Unveiling the Arsenal

Exploring Attacker Toolsets and Tactics

WITH secure

Contents

Unveiling the Arsenal: Exploring Attacker Toolsets and Tactics

Introduction

Cybersecurity has become a crucial part of our digital age. The proliferation of cyber-attacks poses a significant threat to individuals, organizations, and governments alike. As we navigate this digital landscape, understanding the evolving tactics of cyber adversaries is paramount to our collective security.

With each passing day, cybercriminals become more sophisticated and resourceful[1], using a diverse arsenal of tools and techniques to breach networks, steal data, and disrupt critical operations. To defend against these evolving threats, it's vital to understand both attackers' objectives and the weapons they wield.

Attack Toolsets and Their Objectives

Defenders are continually engaged in an intricate battle with cyber adversaries. As organizations strengthen their defenses, attackers adapt, employing increasingly sophisticated toolsets to fly under the radar and achieve their objectives. Understanding these toolsets and their distinct objectives is important in safeguarding against cyber threats. Attackers have diverse objectives and motivations that drive their actions. Their goals range from financial gain through tactics like encrypting files via ransomware to data theft for purposes of espionage or intellectual property theft. Some aim to disrupt critical infrastructure, while others engage in hacktivism to promote their ideological causes. Understanding toolset and tactics, of such attacks, is of utmost importance in the cybersecurity landscape. To understand such attack strategies, let's break down the steps leading to a critical moment — data exfiltration.

The Quest for Data Exfiltration

Data exfiltration has become an attractive tactic for threat groups, especially, ransomware groups due to its potential for financial gain. Stolen data can be sold, it gives an adversary increased leverage over its victim, and it can have a long-term impact on targeted organizations or individuals. Even if a victim can decrypt their encrypted files or recover files from backup, they may still face significant costs and reputational damage if their stolen data is made public.

In this section, we navigate through a devised cyberattack, dissecting its orchestrated steps and uncovering the tools and tactics employed to achieve its primary objective of exfiltrating sensitive data.

Stage 1: Breaching the wall - Initial Access

Most organizations' crown jewels lie within their protected networks and systems. And most adversaries' ultimate goals are to access them. To do this, they first breach the target environment and then launch attacks, move laterally within the organization's networks, and eventually achieve their objectives. Final objectives may include data theft, system manipulation, or other malicious activities.

To achieve initial access, attackers utilize various techniques, each aimed at exploiting vulnerabilities or weaknesses in the target's security posture.

One of the most prevalent methods currently employed is phishing, whereby attackers steal credentials by sending deceptive emails or messages using widely accessible email services. These emails frequently contain malicious links hosted on external platforms. Attackers are known to craft convincing phishing emails using readily available open-source tools like SET (Social Engineer Toolkit).

Spear phishing and social engineering, a targeted variation, is in use too. Threat actors gather information from social media platforms like LinkedIn, research services like ZoomInfo, or company websites, to personalize their messages, making them even more effective.
In August 2023, WithSecure reported on Viet-

[1] The professionalization of cyber crime | WithSecure™

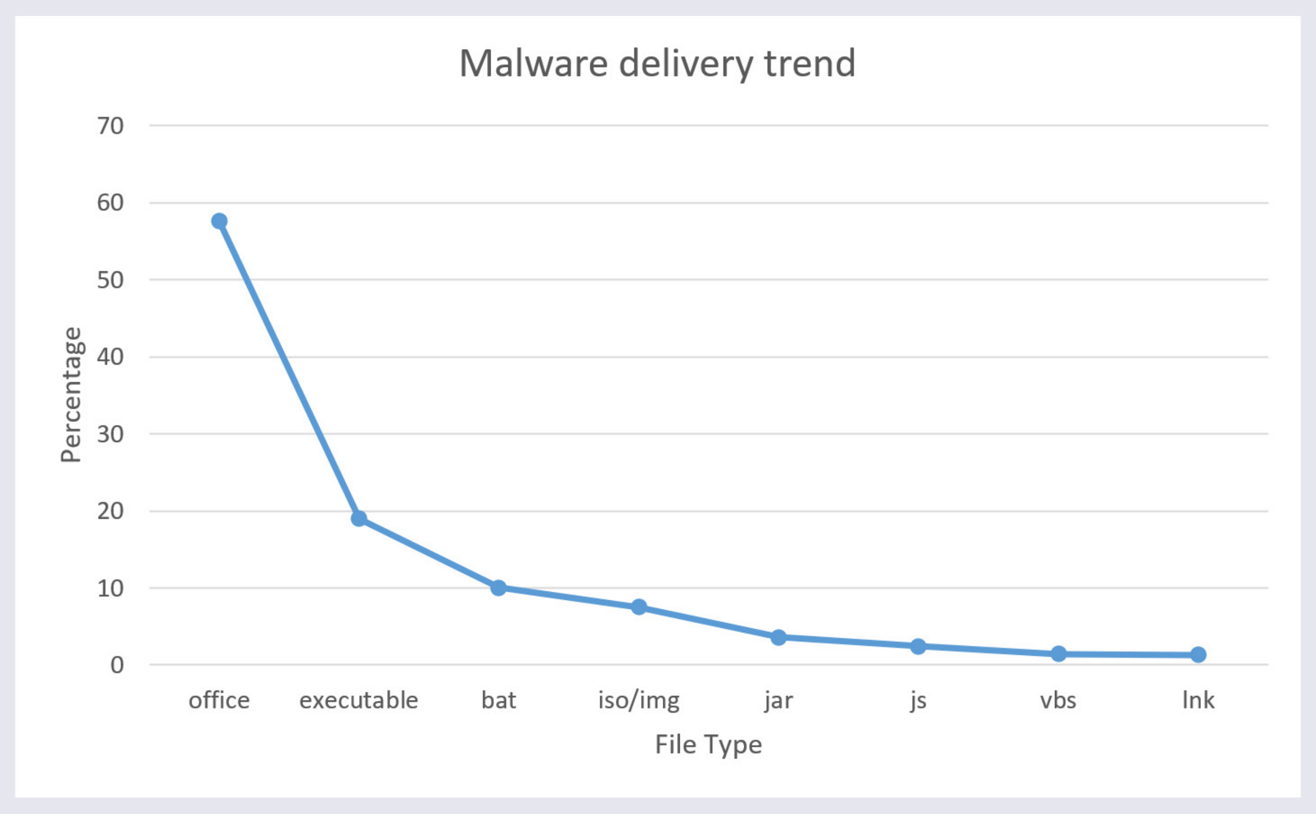


Figure 1: WithSecure Elements Collaboration Protection Malware delivery trend in 2023

namese threat groups targeting individuals through numerous platforms to gain access to Meta Business accounts[2].

Emails delivering malware as attachments represent a highly effective method employed by cybercriminals to compromise individuals and organizations. Malware delivery trends currently skew in favor of office-based files such as Word and Excel. Such documents may contain malicious links, excel formulas, or macros.

In parallel, attackers search for vulnerabilities in public-facing applications and external remote services, including Virtual Private Networks (VPNs), to secure an initial foothold in an organization's network. They utilize internet-scanning tools like Shodan or vulnerability scanners such as Nessus or Qualys to identify weaknesses in public devices and services. Once identified, these vulnerabilities are exploited using well-known tools such as Metasploit or custom-made exploit code.

Furthermore, attackers acquire valid credentials through a variety of means, including social engineering or other cyberattacks. This approach enables them to gain access using legitimate but stolen user information on services such as Windows Remote Desktop Protocol (RDP), SSH (Secure Shell), or VPN solutions like Cisco AnyConnect.

Brute force attacks, which involve repeatedly trying username and password combinations, are also utilized. Automation tools like Hydra or CrackMapExec are often used in these cases. For web applications, attackers rely on tools like Burp Suite to discover and exploit weak authentication mechanisms.

In essence, the world of initial access is not limited to malware alone. It encompasses a vast range of techniques, each with its own unique characteristics and strategies. Recognizing this diversity is pivotal for organizations in their efforts to stay ahead of evolving cyber threats and to secure their digital environments effectively

Stage 2: Identifying the Treasure Trove - Reconnaissance and Discovery

Once a threat actor has gained initial access into the target environment, they are largely unaware of what lies within the environment and how to traverse through its network and systems. Tools like Advanced Port Scanner, PINGCASTLE, Angry IP Scanner, Masscan, and Nmap are commonly deployed to map the target network. The objective here is to identify valuable assets

[2] Meet the Ducks: Vietnamese threat groups targeting Meta Business accounts | WithSecure™ Labs

like servers, databases, and mission-critical systems, discover vulnerabilities, and locate other potential entry points. Enumeration of the network, particularly of Active Directory, is one common step adversaries take. Tools like BloodHound play a pivotal role here, helping attackers map the relationships between users, groups, and devices within an Active Directory environment. This understanding of the network's structure is critical for future lateral movement steps.

Stage 3: Gaining the Master Key - Privilege Escalation

Having secured a foothold and scoured the environment for valuable assets, attackers set their sights on gaining sufficient privileges to access them. Tools such as Rubeus and Mimikatz play pivotal roles at this stage. They allow attackers to manipulate processes and system memory, steal or manipulate Kerberos tickets, and escalate their privileges within the network.

Stage 4: Covering Tracks - Defense Evasion

An intrusion won't take shape if the adversary is caught before, during, or after the attack. To evade detection and cover their tracks, attackers turn to various techniques and tools, including HRSWORD and Defender Control to obscure their actions, manipulate logs, eliminate digital breadcrumbs, and to bypass defensive controls and hinder investigative efforts.

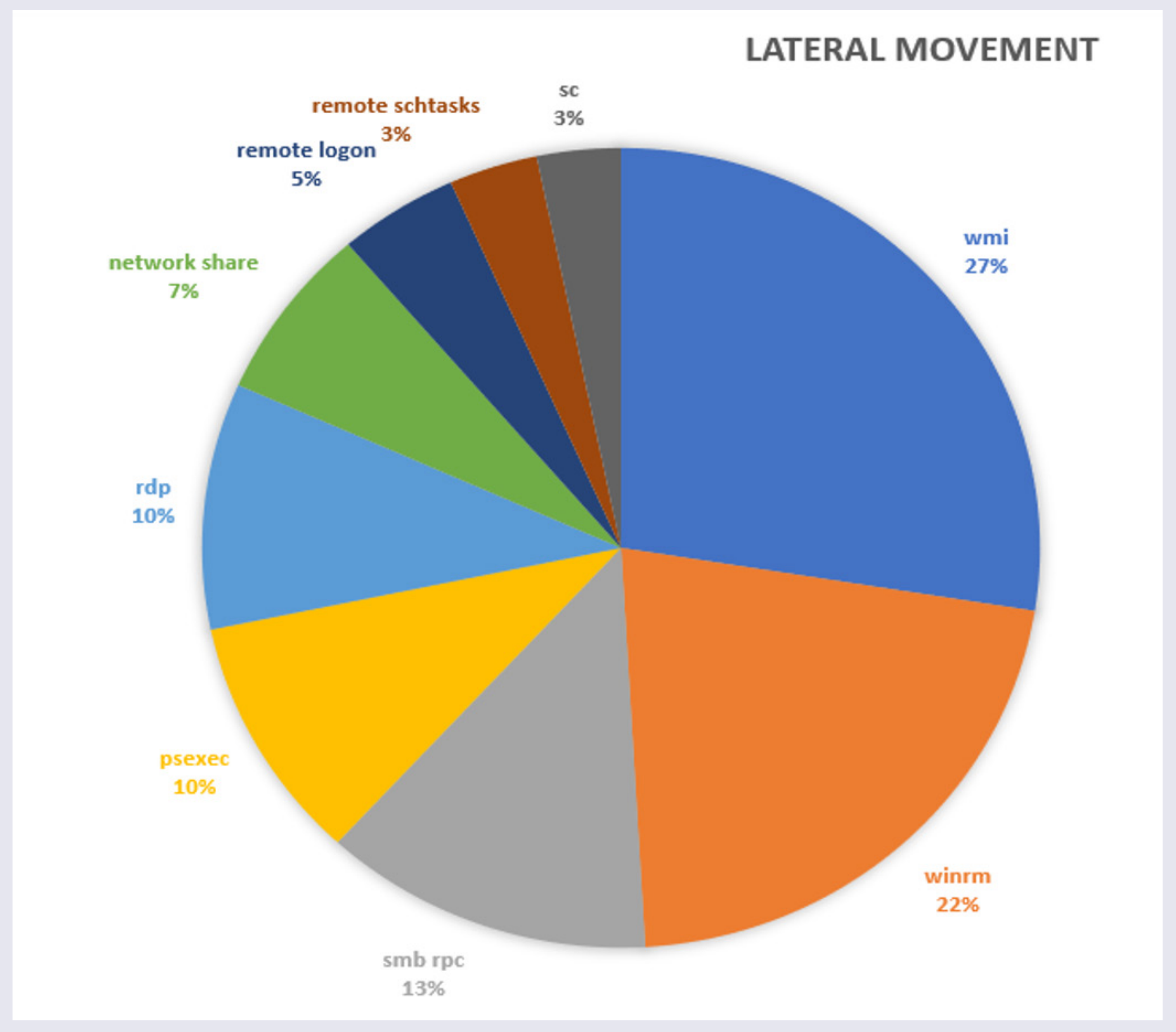
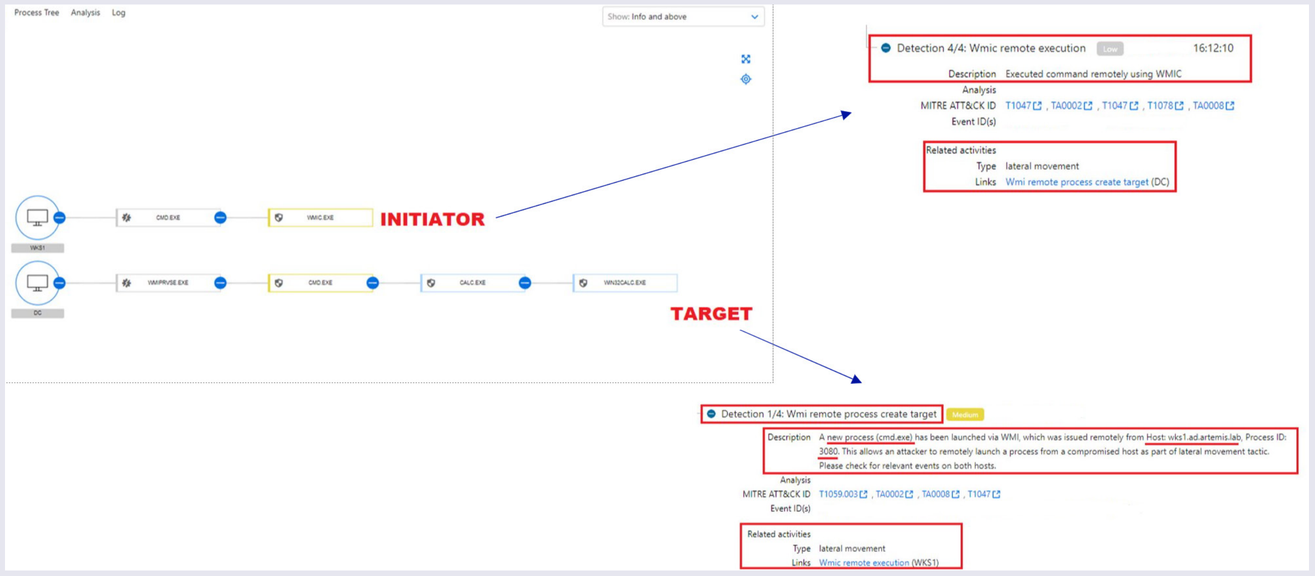


Figure 2: Lateral movement trends as seen in Elements EDR telemetry in 2023



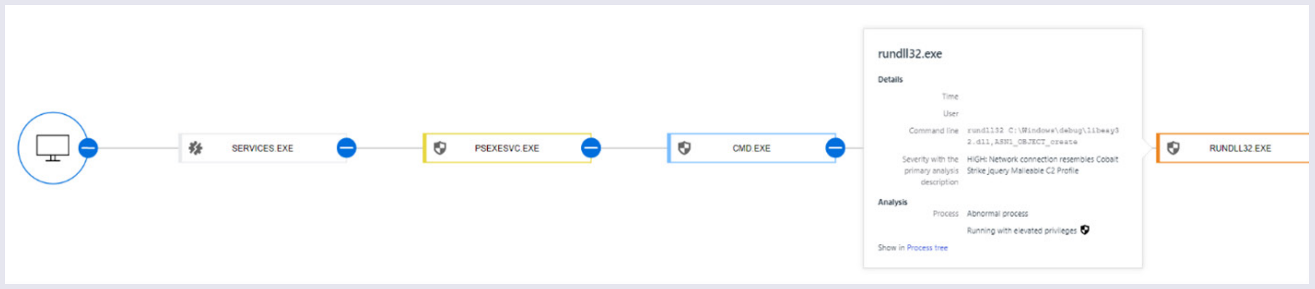
Detection 4/4: Wmic remote execution Low 16:12:10
Description Executed command remotely using WMIC
Analysis
MITRE ATT&CK ID T1047, TA0002, T1047, T1078, TA0008
Event ID(s)

Related activities
Type lateral movement
Links Wmi remote process create target (DC)

Detection 1/4: Wmi remote process create target Medium
Description A new process (cmd.exe) has been launched via WMI, which was issued remotely from Host: wks1.ad.artemis.lab, Process ID: 3080. This allows an attacker to remotely launch a process from a compromised host as part of lateral movement tactic. Please check for relevant events on both hosts.
Analysis
MITRE ATT&CK ID T1059.003, TA0002, TA0008, T1047
Event ID(s)

Related activities
Type lateral movement
Links Wmic remote execution (WKS1)

Figure 3: Lateral movement through WMI



rundll32.exe

Details
Time
User
Command line rundll32 C:\Windows\debug\libeay32.dll,ASN1_OBJECT_create
Severity with the primary analysis description HIGH: Network connection resembles Cobalt Strike jquery Malleable C2 Profile

Analysis
Process Abnormal process
Running with elevated privileges

Show in Process tree

Figure 4: Lateral movement through PSExec

Stage 5: Extending Influence - Lateral Movement

With the right privileges, attackers embark on a journey of moving laterally from one compromised system to another. Tools like PSEXEC and SHARPHOUND facilitate this activity, enabling remote command execution, identifying Active Directory trust relationships, and visualizing potential paths to data repositories.

Figure 2 provides a breakdown of techniques observed in lateral movement activities by WithSecure in 2023.

Windows Management Instrumentation (WMI) represents the most common method used by attackers. WMI can be invoked remotely in a compromised domain and can also be utilized for execution, persistence, discovery, and other post-breach activities. WMI can be interacted with programmatically and via built-in utilities such as wmic. Figure 3 exemplifies of how wmic can be used to launch a command prompt on another system.

Another notable method employed by attackers is the use of PSExec. Service control manager (SCM) supports remote procedure calls over both Transmission Control Protocol (RPC/TCP) and named pipes (RPC/NP). PSExec can be used to create services and launch PSEXESVC on a remote host. Figure 4 is an example where an adversary used PSEXESVC to launch a modified openssl library to set up a cobaltstrike beacon and then established persistence by configuring a scheduled task.

WithSecure Consulting's Attack Detection Fundamentals Workshop series explains such different aspects of lateral movement in-depth[3,4,5,6,7]

[3] Attack Detection Fundamentals: Discovery and Lateral Movement - Lab #1 | WithSecure™ Labs
[4] Attack Detection Fundamentals: Discovery and Lateral Movement - Lab #2 | WithSecure™ Labs
[5] Attack Detection Fundamentals: Discovery and Lateral Movement - Lab #3 | WithSecure™ Labs
[6] Attack Detection Fundamentals: Discovery and Lateral Movement - Lab #4 | WithSecure™ Labs
[7] Attack Detection Fundamentals: Discovery and Lateral Movement - Lab #5 | WithSecure™ Labs

Stage 6: Securing Access - Persistence

At this stage, attackers try to maintain a foothold within a system. Attackers utilize tools like Any-Connect and Ngrok to maintain secure, remote connections to compromised systems, ensuring they can return at will. Additionally, attackers leverage registry manipulations, scheduled tasks, and service modifications to create mechanisms that automatically execute their malicious code whenever the compromised system starts up.

Stage 7: The Grand Heist - Credential Theft and Data Exfiltration

The grand heist is the step that drives the entire operation. At this point, attackers employ tools such as LaZagne and NIRSOFTPASSVIEW to harvest stored passwords and credentials from compromised systems. These stolen credentials can grant access to additional accounts and resources within the network, expanding the attacker's reach. And finally, to exfiltrate the sensitive information and confidential data from compromised systems, attackers use tools such as WinSCP and RCLONE. The stolen data is then often used for extortion or black-market dealings. Understanding this sequence of events is important for defenders and organizations seeking to block attacks. There are numerous sequences of events that attackers may follow, and their tactics can vary widely based on their objectives, targets, and the vulnerabilities they exploit. These sequences are referred as "attack vectors" or "attack chains". Each attack chain is a unique combination of tactics, techniques, and procedures (TTPs) that attackers employ to achieve their goals.

In the following sections, we will dig deeper real-world cases, providing insights into their objectives, tactics, and mitigation strategies.

Attack Toolsets in Action

While we explored the theoretical aspects of cyberattacks and their toolsets, it's crucial to observe these concepts within real-world cases. In this section, we'll go through incidents seen in WithSecure EDR telemetry, which illustrate scenarios in which different toolsets were utilized by threat actors and the tangible impacts they had on target organizations and individuals.

The One with the Complete Set

In April 2023, WithSecure Detection and Response team responded to an incident where an attacker accessed a system via RDP and then went on to utilize numerous other tools to execute an attack. The adversary's arsenal contained a wide range of tools carefully chosen and deployed to ensure comprehensive coverage of the attack lifecycle.

Tools deployed by the attacker in this incident were:

- ToggleDefender
- Advanced Port Scanner
- Rubeus
- Anyconnect
- Zerologon
- ProxifierSetup
- WinSCP
- Secretsdump
- PortStarter

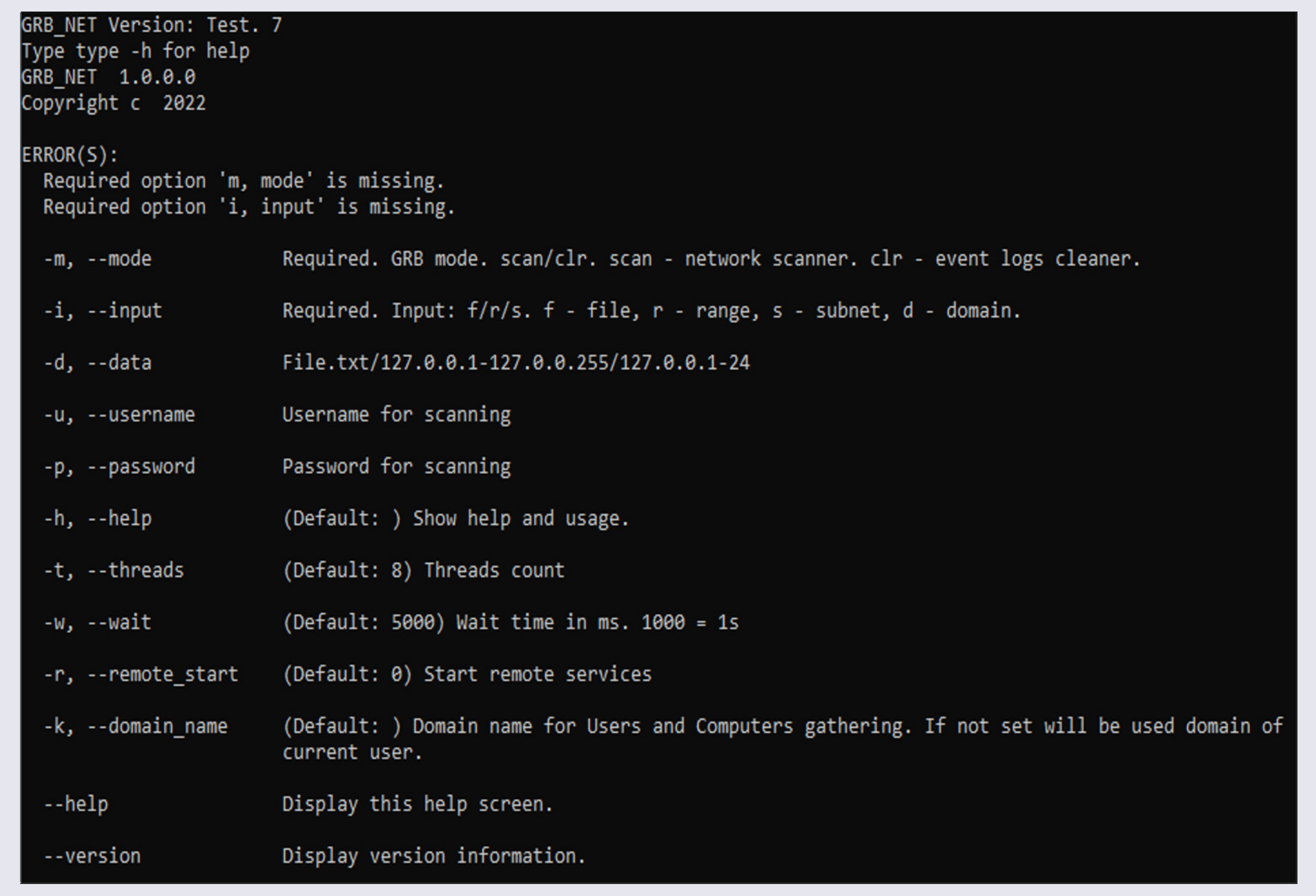
The tools were executed from an attacker's system through drive mapping via an RDP session. An example command line was: "%lan%\Client\C$\Users\Administrator\Desktop\Advanced_Port_Scanner_2.5.3869.exe"

ToggleDefender was employed to impair defenses by disabling and altering security tools.
It is designed to obstruct the security product's ability to detect and respond effectively.

Advanced Port Scanner was used for network service discovery, allowing the adversary to identify open ports and services, providing critical information for potential lateral movement entry points.

Rubeus was used for credential access, enabling the attacker to steal or forge Kerberos tickets, granting unauthorized access and potentially escalating privileges.

Anyconnect served a dual purpose – to ensure persistence and to enable initial access through secure remote connections.



```
GRB_NET Version: Test. 7
Type type -h for help
GRB_NET  1.0.0.0
Copyright c  2022

ERROR(S):
  Required option 'm, mode' is missing.
  Required option 'i, input' is missing.

  -m, --mode             Required. GRB mode. scan/clr. scan - network scanner. clr - event logs cleaner.

  -i, --input            Required. Input: f/r/s. f - file, r - range, s - subnet, d - domain.

  -d, --data             File.txt/127.0.0.1-127.0.0.255/127.0.0.1-24

  -u, --username         Username for scanning

  -p, --password         Password for scanning

  -h, --help             (Default: ) Show help and usage.

  -t, --threads          (Default: 8) Threads count

  -w, --wait             (Default: 5000) Wait time in ms. 1000 = 1s

  -r, --remote_start     (Default: 0) Start remote services

  -k, --domain_name      (Default: ) Domain name for Users and Computers gathering. If not set will be used domain of
                         current user.

  --help                 Display this help screen.

  --version              Display version information.
```

Figure 5: Help options of Grixba

Zerologon is a tool commonly associated with lateral movement, and it was used to exploit remote service vulnerabilities, like the Zerologon vulnerability, to traverse the network. ProxifierSetup.exe aided in command and control, allowing the attacker to establish proxy connections for remote control while avoiding detection.

WinSCP was used for exfiltration, discreetly transferring stolen data from compromised systems to external locations. Lastly, secretsdump was used for OS credential dumping, extracting login credentials from compromised systems, further extending the attackers’ access within the network.

The attacker also deployed a custom backdoor, portstarter, written in Go language. Upon execution, it collected host information using various WinAPIs to read registry values and query user, host, and process information.

The tool execuated two PowerShell commands. It first launched “powershell.exe -command “get-wmiobject win32_computersystem | select-object -expandproperty domain””.

After waiting a while, it launched a second PowerShell command to retrieve the public IP address of the infected system “powershell.exe -command “& nslookup myip.opendns.com resolver1.opendns.com””.

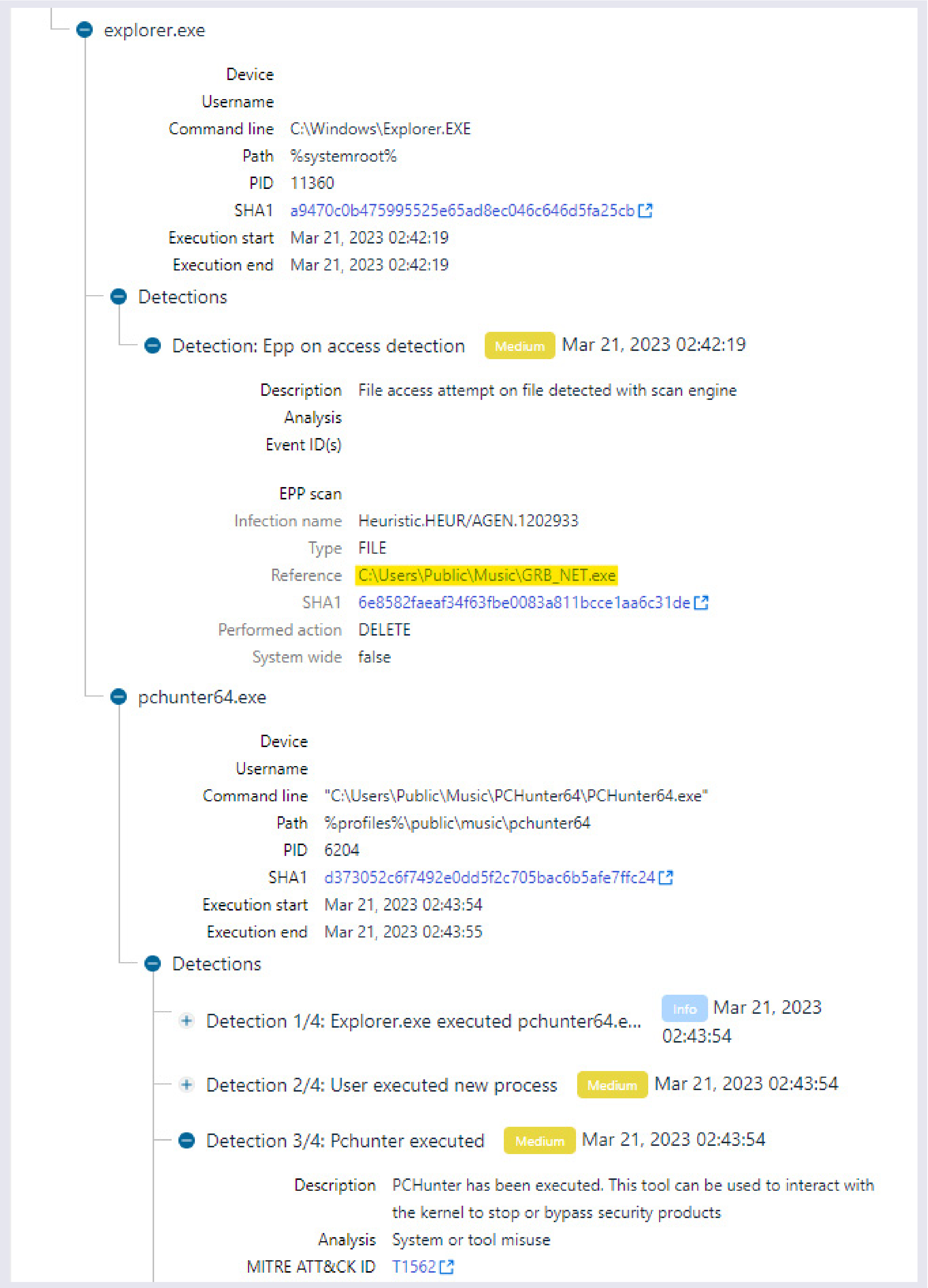
Finally, after a couple of sleep() cycles, it opened a network connection and opened ports to a command-and-control server.

Although portstarter is a commodity tool and can be utilized by any threat group, it is commonly associated with the “VICE SOCIETY” group. In 2023, according to WithSecure telemetry, the portstarter backdoor was seen utilized in multiple incidents in Finland, Norway, Denmark and most recently in an educational institute in Ireland. Vice Society has been earlier reported[8] to target education sector.

Saving the Best for Last

Attackers often stick to methods that are proven to work. When they do decide to change these methods, it is usually in response to the current method getting blocked or to make their attacks work more effectively. In March 2023, WithSecure came across one such incident where, after gaining access, an attacker tried to deploy numerous tools including ransomware, over a multi-day timespan. All the files they attempted to deploy, including PLAY ransomware, were blocked by WithSecure’s Endpoint product. Hence, the

[8] Vice Society: Profiling a Persistent Threat to the Education Sector (paloaltonetworks.com)



explorer.exe

Device	
Username	
Command line	C:\Windows\Explorer.EXE
Path	%systemroot%
PID	11360
SHA1	a9470c0b475995525e65ad8ec046c646d5fa25cb
Execution start	Mar 21, 2023 02:42:19
Execution end	Mar 21, 2023 02:42:19

Detections

Detection: Epp on access detection Medium Mar 21, 2023 02:42:19

Description	File access attempt on file detected with scan engine
Analysis	
Event ID(s)	
EPP scan	
Infection name	Heuristic.HEUR/AGEN.1202933
Type	FILE
Reference	C:\Users\Public\Music\GRB_NET.exe
SHA1	6e8582faeaf34f63fbe0083a811bcce1aa6c31de
Performed action	DELETE
System wide	false

pchunter64.exe

Device	
Username	
Command line	"C:\Users\Public\Music\PCHunter64\PCHunter64.exe"
Path	%profiles%\public\music\pchunter64
PID	6204
SHA1	d373052c6f7492e0dd5f2c705bac6b5afe7ffc24
Execution start	Mar 21, 2023 02:43:54
Execution end	Mar 21, 2023 02:43:55

Detections

Detection 1/4: Explorer.exe executed pchunter64.e... Info Mar 21, 2023 02:43:54

Detection 2/4: User executed new process Medium Mar 21, 2023 02:43:54

Detection 3/4: Pchunter executed Medium Mar 21, 2023 02:43:54

Description	PCHunter has been executed. This tool can be used to interact with the kernel to stop or bypass security products
Analysis	System or tool misuse
MITRE ATT&CK ID	T1562

Figure 6: Endpoint detection of Grixba

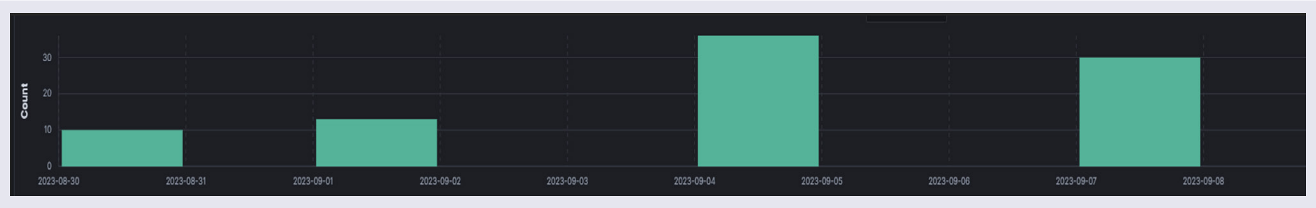


Figure 7: Activity timeline

attacker attempted to deploy a custom tool – “GRB_NET.exe” – as a last resort. However, this tool was also blocked by the Endpoint product.

Tools deployed by attacker in this incident were:

- Nekto/PriviCMD (clfs.exe)
- CLFS CVE-2023-23376 (sys.dll)
- SharpView (av_scan.exe)
- Rubeus (imfa.exe)
- Rubeus (brown_dot.dll)
- SystemBC (host.sa)
- PCHUNTER (PCHunter64ar.sys)
- Grixba (GRB_NET.exe)

The tool dropped in this incident appears to be an early test version of a tool with limited capabilities including network scanning and event log cleaning. However, a newer, more advanced version of this tool with additional capabilities was later reported[9]. The motive of the attacker involved with this incident was to deploy PLAY ransomware. As per WithSecure telemetry, Grixba was utilized in incidents in Sweden as a precursor to deployment of Play ransomware.

The One that Relies on Legit Tools

In August 2023, WithSecure identified and analyzed suspicious activities on a server in an organization in Italy. To fly under the radar, the attacker performed activities mostly after office hours and accessed systems for not more than 2 to 3 hours per day.

Although, activities were performed several hours and days apart, WithSecure Broad Context Detection[10] logic was able to combine all activities into a single incident which allowed us to track the attacker with ease.

Tools deployed in this incident were:

- Gost (Golang simple tunnel)
- NetScan

When these tools were prevented by the Endpoint product from performing suspicious activities, the attacker moved to use legitimate system files to achieve their objectives. Instead of netscan, the attacker started to use built-in command line tools such as netstat. The attacker also utilized PowerShell and PSExec for lateral movement.

Later it was identified that the attacker gained access via the VPN of an external company tasked with managing the servers.
Fortunately, the incident was blocked before the attacker could make a bigger impact.

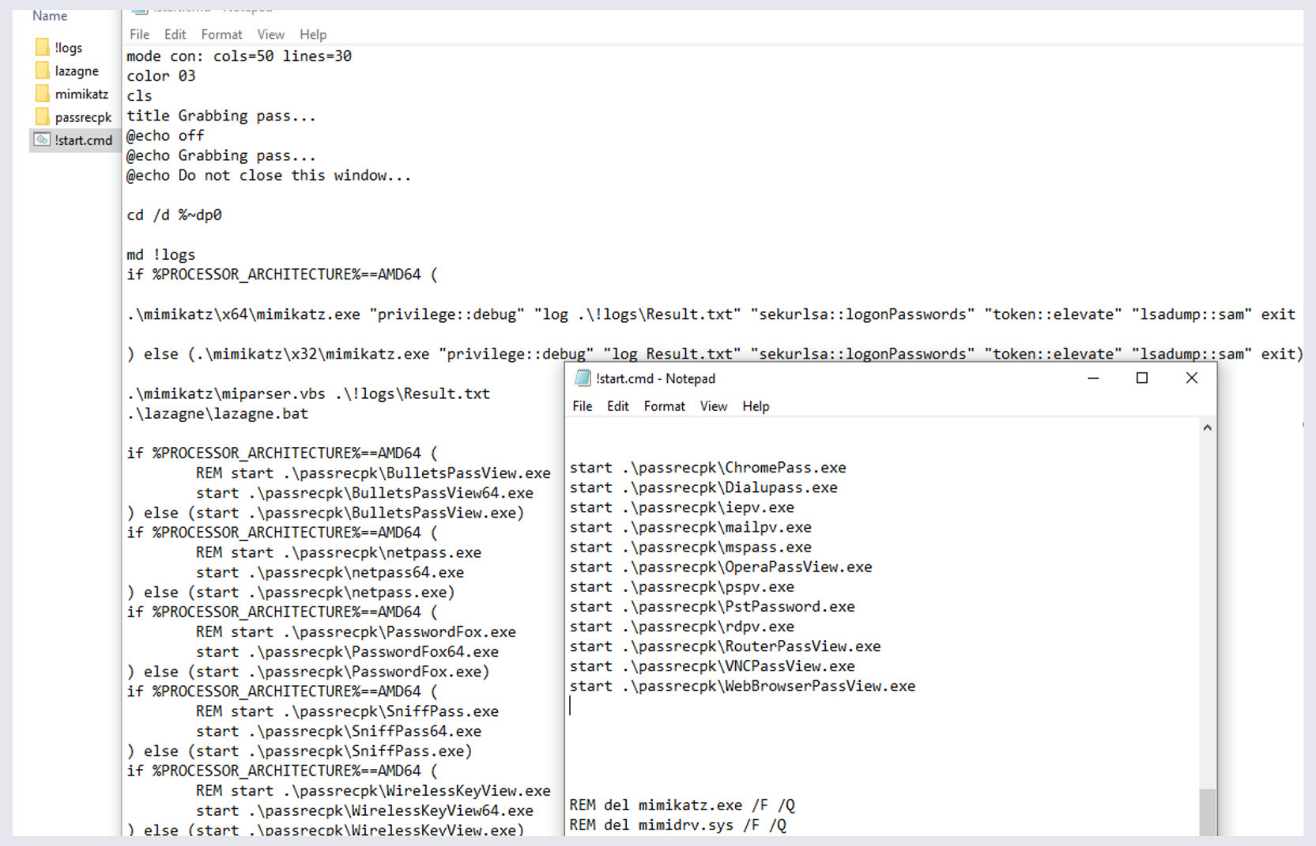
The One that is Most Used

The most common toolset seen across WithSecure’s telemetry is the combined package of Mimikatz, Lazagne and Nirsoft’s password recovery toolset. The toolset can be easily configured by editing start.cmd. It is sometimes utilized in pentesting scenarios and by Initial Access Brokers (IABs) to facilitate the deployment of malware and ransomware. In one recent incident, which appeared to be a precursor to the deployment of Trigona Ransomware, the attacker dropped several batch files designed to disable security products alongside it.

The real-world cases described in this article provide a glimpse into the dynamic and ever-evolving landscape of cyber threats. Beyond theoretical concepts, these tools have real consequences, from data breaches and financial losses to geopolitical tension. As we navigate through these examples, we gain valuable insights into the impact of attack toolsets and the importance of proactive cybersecurity measures.

In the following sections, we illustrate practical strategies and best practices to defend against the deployment of these attack toolsets and touch on how supporting defenses may be designed or implemented.

[9] Play Ransomware Group Using New Custom Data-Gathering Tools | Symantec Enterprise Blogs (security.com)
[10] https://www.withsecure.com/content/dam/with-secure/en/resources/WS-broad-context-detection-whitepaper-EN.pdf



```
mode con: cols=50 lines=30
color 03
cls
title Grabbing pass...
@echo off
@echo Grabbing pass...
@echo Do not close this window...

cd /d %~dp0

md !logs
if %PROCESSOR_ARCHITECTURE%==AMD64 (

.\mimikatz\x64\mimikatz.exe "privilege::debug" "log .\!logs\Result.txt" "sekurlsa::logonPasswords" "token::elevate" "lsadump::sam" exit

) else (.\mimikatz\x32\mimikatz.exe "privilege::debug" "log Result.txt" "sekurlsa::logonPasswords" "token::elevate" "lsadump::sam" exit)

.\mimikatz\miparser.vbs .\!logs\Result.txt
.\lazagne\lazagne.bat

if %PROCESSOR_ARCHITECTURE%==AMD64 (
        REM start .\passrecpk\BulletsPassView.exe
        start .\passrecpk\BulletsPassView64.exe
) else (start .\passrecpk\BulletsPassView.exe)
if %PROCESSOR_ARCHITECTURE%==AMD64 (
        REM start .\passrecpk\netpass.exe
        start .\passrecpk\netpass64.exe
) else (start .\passrecpk\netpass.exe)
if %PROCESSOR_ARCHITECTURE%==AMD64 (
        REM start .\passrecpk\PasswordFox.exe
        start .\passrecpk\PasswordFox64.exe
) else (start .\passrecpk\PasswordFox.exe)
if %PROCESSOR_ARCHITECTURE%==AMD64 (
        REM start .\passrecpk\SniffPass.exe
        start .\passrecpk\SniffPass64.exe
) else (start .\passrecpk\SniffPass.exe)
if %PROCESSOR_ARCHITECTURE%==AMD64 (
        REM start .\passrecpk\WirelessKeyView.exe
        start .\passrecpk\WirelessKeyView64.exe
) else (start .\passrecpk\WirelessKeyView.exe)
```

```
start .\passrecpk\ChromePass.exe
start .\passrecpk\Dialupass.exe
start .\passrecpk\iepv.exe
start .\passrecpk\mailpv.exe
start .\passrecpk\mspass.exe
start .\passrecpk\OperaPassView.exe
start .\passrecpk\pspv.exe
start .\passrecpk\PstPassword.exe
start .\passrecpk\rdpv.exe
start .\passrecpk\RouterPassView.exe
start .\passrecpk\VNCPassView.exe
start .\passrecpk\WebBrowserPassView.exe




REM del mimikatz.exe /F /Q
REM del mimidrv.sys /F /Q
```

Figure 8 !Start.cmd used to execute tools

Predictive Analysis

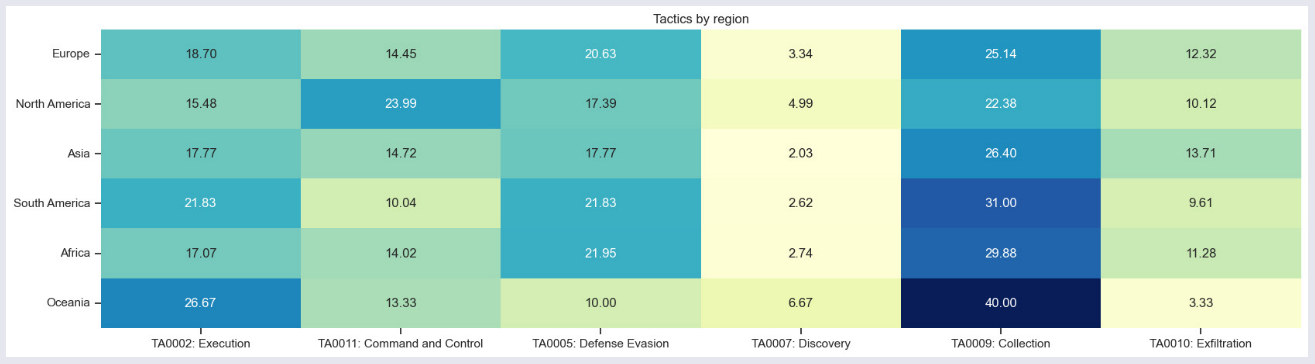
Cybersecurity products and services successfully block attacks most of the time, rendering the complete attack chain ineffective. This makes it exceedingly challenging to predict the motives of attackers and identify the threat groups behind foiled attacks. The limited data points available due to thwarted attacks leave defenders with a significant information gap, making it difficult to ascertain the broader context and motives of adversaries. This combined with affiliate programs and the availability of commodity tooling, means that it is more and more difficult to differentiate between different actors and groups solely based on their TTPs.

Furthermore, adversaries are not confined to a fixed playbook; instead, they adapt their tactics dynamically. This adaptability arises from a variety of factors, including the evolving threat landscape, the target's defense mechanisms, and their own shifting objectives. Furthermore, attackers often have multiple objectives. To maximize their chances of success, they frequently employ parallel attack paths, simultaneously exploring multiple avenues, exploiting numerous vulnerabilities, and using a range of distinct techniques. This parallelism can result in a non-linear progression of tactics, making cyberattacks challenging to predict and defend against effectively.

When observed incident types are correlated with MITRE ATT&CK matrices, it is possible to understand which tactics are often seen together in an incident. This data can also be used to predict which tactics or techniques a threat actor is most likely to use.

Figure 10 is a graph representation of tactics seen in WithSecure telemetry over the past year. Edges were added between nodes when one or more tactics were observed in the same attack. Thus, a representation of commonly used clusters of tactics can be observed.

Larger nodes in the visualization represent higher observed counts of that tactic. Credential access, lateral movement, discovery, and impact were all a lot less prevalent than the other tactics. Observing the widest edges between nodes allows us to determine that pairs such as collection-defense evasion, collection-execution, collection-exfiltration, defense evasion-execution, exfiltration-defense evasion, execution-command and control, and collection-command and control are most common. From this data we can infer that adversaries tend to perform defense evasion prior to most other post-compromise tactics. This is a common tactic that adversaries employ in order to avoid detection while performing their post-compromise activities. Moreover, the graph depicts that both discovery and collection commonly lead to exfiltration and command and



Tactics by region

	TA0002: Execution	TA0011: Command and Control	TA0005: Defense Evasion	TA0007: Discovery	TA0009: Collection	TA0010: Exfiltration
Europe	18.70	14.45	20.63	3.34	25.14	12.32
North America	15.48	23.99	17.39	4.99	22.38	10.12
Asia	17.77	14.72	17.77	2.03	26.40	13.71
South America	21.83	10.04	21.83	2.62	31.00	9.61
Africa	17.07	14.02	21.95	2.74	29.88	11.28
Oceania	26.67	13.33	10.00	6.67	40.00	3.33

Figure 9: MITRE ATT&CK tactics as seen in confirmed incidents in Elements EDR telemetry in 2023

control tactics, indicating adversaries' reliance on information that's gathered and stolen from the victim's machines and sent back to the attackers' to perform their next steps in an attack lifecycle. Lastly, this visualization clearly shows the interconnectedness of various tactics that attackers employ across different attack chains to achieve their objectives rather than a linear chain comprising of tactics being performed in a sequential manner across all threats.

Weighted correlations of MITRE tactics that are often observed together in real attacks can indeed provide valuable insights into the likelihood of certain tools being used together. These correlations can help in predicting tool co-occurrences in cyberattacks to some extent. Here's how:

Identifying Tool Patterns

By analyzing weighted correlations, you can identify patterns where specific tactics tend to co-occur. For example, if you find that tactics related to initial access often correlate with tactics

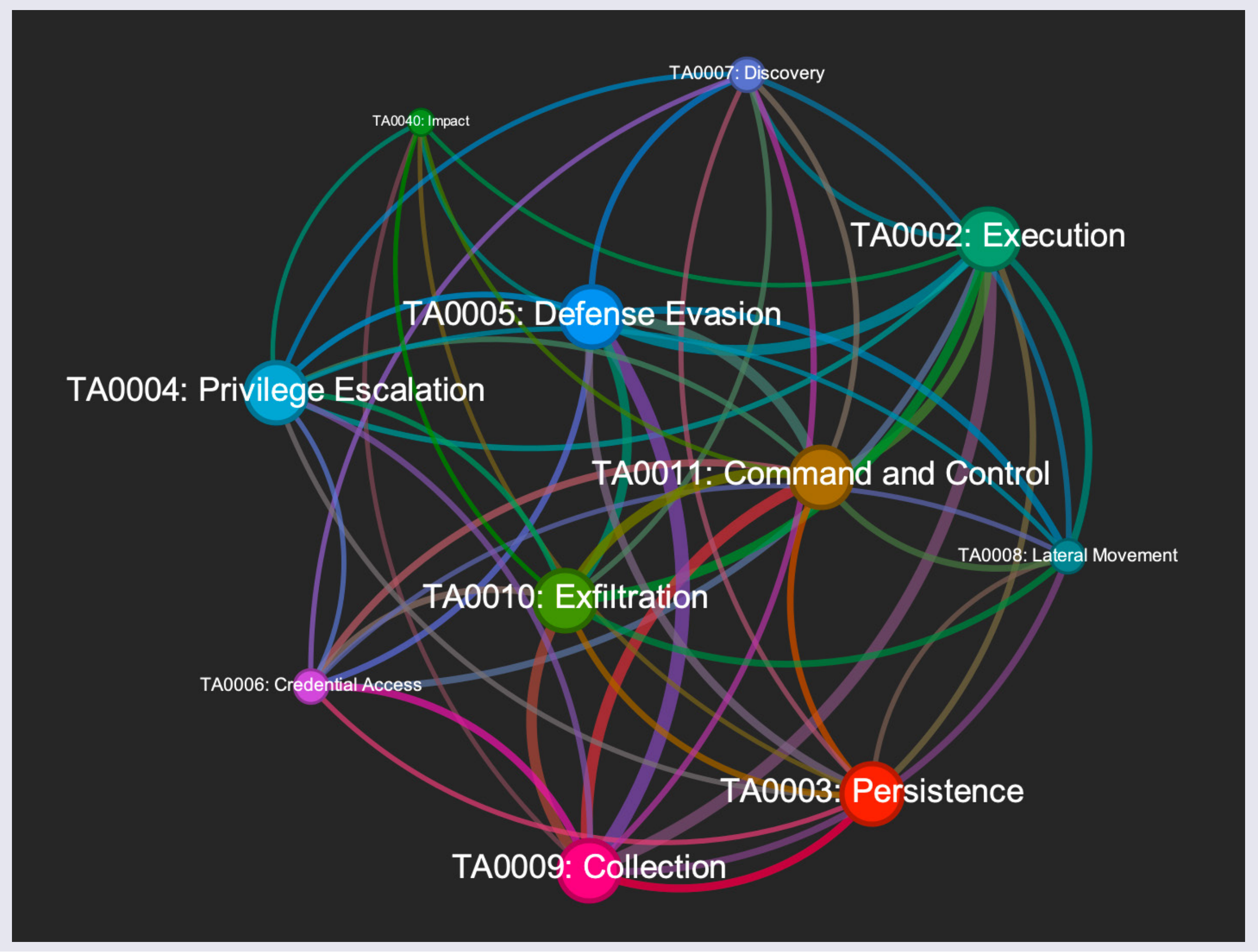
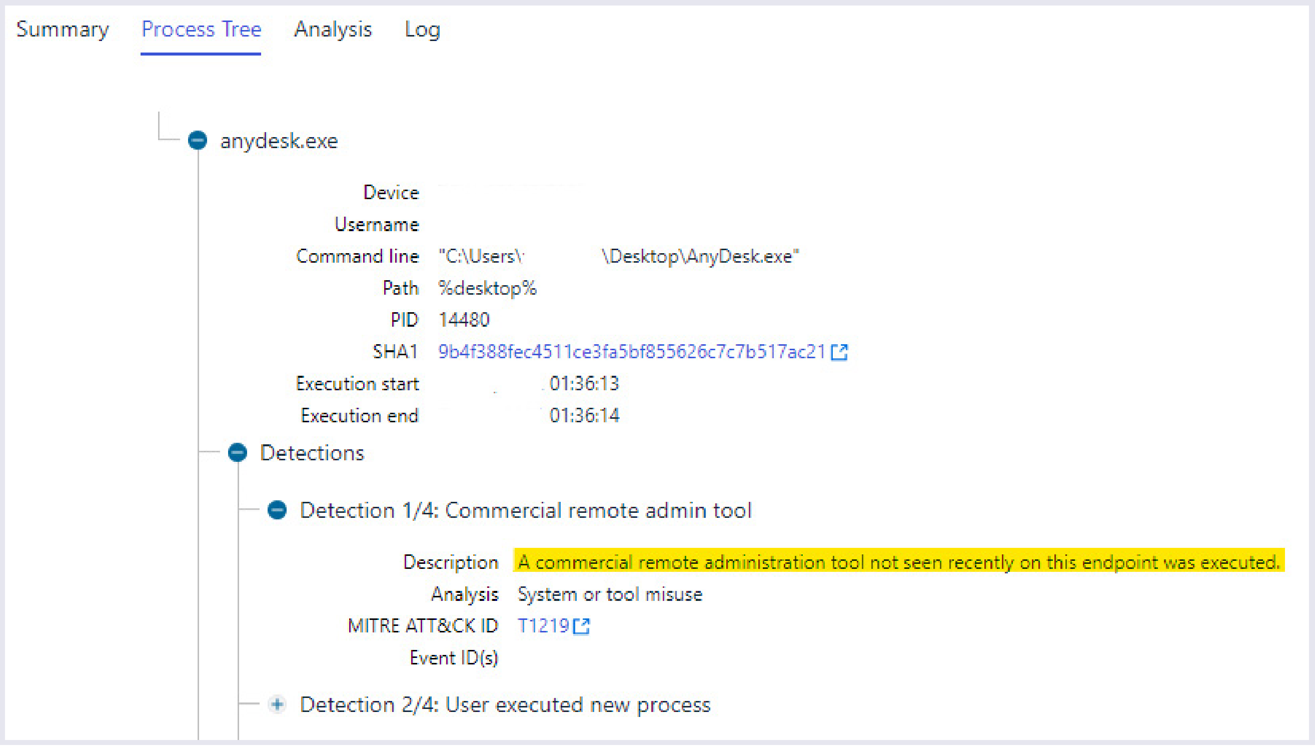


Figure 10: Commonly used clusters of tactics



anydesk.exe

Device

Username

Command line "C:\Users\ \Desktop\AnyDesk.exe"

Path %desktop%

PID 14480

SHA1 9b4f388fec4511ce3fa5bf855626c7c7b517ac21

Execution start 01:36:13

Execution end 01:36:14

Detections

Detection 1/4: Commercial remote admin tool

Description A commercial remote administration tool not seen recently on this endpoint was executed.

Analysis System or tool misuse

MITRE ATT&CK ID T1219

Event ID(s)

Detection 2/4: User executed new process

Figure 11: Example ML model based detection

related to privilege escalation, it suggests that tools associated with both tactics may be used together in many attacks.

Tool Recommendations

These correlations can aid cybersecurity professionals and organizations in making more informed decisions as to which security tools to deploy. If certain tactics frequently go hand in hand, it's likely that the corresponding security tools should also be used together to enhance defenses.

Enhancing Threat Intelligence

Weighted correlations can contribute to threat intelligence by providing insights into the behavior of cyber adversaries. When specific tactics and tools consistently correlate, it indicates that attackers tend to follow certain attack patterns. This information can be used to anticipate and prepare for similar attacks in the future.

Building Predictive Models

While correlations provide valuable insights, they may not be predictive on their own. To make predictions about which tools are most likely to be seen together, gathered data can be used to train machine learning models. Predictive models trained on historical data can be used to identify tool combinations that are frequently observed in specific attack scenarios. Predictive models combined with host profiling can then be used to assess the likelihood of a tool to be present on a system. One such example is to use machine learning models to monitor the unusual installation and usage of tools which can be exploited.

Mitigating Emerging Threats

Recognizing correlations between tactics and tools can help organizations stay ahead of emerging threats. If new correlations emerge in the threat landscape, it may indicate evolving attack strategies that need to be addressed proactively.

Securing Your Enterprise

Maintain an Updated Software Inventory

Create and regularly update a comprehensive list of all software used within your organization, aligning it with your specific business and operational needs. Continuously monitor this inventory. Periodically evaluate and consider removing any tools that are no longer deemed necessary.

Control the Usage of Potentially Exploitable Tools

Implement strict controls over the usage of tools that could potentially enable attackers to exploit your systems. Employees seeking to use such tools should undergo an approval process for a limited duration. This should all be managed through robust application control policies.

Baseline and Monitor Workstation Activity

Establish a baseline for typical workstation activities within your organization. Deviations from this baseline, especially involving the sudden appearance and use of multiple administrative tools, should trigger suspicion and be promptly investigated.

Prioritize Regular Patching and Updates

Ensure that all tools and software applications in your organization are kept up to date with the latest patches and security updates. This practice helps mitigate potential vulnerabilities that malicious actors might exploit for harmful purposes.

Implement Strong Access Controls

Restrict access to critical tools and systems to specifically authorized personnel. Enforce the principle of least privilege, granting employees access to only the resources necessary for their specific roles, and regularly review and adjust these access levels as needed.

Invest in Employee Education

Educate your staff about the risks associated with certain tools and software applications that may be used maliciously. Encourage a culture of cybersecurity awareness, emphasizing the importance of responsible tool usage.

Incident Response Planning

Develop and regularly update incident response plans to effectively address any security incidents that may occur. These plans should include procedures for handling incidents involving the abuse of tools or software for malicious purposes.

Regular Security Audits and Assessments

Conduct periodic security audits and assessments of your organization's systems and software tools to identify vulnerabilities and weaknesses. Address any issues promptly to reduce the potential for exploitation.

By implementing these measures, organizations can strengthen their defenses against tools that may be misused for malicious intent and enhance their overall cybersecurity posture.

Conclusion

Adversaries have become increasingly adept and resourceful over the years, posing significant challenges for individuals, organizations, and governments alike. To combat them, it is paramount to equip organizations and cybersecurity practitioners with novel analysis methodologies, tools and techniques that can drive decision-making with a better understanding of such threats, tilting the balance ever so slightly in our favor. One of the most significant examples of this is the MITRE ATT&CK framework.

In this analysis, we broke down a devised cyberattack with the most common objective using the MITRE ATT&CK framework, highlighting different paths attackers take to achieve each tactic based on real-world observations by WithSecure. Furthermore, we walked through real-world incidents analyzed & handled by WithSecure, highlighting different toolsets in action as the intrusions unfolded, showcasing the dynamics of each intrusion and threat group. Lastly, we provided some unique insights by applying data analysis over confirmed incidents and observed tactics.

It is difficult for organizations to defend against every single threat in the ever-changing threat landscape. However, by looking at true positive trends, attacker's toolsets, incident types and MITRE matrices from a particular region and vertical, an organization can refine and test their defenses by prioritizing against the kind of attacks that will likely affect them the most.

Indicators of Compromise (IOCs)

All relevant IOCs can be found in WithSecure Lab's GitHub[11]

[11] https://github.com/WithSecureLabs/iocs/tree/master/unveiling-the-arsenal

Who We Are

WithSecure™, formerly F-Secure Business, is cyber security's reliable partner. IT service providers, MSSPs and businesses – along with the largest financial institutions, manufacturers, and thousands of the world's most advanced communications and technology providers – trust us for outcome-based cyber security that protects and enables their operations. Our AI-driven protection secures endpoints and cloud collaboration, and our intelligent detection and response are powered by experts who identify business risks by proactively hunting for threats and confronting live attacks. Our consultants partner with enterprises and tech challengers to build resilience through evidence-based security advice. With more than 30 years of experience in building technology that meets business objectives, we've built our portfolio to grow with our partners through flexible commercial models.

WithSecure™ Corporation was founded in 1988, and is listed on NASDAQ OMX Helsinki Ltd.