SE Labs

INTELLIGENCE-LED TESTING

Enterprise Advanced Security

EDR DETECTION

SenseOn

July 2023

SE Labs tested **SenseOn** against a range of hacking attacks designed to compromise systems and penetrate target networks in the same way as criminals and other attackers breach systems and networks.

Full chains of attack were used, meaning that testers behaved as real attackers, probing targets using a variety of tools, techniques and vectors before attempting to gain lower-level and more powerful access. Finally, the testers/ attackers attempted to complete their missions, which might include stealing information, damaging systems and connecting to other systems on the network.

Management
Chief Executive Officer Simon Edwards
Chief Operations Officer Marc Briggs
Chief Human Resources Officer Magdalena Jurenko
Chief Technical Officer Stefan Dumitrascu

Testing Team
Nikki Albesa
Thomas Bean
Solandra Brewster
Gia Gorbold
Anila Johny
Erica Marotta
Luca Menegazzo
Jeremiah Morgan
Julian Owusu-Abrokwa
Joseph Pike
Georgios Sakatzidi
Dimitrios Tsarouchas
Stephen Withey

Marketing
Sara Claridge
Janice Sheridan

Publication
Colin Mackleworth

IT Support
Danny King-Smith
Chris Short

Website selabs.uk
Email info@SELabs.uk
LinkedIn www.linkedin.com/company/se-labs/
Blog blog.selabs.uk
Post SE Labs Ltd,
55A High Street, Wimbledon, SW19 5BA, UK

SE Labs is ISO/IEC 27001 : 2013 certified and
BS EN ISO 9001 : 2015 certified for The Provision
of IT Security Product Testing.

SE Labs is a member of the Microsoft Virus Initiative (MVI);
the Anti-Malware Testing Standards Organization (AMTSO);
the Association of anti Virus Asia Researchers (AVAR);
and NetSecOPEN.

Contents

Document version 1.0 Written 3rd July 2023

Introduction

Endpoint Detection and Response is more than anti-virus

Understand cybersecurity testing with visible threat intelligence

An Endpoint Detection and Response (EDR) product is more than anti-virus, which is why it requires advanced testing. This means testers must behave like real attackers, following every step of an attack.

While it's tempting to save time by taking shortcuts, a tester must go through an entire attack to truly understand the capabilities of EDR security products.

Each step of the attack must be realistic too. You can't just make up what you think bad guys are doing and hope you're right. This is why SE Labs tracks cybercriminal behaviour and builds tests based on how bad guys try to compromise victims.

The cybersecurity industry is familiar with the concept of the 'attack chain', which is the combination of those attack steps. Fortunately the MITRE organisation has documented each step with its ATT&CK framework. While this doesn't give an exact blueprint for realistic attacks, it does present a general structure that testers, security vendors and customers (you!) can use to run tests and understand test results.

The Enterprise Advanced Security tests that SE Labs runs are based on real attackers' behaviour. This means we can present how we run those attacks using a MITRE ATT&CK-style format.

You can see how ATT&CK lists out the details of each attack, and how we represent the way we tested, in **4. Threat Intelligence**, starting on page 13. This brings two main advantages: you can have confidence that the way we test is realistic and relevant; and you're probably already familiar with this way of illustrating cyber attacks.

If you spot a detail in this report that you don't understand, or would like to discuss, please **contact us**. SE Labs uses current threat intelligence to make our tests as realistic as possible. To learn more about how we test, how we define 'threat intelligence' and how we use it to improve our tests please visit our **website** and follow us on **LinkedIn**.

Executive Summary

SenseOn was tested against a range of hacking attacks designed to compromise systems and penetrate target networks in the same way as criminals and other attackers breach systems and networks. Legitimate files were used alongside the threats to measure any false positive detections or other sub-optimum interactions.

We examined its abilities to:

- **Detect the delivery of targeted attacks**
- **Track different elements of the attack chain...**
- **...including compromises beyond the endpoint and into the wider network**

SenseOn was able to detect every targeted attack and tracked each of the hostile activities that occurred during the attacks.

With few exceptions, detection was complete and deep, tracking malicious behaviour from the beginning to the end of the attack. It generated no false positives, which should lighten the load on security operatives using the product.

Enterprise Advanced Security Award

The following product wins the SE Labs award:

SenseOn

Executive Summary

Product Tested	Attacks Detected (%)	Detection Accuracy Rating (%)	Legitimate Accuracy Rating (%)	Total Accuracy Rating (%)
SenseOn	100%	97%	100%	98%

Green highlighting shows that the product was very accurate, scoring 85% or more for Total Accuracy. Yellow means between 75 and 85, while red is for scores of less than 75%.

For exact percentages, see **2. Total Accuracy Ratings** on page 10.

1. How We Tested

Testers can't assume that products will work a certain way, so running a realistic advanced security test means setting up real networks and hacking them in the same way that real adversaries behave.

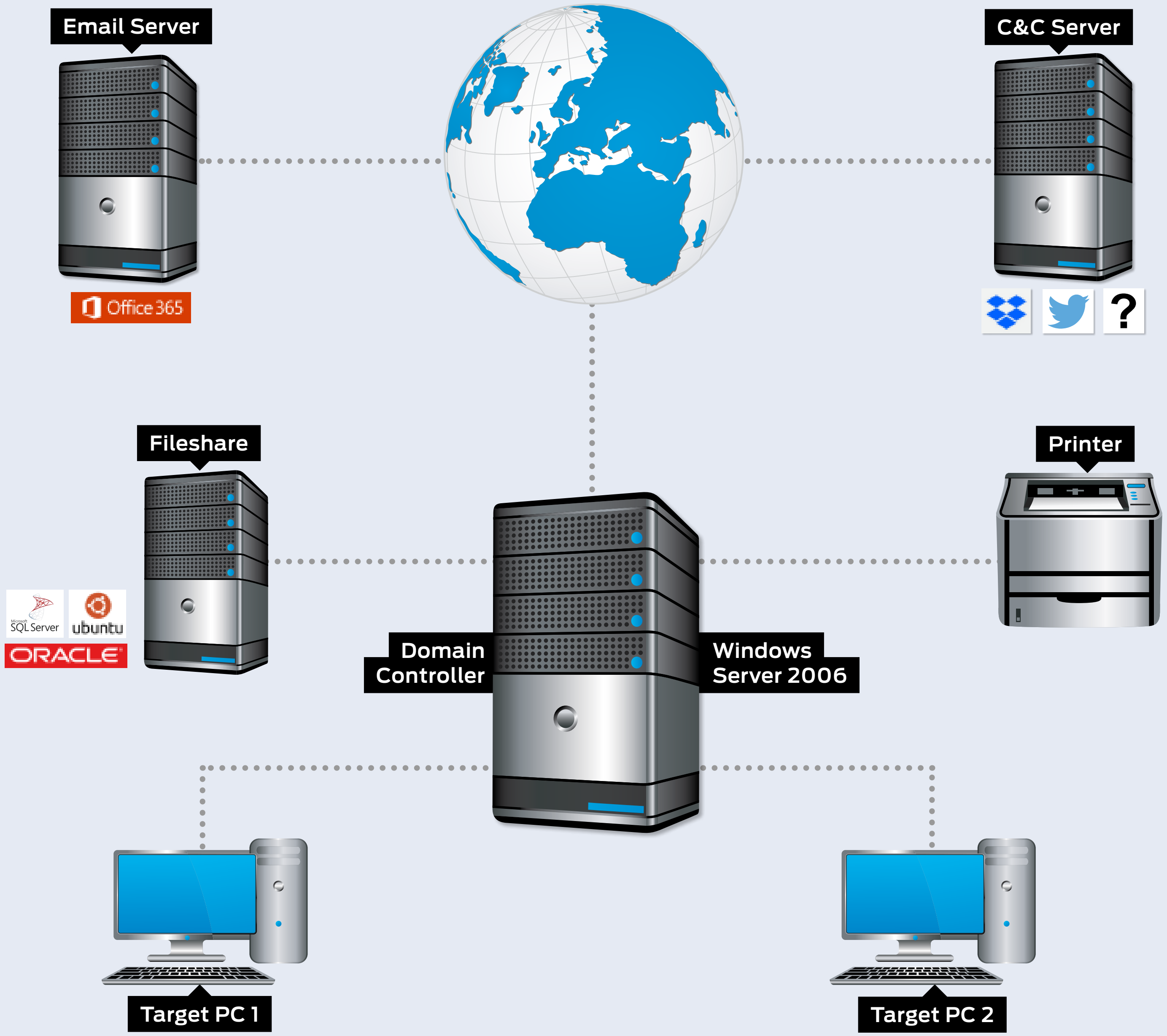
In the diagram on the right you will see an example network that contains workstations, some basic infrastructure such as file servers and a domain controller, as well as cloud-based email and a malicious command and control (C&C) server, which may be a conventional computer or a service such as Dropbox, Twitter, Slack or something else more imaginative.

As you will see in the **Threat Responses** section on page 7, attackers often jump from one compromised system to another in so-called 'lateral movement'. To allow products to detect this type of behaviour the network needs to be built realistically, with systems available, vulnerable and worth compromising.

It is possible to compromise devices such as enterprise printers and other so-called 'IoT' (internet of things) machines, which is why we've included a representative printer in the diagram.

The techniques that we choose for each test case are largely dictated by the real-world behaviour of online criminals. We observe their tactics and replicate what they do in this test. To see more details about how the specific attackers behaved, and how we copied them, see **Hackers vs. Targets** on page 9 and, for a really detailed drill down on the details, **4. Threat Intelligence** on pages 13 to 16 and **Appendix C: Attack Details**.

Test Network Example



This example of a test network shows one possible topology and ways in which enterprises and criminals deploy resources.

Threat Responses

Full Attack Chain: Testing Every Layer of Detection and Protection

Attackers start from a certain point and don't stop until they have either achieved their goal or have reached the end of their resources (which could be a deadline or the limit of their abilities). This means, in a test, the tester needs to begin the attack from a realistic first position, such as sending a phishing email or setting up an infected website, and moving through many of the likely steps leading to actually stealing data or causing some other form of damage to the network.

If the test starts too far into the attack chain, such as executing malware on an endpoint, then many products will be denied opportunities to use the full extent of their protection and detection abilities. If the test concludes before any 'useful' damage or theft has been achieved, then similarly the product may be denied a chance to demonstrate its abilities in behavioural detection and so on.

Attack Stages

The illustration (below) shows some typical stages of an attack. In a test each of these should be attempted to determine the security solution's effectiveness. This test's results record detection and protection for each of these stages.

We measure how a product responds to the first stages of the attack with a detection and/ or protection rating. Sometimes products allow threats to run but detect them. Other times they might allow the threat to run briefly before neutralising it. Ideally they detect and block the threat before it has a chance to run. Products may delete threats or automatically contains them in a 'quarantine' or other safe holding mechanism for later analysis.

Should the initial attack phase succeed we then measure post-exploitation stages, which are represented by steps two through to seven below. We broadly categorise these stages as: Access (step 2); Action (step 3); Escalation (step 4); and Post-escalation (steps 5-7).

In figure 1. you can see a typical attack running from start to end, through various 'hacking' activities. This can be classified as a fully successful breach.

Attack Chain Stages

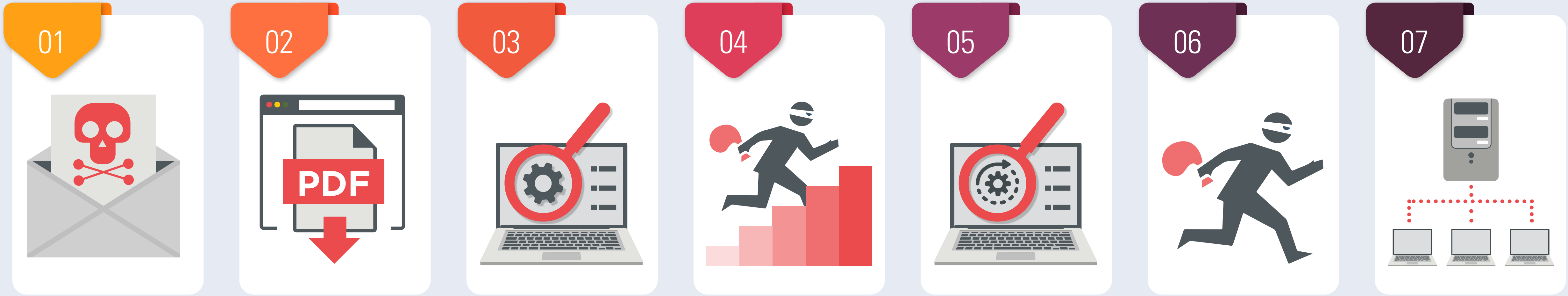


Figure 1. A typical attack starts with an initial contact and progresses through various stages, including reconnaissance, stealing data and causing damage.

In figure 2. a product or service has interfered with the attack, allowing it to succeed only as far as stage 3, after which it was detected and neutralised. The attacker was unable to progress through stages 4 and onwards.

It is possible for an attack to run in a different order with, for example, the attacker attempting to connect to other systems without needing to escalate privileges. However, it is common for password theft (see step 5) to occur before using stolen credentials to move further through the network.

It is also possible that attackers will not cause noticeable damage during an attack. It may be that their goal is persistent presence on the systems to monitor for activities, slowly steal information and other more subtle missions.

In figure 3. the attacker has managed to progress as far as stage five. This means that the system has been seriously compromised. The attacker has a high level of access and has stolen passwords. However, attempts to exfiltrate data from the target were blocked, as were attempts to damage the system.

Attack Chain: How Hackers Progress

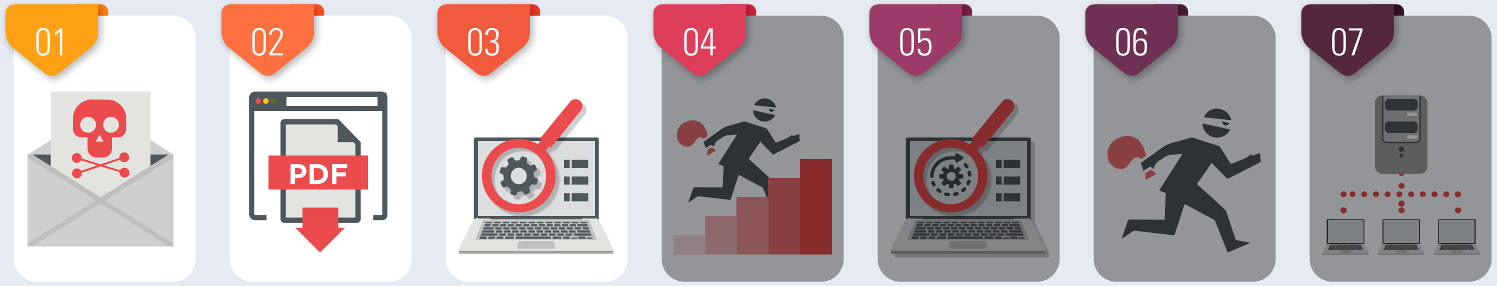


Figure 2. This attack was initially successful but only able to progress as far as the reconnaissance phase

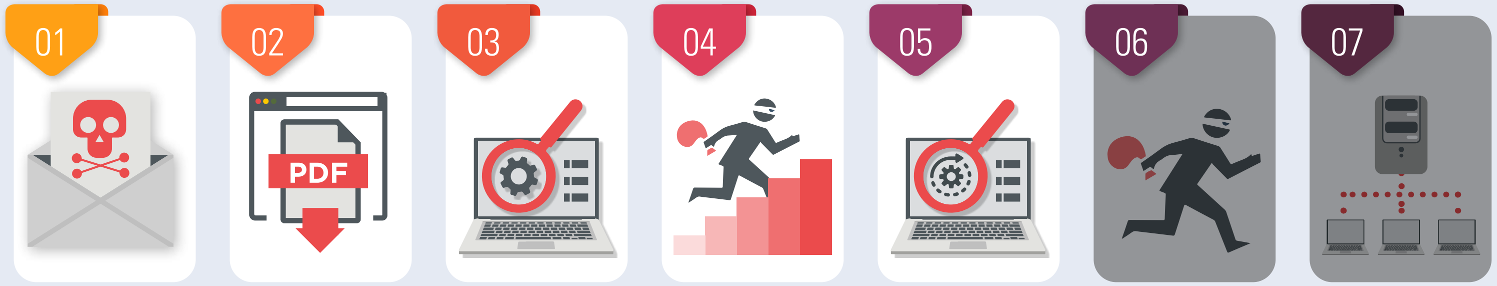


Figure 3. A more successful attack manages to steal passwords but wholesale data theft and destruction was blocked.

Hackers vs. Targets

When testing services against targeted attacks it is important to ensure that the attacks used are relevant. Anyone can run an attack randomly against someone else. It is the security vendor's challenge to identify common attack types and to protect against them. As testers, we need to generate threats that in some way relate to the real world.

All of the attacks used in this test are valid ways to compromise an organisation. Without any security in place, all would succeed in attacking the target. Outcomes would include systems infected with ransomware, remote access to networks and data theft.

But we didn't just sit down and brainstorm how we would attack different companies. Instead we used current threat intelligence to look at what the bad guys have been doing over the last few years and copied them quite closely. This way we can test the services' abilities to handle similar threats to those faced by global governments, financial institutions and national infrastructure.

The graphic on this page shows a summary of the attack groups that inspired the targeted attacks used in this test. If a service was able to detect and protect against these then there's a good chance they are on track to blocking similar attacks in the real world. If they fail, then you might take their bold marketing claims about defeating hackers with a pinch of salt.

For more details about each APT group please see **4. Threat Intelligence** on page 13.

Hackers vs. Targets

Attacker/APT Group	Method	Target	Details
Turla	🎣✉	🏛	Spearphishing campaigns and in-house espionage tools.
Ke3chang	🎩🖥🌐	🛢	Custom malware to maintain persistence and data exfiltration from target.
Threat Group-3390	🎩🖥🌐	🏛 🃏🎲	Modified Mimikatz to dump credentials and data exfiltration via Dropbox.
Kimsuky	🎣✉📎	🏛	Initial access by exploiting software vulnerabilities; dumping credentials from web browsers.

Key

✈ Aviation	🏦 Banking and ATMs	🏭 Energy	🎭 Entertainment
$ Financial	🃏🎲 Gambling	🏛 Government Espionage	⊕ Healthcare
🖥 IT	⚖ Law	🛢 Natural Resources	🛒 US Retail, Restaurant and Hospitality

2. Total Accuracy Ratings

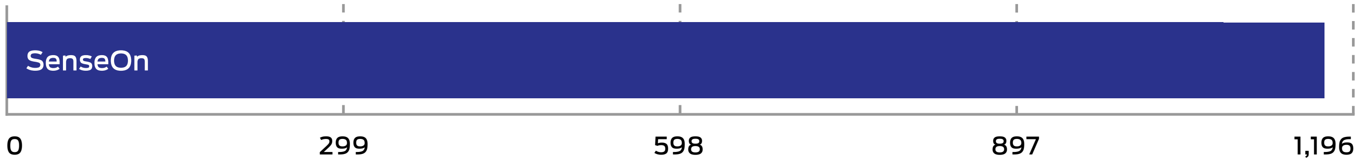
This test examines the total insight a product has, or can provide, into a specific set of attacking actions. We've divided the attack chain into chunks of one or more related actions. To provide sufficient insight, a product must detect at least one action in each chunk.

If you look at the results table in **3. Response Details** on page 11 you'll see that Delivery and Execution are grouped together into one chunk, while Action sits alone. Escalation and Post-Escalation (PE) Action are grouped, while Lateral Movement and Lateral Action are also grouped.

This means that if the product detects either the threat being delivered or executed, it has coverage for that part of the attack. If it detects the action as well as the escalation of privileges and an action involved in lateral movement then it has what we consider to be complete insight, even if it doesn't detect some parts of some chunks (i.e. Lateral Movement, in this example).

Total Accuracy Ratings

Product	Total Accuracy Rating	Total Accuracy (%)	Award
SenseOn	1,176	98%	AAA



Total Accuracy Ratings combine protection and false positives.

3. Response Details

In this test security products are exposed to attacks, which comprise multiple stages. The perfect product will detect all relevant elements of an attack. The term ‘relevant’ is important, because sometimes detecting one part of an attack means it’s not necessary to detect another.

For example, in the table below certain stages of the attack chain have been grouped together. As mentioned in **2. Total Accuracy Ratings**, these groups are as follows:

Delivery/ Execution (+10)
If the product detects either the delivery or execution of the initial attack stage then a detection for this stage is recorded.

Action (+10)
When the attack performs one or more actions, while remotely controlling the target, the product should detect at least one of those actions.

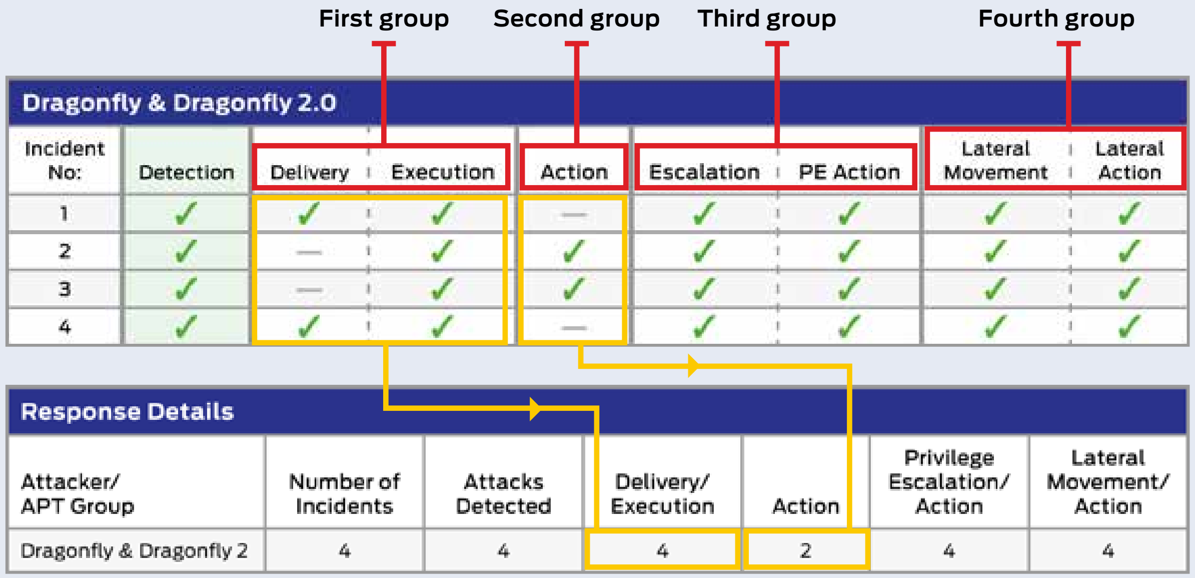
Privilege escalation/ action (+10)
As the attack progresses there will likely be an attempt to escalate system privileges and to perform more powerful and insidious actions. If the product can detect either the escalation process itself, or any resulting actions, then a detection is recorded.

Lateral movement/ action (+10)
The attacker may attempt to use the target as a launching system to other vulnerable systems. If this attempt is discovered, or any subsequent action, a detection is reported.

The Detection Rating is calculated by adding points for each group in a threat chain that is detected. When at least one detection occurs in a single group, a ‘group detection’ is recorded and 10 points are awarded. Each test round contains one threat chain, which itself contains four groups (as shown above), meaning that complete visibility of each attack adds 40 points to the total value.

A product that detects the delivery of a threat, but nothing subsequently to that, wins only 10 points, while a product that detects delivery and action, but not privilege escalation or lateral behaviours, is rated at 20 for that test round.

Understanding Detection Groups


First group
Second group
Third group
Fourth group

Dragonfly & Dragonfly 2.0

Incident No:	Detection	Delivery	Execution	Action	Escalation	PE Action	Lateral Movement	Lateral Action
1	✓	✓	✓	—	✓	✓	✓	✓
2	✓	—	✓	✓	✓	✓	✓	✓
3	✓	—	✓	✓	✓	✓	✓	✓
4	✓	✓	✓	—	✓	✓	✓	✓

Response Details

Attacker/ APT Group	Number of Incidents	Attacks Detected	Delivery/ Execution	Action	Privilege Escalation/ Action	Lateral Movement/ Action
Dragonfly & Dragonfly 2	4	4	4	2	4	4

Elements of the attack chain are put into groups. For example, the Delivery and Execution stages of an attack are in the same group. Similarly, we group the Post Escalation stage with the Post Escalation Action (PE Action) stage. When we count detections we look to see at least one detection (tick) in each group. One or two detections in a group is a success.

In this example we have four test cases, which we call ‘incidents’. In Incident No. 1 there was a detection recorded for the delivery of the threat and when it was executed. These two results count as one detection. In Incident No. 2 the threat delivery was not detected, but its execution was. This also counts as one detection.

When no detection is registered in any part of a group the result will be a ‘miss’. In Incident 1. there was no detection when the attacker performed the ‘Action’ stage of the attack. This is a miss for the product. In fact, this product only detected two of the four Action stages, which is why the Response Details table shows ‘2’ in the Action column.

Turla								
Incident No:	Detection	Delivery	Execution	Action	Escalation	PE Action	Lateral Movement	Lateral Action
1	✓	—	✓	✓	✓	✓	✓	✓
2	✓	—	✓	✓	✓	✓	✓	✓
3	✓	✓	✓	✓	✓	✓	—	✓
4	✓	✓	✓	✓	—	✓	✓	✓

Threat Group-3390								
Incident No:	Detection	Delivery	Execution	Action	Escalation	PE Action	Lateral Movement	Lateral Action
9	✓	—	✓	✓	✓	✓	✓	✓
10	✓	—	✓	✓	✓	✓	✓	✓
11	✓	✓	✓	✓	✓	✓	✓	✓
12	✓	✓	✓	✓	✓	✓	✓	✓

Ke3chang								
Incident No:	Detection	Delivery	Execution	Action	Escalation	PE Action	Lateral Movement	Lateral Action
5	✓	✓	✓	✓	✓	✓	✓	—
6	✓	✓	✓	—	✓	✓	✓	—
7	✓	—	✓	✓	✓	✓	✓	—
8	✓	—	✓	✓	✓	✓	—	—

Kimsuky								
Incident No:	Detection	Delivery	Execution	Action	Escalation	PE Action	Lateral Movement	Lateral Action
13	✓	—	✓	✓	✓	✓	✓	✓
14	✓	—	✓	✓	✓	✓	✓	✓
15	✓	✓	✓	✓	✓	✓	—	✓
16	✓	✓	✓	✓	✓	✓	✓	—

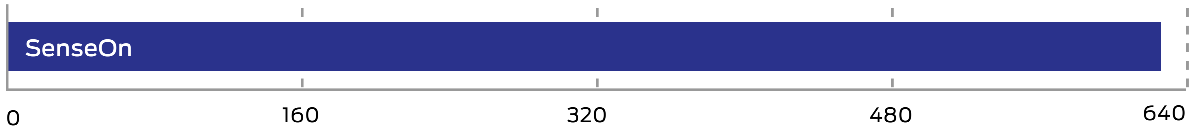
Response Details						
Attacker/ APT Group	Number of Incidents	Attacks Detected	Delivery/ Execution	Action	Privilege Escalation/ Action	Lateral Movement/ Action
Turla	4	4	4	4	4	4
Ke3chang	4	4	4	3	4	3
Threat Group-3390	4	4	4	4	4	4
Kimsuky	4	4	4	4	4	4
Total	**16**	**16**	**16**	**15**	**16**	**15**

This data shows how the product handled different group stages of each APT. The Detection column shows the basic level of detection.

Detection Accuracy Rating Details				
Attacker/ APT Group	Number of Incidents	Attacks Detected	Group Detections	Detection Rating
Turla	4	4	16	160
Ke3chang	4	4	14	140
Threat Group-3390	4	4	16	160
Kimsuky	4	4	16	160
Total	**16**	**16**	**62**	**620**

Different levels of detection, and failure to detect, are used to calculate the Detection Rating.

Detection Accuracy Ratings		
Product	Detection Accuracy Rating	Detection Accuracy Rating (%)
SenseOn	620	97%



Detection Ratings are weighted to show that how products detect threats can be subtler than just 'win' or 'lose'.

Group Detections

We record detections in groups, as described above in Understanding Detection Groups. To get an overview of how a product handled the entire set of threats we then combine these detections into 'Group Detections'.

In a test with four incidents and four detection groups (Delivery/Execution; Action; Escalation/ PE Action; and Lateral Movement/ Lateral Action) the maximum score would be 16. This is because for each of the four threats a product that detects everything would score 4.

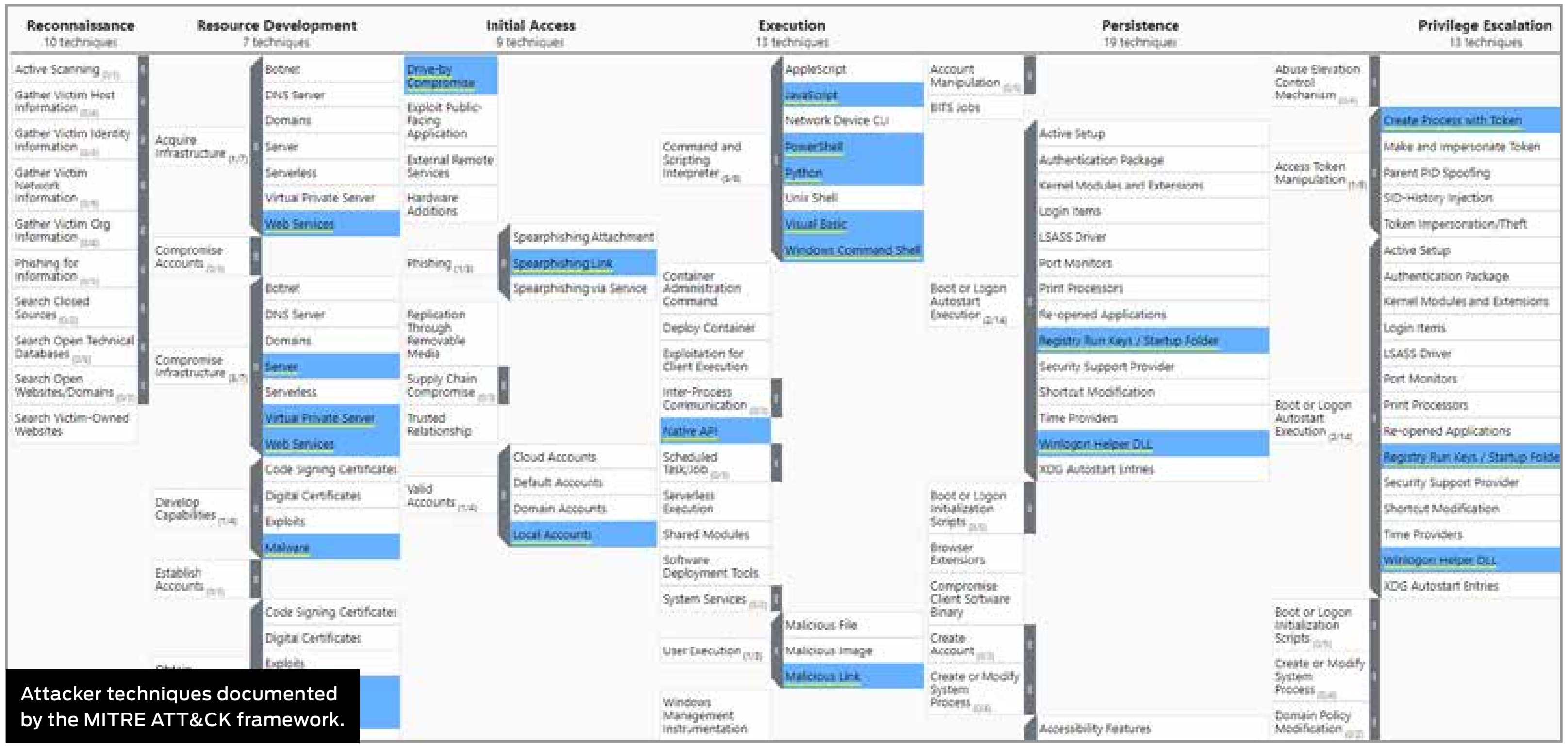
Our overall Detection Rating is based on the number of Detection Groups achieved.

4. Threat Intelligence

Turla

This Russia-based threat group targets victims in different countries and across a wide range of industries. These include governmental organisations, notably including embassies and the military. Its main purpose is gathering intelligence.

Reference Link:
https://attack.mitre.org/groups/G0010/



Reconnaissance 10 techniques
Active Scanning
Gather Victim Host Information
Gather Victim Identity Information
Gather Victim Network Information
Gather Victim Org Information
Phishing for Information
Search Closed Sources
Search Open Technical Databases
Search Open Websites/Domains
Search Victim-Owned Websites

Resource Development 7 techniques
Acquire Infrastructure (1/7): Botnet, DNS Server, Domains, Server, Serverless, Virtual Private Server, Web Services
Compromise Accounts
Compromise Infrastructure (3/7): Botnet, DNS Server, Domains, Server, Serverless, Virtual Private Server, Web Services
Develop Capabilities (1/4): Code Signing Certificates, Digital Certificates, Exploits, Malware
Establish Accounts
Obtain Capabilities: Code Signing Certificates, Digital Certificates, Exploits

Initial Access 9 techniques
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing (1/3): Spearphishing Attachment, Spearphishing Link, Spearphishing via Service
Replication Through Removable Media
Supply Chain Compromise
Trusted Relationship
Valid Accounts (1/4): Cloud Accounts, Default Accounts, Domain Accounts, Local Accounts

Execution 13 techniques
Command and Scripting Interpreter (5/8): AppleScript, JavaScript, Network Device CLI, PowerShell, Python, Unix Shell, Visual Basic, Windows Command Shell
Container Administration Command
Deploy Container
Exploitation for Client Execution
Inter-Process Communication
Native API
Scheduled Task/Job
Serverless Execution
Shared Modules
Software Deployment Tools
System Services
User Execution (1/3): Malicious File, Malicious Image, Malicious Link
Windows Management Instrumentation

Persistence 19 techniques
Account Manipulation
BITS Jobs
Boot or Logon Autostart Execution (2/14): Active Setup, Authentication Package, Kernel Modules and Extensions, Login Items, LSASS Driver, Port Monitors, Print Processors, Re-opened Applications, Registry Run Keys / Startup Folder, Security Support Provider, Shortcut Modification, Time Providers, Winlogon Helper DLL, XDG Autostart Entries
Boot or Logon Initialization Scripts
Browser Extensions
Compromise Client Software Binary
Create Account
Create or Modify System Process
Accessibility Features

Privilege Escalation 13 techniques
Abuse Elevation Control Mechanism
Access Token Manipulation (1/5): Create Process with Token, Make and Impersonate Token, Parent PID Spoofing, SID-History Injection, Token Impersonation/Theft
Boot or Logon Autostart Execution (2/14): Active Setup, Authentication Package, Kernel Modules and Extensions, Login Items, LSASS Driver, Port Monitors, Print Processors, Re-opened Applications, Registry Run Keys / Startup Folde, Security Support Provider, Shortcut Modification, Time Providers, Winlogon Helper DLL, XDG Autostart Entries
Boot or Logon Initialization Scripts
Create or Modify System Process
Domain Policy Modification

Attacker techniques documented by the MITRE ATT&CK framework.

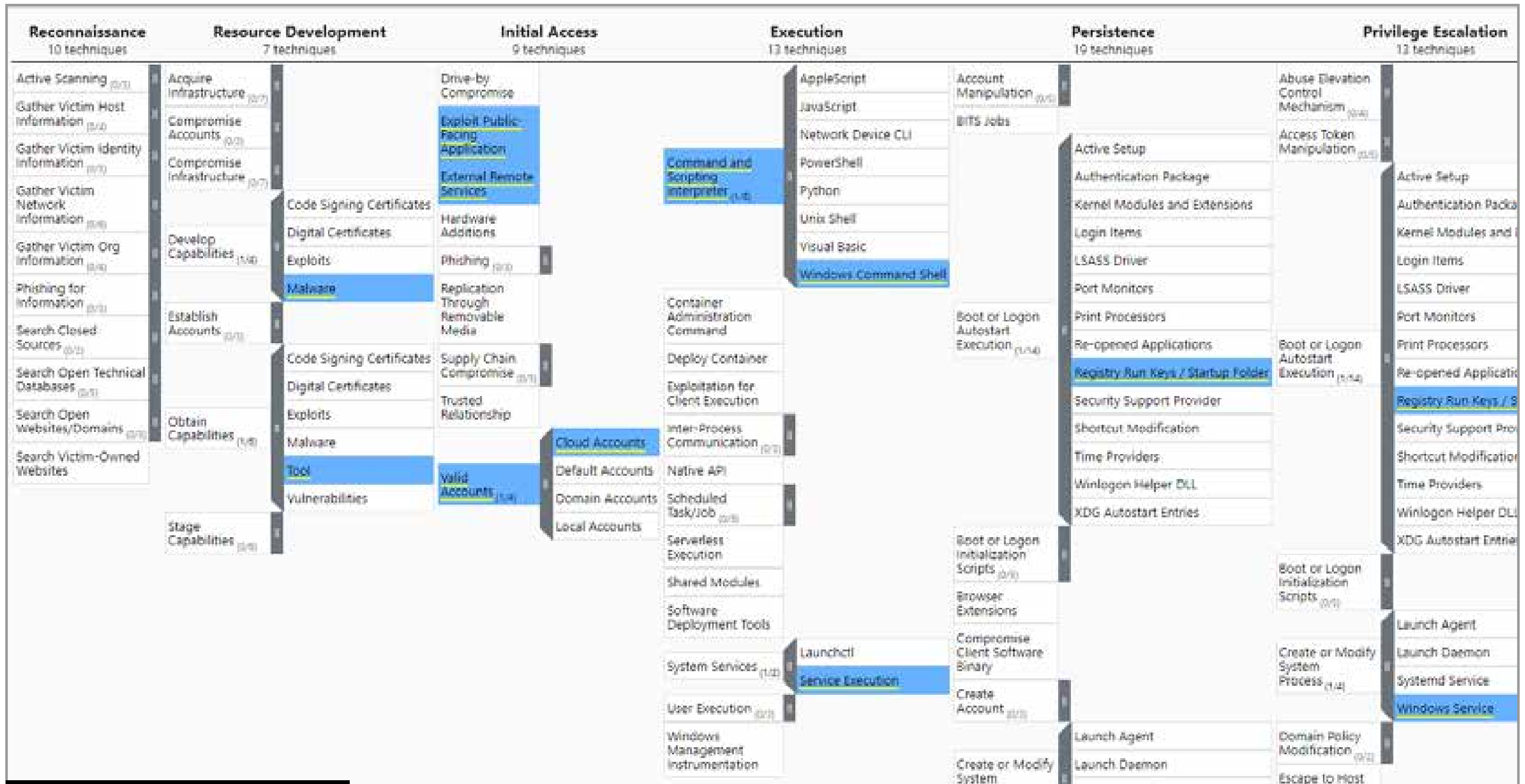
Example Turla Attack

Delivery	Execution	Action	Privilege Escalation	Post-Escalation Action	Lateral Movement	Lateral Action
Spearphishing Attachment	Windows Command Shell	System Information Discovery	Bypass UAC	Registry Run Keys / Startup Folder	SSH	Archive via Utility
	Malicious File	File and Directory Discovery		Modify Registry	SSH Hijacking	Exfiltration over C2 Channel
	Masquerade Task or Service	Process Discovery		Disable or Modify Tools		Deobfuscate/Decode Files or Information
	Match Legitimate Name or Location	Query Registry				
	PowerShell	Remote System Discovery		Powershell Profile		
	Service Execution					
	Steganography					
Spearphishing Attachment	Malicious File	System Information Discovery	Bypass UAC	Modify Registry	SSH	Exfiltration over C2 Channel

Ke3chang

Also known as APT 15, Ke3chang is a Chinese threat group that has targeted natural resource businesses and government entities. The group evades detection by abusing tools provided by target systems, and so 'lives off the land'.

Reference Link:
https://attack.mitre.org/groups/G0004/



Reconnaissance 10 techniques
- Active Scanning (0/3)
- Gather Victim Host Information (0/4)
- Gather Victim Identity Information (0/3)
- Gather Victim Network Information (0/6)
- Gather Victim Org Information (0/4)
- Phishing for Information (0/3)
- Search Closed Sources (0/2)
- Search Open Technical Databases (0/5)
- Search Open Websites/Domains (0/3)
- Search Victim-Owned Websites

Resource Development 7 techniques
- Acquire Infrastructure (0/7)
- Compromise Accounts (0/3)
- Compromise Infrastructure (0/7)
- Develop Capabilities (1/4)
  - Code Signing Certificates
  - Digital Certificates
  - Exploits
  - Malware
- Establish Accounts (0/3)
- Obtain Capabilities (1/6)
  - Code Signing Certificates
  - Digital Certificates
  - Exploits
  - Malware
  - Tool
  - Vulnerabilities
- Stage Capabilities (0/6)

Initial Access 9 techniques
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (0/3)
- Replication Through Removable Media
- Supply Chain Compromise (0/3)
- Trusted Relationship
- Valid Accounts (1/4)
  - Cloud Accounts
  - Default Accounts
  - Domain Accounts
  - Local Accounts

Execution 13 techniques
- Command and Scripting Interpreter (1/8)
  - AppleScript
  - JavaScript
  - Network Device CLI
  - PowerShell
  - Python
  - Unix Shell
  - Visual Basic
  - Windows Command Shell
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication (0/3)
- Native API
- Scheduled Task/Job (0/5)
- Serverless Execution
- Shared Modules
- Software Deployment Tools
- System Services (1/2)
  - Launchctl
  - Service Execution
- User Execution (0/3)
- Windows Management Instrumentation

Persistence 19 techniques
- Account Manipulation (0/5)
- BITS Jobs
- Boot or Logon Autostart Execution (1/14)
  - Active Setup
  - Authentication Package
  - Kernel Modules and Extensions
  - Login Items
  - LSASS Driver
  - Port Monitors
  - Print Processors
  - Re-opened Applications
  - Registry Run Keys / Startup Folder
  - Security Support Provider
  - Shortcut Modification
  - Time Providers
  - Winlogon Helper DLL
  - XDG Autostart Entries
- Boot or Logon Initialization Scripts (0/5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (0/3)
- Create or Modify System Process (1/4)
  - Launch Agent
  - Launch Daemon
  - Systemd Service

Privilege Escalation 13 techniques
- Abuse Elevation Control Mechanism (0/4)
- Access Token Manipulation (0/5)
- Boot or Logon Autostart Execution (1/14)
  - Active Setup
  - Authentication Packa
  - Kernel Modules and
  - Login Items
  - LSASS Driver
  - Port Monitors
  - Print Processors
  - Re-opened Applicati
  - Registry Run Keys / S
  - Security Support Pro
  - Shortcut Modificatio
  - Time Providers
  - Winlogon Helper DL
  - XDG Autostart Entrie
- Boot or Logon Initialization Scripts (0/5)
- Create or Modify System Process (1/4)
  - Launch Agent
  - Launch Daemon
  - Systemd Service
  - Windows Service
- Domain Policy Modification (0/2)
- Escape to Host

Attacker techniques documented by the MITRE ATT&CK framework.

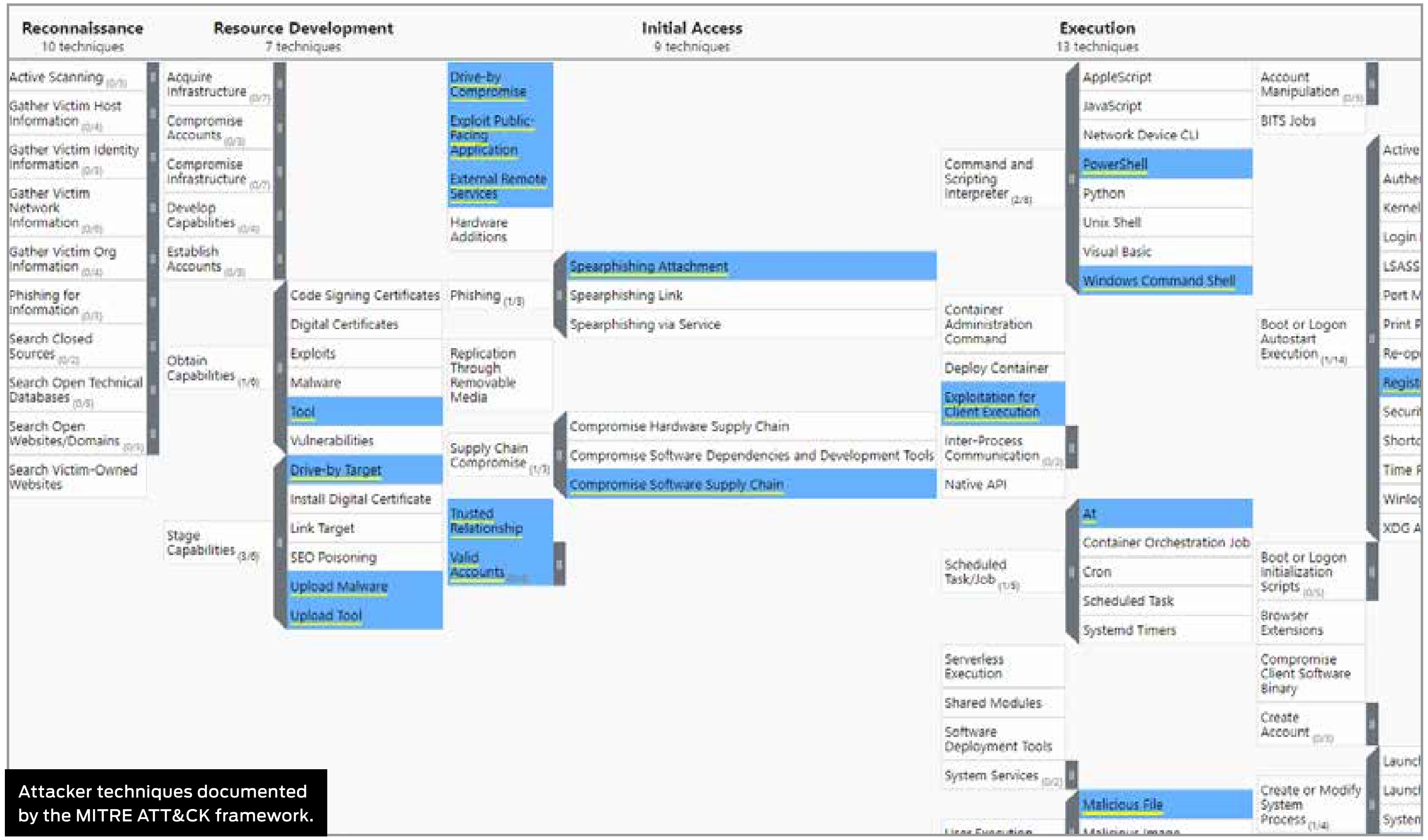
Example Ke3chang Attack

Delivery	Execution	Action	Privilege Escalation	Post-Escalation Action	Lateral Movement	Lateral Action
Exploit Public-Facing Application	Command and Scripting Interpreter	File and Directory Discovery	Valid Accounts	Registry Run Keys /Startup Folder	SMB/Windows Admin Shares	Keylogging
	Windows Command Shell	Process Discovery		Ingress Tool Transfer		Automated Collection
	Right-to-Left Override	System Information Discovery		LSA Secrets		Automated Exfiltration
	Web Protocols	System Network Configuration Discovery		LSASS Memory		
		System Network Connections Discovery		NTDS		
Exploit Public-Facing Application	Web Protocols	System Network Configuration Discovery	Valid Accounts	Ingress Tool Transfer	SMB/Windows Admin Shares	Keylogging

Threat Group-3390

A China-based APT, Threat Group-3390 has targeted US and UK organisations from a wide range of industries. It has used hundreds of compromised websites in its attacks against natural resource businesses and government entities.

References:
https://attack.mitre.org/groups/G0027/



Reconnaissance
10 techniques
Active Scanning (0/3)
Gather Victim Host Information (0/4)
Gather Victim Identity Information (0/3)
Gather Victim Network Information (0/6)
Gather Victim Org Information (0/4)
Phishing for Information (0/3)
Search Closed Sources (0/2)
Search Open Technical Databases (0/5)
Search Open Websites/Domains (0/3)
Search Victim-Owned Websites

Resource Development
7 techniques
Acquire Infrastructure (0/7)
Compromise Accounts (0/3)
Compromise Infrastructure (0/7)
Develop Capabilities (0/4)
Establish Accounts (0/3)
Obtain Capabilities (1/6)
Code Signing Certificates
Digital Certificates
Exploits
Malware
Tool
Vulnerabilities
Stage Capabilities (3/6)
Drive-by Target
Install Digital Certificate
Link Target
SEO Poisoning
Upload Malware
Upload Tool

Initial Access
9 techniques
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing (1/3)
Spearphishing Attachment
Spearphishing Link
Spearphishing via Service
Replication Through Removable Media
Supply Chain Compromise (1/3)
Compromise Hardware Supply Chain
Compromise Software Dependencies and Development Tools
Compromise Software Supply Chain
Trusted Relationship
Valid Accounts

Execution
13 techniques
Command and Scripting Interpreter (2/9)
AppleScript
JavaScript
Network Device CLI
PowerShell
Python
Unix Shell
Visual Basic
Windows Command Shell
Container Administration Command
Deploy Container
Exploitation for Client Execution
Inter-Process Communication (0/3)
Native API
Scheduled Task/Job (1/5)
At
Container Orchestration Job
Cron
Scheduled Task
Systemd Timers
Serverless Execution
Shared Modules
Software Deployment Tools
System Services (0/2)
User Execution
Malicious File
Malicious Image

Account Manipulation (0/5)
BITS Jobs
Boot or Logon Autostart Execution (1/14)
Active
Authe
Kernel
Login
LSASS
Port M
Print P
Re-op
Regist
Securi
Shortc
Time P
Winlog
XDG A
Boot or Logon Initialization Scripts (0/5)
Browser Extensions
Compromise Client Software Binary
Create Account (0/3)
Launc
Launc
Systen
Create or Modify System Process (1/4)

Attacker techniques documented by the MITRE ATT&CK framework.

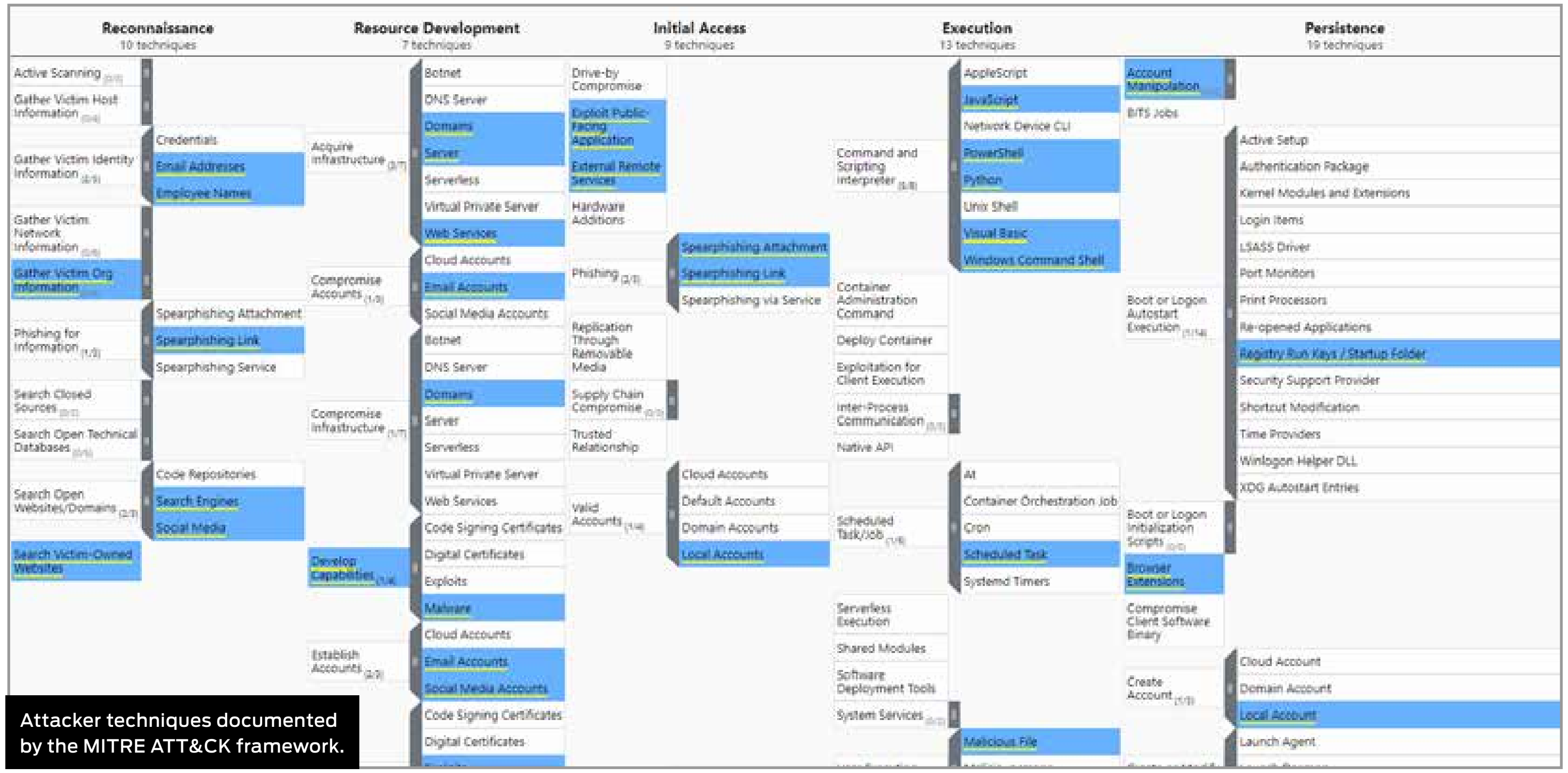
Example Threat Group-3390 Attack

Delivery	Execution	Action	Privilege Escalation	Post-Escalation Action	Lateral Movement	Lateral Action
Spearphishing Attachment	PowerShell	Local Account	Bypass UAC	Registry Run Keys / Startup Folder	External Remote Services	Local Data Staging
	Windows Command Shell	Query Registry		Windows Service		Archive via Library
	Exploitation for Client Execution	System Network Connections Discovery		LSA Secrets		Data Transfer Size Limits
		Remote System Discovery		Security Account Manager		Exfiltration via C2 Channel
				Keylogging		
Spearphishing Attachment	Windows Command Shell	Query Registry	Bypass UAC	Keylogging	External Remote Services	Exfiltration via C2 Channel

Kimsuky

This North Korean espionage group has largely focussed on South Korean thinktanks but has also attacked US and European companies. Its interest appear to be mostly around government organisations and research companies working on COVID-19 vaccinations.

References:
https://attack.mitre.org/groups/G0094/



Reconnaissance 10 techniques
- Active Scanning (0/3)
- Gather Victim Host Information (0/4)
- Gather Victim Identity Information (2/3)
  - Credentials
  - Email Addresses
  - Employee Names
- Gather Victim Network Information (0/6)
- Gather Victim Org Information
- Phishing for Information (1/3)
  - Spearphishing Attachment
  - Spearphishing Link
  - Spearphishing Service
- Search Closed Sources (0/2)
- Search Open Technical Databases (0/5)
- Search Open Websites/Domains (2/3)
  - Code Repositories
  - Search Engines
  - Social Media
- Search Victim-Owned Websites

Resource Development 7 techniques
- Acquire Infrastructure (3/7)
  - Botnet
  - DNS Server
  - Domains
  - Server
  - Serverless
  - Virtual Private Server
  - Web Services
- Compromise Accounts (1/3)
  - Cloud Accounts
  - Email Accounts
  - Social Media Accounts
- Compromise Infrastructure (1/7)
  - Botnet
  - DNS Server
  - Domains
  - Server
  - Serverless
  - Virtual Private Server
  - Web Services
- Develop Capabilities (1/4)
  - Code Signing Certificates
  - Digital Certificates
  - Exploits
  - Malware
- Establish Accounts (2/3)
  - Cloud Accounts
  - Email Accounts
  - Social Media Accounts
  - Code Signing Certificates
  - Digital Certificates

Initial Access 9 techniques
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (2/3)
  - Spearphishing Attachment
  - Spearphishing Link
  - Spearphishing via Service
- Replication Through Removable Media
- Supply Chain Compromise (0/3)
- Trusted Relationship
- Valid Accounts (1/4)
  - Cloud Accounts
  - Default Accounts
  - Domain Accounts
  - Local Accounts

Execution 13 techniques
- Command and Scripting Interpreter (6/8)
  - AppleScript
  - JavaScript
  - Network Device CLI
  - PowerShell
  - Python
  - Unix Shell
  - Visual Basic
  - Windows Command Shell
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication (0/3)
- Native API
- Scheduled Task/Job (1/5)
  - At
  - Container Orchestration Job
  - Cron
  - Scheduled Task
  - Systemd Timers
- Serverless Execution
- Shared Modules
- Software Deployment Tools
- System Services (0/2)
  - Malicious File

Persistence 19 techniques
- Account Manipulation
- BITS Jobs
- Boot or Logon Autostart Execution (1/14)
  - Active Setup
  - Authentication Package
  - Kernel Modules and Extensions
  - Login Items
  - LSASS Driver
  - Port Monitors
  - Print Processors
  - Re-opened Applications
  - Registry Run Keys / Startup Folder
  - Security Support Provider
  - Shortcut Modification
  - Time Providers
  - Winlogon Helper DLL
  - XDG Autostart Entries
- Boot or Logon Initialization Scripts (0/5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (1/3)
  - Cloud Account
  - Domain Account
  - Local Account
  - Launch Agent

Attacker techniques documented by the MITRE ATT&CK framework.

Example Kimsuky Attack

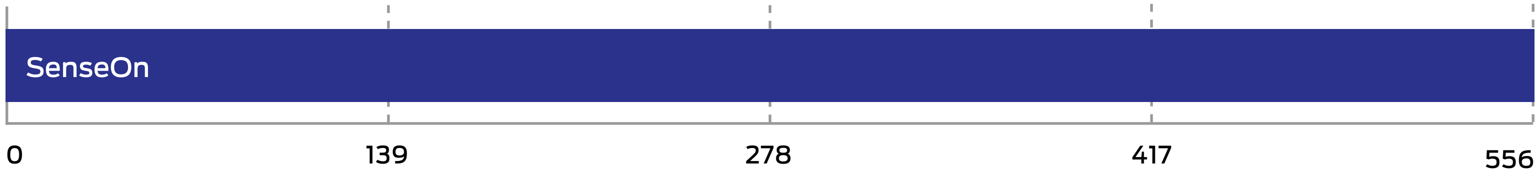
Delivery	Execution	Action	Privilege Escalation	Post-Escalation Action	Lateral Movement	Lateral Action
Spearphishing Attachment	Visual Basic	File and Directory Discovery	Bypass UAC	Process Injection	Pass the Hash	Keylogging
	Code Signing	Process Discovery		Registry Run Keys / Startup Folder	External Remote Services	Local Data Staging
	Web Protocols	System Information Discovery		Scheduled Task		Archive via Utility
	Windows Command Shell	System Network Configuration Discovery		Query Registry		Data from Local System
	Malicious File	System Service Discovery		Ingress Tool Transfer		Exfiltration Over C2 Channel
	Masquerading Task or Service			LSASS Memory		
				Match Legitimate name or Location		
				File Deletion		
Spearphishing Attachment	Visual Basic	System Network Configuration Discovery	Bypass UAC	File Deletion	External Remote Services	Keylogging

5. Legitimate Software Rating

These ratings indicate how accurately the product classifies legitimate applications and URLs, while also taking into account the interactions that the product has with the user. Ideally a product will either not classify a legitimate object or will classify it as safe. In neither case should it bother the user.

We also take into account the prevalence (popularity) of the applications and websites used in this part of the test, applying stricter penalties for when products misclassify very popular software and sites.

Legitimate Software Ratings		
Product	Legitimate Accuracy Rating	Legitimate Accuracy (%)
SenseOn	556	100%



Legitimate Software Ratings can indicate how well a vendor has tuned its detection engine.

Subscribe
Past Issues
Translate
SE Labs
INTELLIGENCE-LED TESTING
News from the security lab
FREE
Security opportunities for Managed Service Providers
Most popular reports of 2022
Your

6. Conclusions

This test exposed **SenseOn** to a diverse set of exploits, file-less attacks and malware attachments, comprising the widest range of threats in any currently available public test.

All of these attack types have been witnessed in real-world attacks over the previous few years. They are representative of a real and present threat to business networks the world over. The threats used in this are similar or identical to those used by the threat groups listed in **Hackers vs. Targets** on page 9 and **4. Threat Intelligence** on pages 13 – 16.

It is important to note that while the test used the same types of attacks, new files were used. This exercised the tested product's abilities to detect and protect against certain approaches to attacking systems rather than simply detecting malicious files that have become well-known over the previous few years. The results are an indicator of potential future performance rather than just a compliance check that the product can detect old attacks.

The product detected all of the threats on a basic level, in that for each attack it detected at least some element of the attack chain. Even better, it also detected in depth, capturing details as each threat proceeded down the attack chain from the initial introduction to the system through to execution and subsequent behaviour by the attacker.

In one case it failed to detect actions by the attackers. However, in that specific test case it detected the delivery of the attack to the target and the subsequent actions of the attacker, including gaining greater access to the target (privilege escalation) and moving to new targets.

In eight other cases the threats were delivered quietly, without detection, but were then noticed as they ran and committed almost all further actions. In the real world all these attacks would be detected at multiple stages.

The results are strong, and all attacks were detected in a comprehensive way. Sometimes products are overly aggressive and detect everything, including threats and legitimate objects. In this test **SenseOn** generated no such false positive results, which is as hoped. **SenseOn** wins a AAA award for its excellent performance.

Appendices

Appendix A: Terms Used

Term	Meaning
Compromised	The attack succeeded, resulting in malware running unhindered on the target. In the case of a targeted attack, the attacker was able to take remote control of the system and carry out a variety of tasks without hindrance.
Blocked	The attack was prevented from making any changes to the target.
False positive	When a security product misclassifies a legitimate application or website as being malicious, it generates a 'false positive'.
Neutralised	The exploit or malware payload ran on the target but was subsequently removed.
Complete Remediation	If a security product removes all significant traces of an attack, it has achieved complete remediation.
Target	The test system that is protected by a security product.
Threat	A program or sequence of interactions with the target that is designed to take some level of unauthorised control of that target.
Update	Security vendors provide information to their products in an effort to keep abreast of the latest threats. These updates may be downloaded in bulk as one or more files, or requested individually and live over the internet.

Appendix B: FAQs

A **full methodology** for this test is available from our website.

- The test was conducted between 17th April and 2nd May 2023.
- The product was configured according to its vendor's recommendations.
- Targeted attacks were selected and verified by SE Labs.
- Malicious and legitimate data was provided to partner organisations once the test was complete.

Q What is a partner organisation? Can I become one to gain access to the threat data used in your tests?

A Partner organisations benefit from our consultancy services after a test has been run. Partners may gain access to low-level data that can be useful in product improvement initiatives and have permission to use award logos, where appropriate, for marketing purposes. We do not share data on one partner with other partners. We do not partner with organisations that do not engage in our testing.

Q We are a customer considering buying or changing our endpoint protection and/ or endpoint detection and response (EDR) product. Can you help?

A Yes, we frequently run private testing for organisations that are considering changing their security products. Please contact us at **info@selabs.uk** for more information.

Appendix C: Attack Details

Turla

Delivery	Execution	Action	Post-Esclation Action	Post-Escalation Action	Lateral Movement	Lateral Action
Spearphishing Attachment	Asymmetric Cryptography	Domain Groups	Bypass User Account Control	Code Signing Policy Modification	Lateral Tool Transfer	Archive via Utility
Spearphishing Link	Bidirectional Communication	File and Directory Discovery	Create Process with Token	Disable or Modify Tools	SMB/Windows Admin Shares	Automated Collection
	Indicator Removal from Tools	Internet Connection Discovery	Token Impersonation/Theft	Disable Windows Event Logging	SSH	Automated Exfiltration
	JavaScript	Local Account		Domain Account	SSH Hijacking	Data from Local System
	Mail Protocols	Local Groups		Dynamic-link Library Injection		Data Transfer Size Limits
	Malicious File	Process Discovery		Email Hiding Rules		Deobfuscate/Decode Files or Information
	Malicious Link	Query Registry		Modify Registry		Exfiltration Over Alternative Protocol
	Masquerade Task or Service	Remote System Discovery		PowerShell Profile		Exfiltration Over C2 Channel
	Match Legitimate Name or Location	System Information Discovery		Registry Run Keys / Startup Folder		Ingress Tool Transfer
	PowerShell	System Network Configuration Discovery		Security Software Discovery		Local Data Staging
	Python	System Network Connections Discovery		Windows Credential Manager		Scheduled Transfer
	Service Execution	System Owner/User Discovery		Windows File and Directory Permissions Modification		
	Steganography	System Service Discovery		Windows Management Instrumentation Event Subscription		
	Visual Basic	System Time Discovery		Winlogon Helper DLL		
	Web Protocols					
	Windows Command Shell					
	Windows Service					

Ke3chang

Delivery	Execution	Action	Privilege Escalation	Post-Esclation Action	Lateral Movement	Lateral Action
Exploit Public-Facing Application	Command and Scripting Interpreter	Domain Account	Valid Accounts	Registry Run Keys /Startup Folder	SMB/Windows Admin Shares	Archive Collected Data
External Remote Services	Windows Command Shell	Local Account		Match Legitimate Name or Location	Service Execution	Archive via Utility
	DNS	File and Directory Discovery		Valid Accounts		Automated Collection
	Web Protocols	Domain Groups		Keylogging		Sharepoint
	Deobfuscate/Decode Files or Information	Process Discovery		LSA Secrets		Data from Local System
	Right-to-Left Override	Remote System Discovery		LSASS Memory		Remote Email Collection
	Obfuscated Files or Information	System Information Discovery		NTDS		Keylogging
	Cloud Accounts	System Language Discovery		Security Account Manager		Automated Exfiltration
		System Network Configuration Discovery		Golden Ticket		Exfiltration Over C2 Channel
		System Network Connections Discovery		Windows Service		
		System Owner/User Discovery		Ingress Tool Transfer		
		System Service Discovery				

Threat Group-3390

Delivery	Execution	Action	Privilege Escalation	Post-Esclation Action	Lateral Movement	Lateral Action
Drive-by Compromise	PowerShell	Local Account	Bypass User Account Control	Registry Run Keys / Startup Folder	Exploitation of Remote Services	Archive via Library
Exploit Public-Facing Application	Windows Command Shell	Network Service Discovery	Exploitation for Privilege Escalation	Windows Service	Windows Remote Management	Automated Collection
Spearphishing Attachment	Exploitation for Client Execution	Query Registry	Valid Accounts	DLL Search Order Hijacking	Ingress Tool Transfer	Data from Local System
	Malicious File	Remote System Discovery		DLL Side-Loading	External Remote Services	Local Data Staging
	Web Protocols	System Network Configuration Discovery		Process Hollowing		Remote Data Staging
	Obfuscated Files or Information	System Network Connections Discovery		Password Managers		Keylogging
	Deobfuscate/Decode File or Information	System Owner/User Discovery		Keylogging		Data Transfer Size Limits
	Web Shell			LSA Secrets		Exfiltration to Cloud Storage
	Software Packing			LSASS Memory		Network Share Connection Removal
	Trusted Relationship			Security Account Manager		
	Compromise Software Supply Chain			File Deletion		
				Windows Management Instrumentation		
				Disable Window Event Logging		
				Modify Registry		

Kimsuky

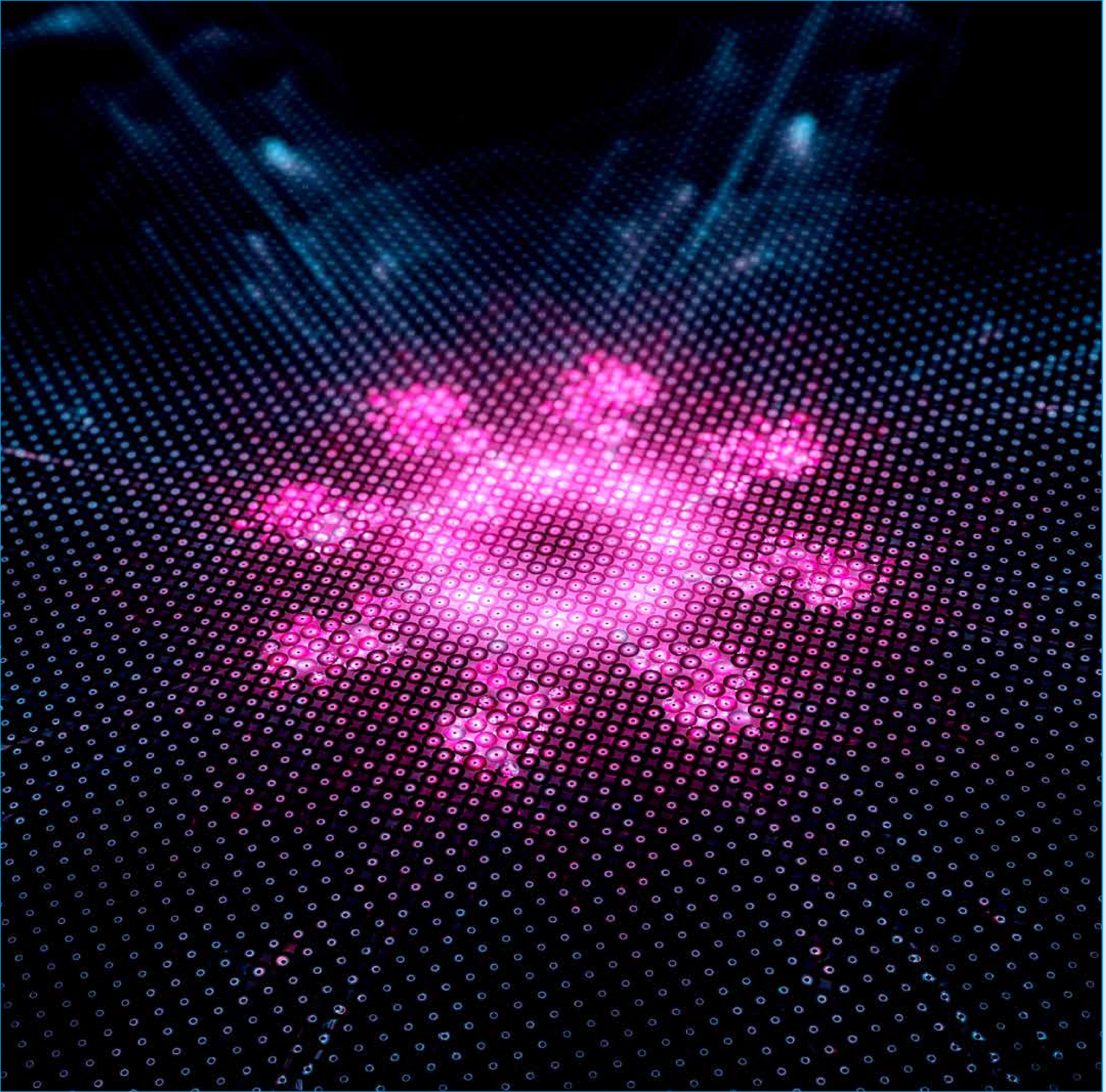
Delivery	Execution	Action	Privilege Escalation	Post-Esclation Action	Lateral Movement	Lateral Action
Exploit Public-Facing Application	JavaScript	File and Directory Discovery	Valid Accounts	Registry Run Keys / Startup Folder	Internal Spearphishing	Archive via Custom Method
Spearphishing Attachment	PowerShell	Process Discovery		Windows Service	Remote Desktop Protocol	Archive via Utility
Spearphishing Link	Python	Security Software Discovery		Process Injection	Pass the Hash	Data from Local System
	Visual Basic	System Information Discovery		Process Hollowing	Remote Access Software	Local Data Staging
	Windows Command Shell	System Network Configuration Discovery		Scheduled Task	External Remote Services	Email Forwarding Rule
	Malicious File	System Service Discovery		Hidden Users		Remote Email Collection
	Malicious Link	Credentials from Web Browsers		Hidden Window		Keylogging
	Mshta	Browser Extensions		Disable or Modify System Firewall		Exfiltration Over C2 Channel
	Web Shell			Disable or Modify Tools		Exfiltration to Cloud Storage
	Deobfuscated/Decode Files or Information			File Deletion		
	Software Packing			Timestomp		
	Obfuscated Files or Information			Local Accounts		
	Code Signing			Match Legitimate name or Location		
	Regsvr32			Modify Registry		
	Rundll32			Query Registry		
	Bidirectional Communication			Adversary-in-the-Middle		
	File Transfer Protocols			Account Manipulation		
	Mail Protocols			Keylogging		
	Web Protocols			Multi-Factor Authentication Interception		
	Adversary-in-the-Middle			Network Sniffing		
	Masquerading Task or Service			LSASS Memory		
				Credentials in Files		
				Ingress Tool Transfer		
				Change Default File Association		

Appendix D: Product Version

The table below shows the service's name as it was being marketed at the time of the test.

Product Versions

Vendor	Product	Build Version (start)	Build Version (end)
SenseOn	SenseOn	5.8.3-dual-running-am	5.8.3-dual-running-am



SE Labs

SE Labs Report Disclaimer

1. The information contained in this report is subject to change and revision by SE Labs without notice.
2. SE Labs is under no obligation to update this report at any time.
3. SE Labs believes that the information contained within this report is accurate and reliable at the time of its publication, which can be found at the bottom of the contents page, but SE Labs does not guarantee this in any way.
4. All use of and any reliance on this report, or any information contained within this report, is solely at your own risk. SE Labs shall not be liable or responsible for any loss of profit (whether incurred directly or indirectly), any loss of goodwill or business reputation, any loss of data suffered, pure economic loss, cost of procurement of substitute goods or services, or other intangible loss, or any indirect, incidental, special or consequential loss, costs, damages, charges or expenses or exemplary damages arising his report in any way whatsoever.
5. The contents of this report does not constitute a recommendation, guarantee, endorsement or otherwise of any of the products listed, mentioned or tested.
6. The testing and subsequent results do not guarantee that there are no errors in the products, or that you will achieve the same or similar results. SE Labs does not guarantee in any way that the products will meet your expectations, requirements, specifications or needs.
7. Any trade marks, trade names, logos or images used in this report are the trade marks, trade names, logos or images of their respective owners.
8. The contents of this report are provided on an “AS IS” basis and accordingly SE Labs does not make any express or implied warranty or representation concerning its accuracy or completeness.