SE Labs

INTELLIGENCE-LED TESTING

Enterprise Advanced Security

Enterprise

EDR DETECTION

July 2022

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.

Website selabs.uk
Twitter @SELabsUK
Email info@SELabs.uk
LinkedIn linkedin.com/company/se-labs/
Blog blog.selabs.uk
Phone +44 (0)203 875 5000
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 Information Alliance (VIA); the Anti-Malware Testing Standards Organization (AMTSO); and NetSecOPEN.

Contents

Document version 1.0 Written 23rd July 2022

INTRODUCTION

Endpoint Detection Compared

We compare endpoint security products directly using real, major threats

Welcome to the first 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 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 **Appendix A: Threat Intelligence**, starting on page 15. 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 via our **Twitter** account. 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 **Twitter**.

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.

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

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

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 majority of products handled legitimate files perfectly. **BlackBerry's** product found this part of the test particularly challenging. The **Anonymous Endpoint Security** product put in a strong performance but generally failed to detect the earliest stage of each attack. Products from **Broadcom**, **Kaspersky** and **CrowdStrike** gave comprehensively strong performances to achieve AAA awards.

Executive Summary				
Products Tested	Attacks Detected (%)	Detection Accuracy (%)	Legitimate Accuracy Rating (%)	Total Accuracy Rating (%)
Kaspersky Endpoint Security	100%	100%	100%	100%
Broadcom Symantec Endpoint Security and Cloud Workload Protection	100%	100%	100%	100%
CrowdStrike Falcon	100%	97%	100%	98%
Anonymous Endpoint Security	100%	94%	97%	95%
BlackBerry CylancePROTECT + OPTICS	100%	97%	61%	79%

Products highlighted in green were the most accurate, scoring 85 per cent or more for Total Accuracy. Those in yellow 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.

Endpoint Detection and Response Awards

The following products win SE Labs awards:

- **Kaspersky** Endpoint Security
- **Broadcom** Symantec Endpoint Security and Cloud Workload Protection
- **CrowdStrike** Falcon
- **Anonymous** Endpoint Security

- **BlackBerry** CylancePROTECT + OPTICS

1. How we Tested

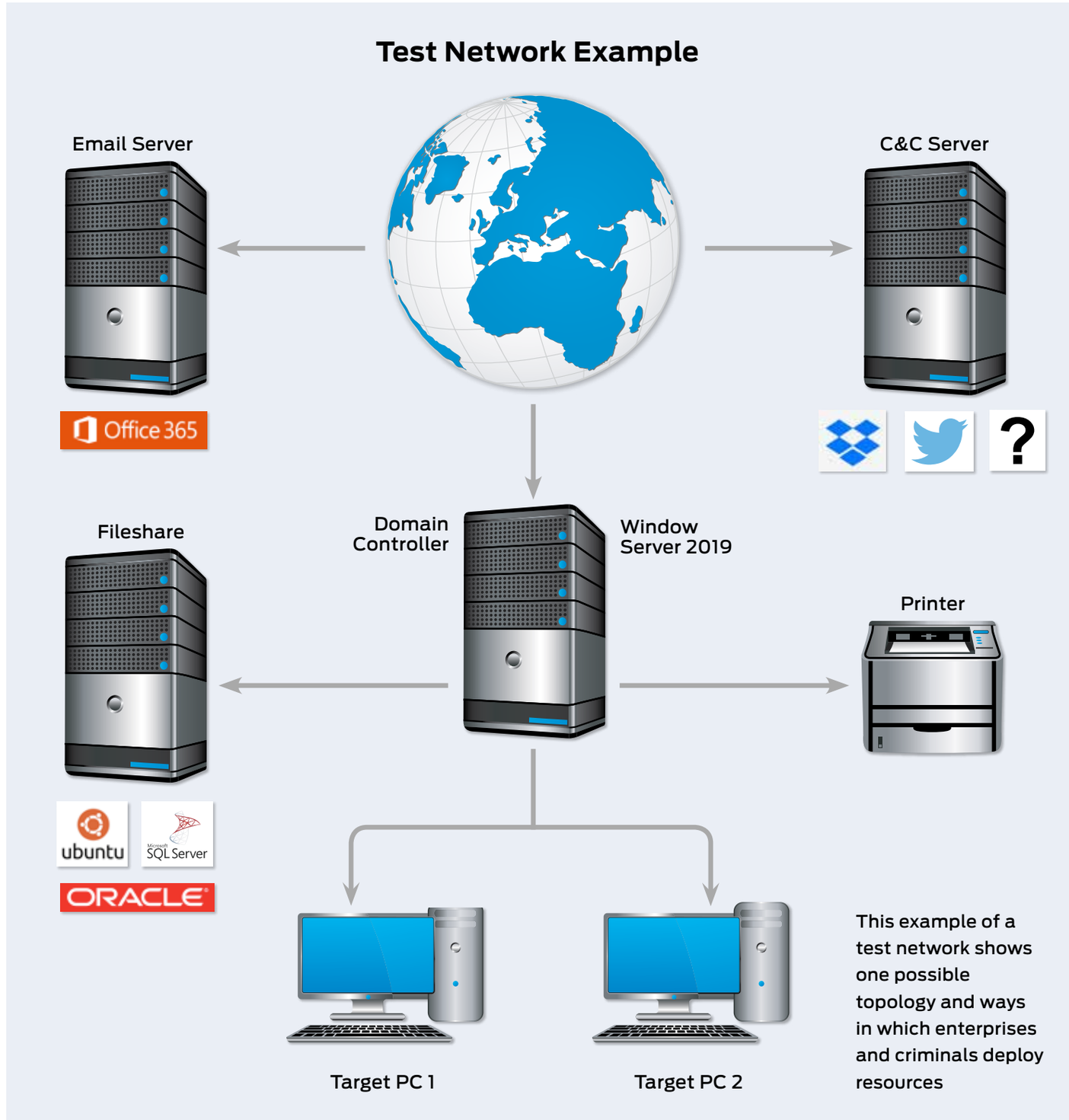
Testers can't assume that products will work a certain way, so running a realistic advanced security test means setting up real networks and hacking them in the same way that real adversaries behave.

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 15 to 18 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 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.

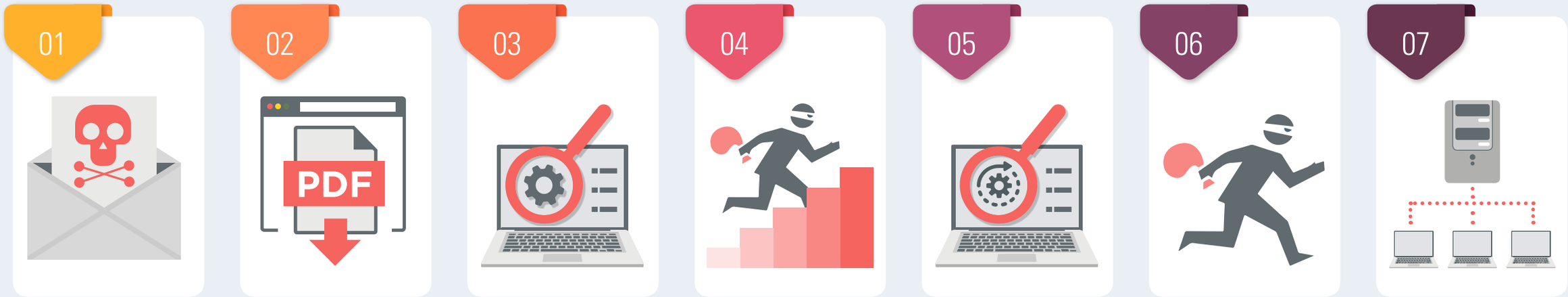


Figure 1. A typical attack starts with an initial contact and progresses through various stages, including reconnaissance, stealing data and causing damage.

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

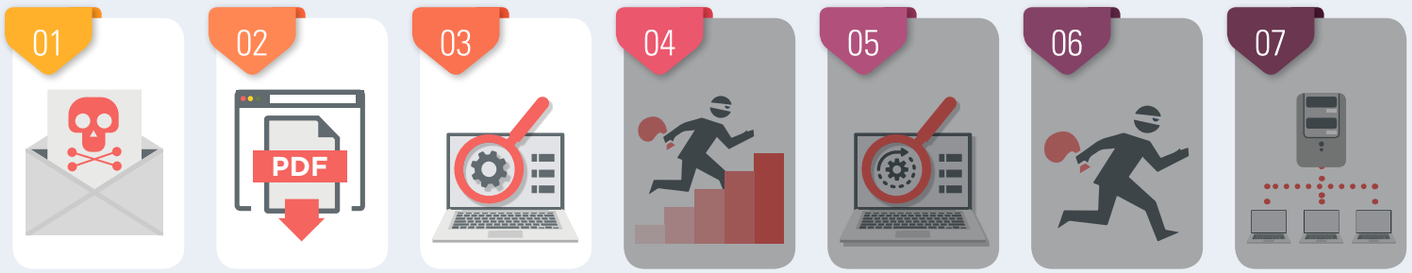


Figure 2. This attack was initially successful but only able to progress as far as the reconnaissance phase

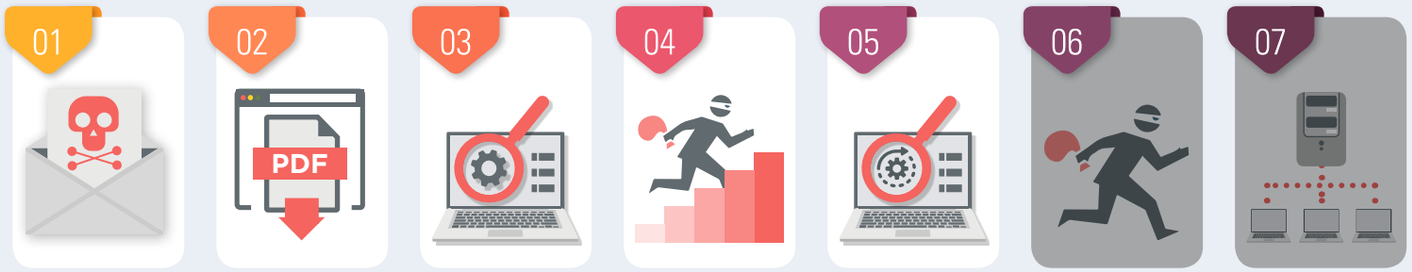


Figure 3. A more successful attack manages to steal passwords but wholesale data theft and destruction was blocked

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.

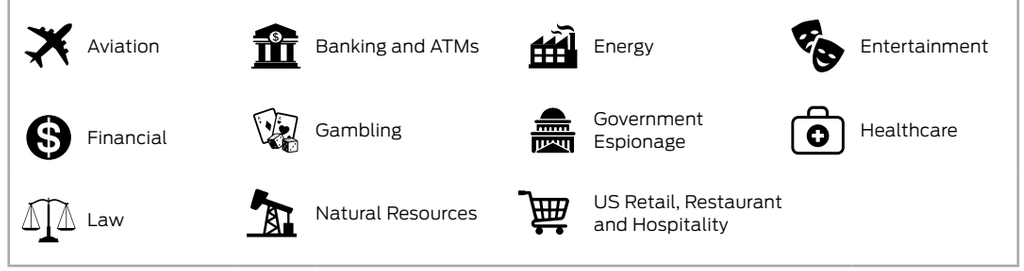
The graphic on this page shows a summary of the attack groups that inspired the targeted attacks used in this test. If a service was able to detect and protect against these then there's a good chance they are on track to blocking similar attacks in the real world. If they fail, then you might take their 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 15 to 18.

Hackers vs. Targets

Attacker/APT Group	Method	Target	Details
Wizard Spider			Credential harvesting, cryptomining and implementation of ransomware.
Sandworm			Obtain sensitive network data via encryption and system data wiping.
Lazarus Group			Phishing and exploitation of public facing servers; data wiping.
Operation Wocao			Exploitation of vulnerable servers with a focus on data exfiltration.

Key



2. Total Accuracy Ratings

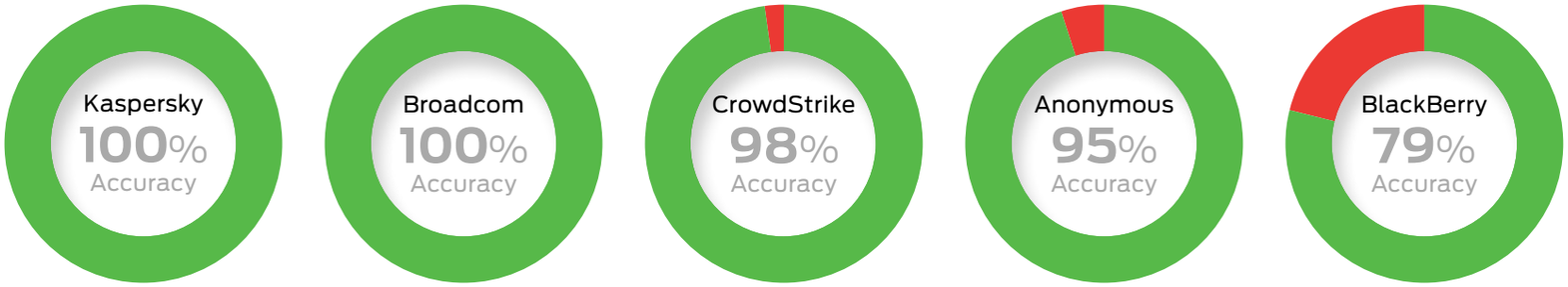
This test examines the total insight a product has, or can provide, into a specific set of attacking actions. We've divided the attack chain into chunks of one or more related actions. To provide sufficient insight, a product must detect at least one action in each chunk.

If you look at the results tables in **Appendix B: Detailed Response** on page 19 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
Kaspersky Endpoint Security	1,328	100%	AAA
Broadcom Symantec Endpoint Security and Cloud Workload Protection	1,328	100%	AAA
CrowdStrike Falcon	1,308	98%	AAA
Anonymous Endpoint Security	1,268	95%	AAA
BlackBerry CylancePROTECT + OPTICS	1,054	79%	A



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 results tables in **Appendix B: Detailed Response** certain stages of the attack chain have been grouped together. 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.

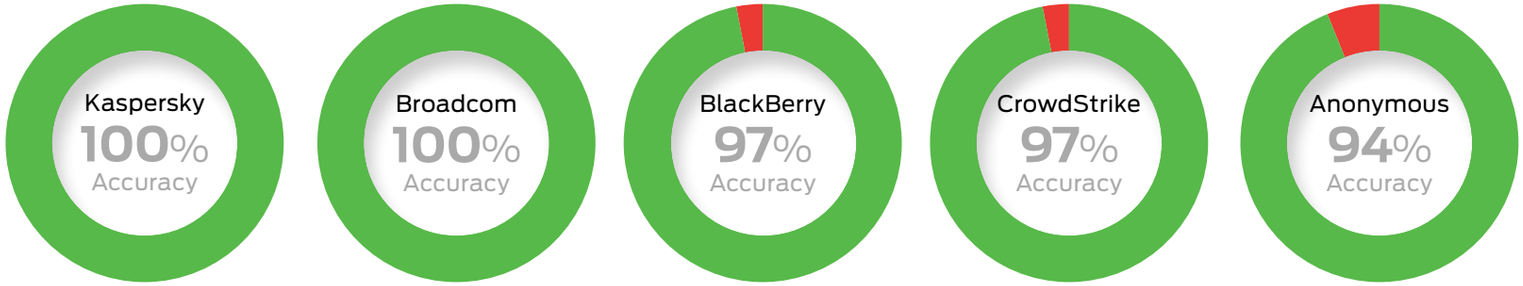
Lateral movement/ action (+10)
The attacker may attempt to use the target as a launching system to other vulnerable systems. If this attempt is discovered, or any subsequent action, a detection is reported.

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 listed, left), 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.

Detection Accuracy Ratings

Product	Detection Accuracy Rating	Detection Accuracy Rating %
Kaspersky Endpoint Security	680	100%
Broadcom Symantec Endpoint Security and Cloud Workload Protection	680	100%
BlackBerry CylancePROTECT + OPTICS	660	97%
Crowdstrike Falcon	660	97%
Anonymous Endpoint Security	640	94%



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 (%)**
Kaspersky Endpoint Security	648	100%
Broadcom Symantec Endpoint Security and Cloud Workload Protection	648	100%
CrowdStrike Falcon	648	100%
Anonymous Endpoint Security	628	100%
BlackBerry CylancePROTECT + OPTICS	394	61%

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, file-less 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 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 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 15 – 18.

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, they could detect malware appearing on the system, notice when that malware runs, stop bad behaviour on a basic level and kick into action when the attackers attempted deeper hacking attacks.

So while the 'Attacks Detected' results show how many of the intrusions each product noticed, the Detection Accuracy rating shows to what extent the product had insight into the whole attack. You would hope that it would be able to detect and report on malicious actions along different stages of the full attack.

For example, **CrowdStrike Falcon** detected some part of every attack, but achieved a detection accuracy of 97%. This is because it missed some important elements of the attacks. In the Wizard Spider attacks it didn't notice the malicious behaviour of the malware after it ran. It did, however, see every subsequent malicious action. So in practice a security team would be able to see that there was a problem, but there would be a small piece of the jigsaw missing. See its detailed results in **Appendix B: Detailed Response**, page 19. In that section you can see how it handled the full attack chain in high resolution. Similarly, the **Anonymous Endpoint Security** product didn't notice the delivery of most of the threats. While this seems much worse than the other products tested, it detected the malware running in all but one case. In the vast majority of cases it also detected the hacker escalating privileges in order to take greater control of the target.

BlackBerry's product managed the same Detection Accuracy Rating as **CrowdStrike** but its inaccurate handling of legitimate applications brought its overall Total Accuracy Rating down significantly. It scored an A rating.

The **Anonymous Endpoint Security** product also achieved an AAA rating, but rated lower overall because of its failed initial detections as described above.

Broadcom and **Kaspersky** products achieved perfect results in this test, detecting every element of each threat, and making no mistakes with legitimate applications. **CrowdStrike's** excellent coverage puts it in the same running and all three products achieved an AAA rating.

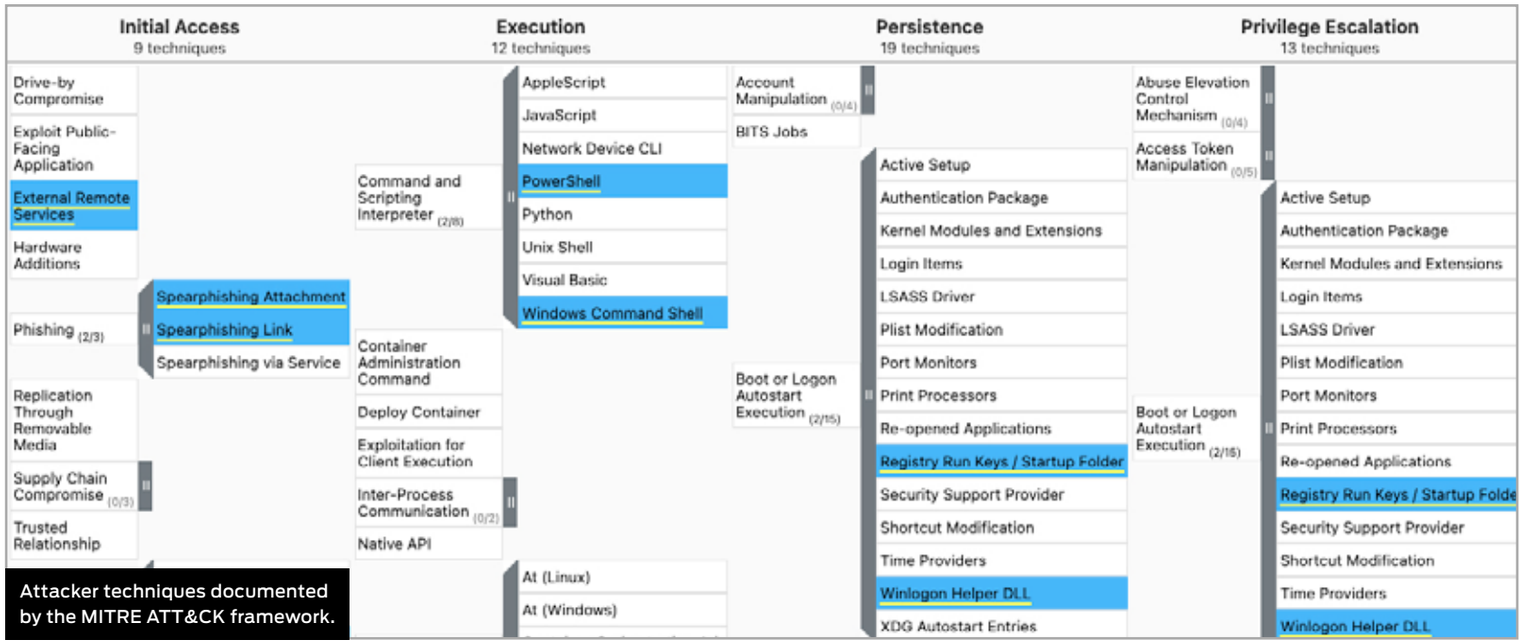
Appendices

Appendix A: Threat Intelligence

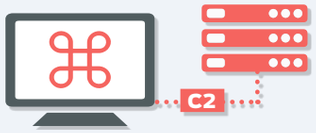
Wizard Spider

Known to have operated since at least 2016, Wizard Spider is considered to be a threat group based in and around St. Petersburg, Russia. It is most notable for developing the TrickBot banking malware. Wizard Spider has infected over a million systems worldwide predominantly by using this malware.

Reference Link:
https://attack.mitre.org/groups/G0102/



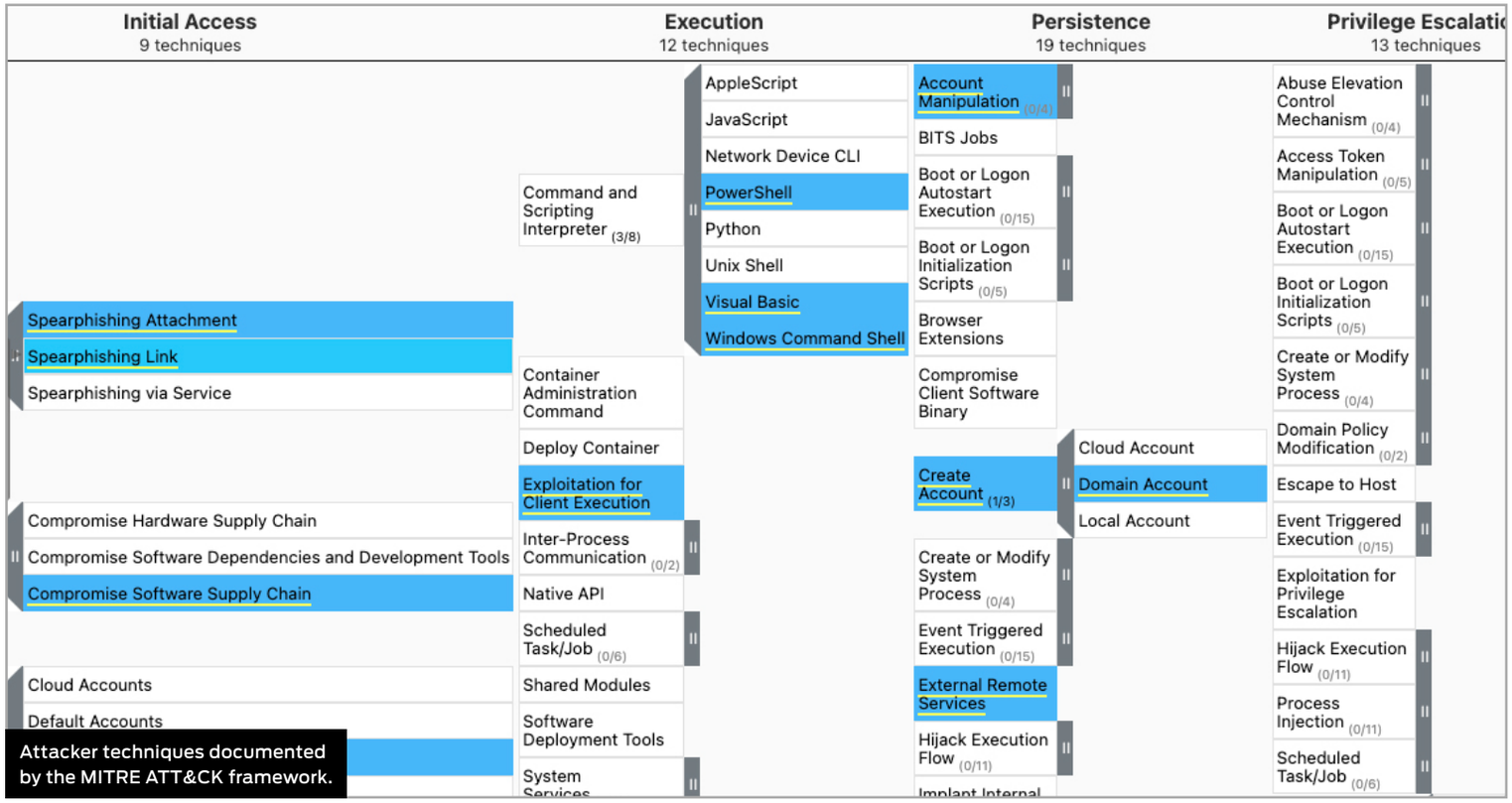
Attacker techniques documented by the MITRE ATT&CK framework.

Example Wizard Spider Attack						
Delivery	**Execution**	**Action**	**Privilege Escalation**	**Post-Escalation Action**	**Lateral Movement**	**Lateral Action**
Spearphishing Attachment	Windows Command Shell	File and Directory Discovery	Bypass User Account Control	Remote System Discovery	Service Execution	Archive Collected Data
	Malicious File	Process Discovery	Valid Accounts	Security Software Discovery	Domain Accounts	Data Staged
	Obfuscated Files or Information	System Information Discovery		LLMNR/NBT-NS Poisoning and SMB Relay		Data from Local System
	Powershell	System Network Configuration Discovery				Exfiltration Over C2 Channel
		System Owner/User Discovery				
 Spearphishing Attachment	 Obfuscated Files or Information	 System Information Discovery	 Valid Accounts	 Security Software Discovery	 Domain Accounts	 Exfiltration over C2 Channel

Sandworm

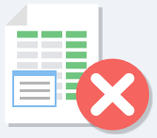
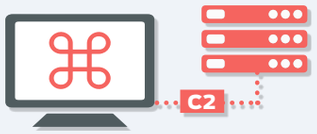
In operation since around 2009, Sandworm Team is threat group that has been connected to Russia's Main Intelligence Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU). It is believed to be the GRU's Unit 74455. Notable campaigns include a targeted attack on the 2017 French Presidential campaign, as well as the worldwide NotPetya ransomware attack in the same year.

References:
https://attack.mitre.org/groups/G0034/



Attacker techniques documented by the MITRE ATT&CK framework.

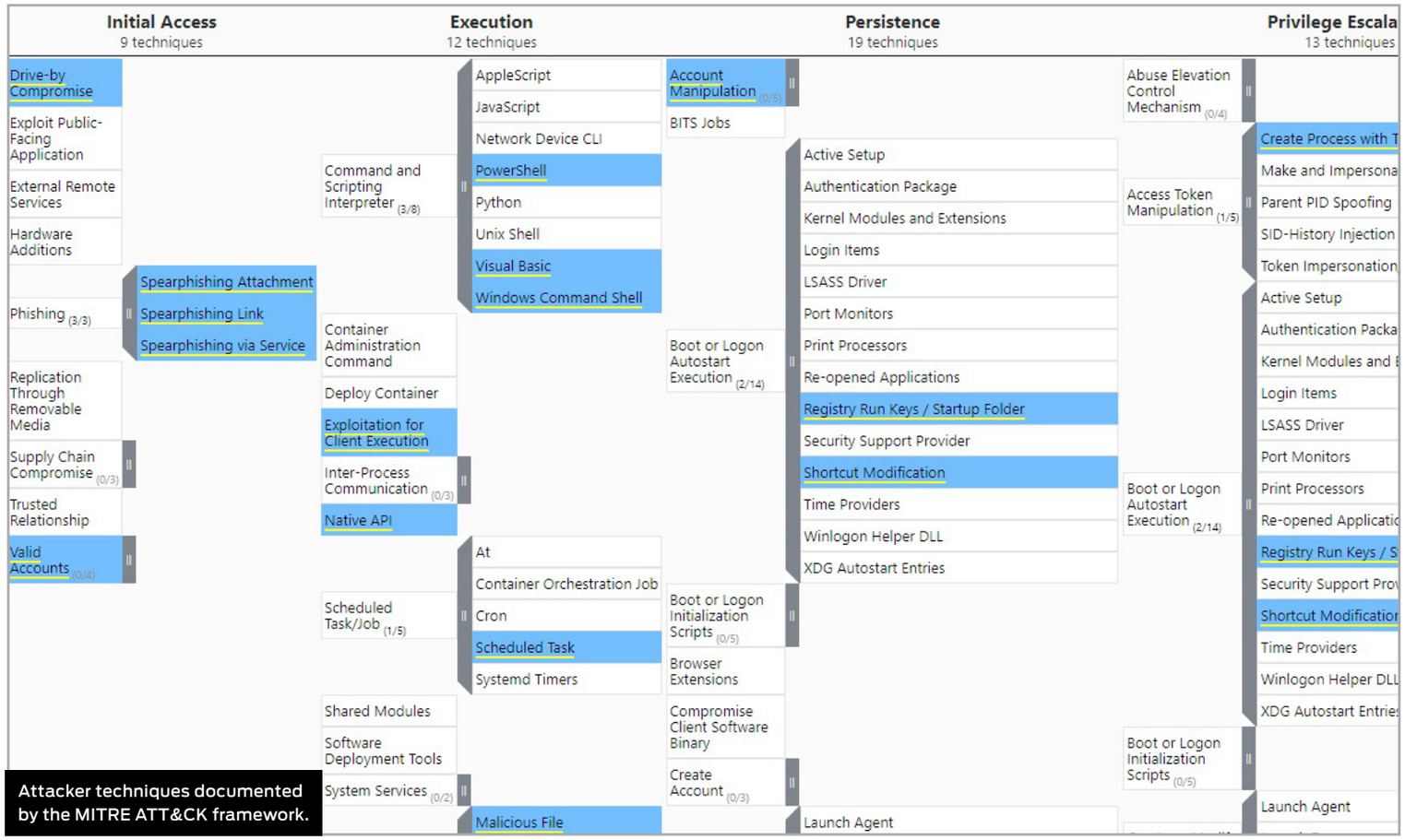
Example Sandworm Attack

Delivery	Execution	Action	Privilege Escalation	Post-Escalation Action	Lateral Movement	Lateral Action
Spearphishing Link	Windows Command Shell	File and Directory Discovery	Domain Accounts	Remote System Discovery	Lateral Tool Transfer	Data from Local System
	Powershell	System Information Discovery	Bypass UAC	LSASS Memory	SMB/Windows Admin Shares	Local Data Staging
	Malicious Link	System Owner/User Discovery				Exfiltration Over C2 Channel
	File Deletion	Data from Local System				Network Sniffing
	Obfuscated Files or Information	Local Data Staging				
		Exfiltration Over C2 Channel				
 Spearphishing Link	 File Deletion	 Data from Local System	 Bypass UAC	 LSASS Memory	 SMB/Windows Admin Shares	 Exfiltration Over C2 Channel

Lazarus Group

Lazarus Group is considered responsible for the November 2014 attack on Sony Pictures Entertainment, in which data was destroyed. Similar malware has been used in other attacks and some researchers use the Lazarus Group label for all North Korean state-sponsored attacks.

References:
https://attack.mitre.org/groups/G0032/



Attacker techniques documented by the MITRE ATT&CK framework.

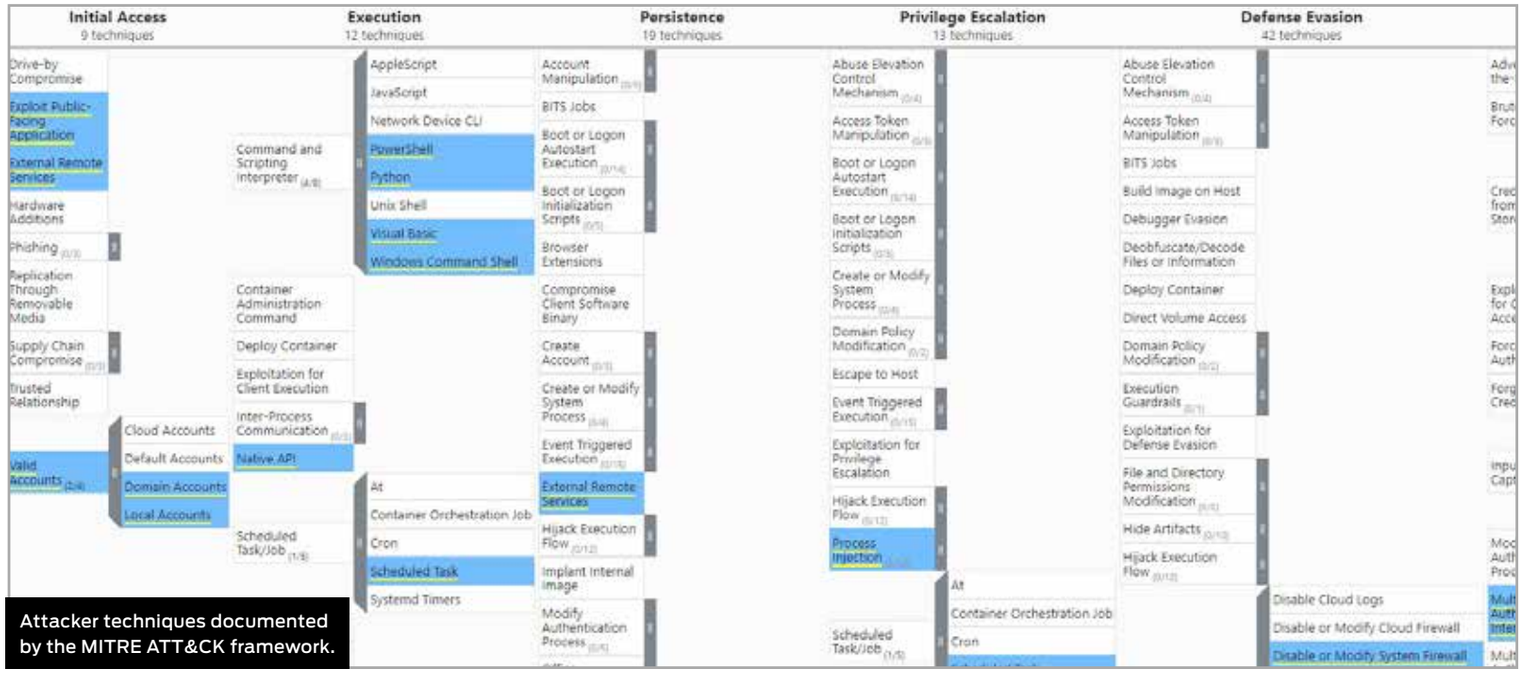
Example Lazarus Group Attack

Delivery	Execution	Action	Privilege Escalation	Post-Escalation Action	Lateral Movement	Lateral Action
Spearphishing Attachment	Malicious File	File and Directory Discovery	Create Process with Token	Query Registry	Windows Management Instrumentation	Exfiltration Over C2 Protocol
	Obfuscated Files or Information	Process Discovery		File Deletion		Archive Collected Data
	Windows Command Shell	System Information Discovery		Hidden Files and Directories		Service Stop
	Windows Management Instrumentation	System Network Configuration Discovery		Windows Service		System Shutdown/Reboot
 Spearphishing Attachment	 Obfuscated Files or Information	 Process Discovery	 Create Process with Token	 File Deletion	 Windows Management Instrumentation	 Exfiltration Over C2 Protocol

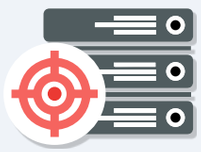
Operation Wocao

This threat group is based in China and has focussed on targets including government, energy and healthcare. It is active in France, Germany and the UK, as well as China itself. Some researchers note a connection with APT20.

References:
https://attack.mitre.org/groups/G0116/



Attacker techniques documented by the MITRE ATT&CK framework.

Example Operation Wocao Attack						
Delivery	**Execution**	**Action**	**Privilege Escalation**	**Post-Escalation Action**	**Lateral Movement**	**Lateral Action**
Exploit Public-Facing Application	Valid Accounts	File and Directory Discovery	Domain Accounts	Keylogging	Lateral Tool Transfer	Archive via Utility
	PowerShell	System Information Discovery	Bypass User Account Control	Kerberoasting	SMB/Windows Admin Shares	Automated Collection
	Windows Command Shell	System Owner/User Discovery		Password Managers		Data from Local System
	Obfuscated Files or Information	System Network Configuration Discovery		Disable or Modify System Firewall		Local Data Staging
	Windows Management Instrumentation	System Network Connections Discovery		Remote System Discovery		Exfiltration Over C2 Channel
	Asymmetric Cryptography	Network Service Scanning		Security Software Discovery		File Deletion
	Non-Application Layer Protocol					Clear Windows Event Logs
 Exploit Public-Facing Application	 PowerShell	 System Information Discovery	 Bypass User Account Control	 Password Managers	 SMB/Windows Admin Shares	 Automated Collection

Appendix B: Detailed Response

BlackBerry CylancePROTECT + OPTICS

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

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

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

Operation Wocao								
Incident No:	Detection	Delivery	Execution	Action	Escalation	PE Action	Lateral Movement	Lateral Action
13	✓	—	✓	✓	✓	✓	✓	✓
14	✓	N/A	✓	✓	✓	✓	✓	✓
15	✓	—	✓	✓	✓	✓	✓	✓
16	✓	N/A	✓	✓	✓	✓	✓	✓
17	✓	N/A	✓	✓	✓	✓	✓	✓

Response Details						
Attacker/APT Group	Number of Test Cases	Attacks Detected	Delivery/ Execution	Action	Privilege Escalation/Action	Lateral Movement/Action
Wizard Spider	4	4	4	3	4	4
Sandworm	4	4	4	4	4	3
Lazarus Group	4	4	4	4	3	4
Operation Wocao	5	5	5	5	5	5
Total	17	17	17	16	16	16

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 Test Cases	Attacks Detected	Group Detections	Detection Rating
Wizard Spider	4	4	15	150
SandWorm	4	4	15	150
Lazarus Group	4	4	15	160
Operation Wocao	5	5	20	200
Total	17	17	65	660

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

Broadcom Symantec Endpoint Security and Cloud Workload Protection

Wizard Spider

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

Lazarus Group

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

Sandworm

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

Operation Wocao

Incident No:	Detection	Delivery	Execution	Action	Escalation	PE Action	Lateral Movement	Lateral Action
13	✓	✓	✓	✓	✓	✓	✓	✓
14	✓	N/A	✓	✓	✓	✓	✓	✓
15	✓	✓	✓	✓	✓	✓	✓	✓
16	✓	N/A	✓	✓	✓	✓	✓	✓
17	✓	N/A	✓	✓	✓	✓	✓	✓

Response Details

Attacker/APT Group	Number of Test Cases	Attacks Detected	Delivery/ Execution	Action	Privilege Escalation/Action	Lateral Movement/Action
Wizard Spider	4	4	4	4	4	4
Sandworm	4	4	4	4	4	4
Lazarus Group	4	4	4	4	3	4
Operation Wocao	5	5	5	5	5	5
Total	17	17	17	17	16	17

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 Test Cases	Attacks Detected	Group Detections	Detection Rating
Wizard Spider	4	4	16	160
Sandworm	4	4	16	160
Lazarus Group	4	4	15	160
Operation Wocao	5	5	20	200
Total	17	17	67	680

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

CrowdStrike Falcon

Wizard Spider

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

Lazarus Group

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

Sandworm

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

Operation Wocao

Incident No:	Detection	Delivery	Execution	Action	Escalation	PE Action	Lateral Movement	Lateral Action
13	✓	—	✓	✓	✓	✓	✓	✓
14	✓	N/A	✓	✓	✓	✓	✓	✓
15	✓	—	✓	✓	✓	✓	✓	✓
16	✓	N/A	✓	✓	✓	✓	✓	✓
17	✓	N/A	✓	✓	✓	✓	✓	✓

Response Details

Attacker/APT Group	Number of Test Cases	Attacks Detected	Delivery/ Execution	Action	Privilege Escalation/Action	Lateral Movement/Action
Wizard Spider	4	4	4	3	4	4
Sandworm	4	4	4	3	4	4
Lazarus Group	4	4	4	4	3	4
Operation Wocao	5	5	5	5	5	5
Total	17	17	17	15	16	17

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 Test Cases	Attacks Detected	Group Detections	Detection Rating
Wizard Spider	4	4	15	150
Sandworm	4	4	15	150
Lazarus Group	4	4	15	160
Operation Wocao	5	5	20	200
Total	17	17	65	660

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

Kaspersky Endpoint Security

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

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

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

Operation Wocao								
Incident No:	Detection	Delivery	Execution	Action	Escalation	PE Action	Lateral Movement	Lateral Action
13	✓	✓	✓	✓	✓	✓	✓	✓
14	✓	N/A	✓	✓	✓	✓	✓	✓
15	✓	✓	✓	✓	✓	✓	✓	✓
16	✓	N/A	✓	✓	✓	✓	✓	✓
17	✓	N/A	✓	✓	✓	✓	✓	✓

Response Details						
Attacker/APT Group	Number of Test Cases	Attacks Detected	Delivery/ Execution	Action	Privilege Escalation/Action	Lateral Movement/Action
Wizard Spider	4	4	4	4	4	4
Sandworm	4	4	4	4	4	4
Lazarus Group	4	4	4	4	3	4
Operation Wocao	5	5	5	5	5	5
Total	17	17	17	17	16	17

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 Test Cases	Attacks Detected	Group Detections	Detection Rating
Wizard Spider	4	4	16	160
Sandworm	4	4	16	160
Lazarus Group	4	4	15	160
Operation Wocao	5	5	20	200
Total	17	17	67	680

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

Anonymous Endpoint Security

Wizard Spider

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

Lazarus Group

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

Sandworm

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

Operation Wocao

Incident No:	Detection	Delivery	Execution	Action	Escalation	PE Action	Lateral Movement	Lateral Action
13	✓	—	✓	✓	✓	✓	✓	—
14	✓	N/A	✓	✓	✓	✓	✓	✓
15	✓	—	✓	✓	✓	✓	✓	—
16	✓	N/A	✓	✓	✓	✓	✓	✓
17	✓	N/A	✓	✓	—	✓	✓	✓

Response Details

Attacker/APT Group	Number of Test Cases	Attacks Detected	Delivery/ Execution	Action	Privilege Escalation/Action	Lateral Movement/Action
Wizard Spider	4	4	4	3	4	4
Sandworm	4	4	4	4	4	4
Lazarus Group	4	4	3	3	3	4
Operation Wocao	5	5	5	5	5	5
Total	17	17	16	15	16	17

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 Test Cases	Attacks Detected	Group Detections	Detection Rating
Wizard Spider	4	4	15	150
Sandworm	4	4	16	160
Lazarus Group	4	4	13	130
Operation Wocao	5	5	20	200
Total	17	17	64	640

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

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 25th April to 7th June 2022.
- This test was conducted independently by SE Labs with similar testing made available to other vendors, at the same time, for their own standalone reports.
- 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 part of our security infrastructure. 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)
BlackBerry	CylancePROTECT + OPTICS	PROTECT 3.0.1001 OPTICS Windows 2.5.3010 OPTICS CentOS 3.2.1108	PROTECT 3.0.1001 OPTICS Windows 2.5.3010 OPTICS CentOS 3.2.1108
Broadcom	Symantec Endpoint Security and Cloud Workload Protection	14.3.7393.4000	14.3.7393.4000
CrowdStrike	Falcon	6.38.15205.0	6.39.15314.0
Kaspersky	Endpoint Security	EDR 4.0	EDR 4.0

Appendix F: Attack Details

Wizard Spider							
Incident no:	Delivery	Execution	Action	Privilege Escalation	Post-Esclation Action	Lateral Movement	Lateral Action
1	Spearphishing Attachment	Windows Command Shell	File and Directory Discovery	Bypass User Account Control	Remote System Discovery	Service Execution	Archive Collected Data
		Malicious File	Process Discovery	Valid Accounts	Security Software Discovery	Domain Accounts	Data staged
		Obfuscated Files or Information	System Information Discovery		LLMNR/NBT-NS Poisoning and SMB Relay		Data from Local System
		Powershell	System Network Configuration Discovery				Exfiltration Over C2 Channel
			System Owner/User Discovery				
2	Spearphishing Link	Malicious Link	File and Directory Discovery	Bypass User Account Control	NTDS	SSH	Archive Collected Data
		Windows Command Shell	Process Discovery	Valid Accounts	Security Account Manager	External Remote Services	Data staged
		Web Protocols	System Information Discovery		Kerberoasting		Data from Local System
		Non-standard Port	Permission Groups Discovery				Exfiltration Over C2 Channel
			System Owner/User Discovery				
3	Spearphishing Attachment	Malicious File	File and Directory Discovery	Bypass User Account Control	Windows Service	Lateral Tool Transfer	Archive Collected Data
		Windows Command Shell	Process Discovery	Valid Accounts	Registry Run Keys / Startup Folder	Remote Desktop Protocol	Data staged
		Web Protocols	System Information Discovery		Scheduled Task	SMB/Windows Admin Shares	Data from Local System
			System Owner/User Discovery		Masquerade Task or Service		Exfiltration Over C2 Channel
					Winlogon Helper DLL		
4	Spearphishing Link	Malicious Link	File and Directory Discovery	Bypass User Account Control	Dynamic-link Library Injection	Windows Remote Management	Archive Collected Data
		Windows Command Shell	Process Discovery	Valid Accounts	Windows File and Directory Permissions Discovery		Data from Local System
		Web Protocols	System Information Discovery				Exfiltration Over C2 Channel
			System Network Configuration Discovery				

Sandworm							
Incident no:	Delivery	Execution	Action	Privilege Escalation	Post-Esclation Action	Lateral Movement	Lateral Action
5	Spearphishing Attachment	Windows Command Shell	File and Directory Discovery	Domain Accounts	Keylogging	SSH	Cron
		Malicious File	Process Discovery	Bypass User Account Control	Domain Account (Discovery)		Boot or Logon Initialization Scripts
		Non-Standard Port	System Information Discovery				RC Scripts
			Data from Local System				Systemd Service
			Local Data Staging				
			Exfiltration Over C2 Channel				
			Credentials from Web Browsers				
6	Spearphishing Link	Windows Command Shell	File and Directory Discovery	Domain Accounts	Remote System Discovery	SMB/Windows Admin Shares	Data from Local System
		Powershell	System Information Discovery	Bypass User Account Control	LSASS Memory		Local Data Staging
		Malicious Link	System Owner/User Discovery				Exfiltration Over C2 Channel
		Obfuscated Files or Information	Data from Local System				Network Sniffing
			Local Data Staging				
			Exfiltration Over C2 Channel				
7	Spearphishing Attachment	Windows Command Shell	File and Directory Discovery	Domain Accounts	Domain Account (Discovery)	SSH	Systemd Service
		Malicious File	System Information Discovery	Bypass User Account Control	Ingress Tool Transfer		Kernel Modules and Extensions
		Web Protocols	System Owner/User Discovery		LSASS Memory		SSH Authorized Keys
			System Network Configuration Discovery				
			System Network Connections Discovery				
8	Spearphishing Link	Windows Command Shell	File and Directory Discovery	Domain Accounts	Remote System Discovery	SSH	/etc/passwd and /etc/shadow
		Malicious Link	System Information Discovery	Bypass User Account Control	Security Software Discovery		Bash History
			System Owner/User Discovery				Clear Linux or Mac System Logs
			System Network Configuration Discovery				
			System Network Connections Discovery				

Lazarus Group							
Incident no:	Delivery	Execution	Action	Privilege Escalation	Post-Esclation Action	Lateral Movement	Lateral Action
9	Spearphishing Attachment	Malicious File	File and Directory Discovery	Create Process with Token	Query Registry	Windows Management Instrumentation	Exfiltration Over C2 Protocol
		Obfuscated Files or Information	Process Discovery		File Deletion		Archive Collected Data
		Windows Command Shell	System Information Discovery		Hidden Files and Directories		Service Stop
		Windows Management Instrumentation	System Network Configuration Discovery		Windows Service		System Shutdown/Reboot
10	Spearphishing Attachment	Malicious File	File and Directory Discovery	Create Process with Token	Shortcut Modification	Remote Desktop Protocol	Exfiltration Over C2 Channel
		Windows Command Shell	Process Discovery		Registry Run Keys / Startup Folder		Archive Collected Data
		Match Legitimate Name or Location	System Information Discovery		Disable or Modify System Firewall		Internal Defacement
			System Network Configuration Discovery		Windows Service		Disk Content Wipe
			System Owner/User Discovery				System Shutdown/Reboot
			System Time Discovery				Account Manipulation
			Application Window Discovery				
11	Spearphishing Attachment	Malicious File	File and Directory Discovery	Create Process with Token	Dynamic-link Library Injection	Remote Desktop Protocol	Data Destruction
		Windows Command Shell	Process Discovery		Disable or Modify System Firewall		Internal Defacement
		Match Legitimate Name or Location	System Information Discovery		Keylogging		File Deletion
			System Owner/User Discovery		Archive Collected Data		Disk Structure Wipe
					Exfiltration Over C2 Channel		Timestomp
12	Spearphishing Attachment	Malicious File	File and Directory Discovery	Create Process with Token	Timestomp	Remote File Copy	Keylogging
		Windows Command Shell	Process Discovery		Archive Collected Data		Archive Collected Data
		Exploitation for Client Execution	System Information Discovery		File Deletion		File Deletion
			System Network Configuration Discovery		Exfiltration Over C2 Channel		Exfiltration Over Unencrypted/ Obfuscated Non-C2 Protocol
			System Owner/User Discovery		Password Spraying		Internal Defacement
			System Time Discovery		Disable or Modify Tools		
					Data Staging		

Operation Wocao							
Incident no:	Delivery	Execution	Action	Privilege Escalation	Post-Esclation Action	Lateral Movement	Lateral Action
13	Exploit Public-Facing Application	Valid Accounts	File and Directory Discovery	Domain Accounts	Modify Registry	Lateral Tool Transfer	Archive via Utility
		PowerShell	System Information Discovery	Bypass User Account Control	Scheduled Task	SMB/Windows Admin Shares	Automated Collection
		Windows Command Shell	System Network Configuration Discovery		Service Execution		Clipboard Data
		Internal Proxy	System Owner/User Discovery		Disable or Modify System Firewall		Data from Local System
		Asymmetric Cryptography	Software Discovery		Ingress Tool Transfer		Local Data Staging
		Non-Application Layer Protocol	System Service Discovery		Private Keys		Exfiltration Over C2 Channel
			Network Service Scanning		Kerberoasting		File Deletion
14	External Remote Services	Valid Accounts	File and Directory Discovery	Domain Accounts	Ingress Tool Transfer	Lateral Tool Transfer	Archive via Utility
		PowerShell	System Information Discovery	Bypass User Account Control	DCSync	SMB/Windows Admin Shares	Automated Collection
		Windows Command Shell	System Owner/User Discovery		LSASS Memory		Clipboard Data
		Multi-hop Proxy	Process Discovery		Security Software Discovery		Data from Local System
		Asymmetric Cryptography	System Time Discovery		Disable or Modify System Firewall		Local Data Staging
		Non-Application Layer Protocol	Peripheral Device Discovery		Query Registry		Exfiltration Over C2 Channel
			Local Groups				Clear Windows Event Logs
			Process Injection				
15	Exploit Public-Facing Application	Valid Accounts	File and Directory Discovery	Domain Accounts	Keylogging	Lateral Tool Transfer	Archive via Utility
		PowerShell	System Information Discovery	Bypass User Account Control	Kerberoasting	SMB/Windows Admin Shares	Automated Collection
		Windows Command Shell	System Owner/User Discovery		Password Managers		Data from Local System
		Obfuscated Files or Information	System Network Configuration Discovery		Disable or Modify System Firewall		Local Data Staging
		Windows Management Instrumentation	System Network Connections Discovery		Remote System Discovery		Exfiltration Over C2 Channel
		Asymmetric Cryptography	Network Service Scanning		Security Software Discovery		File Deletion
		Non-Application Layer Protocol					Clear Windows Event Logs
16	External Remote Services	Valid Accounts	File and Directory Discovery	Domain Accounts	Keylogging	Lateral Tool Transfer	Archive via Utility
		PowerShell	System Information Discovery	Bypass User Account Control	Ingress Tool Transfer	SMB/Windows Admin Shares	Automated Collection
		Windows Command Shell	System Owner/User Discovery		DCSync		Data from Local System
		Internal Proxy	Process Discovery		LSASS Memory		Local Data Staging
		Asymmetric Cryptography	Peripheral Device Discovery		Private Keys		Exfiltration Over C2 Channel
		Non-Application Layer Protocol	Local Groups		File Deletion		
		Visual Basic	Process Injection				
17	External Remote Services	Valid Accounts	File and Directory Discovery	Domain Accounts	DCSync	SMB/Windows Admin Shares	Archive via Utility
		PowerShell	System Information Discovery	Bypass User Account Control	LSASS Memory		Automated Collection
		Windows Command Shell	System Owner/User Discovery		File Deletion		Keylogging
		Internal Proxy	System Network Configuration Discovery		Clear Windows Event Logs		Data from Local System
		Asymmetric Cryptography	System Network Connections Discovery		Remote System Discovery		Local Data Staging
		Non-Application Layer Protocol	Local Groups		Security Software Discovery		Exfiltration Over C2 Channel
		Data Obfuscation	Domain Accounts		Password Managers		
		Native API	Software Discovery		Kerberoasting		

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.