КИБЕРУГРОЗЫ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ 2.0

Новый взгляд на защиту промышленных компаний

GROUP-IB

450+

Enterprise customers around the World

1,200+

Successful Investigations of HI-tech Cybercrime Cases

65,000+

Hours of Hands-on Incident Response

500+

Employees Worldwide

Recognized by Top Industry Experts

FORRESTER®

IDC Analyze the Future

Gartner®

Official Partner

EUROPOL EUROPEAN LAW ENFORCEMENT AGENCY

INTERPOL

Recommended by

OSCE

SWIFT

Some of Our High-end Clients

Deutsche Bank

UNIQLO

Commonwealth Bank

Raiffeisen BANK

SONY PICTURES

ИСТОРИЯ GROUP-IB

О нас говорят

theguardian Bloomberg Forbes REUTERS Esquire

The Washington Post CNN The Register Biting the hand that feeds IT InformationWeek DARKReading SC MAGAZINE

КТО АТАКУЕТ ТЕХНОЛОГИЧЕСКИЕ СЕТИ

Спецслужбы

Мотивация:
шпионаж и саботаж

Активность: 2005 – н.в.

Особенность: обнаруживаются только после нанесения ущерба

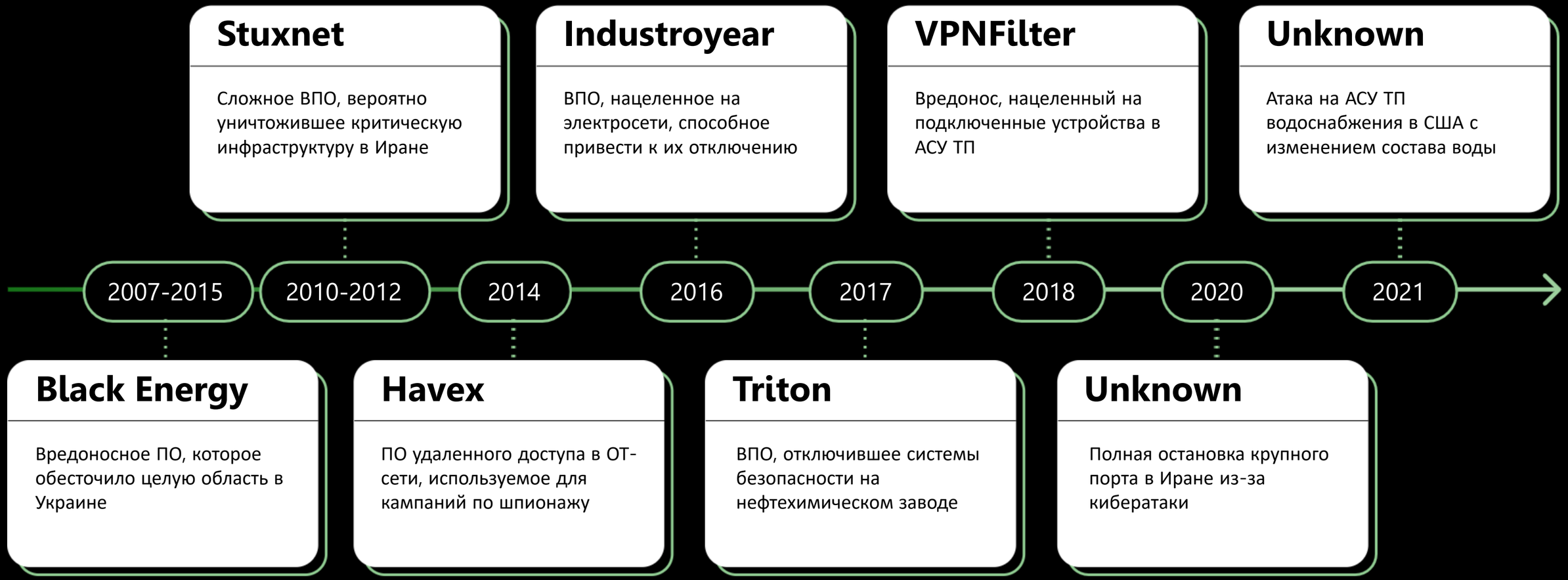
Криминал

Мотивация:
шпионаж и саботаж

Активность: 2019 – н.в.

Особенность:
обнаруживаются только после нанесения ущерба

ЭВОЛЮЦИЯ ВПО: 2007 – Н.В.



2019 – 2020

Атака на ГЭС Венесуэлы

Успешная атака на ГЭС Гури, которая привела к массовым отключениям энергии в Каракасе и 22 штатах страны из 23. Без электричества на протяжении нескольких дней оставалась большая часть страны.

Инструменты атакующих не установлены!

Март 2019

Атака на Израильские объекты водоснабжения и канализации

Управление водных ресурсов подтвердили факт атаки. Водоснабжение не пострадало и оно работало и продолжает работать без перебоев. Всех сотрудников отвечающих за хлорирование скважин попросили изменить пароли и защитить системы

Инструменты атакующих не установлены!

Апрель 2020

Атака на Иранский порт Шахид Раджаи

9 мая грузопотоки в иранском портовом терминале Шахид Раджаи внезапно остановился. Компьютеры, которые регулируют поток судов, грузовиков и товаров, все сразу вышли из строя, создавая огромные заторы на водных путях и дорогах, ведущих к объекту.Через день иранские официальные лица признали, что порт был остановлен в результате кибератаки.

Инструменты атакующих не установлены!

Май 2020

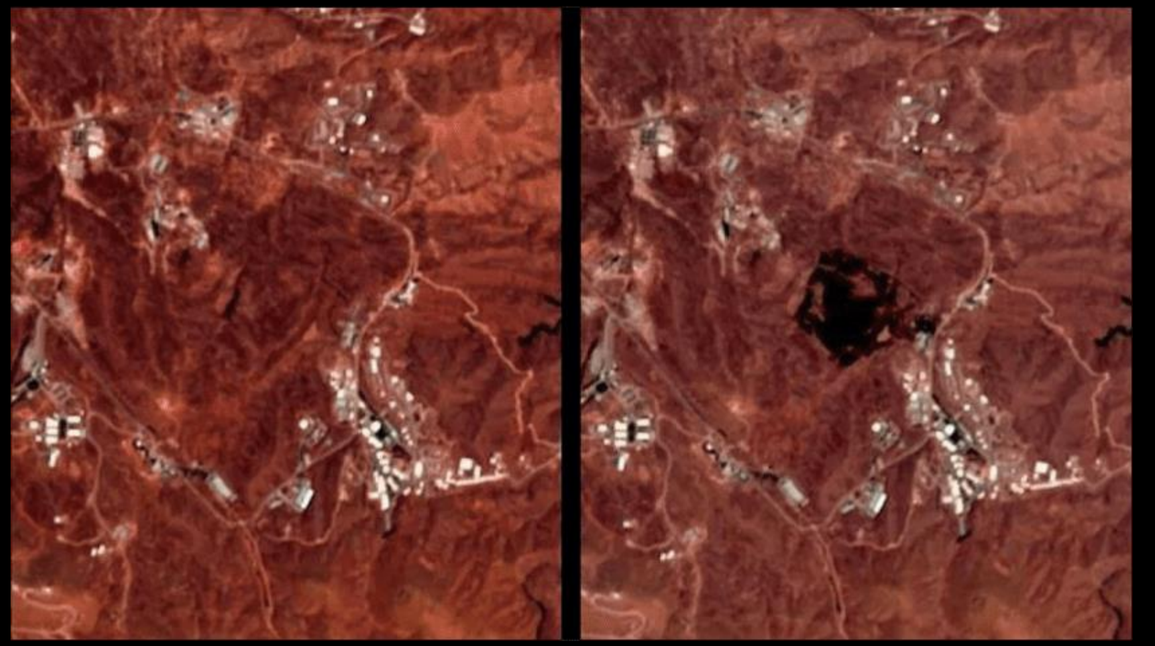
2019 - 2020

Атака на Иранский ракетный завод

Shahid Hemat Industrial Group (SHIG) – подразделение Иранской организации аэрокосмической промышленности (AIO), ответственный за иранскую программу баллистических ракет на жидком топливе. Взрыв бензобака возле военной базы в Тегеране был результатом израильской кибератаки.

Инструменты атакующих не установлены!

Июнь 2020



2.0

ЧТО ОБЩЕГО
У ЭТИХ КОМПАНИЙ?

CANADA

GROUP-IB

BOMBARDIER

Самолеты

BRAZIL

GROUP-IB

JBS

Мясо

SWITZERLAND

GROUP-IB

GARMIN

Спутниковая навигация

US

COLLONIAL PIPELINE

Нефтепроводы

RUSSIA

GROUP-IB

100+ больших, средних и малых компаний, пожелавших остаться неизвестными

Неизвестно

Карта союзов:

кооперация операторов шифровальщиков
и распространителей вредоносных программ в 2020 году

TRICKBOT	QAKBOT	DRIDEX	SDBBOT
Ryuk **Conti** **REvil** **RansomExx**	**ProLock** **Egregor** **DoppelPaymer**	**DoppelPaymer**	**ClOp**

ZLOADER	ICEDID	BUER	BAZAR
Ryuk **Egregor**	**RansomExx** **Maze** **Egregor**	**Maze** **Ryuk**	**Ryuk**

Источник: “Программы-вымогатели 2020-2021”, Group-IB, 2021

Программы-вымогатели 2020/2021
Обзор тактик, техник и процедур (TTPs) операторов вымогателей по матрице MITRE ATT&CK®

2.0 = атакует кто попало

Что печальней всего,
в большинстве случаев все начинается с очень простых вещей

Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Operating Mode	Modify Program	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Engineering Workstation Compromise	Execution through API	Project File Infection		Indicator Removal on Host	Remote System Discovery	Lateral Tool Transfer	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
Exploit Public-Facing Application	Graphical User Interface	System Firmware		Masquerading	Remote System Information Discovery	Program Download	I/O Image		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Exploitation of Remote Services	Hooking	Valid Accounts		Rootkit	Wireless Sniffing	Remote Services	Man in the Middle		Block Serial COM	Unauthorized Command Message	Loss of Control
External Remote Services	Modify Controller Tasking			Spoof Reporting Message		Valid Accounts	Monitor Process State		Data Destruction		Loss of Productivity and Revenue
Internet Accessible Device	Native API						Point & Tag Identification		Denial of Service		Loss of Protection
Remote Services	Scripting						Program Upload		Device Restart/Shutdown		Loss of Safety
Replication Through Removable Media	User Execution						Screen Capture		Manipulate I/O Image		Loss of View
Rogue Master							Wireless Sniffing		Modify Alarm Settings		Manipulation of Control
Spearphishing Attachment									Rootkit		Manipulation of View
Supply Chain Compromise									Service Stop		Theft of Operational Information
Wireless Compromise									System Firmware		

Drive-by Compromise

External Remote Services

Spearphishing Attachment

Purchase Servers

Search

United States | New York | Choose a City... | ZIP

Choose Provider... | Choose an OS...

Direct IP: ON | Admin Privilege: ON | No PayPal: OFF | Port 25: OFF | Port 80: OFF | Show VM: ON | Show Reselling: ON

Request a server | Search

IP	COUNTRY	REGION, STATE	CITY	OS	RAM	DOWN	UPL.	DIRECT IP	ADMIN PRIVILEGE	LAST CHECK	SELLER	PRICE, $
96.8... [Full Info]	US	New York	Buffalo	Server 2012 R2	1023 MB	46.55 Mbit/s	7.54 Mbit/s	√	√	30.08.2018	selez	19.25
23.94... [Full Info]	US	New York	Buffalo	Server 2012 R2	1023 MB	101.48 Mbit/s	21.06 Mbit/s	√	√	24.08.2018	selez	31.75

DE 46.16...

Schleswig-holste..., Tangstedt | ZIP: *22889*

[redacted]

Checked	Uptime
13.06.2016	25 Days

10.00$

Windows 7 | x64 | DE

Intel(R) Core(TM) i5-4670 CPU @ 3.40...

Ram: ***3.86 GB*** | *CPU Cores:* ***4***

6.7 Mbit/s *3.63 Mbit/s*

Check IP-Score (0.20$)

Admin Privilege: *Yes*

Direct IP: *No*

Antivirus: *Unknown*

Browsers:

Blacklist: **1** / 178

Opened Ports: 80, 25

Virtual: *No*

Payment Systems

1. *paypal.com*

Poker Systems

Not Found.

Internet Shops

1. *amazon.com*
2. *ebay.com*
3. *target.com*

Dating Sites

1. *meetic.com*

FXMSP: НЕВИДИМЫЙ БОГ СЕТИ

Исследование эволюции одного из самых известных продавцов доступа к корпоративным сетям на андерграундных форумах, который атаковал более 130 компаний из разных отраслей по всему миру. В 2018 году пользователь андеграундного форума с ником Lampeduza опубликовал пост, рекламирующий услуги по взлому корпоративных сетей и продаже доступа к ним. В посте он писал: "...У вас будет полный доступ ко всей сети компании. Вы станете невидимым богом сети". Как удалось установить, Lampeduza работал в паре с Fxmsp в качестве менеджера по продажам. Несмотря на прекращение публичной активности в 2019, Fxmsp остается на свободе и продолжает представлять угрозу.

АТАКИ КРИМИНАЛА НА ПРОМЫШЛЕННЫЕ ПРЕДПРИЯТИЯ

RANSOMWARE | THREAT ANALYSIS

Honda and Enel impacted by cyber attack suspected to be ransomware

~~Lampeduza~~
megabyte
●●●

~~BANNED~~
0
98 posts
Joined

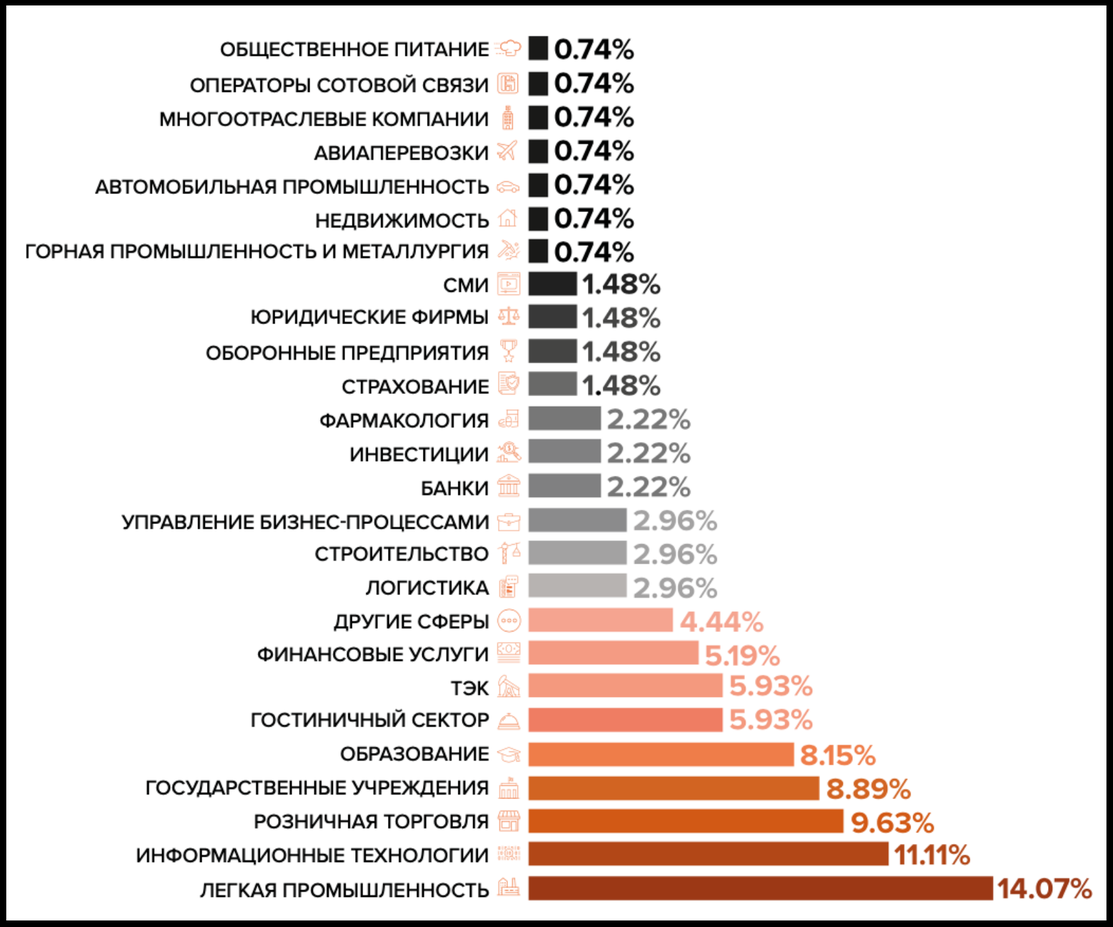
Posted September 12, 2018 (edited) Report post

доступ к банку в Нигерии ATM - 25к

компания californiaoliveranch.com около 1000 ПК, там есть шоп внутри цена 5 к
dizucar.com (около 500-900 пк и сер)- 4к
https://www.enel.com - 10к

Edited September 12, 2018 by Lampeduza

+ Quote



EKANS/SNAKE – СПИСОК УБИВАЕМЫХ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ

Process	Description
bluestripecollector.exe	BlueStripe Data Collector
ccflic0.exe	Proficy Licensing
ccflic4.exe	Proficy Licensing
collwrap.exe	BlueStripe Data Collector
fnplicensingservice.exe	FLEXNet Licensing Service
hasplmv.exe	Sentinel Hasp License Manager
hdb.exe	Honeywell HMIWeb
ilicensesvc.exe	GE Fanuc Licensing
pralarmmgr.exe	Proficy Related
prcalculationmgr.exe	Proficy Historian Data Calculation Service
prconfigmgr.exe	Proficy Related
prdatabasemgr.exe	Proficy Related
premailengine.exe	Proficy Related
preventmgr.exe	Proficy Related
prftpengine.exe	Proficy Related
prgateway.exe	Proficy Secure Gateway

Process	Description
prlicensemgr.exe	Proficy License Server Manager
proficy administrator.exe	Proficy Related
proficyclient.exe	Proficy Related
proficypublisherservice.exe	Proficy Related
proficyserver.exe	Proficy Server
proficysts.exe	Proficy Related
prprintserver.exe	Proficy Related
prproficymgr.exe	Proficy Plant Applications
prrds.exe	Proficy Remote Data Service
prreader.exe	Proficy Historian Data Calculation Service
prrouter.exe	Proficy Related
prschedulemgr.exe	Proficy Related
prstubber.exe	Proficy Related
prsummarymgr.exe	Proficy Related
prwriter.exe	Proficy Historian Data Calculation Service
prlicensemgr.exe	Proficy License Server Manager

DARKSIDE

GROUP-IB

Initial Compromise

- Suspected password attacks on perimeter infrastructure
- CVE-2021-20016
- Malicious emails with links

Establish Foothold

- BEACON
- SMOKEDHAM
- F-Secure C3

Escalate Privileges

- CVE-2020-1472
- Mimikatz
- LSASS process memory dumps

Internal Reconnaissance

- PowerView
- Built-in Windows utilities
- BLOODHOUND
- Advanced IP Scanner

Complete Mission

- Data exfiltration via rclone or WinSCP
- Data theft extortion
- DARKSIDE ransomware deployment (generally via PsExec)

Maintain Presence

- TeamViewer
- Legitimate Credentials

Move Laterally

- BEACON
- RDP
- plink
- F-Secure

1

Refresh

INFO

Company: 1

Description: 1

FILES

Linux

Windows

Show builds

PAYMENT INFO

$ [redacted]

Paid: $ 0

Pending: $ 0

Remaining to pay

[redacted] BTC (+20%) Rate: $ [redacted]

[redacted] XMR Rate: $ [redacted]

Fixed rate:

Enable BTC:

Enable XMR:

Not paid

Transactions [0]

BOTS STATISTIC

0	0 (0%)	0	0 GB	0	0
Bots	With reports	Summary files	Summary size	Windows	Linux

Search...

All

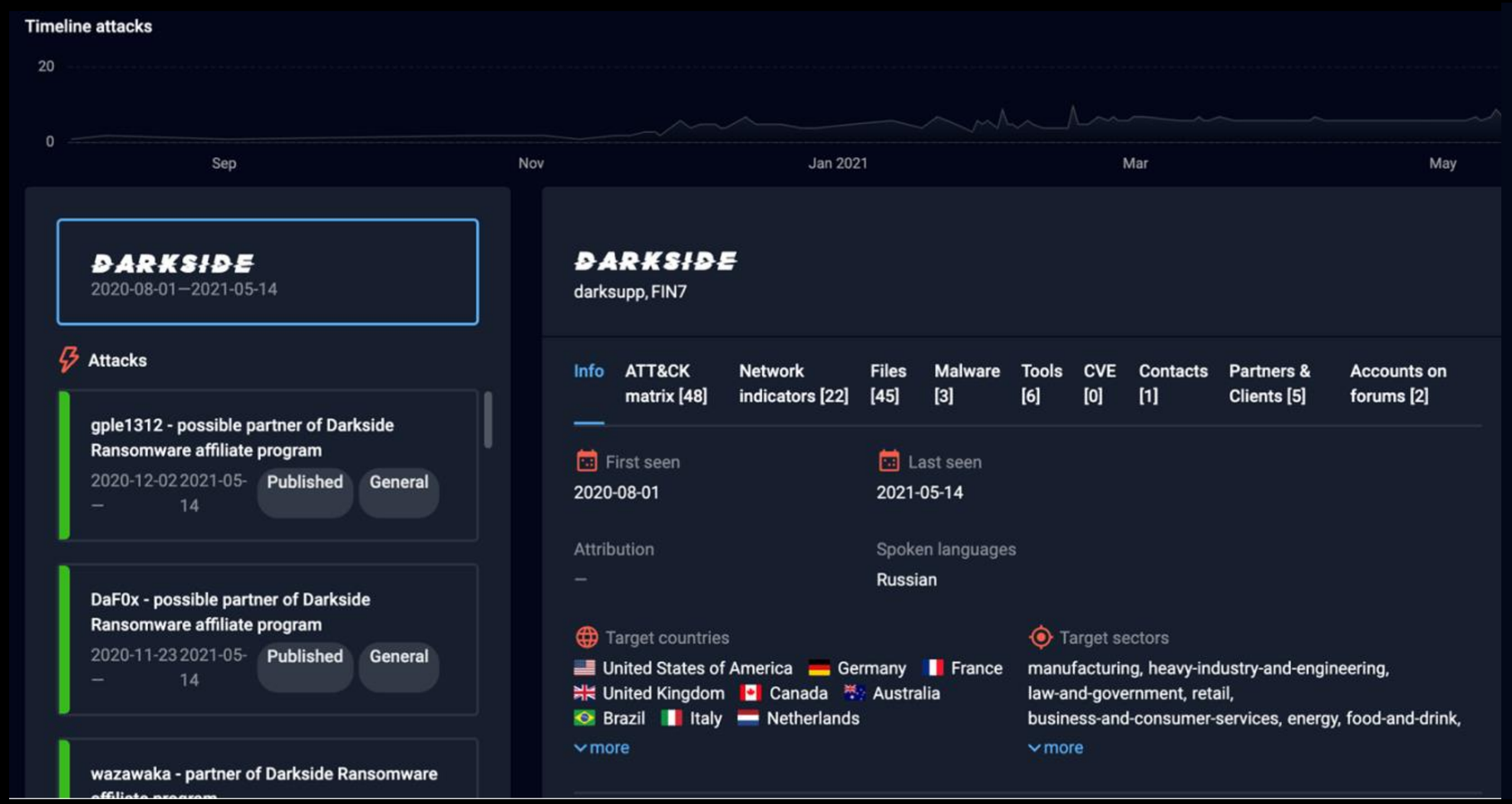
Bots not found

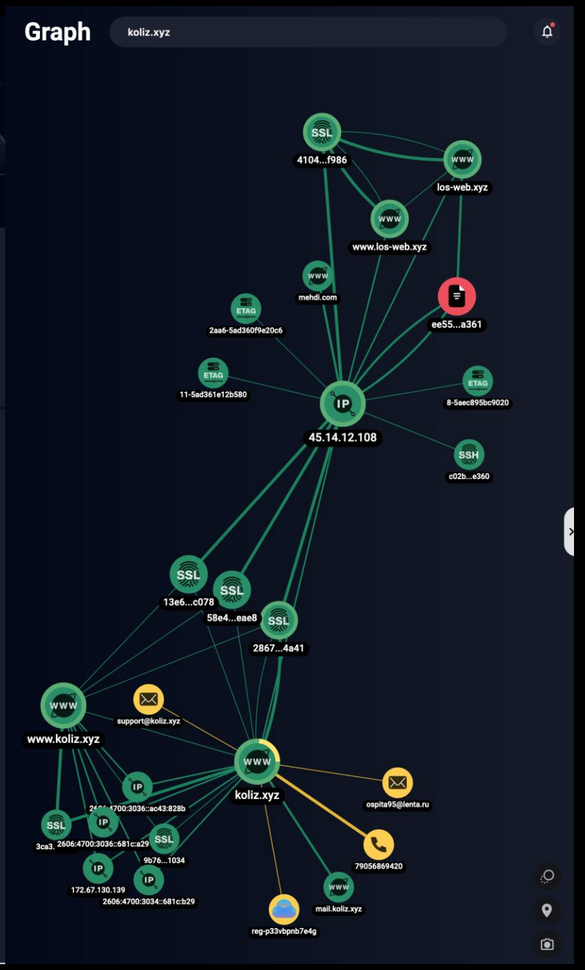
LANDING INFO

Discount price: 10 days , 00:00:00 (not launched)

User status: Offline

DARKSIDE

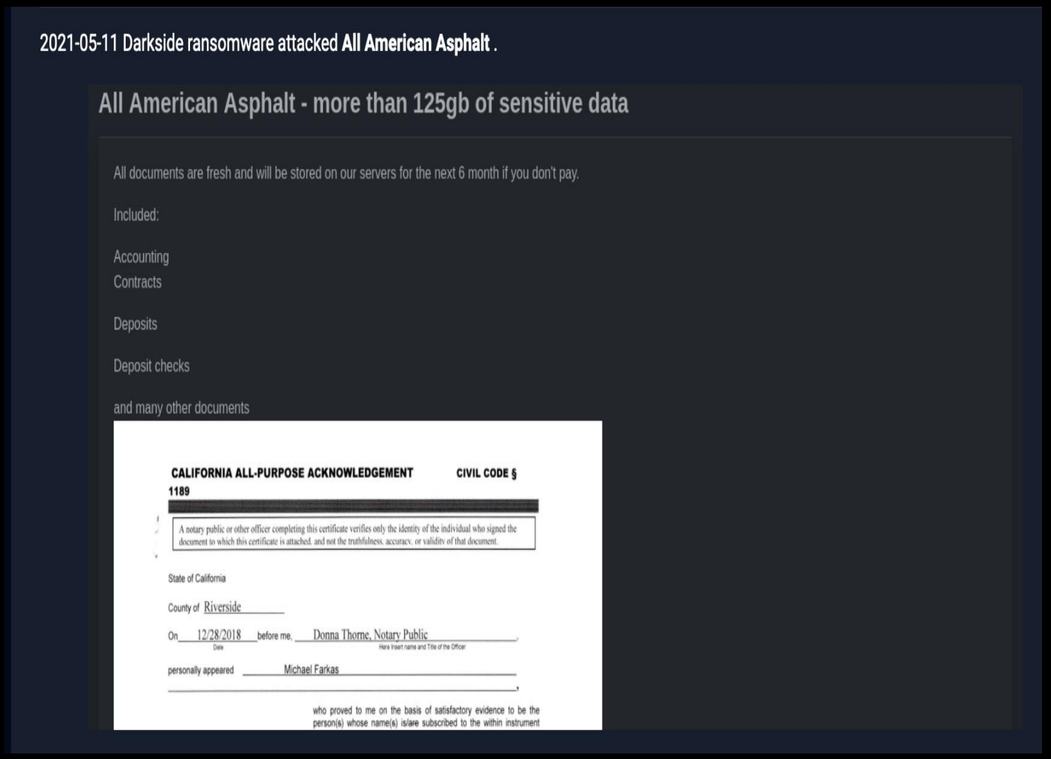

Timeline attacks
20
0
Sep
Nov
Jan 2021
Mar
May
DARKSIDE
2020-08-01—2021-05-14
Attacks
gple1312 - possible partner of Darkside Ransomware affiliate program
2020-12-02 — 2021-05-14
Published
General
DaF0x - possible partner of Darkside Ransomware affiliate program
2020-11-23 — 2021-05-14
Published
General
wazawaka - partner of Darkside Ransomware
DARKSIDE
darksupp, FIN7
Info
ATT&CK matrix [48]
Network indicators [22]
Files [45]
Malware [3]
Tools [6]
CVE [0]
Contacts [1]
Partners & Clients [5]
Accounts on forums [2]
First seen
2020-08-01
Last seen
2021-05-14
Attribution
—
Spoken languages
Russian
Target countries
United States of America
Germany
France
United Kingdom
Canada
Australia
Brazil
Italy
Netherlands
more
Target sectors
manufacturing, heavy-industry-and-engineering, law-and-government, retail, business-and-consumer-services, energy, food-and-drink,
more


Graph
koliz.xyz
SSL
4104...f986
www
los-web.xyz
www.los-web.xyz
www
mehdi.com
ETAG
2aa6-5ad360f9e20c6
ee55...a361
ETAG
11-5ad361e12b580
ETAG
8-5aec895bc9020
IP
45.14.12.108
SSH
c02b...e360
SSL
13e6...c078
SSL
58e4...eae8
SSL
2867...4a41
www
www.koliz.xyz
support@koliz.xyz
www
koliz.xyz
ospita95@lenta.ru
IP
2606:4700:3036::ac43:828b
SSL
3ca3...
IP
2606:4700:3036::681c:a29
SSL
9b76...1034
IP
172.67.130.139
IP
2606:4700:3034::681c:b29
79056869420
www
mail.koliz.xyz
reg-p33vbpnb7e4g

ALL AMERICAN ASPHALT

2021-05-11 Darkside ransomware attacked All American Asphalt.

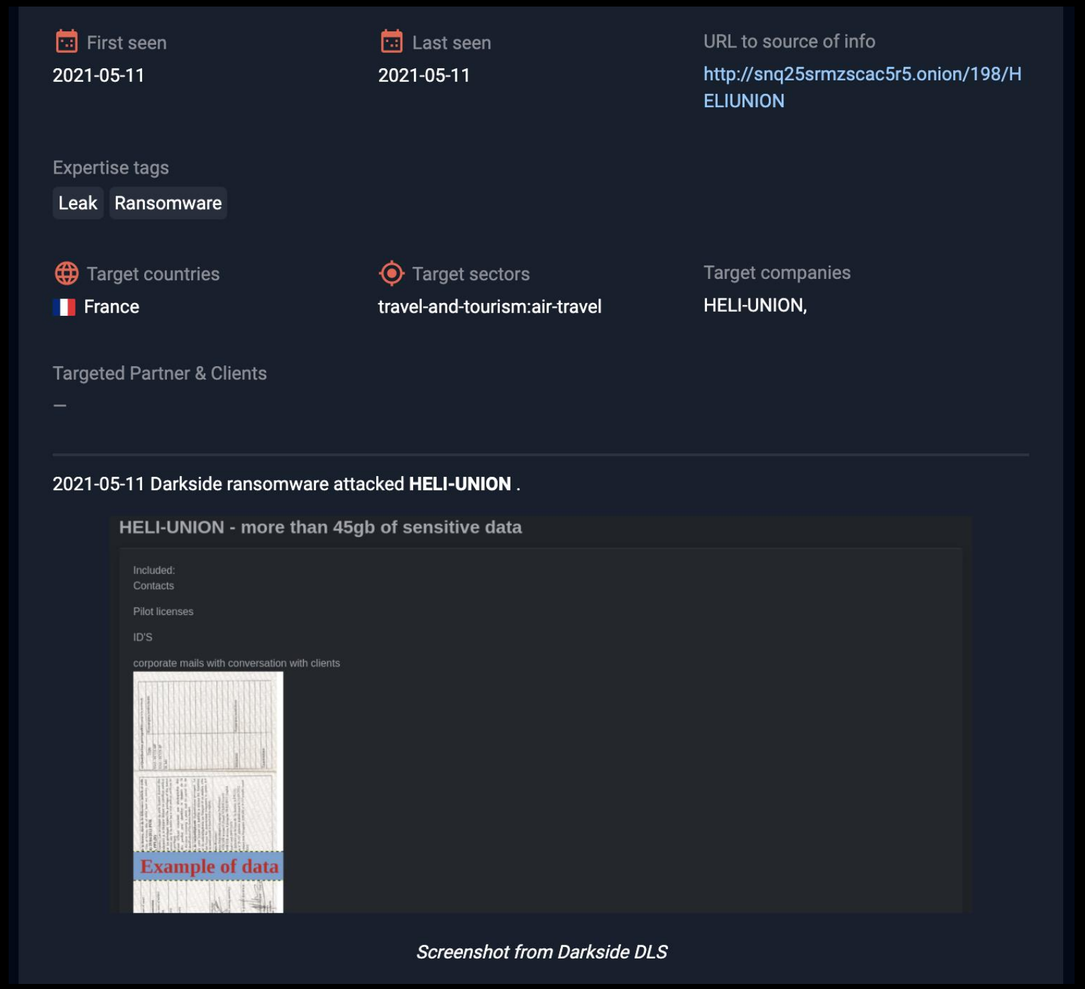
Производитель асфальта в Берлингтоне, штат Нью-Джерси. 12 заводов по производству.



125Гб чувствительных данных. АСУ ТП не пострадала

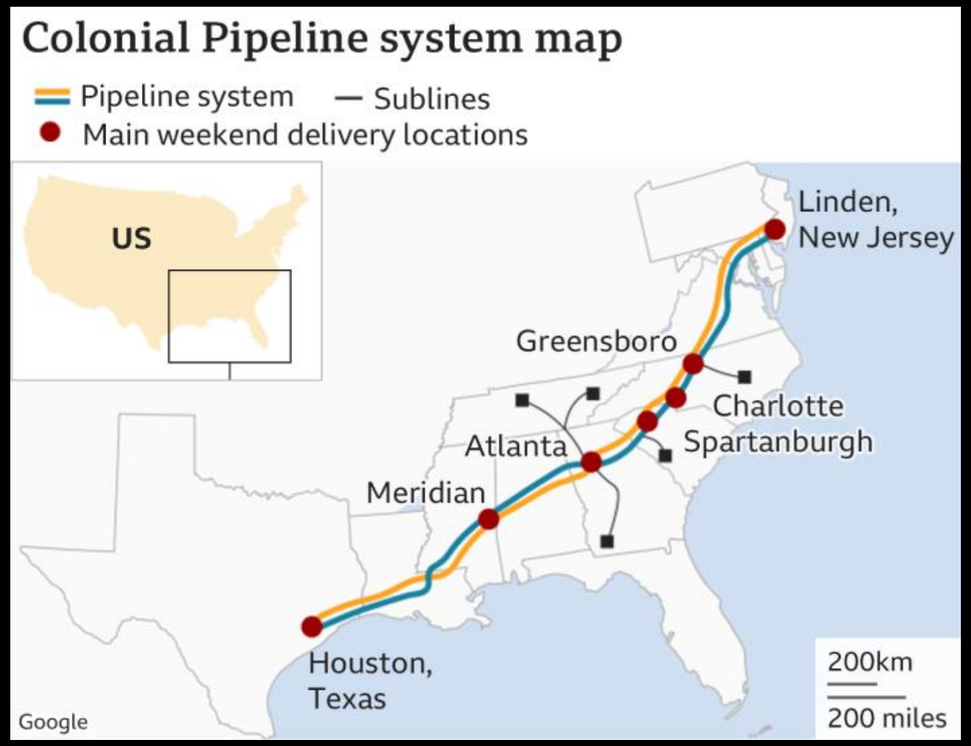
HELI-UNION

Компания Heli-Union предлагает услуги по техническую и оперативную поддержке гражданских и военных организаций, вертолетные операции, услуги по обучению пилотов и инженеров.



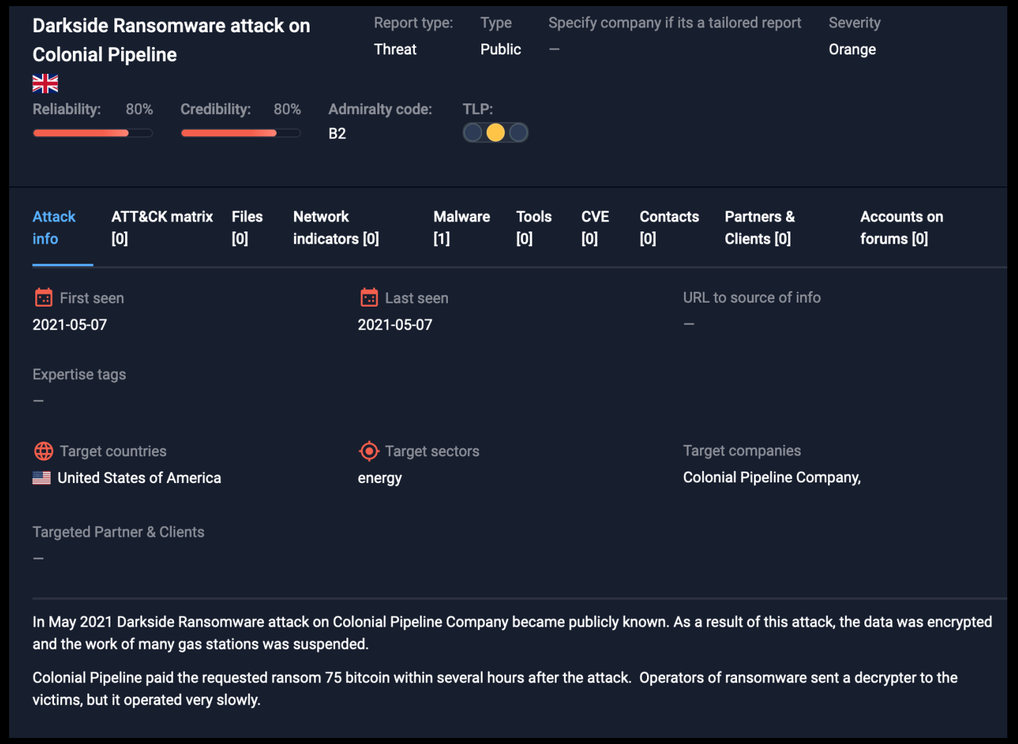
Screenshot from Darkside DLS

COLONIAL PIPELINE



По трубопроводу проходит 2,5 миллиона баррелей в день - 45% поставок дизельного топлива, бензина и авиакеросина на Восточное побережье.

Colonial Pipeline выплатила выкуп в размере 75 биткойнов в течение нескольких часов после атаки. Операторы вымогателей отправили жертвам дешифратор, но он работал очень медленно.



Группа перечисляет все типы украденных данных и отправляет жертвам URL-адрес «личной страницы утечки», где данные уже загружены и ожидают автоматической публикации. DarkSide также сообщает жертвам, что предоставит доказательства полученных данных и готов удалить их все из сети жертвы.

BRIEFING ROOM

Remarks by President Biden on the Colonial Pipeline Incident

MAY 13, 2021 • SPEECHES AND REMARKS

Roosevelt Room

12:27 P.M. EDT

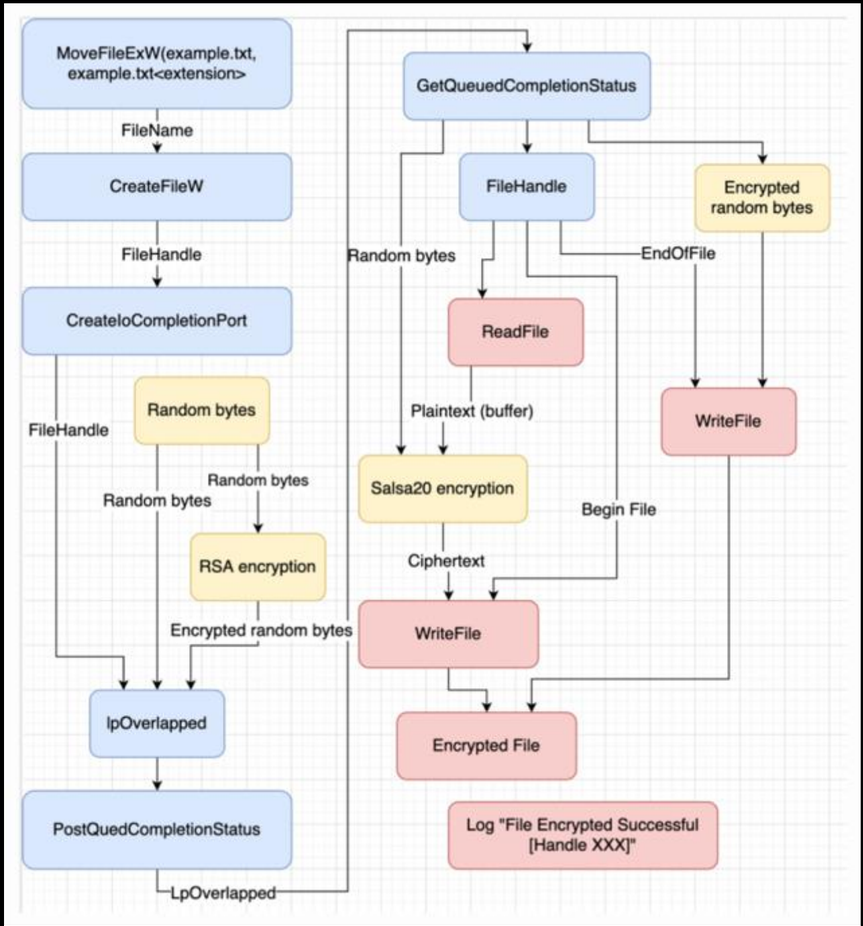
THE PRESIDENT: Hello, folks. I want to update everyone on the ransomware cyberattack that impacted on the Colonial Pipeline over this past week.

About the latest news.

10.05.2021

We are apolitical, we do not participate in geopolitics, **do not need** to tie us with a defined goverment and look for other our motives.
Our goal is to make money, and not creating problems for society.
From today we introduce moderation and check each company that our partners want to encrypt to avoid social consequences in the future.

ИЗБИРАТЕЛЬНАЯ ГЕОГРАФИЯ DARKSIDE




```
00122DCA    53              push ebx
00122DCB    BB 01000000     mov ebx,1
00122DD0    FF15 4EB91200   call dword ptr ds:[<&GetSystemDefaultUILanguage>]
00122DD6    8BF0            mov esi,eax
00122DD8    FF15 4AB91200   call dword ptr ds:[<&GetUserDefaultLangID>]
```

Используя функции GetSystemDefaultUILanguage () и GetUserDefaultLangID (), DarkSide проверяет местоположение машины, чтобы избежать шифрования систем, расположенных в странах бывшего Советского Союза.

Russian - 419	Azerbaijani (Latin) - 42C	Tatar - 444
Ukrainian - 422	Georgian - 437	Romanian (Moldova) - 818
Belarusian - 423	Kazakh - 43F	Russian (Moldova) - 819
Tajik - 428	Kyrgyz (Cyrillic) - 440	Azerbaijani (Cyrillic) - 82C
Armenian - 42B	Turkmen - 442	Uzbek (Cyrillic) - 843
	Uzbek (Latin) - 443	Arabic (Syria) - 2801

«У МЕНЯ ВОЗДУШНЫЙ ЗАЗОР»

Очень часто «Воздушный зазор» = Security through obscurity, т.к. какая-либо связность из корп. сети до технологической все-таки есть. Если сеть действительно физически изолирована, это все еще не гарантия защиты

Связность цепочки будет реализована через:

Любые устройства: доверенные USB, ноутбук сотрудника, вернувшегося из командировки и т.п.
Модем вставленный в конечную станцию Raspberry Pie, подключенный к сети
Новый сервер, скомпрометированный (прим.: троян в UEFI) еще на этапе производства

Настоящая изоляция

Технологический сегментр

Верхний уровень АСУТП


АРМ инженера

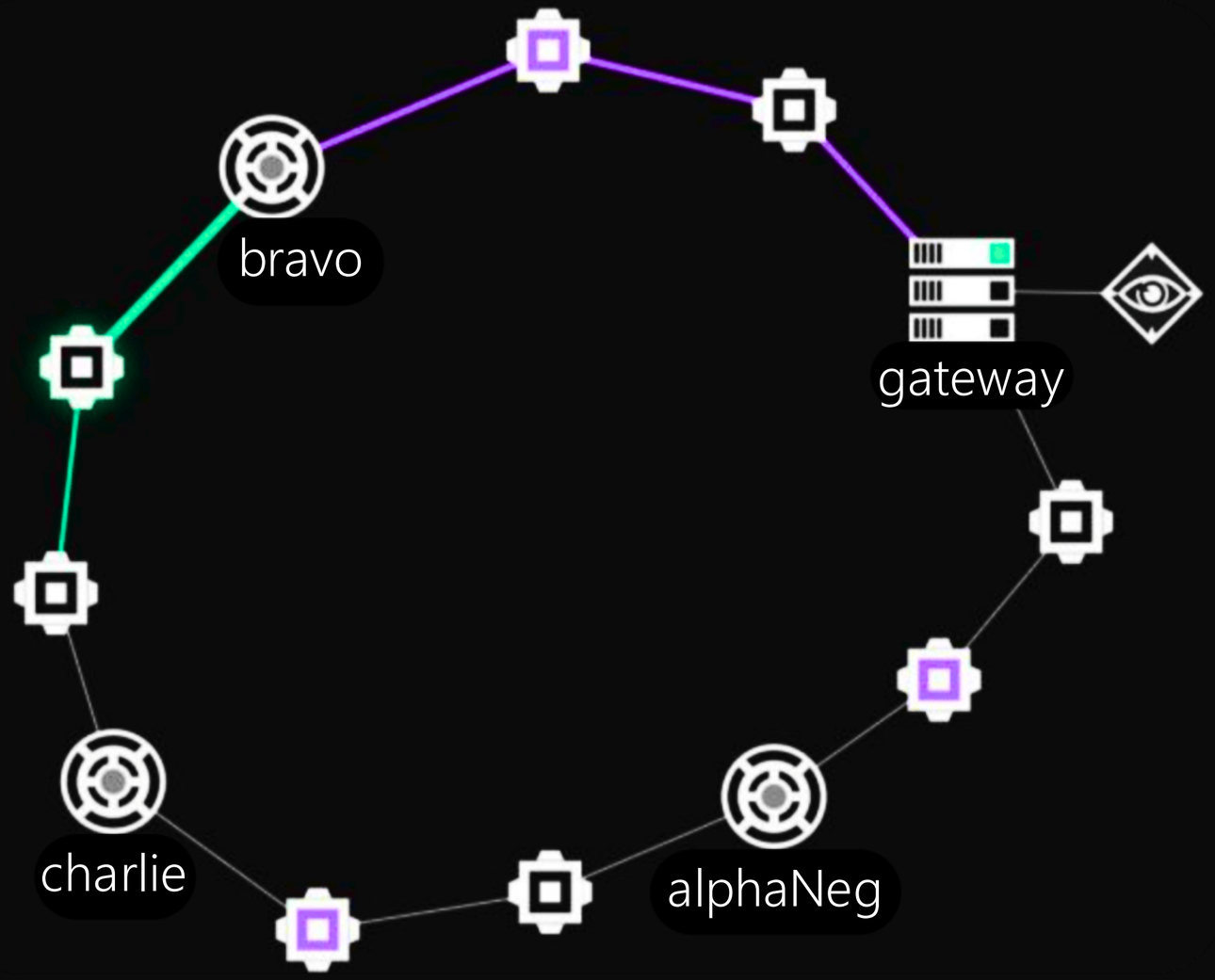

SCADA

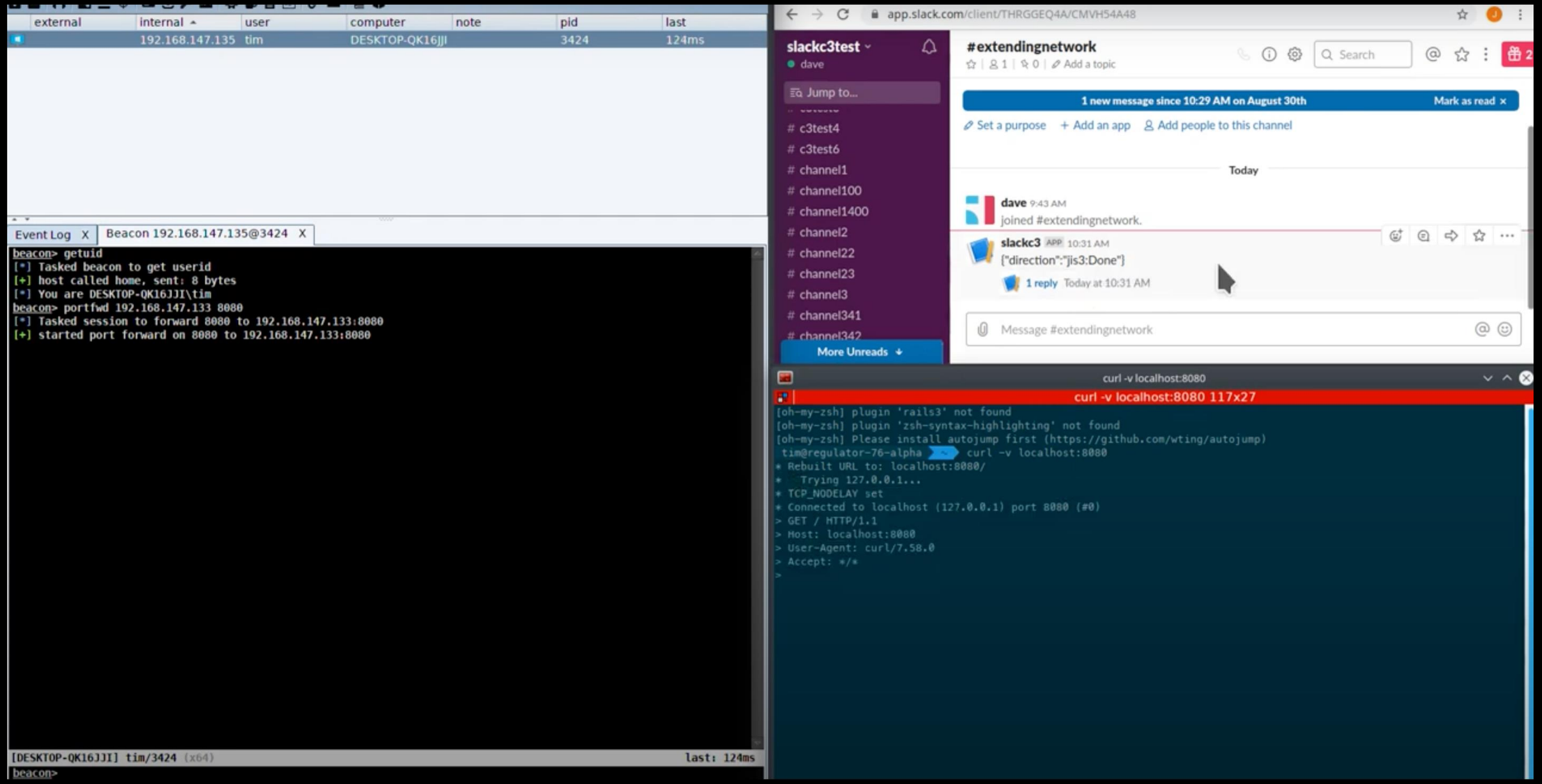
Средний уровень АСУТП


ПЛК Siemens


Другие контроллеры

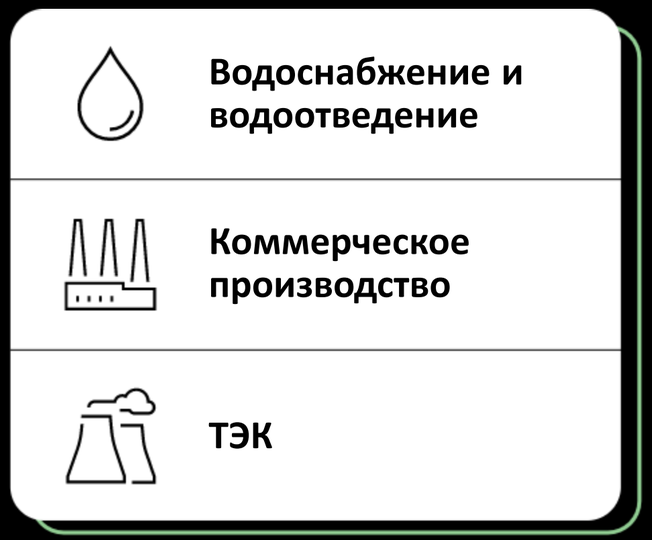
Туннели через цепочки хостов и протоколов




external
internal
user
computer
note
pid
last
192.168.147.135
tim
DESKTOP-QK16JJI
3424
124ms
Event Log X
Beacon 192.168.147.135@3424 X
beacon> getuid
[*] Tasked beacon to get userid
[+] host called home, sent: 8 bytes
[*] You are DESKTOP-QK16JJI\tim
beacon> portfwd 192.168.147.133 8080
[*] Tasked session to forward 8080 to 192.168.147.133:8080
[+] started port forward on 8080 to 192.168.147.133:8080
[DESKTOP-QK16JJI] tim/3424 (x64)
last: 124ms
beacon>
app.slack.com/client/THRGGEQ4A/CMVH54A48
slackc3test
dave
Jump to...
c3test4
c3test6
channel1
channel100
channel1400
channel2
channel22
channel23
channel3
channel341
channel342
More Unreads
#extendingnetwork
Search
1 new message since 10:29 AM on August 30th
Mark as read
Set a purpose
Add an app
Add people to this channel
Today
dave 9:43 AM
joined #extendingnetwork.
slackc3 APP 10:31 AM
{"direction":"jis3:Done"}
1 reply Today at 10:31 AM
Message #extendingnetwork
curl -v localhost:8080
curl -v localhost:8080 117x27
[oh-my-zsh] plugin 'rails3' not found
[oh-my-zsh] plugin 'zsh-syntax-highlighting' not found
[oh-my-zsh] Please install autojump first (https://github.com/wting/autojump)
tim@regulator-76-alpha ~ curl -v localhost:8080
* Rebuilt URL to: localhost:8080/
* Trying 127.0.0.1...
* TCP_NODELAY set
* Connected to localhost (127.0.0.1) port 8080 (#0)
> GET / HTTP/1.1
> Host: localhost:8080
> User-Agent: curl/7.58.0
> Accept: */*
>

УГРОЗЫ ДЛЯ ОТ-СЕГМЕНТА К 2021 В ЦИФРАХ

Наибольшее количество уязвимостей АСУ ТП во втором полугодии 2020 раскрыто в секторах:



>70%

обнаруженных уязвимостей АСУ ТП можно использовать удаленно

78%

выявленных уязвимостей АСУ ТП не требуют аутентификации для эксплуатации

На 25%

в год растет количество обнаруживаемых уязвимостей АСУ ТП

70-80%

уязвимостей АСУ ТП получают высокий уровень критичности при обнаружении

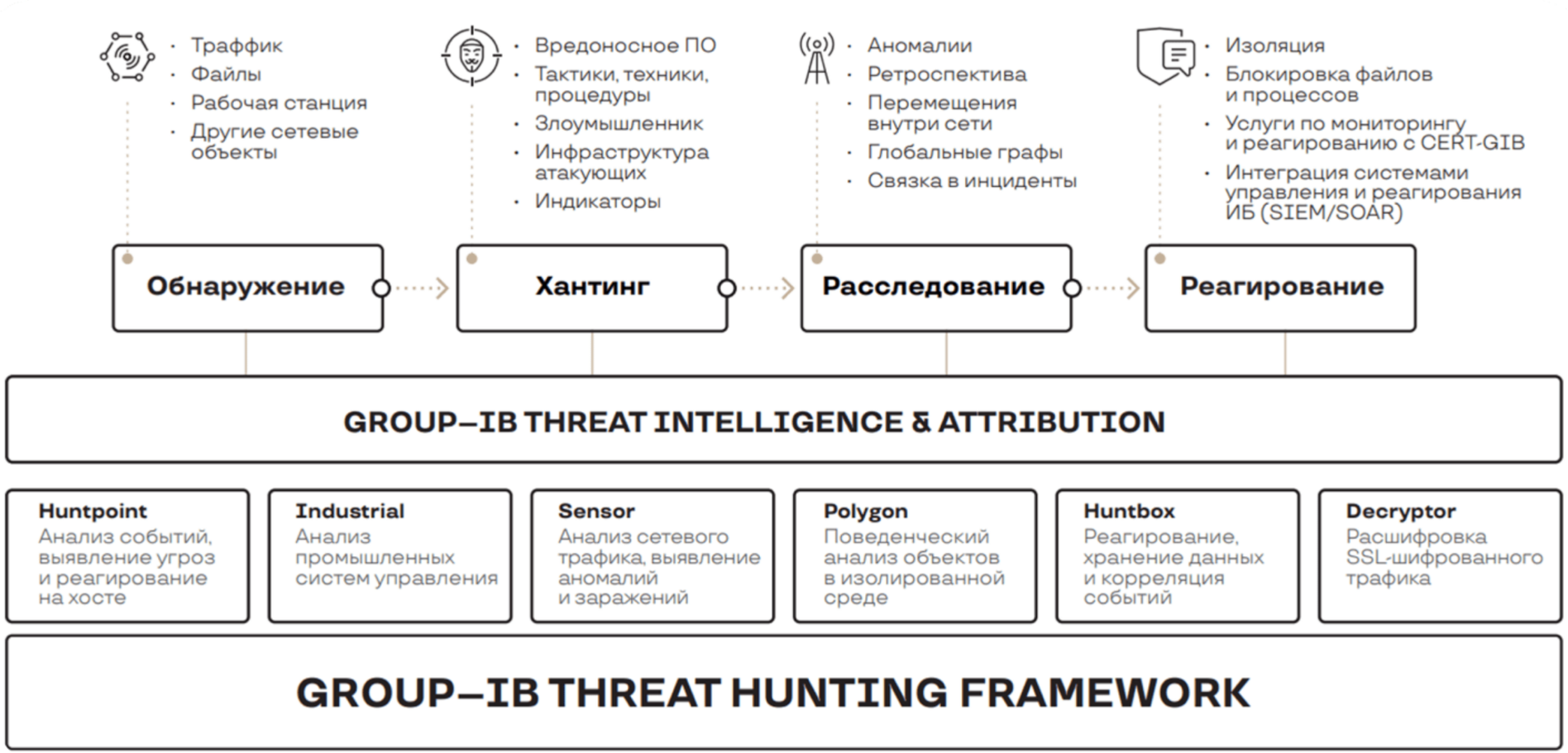
Около 45%

выявленных уязвимостей затрагивают средний уровень АСУ ТП

До 60%

предприятий закрываются после успешной целевой атаки шифровальщика

ОБЩАЯ АРХИТЕКТУРА GROUP-IB THF



ВОЗМОЖНОСТИ GROUP-IB THF INDUSTRIAL

Контроль топологии и карты соединений

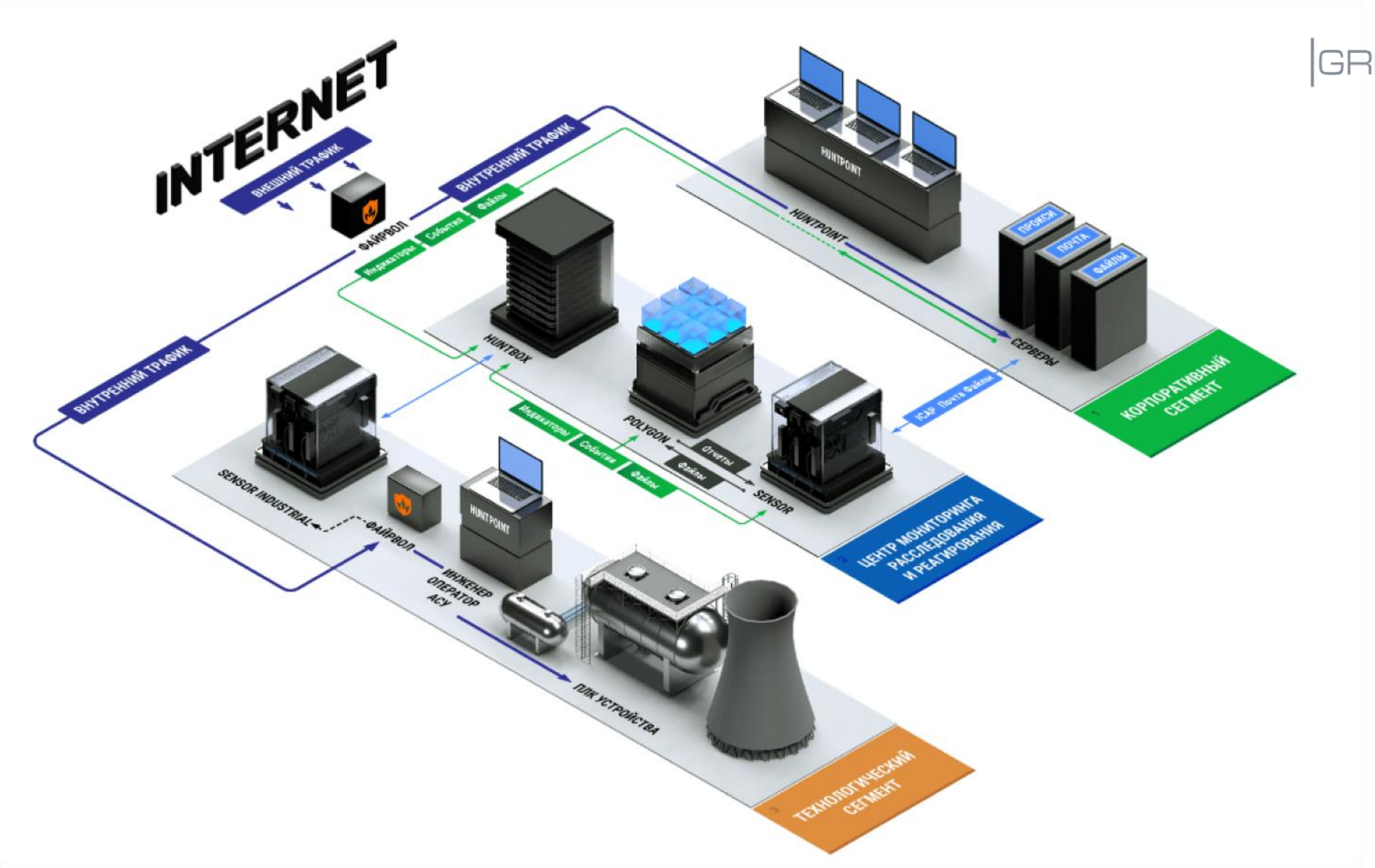
- Детектирование новых устройств
- Непрерывная инвентаризация компонентов и процессов
- Обнаружение аномалий в трафике
- Отслеживание новых подключений
- Использование самоубучаемых моделей

Контроль программ управления

- Пассивное определение версий ПО и ПЛК
- Контроли изменений загруженных программ управления
- Обнаружение не задокументированных возможностей промышленных протоколов и нестандартной активности в АСУ ТП

Поддержка протоколов и специфичных политик

- Поддержка ключевых проприетарных и открытых технологических протоколов
- Детектирование атак и поиск аномалий на основании клиенто-специфичных политик, настраиваемых в интерфейсе решения


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

GROUP-IB THREAT HUNTING FRAMEWORK

Единый интерфейс

Управление всеми модулями системы и их динамическая конфигурация

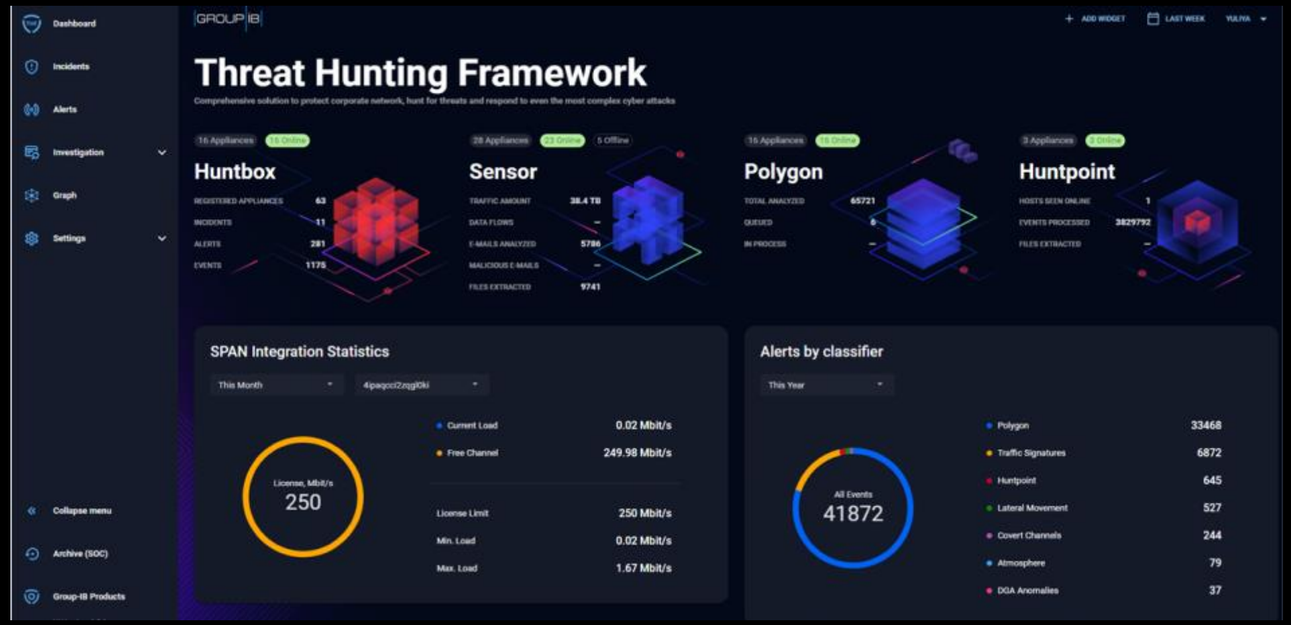
Управление инцидентами

Корреляция и группировка событий в инциденты, для сокращения времени их обработки

Гибкие опции поставки

- Локальная установка для хранения всех данных внутри периметра
- Облачная инфраструктура
- с настраиваемыми службами безопасности

Полностью автоматизированный поиск внутренних и внешних угроз и оптимизированное реагирование



ПРОЕКТЫ И ВНЕДРЕНИЯ GROUP-IB THF INDUSTRIAL

Производство СЧВ РФ

Протоколы

- Modbus
- OPCUA
- Modbus proprietary

Подстанции ГЭК в Италии

Контроллеры

- S7-1200
- S7-300

Сингапур

Контроллеры

- Emerson DeltaV MD
- Modbus custom

ГЭС Казахстан

Протоколы

- OPCUA
- FINS (OMRON)

Энергокомпании РФ

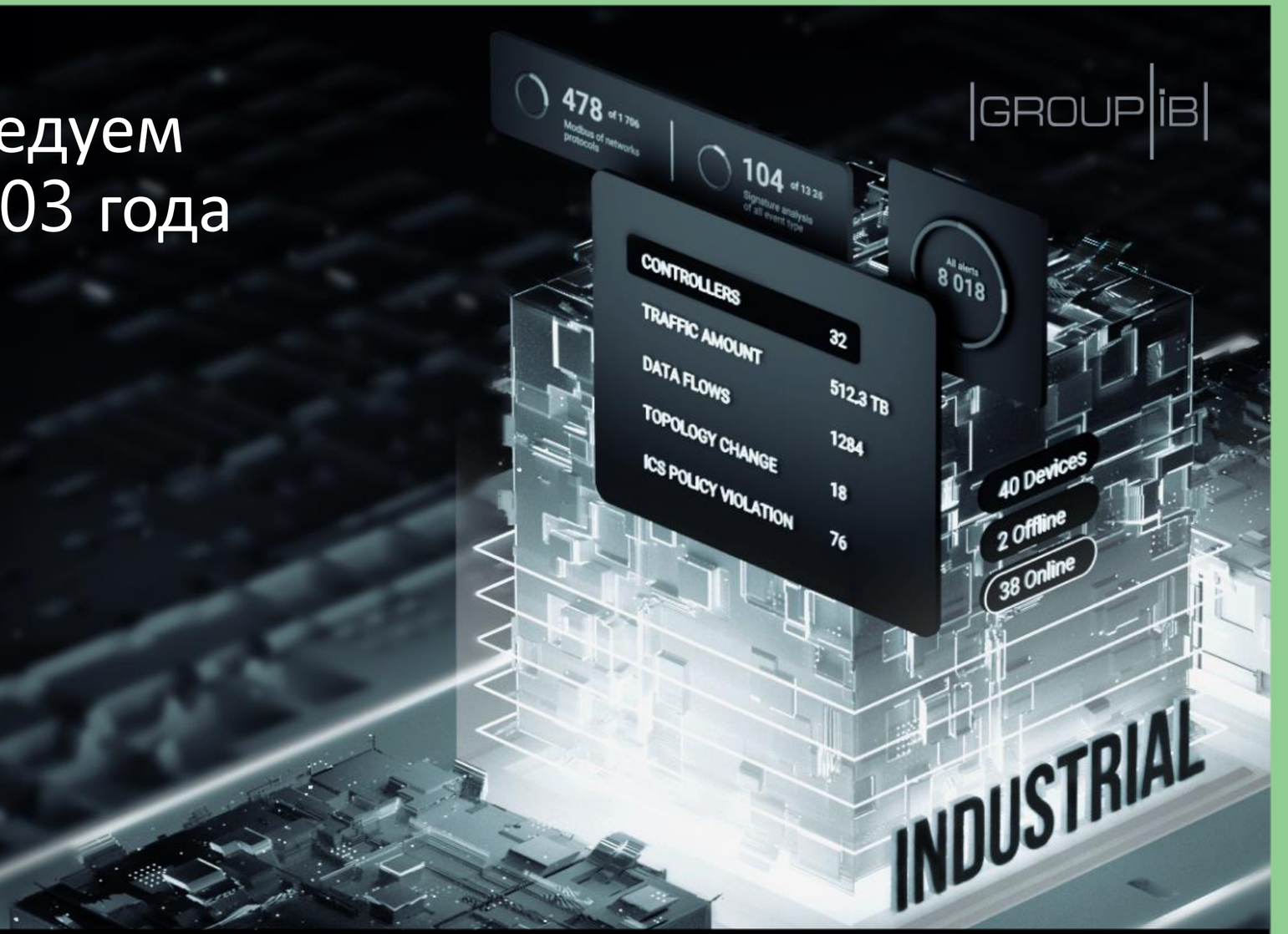
Протоколы

- OPCUA
- OPCDA
- S7Comm/S7CommPlus

Предотвращаем и расследуем киберпреступления с 2003 года

Суслин Андрей

Руководитель отдела по разработке решений для АСУ ТП Group-IB



www.group-ib.ru
group-ib.ru/blog

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

twitter.com/groupib
facebook.com/groupib

t.me/group_ib
instagram.com/group_ib