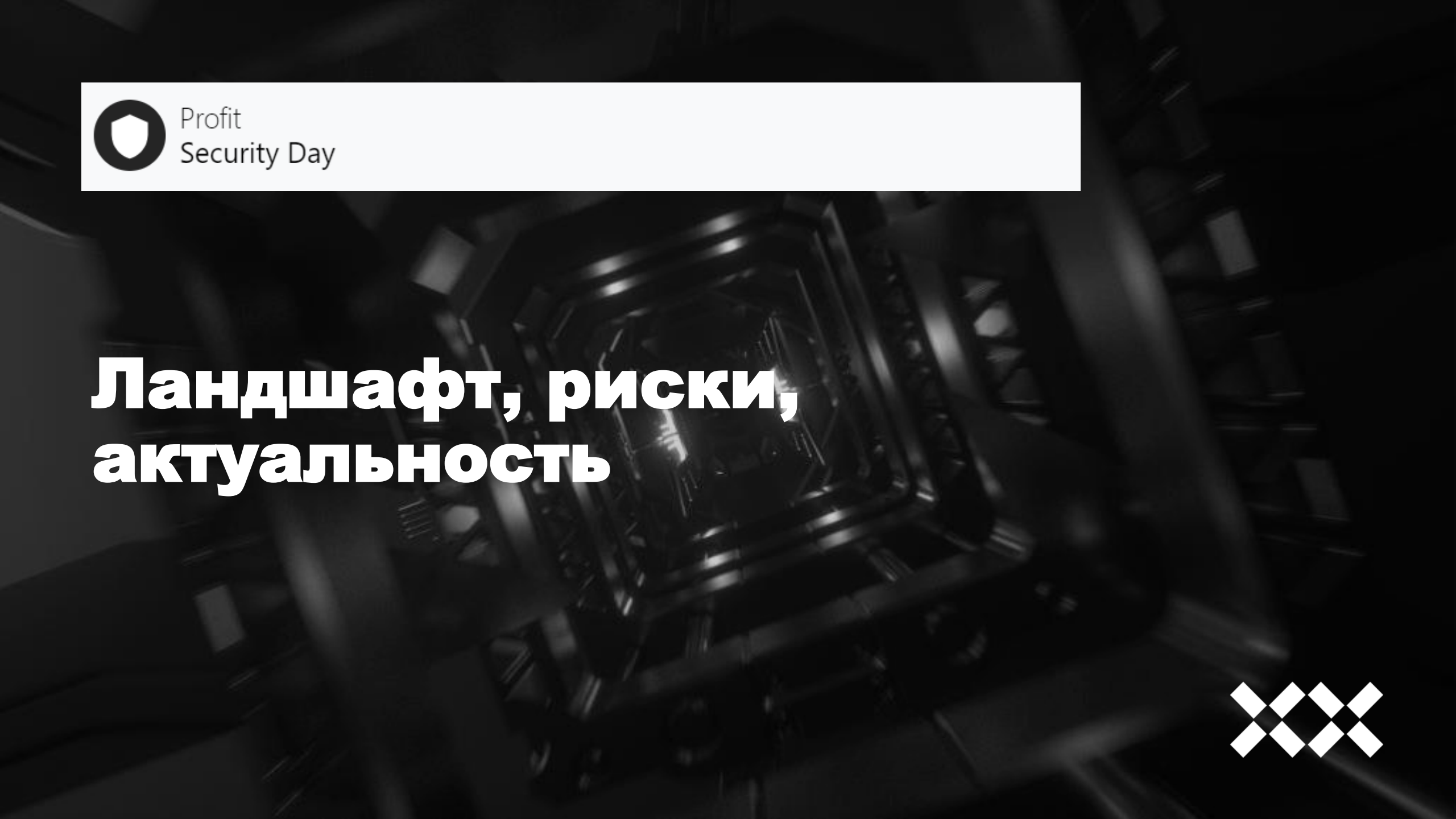
Profit
Security Day

Ландшафт угроз 2020. Комплексный подход Group-IB к противодействию сложным целевым атакам и неизвестным угрозам

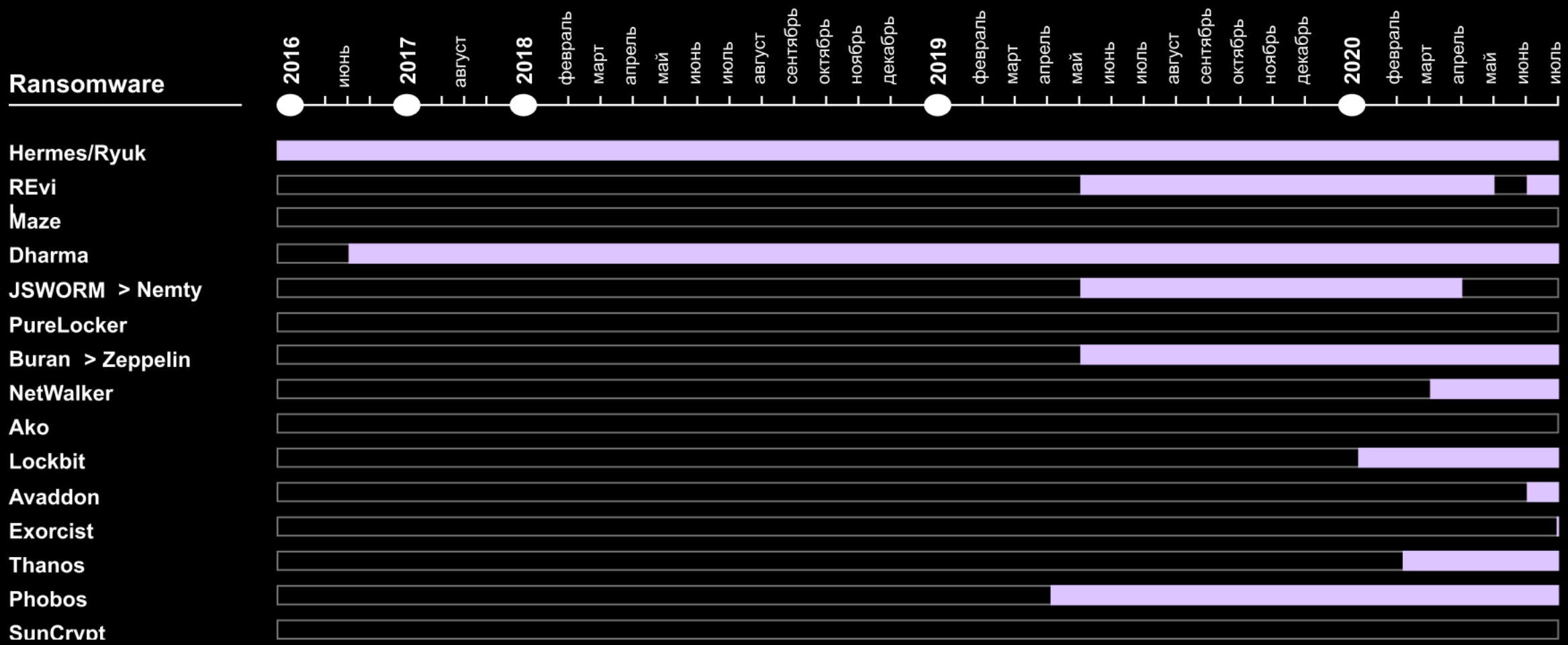
Станислав Фесенко

Руководитель Департамента системных решений Group-IB



Ландшафт, риски, актуальность

RANSOMWARE-ПАРТНЕРКИ — ОСНОВА ВСЕГО



RANSOMWARE-ПАРТНЕРКИ — ОСНОВА ВСЕГО

НА 50% УВЕЛИЧИЛОСЬ КОЛИЧЕСТВО ПАРТНЕРОК

7 из 15 партнерских программ были запущены в период H2 2019 — H1 2020

БАНКОВСКИЕ БОТ-СЕТИ — RANSOMWARE-ПАРТНЕРЫ

Владельцы банковских бот-сетей — TrickBot, Qbot, Silent Night, RTM — начали использовать свои бот-сети для установки Ransomware

COBALT И SILENCE — ТОЖЕ ПАРТНЕРЫ

Предположительно, Cobalt и Silence, которые ранее специализировались на банковских атаках, стали участниками приватных партнерских программ

RANSOMWARE: УЩЕРБ И МОТИВАТОРЫ

ГРУППА	СРЕДНЯЯ СУММА ВЫКУПА ($)	КОЛИЧЕСТВО ЖЕРТВ	ПОТЕНЦИАЛЬНЫЙ УЩЕРБ
Ako	555	9	4995
Avaddon	7500	1	7500
Clop	1500	15	22 500
Conti	1500	2	3000
DoppelPaymer	1 143 500	53	60 605 500
Maze	2 420 000	155	375 100 000
MegaCortex	2 700 000	1	2 700 000
Nefilim	1000	13	13 000
NetWalker	720 000	49	35 280 000
Pysa	None	25	None
Ragnar	7 750 000	10	77 500 000
REvil	260 000	103	26/780 000
Ryuk	1 451 500	62	89 993 000
Sekhmet	None	6	None
Snake	None	3	None
SunCrypt	400 000	2	80 000
WastedLocker	10 000 000	32	320 000 000

RANSOMWARE: УЩЕРБ И МОТИВАТОРЫ

1	ОТКРЫТАЯ ПУБЛИКАЦИЯ ДАННЫХ
2	ПРОВЕДЕНИЕ АУКЦИОНОВ
3	DDOS-АТАКИ

$10 МЛН — МАКСИМАЛЬНАЯ СУММА ВЫМОГАТЕЛЬСТВА

Суммы вымогательства варьируются от десятков тысяч долларов до 10 миллионов.

>$1 МЛРД — МИНИМАЛЬНАЯ СУММА УЩЕРБА

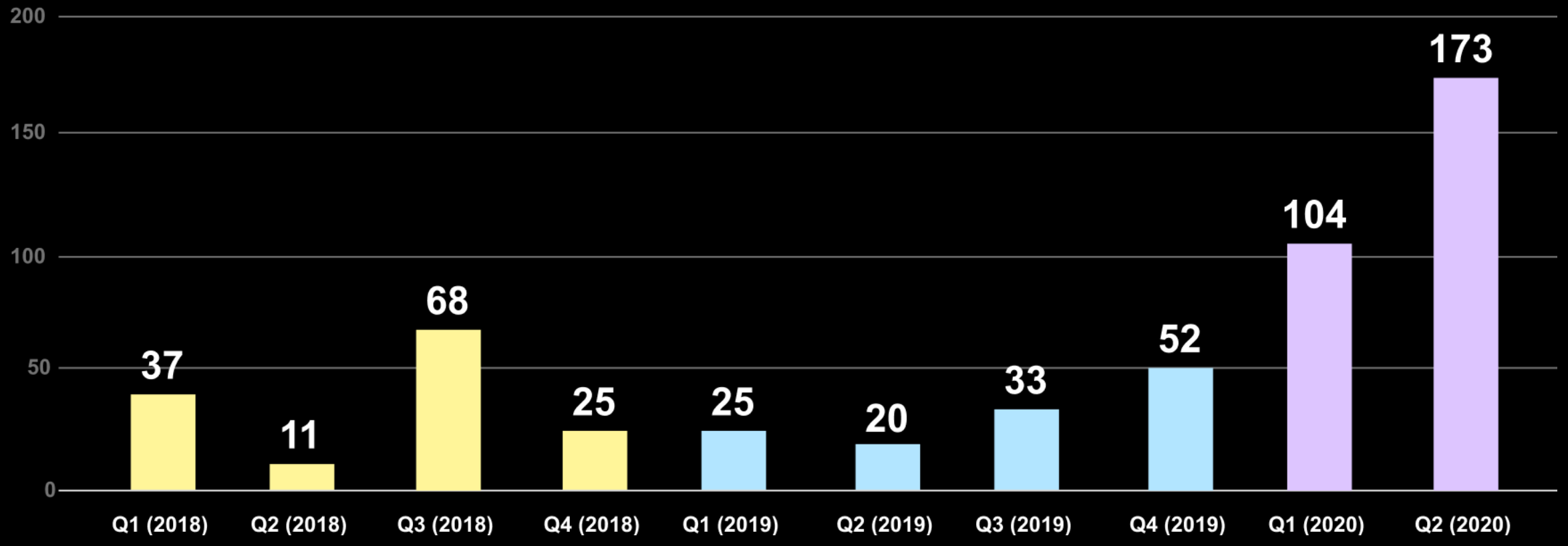
Расчетная сумма минимального ущерба по открытым данным от 17 семейств шифровальщиков.

2,5% ИНЦИДЕНТОВ СТАНОВЯТСЯ ПУБЛИЧНЫМИ

Trickbot успешно зашифровали более 2500 разных сетей, используя Ryuk, Kraken, Thanos. 62 известных инцидента — это лишь 2,5% от общего числа.

РОСТ РЫНКА ПРОДАЖИ ДОСТУПОВ К КОРПОРАТИВНЫМ СЕТЯМ

В 4 раза вырос рынок продаж доступов
в корпоративные сети за 1 год



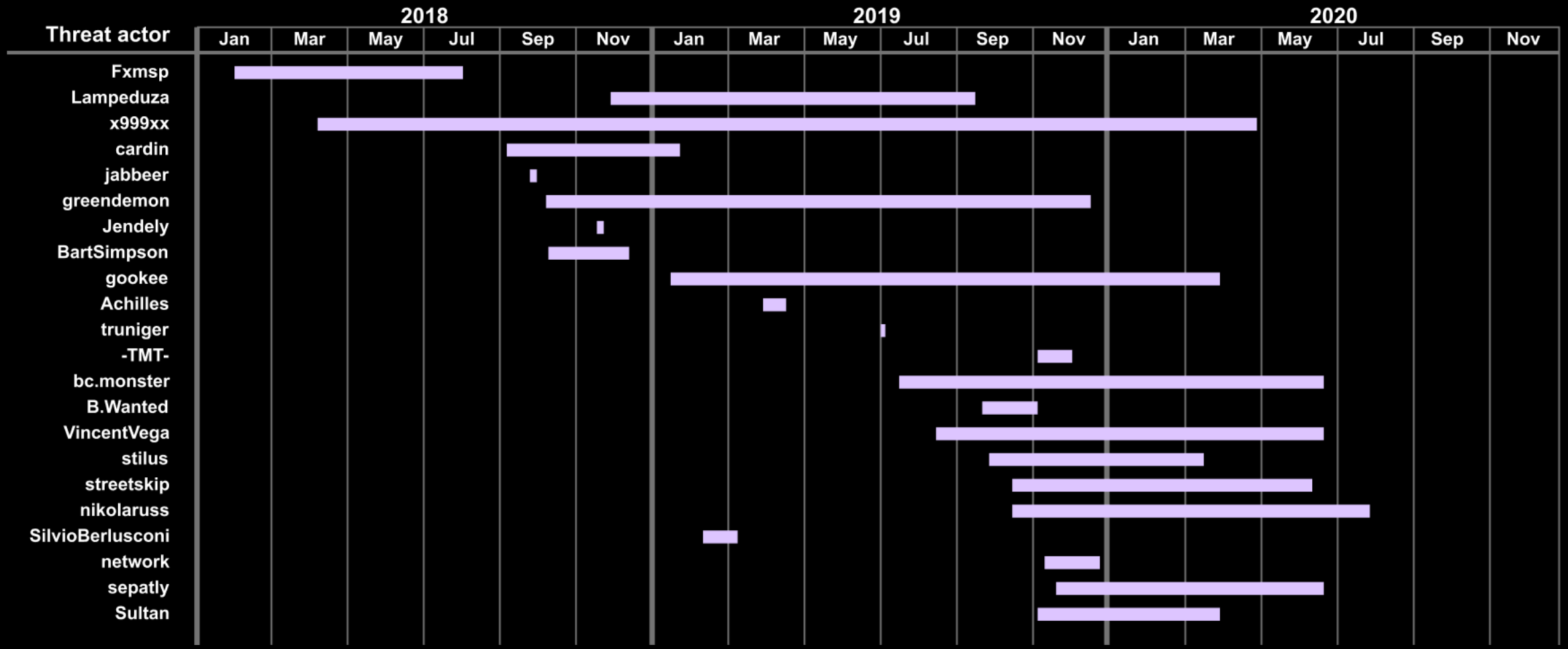
РОСТ РЫНКА ПРОДАЖИ ДОСТУПОВ К КОРПОРАТИВНЫМ СЕТЯМ

1	В 2,6 РАЗА ВЫРОСЛО КОЛИЧЕСТВО ПРОДАЖ
2	277 ПРОДАННЫХ ДОСТУПОВ ТОЛЬКО В H1 2020
3	$1,6 МЛН — СУММАРНАЯ СТОИМОСТЬ ДОСТУПОВ В ПРОШЛОМ ГОДУ
4	$6,1 МЛН — СУММАРНАЯ СТОИМОСТЬ ДОСТУПОВ В ЭТОМ ГОДУ

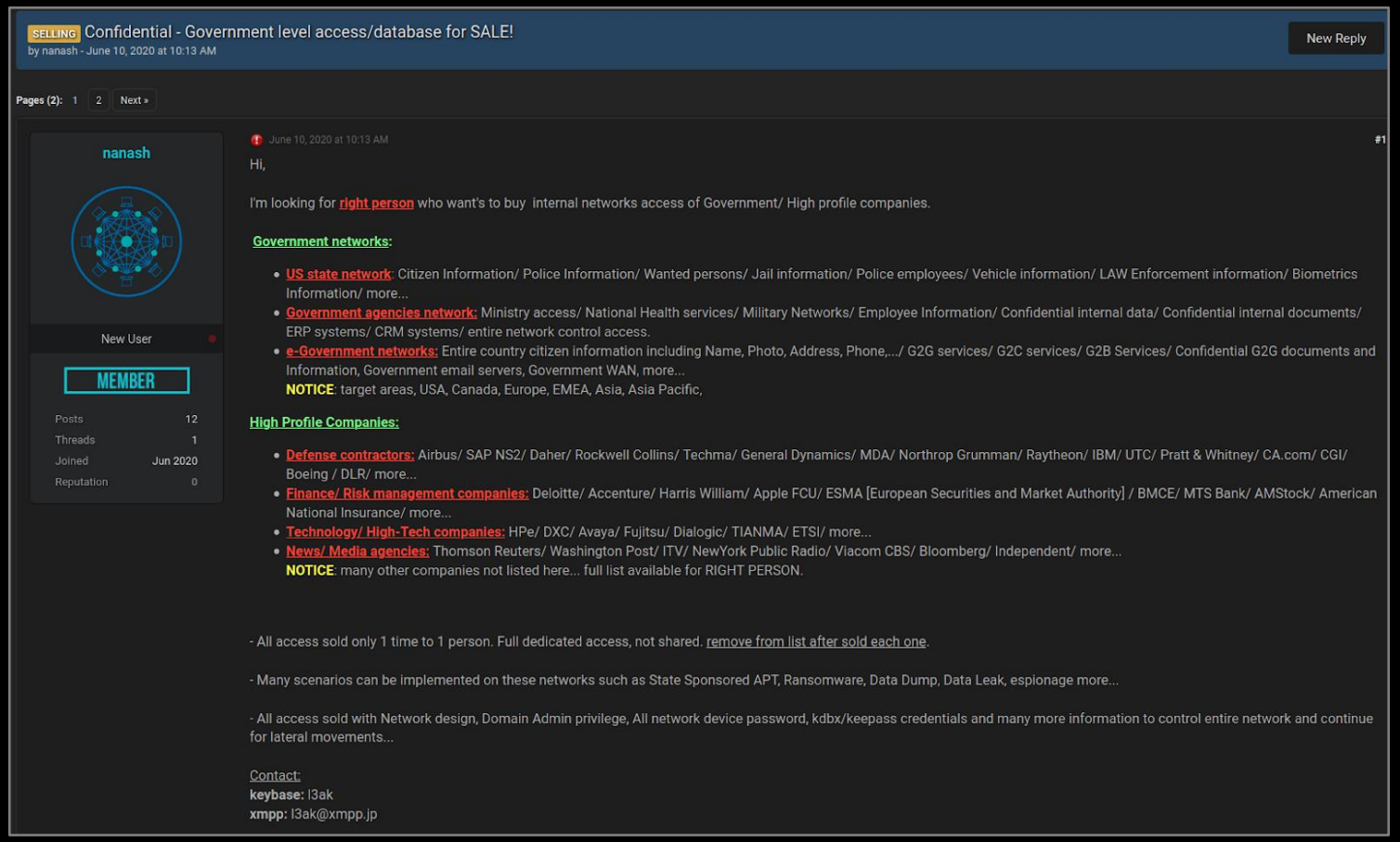
РОСТ РЫНКА ПРОДАЖИ ДОСТУПОВ К КОРПОРАТИВНЫМ СЕТЯМ

1	В 2018-М БЫЛО АКТИВНО 37 ПРОДАВЦОВ
2	В 2020-М ТОЛЬКО В ПЕРВОЙ ПОЛОВИНЕ ГОДА АКТИВНЫМИ БЫЛИ 63 ПРОДАВЦА
3	52 ИЗ 63 ПРОДАВЦОВ НАЧАЛИ СВОЮ АКТИВНОСТЬ В 2020 ГОДУ

РОСТ РЫНКА ПРОДАЖИ ДОСТУПОВ К КОРПОРАТИВНЫМ СЕТЯМ



РОСТ РЫНКА ПРОДАЖИ ДОСТУПОВ ХАКЕРАМИ, СПОНСИРУЕМЫМИ ГОСУДАСРТВАМИ



SELLING Confidential - Government level access/database for SALE!
by nanash - June 10, 2020 at 10:13 AM

New Reply

Pages (2): 1 2 Next »

nanash

New User

MEMBER

Posts	12
Threads	1
Joined	Jun 2020
Reputation	0

June 10, 2020 at 10:13 AM #1

Hi,

I'm looking for right person who want's to buy internal networks access of Government/ High profile companies.

Government networks:

- **US state network**: Citizen Information/ Police Information/ Wanted persons/ Jail information/ Police employees/ Vehicle information/ LAW Enforcement information/ Biometrics Information/ more...
- **Government agencies network:** Ministry access/ National Health services/ Military Networks/ Employee Information/ Confidential internal data/ Confidential internal documents/ ERP systems/ CRM systems/ entire network control access.
- **e-Government networks:** Entire country citizen information including Name, Photo, Address, Phone,.../ G2G services/ G2C services/ G2B Services/ Confidential G2G documents and Information, Government email servers, Government WAN, more...
  NOTICE: target areas, USA, Canada, Europe, EMEA, Asia, Asia Pacific,

High Profile Companies:

- **Defense contractors:** Airbus/ SAP NS2/ Daher/ Rockwell Collins/ Techma/ General Dynamics/ MDA/ Northrop Grumman/ Raytheon/ IBM/ UTC/ Pratt & Whitney/ CA.com/ CGI/ Boeing / DLR/ more...
- **Finance/ Risk management companies:** Deloitte/ Accenture/ Harris William/ Apple FCU/ ESMA [European Securities and Market Authority] / BMCE/ MTS Bank/ AMStock/ American National Insurance/ more...
- **Technology/ High-Tech companies:** HPe/ DXC/ Avaya/ Fujitsu/ Dialogic/ TIANMA/ ETSI/ more...
- **News/ Media agencies:** Thomson Reuters/ Washington Post/ ITV/ NewYork Public Radio/ Viacom CBS/ Bloomberg/ Independent/ more...
  NOTICE: many other companies not listed here... full list available for RIGHT PERSON.

- All access sold only 1 time to 1 person. Full dedicated access, not shared. remove from list after sold each one.

- Many scenarios can be implemented on these networks such as State Sponsored APT, Ransomware, Data Dump, Data Leak, espionage more...

- All access sold with Network design, Domain Admin privilege, All network device password, kdbx/keepass credentials and many more information to control entire network and continue for lateral movements...

Contact:
keybase: l3ak
xmpp: l3ak@xmpp.jp

РОСТ РЫНКА ПРОДАЖИ ДОСТУПОВ ХАКЕРАМИ, СПОНСИРУЕМЫМИ ГОСУДАСРТВАМИ

11 BTC

$125 000 — ДОСТУП
В КАЖДУЮ КОМПАНИЮ

$5 млн

СУММАРНАЯ СТОИМОСТЬ ДОСТУПОВ
ТОЛЬКО В НАЗВАННЫЕ КОМПАНИИ

БЕЗОПАСНОСТЬ ВНЕШНЕГО ПЕРИМЕТРА ВЫРОСЛА КАК НИКОГДА

10

ГРУПП ИСПОЛЬЗУЮТ ПЕРЕБОР ПАРОЛЕЙ К RDP

3

ГРУППЫ ЭКСПЛУАТИРУЮТ УЯЗВИМОСТИ В VPN

5

НАИБОЛЕЕ ЧАСТО ИСПОЛЬЗУЕМЫХ СЕТЕВЫХ УЯЗВИМОСТЕЙ:

- CVE-2019-19781 (Citrix)
- CVE-2019-11510 (Pulse Secure)
- CVE-2018-13379 (FortiGate)
- CVE-2019-9670 (Zimbra)
- CVE-2019-10149 (Exim)

ВОЗРОСШАЯ АКТИВНОСТЬ POST EXPLOITATION ФРЕЙМВОРКОВ

На 67% выросло количество активных серверов
Post exploitation фреймворками за 1 год

Атакующий		Cobalt Strike	Metasploit	Covenant	CrackMapExec	PoshC2	Koadic
Ransomware	Ryuk	+	+				
	REvil		+		+		
	MegaCortex	+					
	Maze	+					
	DoppelPaymer					+	+
	Clop	+	+				
	Lockbit				+		
Cybercrime	Cobalt	+					
	Silence		+				
	Fxmsp		+				
	FIN6	+	+				
APT	Lazarus	+					
	OilRig	+	+	+			
	APT41	+	+				
	APT32	+					
	Gamaredon		+				
	Chimera	+					
	Mustang Panda	+					
	Chafer		+				

ВОЗРОСШАЯ АКТИВНОСТЬ POST EXPLOITATION ФРЕЙМВОРКОВ

6 тыс.

СЕРВЕРОВ С АКТИВНЫМИ ФРЕЙМВОРКАМИ БЫЛО В H2 2018 — H1 2019

10 тыс.

СЕРВЕРОВ С АКТИВНЫМИ ФРЕЙМВОРКАМИ БЫЛО В H2 2019 — H1 2020

ПРОГНОЗЫ

ТОРГОВЫЕ ПЛОЩАДКИ

Специализированные площадки для выкладывания информации и проведения аукционов сократят издержки атакующих.

LINUX-БЭКДОРЫ

Необходимость во вредоносном коде для Linux резко возрастает при первоначальном доступе и при Lateral movement.
Часто на Linux-системах службы безопасности слепы.

IOT — ТОЧКА КОМПРОМЕТАЦИИ

Владельцы IoT-ботнетов могут начать продавать доступ к устройствам, которые установлены в корпоративных сетях.

СТАБИЛИЗАЦИЯ РЫНКА В 2020-М

Рынок насытится, и количество вымогательских партнерских программ замедлится.

ПОЧТА — ЦЕЛЬ ВЫМОГАТЕЛЕЙ

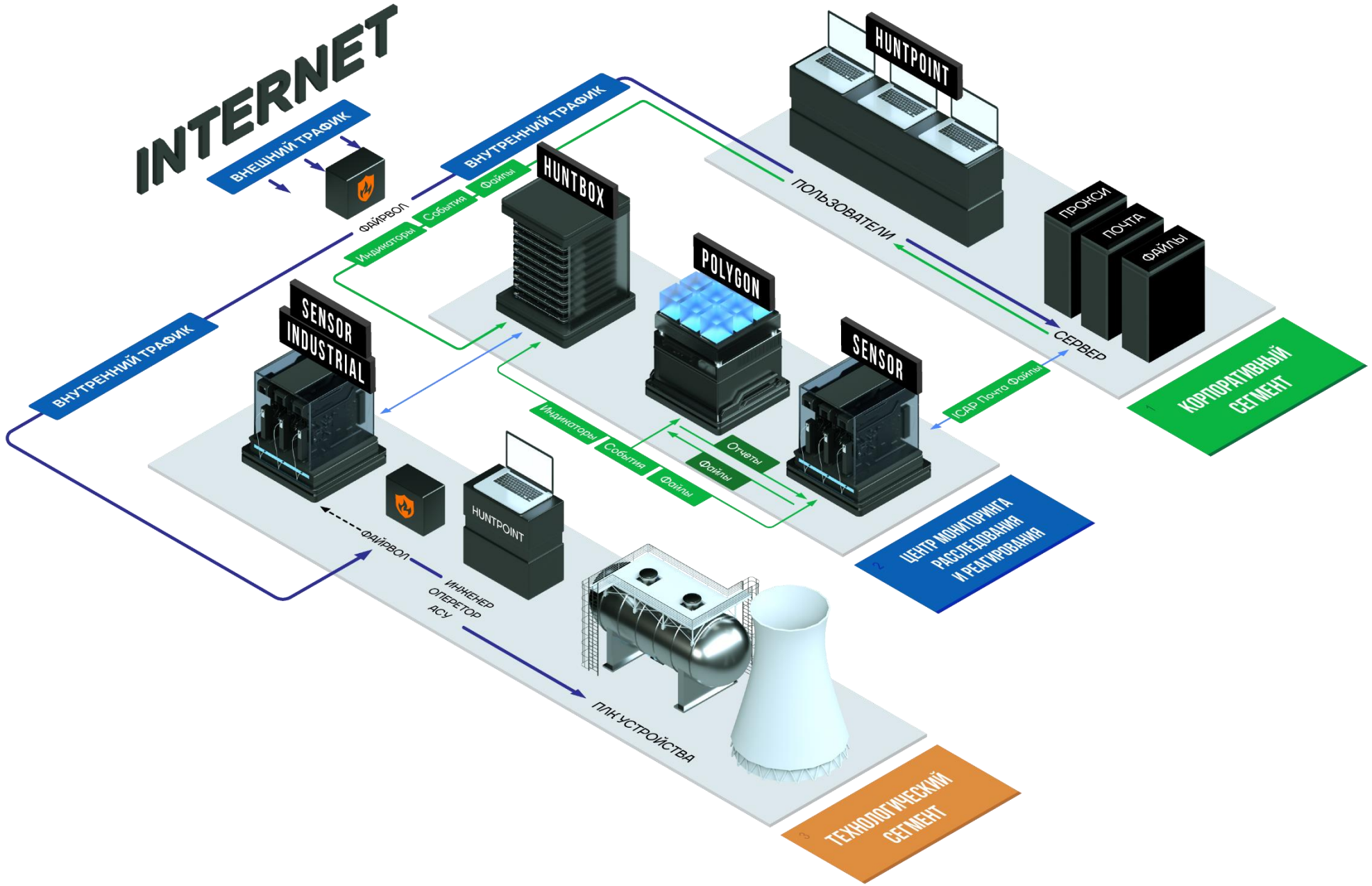
Целенаправленные похищения данных локальных почтовых серверов.

АТАКИ СПЕЦСЛУЖБ И ПРИНУЖДЕНИЕ ВЛАДЕЛЬЦЕВ ПАРТНЕРОК

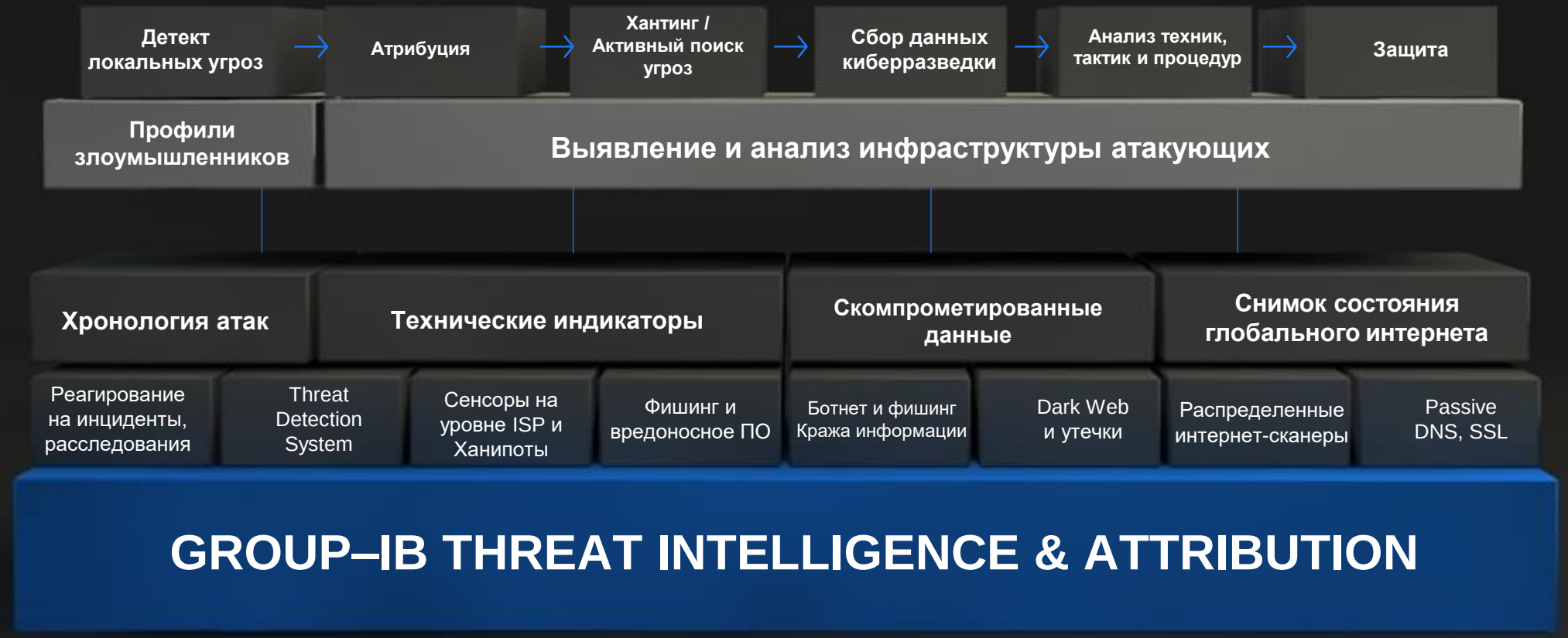
Спецслужбы могут заинтересоваться владельцами партнерских программ, чтобы использовать их для доступа к интересующим сетям.

Комплексный подход Group-IB

Комплексный подход


INTERNET
ВНЕШНИЙ ТРАФИК
ФАЙРВОЛ
ВНУТРЕННИЙ ТРАФИК
Файлы
События
Индикаторы
HUNTBOX
HUNTPOINT
ПОЛЬЗОВАТЕЛИ
ПРОКСИ
ПОЧТА
ФАЙЛЫ
СЕРВЕР
POLYGON
SENSOR INDUSTRIAL
SENSOR
ICAP Почта Файлы
Отчеты
Файлы
События
Индикаторы
ВНУТРЕННИЙ ТРАФИК
КОРПОРАТИВНЫЙ СЕГМЕНТ
ЦЕНТР МОНИТОРИНГА РАССЛЕДОВАНИЯ И РЕАГИРОВАНИЯ
ФАЙРВОЛ
HUNTPOINT
ИНЖЕНЕР ОПЕРАТОР АСУ
ПЛК УСТРОЙСТВА
ТЕХНОЛОГИЧЕСКИЙ СЕГМЕНТ

Архитектура Threat Intelligence & Attribution



Архитектура Group-IB Fraud Hunting Platform

GROUP-IB FRAUD HUNTING PLATFORM

Web Snippet

Сбор информации о поведении пользователя и окружении, в котром работает веб-приложение

Mobile SDK

Сбор информации о поведении пользователя и окружении, в котром работает мобильное приложение

Processing Hub

Корреляция и анализ данных о поведении и окружении

Preventive Proxy

Выявление и блокирование бот-активности

Услуги по аналитике и реагированию

- Мониторинг событий
- Управление инцидентами
- Аналитика по запросу
- Создание антифрод-правил
- Разбор критичных угроз

Расследование инцидентов

Использование данных Group-IB Fraud Hunting Platform для идентификации и поиска мошенников и их инфраструктуры

Облачное решение

Гибкая и быстрая интеграция с облачной инфраструктурой в стране заказчика

или

Автономное решение

Для хранения всей информации в периметре заказчика

или

Гибридное решение

Смешанная реализация в соответствии с индивидуальными требованиями заказчика

Profit
Security Day

БЛАГОДАРЮ ЗА ВНИМАНИЕ!

Контакты представителя в Казахстане:

Вячеслав Нозиков,

Менеджер по развитию бизнеса Group-IB, MONT

+7 (727) 355 60 05 (вн. 150)

vnozikov@mont.com