SE Labs

INTELLIGENCE-LED TESTING

Enterprise Advanced Security

Enterprise

EDR DETECTION

Apr - Jun 2023

SE Labs tested a variety of Endpoint Detection and Response products 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

Publication and Marketing
Colin Mackleworth
Sara Claridge
Janice Sheridan

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 19th July 2023

Introduction

Endpoint Detection Compared

We compare endpoint security products directly using real, major threats

Welcome to the second edition of the Enterprise Advanced Security test that compares different endpoint security products directly. We look at how they handle the major threats that face all businesses, from the Global 100 and down to medium enterprises. Most likely small businesses, too. We give an overall score but also dig down into the details that your security team will care about. This report explains the different levels of coverage that these products provide.

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 cyber criminal behaviour and builds tests based on how bad guys try to compromise victims.

The cyber security 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 **Appendix A: Threat Intelligence**, starting on page 16. 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

SE Labs ran real, significant attacks against market leading EDR products to assess their abilities to detect threats. These attacks were designed to compromise systems and penetrate target networks in the same way that criminals and other attackers breach systems and networks.

We examined each product's abilities to:

- **Detect the delivery of targeted attacks**
- **Track different elements of the attack chain…**
- **…including compromises beyond the endpoint, to the wider network**

Legitimate files were used alongside the threats to measure any false positive detections or other sub-optimal interactions.

All products were able to detect some part of each targeted attack. They were also capable of tracking most of the subsequent malicious activities that occurred during the attacks.

The products that achieved perfect scores for detection accuracy and effective response were **CrowdStrike Falcon**, **Kaspersky EDR Expert** and **Symantec Endpoint Security Complete**. **Microsoft 365 Defender** came close, achieving a 97% Detection Accuracy Rating.

Malwarebytes EDR also put in a strong performance with its 89% Detection Accuracy Rating. **Bitdefender GravityZone** was less accurate, scoring a 67% Detection Accuracy Rating for missing some threat elements. All the products handled legitimate applications appropriately, allowing them to run unimpeded.

Executive Summary				
Products Tested	Attacks Detected (%)	Detection Accuracy (%)	Legitimate Accuracy Rating (%)	Total Accuracy Rating (%)
CrowdStrike Falcon	100%	100%	100%	100%
Kaspersky EDR Expert	100%	100%	100%	100%
Symantec Endpoint Security Complete	100%	100%	100%	100%
Microsoft 365 Defender	100%	97%	100%	98%
Malwarebytes EDR	100%	89%	100%	94%
Bitdefender GravityZone	100%	67%	100%	82%

Products highlighted in green were the most accurate, scoring 85 per cent or more for Total Accuracy. Those in orange scored less than 85 but 75 or more. Products shown in red scored less than 75 per cent.

For exact percentages, see **2. Total Accuracy Ratings** on page 11.

Enterprise Advanced Security Detection Award

The following products win SE Labs awards:

- **CrowdStrike** Falcon
- **Kaspersky** EDR Expert
- **Microsoft** 365 Defender
- **Symantec** Endpoint Security Complete
- **Malwarebytes** EDR

- **Bitdefender** GravityZone

1. How We Tested

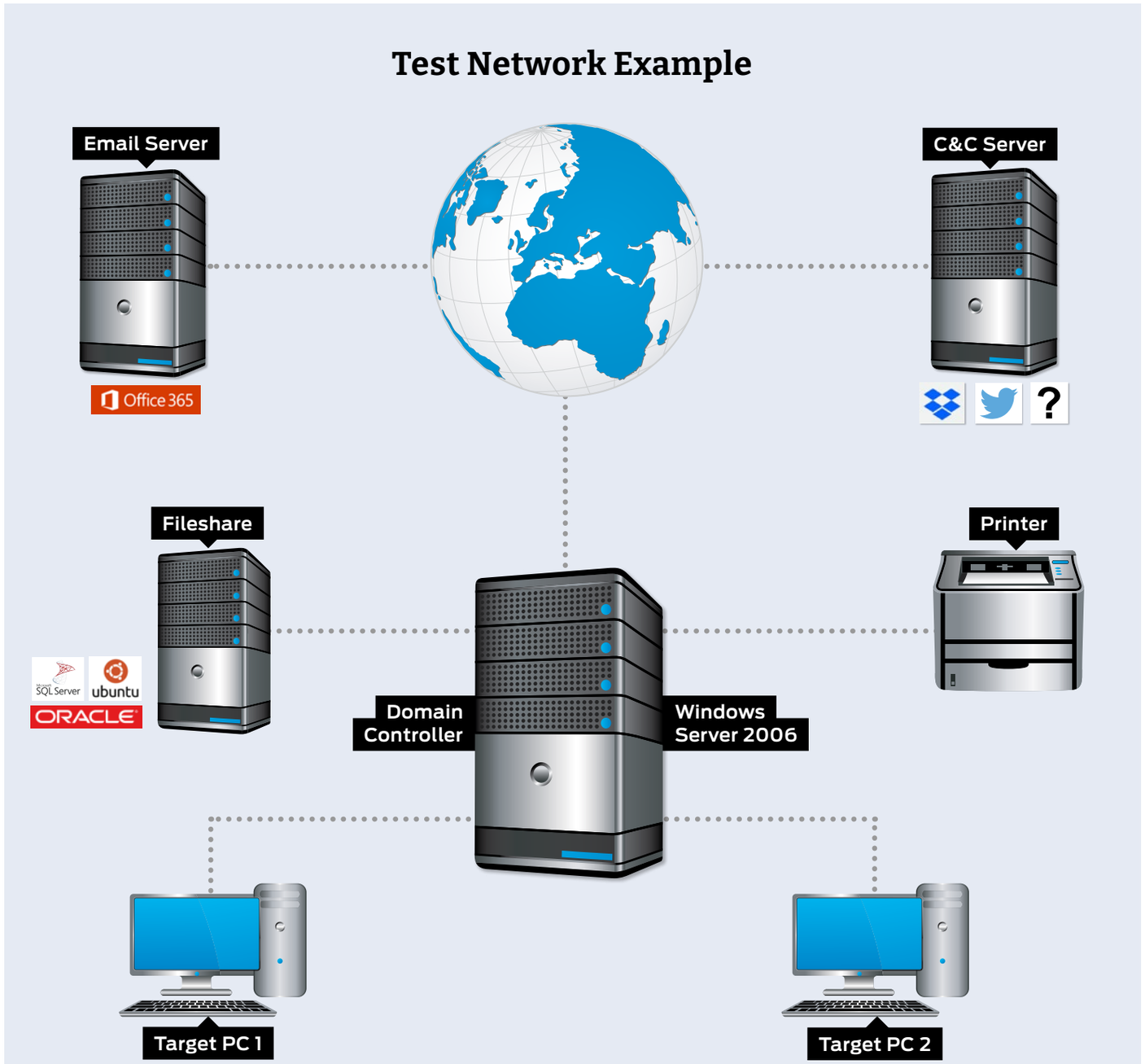
Testers can't assume that products will work a certain way, so running a realistic advanced security test means setting up real networks and hacking them in the same way that real adversaries behave.

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 8, 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 10 and, for a really detailed drill down on the details, **Appendix A: Threat Intelligence** on pages 16 to 19 and **Appendix F: Attack Details**.



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 contain 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.

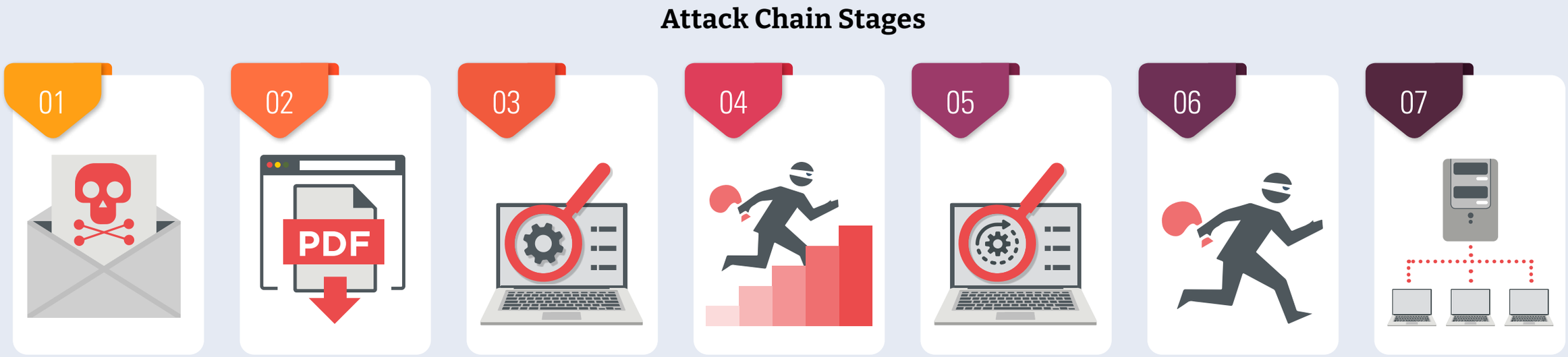


Figure 1. A typical attack starts with an initial contact and progresses through various stages, including reconnaissance, stealing data and causing damage.

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

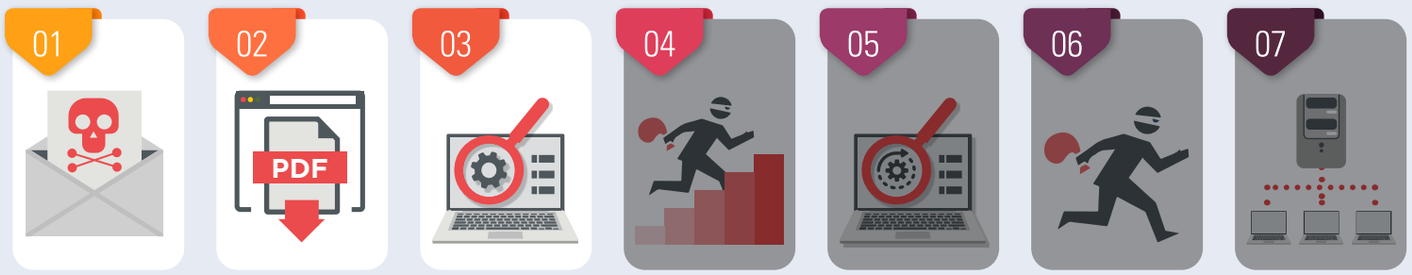


Figure 2. This attack was initially successful but only able to progress as far as the reconnaissance phase

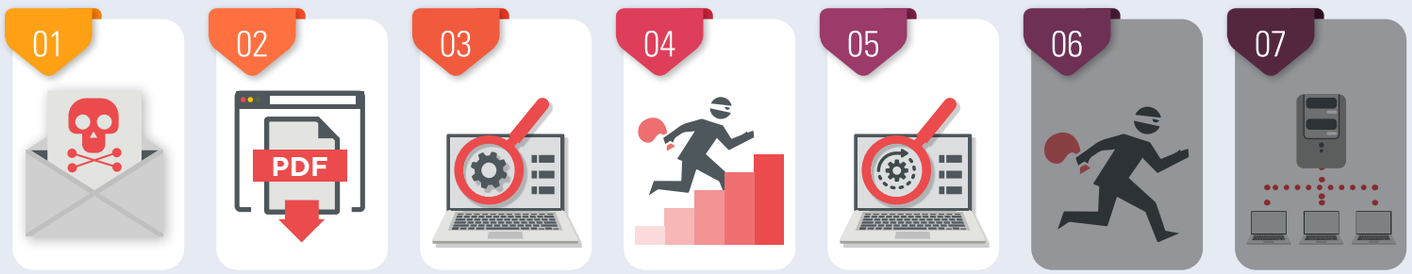


Figure 3. A more successful attack manages to steal passwords but wholesale data theft and destruction was blocked.

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 **Appendix A: Threat Intelligence** on pages 16 to 19.

Hackers vs. Targets			
Attacker/APT Group	**Method**	**Target**	**Details**
Turla			Spear phishing 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

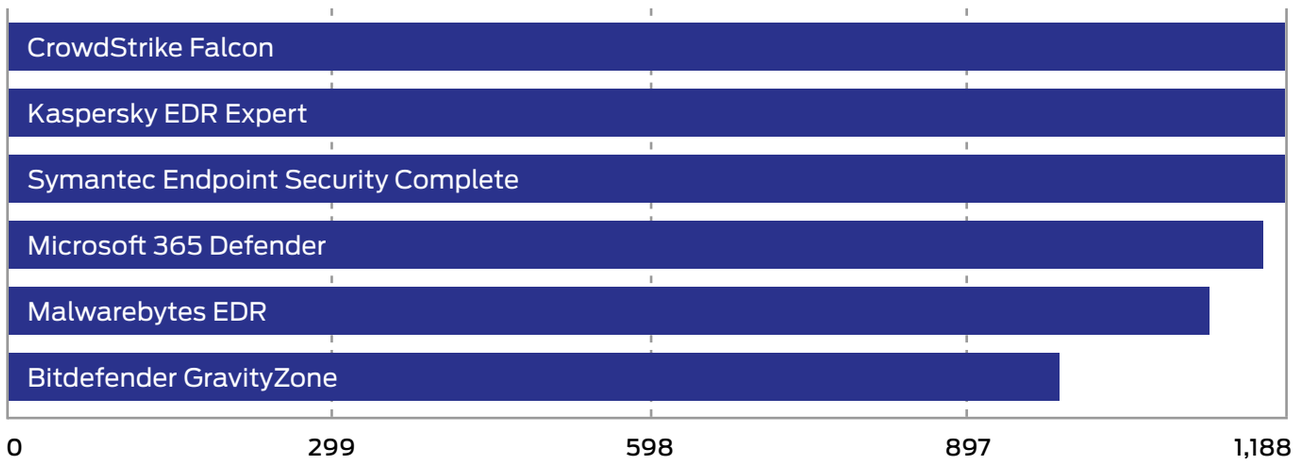
This test examines the total insight a product has, or can provide, into a specific set of attacking actions. We've divided the attack chain into chunks of one or more related actions. To provide sufficient insight, a product must detect at least one action in each chunk.

If you look at the results tables in **Appendix B: Detailed Response** on page 20 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
CrowdStrike Falcon	1,188	100%	**AAA**
Kaspersky EDR Expert	1,188	100%	**AAA**
Symantec Endpoint Security Complete	1,188	100%	**AAA**
Microsoft 365 Defender	1,168	98%	**AAA**
Malwarebytes EDR	1,118	94%	**AAA**
Bitdefender GravityZone	978	82%	**AA**



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

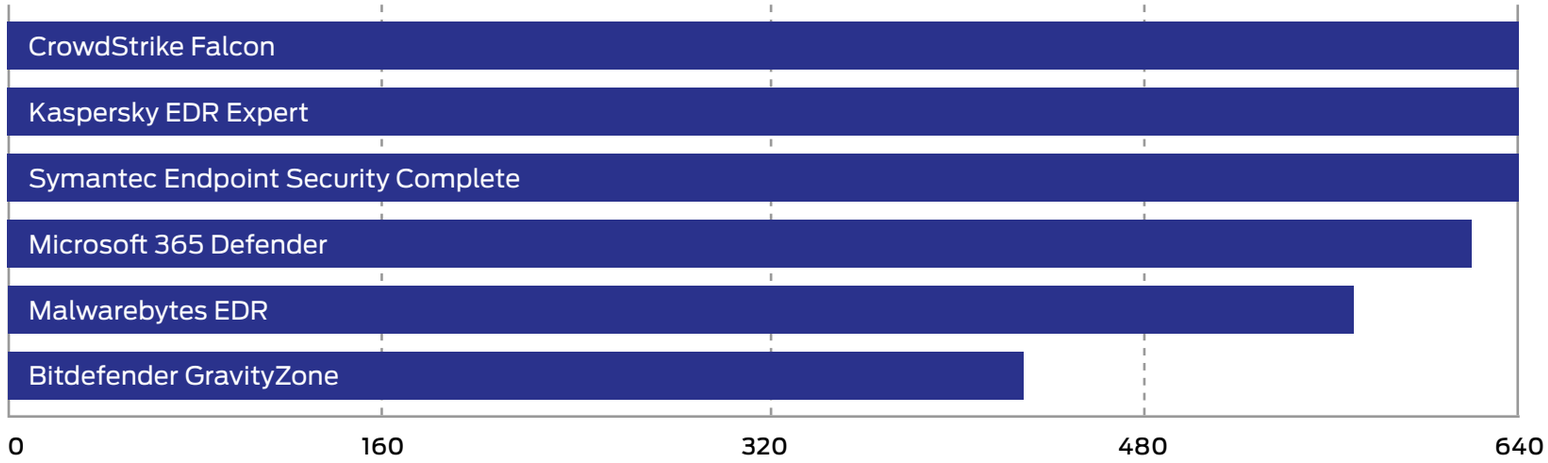
Elements of the attack chain are put into groups. For example, the Delivery and Execution stages of an attack are in the same group. Similarly, we group the Post Escalation stage with the Post Escalation Action (PE Action) stage. When we count detections we look to see at least one detection (tick) in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

Detection Accuracy Ratings

Detection Accuracy Ratings		
Product	Detection Accuracy Rating	Detection Accuracy Rating (%)
CrowdStrike Falcon	640	100%
Kaspersky EDR Expert	640	100%
Symantec Endpoint Security Complete	640	100%
Microsoft 365 Defender	620	97%
Malwarebytes EDR	570	89%
Bitdefender GravityZone	430	67%



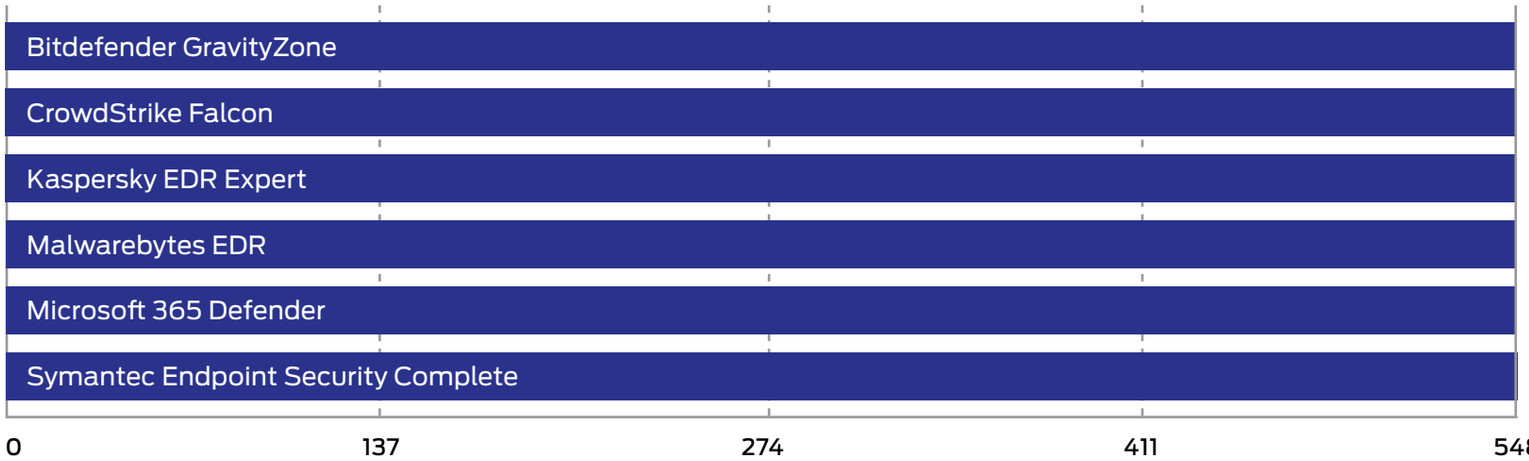
Detection Ratings are weighted to show that how products detect threats can be subtler than just 'win' or 'lose'.

4. Legitimate Software Rating

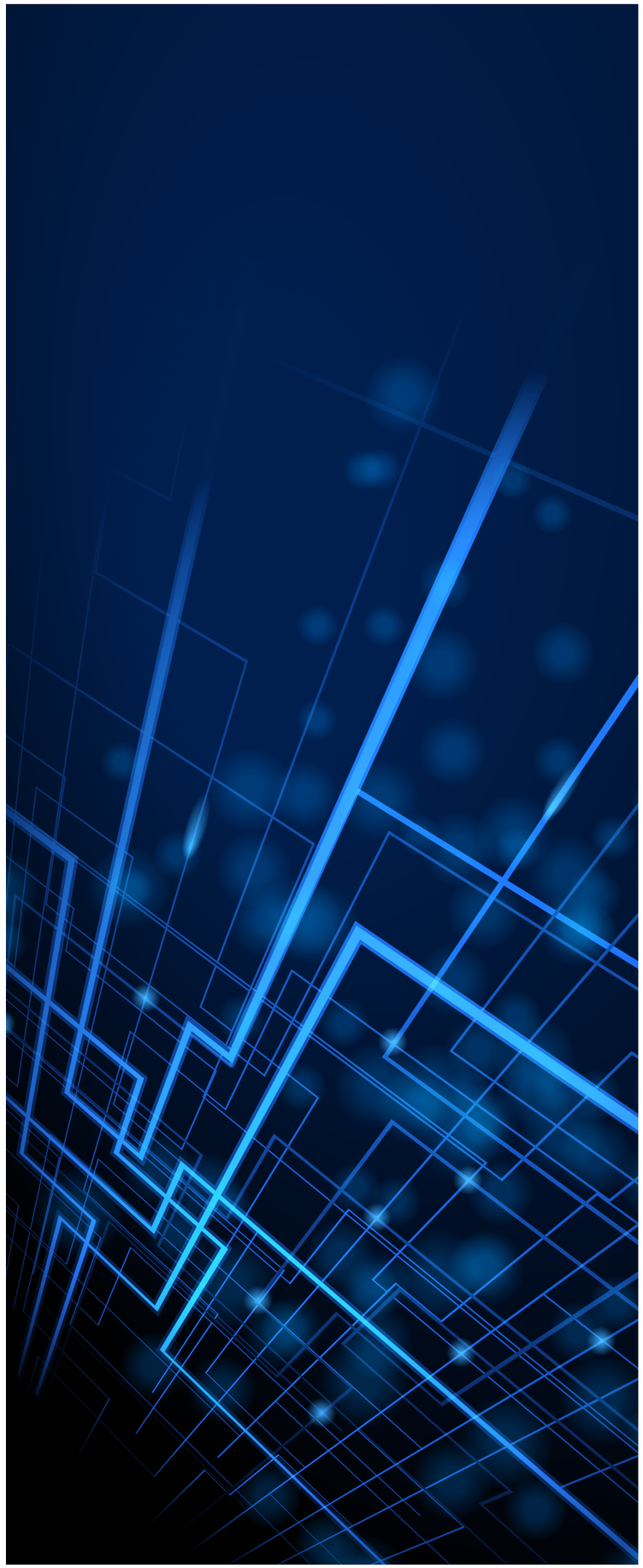
These ratings indicate how accurately the product classifies legitimate applications and URLs, while also taking into account the interactions that the product has with the user. Ideally a product will either not classify a legitimate object or will classify it as safe. In neither case should it bother 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 Ratings	Legitimate Accuracy Ratings (%)
Bitdefender GravityZone	548	100%
CrowdStrike Falcon	548	100%
Kaspersky EDR Expert	548	100%
Malwarebytes EDR	548	100%
Microsoft 365 Defender	548	100%
Symantec Endpoint Security Complete	548	100%



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



5. Conclusions

This test exposed market-leading endpoint security products to a diverse set of exploits, fileless attacks and malware, comprising the widest range of threats in any currently available public test.

All of these attack types have been witnessed in real-world attack 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 test are similar or identical to those used by the threat groups listed in **Hackers vs. Targets** on page 10 and **4. Threat Intelligence** on pages 16-19.

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 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 good news is that all of the products detected all of the threats on a basic level. By that we mean that in each attack, every product detected at least some element of the attack chain. But that is a very basic analysis of the results. In fact, these products had many opportunities to report and potentially block multiple parts of each attack.

For example, **Bitdefender Gravity Zone** detected all the elements of every threat but only achieved a 67% Detection Accuracy Rating. It did not take any action against the Turla and Ke3Chang threats at the point of execution. It also missed one opportunity to block an element from the Threat-Group-3390 attack, and two from the Kimsuky threat.

Bitdefender Gravity Zone was very good at denying hackers further system privileges, preventing them from performing more powerful and insidious attacks against the target system itself. However, it was less effective at preventing hackers from using a compromised system to launch Threat Group-3390 and Kimsuky attacks against other targets in the network.

Malwarebytes EDR is interesting in that it could sometimes detect elements of a threat upon delivery, a facility that it has in common with **CrowdStrike Falcon**, **Kaspersky EDR Expert** and **Symantec Endpoint Security Complete**. The latter three products practiced early detection more consistently, however, and were able to block threats before they had a chance to run. In contrast, there was one instance when **Malwarebytes EDR** reported the delivery of a malicious element but only took effective action against it after it ran.

When tested against the Turla and Ke3Chang attacks, **Malwarebytes EDR** behaved like **Bitdefender Gravity Zone** and **Microsoft 365 Defender** – i.e., more often able to detect elements of these threats during execution rather than when they're being delivered. In one instance, it did not act even if it had detected the threat. In two cases, it did not detect the threats at either stage, leading to a compromised target system. Despite these few misses, **Malwarebytes EDR** prevented any malware from spreading from the target system to others in the network.

As mentioned, **Microsoft 365 Defender** rarely reported detection during delivery, but did so at every instance of execution. It would then respond effectively to each threat element, missing only one from Kimsuky. **Microsoft's** performance shows that while earliest detection is best for successful protection, quick action during its execution can be as effective.

CrowdStrike, **Broadcom** and **Kaspersky** products achieved perfect results in this test, detecting and acting against every element of each threat, and making no mistakes with legitimate applications. **Microsoft's** and **Malwarebytes'** excellent coverage put them in the same running and all five products achieved an AAA rating.

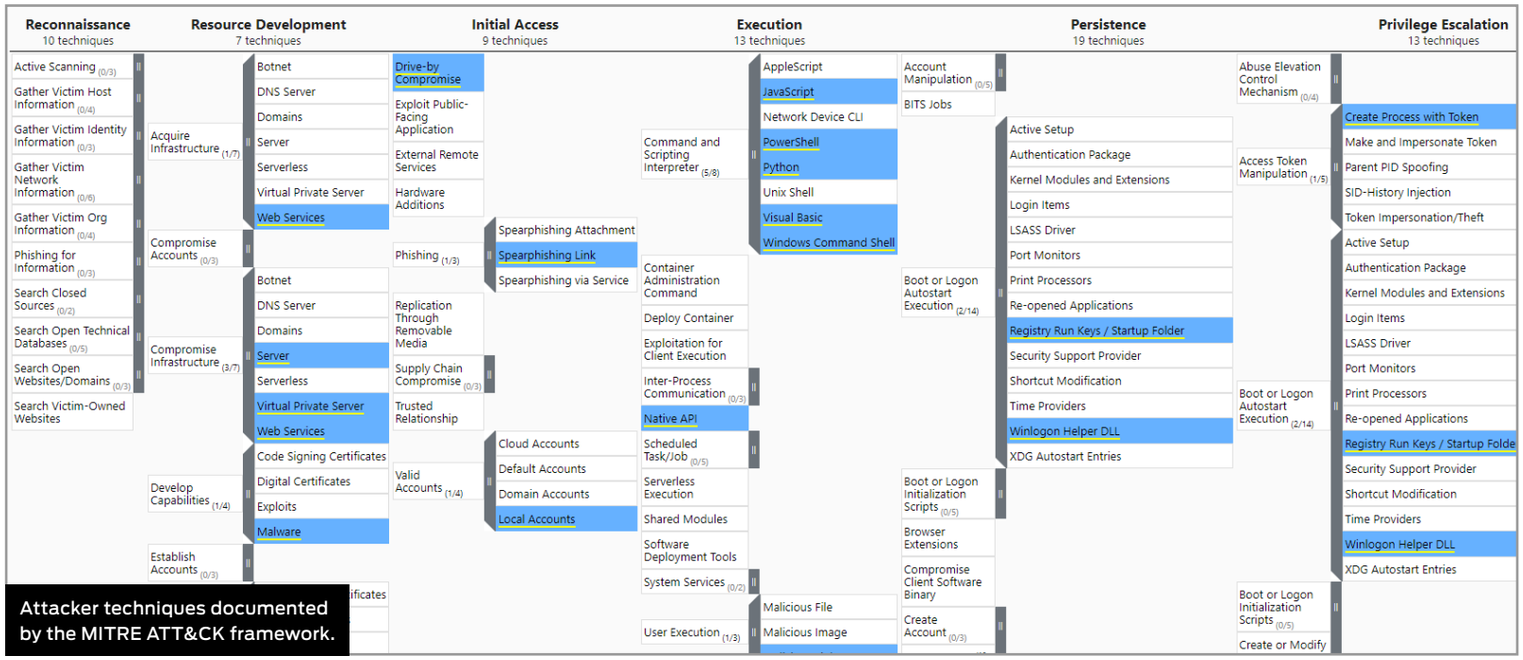
Appendices

Appendix A: 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/



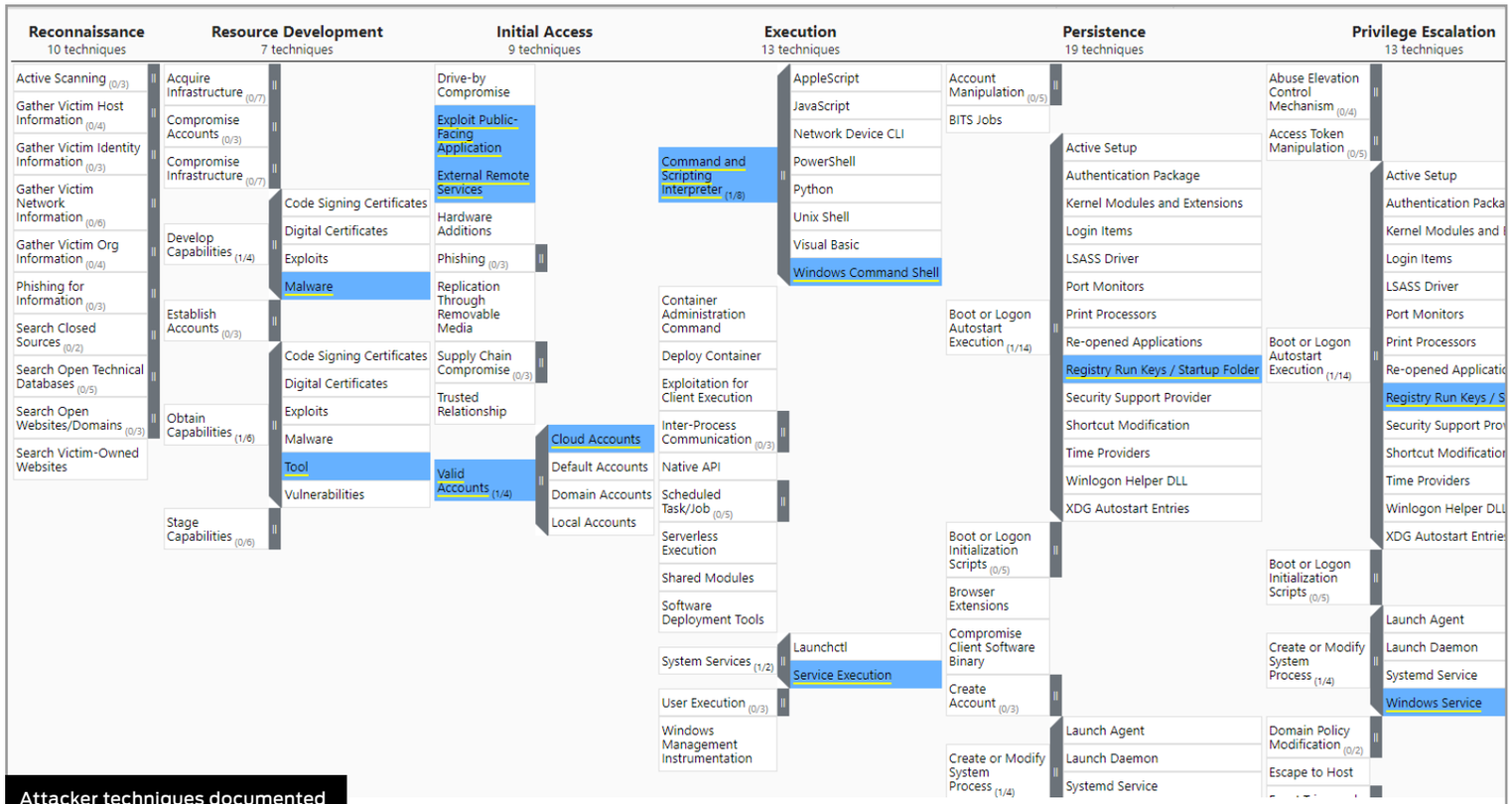
Attacker techniques documented by the MITRE ATT&CK framework.

Example Turla Attack						
Delivery	**Execution**	**Action**	**Privilege Escalation**	**Post-Escalation Action**	**Lateral Movement**	**Lateral Action**
Spear Phishing 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					
 Spear Phishing Attachment	 Malicious File	 System Information Discovery	 Bypass UAC	 Modify Registry	 SSH	 Exfiltration over C2 Channel

Ke3chang

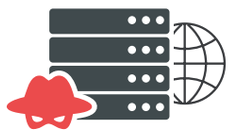
Also known as APT 15, Ke3chang is a Chinese threat group that has targeted natural resource businesses and government entities. The group evades detection by abusing tools provided by target systems, and so 'lives off the land'.

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



Attacker techniques documented by the MITRE ATT&CK framework.

Example Ke3chang Attack

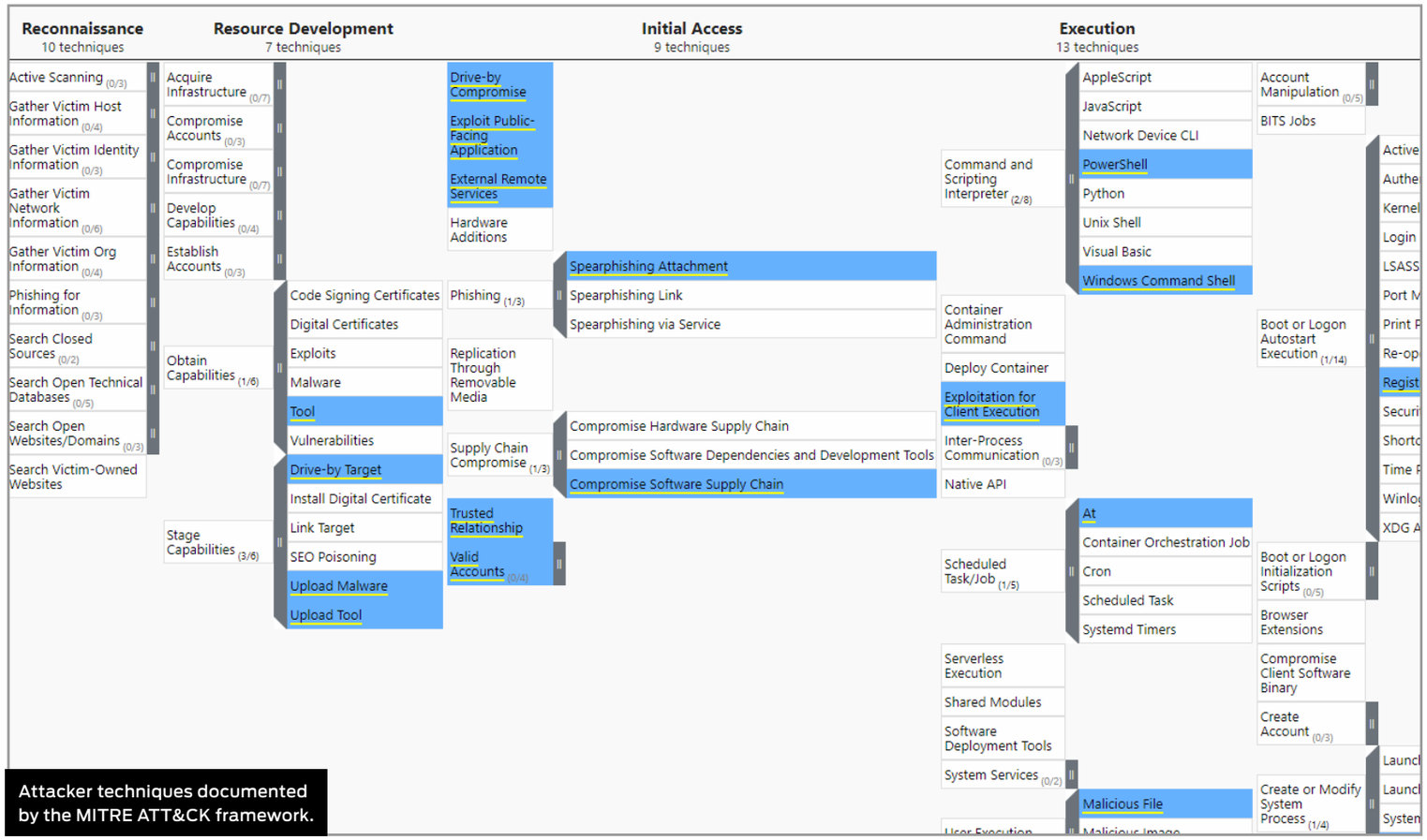
Delivery	Execution	Action	Privilege Escalation	Post-Escalation Action	Lateral Movement	Lateral Action
Exploit Public-Facing Application	Command and Scripting Interpreter	File and Directory Discovery	Valid Accounts	Registry Run Keys /Startup Folder	SMB/Windows Admin Shares	Keylogging
	Windows Command 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/



Attacker techniques documented by the MITRE ATT&CK framework.

Example Threat Group-3390 Attack

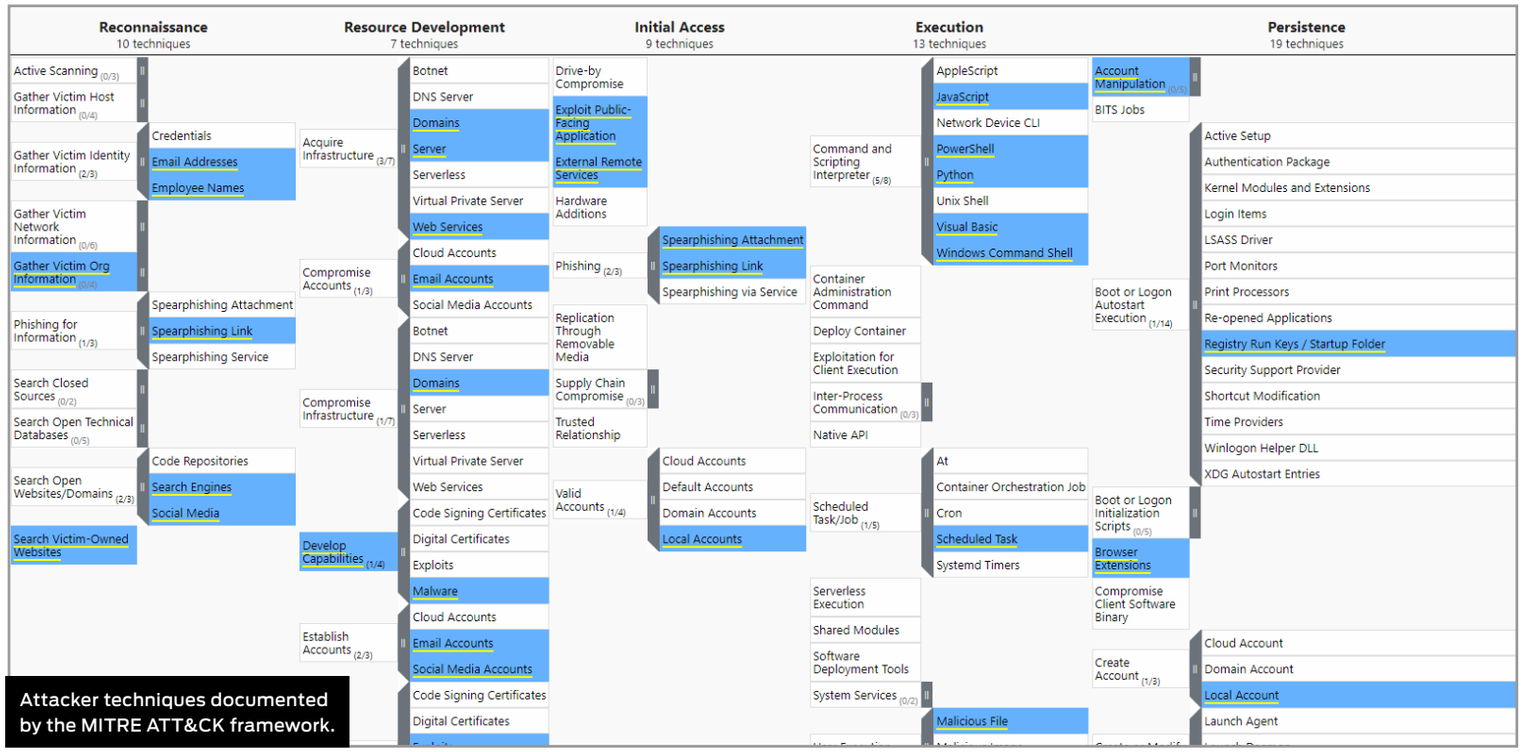
Delivery	Execution	Action	Privilege Escalation	Post-Escalation Action	Lateral Movement	Lateral Action
Spear Phishing Attachment	PowerShell	Local Account	Bypass UAC	Registry Run Keys / Startup Folder	External Remote Services	Local Data Staging
	Windows Command Shell	Query Registry		Windows Service		Archive 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		
 Spear Phishing 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/



Example Kimsuky Attack

Delivery	Execution	Action	Privilege Escalation	Post-Escalation Action	Lateral Movement	Lateral Action
Spear Phishing 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		
 Spear Phishing Attachment	 Visual Basic	 System Network Configuration Discovery	 Bypass UAC	 File Deletion	 External Remote Services	 Keylogging

Appendix B: Detailed Response

Bitdefender GravityZone

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

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

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

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	0	4	3
Ke3chang	4	4	4	0	4	3
Threat Group-3390	4	4	4	3	4	0
Kimsuky	4	4	4	2	4	0
Total	**16**	**16**	**16**	**5**	**16**	**6**

This data shows how the product handled different group stages of each APT. The Detection and Attacks Detected columns show the basic level of detection.

Detection Accuracy Rating Details				
Attacker/ APT Group	Number of Incidents	Attacks Detected	Group Detections	Detection Rating
Turla	4	4	11	110
Ke3chang	4	4	11	110
Threat Group-3390	4	4	11	110
Kimsuky	4	4	10	100
Total	**16**	**16**	**43**	**430**

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

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.

CrowdStrike Falcon

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

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

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

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	4	4	4
Threat Group-3390	4	4	4	4	4	4
Kimsuky	4	4	4	4	4	4
Total	**16**	**16**	**16**	**16**	**16**	**16**

This data shows how the product handled different group stages of each APT. The Detection and Attacks Detected columns show 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	16	160
Threat Group-3390	4	4	16	160
Kimsuky	4	4	16	160
Total	**16**	**16**	**64**	**640**

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

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.

Kaspersky EDR Expert

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

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

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

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	4	4	4
Threat Group-3390	4	4	4	4	4	4
Kimsuky	4	4	4	4	4	4
Total	**16**	**16**	**16**	**16**	**16**	**16**

This data shows how the product handled different group stages of each APT. The Detection and Attacks Detected columns show 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	16	160
Threat Group-3390	4	4	16	160
Kimsuky	4	4	16	160
Total	**16**	**16**	**64**	**640**

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

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.

Malwarebytes EDR

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

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

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

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	3	2	3	4
Ke3chang	4	4	3	3	3	4
Threat Group-3390	4	4	4	4	4	4
Kimsuky	4	4	4	4	4	4
Total	**16**	**16**	**14**	**13**	**14**	**16**

This data shows how the product handled different group stages of each APT. The Detection and Attacks Detected columns show the basic level of detection.

Detection Accuracy Rating Details				
Attacker/ APT Group	Number of Incidents	Attacks Detected	Group Detections	Detection Rating
Turla	4	4	12	120
Ke3chang	4	4	13	130
Threat Group-3390	4	4	16	160
Kimsuky	4	4	16	160
Total	**16**	**16**	**57**	**570**

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

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.

Microsoft 365 Defender

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

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

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

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	4	4	4
Threat Group-3390	4	4	4	4	4	4
Kimsuky	4	4	4	3	4	3
Total	**16**	**16**	**16**	**15**	**16**	**15**

This data shows how the product handled different group stages of each APT. The Detection and Attacks Detected columns show 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	16	160
Threat Group-3390	4	4	16	160
Kimsuky	4	4	14	140
Total	**16**	**16**	**62**	**620**

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

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.

Symantec Endpoint Security Complete

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

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

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

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	4	4	4
Threat Group-3390	4	4	4	4	4	4
Kimsuky	4	4	4	4	4	4
Total	**16**	**16**	**16**	**16**	**16**	**16**

This data shows how the product handled different group stages of each APT. The Detection and Attacks Detected columns show 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	16	160
Threat Group-3390	4	4	16	160
Kimsuky	4	4	16	160
Total	**16**	**16**	**64**	**640**

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

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.

Appendix C: 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 D: FAQs

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

- The test was conducted between 13th April and 25th 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 E: Product Versions

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)
Bitdefender	GravityZone	7.8.4.270	7.8.4.270
CrowdStrike	Falcon	6.53.16705.0	6.56.17010.0
Kaspersky	EDR Expert	11.11.0.452	11.11.0.452
Malwarebytes	EDR	1.2.0.1040	1.2.0.1040
Microsoft	365 Defender	Antivirus Version: 1.387.899.0 Engine Version: 1.1.20200.4 Client Version: 4.18.2303.8	Antivirus Version: 1.387.899.0 Engine Version: 1.1.20200.4 Client Version: 4.18.2303.8
Symantec	Endpoint Security Complete	14.3.9681.7000	14.3.9681.7000

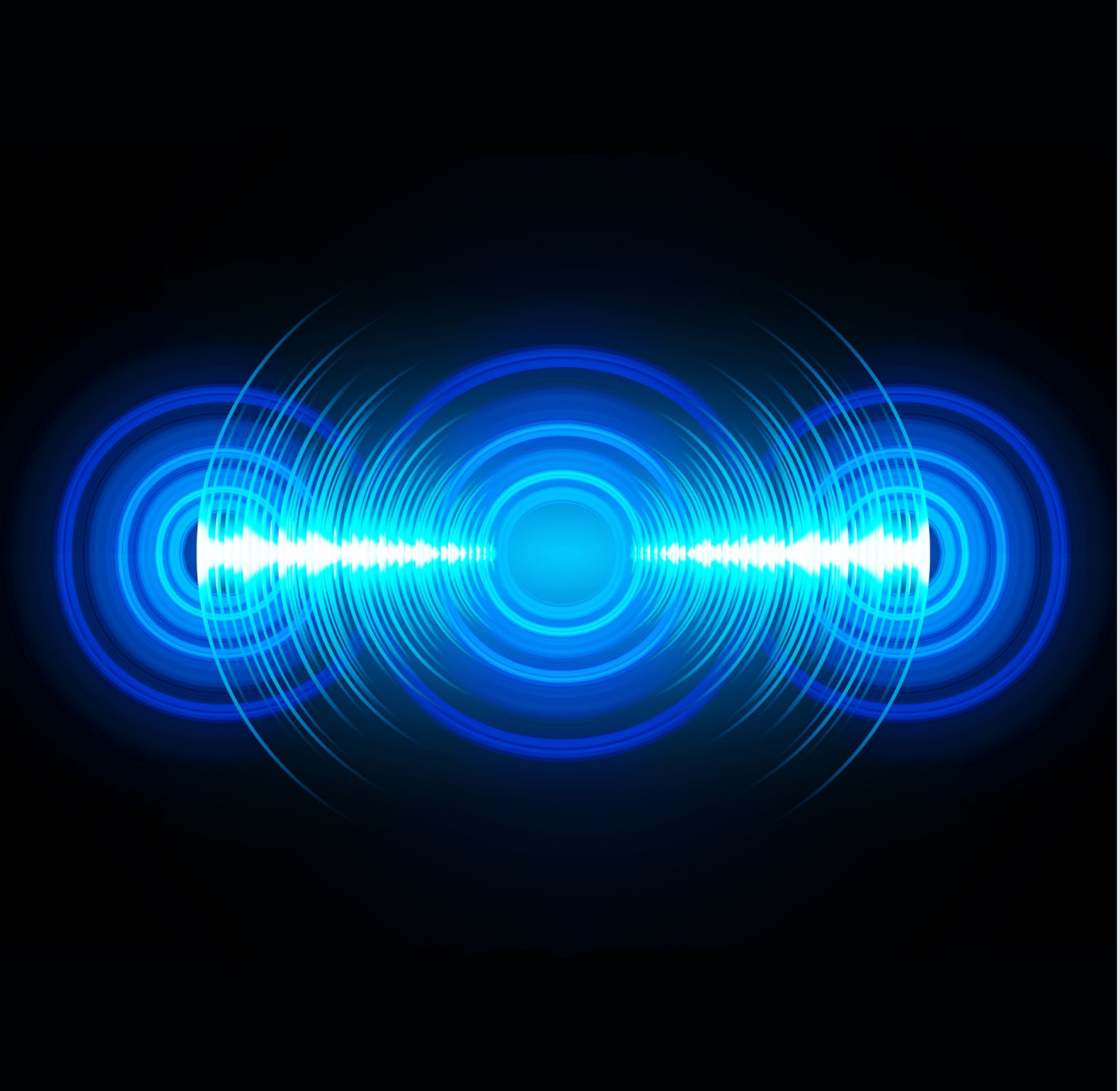
Appendix F: Attack Details

Turla						
Delivery	**Execution**	**Action**	**Post-Esclation Action**	**Post-Escalation Action**	**Lateral Movement**	**Lateral Action**
Spear Phishing Attachment	Asymmetric Cryptography	Domain Groups	Bypass User Account Control	Code Signing Policy Modification	Lateral Tool Transfer	Archive via Utility
Spear Phishing 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
Spear Phishing 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
Spear Phishing Attachment	PowerShell	Process Discovery		Windows Service	Remote Desktop Protocol	Archive via Utility
Spear Phishing 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		



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.