

Статистика и практика инцидентов ИБ

kaspersky



Борис Осепов,
старший инженер
предпродажной поддержки

Forbes. ТОП-200 наиболее "киберзащищенных" компаний США

Most CyberSecure in USA

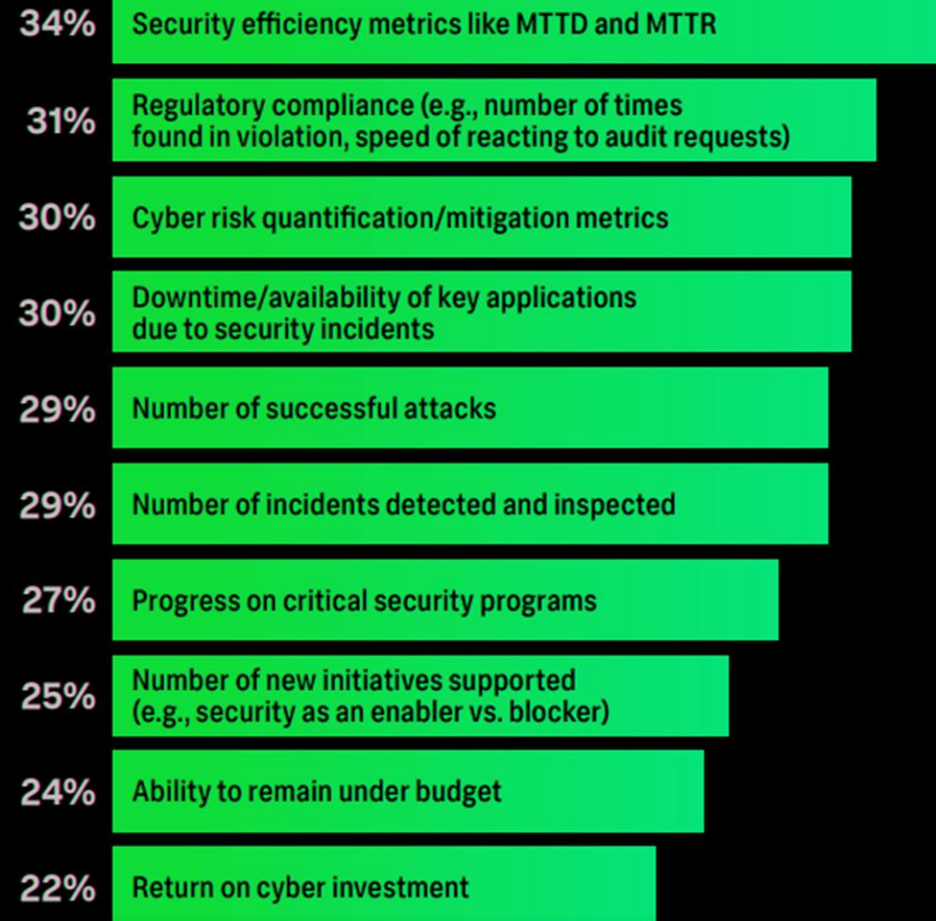
Top 20, as ranked by Forbes & SecurityScorecard

Security Scorecard **Forbes** Forbes & SecurityScorecard
Published June 8th 2023

Успешное ИБ, это что?

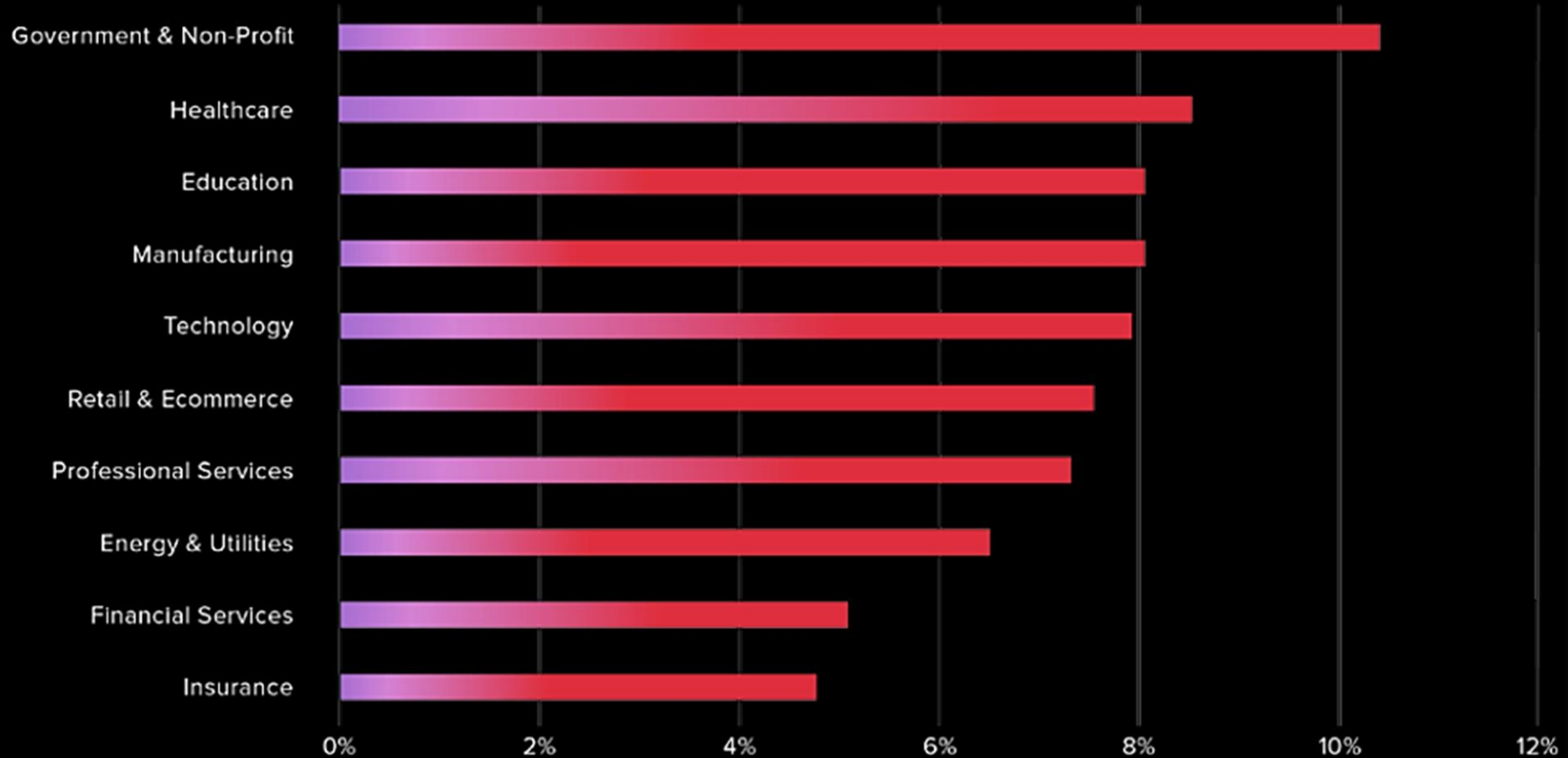
How Business Leaders Measure Security Success

Top metrics used by business leaders to understand cybersecurity



Статистика по уязвимостям на основе 300к пентестов

Percentage of High and Critical Vulnerabilities, by Industry



Время закрытия критической уязвимости по регламенту

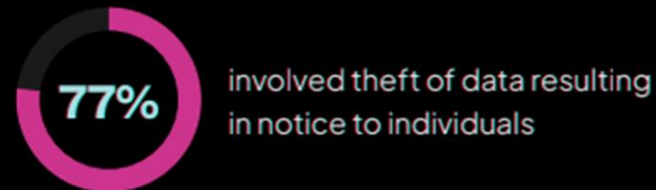
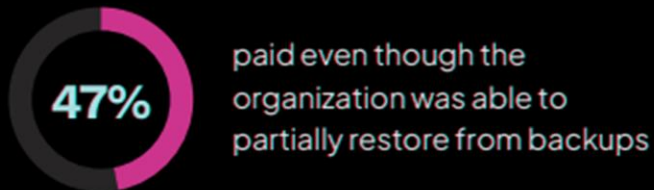
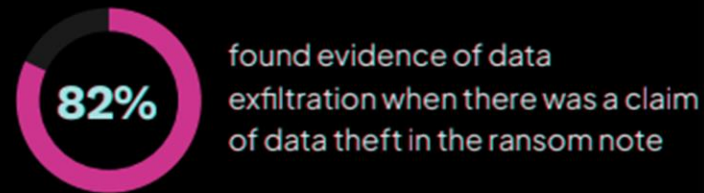
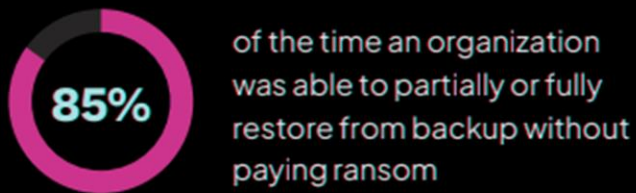
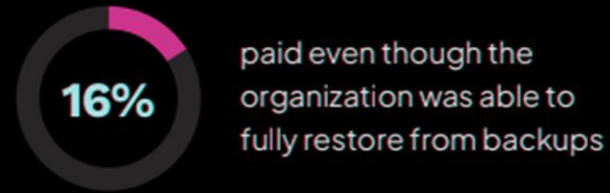
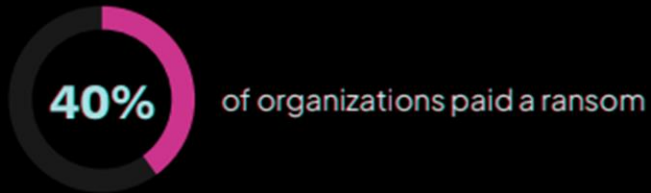


Цифры и статистика по шифровальщикам

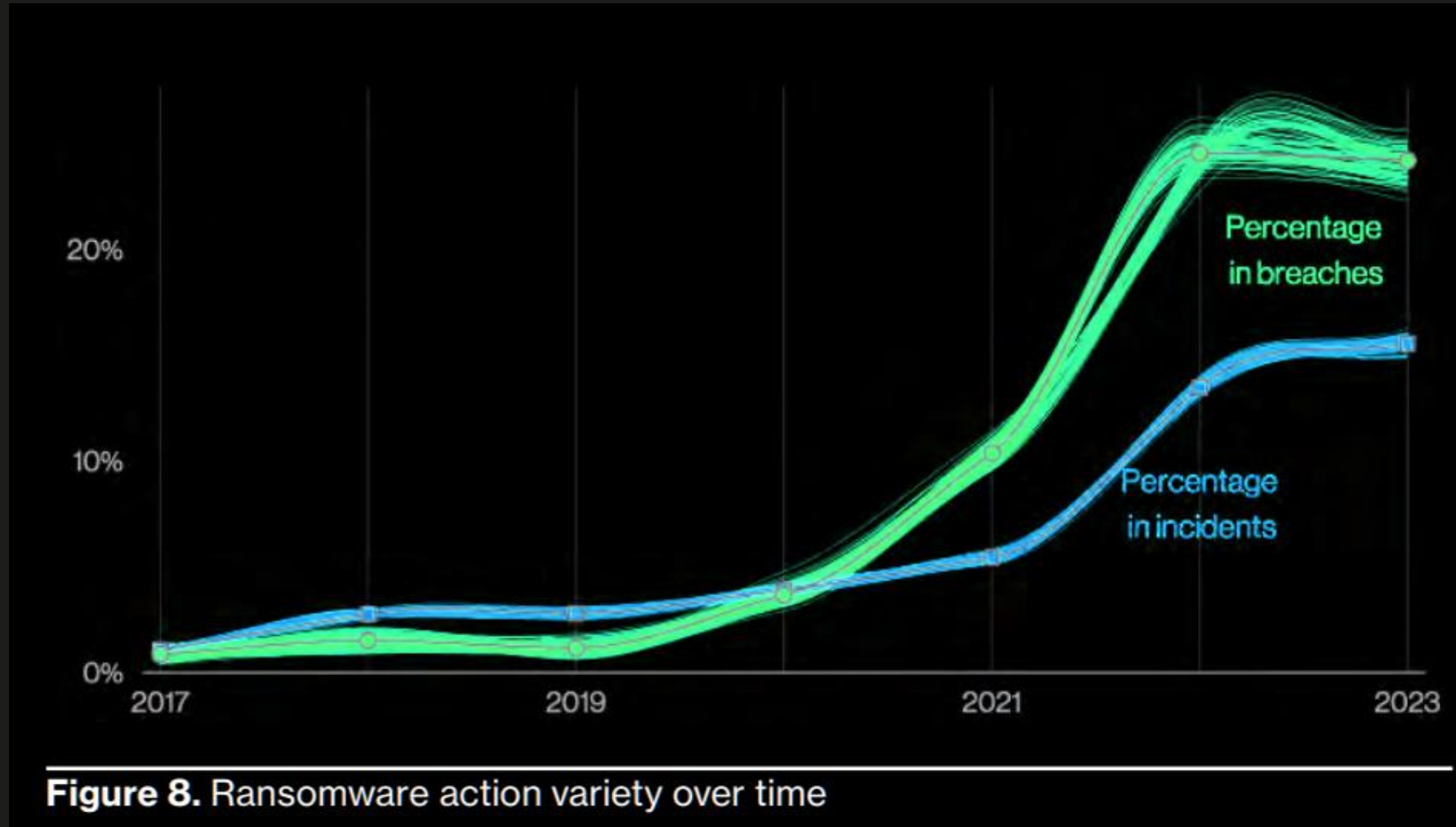
Largest Ransom Demand in 2022:
\$90+ million
(\$60+ million in 2021)

Largest Ransom Paid in 2022:
\$8+ million
(\$5.5 million in 2021)

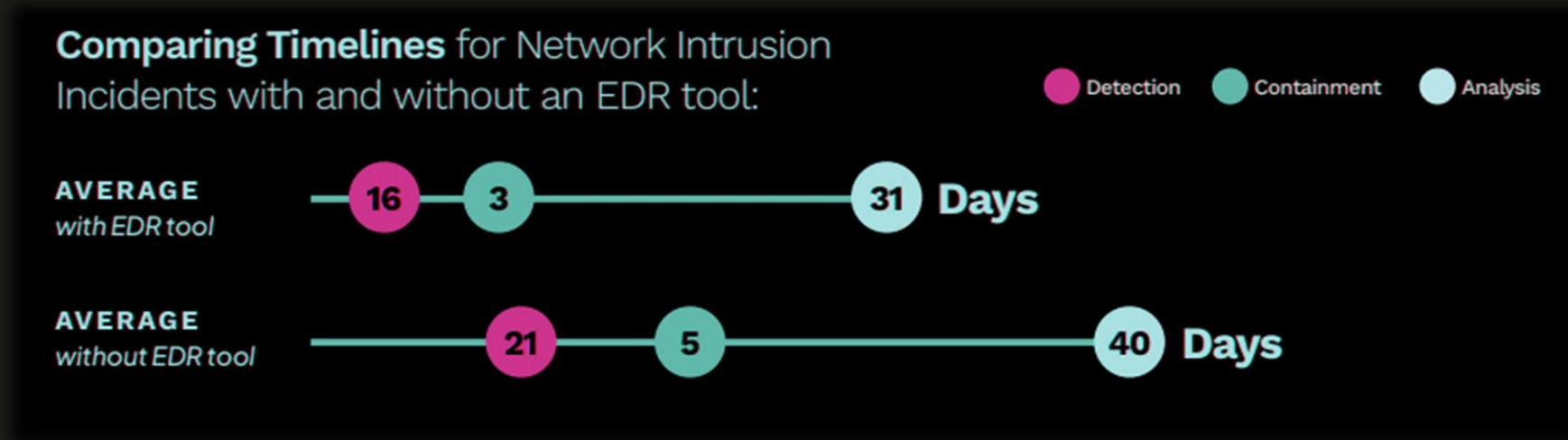
Average Ransom Paid in 2022:
\$600,688
(\$511,957 in 2021)



Цифры и статистика по шифровальщикам

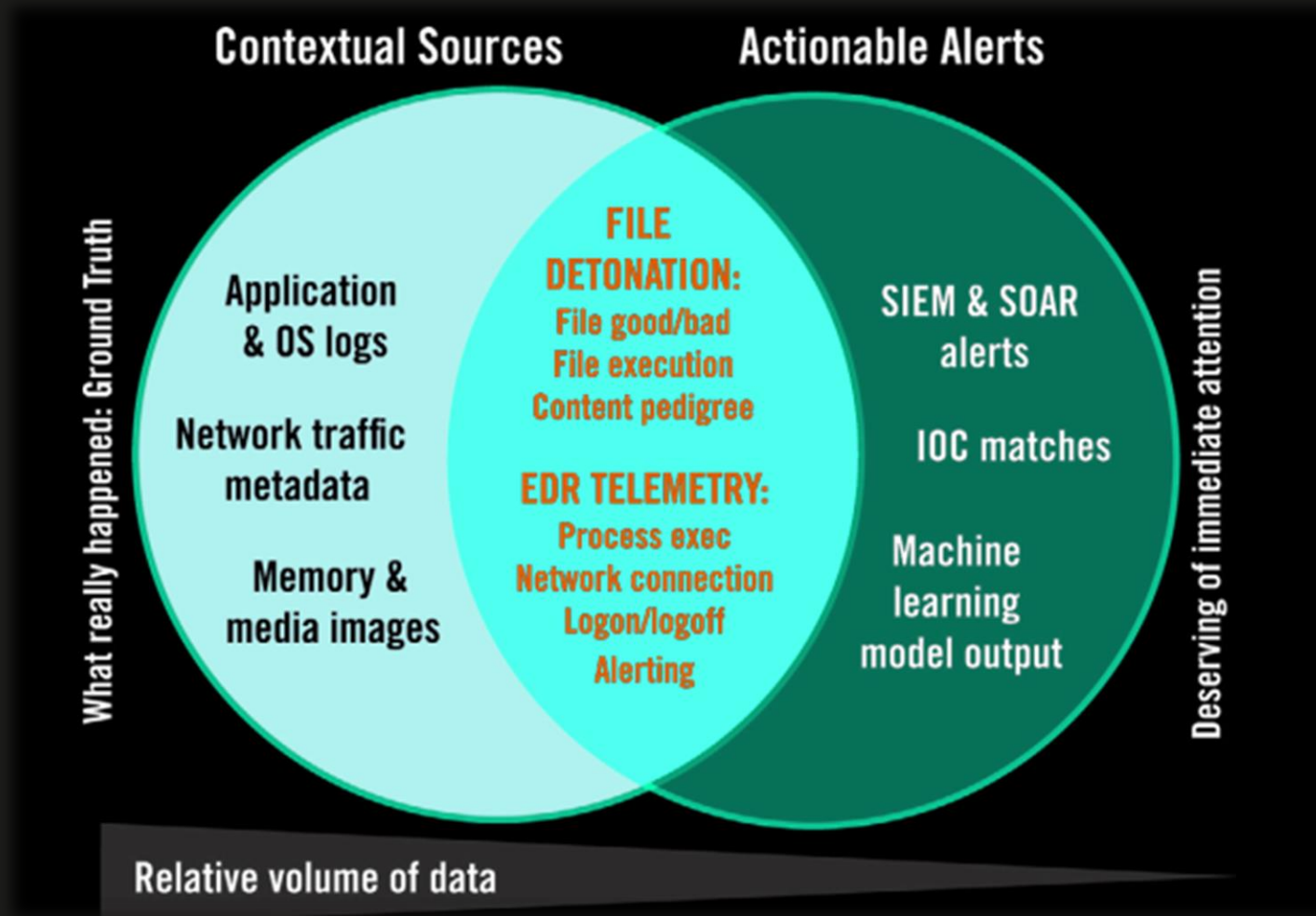


Что помогает?



Улучшение метрик на **22,5 %**

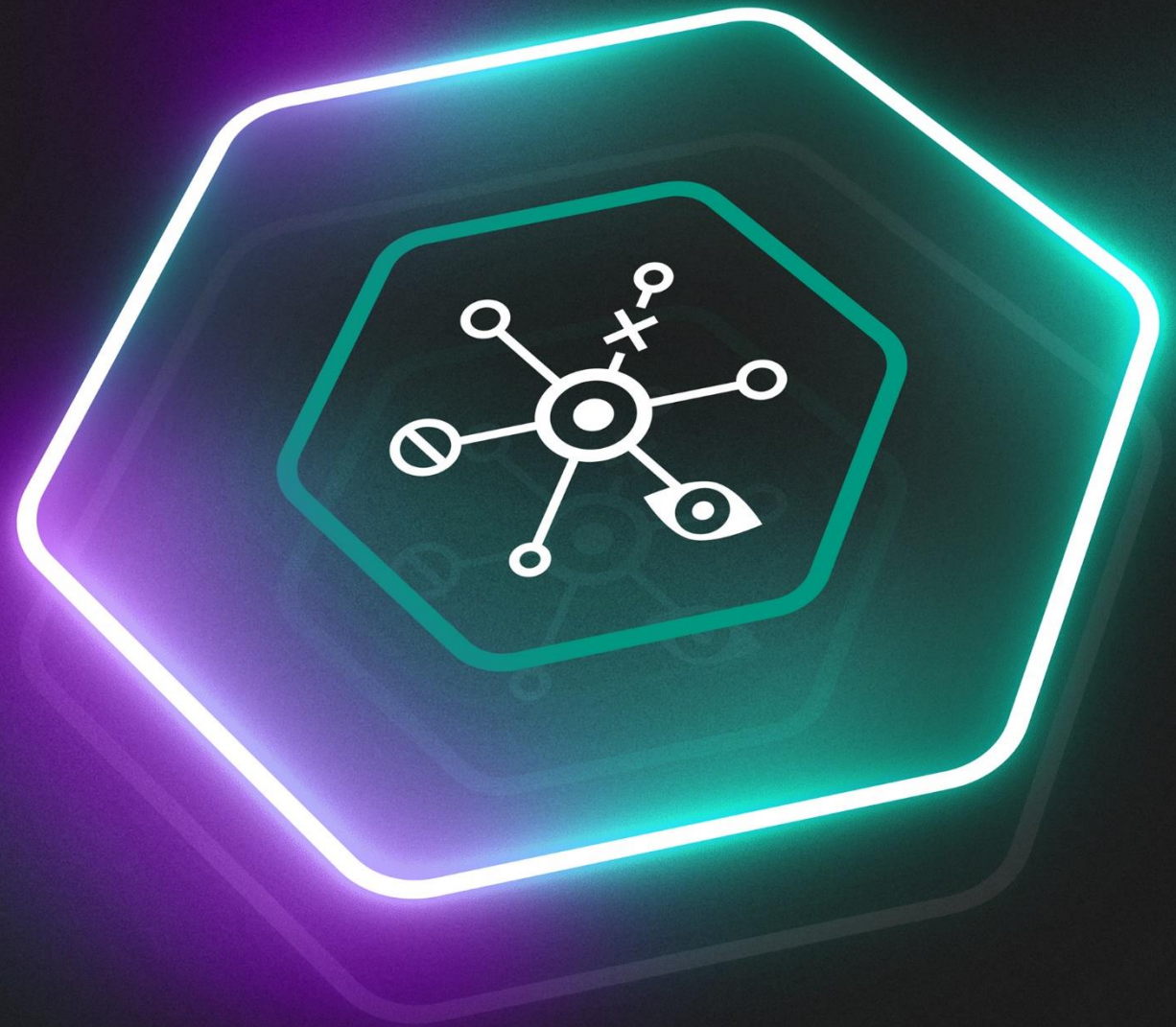
Что помогает?



Больше тренировок!



**Реальный кейс
на пилоте
(окт 2019)**



Находим первое проявление PowerShell с сетевой активностью

Alerts Processed Filters Show all

12 of 685 | 0 VIP | 12 High | 0 Medium | 0 Low | 12 New | 0 In process

<input type="checkbox"/>	VIP	Created	Detected x	Details	Source	Destination	Technologies	State
<input type="checkbox"/>	☆	30/10 11:17	powershell_with_network_activity	Detect 1	-	-	IOA	New
<input type="checkbox"/>	☆	28/10 10:45	powershell_with_network_activity	Detect 1	-	-	IOA	New
<input type="checkbox"/>	☆	26/10 15:00	powershell_with_network_activity	Detect 1	-	-	IOA	New
<input type="checkbox"/>	☆	23/10 14:46	powershell_with_network_activity	Detect 1	-	-	IOA	New
<input type="checkbox"/>	☆	20/10 15:00	powershell_with_network_activity	Detect 1	-	-	IOA	New
<input type="checkbox"/>	☆	18/10 12:01	powershell_with_network_activity	Detect 1	-	-	IOA	New
<input type="checkbox"/>	☆	16/10 17:15	powershell_with_network_activity	Detect 1	-	-	IOA	New
<input type="checkbox"/>	☆	10/10 02:45	powershell_with_network_activity	Detect 1	-	-	IOA	New
<input type="checkbox"/>	☆	07/10 09:45	powershell_with_network_activity	Detect 2	-	-	IOA	New
<input type="checkbox"/>	☆	05/10 20:45	powershell_with_network_activity	Detect 1	-	-	IOA	New
<input type="checkbox"/>	☆	04/10 13:15	powershell_with_network_activity	Detect 1	-	-	IOA	New
<input type="checkbox"/>	☆	02/10 17:30	powershell_with_network_activity	Detect 5	-	-	IOA	New

Находим очень подозрительную проверку доступности ресурса



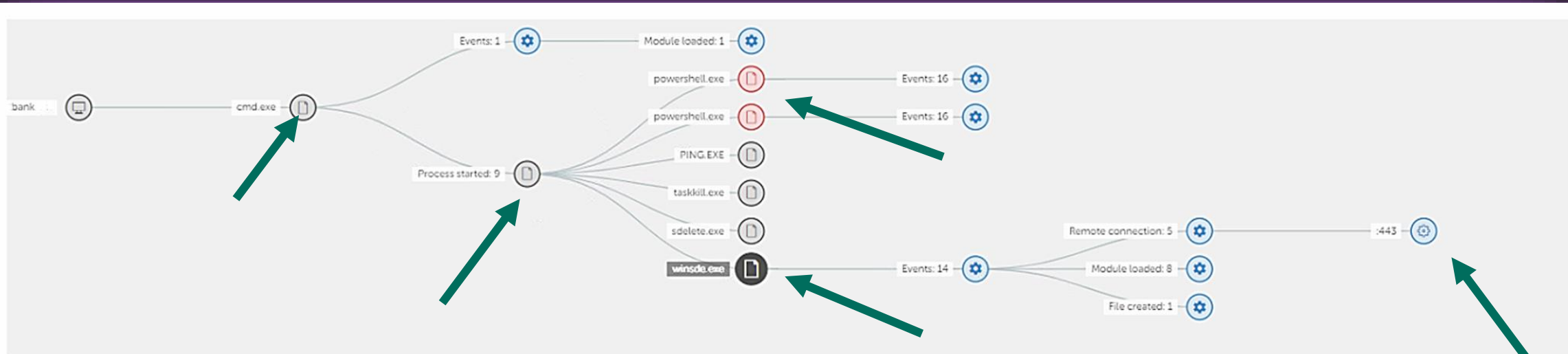
Process started

IOA tags	suspicious_powershell_cmdline_downloading powershell_with_network_activity
Event time	03 October 2019 02:20
File	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Launch parameters	powershell try(\$ip='216.58.213.142';\$es=New-Object System.Net.Sockets.TcpClient(\$ip,443);Write-Host '[OK]');catch{Write-Host '[FAIL]';}
MD5	92f44e405db16ac55d97e3bfe3b132fa
SHA256	6c05e11399b7e3c8ed31bae72014cf249c144a8f4a2c54a758eb2e6fad47aec7
Size	442 KB
Process ID	5012
Process end time	03 October 2019 02:20
Time created	14 July 2009 04:32

Parent process

File	C:\Windows\System32\cmd.exe
MD5	ad7b9c14083b52bc532fba5948342b98
SHA256	17f746d82695fa9b35493b41859d39d786d32b23a9d2e00f4011dec7a02402ae
Process ID	9564

Раскрываем ветки активности и смотрим проявление всей активности



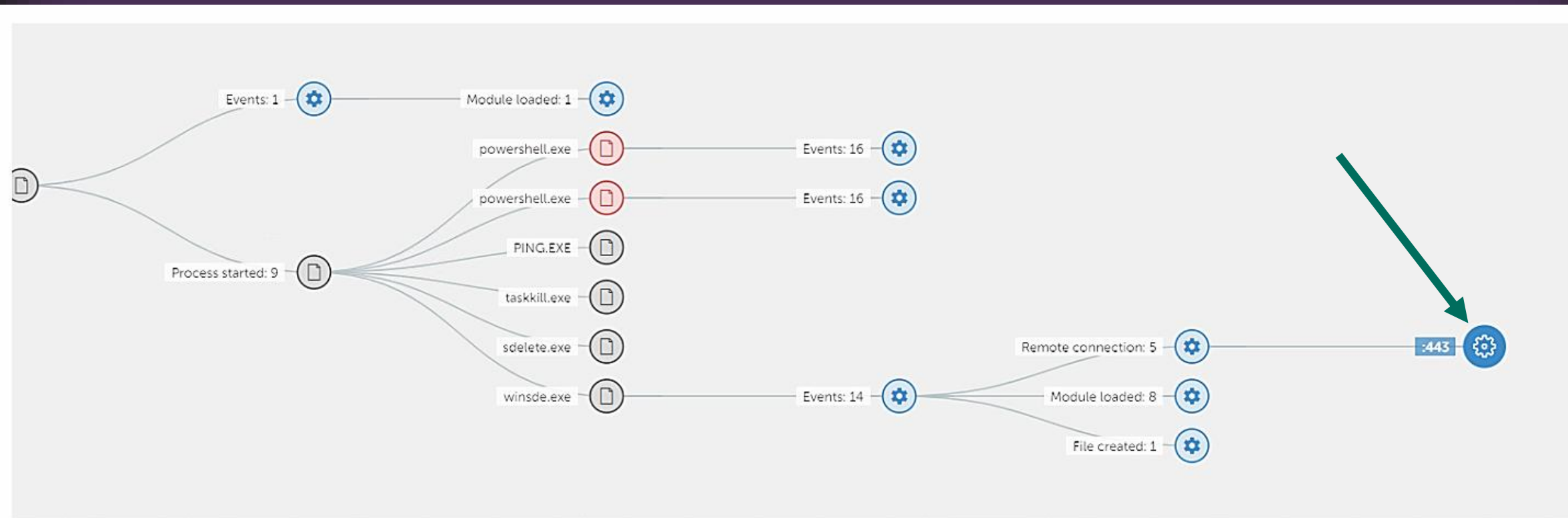
Process started

Event time	02 October 2019 17:08
File	C:\PerfLogs\winsde.exe
Launch parameters	ping 192.168.10.55 -n 1
MD5	6242e3d67787ccbf4e06ad2982853144
SHA256	4ca10dba7ff487fdb3f1362a3681d7d929f5aa1262cdfd31b04c30826983fb1d
Size	55 KB
Process ID	3796

Parent process

File	C:\Windows\System32\cmd.exe
MD5	ad7b9c14083b52bc532fba5948342b98
SHA256	17f746d82695fa9b35493b41859d39d786d32b23a9d2e00f4011dec7a02402ae
Process ID	5132

Проверим сетевое обращение от winsde.exe



Remote connection

Event time	02 October 2019 17:09
Remote IP	79.141.168.114:443
Local IP	192.168.178.114
Host name	[REDACTED]
User name	NT AUTHORITY\SYSTEM

Parent process

File	C:\PerfLogs\winsde.exe
MD5	71fa6c1937eff70f619b5fb3ed5e9d37
SHA256	306dc58e4b023c9a72e1805341078736e4fd2138ad528ec3a57e99c89ac36fb2

winsde.exe – Вредоносный?

Browser address bar: <http://79.141.168.114:443/>

0
/ 71

Community Score

✓ No engines detected this URL

<http://79.141.168.114:443/>
79.141.168.114

2019-10-08 16:09:21 UTC
29 days ago

DETECTION	DETAILS	COMMUNITY
ADMINUSLabs	✓ Clean	AegisLab WebGuard ✓ Clean
AlienVault	✓ Clean	Antiy-AVL ✓ Clean

winsde.exe – Вредоносный !!!

Kaspersky Threat Intelligence Portal

Home Reporting Threat Lookup WHOIS Track

You are using a trial version of the service. Purchase a commercial license for a large

Hash, IP address
Enter
More about

Report for IP address: Dangerous Copy report

79.141.168.114:443

Hits —
First seen —
Threat score 100

Categories **APT Related**

Reports **Early alert: Silence active in Eastern Europe**

Reports (1)

Master YARA (APT) Master IOC (APT) Master YARA (Financial) Master IOC (Financial) (available only for commercial licenses)

Oct 01, 2019 **Early alert: Silence active in Eastern Europe**

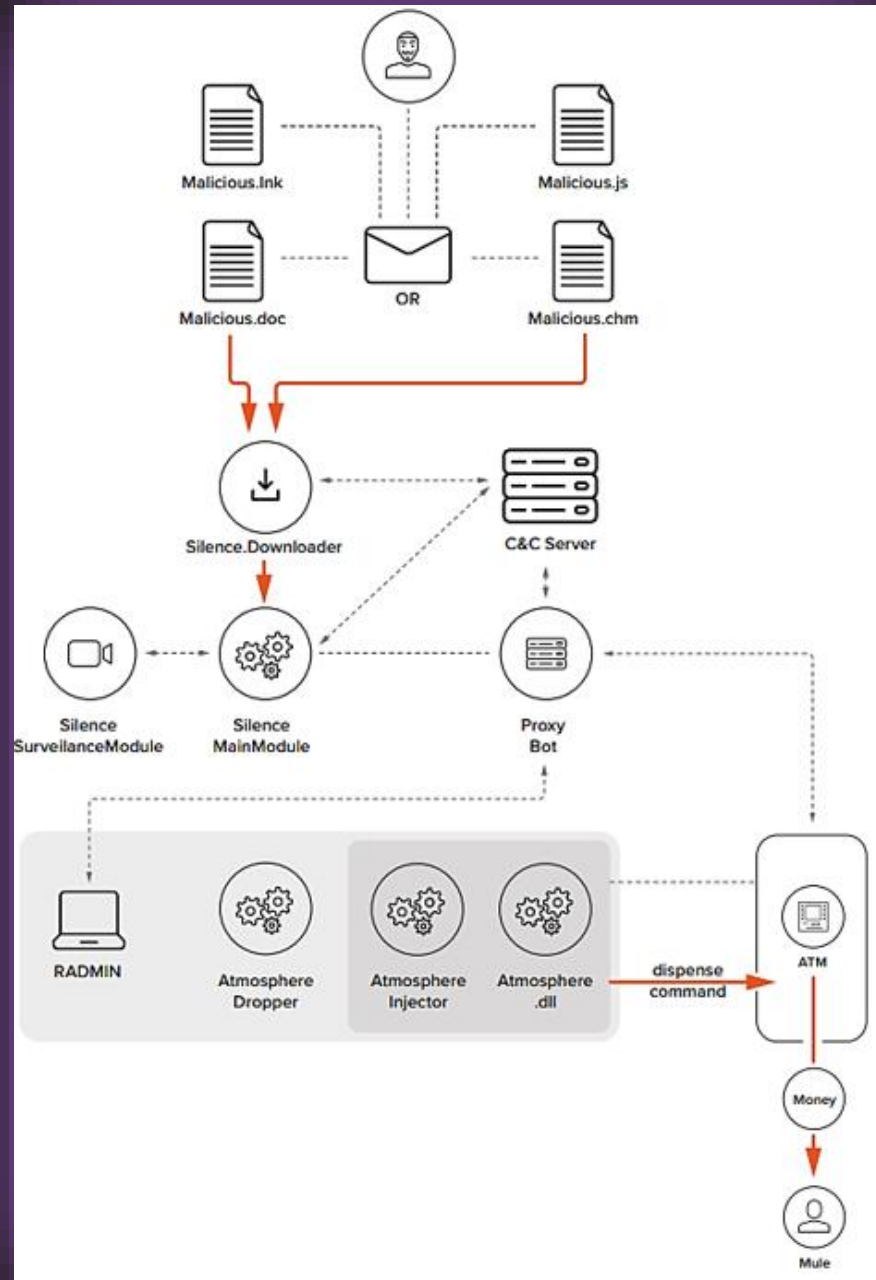
Bosnia and Herzegovina Silence Banks

At the beginning of the 2019 summer, the Silence group changed their tactics and started to attack financial organizations all over the globe. Now they are one of the most active financial-motivated targeted attack groups. In September they added new proxy tools to their arsenal that was used during the attack on a bank in Bosnia and Herzegovina. This report describes these tools and provides IOCs of the current attack.

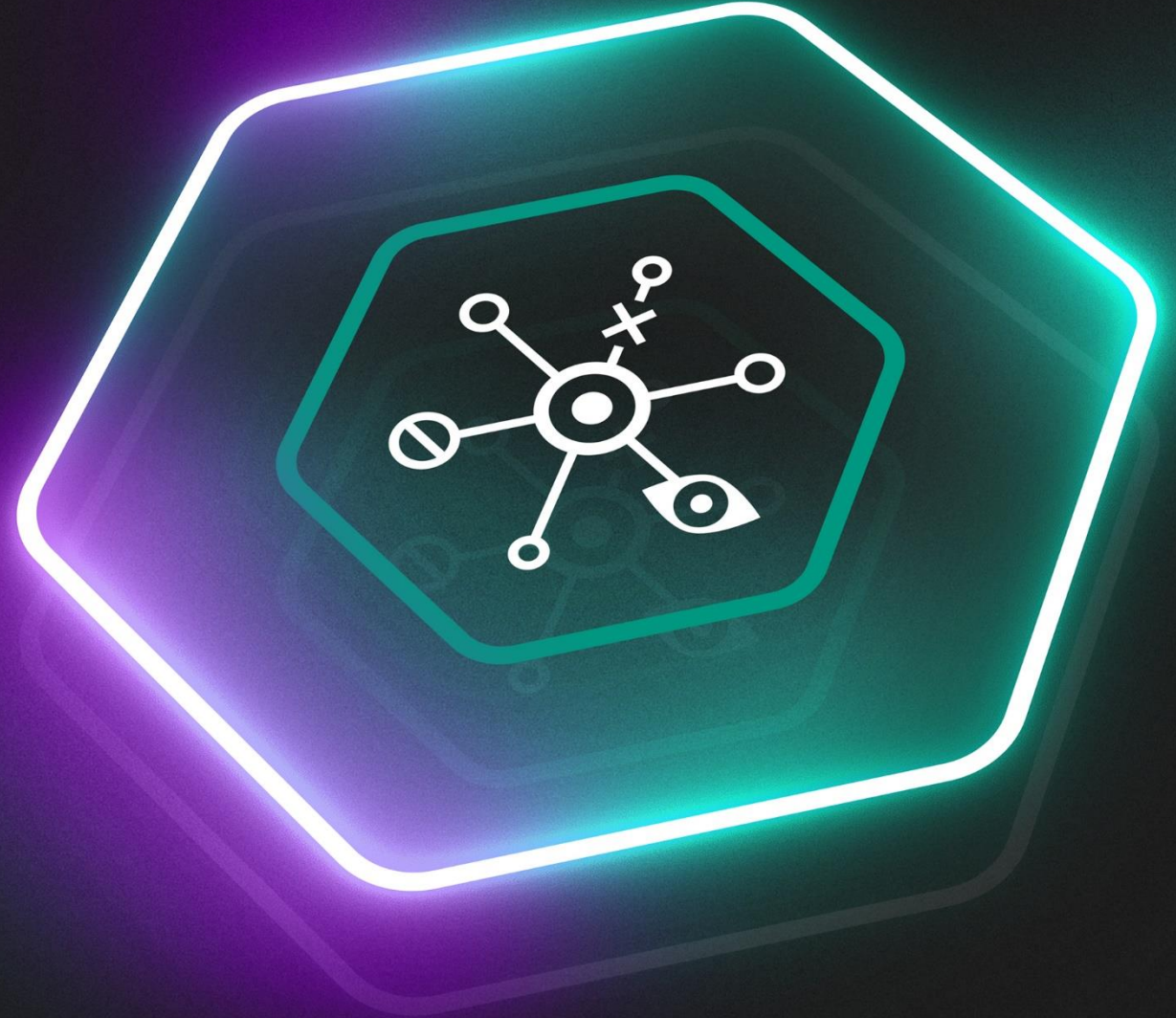
WHOIS

IP range	Net name	Net description	Created	Changed	AS description	ASN
79.141.168.0-79.141.169.255	HZ-NA28	—	Aug 03, 2018	Aug 30, 2018	—	133398


APT – Silence



**Реальный кейс
у партнера
(май 2022)**



Шпионское ПО на мобильном устройстве (PEGASUS)



Kaspersky
Anti Targeted
Attack Platform

- Мониторинг
- Обнаружения** 303
- Поиск угроз
- Задачи
- Политики
- Пользовательские правила
- Хранилище
- Endpoint Agents
- Отчеты
- Параметры

SO

Обнаружения

Показывать закрытые обнаружения

Сохраненные фильтры

146 из 440

0 VIP

146 Высокая

0 Средняя

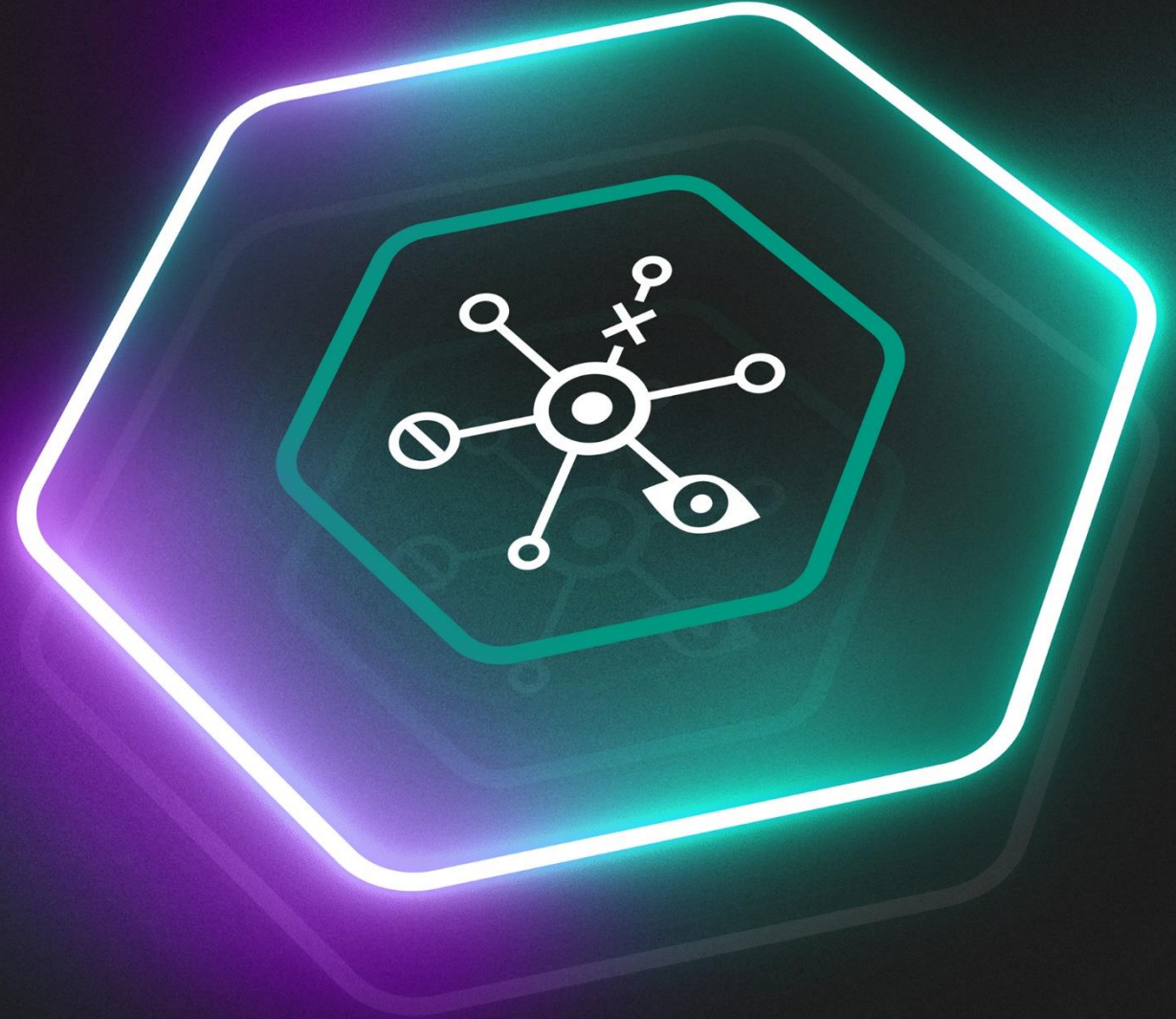
0 Низкая

146 Новое

0 В обработке

<input type="checkbox"/>	VIP	Создано	Обнаружено	Сведения	Адрес источника	Адрес назначения	Технологии	Состояние	Назначено
<input type="checkbox"/>	-	2022-06-06 14 23 23	TA-related host (NSO_Group), Malicious host	Домен: chubaka.org	192.168.779	192.168.71	URL	Новое	-
<input type="checkbox"/>	-	2022-06-06 14 23 22	TA-related host (NSO_Group), Malicious host	Домен: chubaka.org	192.168.779	192.168.71	URL	Новое	-
<input type="checkbox"/>	-	2022-06-06 14 23 22	TA-related host (NSO_Group), Malicious host	Домен: breakfastisgood.com	192.168.779	192.168.71	URL	Новое	-
<input type="checkbox"/>	-	2022-06-06 14 23 22	TA-related host (NSO_Group), Malicious host	Домен: breakfastisgood.com	192.168.779	192.168.71	URL	Новое	-
<input type="checkbox"/>	-	2022-06-06 14 23 21	TA-related host (NSO_Group), Malicious host	Домен: topadblocker.net	192.168.779	192.168.71	URL	Новое	-
<input type="checkbox"/>	-	2022-06-06 14 23 21	TA-related host (NSO_Group), Malicious host	Домен: topadblocker.net	192.168.779	192.168.71	URL	Новое	-
<input type="checkbox"/>	-	2022-06-06 14 23 20	TA-related host (NSO_Group)	Домен: noextramoney.com	192.168.779	192.168.71	URL	Новое	-
<input type="checkbox"/>	-	2022-06-06 14 23 20	TA-related host (NSO_Group)	Домен: noextramoney.com	192.168.779	192.168.71	URL	Новое	-
<input type="checkbox"/>	-	2022-06-06 14 23 20	TA-related host (NSO_Group)	Домен: lawlowvat.net	192.168.779	192.168.71	URL	Новое	-
<input type="checkbox"/>	-	2022-06-06 14 23 19	TA-related host (NSO_Group)	Домен: lawlowvat.net	192.168.779	192.168.71	URL	Новое	-
<input type="checkbox"/>	-	2022-06-06 14 23 19	TA-related host (NSO_Group), Malicious	Домен: easy-pay.info	192.168.779	192.168.71	URL	Новое	-

Реальный кейс у клиента (2021)



Письмо, которое прошло несколько проверок ...



Kaspersky
Anti Targeted
Attack Platform

Мониторинг

Обнаружения 999+

Поиск угроз

Задачи

Политики

Пользовательские правила ▾

Хранилище ▾

Endpoint Agents

Отчеты ▾

Параметры >

@ SO >

[Все обнаружения](#) > Обнаружение #85 [redacted] 4 ...

Назначить @Мне ▾

Отметить как обработанное

Состояние ● Новое

Время создания [redacted] 2021 12 36

Важность ■ ■ ■ Высокая

Время обновления [redacted] 2021 12 37

Хост -

Источник данных Внешняя система Sensor 192.168.10.123 ([redacted] 2.36.36)

Информация об объекте

Сообщение от sales@dpttel.com

Получатели сообщения [redacted] m

Тема сообщения Order inquiry

Заголовки сообщения

```
=?us-ascii?q?hD6mLwRA09T+WzkceykPMHkSLlKtp5YhodsP2jGI3Fe3PT8pZp/ZIcVI3LYC?=  
=?us-ascii?q?DKsHalRbsN0aLM2DvlheQysd49YNNN5dzE8fxC18St6zHyTK1Gdoh39WLMZ?=  
=?us-ascii?q?rAuc7l03xvQQt2Apr40y5FDG+gfnFLeA=3D=3D?=  
X-[redacted] Anti-Spam-Filtered: true  
X-[redacted] Anti-Spam-Result: =?us-ascii?q?A0ArAwDTS3lgUxKa7MCBbLobhKxxGgM?=  
=?us-ascii?q?CAQYEATgHRIVdgjgihDE6tmSJaiHpeBk0?=  
X-IPAS-Result: =?us-ascii?q?A0ArAwDTS3lgUxKa7MCBbLobhKxxGgMCAQYEATgHRIVdg?=  
=?us-ascii?q?jaihDF6tSJaiHpeBk0?=  
X-[redacted] AV: E=McAfee; i="6200,9189,9955"; a="11817746"  
X-[redacted] AV: E=Sophos; i="5.82,226,1613419200";  
d="scan"; a="11817746"
```

✉ Order inquiry

OfficeEml

Скачать

Рекомендации

Оценка

🔍 Найти похожие обнаружения ^ 5

По MD5 1

По адресу отправителя 3


По адресу получателя 1

🔄 Найти похожие EPP-события 0

Расследование

🔄 Найти похожие события 0

Содержит потенциальный шифровальщик



Kaspersky
Anti Targeted
Attack Platform

- Мониторинг
- Обнаружения** 999+
- Поиск угроз
- Задачи
- Политики
- Пользовательские правила ▾
- Хранилище ▾
- Endpoint Agents
- Отчеты ▾
- Параметры ▶

SO ▶


[Все обнаружения](#) > Обнаружение #E[REDACTED]4 ...

Назначить @Мне ▾ [Отметить как обработанное](#)


OfficeEmI

[Скачать](#)

Результаты проверки

	Order inquiry//[From "Isab...RDER.PDF.iso//ORDER.PDF.exe	MDS
AM	✓ Не обнаружено	
SB	Trojan.MSIL.Crypt.sb	
YARA	⊖ Не выполнялась	

[Sandbox-обнаружение](#) [Найти на KL TIP ▶](#) [Изменить политику](#)

	Order inquiry//[From "Isab...rder inquiry//ORDER.PDF.iso	MDS
AM	HEUR:Trojan.Win32.Generic	
SB	✓ Не обнаружено	
YARA	⊖ Не выполнялась	

[Найти на KL TIP ▶](#) [Создать правило запрета](#)

Журнал изменений

[Добавить](#)

Плейбуки CERT Societe Generale



Руководство по IR от Kaspersky



Спасибо