kaspersky

Азиатские APT-группировки

Тактики, техники и процедуры

Никита Назаров

Руководитель отдела расширенного исследования угроз

Кирилл Митрофанов

Руководитель группы разведки киберугроз

Предисловие

«Лаборатория Касперского» отслеживает сотни различных кибергруппировок по всему миру, включая продвинутые группы, способные проводить сложные кибератаки. Такие группировки известны в мире как продвинутые постоянные угрозы или APT

Предисловие

«Лаборатория Касперского» отслеживает сотни различных кибергруппировок по всему миру, включая продвинутые группы, способные проводить сложные кибератаки. Такие группировки известны в мире как продвинутые постоянные угрозы или APT

За время нашей работы мы отметили, что эти группировки затронули больше всего стран и индустрий.

Мы не преследуем цель атрибутировать какую-либо группировку к конкретной стране в Азии.

Наша цель — предоставить максимально возможное количество информации о подходах злоумышленника, TTPs и способах митигации таких атак.

“

There is no teacher but the enemy

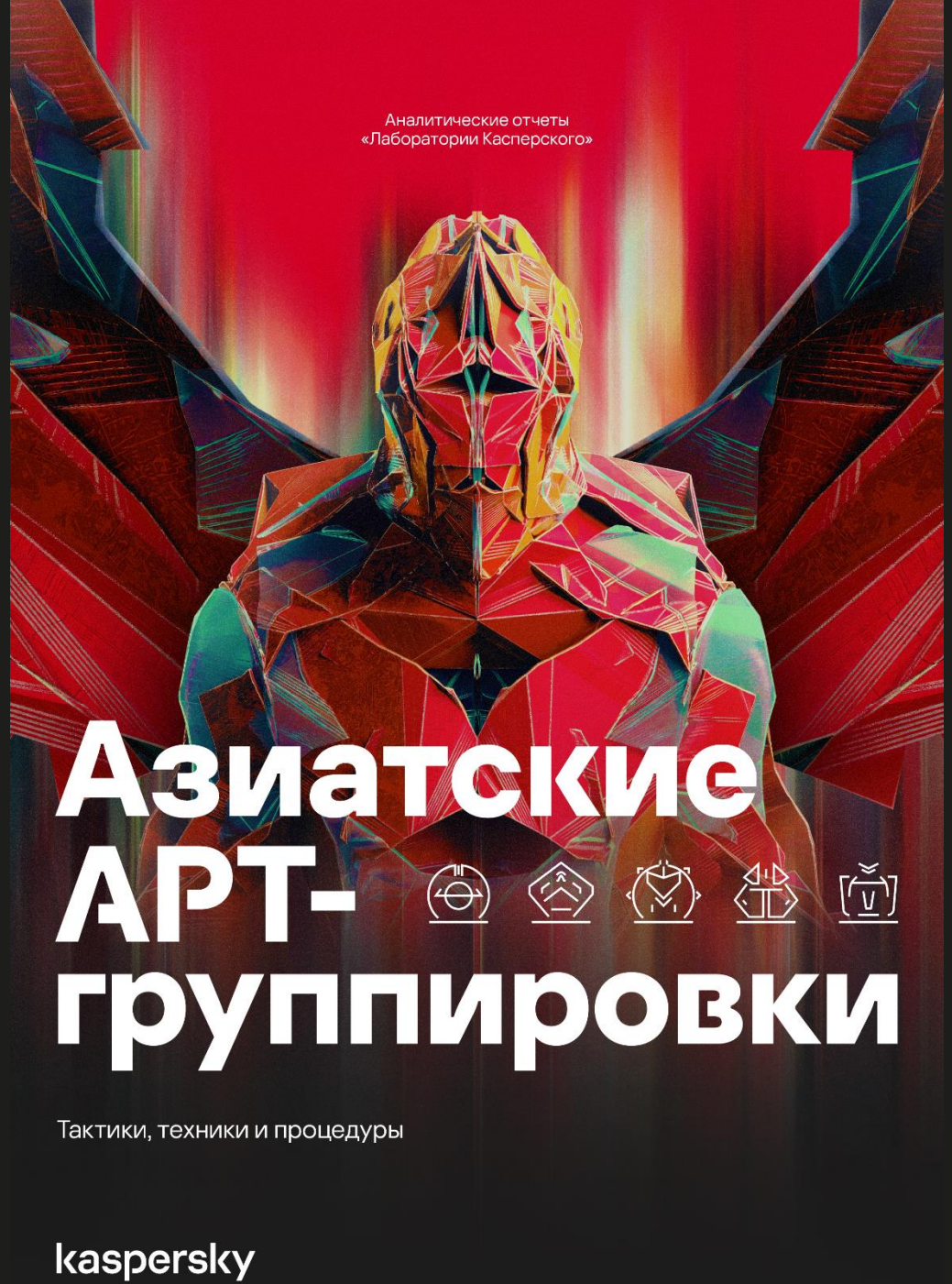
Ender's Game

Команда Kaspersky Cyber Threat Intelligence

Команда Kaspersky Cyber Threat Intelligence

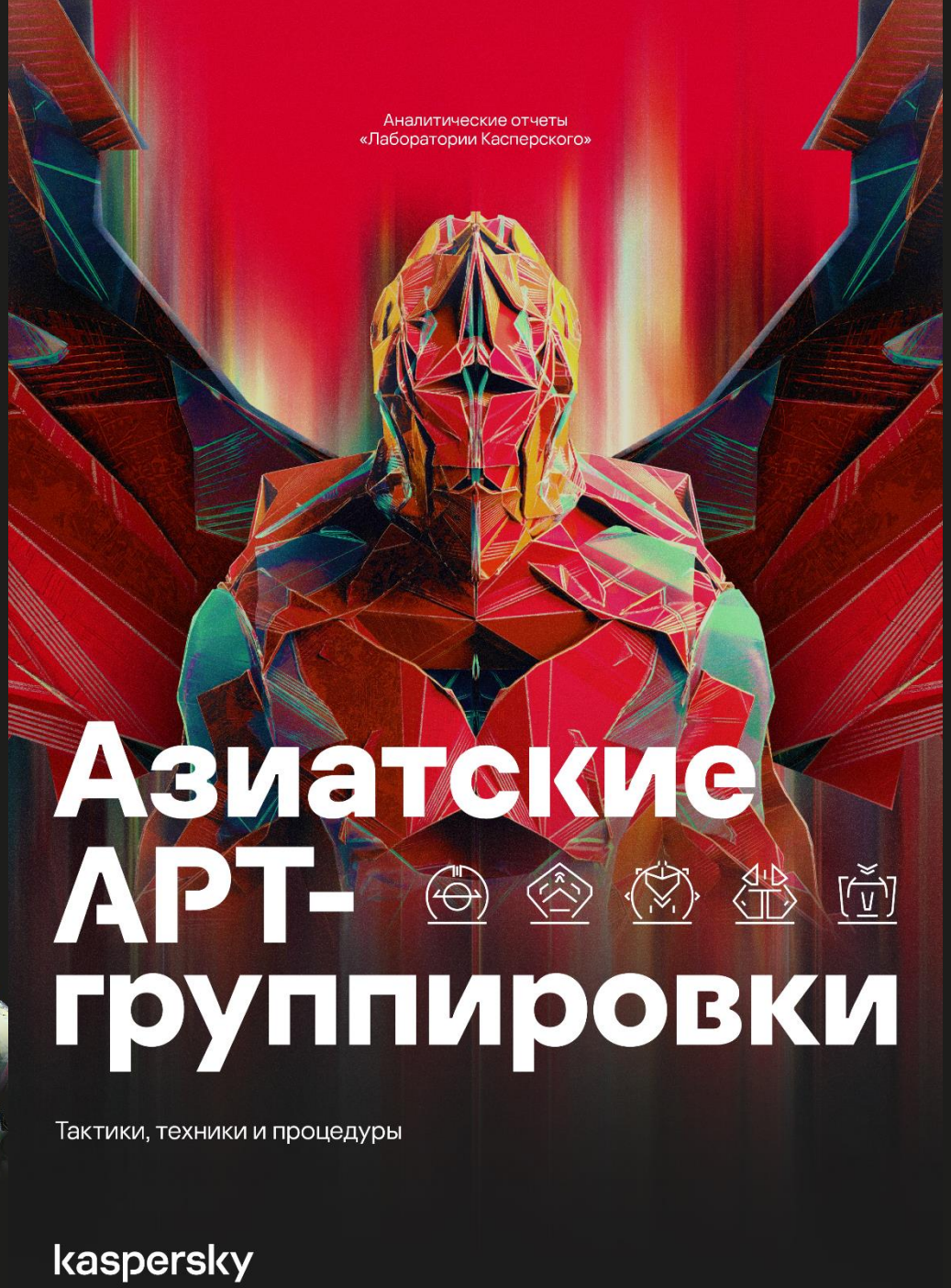
Как создавался этот отчет

- TTPs
- MITRE ATT&CK
- Pyramid of Pain
- Intelligence Driven Incident Response
- Unified Kill Chain



Как создавался этот отчет

- TTPs
- MITRE ATT&CK
- Pyramid of Pain
- Intelligence Driven Incident Response
- Unified Kill Chain



Структура отчета

Данный отчет состоит из 6 основных разделов, в которых каждый читатель в зависимости от своих потребностей сможет найти то, что ему необходимо

1 Инциденты с азиатскими APT в разных уголках планеты

Данный раздел содержит информацию о 5 уникальных инцидентах, обнаруженных нами в разных точках мира. Каждый инцидент — это уникальный кейс в своей стране и индустрии, описывающий действия и TTPs злоумышленников. В конце раздела мы собрали сводную таблицу TTPs встретившихся нам APT-группировок в этих инцидентах. Данная таблица состоит из списка TTPs и пересечений их использования в этих инцидентах.

2 Технические детали

Раздел «Технические детали» содержит подробное описание отдельной техники, обнаруженной нами у азиатских APT-группировок. Каждая техника содержит:

Основное описание

Подробные технические данные, как работает данная техника

Примеры процедур

Обнаруженные нами примеры использования данной техники азиатскими APT

Обнаружение

Данные по подходам обнаружения описываемой техники, а также EventID событий различных агентов мониторинга для обнаружения данной угрозы

Sigma-правила

Список Sigma-правил, относящихся к этой технике. Сами Sigma-правила вы можете найти в Приложении Sigma

3 Анализ действий атакующих на основе Unified Kill Chain

Основываясь на Unified Kill Chain, мы создали собственную таблицу, связанную с азиатскими APT-группировками, с целью дать верхнеуровневое понимание по мотивации и почерку злоумышленников, а также предоставить данные, как могут продвигаться азиатские APT-группировки в потенциальных атаках.

4 Митигации

Раздел с описанием митигаций рисков, основанный на описанных TTPs.

5 Статистика по жертвам

Собранная статистика по жертвам азиатских группировок в мире, включающая разделение по странам и индустриям.

6 Приложение: Sigma

Приложение с Sigma-правилами, которые можно применять для обнаружения описанных техник в этом отчете.

Для кого этот отчет

- Аналитиков SOC
- Аналитиков Cyber Threat Intelligence
- Специалистов по цифровой криминалистике (DFIR)
- Специалистов по Threat Hunting
- Экспертов по кибербезопасности
- C-Level руководителей, ответственных за решения ИБ в организации

Пять инцидентов с азиатскими APT в разных уголках планеты

Инциденты с азиатскими APT в разных уголках планеты

Инцидент 1 — Россия и Беларусь

Инциденты с азиатскими APT в разных уголках планеты

Инцидент 2 — Индонезия

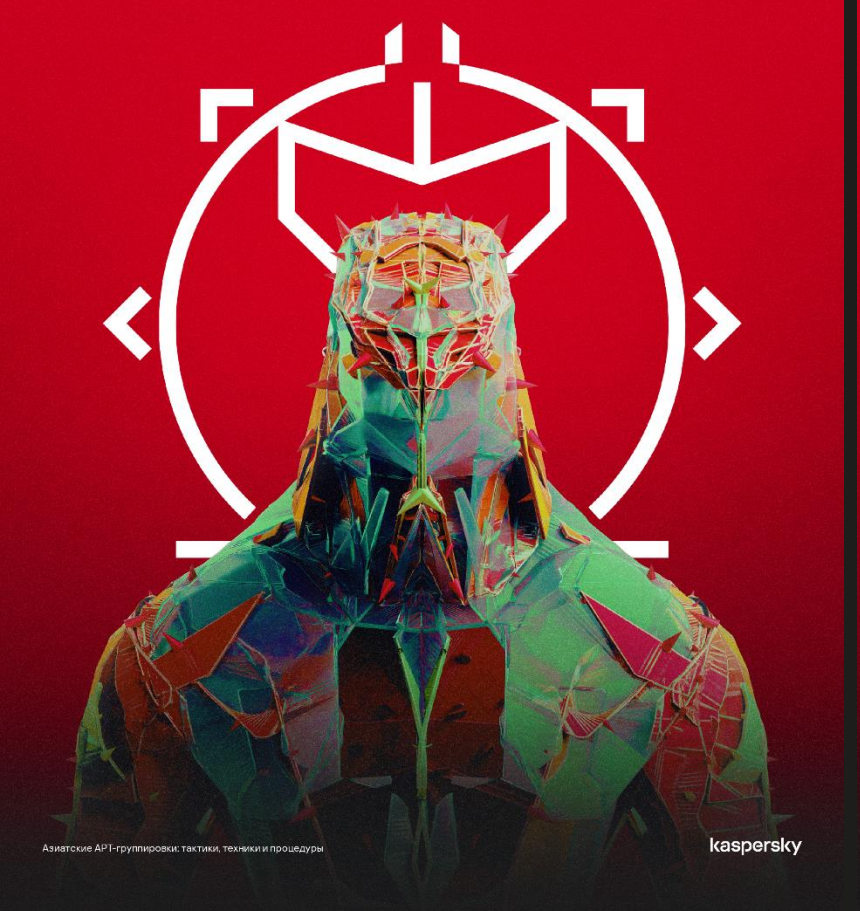
Инциденты с азиатскими APT в разных уголках планеты

Инцидент 3 — Пакистан

Пять инцидентов с азиатскими APT в разных уголках планеты

Инциденты с азиатскими APT в разных уголках планеты

Инцидент 3 — Пакистан



Инциденты с азиатскими APT в разных уголках планеты

Инцидент 4 — Малайзия

Инциденты с азиатскими APT в разных уголках планеты

Инцидент 5 — Аргентина

География жертв и C&C серверов

Рисунок 1 География жертв, упомянутых в разделе «Инциденты»

1. Россия
2. Беларусь
3. Индонезия
4. Пакистан
5. Малайзия
6. Аргентина

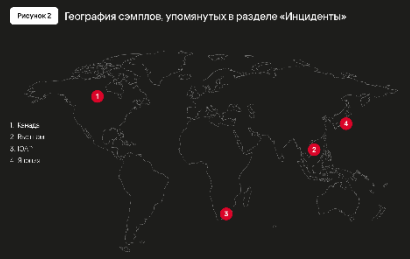


Рисунок 2 География сэмплов, упомянутых в разделе «Инциденты»

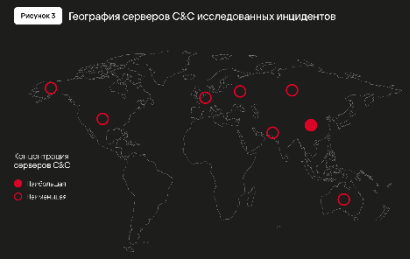
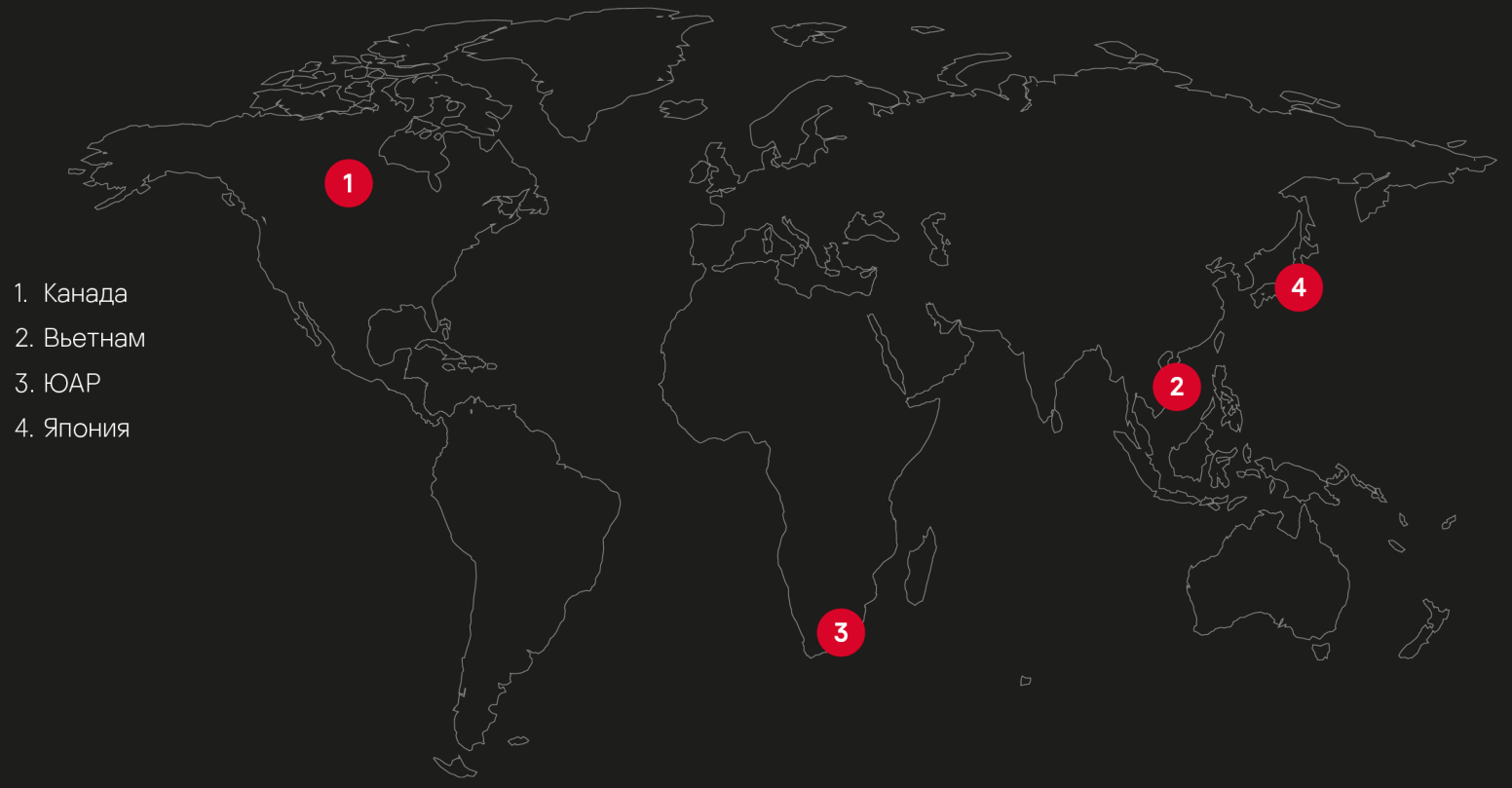


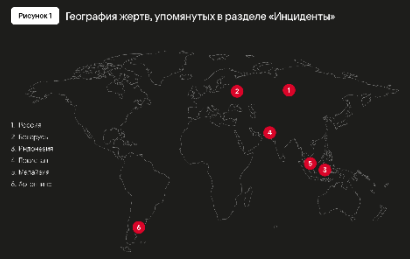
Рисунок 3 География серверов C&C исследованных инцидентов

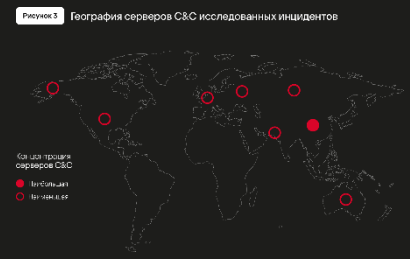
География жертв и C&C серверов

Рисунок 2 География сэмплов, упомянутых в разделе «Инциденты»



1. Канада
2. Вьетнам
3. ЮАР
4. Япония





География жертв и C&C серверов

Рисунок 1 География жертв, упомянутых в разделе «Инциденты»

Рисунок 2 География сэмплов, упомянутых в разделе «Инциденты»

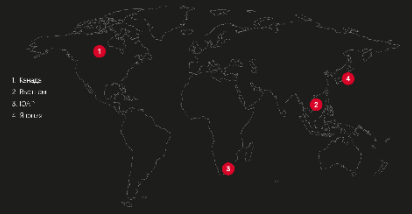


Рисунок 3 География серверов C&C исследованных инцидентов

Структура инцидента

Каждый инцидент — это уникальный кейс в своей стране и индустрии, описывающий действия и TTPs злоумышленников

Инцидент 1 — Россия и Беларусь

Сводка по жертве

Индустрия	Затронутые страны	Угроза
Госструктура	Россия, Беларусь	WebDav-O

Описание инцидента

В 2022 году нашими системами была обнаружена атака с использованием вредоносного ПО WebDav-O на государственную структуру в России. Ранее несколько исследователей описали серии атак с применением WebDav-O и Mail-O. Мы смогли проследить активность импланта WebDav-O в нашей телеметрии по крайней мере до 2018 года, указывающую на цели, базирующиеся в Беларуси и связанные с правительством. На основе нашего расследования мы смогли найти дополнительные варианты вредоносного ПО и наблюдать команды, выполняемые атакующими на скомпрометированных хостах.

Затем добавили описание службы и путь к вредоносной DLL в соответствующем ключе реестра для SQLReader и запустили службу:

```
reg add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SQLReader /v Description /t
REG_SZ /d "SQL Server VSS Reader"
reg add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SQLReader\Parameters /v
ServiceDll /t REG_EXPAND_SZ /d "C:\Windows\System32\sqlrder.dll"
sc start SQLReader
```

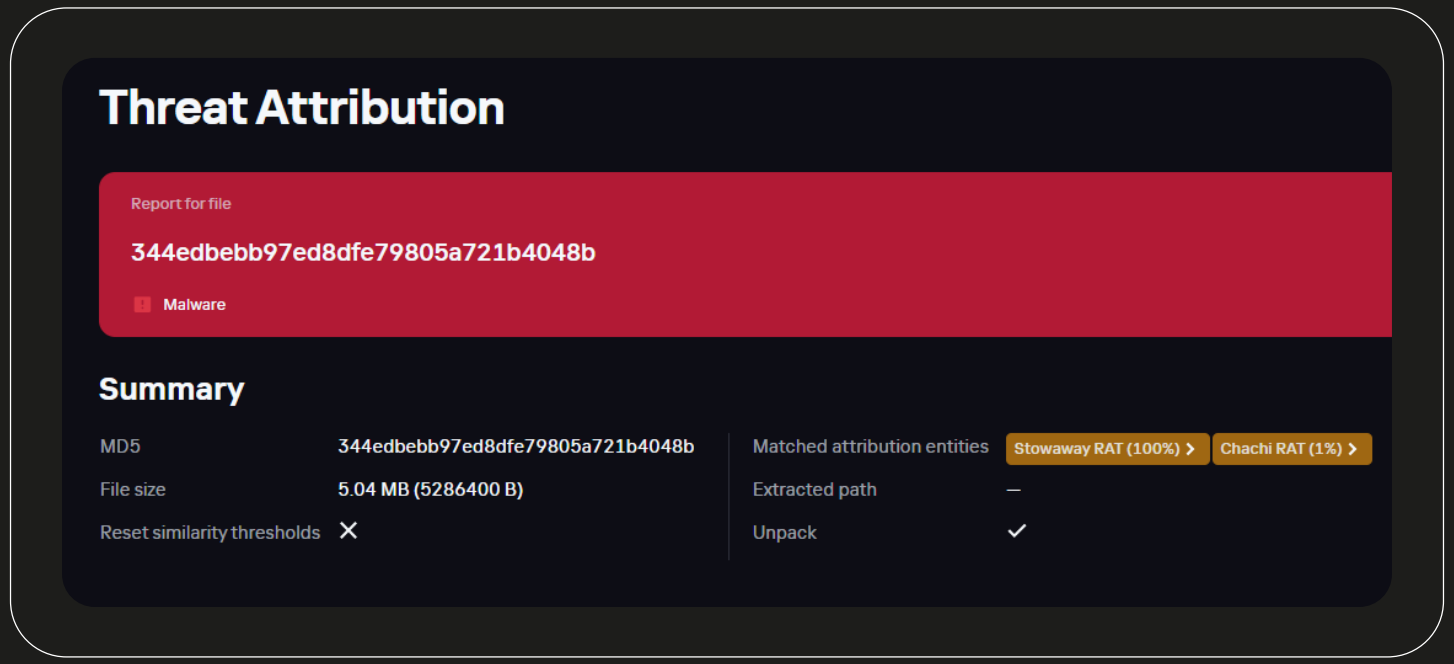
Итоги

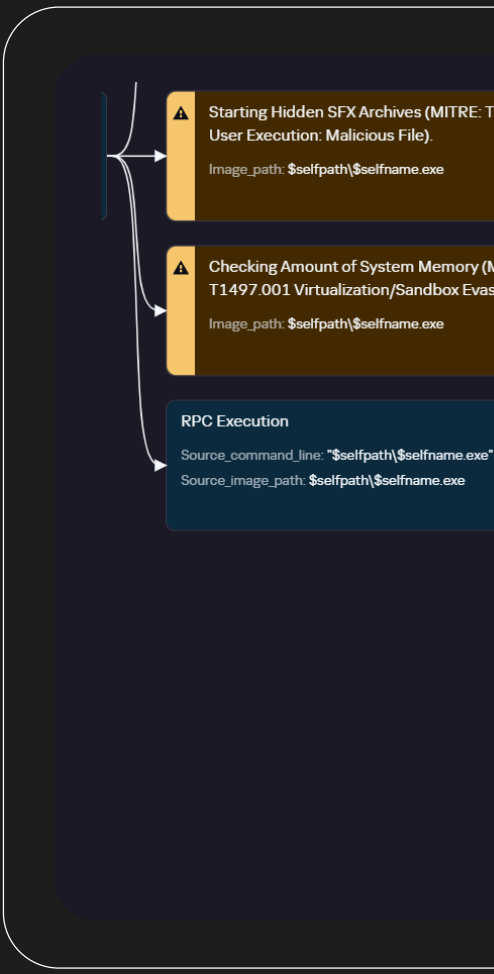
Описанная активность представляет собой продолжительную кампанию, направленную против одной из государственных структур России. Согласно нашей телеметрии, применение этого вредоноса было замечено также против Беларуси, в основном государственных структур. У этой активности есть некоторые связи с группой CoughingDown. У группы, ответственной за эту операцию, прослеживается высокая мотивация, основной целью является постоянное присутствие в инфраструктуре и шпионаж.

Скачать техники в формате .json для MITRE Navigator.

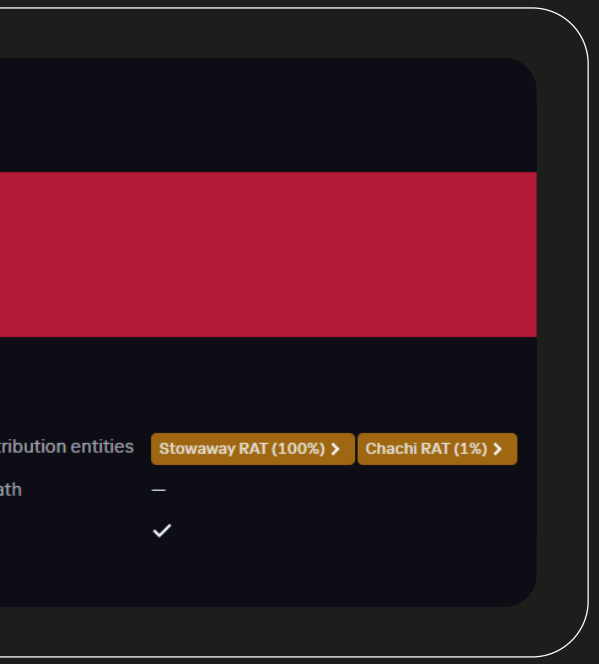
Подробнее

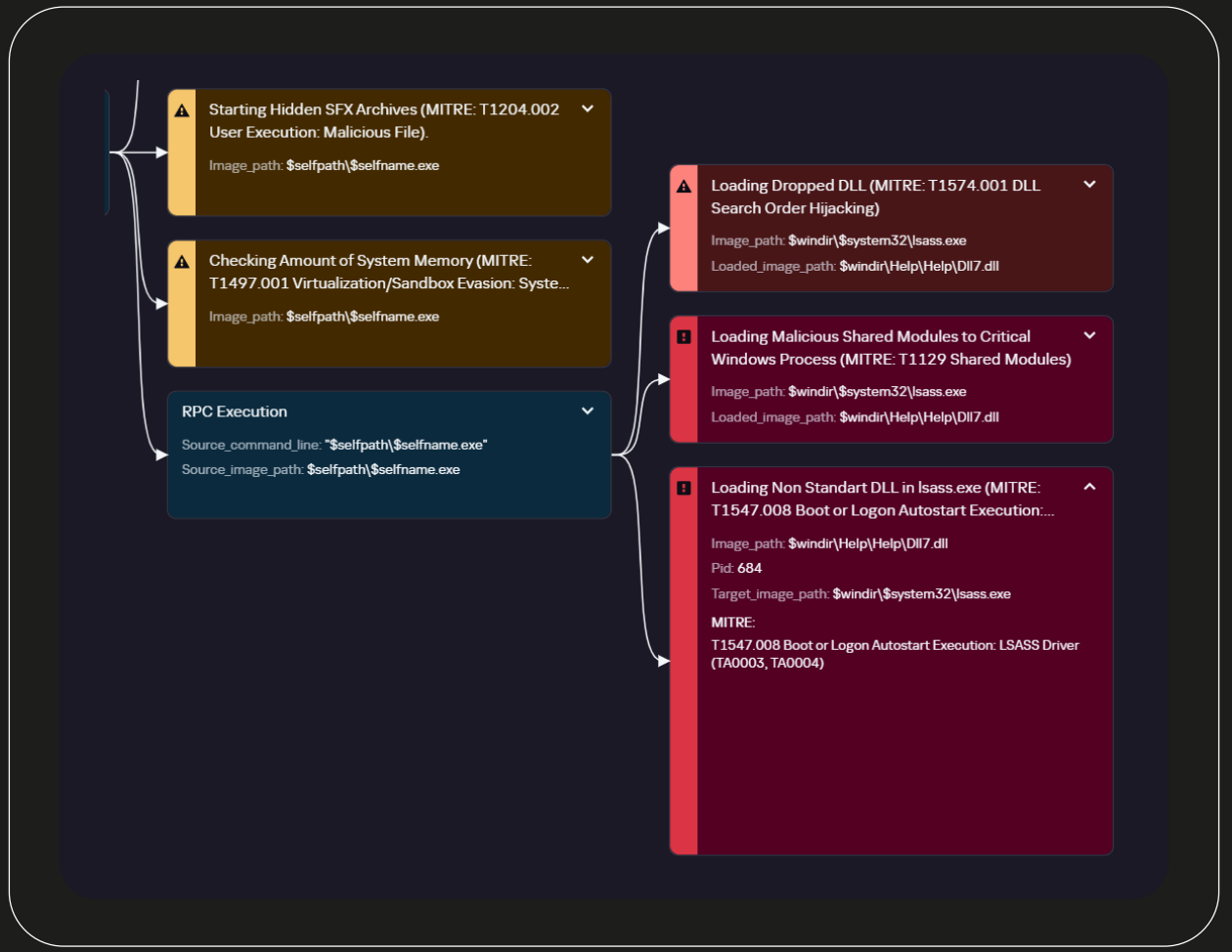
Kaspersky Threat Intelligence Portal

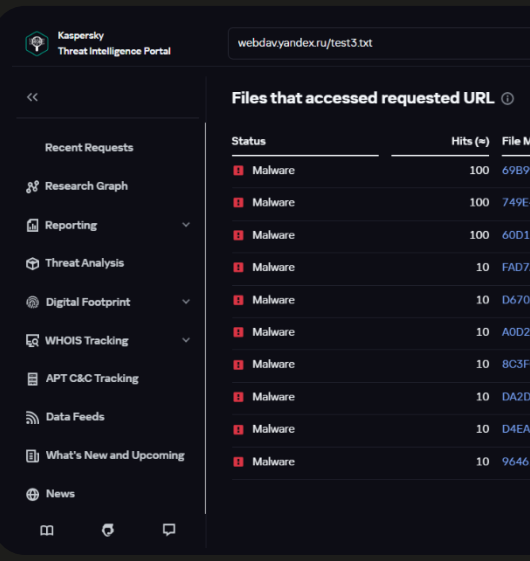




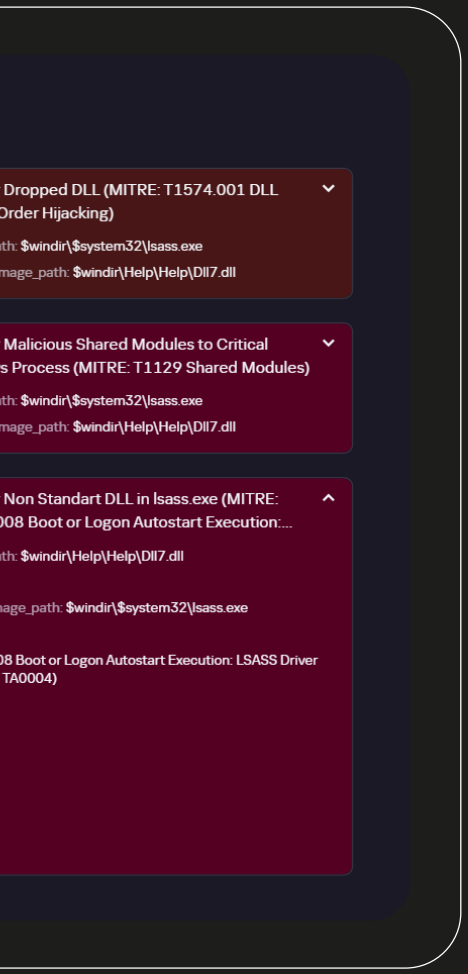
Kaspersky Threat Intelligence Portal

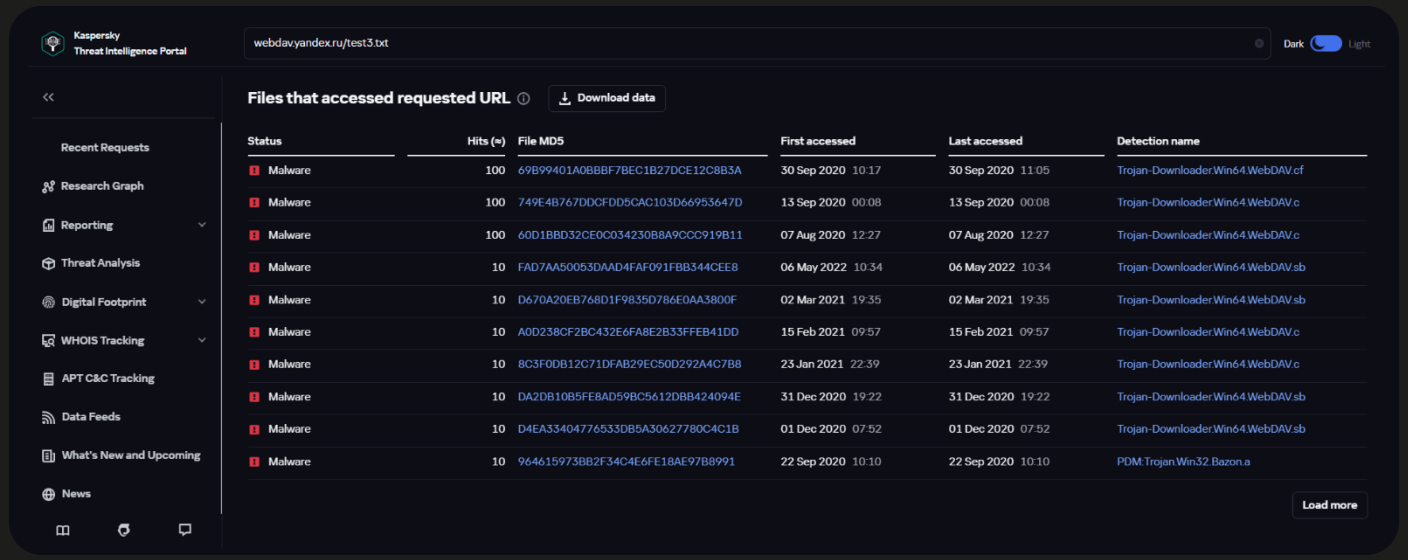


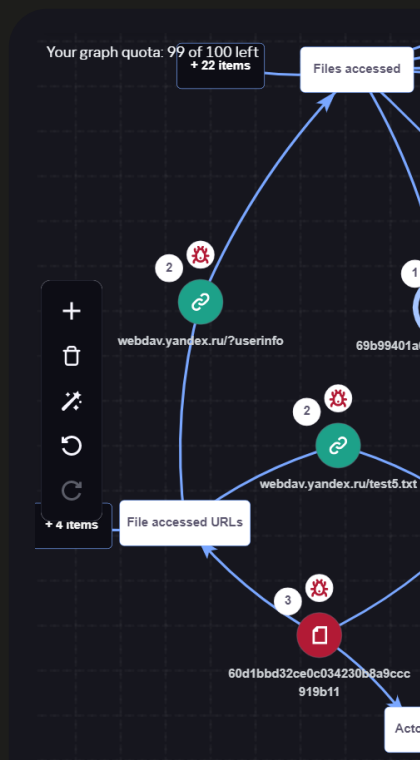




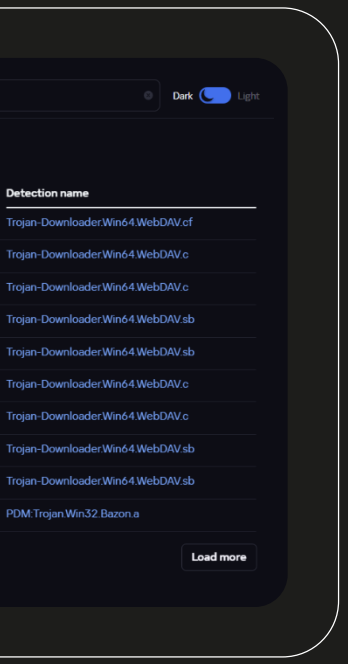
Kaspersky Threat Intelligence Portal

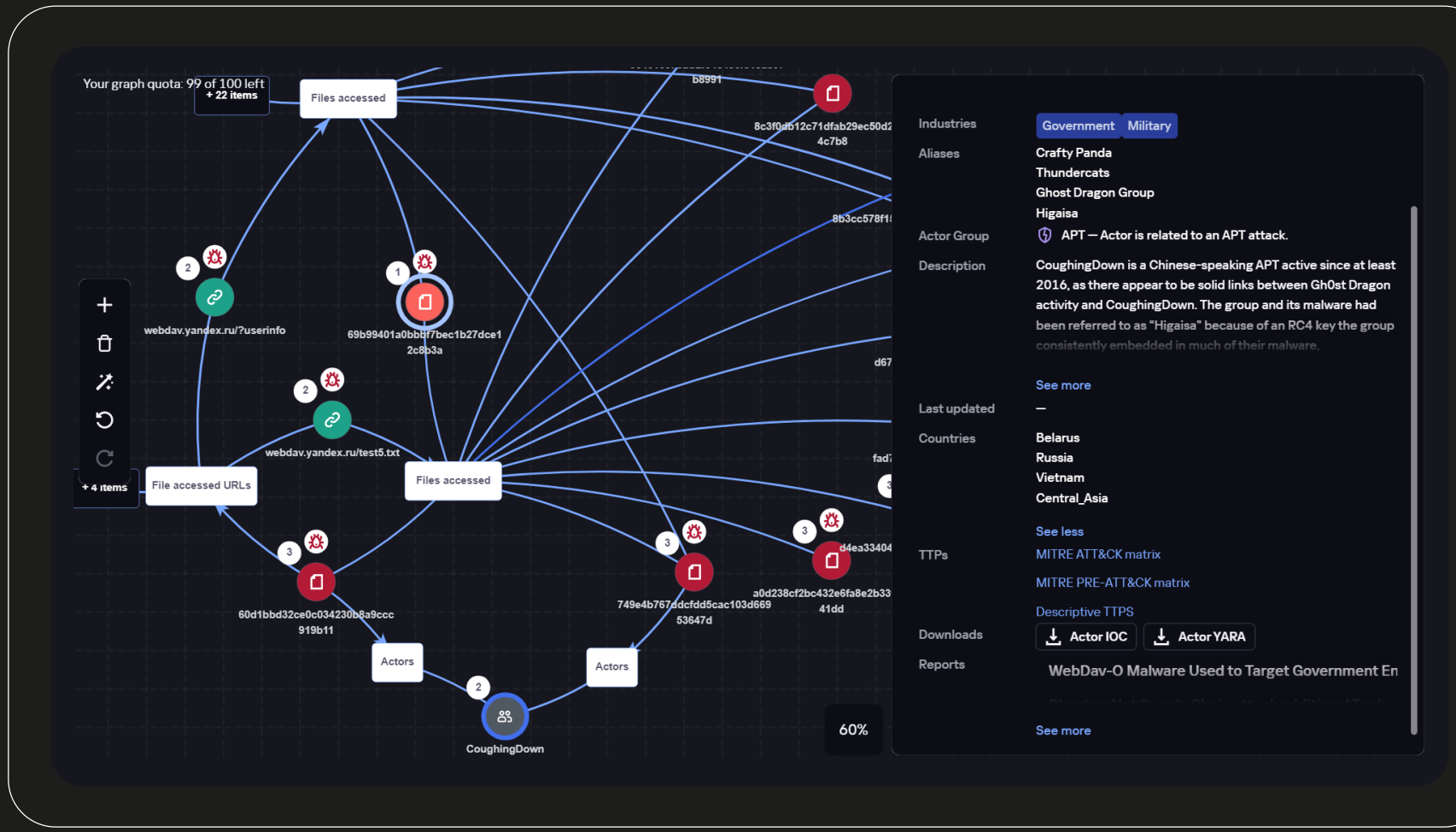






Kaspersky Threat Intelligence Portal





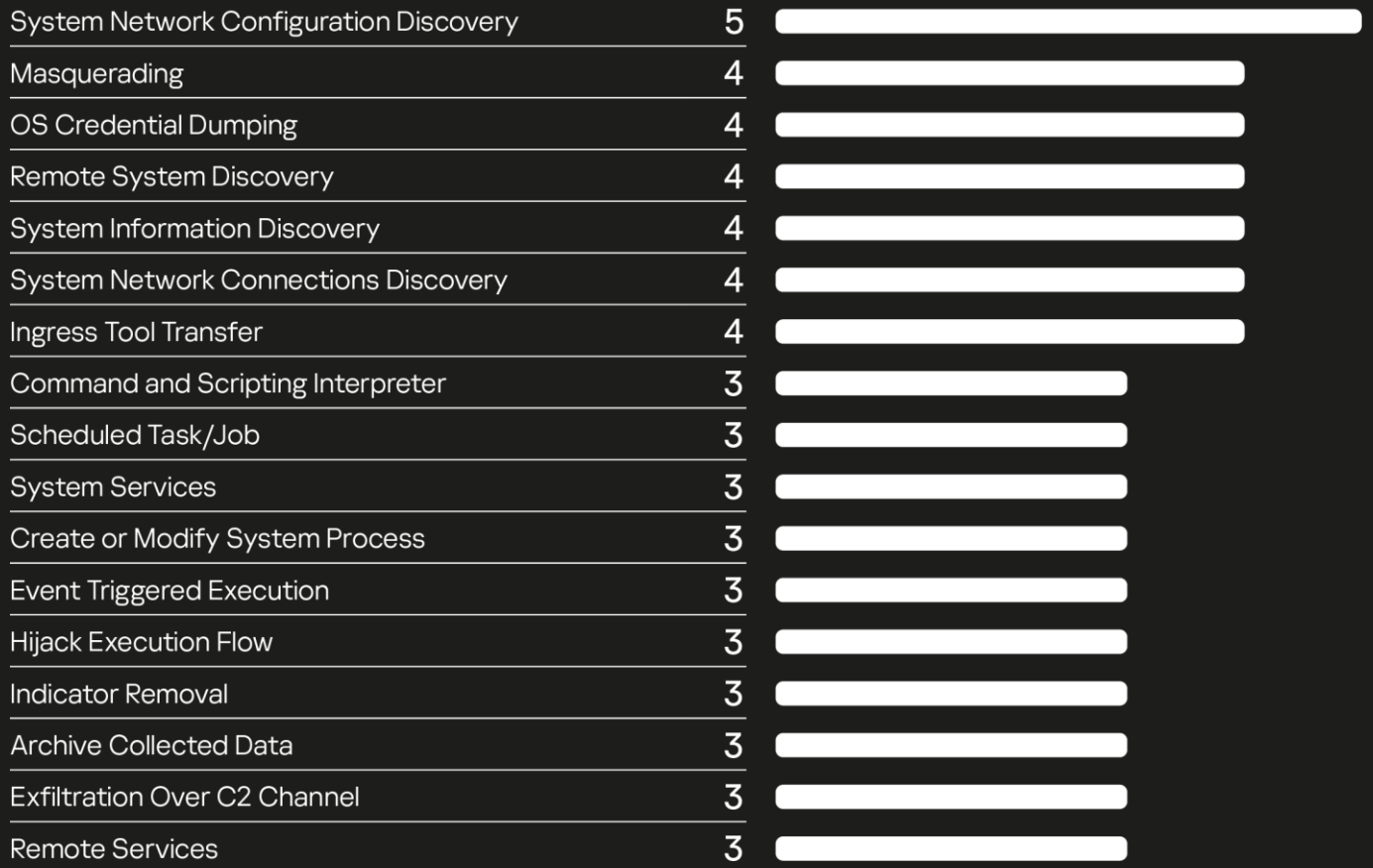
Итог рассмотренных инцидентов

Жертвы географически распределены по всему миру, и проблематично выявить какой-то отдельный более атакуемый регион

Отличительной чертой атакующих является связка техник Create or Modify System Process: Windows Service T1543.003 + Hijack Execution Flow: DLL Side-Loading T1574.002

Основными целями азиатских группировок являются кибершпионаж с эксфильтрацией собранных данных

Топ-20 техник, использованных в описанных инцидентах



Технические детали

Каждая из техник, задействованная в аналитическом отчете, сопровождается описанием, подходами к обнаружению, а также примерами процедур, использованных в атаках азиатских группировок

Во второй части отчета представлено подробное техническое описание большинства TTPs, обнаруженных нами в процессе анализа азиатских APT-группировок. Каждая описанная техника состоит из следующих подразделов:

Основное описание

Описание реализации техники.

Примеры процедур

Обнаруженные нами примеры использования техники азиатскими APT.

Обнаружение

Подходы к обнаружению техники, а также EventID событий различных агентов мониторинга, на основе которых можно выстроить обнаружение.

Пример:

Источник событий	Журнал	Event ID
Windows	System	7045
Windows	Security	4688
Sysmon	Sysmon	1, 13

Sigma-правила

Список Sigma-правил, относящихся к этой технике. Сами Sigma-правила находятся в разделе Sigma.

- Sigma-Generic-Anomaly in the Windows Critical Process Tree
- Sigma-Generic-Svchost.exe Start with no Standard Parameters

Masquerading T1036

Техника Masquerading T1036 является наиболее простой с точки зрения понимания ее работы и детектирования. Несмотря на свою простоту, она является крайне надежным индикатором присутствия, атакующего в инфраструктуре

Masquerading T1036

Основное описание

Техника Masquerading T1036 является наиболее простой с точки зрения понимания ее работы и детектирования. Несмотря на свою простоту, она является крайне надежным индикатором присутствия атакующего в инфраструктуре. Эта техника является одним из методов, используемых азиатскими группировками, чтобы скрыть свою активность и обойти различные механизмы защиты. Она подразумевает использование легитимных процессов, файлов или команд, чтобы замаскировать вредоносную деятельность под нормальные операции или легитимные приложения. Злоумышленник может прибегать к методам запуска уже знакомых наименований процессов в операционной системе, создания файлов с легальным наименованием в общедоступных директориях, запускать службы со знакомым наименованием процессов и описаний служб.

Проанализировав десятки инцидентов по всему миру, мы собрали топ наиболее частых директорий, куда азиатские APT помещают свои исполняемые файлы во время атаки.

Встречается в подавляющем большинстве случаев (отсортировано по популярности):

- C:\Windows\Temp
- C:\Windows\tasks
- C:\Windows\help
- C:\Windows\help\help
- C:\Intel
- C:\intel\logs
- C:\perflogs
- C:\system

Мы рекомендуем обращать пристальное внимание на создание исполняемых файлов в этих директориях от незнакомых процессов или учетных записей.

Также по нашим наблюдениям в подавляющем большинстве при выполнении техники Hijack Execution Flow: DLL Side-Loading T1574.002 противник старается расположить легитимный исполняемый файл и вредоносную библиотеку по следующим путям:

- C:\Program Files
- C:\ProgramData

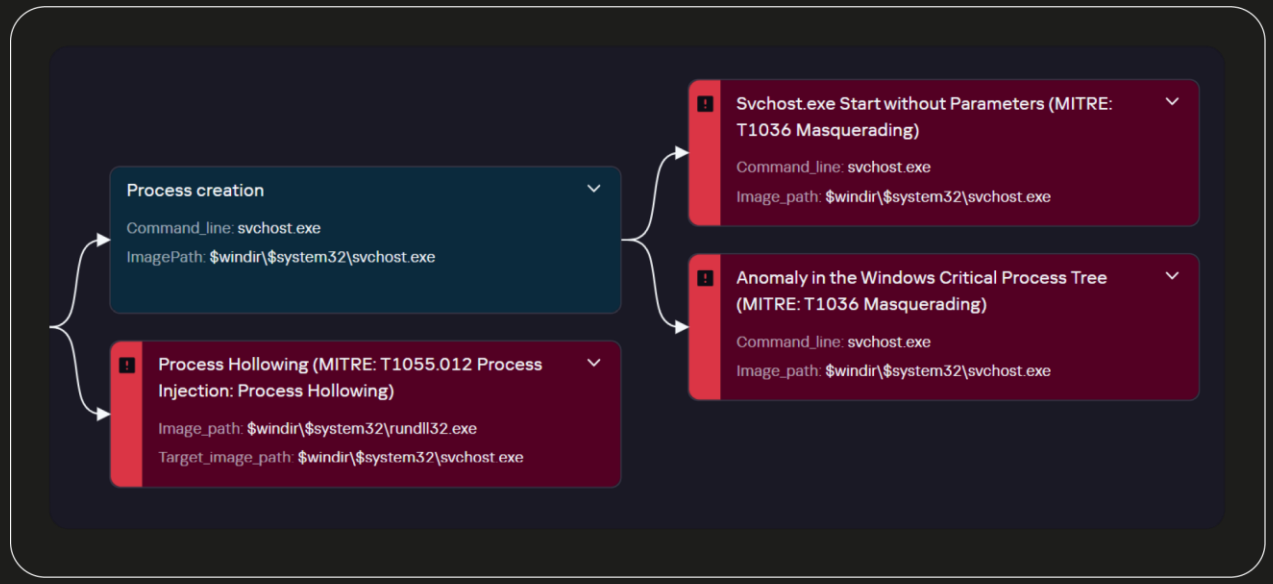
В этом случае тяжело отслеживать создание всех исполняемых файлов в указанных директориях, так как в них хранится большое количество легитимного программного обеспечения в операционной системе. Лучше всего подойдет профилирование программного обеспечения, которое разрешено и установлено на компьютерах у вас в домене. Азиатские APT предпочитают маскироваться под различные средства защиты информации, например:

Примеры процедур

Примеры процедур

Часто используемой разновидностью маскарадинга является мимикрия под легальные процессы операционной системы с целью создать препятствия специалистам информационной безопасности, анализирующим систему. В схеме этой процедуры у азиатских группировок можно выделить схожие паттерны. В основном это происходит на этапе выполнения техник Hijack Execution Flow: DLL Side-Loading T1574.002 и Process Injection: Process Hollowing T1055.012 (подробное описание в разделе техник). Атакующий доставляет вредоносную библиотеку и легальное программное обеспечение для перехвата потока выполнения и запуска своего кода в контексте легитимного процесса или производит инъекцию кода, используя возможность создания процесса в приостановленном состоянии. После чего создается процесс с легальным именем; уже после «замены» исполняемого файла в адресном пространстве процесса производится вредоносная активность. Эта активность обнаруживается посредством детектирования аномалий в родительских и дочерних процессах Windows.

Рисунок 52 Детектирование аномалий в родительских и дочерних процессах в Kaspersky TIP



Примеры процедур

Пример 1

Вредоносное ПО WebDav-O по пути C:\Windows\system32\conhost64.exe (conhost64.exe — выдуманное имя; настоящее — C:\Windows\system32\conhost.exe).

```
cmd.exe /c C: & cd\ & cd "" & dir \\<ip>\c$\windows\system32\conhost64.exe
cmd.exe /c C: & cd\ & cd "" & wmic /node:<ip> /user:<domain>\<username> /password:<password>
process call create "cmd /c $system32\conhost64.exe"
```

Пример 2

В кампании, направленной на государственное учреждение Тихоокеанского региона, атакующий использует архиватор, скрывающийся под именем процесса svchost.exe — C:\Windows\ime\svchost.exe (MD5: D263D26A2BE8D971273F6C9FA2EC6608).

```
C:\Windows\ime\svchost.exe  a -r -hpzxcv@wsx -ta20220627 C:\Windows\ime\microsoft.dat c:\*.doc*
d:\*.doc* e:\*.doc* c:\*.pdf* d:\*.pdf* e:\*.pdf* h:\*.doc* h:\*.xls* h:\*.pdf* f:\*.doc* f:\*.xls* f:\*.pdf* g:\*.doc*
g:\*.xls* g:\*.pdf*
```

Обнару-жение

Обнаружение

В процессе детектирования этой техники стоит опираться на материал Find Evil - Know Normal[11] от SANS Institute. Этот плакат представляет собой наглядное руководство для обнаружения вредоносной активности путем сравнения нормального поведения ОС с потенциально подозрительной или злонамеренной деятельностью. Он описывает нормальное поведение процесса, а также легитимные комбинации дочерних и родительских процессов. На события, являющиеся отклонением от нормы, стоит возводить алерт. Рекомендуем обратить внимание на наше правило Sigma-Generic-Anomaly in the Windows Critical Process Tree — этот хант неоднократно выручал нас в непростых ситуациях.

Дополнительно необходимо отслеживать события создания файлов, например, имеющих имя легитимного процесса, но необычное расположение в системе: C:\ProgramData\svchost**svchost.exe.** По этой же логике можно отслеживать события создания процессов.

[11] **Find Evil**

Подробнее

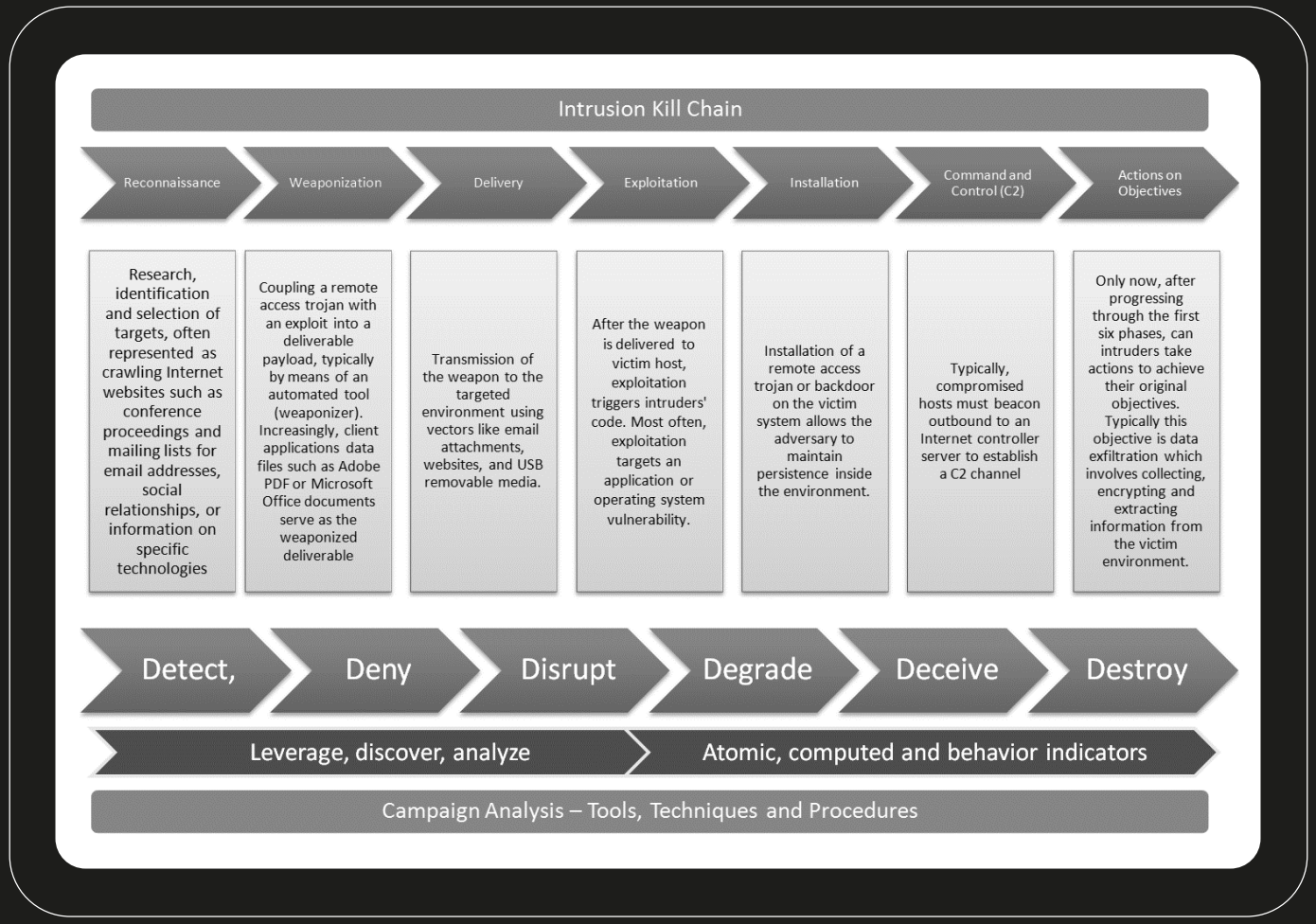
Источник событий	Журнал	Event ID
Windows	Security	4688
Sysmon	Sysmon	1, 11

Sigma-правила

- Sigma-Generic-Anomaly in the Windows Critical Process Tree
- Sigma-Generic-Svchost.exe Start with no Standard Parameters
- Sigma-Generic-Shell Creation by Critical Windows Process
- Sigma-Generic-Rundll32 Start with no Standard Parameters

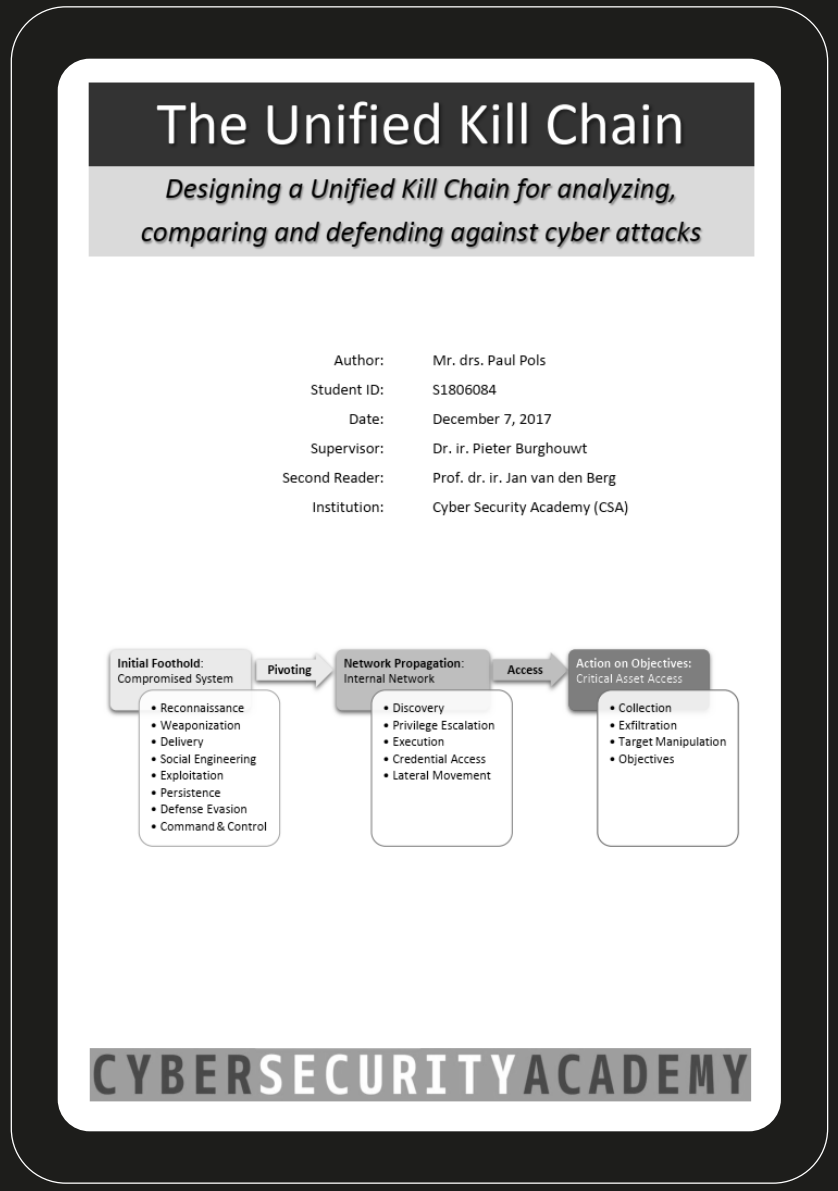
2011

Cyber Kill Chain



2017

Unified Kill Chain



The Unified Kill Chain

Designing a Unified Kill Chain for analyzing, comparing and defending against cyber attacks

Author: Mr. drs. Paul Pols
Student ID: S1806084
Date: December 7, 2017
Supervisor: Dr. ir. Pieter Burghouwt
Second Reader: Prof. dr. ir. Jan van den Berg
Institution: Cyber Security Academy (CSA)

CYBERSECURITYACADEMY

2017

Unified Kill Chain

Последовательность этапов атаки в Unified Kill Chain

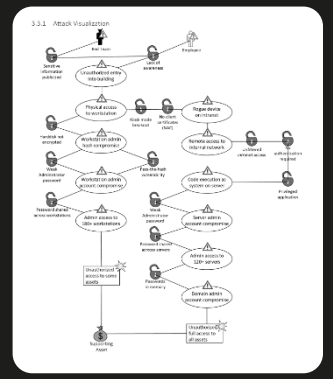
1	Reconnaissance	Поиск, идентификация и выбор целей с помощью активной или пассивной разведки.
2	Resource Development	Подготовительные действия, направленные на создание инфраструктуры, необходимой для проведения атаки.
3	Delivery	Техники передачи вредоносного объекта в целевую инфраструктуру.
4	Social Engineering	Методы манипулирования людьми для выполнения действий, нужных атакующему.
5	Exploitation	Методы эксплуатации уязвимостей, которые могут привести к выполнению вредоносного кода.
6	Persistence	Любые действия, направленные на сохранение постоянного доступа к целевой системе.
7	Defense Evasion	Методы уклонения от обнаружения или обхода средств защиты.
8	Command & Control	Методы взаимодействия с командными центрами из целевой сети.
9	Pivoting	Туннелирование трафика через контролируемую систему к другим системам, к которым у атакующих нет прямого доступа.
10	Discovery	Техники, позволяющие злоумышленнику получить информацию о системе и ее сетевом окружении.
11	Privilege Escalation	Методы повышения привилегий в системе или сети.
12	Execution	Техники, которые приводят к выполнению кода, контролируемого злоумышленником, в локальной или удаленной системе.
13	Credential Access	Техники, позволяющие получить доступ или контроль над учетными данными системы, сервиса или домена.
14	Lateral Movement	Техники, позволяющие злоумышленнику горизонтально перемещаться и управлять удаленными системами.
15	Collection	Техники, используемые для идентификации и сбора данных в целевой сети перед их эксфильтрацией.
16	Exfiltration	Техники, которые помогают злоумышленнику эксфильтровать данные из целевой сети.
17	Impact	Техники, направленные на управление, остановку или уничтожение целевой системы.
18	Objectives	Социально-технические цели атаки, предназначенные для достижения стратегической цели.

Unified Kill Chain

Обзор развития методологии
Unified Kill Chain (UKC)

#	Unified Kill Chain	Cyber Kill Chain® (CKC)	Lalliberte	Nachreiner	Bryant	Malone	MITRE ATT&CK™	UKC after literature study	UKC after Red Team C1	UKC after Red Team C2	UKC after Red Team C3	UKC after Red Team KC	UKC after APT28 C4 & KC
1	Reconnaissance	1	1	1	1	1		1	1	1	1	1	1
2	Weaponization	2	3	3	3	2		2	2	2	2	2	2
3	Delivery	3	5	5	6	3		7	7	3	3	3	3
4	Social Engineering	5	6	6	11	5		3	3	4	4	4	4
5	Exploitation	6	8	8	14	6		5	4	5	5	5	5
6	Persistence	8	14	9	18	8	6	6	5	6	6	6	6
7	Defense Evasion	18	18	14	16	10	11	8	6	7	7	7	7
8	Command & Control			18		5	7	9	8	8	8	8	8
9	Pivoting					11	13	11	9	9	9	9	9
10	Discovery					14	10	10	11	11	11	10	10
11	Privilege Escalation					17	14	14	10	10	10	11	11
12	Execution					18	12	12	14	14	14	12	12
13	Credential Access						15	13	12	12	12	13	13
14	Lateral Movement						16	17	13	13	13	14	14
15	Collection						8	15	17	17	17	17	15
16	Exfiltration							16	15	15	15	15	16
17	Target Manipulation								16	16	16	16	17
18	Objectives												18

Визуализация атаки физического проникновения в офис компании с использованием методов социальной инженерии



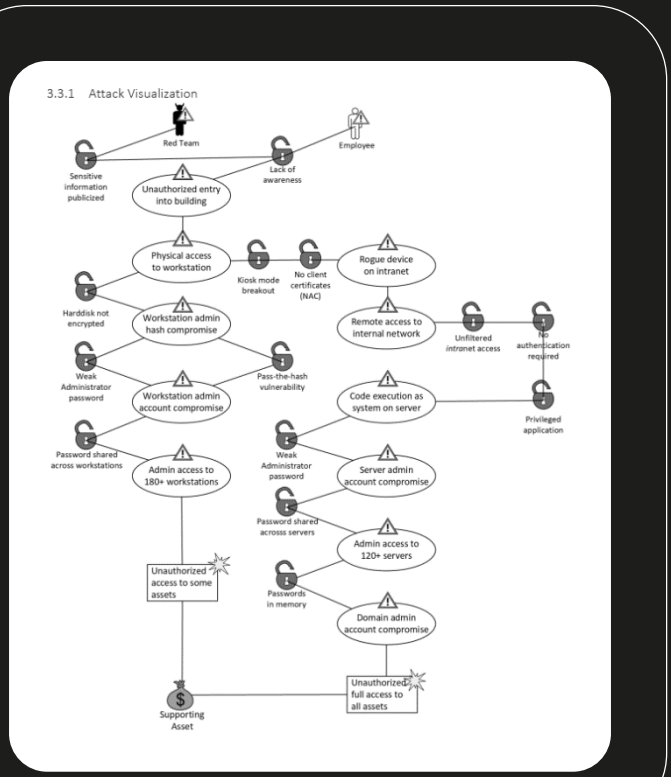
Обзор выявленных APT-тактик

Unified Kill Chain

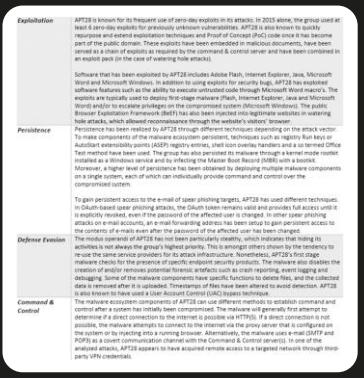
Визуализация атаки физического проникновения в офис компании с использованием методов социальной инженерии

Обзор развития методологии Unified Kill Chain (UKC)

#	Unified Kill Chain	Cyber Kill Chain® (CKC)	Lalliente	Nachtrainer	Bryant	Malone	MITRE ATT&CK™	UKC after literature study	UKC after Red Team C1	UKC after Red Team C2	UKC after Red Team C3	UKC after Red Team KC	UKC after APT28 C4 & KC
1	Reconnaissance	1	1	1	1	1		1	1	1	1	1	1
2	Weaponization	2	3	3	3	2		2	2	2	2	2	2
3	Delivery	3	5	5	6	3		7	7	3	3	3	3
4	Social Engineering	5	6	6	11	5		3	3	4	4	4	4
5	Exploitation	6	8	8	14	6		5	4	5	5	5	5
6	Persistence	8	14	9	18	8	6	6	5	6	6	6	6
7	Defense Evasion	18	18	14	16	10	11	8	6	7	7	7	7
8	Command & Control			18		5	7	9	8	8	8	8	8
9	Pivoting					11	13	11	9	9	9	9	9
10	Discovery					14	10	10	11	11	11	10	10
11	Privilege Escalation					17	14	14	10	10	10	11	11
12	Execution					18	12	12	14	14	14	12	12
13	Credential Access						15	13	12	12	12	13	13
14	Lateral Movement						16	17	13	13	13	14	14
15	Collection						8	15	17	17	17	17	15
16	Exfiltration							16	15	15	15	15	16
17	Target Manipulation								16	16	16	16	17
18	Objectives												18



Обзор выявленных APT-тактик

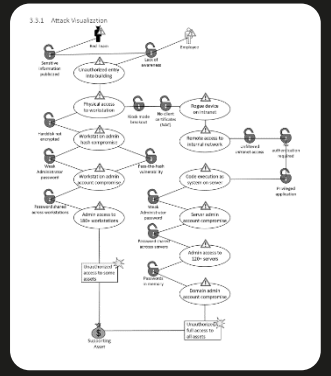


Unified Kill Chain

Обзор развития методологии
Unified Kill Chain (UKC)

#	Unified Kill Chain	Cyber Kill Chain® (CKC)	Lalliente	Nachreiner	Bryant	Malone	MITRE ATT&CK™	UKC after literature study	UKC after Red Team C1	UKC after Red Team C2	UKC after Red Team C3	UKC after Red Team KC	UKC after APT28 C4 & KC
1	Reconnaissance	1	1	1	1	1		1	1	1	1	1	1
2	Weaponization	2	3	3	3	2		2	2	2	2	2	2
3	Delivery	3	5	5	6	3		7	7	3	3	3	3
4	Social Engineering	5	6	6	11	5		3	3	4	4	4	4
5	Exploitation	6	8	8	14	6		5	4	5	5	5	5
6	Persistence	8	14	9	18	8	6	6	5	6	6	6	6
7	Defense Evasion	18	18	14	16	10	11	8	6	7	7	7	7
8	Command & Control			18		5	7	9	8	8	8	8	8
9	Pivoting					11	13	11	9	9	9	9	9
10	Discovery					14	10	10	11	11	11	10	10
11	Privilege Escalation					17	14	14	10	10	10	11	11
12	Execution					18	12	12	14	14	14	12	12
13	Credential Access						15	13	12	12	12	13	13
14	Lateral Movement						16	17	13	13	13	14	14
15	Collection						8	15	17	17	17	17	15
16	Exfiltration							16	15	15	15	15	16
17	Target Manipulation								16	16	16	16	17
18	Objectives												18

Визуализация атаки физического проникновения в офис компании с использованием методов социальной инженерии



Обзор выявленных
APT-тактик

Exploitation	APT28 is known for its frequent use of zero-day exploits in its attacks. In 2015 alone, the group used at least 6 zero-day exploits for previously unknown vulnerabilities. APT28 is also known to quickly repurpose and extend exploitation techniques and Proof of Concept (PoC) code once it has become part of the public domain. These exploits have been embedded in malicious documents, have been served as a chain of exploits as required by the command & control server and have been combined in an exploit pack (in the case of watering hole attacks). Software that has been exploited by APT28 includes Adobe Flash, Internet Explorer, Java, Microsoft Word and Microsoft Windows. In addition to using exploits for security bugs, APT28 has exploited software features such as the ability to execute untrusted code through Microsoft Word macro's. The exploits are typically used to deploy first-stage malware (Flash, Internet Explorer, Java and Microsoft Word) and/or to escalate privileges on the compromised system (Microsoft Windows). The public Browser Exploitation Framework (BeEF) has also been injected into legitimate websites in watering hole attacks, which allowed reconnaissance through the website's visitors' browser.
Persistence	Persistence has been realized by APT28 through different techniques depending on the attack vector. To make components of the malware ecosystem persistent, techniques such as registry Run keys or AutoStart extensibility points (ASEP) registry entries, shell icon overlay handlers and a so termed Office Test method have been used. The group has also persisted its malware through a kernel mode rootkit installed as a Windows service and by infecting the Master Boot Record (MBR) with a bootkit. Moreover, a higher level of persistence has been obtained by deploying multiple malware components on a single system, each of which can individually provide command and control over the compromised system. To gain persistent access to the e-mail of spear phishing targets, APT28 has used different techniques. In OAuth-based spear phishing attacks, the OAuth token remains valid and provides full access until it is explicitly revoked, even if the password of the affected user is changed. In other spear phishing attacks on e-mail accounts, an e-mail forwarding address has been setup to gain persistent access to the contents of e-mails even after the password of the affected user has been changed.
Defense Evasion	The modus operandi of APT28 has not been particularly stealthy, which indicates that hiding its activities is not always the group's highest priority. This is amongst others shown by the tendency to re-use the same service providers for its attack infrastructure. Nonetheless, APT28's first stage malware checks for the presence of specific endpoint security products. The malware also disables the creation of and/or removes potential forensic artefacts such as crash reporting, event logging and debugging. Some of the malware components have specific functions to delete files, and the collected data is removed after it is uploaded. Timestamps of files have been altered to avoid detection. APT28 is also known to have used a User Account Control (UAC) bypass technique.
Command & Control	The malware ecosystem components of APT28 can use different methods to establish command and control after a system has initially been compromised. The malware will generally first attempt to determine if a direct connection to the internet is possible via HTTP(S). If a direct connection is not possible, the malware attempts to connect to the internet via the proxy server that is configured on the system or by injecting into a running browser. Alternatively, the malware uses e-mail (SMTP and POP3) as a covert communication channel with the Command & Control server(s). In one of the analyzed attacks, APT28 appears to have acquired remote access to a targeted network through third-party VPN credentials.

Unified Kill Chain

Основываясь на Unified Kill Chain, мы создали собственную таблицу, связанную с азиатскими APT-группировками, с целью дать читателю понимание мотивации злоумышленников, а также предоставить данные, как могут продвигаться азиатские APT-группировки в потенциальных кампаниях

Этап	Техника	Описание
Persistence	T1546 T1546.003 T1546.012 T1546.015 T1197 T1078 T1078.002 T1053 T1053.005 T1543.003 T1505 T1505.003	Как показывают наши наблюдения, азиатские APT закрепляются внутри инфраструктуры многими процедурами и техниками, начиная с самых простых и заканчивая наиболее сложными: • Valid Accounts T1078 • Scheduled Task/Job T1053 • Windows Service T1543.003 • Windows Management Instrumentation Event Subscription T1546.003 • Image File Execution Options Injection T1546.012 • Component Object Model Hijacking T1546.015 Данный набор техник мы наблюдаем не в каждом обнаруженном инциденте, связанном с азиатскими APT. Это зависит от конкретной группировки и возможности применения той или иной техники в инфраструктуре жертвы. Но в подавляющем большинстве инцидентов с участием азиатских APT-групп мы наблюдаем один и тот же подход к закреплению. Это связка техник Create or Modify System Process: Windows Service T1543.003 + Hijack Execution Flow: DLL Side-Loading T1574.002 и дальнейшее применение Process Injection: Process Hollowing T1055.012 для избежания обнаружения действий атакующего. Данная связка примечательна тем, что техники относятся сразу к нескольким тактикам MITRE ATT&CK — закреплению, повышению привилегий, избежанию обнаружения, в результате чего атакующий занимает выгодную позицию для дальнейших действий атаки. Как мы уже описывали в разделе технических деталей, злоумышленник сперва доставляет вредоносную динамическую библиотеку и чистый исполняемый файл, уязвимый к DLL Hijacking, после чего создает службу Windows на основе принесенного на хост легитимного файла и запускает ее, в результате чего выполняется вредоносная библиотека. Далее злоумышленник прибегает к использованию техники Process Injection: Process Hollowing T1055.012, и процесс службы создает новый легитимный процесс в приостановленном состоянии, в который внедряет бэкдор для взаимодействия с командным центром. Для маскировки вредоносной службы, кроме использования техники DLL Side-Loading T1574.002, азиатские APT-группы часто создают службу, скрытую за процессом svchost.exe. Как результат — злоумышленник всегда имеет запущенный процесс с правами System, закрепленный через службу, от которого далее производит дальнейшие шаги в своей атаке.

Митигации

Мы собрали лучшие практики из NIST, NCSC, CISA, SANS в организованную структуру, которую можно применять в организациях

Меры, которые можно предпринять для снижения риска компрометации инфраструктуры

Hardening&Security

Комплекс мер по укреплению защиты инфраструктуры организации, в том числе выстраивание процессов BlueTeam:

- Security Operations (SOC)
- Threat Hunting (TH)
- Digital Forensics & Incident Response (DFIR)
- Cyber Threat Intelligence (CTI)

Asset Management

Процесс своевременной инвентаризации активов

Vulnerability Management

Процесс управления уязвимостями

Security Products

Внедрение EPP / EDR / Sandbox / IDS / IPS / Deception решений

Противодействие загрузке и запуску ВПО

- Блокировка вредоносных ресурсов
- Принцип наименьших привилегий
- Фильтрация входящего трафика
- Whitelisting соединений
- Patch Management
- Application Policies
- EPP и EDR
- DPI

In ⟶ **Through**

1. Reconnaissance
2. Resource Development
3. Delivery
4. Social Engineering
5. Exploitation
6. Persistence
7. Defense Evasion
8. Command & Control

9. Pivoting
10. Discovery
11. Privilege Escalation
12. Execution
13. Credential Access
14. Lateral Movement

Противодействие распространению по сети

- Сегментация сети
- Замена устаревших технологий
- Парольные политики
- Защита учётных данных
- Защита привилегированных учетных записей
- Использование приманок
- Использование ханипотов

In ⟶ Through

1. Reconnaissance
2. Resource Development
3. Delivery
4. Social Engineering
5. Exploitation
6. Persistence
7. Defense Evasion
8. Command & Control

9. Pivoting
10. Discovery
11. Privilege Escalation
12. Execution
13. Credential Access
14. Lateral Movement

Методология

Сэмплы, взятые из Kaspersky Security Network (KSN — сложная распределенная инфраструктура, предназначенная для интеллектуальной обработки потоков данных, связанных с киберугрозами и предоставляемых добровольно миллионами пользователей по всему миру), были поданы на вход Kaspersky Threat Attribution Engine. Те из них, которые были атрибутированы к азиатским APT-группировкам, были дополнительно обогащены информацией об индустрии и стране

Методология

Сэмплы, взятые из Kaspersky Security Network (KSN — сложная распределенная инфраструктура, предназначенная для интеллектуальной обработки потоков данных, связанных с киберугрозами и предоставляемых добровольно миллионами пользователей по всему миру), были поданы на вход Kaspersky Threat Attribution Engine. Те из них, которые были атрибутированы к азиатским APT-группировкам, были дополнительно обогащены информацией об индустрии и стране

75 алиасов разбиты на 8 основных группировок

Топ-5 по геолокации и Топ-3 по индустриям

Суммарно количество атакованных в % по категориям

Ограничение выборки

При интерпретации результатов нашей статистики важно помнить об ограничениях исследования. Следует отметить, что проанализировав более сотни различных инцидентов и тысячи образцов вредоносного ПО, связанных с азиатскими APT, объем проанализированной выборки не полностью отражает общий объем угроз и статистики по миру

APT-актор	Топ-5 по геолокации	Топ-5 стран по количеству атакованных (организаций)	Суммарное количество атакованных
APT41 Aliases: · Blackfly (Symantec) · Wicked Panda (CrowdStrike) · Winnti Group (Kaspersky) · Barium (Microsoft)	Египет Россия Иран Индия США	16% 12% 11% 7% 4%	13%
Vicious Panda Aliases: · Microcin · SixLittleMonkeys · Bronze Dudley (SecureWorks)	Россия Казахстан Китай Кыргызстан Таджикистан	38% 16% 14% 4% 3%	12%

APT-актор	Топ по индустриям	Топ по количеству жертв (организаций)
Stone Panda	Здравоохранение Госструктуры Промышленность	70% 27% 3%
Emissary Panda	Здравоохранение Госструктуры Промышленность	68% 28% 4%

Sigma-правила

В данном отчете мы предоставляем более сотни SIGMA-правил, которые вы можете использовать в своих SIEM системах, чтобы обнаруживать потенциальную активность азиатских APT-группировок

Техники	Sigma
Phishing: Spearphishing Attachment T1566.001	• Sigma-Generic-Shell Creation by Trusted Process • Sigma-Generic-Drop and execution file from a trusted process • Sigma-Generic-LNK Creation from Archive
Command and Scripting Interpreter: Windows Command Shell T1059.003	• Sigma-Generic-System Information Discovery via Standard Windows Utilities • Sigma-Generic-System Network Configuration Discovery via Standard Windows Utilities • Sigma-Generic-Remote System Discovery via Standard Windows Utilities • Sigma-Generic-File Download via Bitsadmin • Sigma-Generic-Ingress Tool Transfer via curl.exe • Sigma-Generic-Compress Data for Exfiltration via Archiver
Command and Scripting Interpreter: PowerShell T1059.001	• Sigma-Generic-PowerShell Suspicious Arguments • Sigma-Generic-Execution of Downloaded PowerShell Code • Sigma-Generic-PowerShell Code Execution from File • Sigma-Generic-PowerShell Code Execution from Registry
Windows Management Instrumentation T1047	• Sigma-Generic-Suspicious Command wmic.exe • Sigma-Generic-Suspicious Child Process Wmiprvse.exe • Sigma-Generic-System Service Discovery via wmic • Sigma-Generic-Permission Local Groups Discovery via wmic • Sigma-Generic-Security Software Discovery via wmic
Event Triggered Execution: Windows Management Instrumentation Event Subscription T1546.003	• Sigma-Generic-Changing MOF Self-Install Directory via Registry • Sigma-Generic-MOF file changing/creation
Event Triggered Execution: Image File Execution Options Injection T1546.012	• Sigma-Generic-Persistence by Image File Execution Options via Registry • Sigma-Generic-Accessibility Features Backdoor Installation via ifeo debugger • Sigma-Generic-Silent Process Exit Monitoring persistence via PowerShell • Sigma-Generic-Application Verifier Persistence via PowerShell • Sigma-Generic-Image File Execution Options Injection via SilentProcessExit • Sigma-Generic-Accessibility Features Backdoor Installation via SilentProcessExit Monitoring
BITS Jobs T1197	• Sigma-Generic-File Download via Bitsadmin • Sigma-Generic-Not Standard Parent Process Bitsadmin
Scheduled Task/Job: Scheduled Task T1053.005	• Sigma-Generic-Windows Shell Started Schtasks • Sigma-Generic-Suspicious Schtasks.exe Arguments • Sigma-Generic-Scheduled Task Start from Public Directory

Какие выводы можно сделать, ознакомившись с отчетом?

1 часть:

Азиатские APT особенно опасны для госструктур и промышленных предприятий

Успех этих атак объясняется слабым уровнем развития процессов ИБ в организациях жертв

У азиатских APT-группировок есть свой характерный почерк

Неверное мнение будто атаки азиатских APT настолько сложны и продуманы, что вероятность их вовремя обнаружить и остановить близка к нулю

2 часть:

Отчет можно использовать в качестве руководства по выстраиванию защиты от атак азиатских APT

Эффективная стратегия защиты включает правильно организованные процессы в SOC, защитные инструменты и специальные защитные механизмы

В самом начале отчета мы использовали цитату:

There is no teacher but the enemy.

В самом начале отчета мы использовали цитату:

There is no teacher
but the enemy.

Надеемся, что изучив материал, вы станете опытнее в защите от киберугроз.


Спасибо!
kaspersky