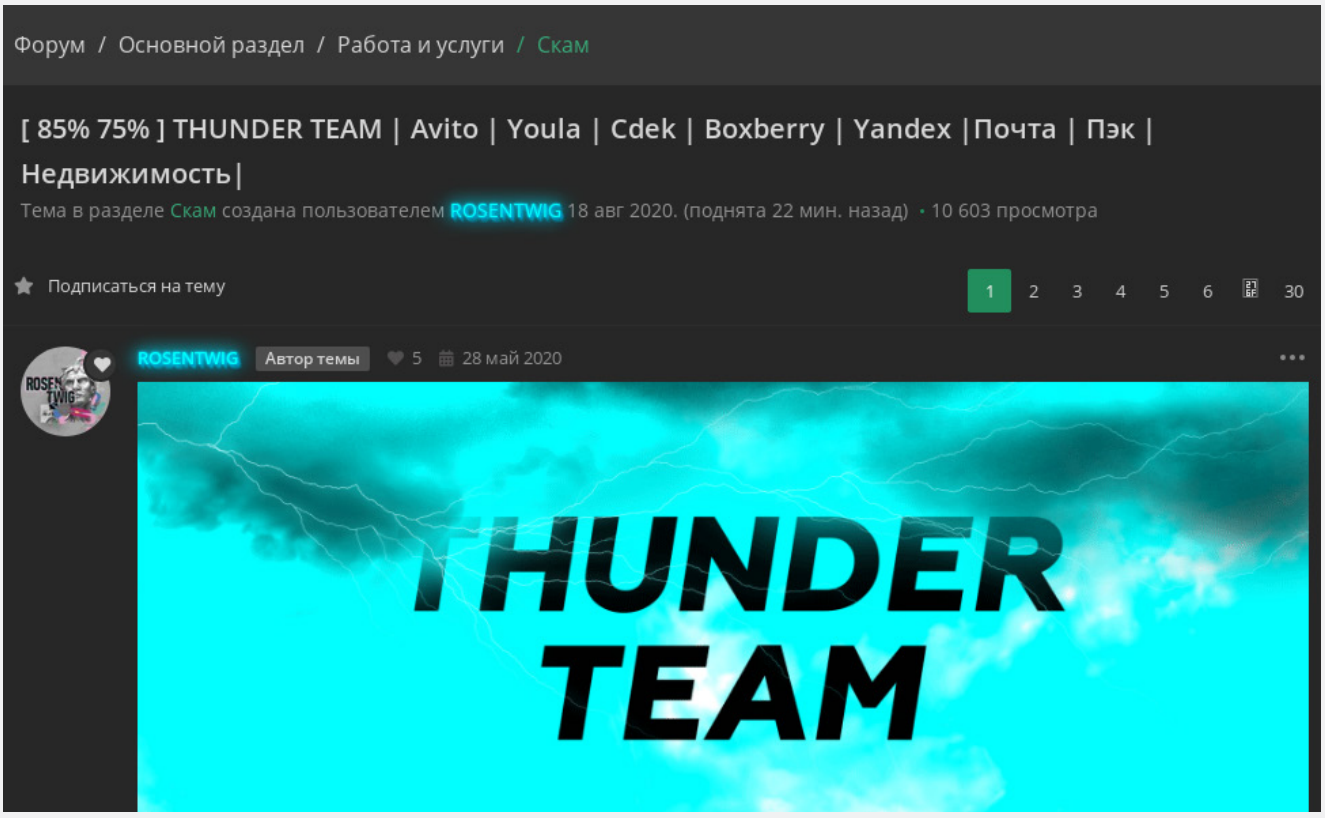
Предположительно, расширение списка атакуемых брендов и регионов стало происходить благодаря следующим факторам:

- злоумышленники боялись быть пойманными, работая над одним брендом;
- большая конкуренция на ограниченной территории;
- высокий уровень осведомленности о проблеме в странах СНГ;
- желание начать атаки в незанятой нише и получить больше прибыли.

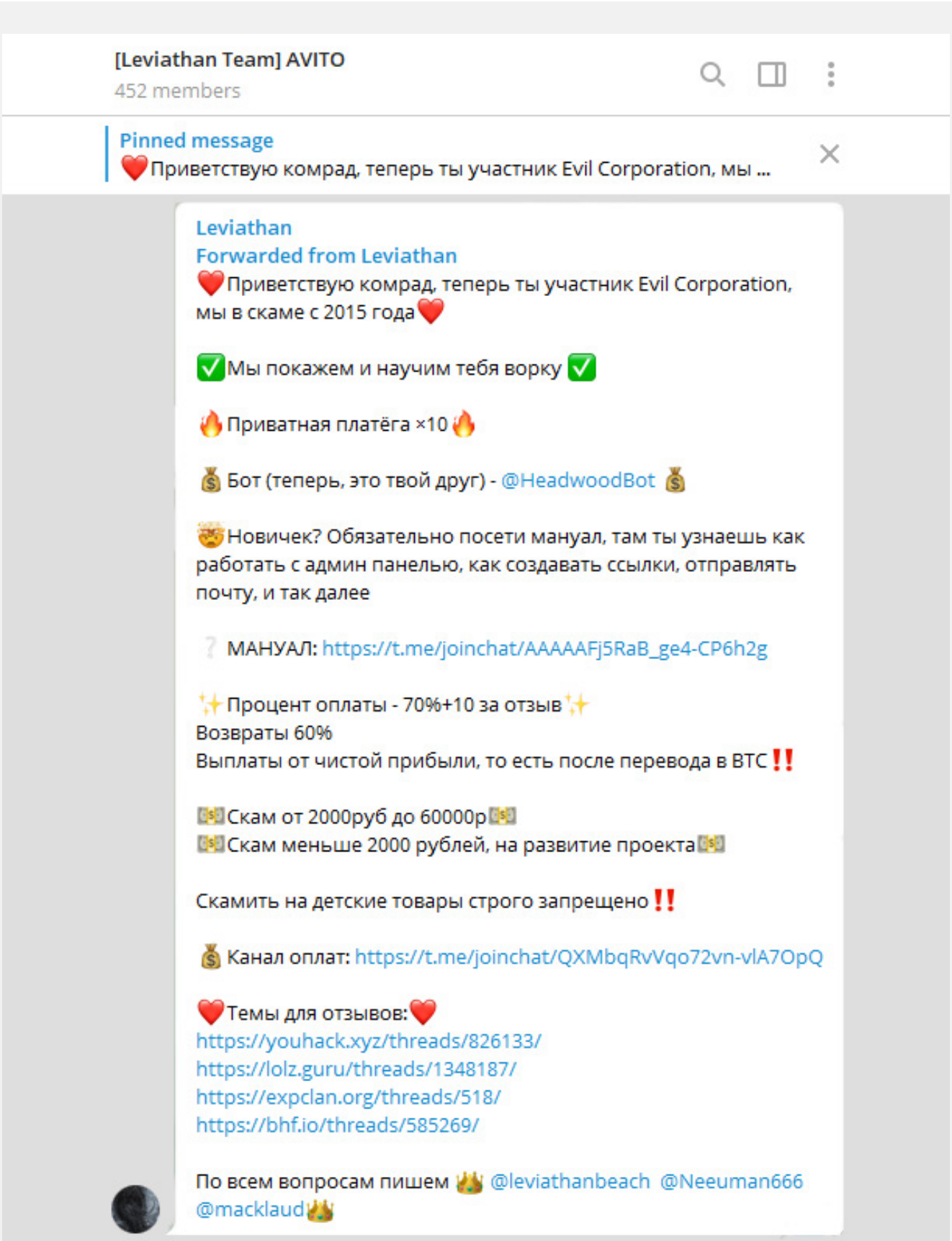
В «партнерках» задействовано большое количество людей, которых можно разделить на три группы: владельцы, технические специалисты и «воркеры».

«Воркеры» — низкоквалифицированные мошенники — занимаются поиском жертв. Новых членов партнерок ищут на андеграундных форумах или в тематических Telegram-каналах. За отчетный период эксперты Group-IB обнаружили порядка 2000 тем на 60 андеграундных форумах, связанных с поиском воркеров для фишинговых партнерок:

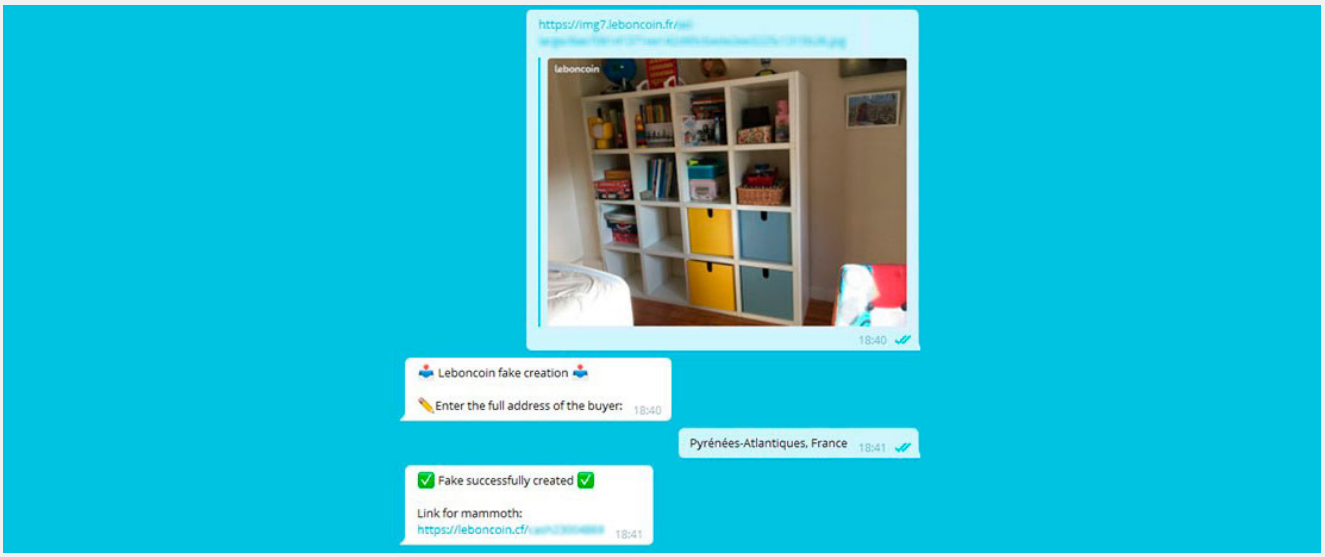




Вступая в партнерку, «воркер» получает мануал с алгоритмом и условиями работы и доступ к Telegram-боту.

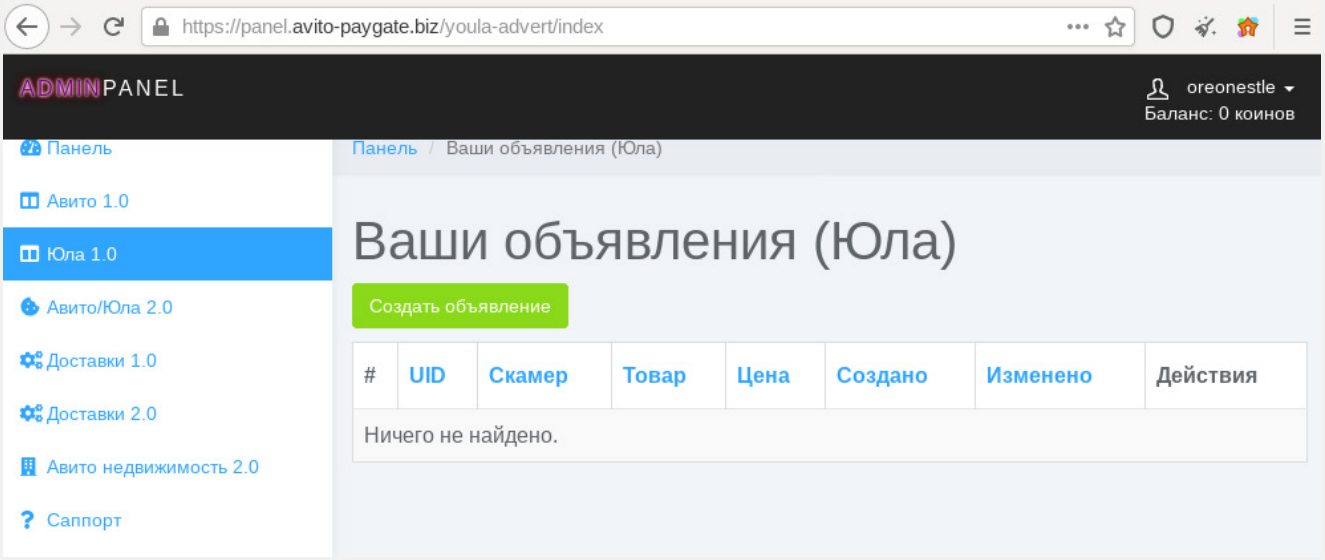


Найдя жертву и вступив с ней в диалог, например на популярном маркетплейсе, «воркер» убеждает жертву перейти на стороннюю фишинговую страницу и ввести данные своей банковской карты для оплаты товара/доставки или получения денег. Фишинговую страницу воркеры также создают и получают через Telegram-ботов. Жертву стараются вывести за пределы легитимной площадки (маркетплейса или сайта объявлений), так как внутренние антифрод-системы не пропустят фишинговую ссылку, отправленную в чат.



В результате такого мошенничества жертва теряет как деньги, так и данные банковской карты.

Взаимодействие «воркеров» с «партнеркой» может происходить как через Telegram-ботов, так и через административные панели.



После создания ссылки панель выглядит следующим образом:

Показаны записи **1-2** из **2**.

#	Оплата	Возврат	Пометка	Статус	Действия
1	https://avito-xpay.site/payment/59950cb1-3c3f-4030-a555-bd5cefac4e3c QR	https://avito-xpay.site/payment/59950cb1-3c3f-4030-a555-bd5cefac4e3c/refund QR		Активная	Сделать основной Отправить EMail Заблокировать
2	https://avito-xpay.site/payment/918edb56-de1b-41ba-8403-db0fec369c07 QR	https://avito-xpay.site/payment/918edb56-de1b-41ba-8403-db0fec369c07/refund QR	Основная ссылка	Активная	Заблокировать

В такой партнерской программе реализована отправка писем по email. При отправке на почту жертве приходит письмо. При переходе по ссылке в письме открывается уже сама фишинговая страница.

Разработкой мануалов, фишинговых китов, Telegram-ботов, и административных панелей занимаются технические специалисты.

Владельцы, как и технические специалисты, не участвуют в мошенничестве напрямую. Их задача — бесперебойная работа мошеннической партнерской программы, организация и поддержка финансовой инфраструктуры для приема платежей от жертв и вывода похищенных средств через банковские карты или электронные кошельки, оформленные на дропов.

Изначально фишинговые и мошеннические партнерские программы ориентировались на Россию и страны СНГ. Сейчас в поле зрения специалистов Group-IB все чаще попадают партнерки, нацеленные на европейские, азиатские, ближневосточные и американские компании. Известно о 71 бренде из 36 стран, под которые создают и распространяют фишинг участники партнерок.

Страна	%
Россия	38
Беларусь	6
Франция	4
Нидерланды	4
Украина	4
Польша	4
Эстония	3
Чехия	3
Испания	3
Норвегия	3
Австрия	1
Финляндия	1
Казахстан	1
Болгария	1
Другие	23

Количество контролируемых членами партнерок доменов превышает 10 000. Наиболее часто используемые домены, распределенные по странам (национальные домены):

Доменная зона	%
.ru	40,4
.online	13,3
.site	7,4
.com	6,2
.su	6,0
.info	5,8
.xyz	2,8
.net	2,7
.store	2,6
.cc	1,4
Другие	11,4

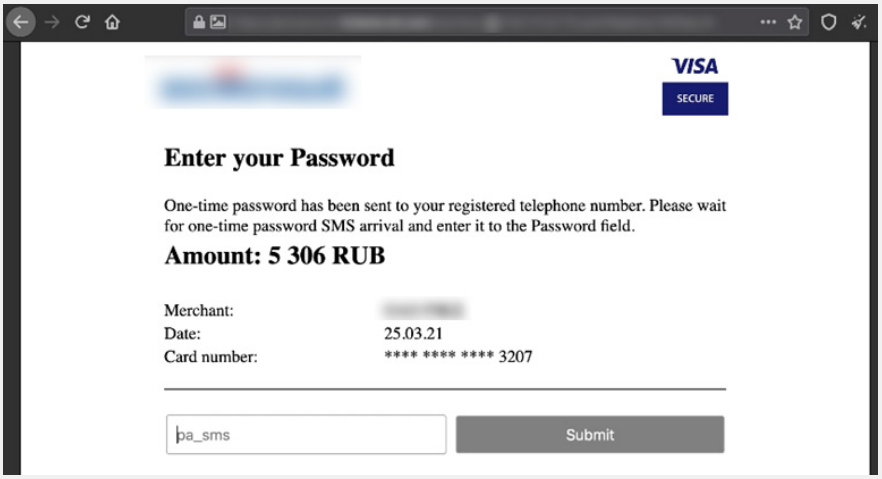
CNP-МОШЕННИЧЕСТВО[1]: ПОДЛОЖНЫЕ СТРАНИЦЫ ПРИЕМА ПЛАТЕЖЕЙ

07

Создавая фишинговые сайты под популярные сервисы и онлайн-магазины, мошенники стали применять новую схему с подложными страницами приема и подтверждения платежей, с которых деньги покупателей уходят напрямую мошенникам через легальную транзакцию в банке. Схема активно используется для проведения транзакций в фишинговых партнерских программах. Круг пострадавших в этой схеме достаточно широк — это и клиент банка, потерявший свои деньги и не получивший покупку, это банк-эмитент, одобривший транзакцию, онлайн-сервис или магазин, сайт которого подделали злоумышленники, и платежные системы, чьи бренды нелегально и без их ведома используются в мошеннической схеме. Только в России ущерб от данной схемы составляет 3,15 млрд. рублей за отчетный период, исходя из среднего размера транзакции, умноженного на количество выявленных операций на фишинговых платежных страницах. Эксперты Group-IB считают, что схема получит широкое распространение и в других регионах, нанося существенный финансовый ущерб.

Классическая схема фейковых мерчантов выглядит следующим образом. Жертва попадает на фишинговую страницу магазина (фейкового мерчанта) через подставную рекламу, спам-рассылку или фальшивое объявление о продаже/покупке товара. Далее для оплаты выбранного товара пользователю предлагается ввести реквизиты банковской карты в подложной форме приема платежа. Она может располагаться как на мошенническом сайте, так и на стороннем ресурсе. После этого данные отправляются на сервер мошенника.

[1] CNP (англ. Card not present, CNP) – операции без присутствия карты. Тип транзакций, при которых клиент банка с своей картой физически не присутствует во время и в месте проведения оплаты.



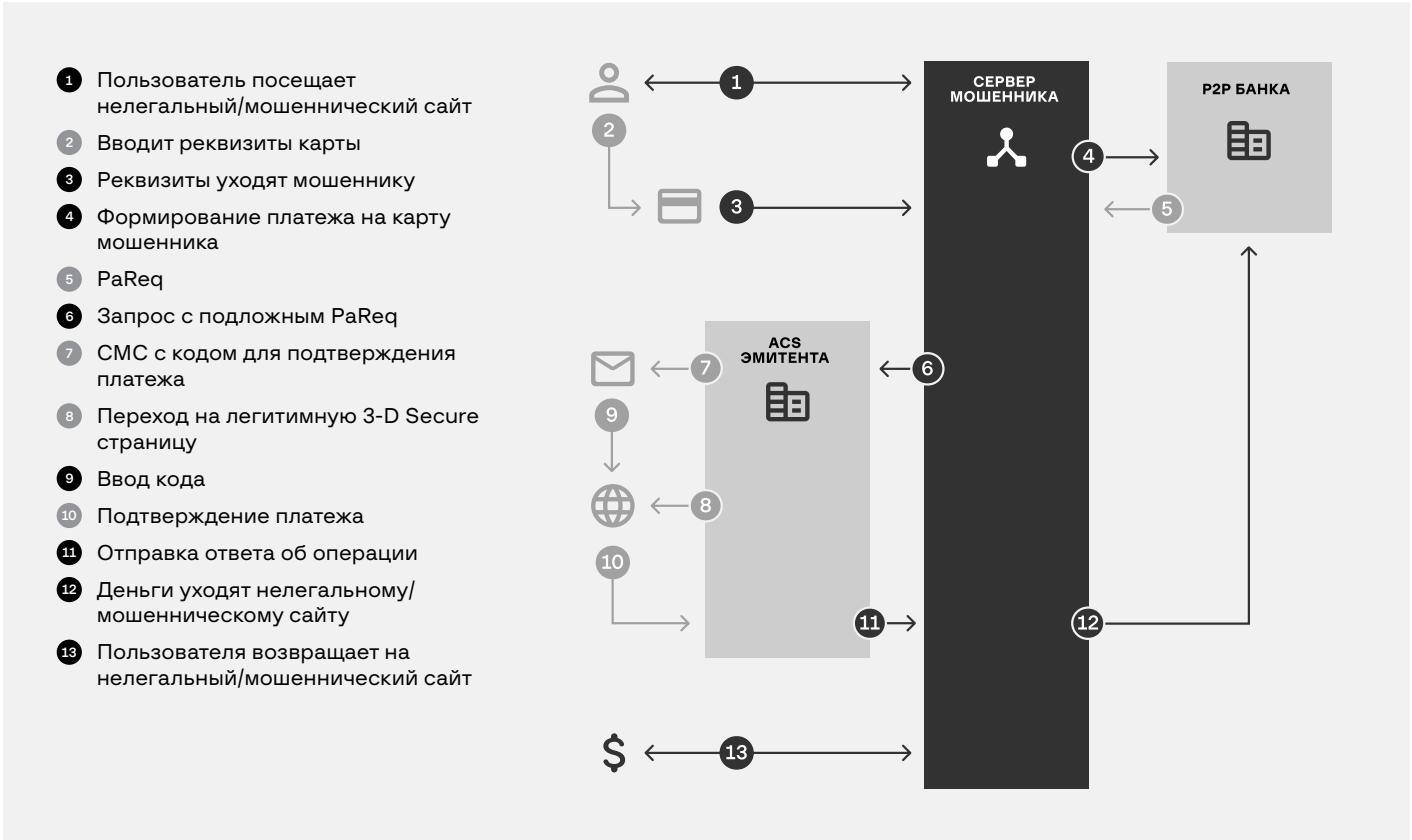
Пример подложной платежной формы

Далее для получения денег на свой счет злоумышленник формирует платеж, используя один из публичных сервисов перевода денежных средств с карты на карту (P2P), предоставляемых банками. В качестве получателя платежа мошенники указывают данные собственной карты.

Как и в случае с легитимной оплатой интернет-покупки, пользователю приходит СМС-код для подтверждения операции. Но на самом деле, вводя код на странице 3DS, пользователь подтверждает не покупку в онлайн-магазине, а отправляет перевод на счет злоумышленника. Для сокрытия следов использования сторонних P2P-сервисов от пользователя, преступники подменяют URL-адрес возврата результата авторизации и данные о мерчанте в PaReq — получателе платежа, чтобы на странице 3DS для ввода СМС-кода отображалась не вызывающая у жертвы подозрений информация.

Технология 3DS версии 1.0, которая сегодня используется повсеместно, хоть и защищает платежи от внешнего мошенника и пресекает попытки воспользоваться данными украденных карт, не предусматривает защиту от мошенничества со стороны онлайн-магазинов.

В протоколе 3-D Secure первой версии есть возможность подмены PaReq создаваемого MPI эквайера. PaReq представляет собой XML-сообщение, которое сжато и закодировано в base64. Какой-либо код контроля целостности или подпись при этом отсутствуют, что позволяет мошенникам менять содержимое произвольным образом.



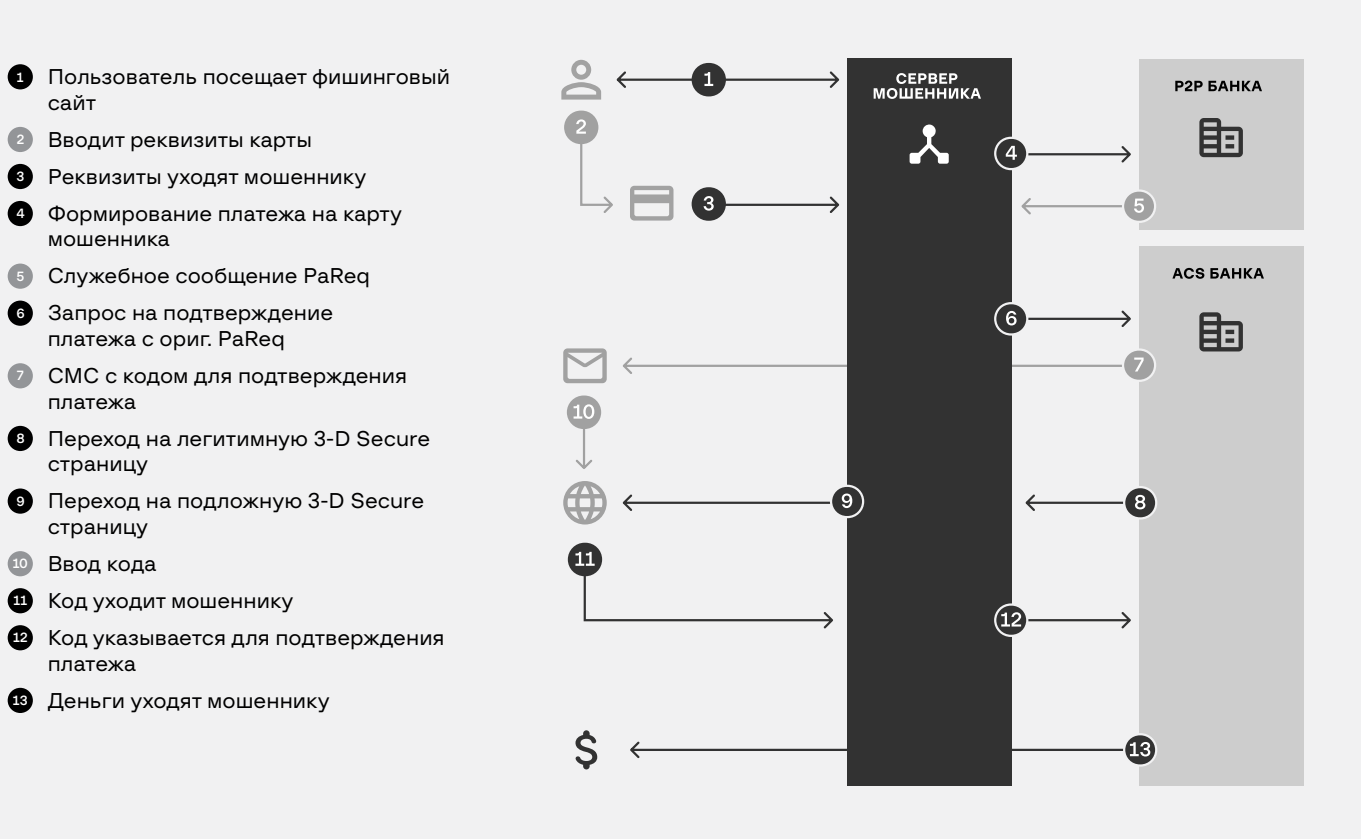
Чтобы обезопасить себя от подобного мошенничества, некоторые банки стали сами проверять соответствие указанных данных в PaReq. Однако злоумышленники модифицировали схему. Теперь в ней применяется подложная страница 3-D Secure.

Опасность новой схемы заключается в следующем:

- Процесс оплаты на мошенническом ресурсе выглядит для держателя карты аналогично оплате на легальном ресурсе.
- Для банка-эмитента процесс проведения платежа выглядит как типичный перевод с карты на карту.
- Схема применима для 3-D Secure версии 2.x.

Как и в случае с фейковым мерчантом, сначала пользователь попадает на мошенническую страницу магазина. Желая оплатить выбранный товар или услугу, он вводит на мошенническом ресурсе реквизиты своей банковской карты в форму приема платежа по аналогии с тем, как это обычно делается на привычных легитимных ресурсах. Далее его данные попадают на сервер мошенника, откуда происходит обращение к P2P-сервисам различных банков с указанием в качестве получателя одной из карт мошенника. В ответ от P2P-сервиса банка сервер мошенника получает служебное сообщение (так называемое PaReq-сообщение), в котором закодирована информация о банковской карте плательщика, сумме перевода, названии и реквизиты использованного P2P-сервиса. Чтобы скрыть от жертвы факт использования P2P-сервиса банка, на сервере мошенника в полученной от банка странице 3-D Secure производится подмена реальной информации на подложные данные об онлайн-магазине. Затем мошенники перенаправляют покупателя на эту 3-D Secure страницу банка, но уже с подмененными данными, которые он и видит на этой странице.

Как ни в чем не бывало, жертва вводит платежные данные, оплачивая выбранный товар. Для подтверждения транзакции ей на телефонный номер приходит СМС-код. Она вводит код в ту же форму на легитимной 3-D Secure странице. Злоумышленники используют полученный код, чтобы от имени жертвы ввести его на сервисе перевода денежных средств с карты на карту. Деньги жертвы переводятся на карту мошенников.



АТАКИ ФИНАНСОВО МОТИВИРОВАННЫХ ХАКЕРСКИХ ГРУППИРОВОК

08

MoneyTaker

В феврале 2021 специалисты лаборатории компьютерной криминалистики Group-IB были привлечены к реагированию на инцидент в одном из российских банков, в ходе которого атакующие смогли получить доступ к системе межбанковских переводов АРМ КБР. Изучив тактики, техники и процедуры (TTPs) киберпреступников, эксперты Group-IB предположили, что за атакой может стоять группа **MoneyTaker**.

В 2016-2019 гг. эта группа совершала атаки АРМ КБР и системы карточного процессинга в Великобритании, Гонконге, США, Украине и России. После более чем годового затишья MoneyTaker вновь начали атаковать финансовые организации.

В ходе реагирования на инцидент было установлено, что атака началась в июне 2020 через компрометацию аффилированной с банком компании. Предположительно, они начали с физического устройства, установленного в аффилированной сети. В процессе реагирования не удалось найти компьютер, с которого началась атака. Однако были обнаружены признаки эксплуатации старой уязвимости Fortigate OS fortiOS 5.6.4 (CVE-2018-13379).

В течение месяца атакующие получили доступ к сети банка. В последующие шесть месяцев они исследовали сеть.

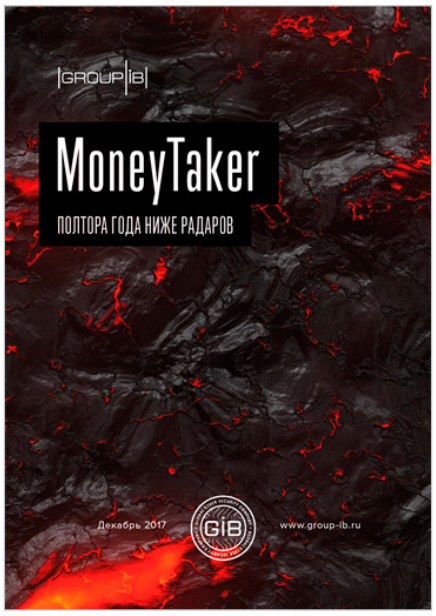
В ходе атаки злоумышленники использовали ПО Mimikatz, встроенные утилиты в ОС Windows – WinRM и WMI, ПО RStudio, ПО для удаленного доступа DameWare, фреймворк Metasploit для удаленного исполнения команд, утилиты nbtstat, netstat, tasklist, PsExec и другие.

В январе 2021 атакующие приступили к финальной фазе атаки. Они зарегистрировали доменные имена, схожие с названием банка: оригинальный домен был <BANK>.ru, поддельные <BANK>.org и <BANK>.com.

В феврале 2021 атакующие похитили цифровые ключи и позже использовали их для подписания платежей, проходящих через транспортный шлюз Банка России. После этого они вручную скопировали поддельные подписанные платежи в специальную папку в системе АРМ КБР.

В конце атакующие применили MBR killer на атакованной машине. Большинство логов было стерто. После завершения операции злоумышленники удалили конфигурацию межсетевого экрана Fortigate, отвечающего за изоляцию сегмента АРМ КБР.

MoneyTaker отчет



OPERA1ER

В отчетном периоде специалисты Group-IB фиксировали атаки на банки и финансовые организации Африки, Азии и Латинской Америки. В ходе исследования инцидентов команда Group-IB Threat Intelligence установила, что за атаками стоит финансово мотивированная франкоговорящая хакерская группировка под названием OPERA1ER (aka DESKTOP-GROUP, Common Raven). Экспертам Group-IB известно о десятках успешных атак OPERA1ER на банки, финансовые организации и телекоммуникационные компании Африки, Азии и Латинской Америки. Некоторые жертвы были атакованы дважды.

В качестве первичного вектора атаки OPERA1ER используют фишинговые письма с документами-приманками на финансовые темы. Фишинговые письма создаются отдельно под каждую атакуемую компанию. OPERA1ER выкачивают внутреннюю документацию для последующего использования в фишинговых атаках, тщательно изучают инфраструктуру жертвы. Особенностью группы является отсутствие самописного ВПО в арсенале — OPERA1ER полагаются только на уже известные инструменты. Из интересных тактик можно отметить, что злоумышленники разворачивали Metasploit прямо в сети атакованных банков, а точнее на их серверах.

Главной целью OPERA1ER является платформа электронных платежей, которую использовали атакованные компании.

РЫНОК КАРДИНГА 09

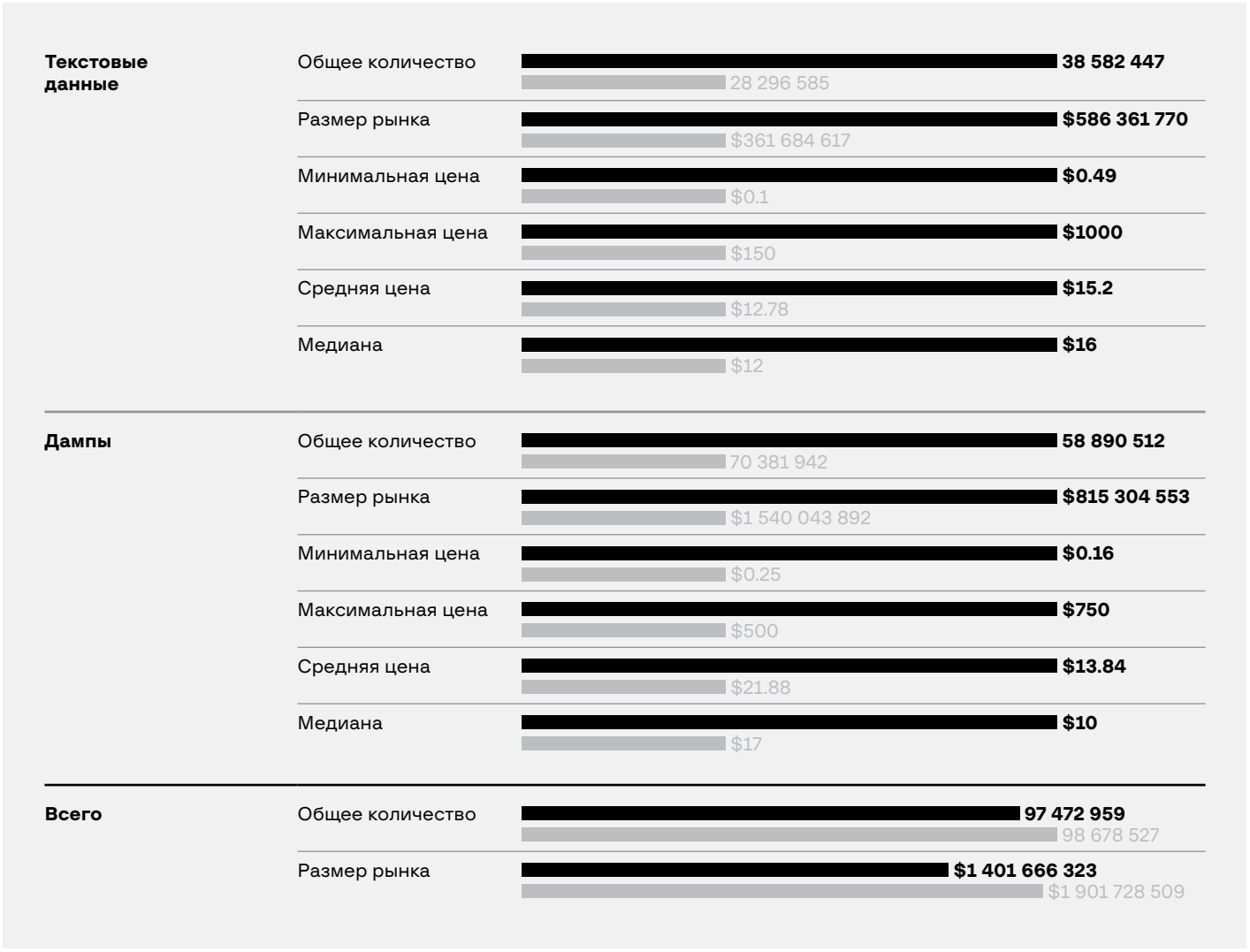
Текстовые данные собираются с помощью фишинговых сайтов, банковских троянов для ПК, Android и банкоматов, а также в результате взломов сайтов электронной коммерции и использования JS-снифферов.

Дампы получают через скимминговые устройства, а также с использованием троянов для компьютеров с подключенными POS-терминалами.

За отчетный период общий рынок кардинга уменьшился с $1,9 млрд до $1,4 млрд по сравнению с прошлым годом. Падение объясняется уменьшением количества дампов в продаже (58 млн. против 70 млн.) из-за закрытия крупнейшего кардшопа – Joker's Stash.

А вот количество текстовых данных в продаже, напротив, увеличилось с 28 млн. до 38 млн., что объясняется в том числе и ростом фишинговых ресурсов в период пандемии.

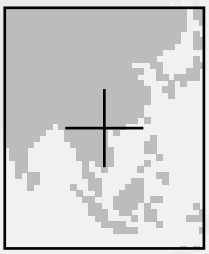
Рынок кардеров можно поделить на два основных сегмента: продажа текстовых данных о картах (номер, срок действия, имя держателя, адрес, CVV) и дампов (информация с магнитной полосы карты).



Азиатско-Тихоокеанский регион

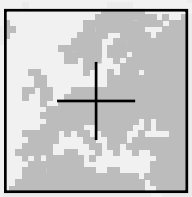
■ H2 2020 — H1 2021
■ H2 2019 — H1 2020

		H2 2020 — H1 2021	H2 2019 — H1 2020
Текстовые данные	Общее количество	**9 767 812**	3 886 750
	Размер рынка	**$197 935 368**	$55 302 460
	Минимальная цена	**$0.49**	$0.3
	Максимальная цена	**$150.18**	$149.99
	Средняя цена	**$20.26**	$14.23
	Медиана	**$22**	$16
Дампы	Общее количество	**2 364 263**	3 637 124
	Размер рынка	**$93 548 248**	$273 393 726
	Минимальная цена	**$0.16**	$0.25
	Максимальная цена	**$750**	$500
	Средняя цена	**$39.57**	$75.17
	Медиана	**$15**	$100
Всего	Общее количество	**12 132 075**	7 523 874
	Размер рынка	**$291 483 615**	$328 696 186



Европа

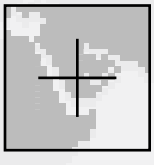
		H2 2020 — H1 2021	H2 2019 — H1 2020
Текстовые данные	Общее количество	**5 108 335**	5 934 323
	Размер рынка	**$96 733 537**	$89 974 285
	Минимальная цена	**$0.9**	$0.3
	Максимальная цена	**$1000**	$500
	Средняя цена	**$18.94**	$15.16
	Медиана	**$19**	$16
Дампы	Общее количество	**803 586**	1 670 699
	Размер рынка	**$21 870 228**	$129 134 358
	Минимальная цена	**$0.16**	$0.5
	Максимальная цена	**$250**	$500
	Средняя цена	**$27.22**	$77.29
	Медиана	**$15**	$35
Всего	Общее количество	**5 911 921**	7 605 022
	Размер рынка	**$118 603 765**	$219 108 642



Ближний Восток

■ H2 2020 — H1 2021
■ H2 2019 — H1 2020

Текстовые данные	Общее количество	**1 254 343**	1 917 521
	Размер рынка	**$17 669 265**	$17 168 560
	Минимальная цена	**$0.75**	$0.3
	Максимальная цена	**$150.18**	$149.99
	Средняя цена	**$14.09**	$8.95
	Медиана	**$12**	$6
Дампы	Общее количество	**292 499**	436 333
	Размер рынка	**$6 701 097**	$30 466 396
	Минимальная цена	**$0.25**	$1
	Максимальная цена	**$234**	$500
	Средняя цена	**$22.91**	$69.82
	Медиана	**$15**	$16
Всего	Общее количество	**1 546 842**	2 353 854
	Размер рынка	**$24 370 362**	$47 634 955



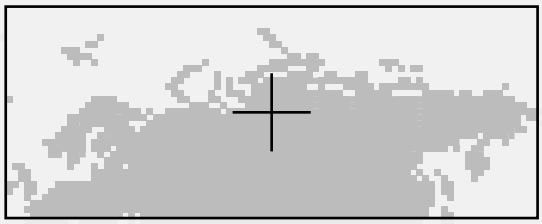
Северная Америка

■ H2 2020 — H1 2021
■ H2 2019 — H1 2020

Текстовые данные	Общее количество	**14 935 741**	12 310 510
	Размер рынка	**$181 056 119**	$141 857 392
	Минимальная цена	**$0.49**	$0.5
	Максимальная цена	**$1000**	$149.99
	Средняя цена	**$12.01**	$15.61
	Медиана	**$12.0**	$9.0
Дампы	Общее количество	**40 408 251**	46 770 337
	Размер рынка	**$485 407 685**	$730 024 615
	Минимальная цена	**$0.16**	$0.25
	Максимальная цена	**$750**	$500
	Средняя цена	**$12.2**	$11.52
	Медиана	**$10.0**	$16.94
Всего	Общее количество	**55 343 992**	59 080 847
	Размер рынка	**$666 463 805**	$871 882 007

Россия и СНГ

		H2 2020 — H1 2021	H2 2019 — H1 2020
Текстовые данные	Общее количество	**10 100**	19 779
	Размер рынка	**$155 838**	$278 513
	Минимальная цена	**$1.2**	$0.3
	Максимальная цена	**$150.18**	$149.99
	Средняя цена	**$15.43**	$14.08
	Медиана	**$16**	$14
Дампы	Общее количество	**3 699**	15 037
	Размер рынка	**$115 098**	$931 978
	Минимальная цена	**$0.5**	$1
	Максимальная цена	**$284**	$284
	Средняя цена	**$31.12**	$61.98
	Медиана	**$15**	$30
Всего	Общее количество	**13 799**	34 816
	Размер рынка	**$270 935**	$1 210 490



БАНКОВСКИЕ ТРОЯНЫ ДЛЯ ПК

10

Всего в исследуемом периоде активность проявляли 18 банковских троянов. Из них 8 разработаны авторами из Латинской Америки, 9 – русскоязычными злоумышленниками.

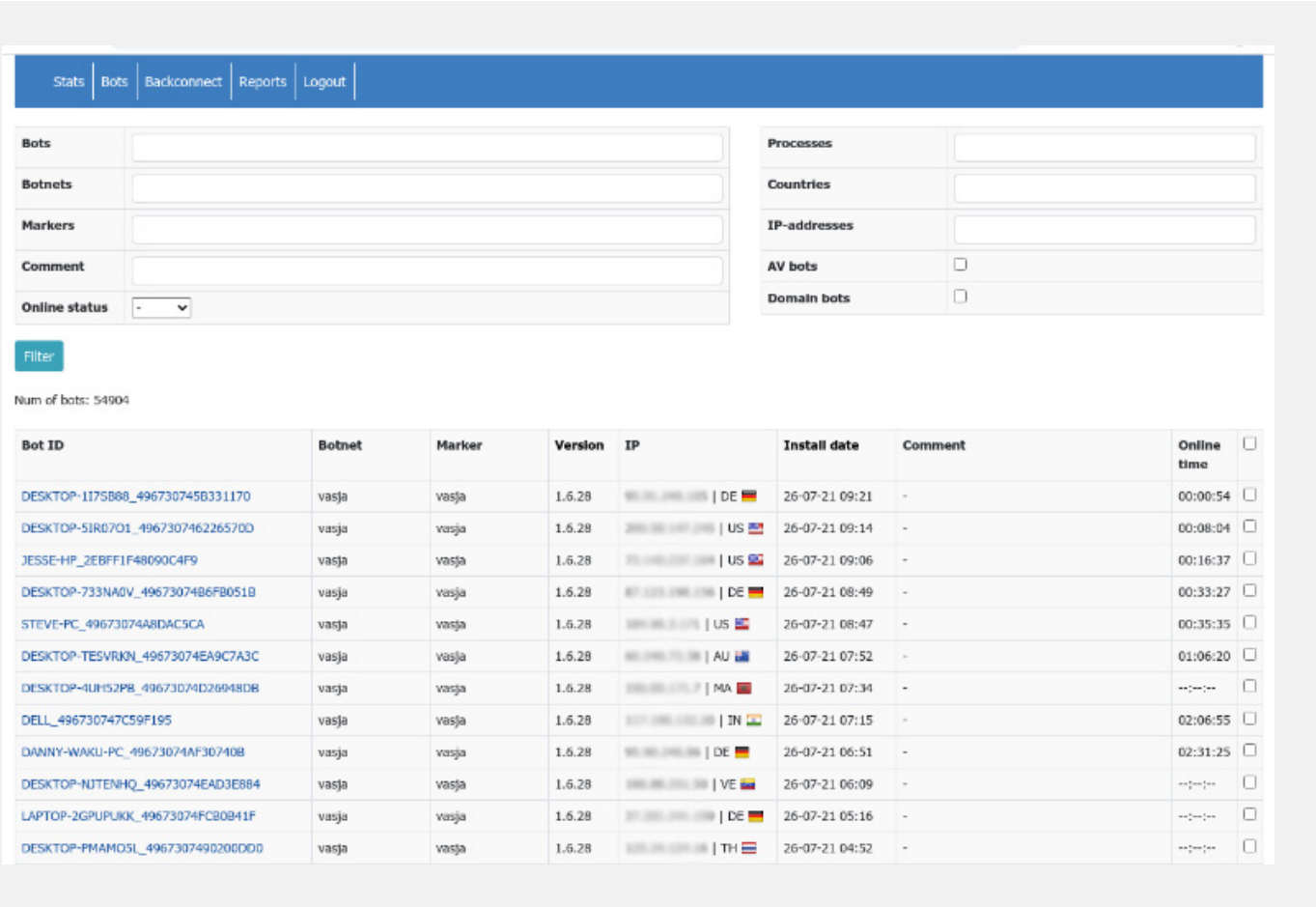
Активные банкеры в регионах

Статус	Троян	Дата появления	Регион разработчика	Регион атаки
НОВЫЙ	BBtok	Q4 2020	Латинская Америка	Латинская Америка
НОВЫЙ	Bizarro	Q1 2021	Латинская Америка	Латинская Америка
АКТИВНЫЙ	Grandoreiro	2017	Латинская Америка	США и Канада, Латинская Америка, Европа
АКТИВНЫЙ	Javali	2017	Латинская Америка	Латинская Америка
АКТИВНЫЙ	Guildma	2017	Латинская Америка	Латинская Америка
АКТИВНЫЙ	Pazera	2015	Латинская Америка	Латинская Америка
АКТИВНЫЙ	Metamorfo (Casbaneiro)	2018	Латинская Америка	Латинская Америка
АКТИВНЫЙ	Janeleiro	2019	Латинская Америка	Латинская Америка
АКТИВНЫЙ	RTM	2015	Россия	Россия
АКТИВНЫЙ	zLoader	2019	Россия	США и Канада, Европа, Азиатско-Тихоокеанский регион
АКТИВНЫЙ	Qbot	2009	Россия	США и Канада
АКТИВНЫЙ	Trickbot	2016	Россия	США и Канада, Азиатско-Тихоокеанский регион
АКТИВНЫЙ	IcedID	2017	Россия	США и Канада, Европа, Азиатско-Тихоокеанский регион

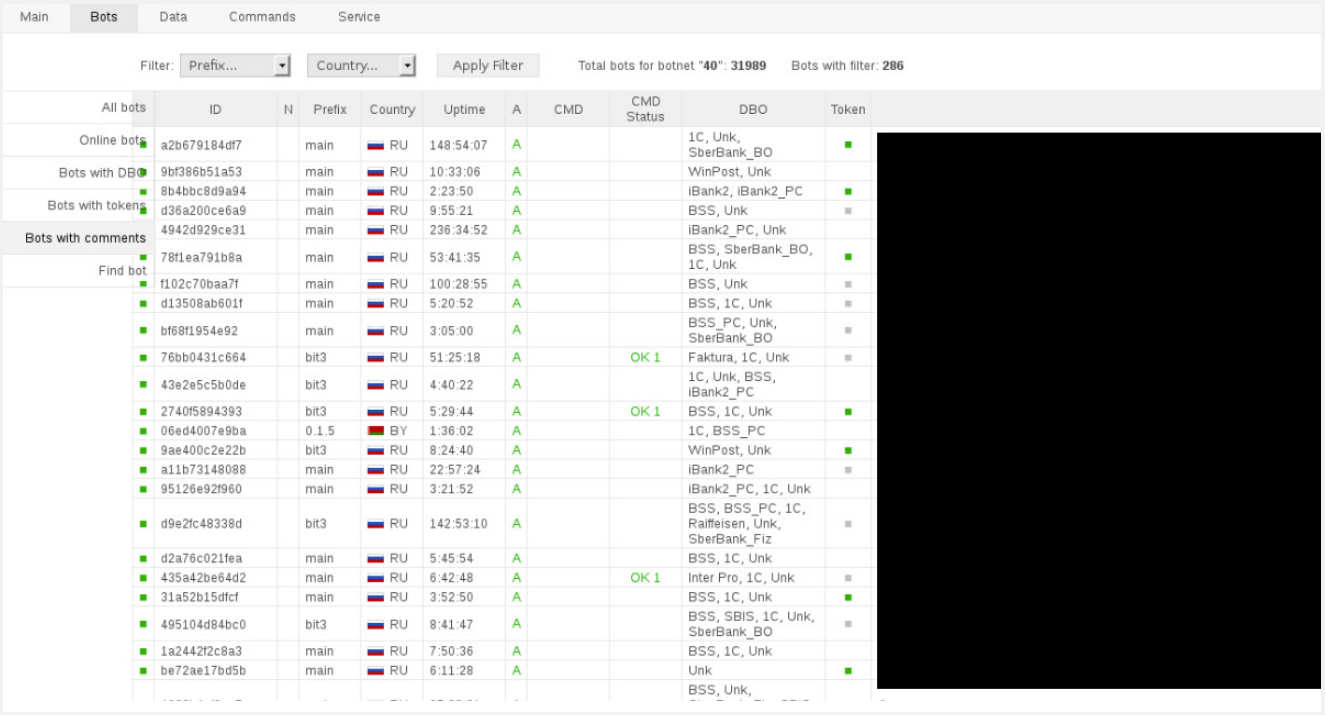
Статус	Троян	Дата появления	Регион разработчика	Регион атаки
АКТИВНЫЙ	Ramnit	2010	Россия	США и Канада, Европа, Азиатско-Тихоокеанский регион
АКТИВНЫЙ	LokiPWS	2015	Россия	США и Канада, Европа
АКТИВНЫЙ	Gozi	2007	Россия	Азиатско-Тихоокеанский регион
АКТИВНЫЙ	Danabot	2018	Россия	Европа, Азиатско-Тихоокеанский регион
АКТИВНЫЙ	Backswap	2018	Неизвестно	Европа
МАЛОАКТИВНЫЙ	Retefe	2014	Россия	Европа
МАЛОАКТИВНЫЙ	MnuBot	2018	Латинская Америка	Латинская Америка
МАЛОАКТИВНЫЙ	CamuBot	2018	Латинская Америка	Латинская Америка
МАЛОАКТИВНЫЙ	Melcoz	2018	Латинская Америка	Латинская Америка

Снимки экрана некоторых панелей вредоносных программ:

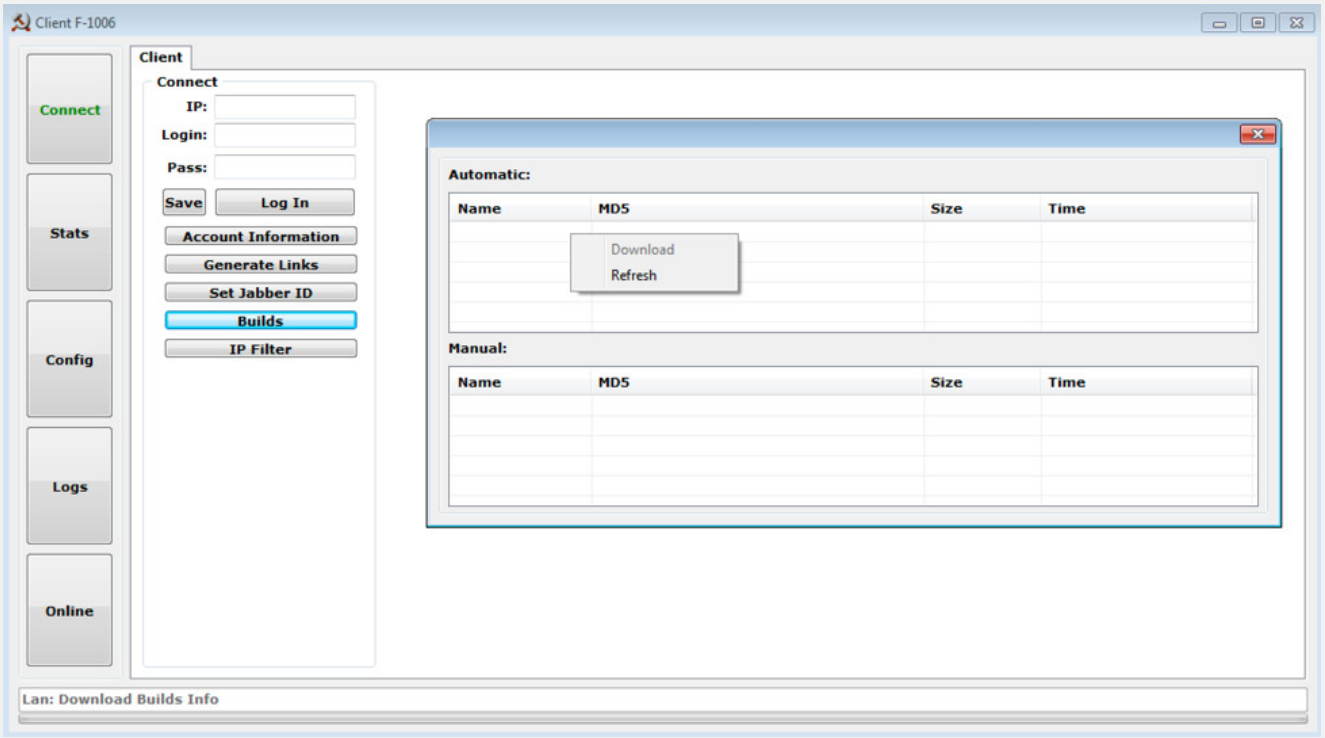
zLoader



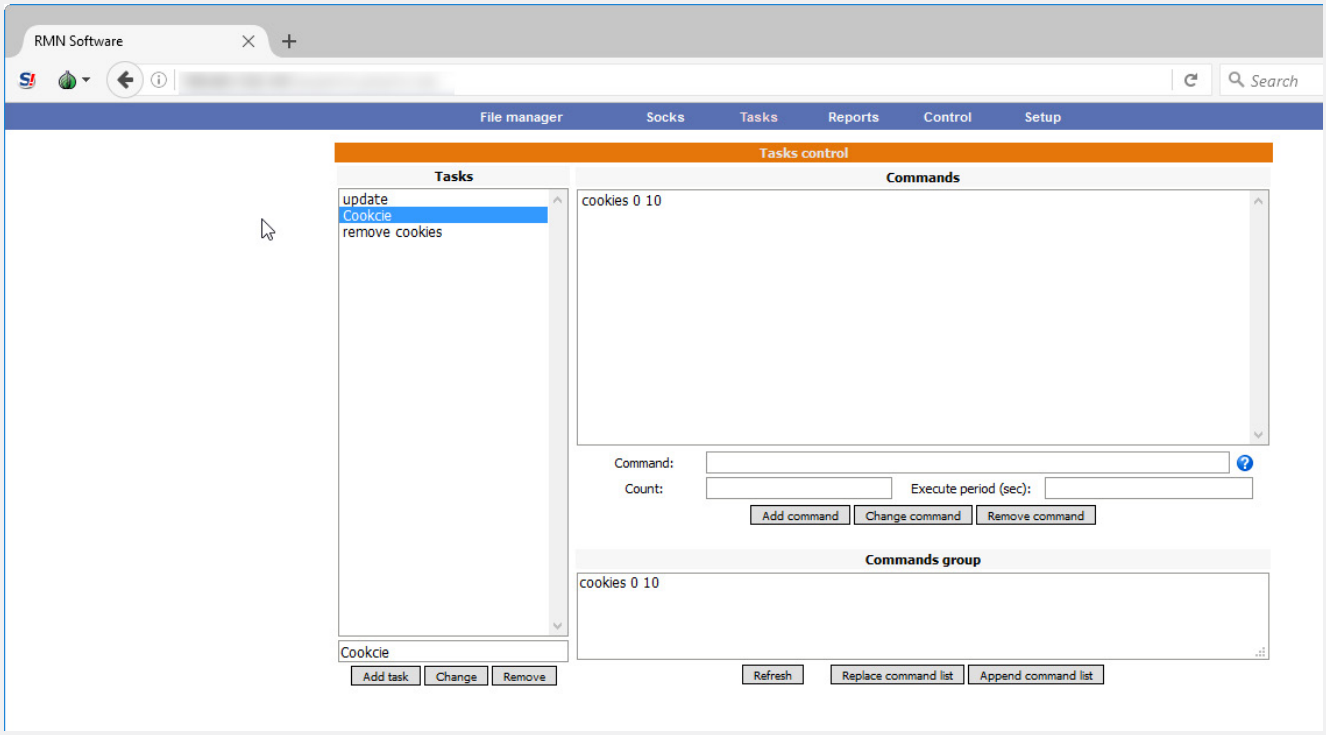
RTM


Main
Bots
Data
Commands
Service
Filter: Prefix... Country... Apply Filter
Total bots for botnet "40": 31989
Bots with filter: 286
All bots
Online bots
Bots with DBO
Bots with tokens
Bots with comments
Find bot
ID N Prefix Country Uptime A CMD CMD Status DBO Token
a2b679184df7 main RU 148:54:07 A 1C, Unk, SberBank_BO
9bf386b51a53 main RU 10:33:06 A WinPost, Unk
8b4bbc8d9a94 main RU 2:23:50 A iBank2, iBank2_PC
d36a200ce6a9 main RU 9:55:21 A BSS, Unk
4942d929ce31 main RU 236:34:52 A iBank2_PC, Unk
78f1ea791b8a main RU 53:41:35 A BSS, SberBank_BO, 1C, Unk
f102c70baa7f main RU 100:28:55 A BSS, Unk
d13508ab601f main RU 5:20:52 A BSS, 1C, Unk
bf68f1954e92 main RU 3:05:00 A BSS_PC, Unk, SberBank_BO
76bb0431c664 bit3 RU 51:25:18 A OK 1 Faktura, 1C, Unk
43e2e5c5b0de bit3 RU 4:40:22 A 1C, Unk, BSS, iBank2_PC
2740f5894393 bit3 RU 5:29:44 A OK 1 BSS, 1C, Unk
06ed4007e9ba 0.1.5 BY 1:36:02 A 1C, BSS_PC
9ae400c2e22b bit3 RU 8:24:40 A WinPost, Unk
a11b73148088 main RU 22:57:24 A iBank2_PC
95126e92f960 main RU 3:21:52 A iBank2_PC, 1C, Unk
d9e2fc48338d bit3 RU 142:53:10 A BSS, BSS_PC, 1C, Raiffeisen, Unk, SberBank_Fiz
d2a76c021fea main RU 5:45:54 A BSS, 1C, Unk
435a42be64d2 main RU 6:42:48 A OK 1 Inter Pro, 1C, Unk
31a52b15dfcf main RU 3:52:50 A BSS, 1C, Unk
495104d84bc0 bit3 RU 8:41:47 A BSS, SBIS, 1C, Unk, SberBank_BO
1a2442f2c8a3 main RU 7:50:36 A BSS, 1C, Unk
be72ae17bd5b main RU 6:11:28 A Unk
BSS, Unk,

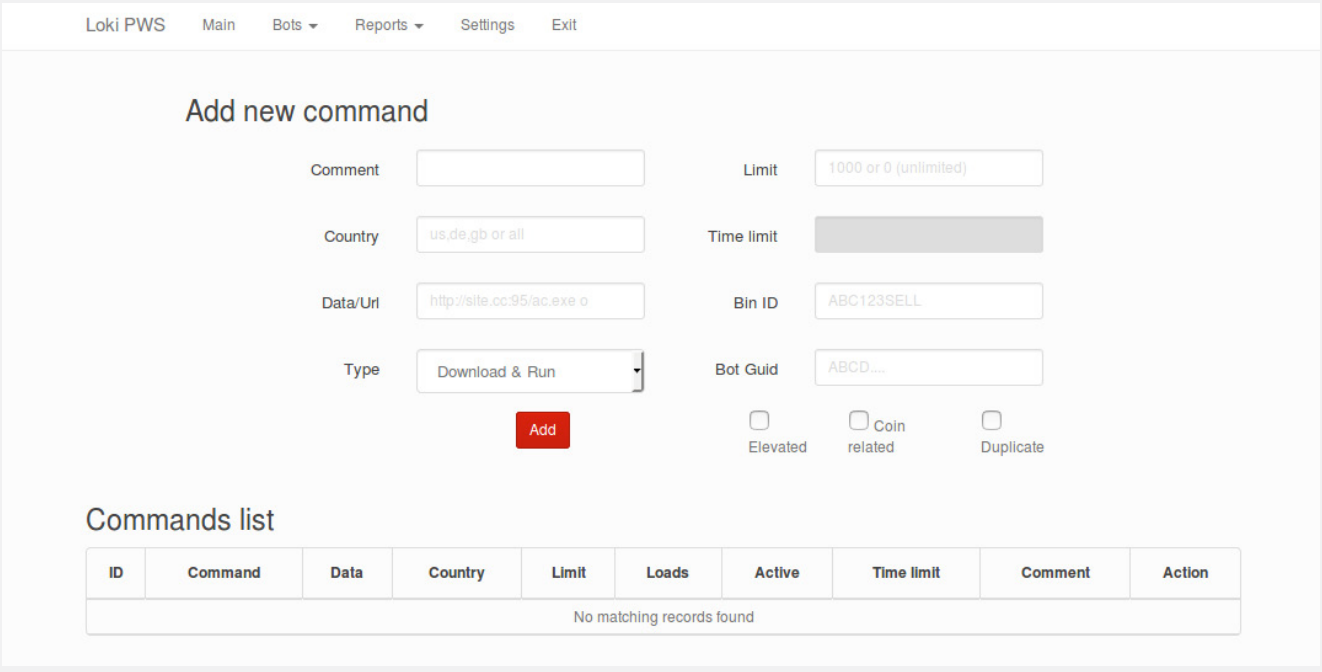
Danabot


Client F-1006
Connect
Stats
Config
Logs
Online
Client
Connect
IP:
Login:
Pass:
Save
Log In
Account Information
Generate Links
Set Jabber ID
Builds
IP Filter
Automatic:
Name MD5 Size Time
Download
Refresh
Manual:
Name MD5 Size Time
Lan: Download Builds Info

Ramnit



LokiPWS



Продолжается тенденция прошлого года, описанная в отчете Group-IB «**Программы-вымогатели 2020-2021**», согласно которой распространители ВПО помогают операторами программ-вымогателей получить первоначальный доступ в сеть:

- Qbot → ProLock, DoppelPaymer, Egregor
- Gozi → Egregor, Revil
- zLoader → Ryuk, Egregor, DarkSide
- Trickbot → Cl0p, Conti, Ryuk, RansomEXX
- IcedID → Maze, Egregor, RansomEXX, Revil, Conti
- Dridex* → DoppelPaymer, Grief

Из-за того, что в последнее время большинство кибератак связаны с программами-вымогателями, банковские трояны практически не развиваются. Единственным регионом, в котором заметны изменения, является Латинская Америка.

В начале июня 2021 Минюст США предъявил **обвинение** задержанной в Майами 55-летней гражданке Латвии, которую правоохранительные органы называют одним из разработчиков трояна Trickbot. В сентябре в Южной Корее задержали еще одного разработчика. Однако вредоносная программа все еще активна.

Разработчики трояна Qbot продолжают активно развивать свой продукт. Был усовершенствован сетевой протокол и защитные механизмы (проверки безопасности на стороне сервера). Была внедрена проверка безопасности, согласно которой данные отправлялись только через час после того, как бот был зарегистрирован в ботнете.

Что касается zLoader, специалисты Group-IB обнаружили и проанализировали два ботнета, содержащих более 350 тысяч ботов. Большинство зараженных устройств относятся к Германии, Канаде, США, Японии.

Отдельно стоит сказать о трояне Ramnit. С одной стороны, за отчетный период не было выявлено характерных для него атак на финансовые организации, как это происходило ранее, а целями стали компании из сфер образования, страхования, госсектора. В первом квартале 2021 были отмечены заражения этим трояном в Великобритании, Индии, России, Турции, США.

Программы-вымогатели 2020/2021

* В отчетном периоде Dridex не выявлялся как самостоятельный банковский троян, а только в связке с распространением шифровальщиков.

БАНКОВСКИЕ ТРОЯНЫ ДЛЯ ANDROID

11

Как и в случае с троянами для ПК, рынок троянов для Android изменился несущественно. За отчетный период предложений о продаже/аренде новых вредоносных программ на андеграундных форумах замечено не было.

Однако за это время появились три новых трояна: Ghimob, активный в Латинской Америке, FluBot — в Европе, TeaBot (Anatsa, Toddler), который атакует своих жертв в Европе и России.

Считается, что Ghimob — это разработка той же латиноамериканской группы злоумышленников, которая создала троян Guildma (Astaroth). А вот где и кем именно были созданы FluBot и TeaBot, на данный момент неизвестно.

Бразильские банкеры OperadorMIB и BasBanke (Coybot) перестали быть активными, как и Alien Bot. Напомним, что OperadorMIB был разработан злоумышленником из Бразилии, и пик его активности пришелся на первую половину 2020.

Отметим, что исчез и троян Gustuff, который в прошлом был очень активен.

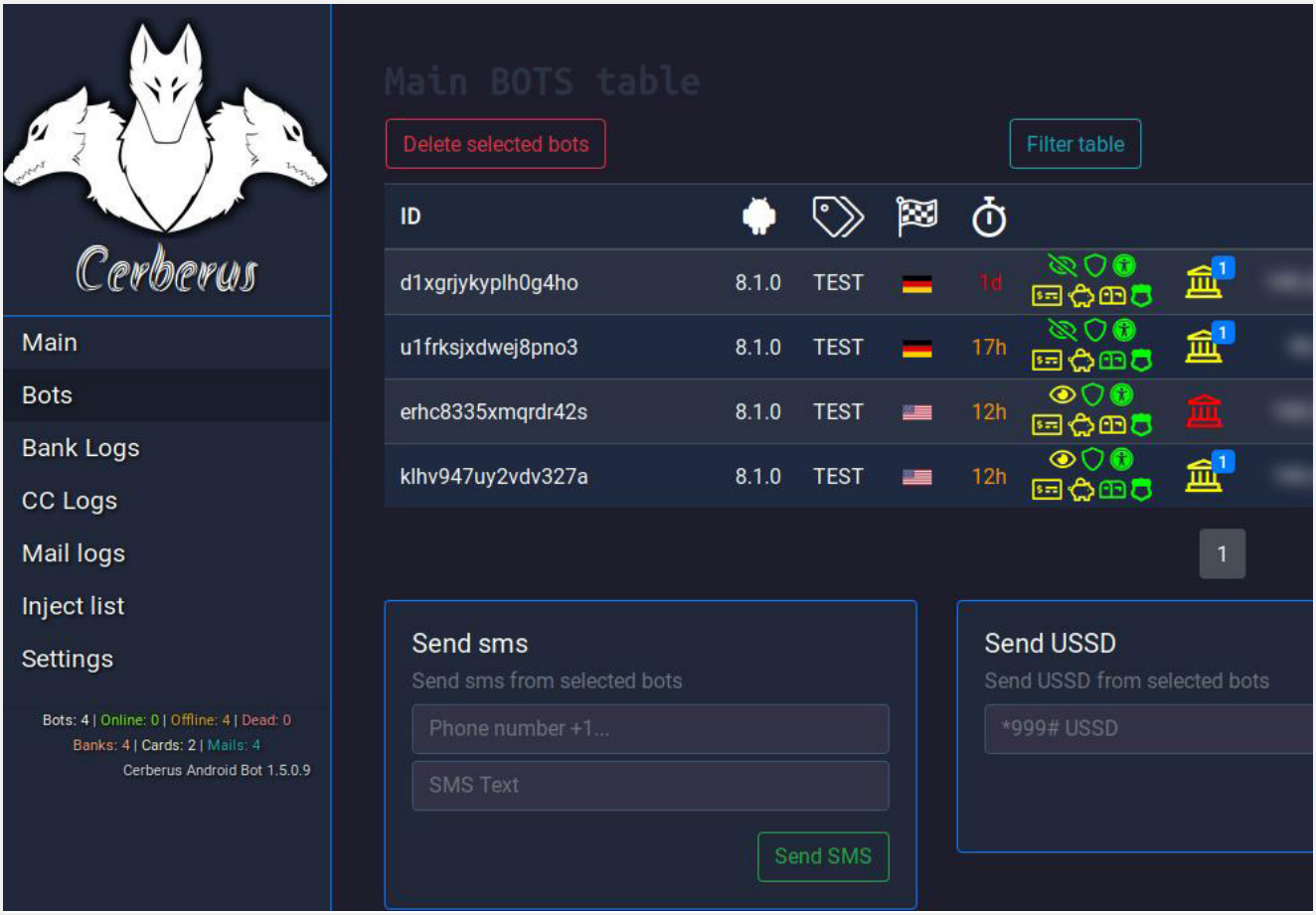
Активные Android-банкеры в регионах

Статус	Троян	Дата появления	Регион разработчика	Регион атаки
НОВЫЙ	Ghimob	Q4 2020	Латинская Америка	Латинская Америка
НОВЫЙ	TeaBot (Anatsa)	Q1 2021	Неизвестно	Россия, Европа
АКТИВНЫЙ	EventBot	Q1 2020	Неизвестно	Европа
АКТИВНЫЙ	Cerberus v2	Q2 2020	Россия	США и Канада, Азиатско-Тихоокеанский регион, Европа
АКТИВНЫЙ	Anubis	Q4 2019	Россия	США и Канада, Азиатско-Тихоокеанский регион, Европа
АКТИВНЫЙ	Ginp	Q3 2019	Неизвестно	Европа

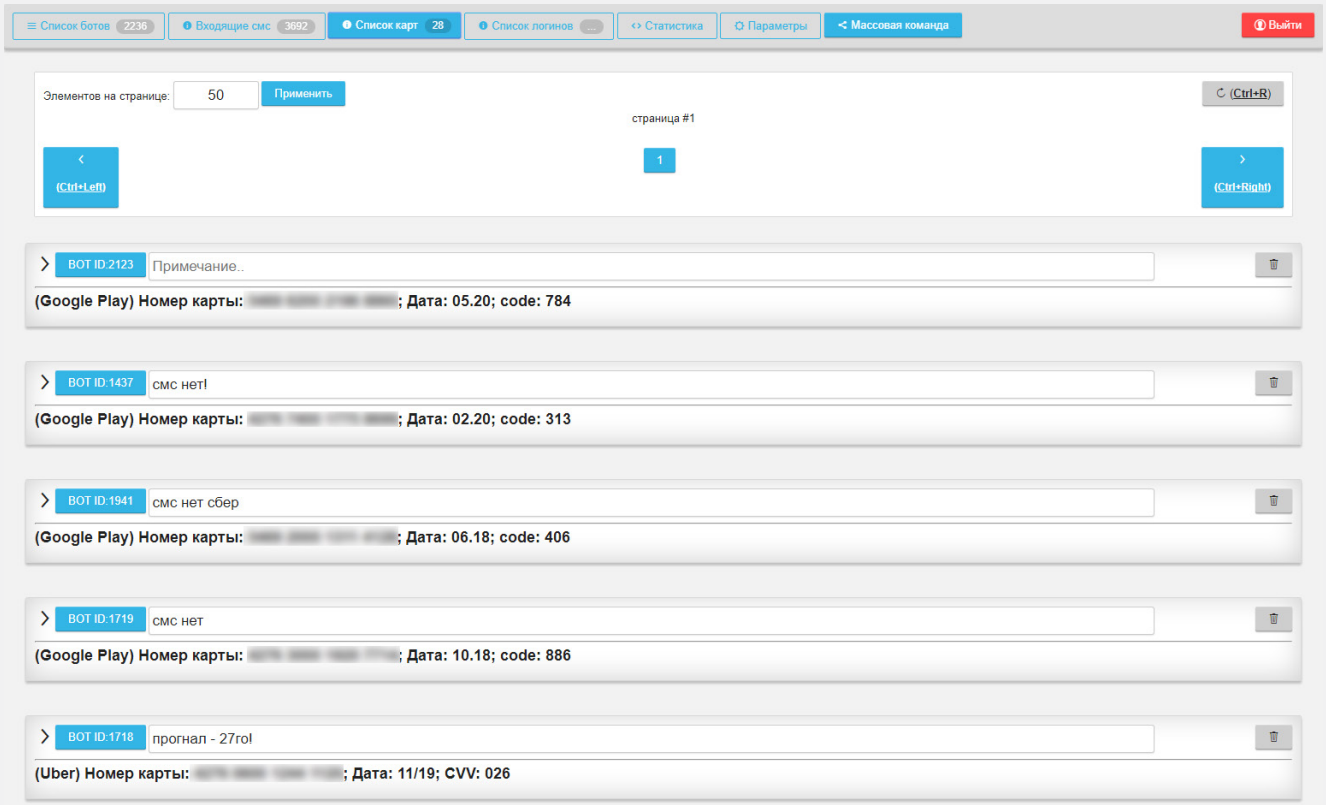
Статус	Троян	Дата появления	Регион разработчика	Регион атаки
АКТИВНЫЙ	BlackRock	Q2 2020	Неизвестно	США и Канада, Азиатско-Тихоокеанский регион
АКТИВНЫЙ	FluBot	Q1 2021	Россия	Европа
МАЛОАКТИВНЫЙ	Alien Bot	Q12020	Россия	США и Канада, Азиатско-Тихоокеанский регион, Европа
МАЛОАКТИВНЫЙ	OperadorMIB	Q12020	Латинская Америка	Латинская Америка
МАЛОАКТИВНЫЙ	BasBanke (Coybot)	2018	Латинская Америка	Латинская Америка
МАЛОАКТИВНЫЙ	Gustuff	Q4 2017	Россия	США и Канада, Азиатско-Тихоокеанский регион
МАЛОАКТИВНЫЙ	FlexNet	2014	Россия	Россия

Снимки экрана некоторых панелей вредоносных программ:

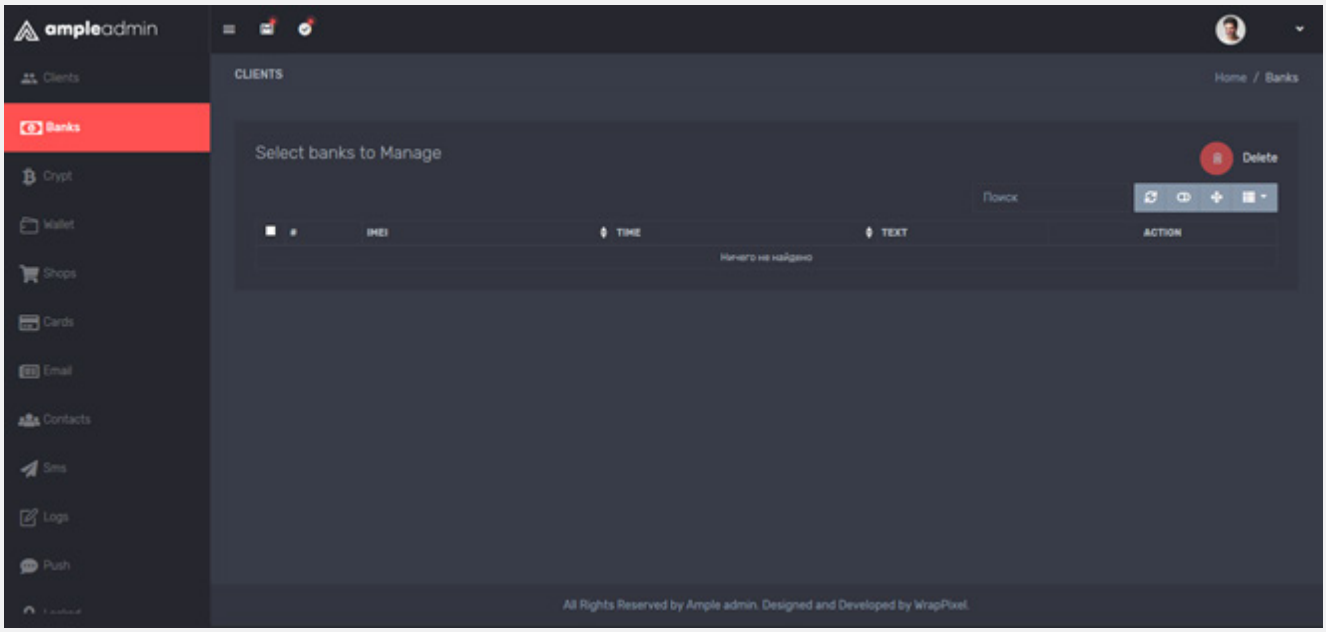
Cerberus



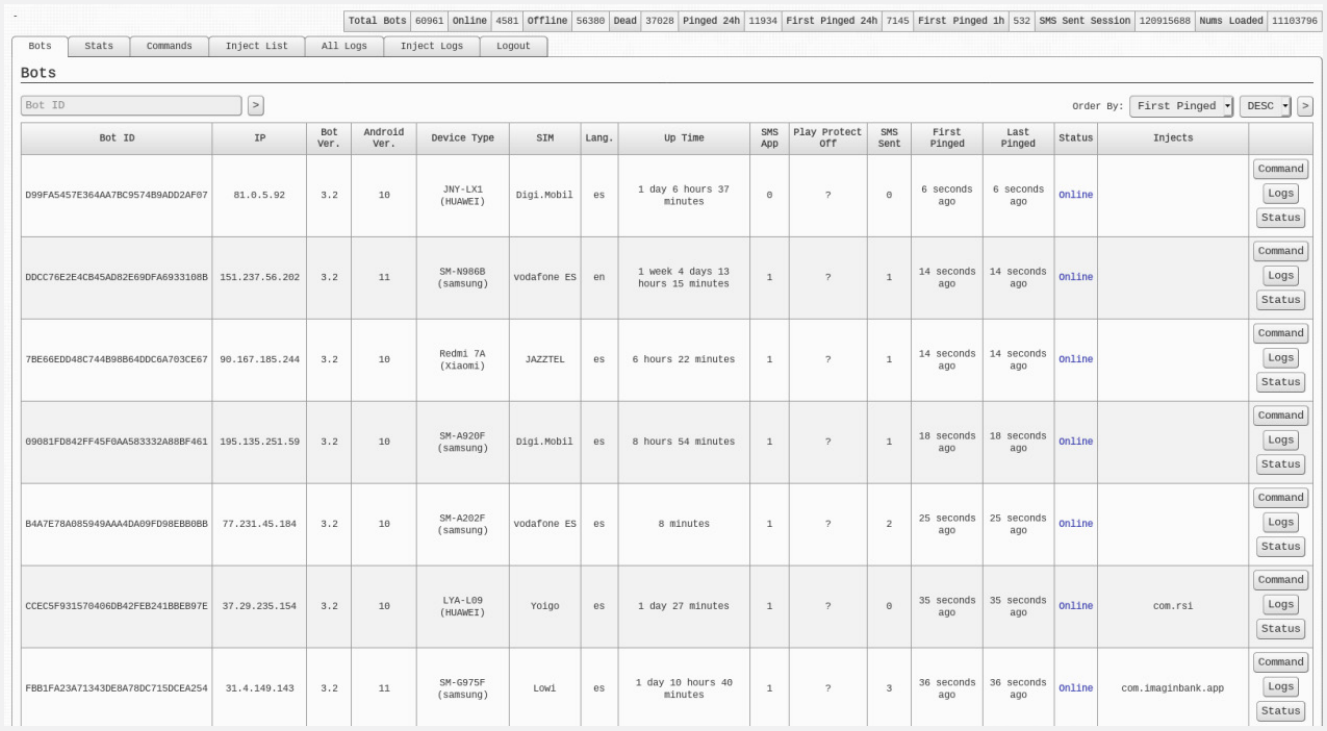
FlexNet



BlackRock



FluBot



Total Bots 60961 | Online 4581 | Offline 56380 | Dead 37028 | Pinged 24h 11934 | First Pinged 24h 7145 | First Pinged 1h 532 | SMS Sent Session 120915688 | Nums Loaded 11103796

Bots | Stats | Commands | Inject List | All Logs | Inject Logs | Logout

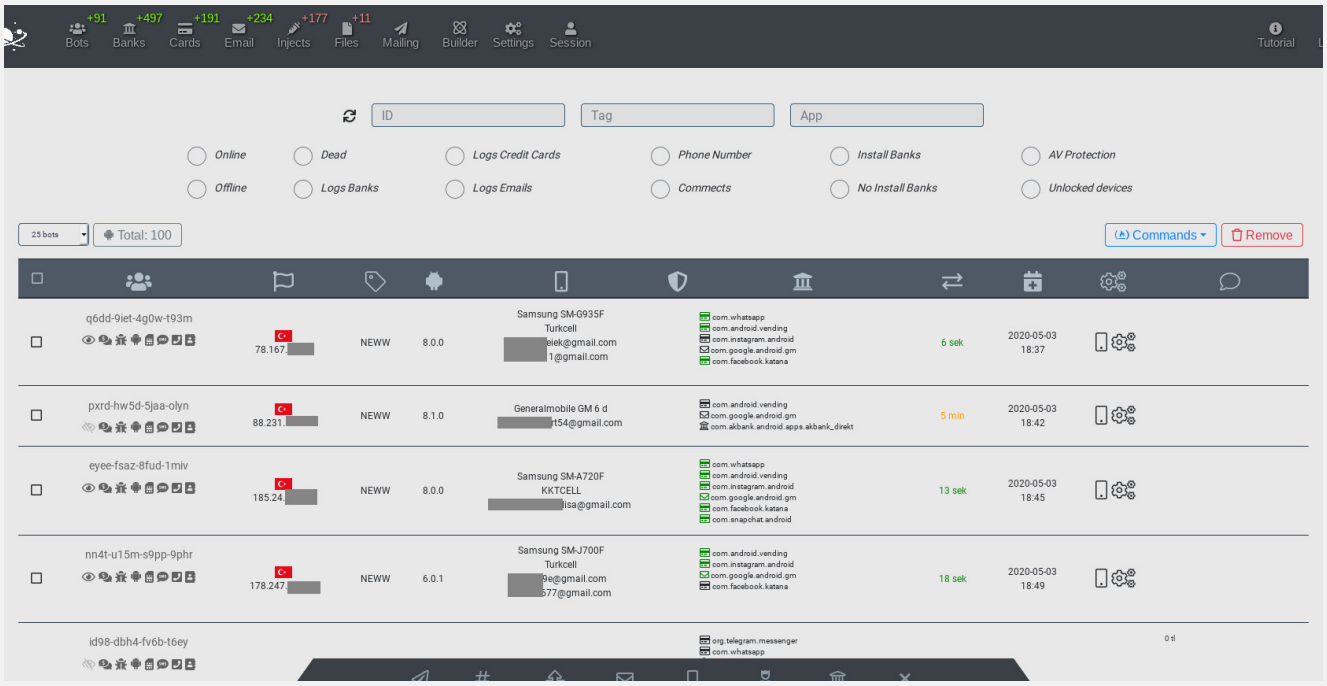
Bots

Bot ID >

Order By: First Pinged DESC >

Bot ID	IP	Bot Ver.	Android Ver.	Device Type	SIM	Lang.	Up Time	SMS App	Play Protect Off	SMS Sent	First Pinged	Last Pinged	Status	Injects	
D99FA5457E364AA7BC9574B9ADD2AF07	81.0.5.92	3.2	10	JNY-LX1 (HUAWEI)	Digi.Mobil	es	1 day 6 hours 37 minutes	0	?	0	6 seconds ago	6 seconds ago	Online		Command Logs Status
DDCC76E2E4CB45AD82E69DFA6933108B	151.237.56.202	3.2	11	SM-N986B (samsung)	vodafone ES	en	1 week 4 days 13 hours 15 minutes	1	?	1	14 seconds ago	14 seconds ago	Online		Command Logs Status
7BE66EDD48C744B98B64DDC6A703CE67	90.167.185.244	3.2	10	Redmi 7A (Xiaomi)	JAZZTEL	es	6 hours 22 minutes	1	?	1	14 seconds ago	14 seconds ago	Online		Command Logs Status
09081FD842FF45F0AA583332A88BF461	195.135.251.59	3.2	10	SM-A920F (samsung)	Digi.Mobil	es	8 hours 54 minutes	1	?	1	18 seconds ago	18 seconds ago	Online		Command Logs Status
B4A7E78A085949AAA4DA09FD98EB80BB	77.231.45.184	3.2	10	SM-A202F (samsung)	vodafone ES	es	8 minutes	1	?	2	25 seconds ago	25 seconds ago	Online		Command Logs Status
CCECSF931570406DB42FEB241BBEB97E	37.29.235.154	3.2	10	LYA-L09 (HUAWEI)	Yoigo	es	1 day 27 minutes	1	?	0	35 seconds ago	35 seconds ago	Online	com.rsi	Command Logs Status
FBB1FA23A71343DE8A78DC715DCEA254	31.4.149.143	3.2	11	SM-G975F (samsung)	Low1	es	1 day 10 hours 40 minutes	1	?	3	36 seconds ago	36 seconds ago	Online	com.imaginbank.app	Command Logs Status

Alien Bot



Bots +91 | Banks +497 | Cards +191 | Email +234 | Injects +177 | Files +11 | Mailing | Builder | Settings | Session | Tutorial

ID | Tag | App

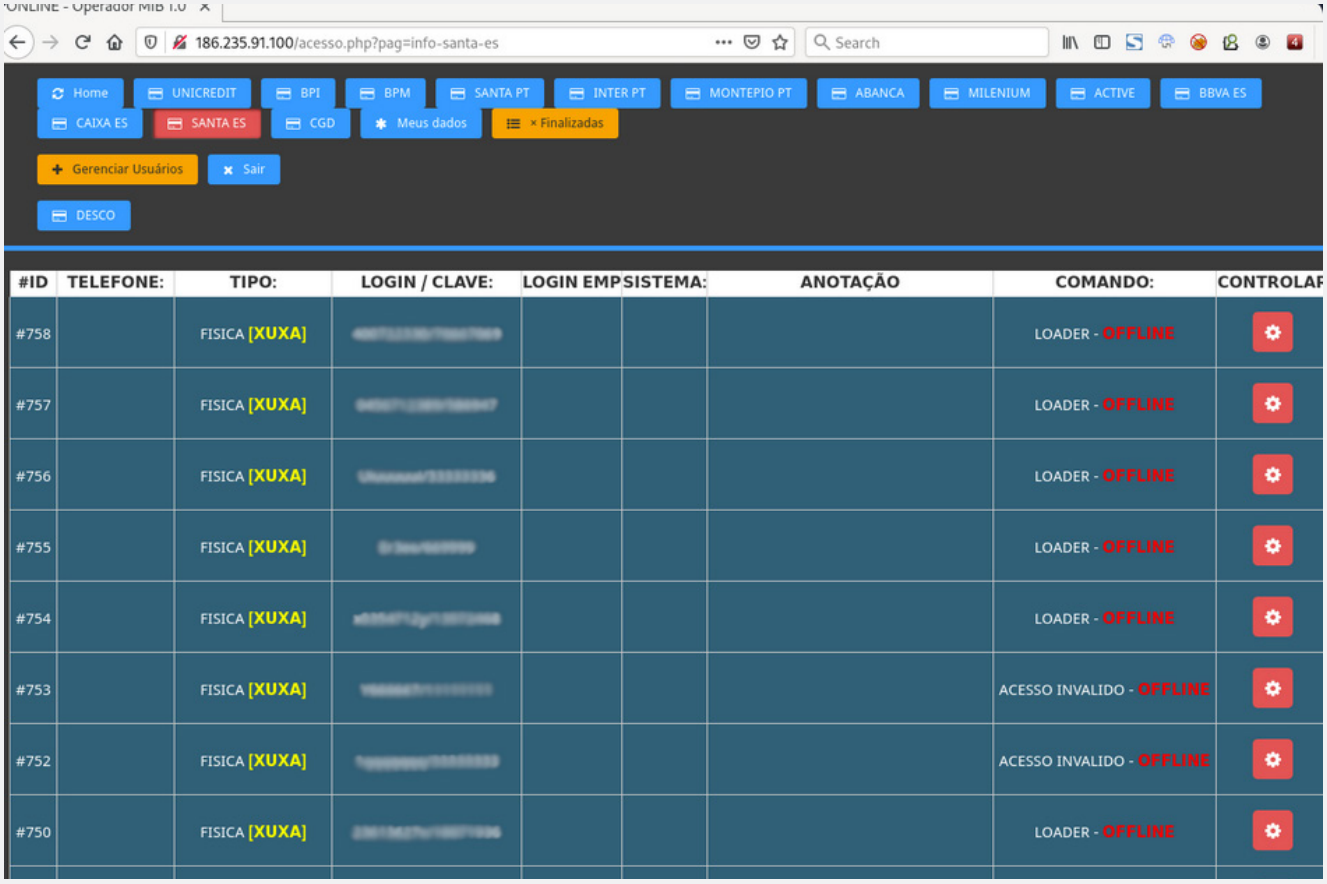
Online | Dead | Logs Credit Cards | Phone Number | Install Banks | AV Protection

Offline | Logs Banks | Logs Emails | Commects | No Install Banks | Unlocked devices

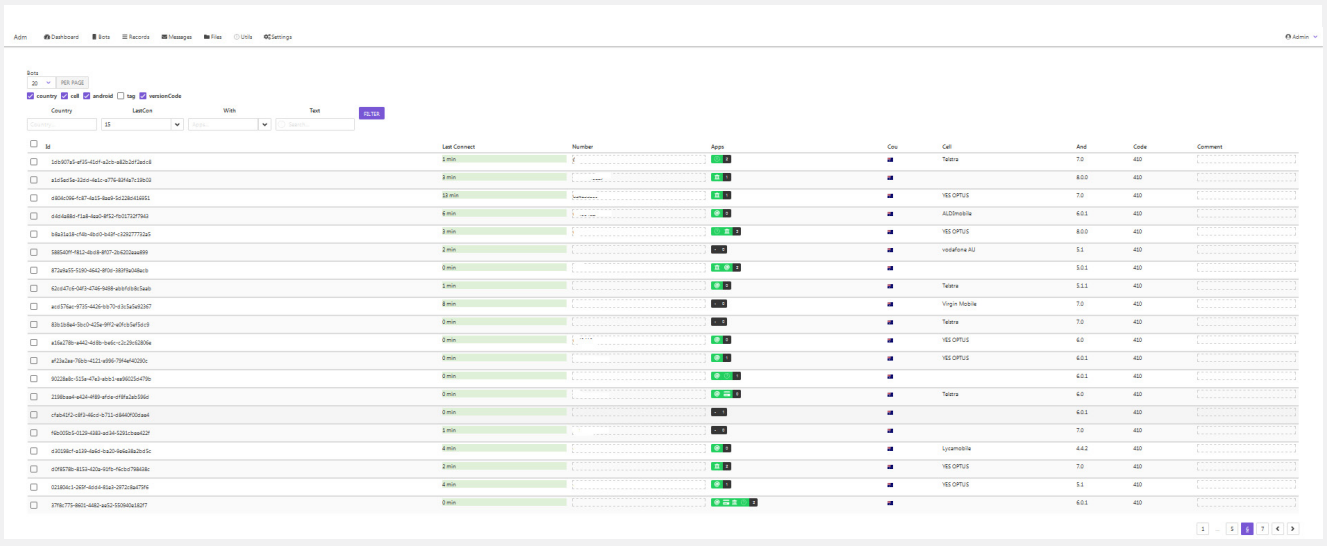
25 bots | Total: 100 | Commands | Remove

q6dd-9iet-4g0w-t93m	78.167.[redacted]	NEWW	8.0.0	Samsung SM-G935F Turkcell [redacted]1@gmail.com	com.whatsapp, com.android.vending, com.instagram.android, com.google.android.gm, com.facebook.katana	6 sek	2020-05-03 18:37			
pxrd-hw5d-5jaa-olyn	88.231.[redacted]	NEWW	8.1.0	Generalmobile GM 6 d [redacted]154@gmail.com	com.android.vending, com.google.android.gm, com.akbank.android.apps.akbank_direkt	5 min	2020-05-03 18:42			
eyee-fsaz-8fud-1miv	185.24.[redacted]	NEWW	8.0.0	Samsung SM-A720F KKTCELL [redacted]isa@gmail.com	com.whatsapp, com.android.vending, com.instagram.android, com.google.android.gm, com.facebook.katana, com.snapchat.android	13 sek	2020-05-03 18:45			
nn4t-u15m-s9pp-9phr	178.247.[redacted]	NEWW	6.0.1	Samsung SM-J700F Turkcell [redacted]9e@gmail.com [redacted]577@gmail.com	com.android.vending, com.instagram.android, com.google.android.gm, com.facebook.katana	18 sek	2020-05-03 18:49			
id98-dbh4-fv6b-t6ey					org.telegram.messenger, com.whatsapp					

OperadorMIB



Gustuff



ФИШИНГОВЫЕ ФРЕЙМВОРКИ

12

За прошедший год специалисты Group-IB фиксировали атаки с использованием 11 самых популярных фишинговых фреймворков[1], на которые пришлось почти 10 000 выявленных случаев фишинговых атак. Оказалось, что разработчик фишинг-китов зачастую находится в том же регионе, что и атакуемые банки и организации. Другая тенденция – продолжение атак с использованием конкретного фреймворка даже после ареста его разработчика. Например, многие злоумышленники создали собственные версии фишинг-китов на основе доступных исходников фишинговой панели U-Admin и используют их для атак.

[2] Фишинговые фреймворки – набор инструментов для фишинга, включающий киты для быстрого создания фишинговых сайтов и панели для взаимодействия с фишинговыми сайтами и сбора украденной информации.

U-Admin

#1

Атакуемые страны

Австралия, Бельгия, Германия, Греция, Дания, Ирландия, Испания, Италия, Колумбия, Нидерланды, Новая Зеландия, Польша, США, Канада, Сингапур, Финляндия, Франция, Швеция.

Создатель

Kaktys1010*

Первая активность

Неизвестно

Фишинговых панелей

1593

Панель U-Admin ↗

* Kaktys1010 был задержан украинскими правоохранительными органами в феврале 2021 года.

Contiinued

#2

Атакуемые страны

Австралия, Великобритания, Ирландия, Литва, Сингапур, Швеция

Создатель
Contiinued

Первая активность
Апрель 2021

Фишинговых панелей
34*

Панель Contiinued ↗

Core Actions

#3

Атакуемые страны

Австралия, Великобритания, Ирландия, Испания, Колумбия, Новая Зеландия, Норвегия, Филиппины

Создатель
Неизвестно

Первая активность
Апрель 2021

Фишинговых панелей
26

Express

#4

Атакуемые страны
Неизвестно

Создатель
Express**

Первая активность
Неизвестно

Фишинговых панелей
109

Панель Express ↗

* С 17 мая 2021 года исследователи обнаружили 34 фишинговые панели. Это означает, что панель такого типа была обнаружена на 34 различных доменах.

** Разработчик фишинговой панели Express был арестован 20 июля 2021 года в ходе совместных действий специалистов Group-IB и Национальной полиции Нидерландов.

Haiku

#5

Атакуемые страны

Бельгия, Нидерланды

Создатель
Haiku*

Первая активность
Апрель 2021

Фишинговых панелей
420

Панель Haiku ↗

Kr3pto

#6

Атакуемые страны

Австралия, Великобритания, Ирландия

Создатель
Kr3pto

Первая активность
Неизвестно

Фишинговых панелей
420

Панель Kr3pto ↗

Kr3pto-A2 (ATPro)

#7

Атакуемые страны

Великобритания, Дания, Норвегия, Сингапур

Создатель
Неизвестно**

Первая активность
Апрель 2021

Фишинговых панелей
18

* Haiku был заключен под стражу 19 октября 2020 года благодаря действиям отдела по борьбе с киберпреступлениями полиции Гааги.

** Фишинговая панель, основанная на коде панели Kr3pto и также известная как ATPro, была разработана злоумышленником, который предположительно находится в Великобритании

Reliable* #8

Атакуемые страны

Бельгия, Нидерланды

Создатель
Reliable**

Первая активность
Неизвестно

Фишинговых панелей
17

Панель Reliable ↗

Secure Key #9

Атакуемые страны

Великобритания, Австралия

Создатель
Неизвестно

Первая активность
Март 2020

Фишинговых панелей
2679

sm_o #10

Атакуемые страны

США

Создатель
Неизвестно

Первая активность
Июль 2020

Фишинговых панелей
249

* Эта фишинговая панель включает все возможности и исключает недостатки другой популярной фишинговой панели, U-Admin

** Разработчик Reliable был арестован 20 июля 2021 года в ходе совместных действий специалистов Group-IB и Национальной полиции Нидерландов

SPOX

#11

Атакуемые страны

США

Создатель

Dila Belmili*

Первая активность

Неизвестно

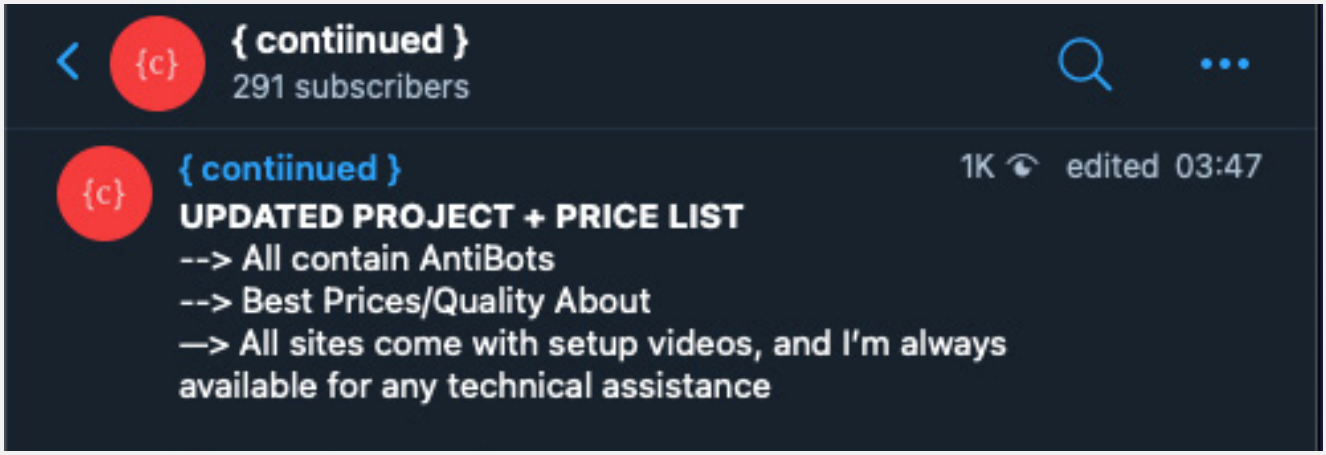
Фишинговых панелей

78

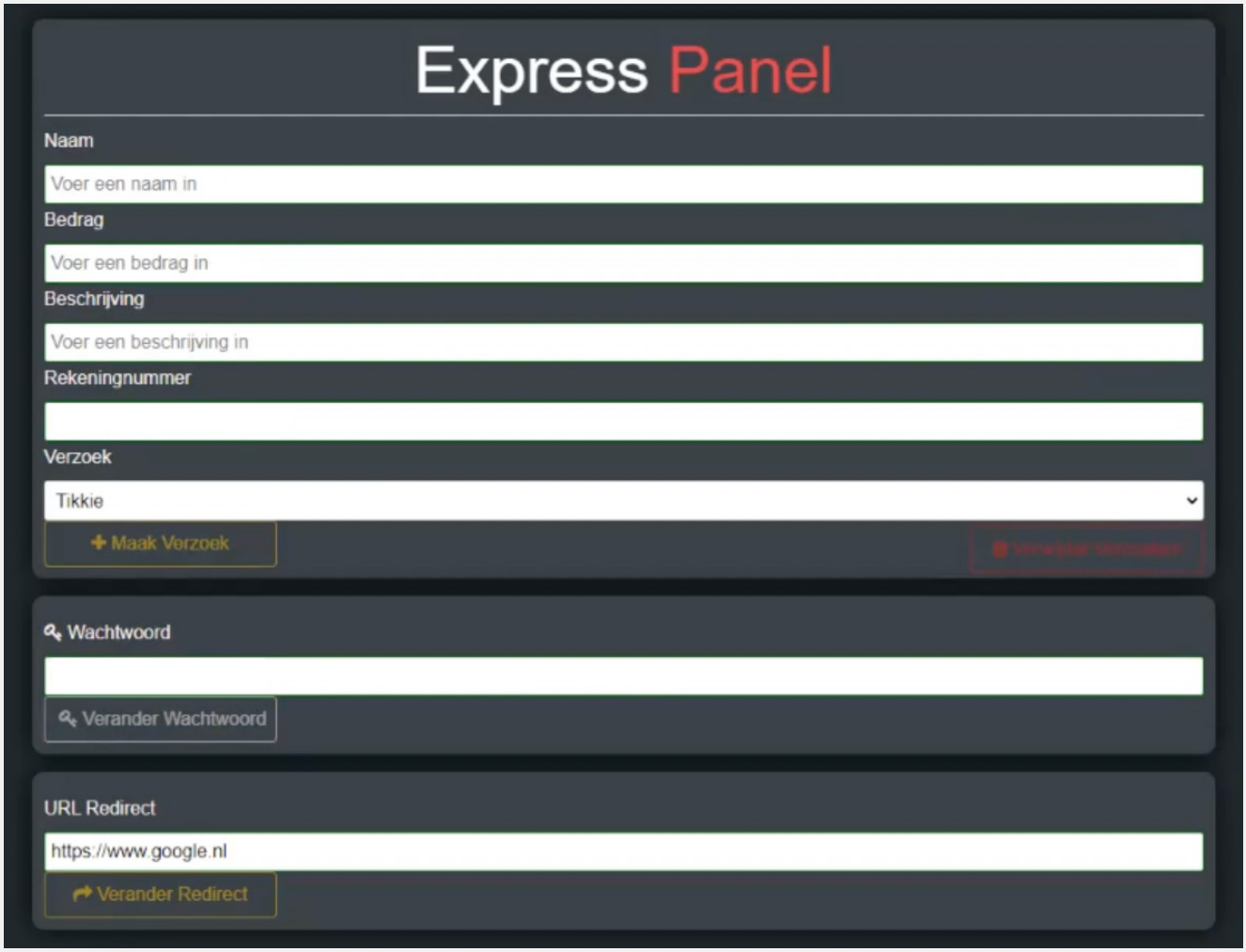
* Фишинговая панель, разработанная алжирским злоумышленником по имени Dila Belmili

Панель U-Admin

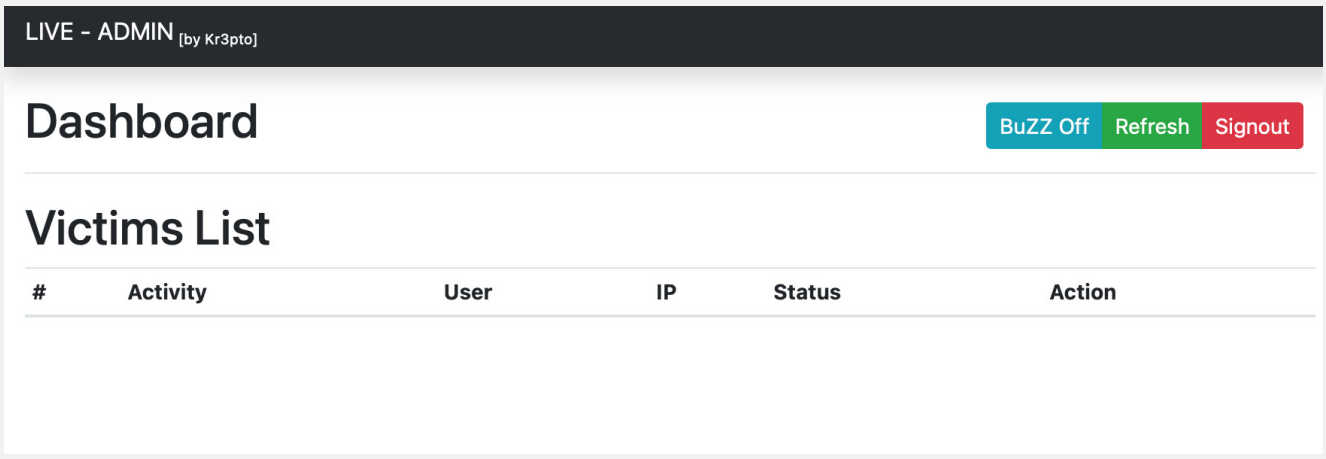
Панель Contiinued



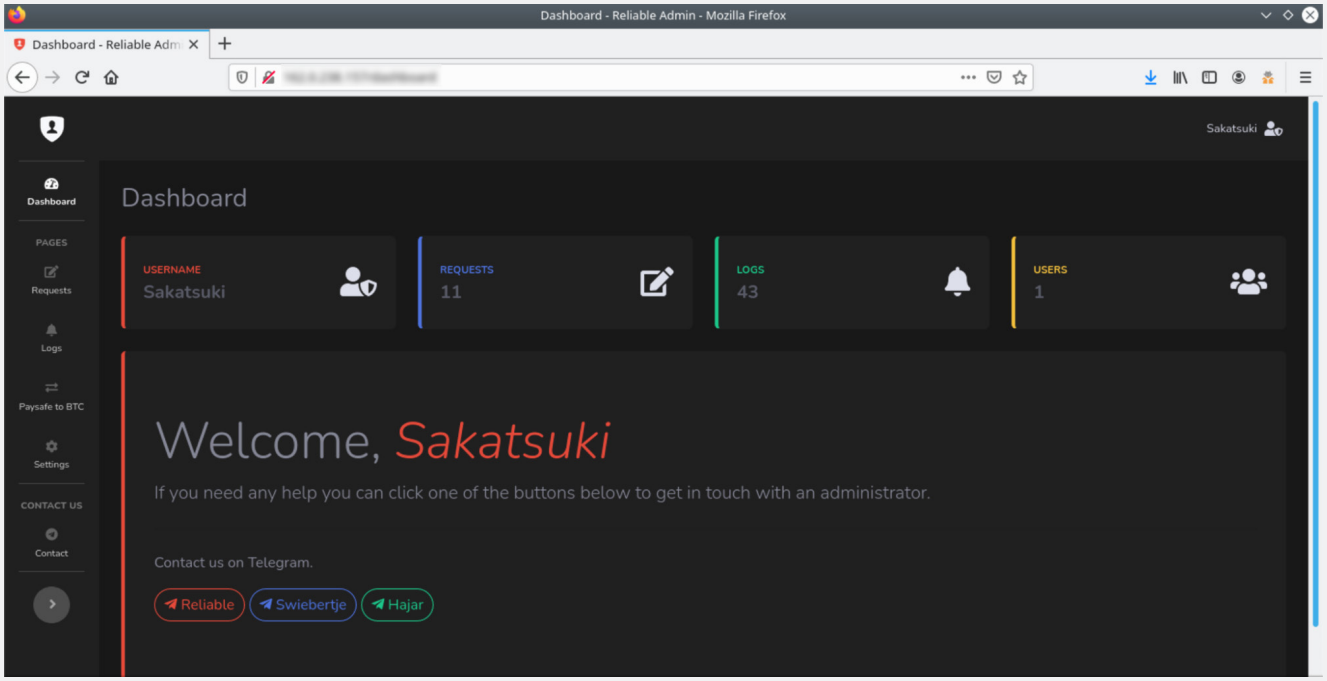
Панель Express



Панель Kr3pto



Панель Reliable и примеры рекламных объявлений



АКТИВНОСТЬ JS-СНИФФЕРОВ

Специалисты Group-IB обнаружили за отчетный период более 80 000 банковских карт, скомпрометированных с помощью JavaScript--снифферов. В топ-5 банков, чьи карты скомпрометировали злоумышленники, входят исключительно банки США, а в топ-20 присутствуют банки Бразилии, Великобритании, Индии, Канады, Малайзии и Сингапура. Это означает, что хотя злоумышленники и заинтересованы в атаках на онлайн-магазины большого числа стран, карты американских пользователей все еще являются приоритетом для хакеров. Из 98 семейств, известных специалистам Group-IB, активными за отчетный период были 42.

Более 33 000 карт было скомпрометировано при помощи JS-сниффера ImageId, разработанного злоумышленником под ником poter. Преступная группа, получившая название Improved-ImageID, по-прежнему использует модифицированную версию разработки poter'а для атак на онлайн-магазины. В октябре 2020 года специалисты MalwareBytes **обнаружили**, что данная группировка заразила сайт американского мобильного оператора "boom! MOBILE".

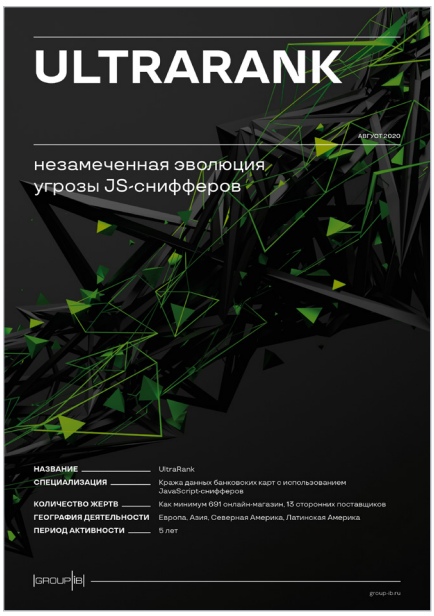
Группа **CoffeMokko** по-прежнему активна. По данным Group-IB, хакеры украли более 29 тысяч банковских карт при помощи JS-снифферов. В ноябре 2020 года специалисты Group-IB заметили, что почти вся инфраструктура группы ушла в офлайн, однако вскоре атаки на e-commerce сайты с использованием CoffeMokko возобновились.

В марте 2021 года специалисты Group-IB обнаружили новое семейство снифферов, получившее название WorldCommerce. В качестве гейтов для сбора украденных данных хакеры используют взломанные сайты. За обозначенный период при помощи данного сниффера было украдено почти 300 карт, однако чуть позднее группа скомпрометировала еще почти 6000 банковских карт.

Несколько преступных групп, использующих сниффер Inter, разработанный злоумышленником под псевдонимом Sochi, также были активны за прошедший год. По данным Group-IB, с использованием сниффера Inter было украдено более 16 000 банковских карт. Одной из жертв преступной группы, использующей сниффер Inter, стала платформа для видеоконференций Playback Now, о взломе которой специалисты Malwarebytes **сообщили** в октябре 2020 года.

В ноябре 2020 года специалисты Group-IB **обнаружили** новые атаки на сайты электронной коммерции, проведенные группой UltraRank, активной с 2015 года. В ходе новой кампании группа взломала 12 сайтов онлайн-магазинов и заразила их снифферoм SnifLite, который группа начала использовать еще в сентябре 2018 года. Однако в конце января 2021 года кардшоп ValidCC, предположительно используемый группой для монетизации украденных карт, прекратил свою работу. Представитель кардшопа, известный на подпольных форумах под ником SPR, заявил, что это связано с изъятием и отключением серверов

UltraRank: Незамеченная эволюция угрозы JS-снифферов



правоохранительными органами.

В связи с этим операторы кардшопа потеряли доступ к базе скомпрометированных карт и бэкенд магазина. С момента закрытия магазина специалисты Group-IB не обнаружили новых атак группы **UltraRank** несмотря на то, что часть инфраструктуры группы по-прежнему активна.

Некоторые преступные группы, проводящие атаки на онлайн-магазины, экспериментируют с легитимной инфраструктурой для размещения вредоносного кода. В мае 2021 года специалисты Group-IB **описали** активность группы GrelosGTM, обнаруженной в апреле 2020 года, в ходе которой группа использовала легитимный сервис Google Tag Manager для доставки вредоносного кода на зараженные сайты. В феврале 2021 года ресерчер Eric Brandel совместно со специалистами Sansec обнаружили, что группа GrelosGTM использовала другую платформу, Google Apps Script для доставки вредоносного кода на сайты онлайн-магазинов.

Преступники экспериментируют со способами эксфильтрации банковских карт, украденных у пользователей зараженных сайтов онлайн-магазинов. Сниффер, получивший название TelegramExfil, использовал Telegram Bot API для отправки перехваченных карт операторам сниффера, о чем **сообщили** специалисты Malwarebytes в сентябре 2020 года.

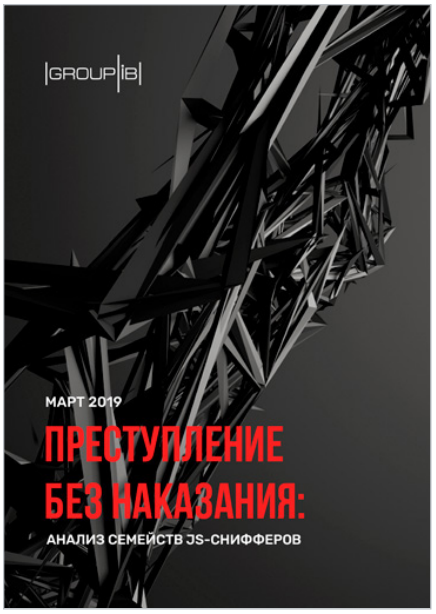
В январе 2021 года специалисты Group-IB обнаружили новое семейство сниффероов, получившее название **E1RB**. Преступная группа, стоящая за разработкой сниффера, использовала несколько нестандартных подходов для обфускации образцов вредоносного кода: при каждом запросе к серверу злоумышленников он генерировал новый уникальный обфусцированный сэмпл сниффера, а частью механизма обфускации было время запроса, где значение минут использовалось для расшифровки кода сниффера во время исполнения кода. Для обфускации JS-кода злоумышленники использовали обфускатор с открытым исходным кодом под названием **Hunter**.

В декабре 2020 года специалисты Group-IB опубликовали подробное **исследование** операций преступной группы FakeSecurity, проводившей вредоносные кампании. Они были нацелены на администраторов онлайн-магазинов с целью заражения их сайтов вредоносным JS-кодом для кражи банковских карт. В ходе атак группа использовала фреймворк для создания лендинговых страниц для распространения вредоносных программ Mephistophilus, стилеров Vidar и Raccoon, а также разработанного группой сниффера FakeSecurity, обфусцированного при помощи алгоритма aaencode.

Продолжаются атаки с использованием сниффера Mr.Sniffa, созданного злоумышленником под ником Billar. Также неизвестные злоумышленники адаптировали административную панель сниффера для распространения вредоносного ПО под видом обновлений Adobe Flash. Специалисты Sucuri в ноябре 2020 года описали кампанию, в ходе которой использовался инжектор, позаимствованный у сниффера Mr.Sniffa, но вместо кода для кражи карт он загружал обфусцированный код для показа поддельного окна обновлений.

По-прежнему активны как минимум 4 группы, стоящие за снифферами, описанными в отчете «Преступление без наказания: анализ семейств JS-сниффероов». Группа, использующая сниффер PostEval, продолжает свои атаки на сайты онлайн-магазинов. Также активна группа, стоящая за снифферoм Illum. Группа, использовавшая сниффер MagentoName, модифицировала код из своего арсенала и провела одну из самых крупных атак на Magento-сайты, обнаруженную специалистами Sansec в сентябре 2020 года. Тогда группа единоразово заразила 2806 сайтов,

Преступление без наказания: анализ семейств js-сниффероов



работающих под управлением Magento первой версии. По-прежнему активна группа, использующая сниффер ReactGet: активно заражает сайты, поддерживает свою инфраструктуру и проводит фишинговые атаки, примеры которых были обнаружены в сентябре-декабре 2020 и январе-марте 2021

Таблица по активным и неактивным снифферам за отчетный период (H2 2020 — H1 2021)

Название сниффера	Дата появления/Дата обнаружения	Активность в отчетном периоде
Qoogle	Апрель 2018	Да
FareCloud	Апрель 2020	Да
SF_GATE	Апрель 2020	Да
ant_cockroach	Август 2019	Да
AnyCDN	Август 2020	Да
Inter	Декабрь 2018	Да
docReady	Декабрь 2019	Да
CounterApi	Декабрь 2020	Да
ShipBill	Декабрь 2020	Да
Shopi-DGA	Декабрь 2020	Да
ArrCut	Февраль 2020	Да
EpikCDN	Февраль 2020	Да
OurHoney	Февраль 2021	Да
FakeClicky	Январь 2018	Да
E1RB	Январь 2021	Да
ImageId/Poter/Improved-ImageId	Июль 2016	Да
FakeGraph	Июнь 2020	Да
Mr.Sniffa	Март 2020	Да
SunPearl	Март 2020	Да
WorldCommerce	Март 2021	Да
ReactGet	Май 2017	Да
OrderManagement	Май 2021	Да
Illum	Ноябрь 2016	Да
FakeSecurity	Ноябрь 2018	Да
OrderData	Ноябрь 2019	Да
AngryBeaver	Ноябрь 2020	Да
ClearConsole	Ноябрь 2020	Да
SadPixel	Октябрь 2019	Да
FellSoGood	Июль 2020	Да
CoffeMokko	Сентябрь 2017	Да
PostEval	Сентябрь 2017	Да

Название сниффера	Дата появления/Дата обнаружения	Активность в отчетном периоде
SnifLite	Сентябрь 2018	Да
occhurch	Сентябрь 2020	Да
TelegramExfil	Сентябрь 2020	Да
GuettaTech	Октябрь 2020	Да
HostSSL	Апрель 2020	Да
JCI	Октябрь 2019	Да
LazySale	Ноябрь 2020	Да
TrackStat	Декабрь 2019	Да
WooAnalytics	Июль 2021	Да
XStatic	Ноябрь 2020	Да
zzzerohost/Baka	Март 2020	Да
MirrorThief	Апрель 2019	Нет
SJTI	Апрель 2019	Нет
PokerFace	Август 2019	Нет
OldGrelos	Декабрь 2015	Нет
MagentoName	Декабрь 2017	Нет
event_handler	Декабрь 2019	Нет
fouhasgfuas	Декабрь 2019	Нет
GetBilling	Февраль 2018	Нет
Atlas	Февраль 2019	Нет
MageConnectors	Февраль 2019	Нет
TimedMe	Январь 2018	Нет
FabricRelay	Январь 2019	Нет
Luna	Январь 2019	Нет
MakeFrame	Январь 2020	Нет
SeoStat	Январь 2020	Нет
SpaceManager	Январь 2020	Нет
FakeLogistics	Июль 2015	Нет
EUTag	Июль 2018	Нет
addtoev	Июль 2019	Нет
simplewheel	Июль 2019	Нет
TokenMSN	Июнь 2016	Нет
CheckTrack	Июнь 2020	Нет
TokenLogin	Март 2016	Нет
Analyt	Май 2019	Нет
ATMZOW	Май 2019	Нет
AwesomeSocket	Май 2019	Нет
CDNAPI	Май 2019	Нет

Название сниффера	Дата появления/Дата обнаружения	Активность в отчетном периоде
GMO.LI	Май 2019	Нет
ShellSn	Май 2019	Нет
FakeCDN	Ноябрь 2016	Нет
PreMage	Ноябрь 2016	Нет
LoadReplay	Ноябрь 2017	Нет
503Susp	Ноябрь 2018	Нет
Pipka	Ноябрь 2019	Нет
cCreateSelectionDiv	Март 2020	Нет
WebRank	Октябрь 2016	Нет
MatrixShop	Октябрь 2018	Нет
FakePixel	Октябрь 2019	Нет
MakeEvent	Октябрь 2020	Нет
G-Analytics	Сентябрь 2016	Нет
OrgCDN	Сентябрь 2018	Нет
FakeGAds	Сентябрь 2019	Нет
GrelosAnalytics	Июль 2019	Нет
HellGate	Май 2019	Нет
HotelTrack	Август 2019	Нет
Iranimo	Октябрь 2019	Нет
jQueryFact	Май 2019	Нет
Lazarus clientToken	Май 2019	Нет
Lazarus preloader	Февраль 2020	Нет
LinkCatalog	Июнь 2017	Нет
LogEvil	Январь 2019	Нет
MajorMs	Октябрь 2018	Нет
WebPackCDN	Июль 2019	Нет
VeterinaryConcepts	Сентябрь 2018	Нет
Voldemort	Август 2018	Нет
XMLRAW	Сентябрь 2019	Нет

РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ

14

Финансовые организации сталкиваются с различными киберугрозами. Изучив техники и методы злоумышленников, специалисты Group-IB разработали рекомендации для защиты от каждого вида атак.

Продажа доступов в финансовые учреждения

1. Настройка блокировки учетной записи для защиты от брутфорс-атак.
2. Проверка логинов и паролей в публичных утечках и смена паролей, которые уже находятся в утечках.
3. Ограничение удаленного доступа только с доверенных IP-адресов, либо после успешной идентификации устройства, с которого осуществляется удаленный доступ. Если такие меры невозможны, то необходимо ввести фильтрацию по Geo IP.
4. Отключение или блокировка невостребованных удаленных сервисов.
5. Использование многофакторной аутентификации для учетных записей удаленных сервисов. Это ограничивает возможности использования скомпрометированных учетных данных.
6. Использование минимальных привилегий для учетных записей служб ограничивает права, получаемые процессом, уязвимость в котором может быть использована.
7. Своевременное и регулярное обновление программного обеспечения, которое позволяет закрывать обнаруженные уязвимости.
8. Регулярное проведение анализа защищенности и тестирования на проникновение, чтобы выявить слабые места и возможные векторы атак.
9. Проведение инвентаризации внешнего сетевого периметра, правил межсетевого экранирования (Firewall) и правил трансляции сетевых адресов (NAT) для исключения ошибочно опубликованных сервисов.

10. Осуществление непрерывной идентификации теневых ИТ для управления поверхностью атаки.
11. Запрет на публикацию в интернете устройств, которые могут быть легко скомпрометированы: видеонаблюдение, «умный дом», оргтехнику (принтеры, сканеры, МФУ), устройства хранения (типа NAS-серверов сегмента SOHO).
12. Ограничение сетевого доступа по задачам конкретной учетной записи. К примеру, подрядчик получает доступ только к нужному ему серверу, а не всему сегменту или всей сети.
13. Выставление поля вида “expires at” для учетных записей и правил доступа на случай, если даст сбой процесс ручного отзыва удаленного доступа.
14. Выявление признаков изначального доступа, закрепления в системе, продвижения по сети. Хотя чаще всего техники атакующих достаточно примитивны, с более сложными атаками может помочь регулярная проактивная охота за угрозами (threat hunting).
15. Детектирование и регулярная дополнительная проверка инфраструктуры на известные индикаторы компрометации.
16. Запрет пользователям регистрироваться на сторонних сервисах с использованием корпоративной почты.

Атаки операторов программ-шифровальщиков

1. Отслеживайте события, связанные с созданием подозрительных папок или файлов или запуском таких процессов, как rundll32.exe или regsvr32.exe с помощью winword.exe/excel.exe.
2. Выявляйте подозрительные запуски cscript.exe/wscript.exe, особенно те, которые связаны с сетевой активностью.
3. Выявляйте процессы powershell.exe с подозрительными или обфусцированными командными строками.
4. Анализируйте исполняемые файлы и скрипты, помещенные в папку автозагрузки, добавленные в ключи Run или запускаемые с помощью планировщика задач.
5. Отслеживайте выполнение sdbinst.exe на предмет подозрительных аргументов командной строки.
6. Проверяйте создание новых ключей в разделе HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options.
7. Убедитесь, что ваши системы защиты умеют выявлять командные строки, характерные для средств дампинга учетных данных, таких, как Mimikatz.
8. Ищите артефакты, характерные для инструментов сетевой разведки, такие, как аргументы командной строки AdFind.
9. Выявляйте артефакты, связанные с выполнением файлов из необычных мест, таких, как “C:\ProgramData, %TEMP% or %AppData%”.
10. Выявляйте модификации реестра и брандмауэра Windows, связанные с подключениями по RDP.
11. Отслеживайте и анализируйте соединения по RDP, чтобы выявлять попытки продвижения по сети.

12. Выявляйте запуски wmic.exe с использованием подозрительных командных строк.
13. Отслеживайте аномальное поведение bitsadmin.exe , особенно связанное с загрузкой потенциально вредоносных файлов.
14. Убедитесь, что ваши системы умеют выявлять полезные нагрузки Cobalt Strike Beacon и подобных им инструментов, характерных для пост-эксплуатационных фреймворков. Как минимум обратите внимание на те системы, которые запускаются с типичными аргументами командной строки и из типичных мест.
15. Отслеживайте сетевые соединения из распространенных системных процессов. Используйте известные списки серверов Cobalt Strike, которые вы можете получить у вашего поставщика Cyber Threat Intelligence.
16. Отслеживайте события создания новых служб, связанных с PsExec, SMBExec и другими средствами двойного назначения или инструментами пентестинга.
17. Отслеживайте исполняемые файлы, замаскированные под общие системные файлы (такие как svchost.exe), но имеющие аномальные родительские файлы или местоположение.
18. Отслеживайте признаки несанкционированного использования инструментов удаленного доступа в вашей сети.
19. Отслеживайте события установки клиентов облачных хранилищ и события доступа к облачном хранилищам, и проверяйте, являются ли они легитимными.
20. Отслеживайте распространенные FTP-программы на конечных хостах для выявления событий установки файлов с вредоносными конфигурациями.

Фишинг, фишинговые и мошеннические партнерские программы, подложные страницы приема платежей

1. Необходим процесс сбора информации о мошеннических ссылках и скриншотов со ссылками от клиентов.
2. Ссылки должны быть исследованы и заблокированы.
3. Проводить анализ транзакцией с целью определения схем обналичивания средств.
4. Проактивная охота за фишинговыми сайтами.
5. Информировать клиентов о мошеннических схемах.

Банковские бот-сети и трояны

1. Применение сессионного анализа для выявления атак Man-in-the-browser.
2. Анализ сессий для выявления факта удаленного управления компьютером в момент совершения платежа.
3. Анализ и выявление симуляции окружения пользовательского компьютера.
4. Выявление скомпрометированных логинов, паролей и банковских карт.

Вредоносные программы для Android

1. Используя мобильные приложения, анализировать окружение и выявлять подозрительные приложения на устройстве.
2. Выявлять факт запуска приложения на устройстве с root-правами.
3. Выявление показа оверлей окон.
4. Выявление перехвата СМС- или push-уведомлений.

JS-сниффферы

1. Требовать от e-commerce сайтов соблюдение мер безопасности.
2. В договорах предусмотреть возможность экспресс-проверки e-commerce сайтов на наличие уязвимого ПО.
3. Проводить экспресс-проверки.
4. Выявлять точки компрометации карт путем анализа пересечений мест использования скомпрометированных карт.
5. Анализировать продаваемые карты на кардшопах для выявления точек компрометации.

Group-IB

— один из ведущих разработчиков решений для детектирования и предотвращения кибератак, выявления мошенничества, расследования высокотехнологичных преступлений и защиты коммерческой и интеллектуальной собственности в сети.

Миссия Group-IB: Fight Against Cybercrime

Interpol и Europol

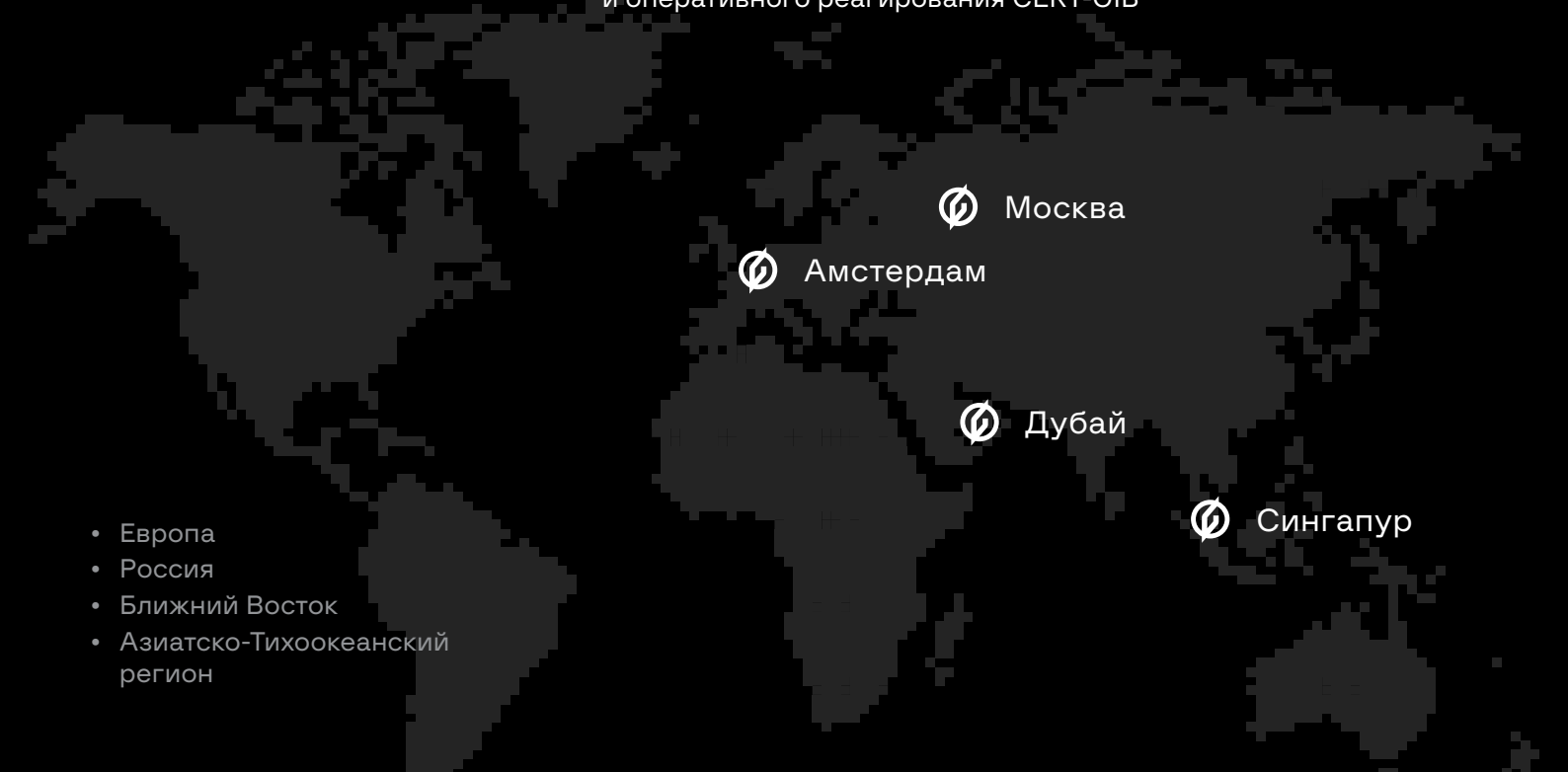
Group-IB — партнер и участник совместных расследований

Топ-10 в APAC

Group-IB вошла в топ-10 компаний по кибербезопасности в регионе APAC согласно APAC CIO Outlook

Центры исследования киберугроз Group-IB

- Распределенная по миру инфраструктура наблюдения за киберпреступностью
- Лаборатории компьютерной криминалистики
- Реагирование и исследование киберпреступлений
- Круглосуточные центры мониторинга и оперативного реагирования CERT-GIB



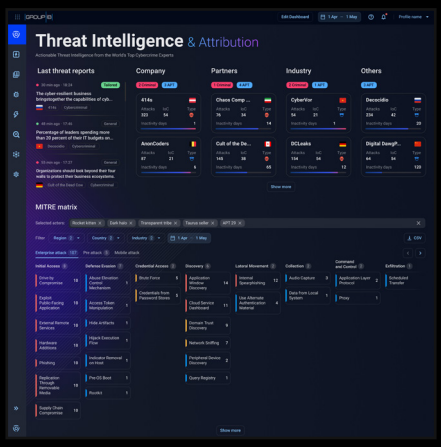
- Европа
- Россия
- Ближний Восток
- Азиатско-Тихоокеанский регион

Решения Group-IB

Опыт Group-IB в международных расследованиях, киберразведке и выявлении преступлений на разных уровнях подготовки был интегрирован в экосистему решений, объединяющую чрезвычайно сложное программное и системное обеспечение, с целью мониторинга, обнаружения и предотвращения кибератак и мошенничества.

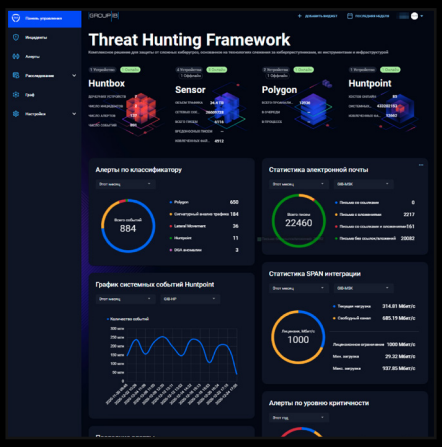
Решения Group-IB признаны мировыми агентствами

IDC Gartner FORRESTER kuppingercole ANALYSTS FROST & SULLIVAN



Threat Intelligence & Attribution

Система исследования и атрибуции кибератак, охоты за угрозами и защиты сетевой инфраструктуры

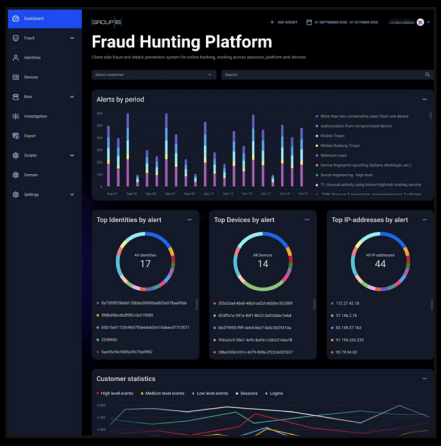


Threat Hunting Framework

Система защиты от сложных целевых атак и проактивной охоты за угрозами внутри и за пределами периметра

Digital Risk Protection

Выявление и устранение цифровых рисков на основе искусственного интеллекта



Fraud Hunting Platform

Цифровая защита и противодействие мошенничеству в реальном времени

Atmosphere: Cloud Email Protection

Облачная защита электронной почты от целевых атак, детонация полезных нагрузок и атрибуция угроз

AssetZero

Мониторинг внешнего периметра с помощью данных киберразведки

Экспертиза Group-IB

600+

экспертов международного класса

70 000+

часов реагирования на инциденты информационной безопасности

1 300+

успешных расследований по всему миру

18 лет

практического опыта

Intelligence-driven services

В основе технологического лидерства компании, возможностей в сфере научных исследований и разработки — 18-летний практический опыт расследования киберпреступлений по всему миру и более 70 000 часов реагирования на инциденты информационной безопасности, аккумулированные в распределенной по миру инфраструктуре наблюдения за киберпреступностью.

Предотвращение

- Аудит безопасности
- Оценка безопасности
- Red Teaming
- Pre-IR Assessment
- Compromise Assessment
- Обучение

Реагирование

- Managed Incident reponse
- Managed detection and threat hunting

Расследование

- Компьютерная криминалистика
- Расследования
- Финансовые расследования
- eDiscovery

ПРЕДОТВРАЩАЕМ И ИССЛЕДУЕМ КИБЕРПРЕСТУПЛЕНИЯ С 2003 ГОДА

www.group-ib.ru info@group-ib.com group-ib.ru/blog +7 495 984 3364