SE LABS

EDR
DETECTION

THREAT SERIES: 10

Enterprise Advanced Security

Enterprise

ONLINE REPORT

JULY - SEPTEMBER 2024

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.

Contents

Document version 1.0 Written 1 November 2024

SE LABS

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
Jarred Earlington
Gia Gorbold
Anila Johny
Erica Marotta
Jeremiah Morgan
Julian Owusu-Abrokwa
Joseph Pike
Georgios Sakatzidi
Dimitrios Tsarouchas
Stephen Withey

Marketing
Sara Claridge
Janice Sheridan

Publication
Rahat Hussain
Colin Mackleworth

IT Support
Danny King-Smith
Chris Short

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

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

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

CEO
Simon Edwards

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.

Endpoint Detection Compared

We compare endpoint security products directly using real, major threats

Welcome to the third edition of the Enterprise Advanced Security test, where we directly compare various endpoint security products. This report examines how these products tackle major threats faced by businesses of all sizes from the Global 100 down to medium enterprises, and likely small businesses too. While we provide an overall score, we also delve into the specific details that matter most to your security team, outlining the different levels of protection these products offer.

Endpoint Detection and Response (EDR) solutions go beyond traditional antivirus software, requiring more advanced testing methods. To truly evaluate EDR capabilities, testers need to act like real attackers, meticulously replicating each step of an attack.

It might be tempting to take shortcuts during testing, but to genuinely assess an EDR product's effectiveness, it's crucial to execute every stage of an attack. And each of these stages needs to be realistic you can't just guess what cybercriminals might do. That's why SE Labs carefully tracks real-world cybercriminal behaviour and designs tests based on their tactics.

In the cyber security field, the concept of the "attack chain" is well known. It's a sequence of steps attackers use.

Thankfully, the MITRE organization has outlined these steps through its ATT&CK framework. While this framework doesn't provide a precise guide for every attack scenario, it offers a valuable structure that testers, security vendors, and customers (like you!) can use to conduct tests and interpret results.

The Enterprise Advanced Security tests conducted by SE Labs are based on real attacker behaviour, allowing us to present our testing process using a MITRE ATT&CK style format.

For a detailed breakdown of the ATT&CK framework and how we applied it in our testing, see **Appendix A: Threat Intelligence**, starting on page 14. This approach offers two main benefits: it ensures that our testing methods are both realistic and relevant, and it aligns with a familiar way of visualising cyber attacks.

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** and **Symantec Endpoint Security Complete**.

Malwarebytes EDR and **Open EDR** also put in strong performances, with both scoring Detection Accuracy Ratings of 88%. **Bitdefender Gravity Zone** was less accurate, scoring a 59% Detection Accuracy Rating for missing some threat elements.

Apart from a few misses, all the products handled legitimate products appropriately, allowing them to run unimpeded.

CrowdStrike Falcon garnered an AAA award for its Total Accuracy Rating of 100%. **Symantec Endpoint Security Complete**, **Malwarebytes EDR** and **Open EDR** were also awarded with AAA ratings for Total Accuracy scores in the 90s. **Bitdefender Gravity Zone** achieved an A rating for its Total Accuracy score of 75%.

Executive Summary

Product Tested	Detection Accuracy Rating (%)	Legitimate Accuracy Rating (%)	Total Accuracy Rating (%)
CrowdStrike Falcon	100%	100%	100%
Symantec Endpoint Security Complete	100%	99%	99%
Malwarebytes EDR	88%	100%	93%
Open EDR	88%	96%	92%
Bitdefender Gravity Zone	59%	96%	75%

● **Products highlighted in green were the most accurate, scoring 90 per cent or more for Total Accuracy. Those in orange scored less than 90 but 71 or more. Products shown in red scored less than 71 per cent.**

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

Enterprise Advanced Security Detection Awards

The following products win SE Labs awards:

CrowdStrike Falcon

Symantec Endpoint Security Complete

Malwarebytes EDR

Open EDR

SE LABS
AAA
JUL-SEPT 2024
ENTERPRISE ADVANCED SECURITY

Bitdefender Gravity Zone

SE LABS
A
JUL-SEPT 2024
ENTERPRISE ADVANCED SECURITY

1. How We Tested

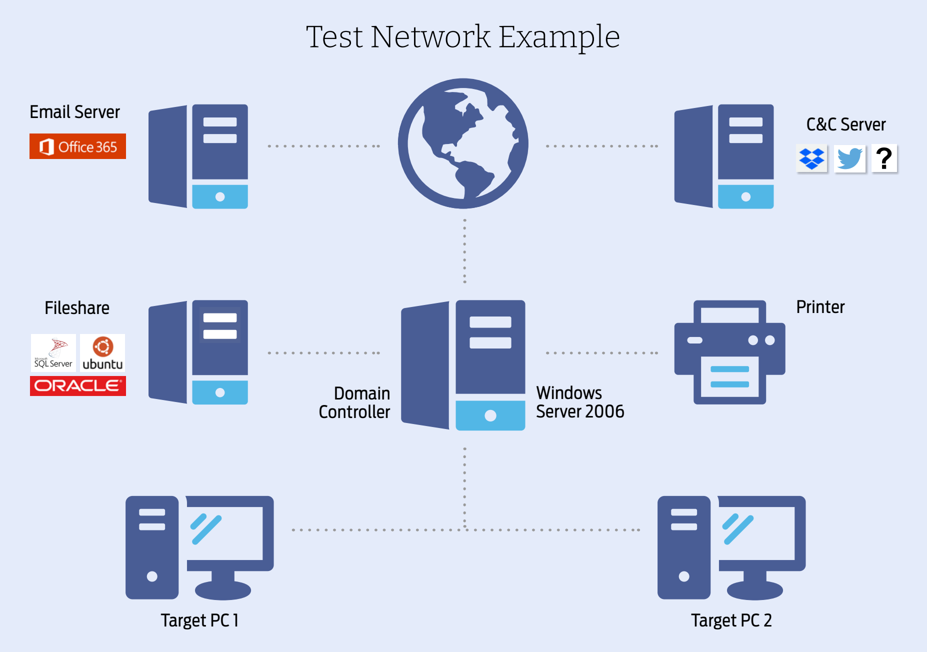
Testers can't assume that products will work a certain way, so running a realistic advanced security test means setting up real networks and hacking them in the same way that real adversaries behave.

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 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 **Attack Details** on page 9 and, for a really detailed drill down on the details, **Appendix A: Threat Intelligence** on pages 14-16 and **Appendix E: Attack Details** on pages 23-28.



● 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 that, 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 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 yet still 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 5-6).

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.

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 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.

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

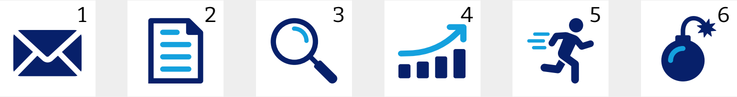
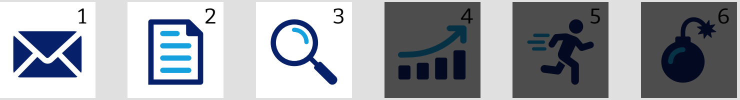


Figure 2. This attack was initially successful but only able to progress as far as the reconnaissance phase.



Attack Details

Attacker/ APT Group	Method	Target	Details
APT29	Compromised Credentials/ VPN Access	🔍	A common tactic of this group is to embed ransomware inside PDF documents.
Scattered Spider	Exploiting Applications/ Valid Accounts	🎲	Financially motivated group most famous for the MGM Resorts International attack.
DPRK Ransomware	Ransomware	🏛	Ransomware as used by North Korean groups targeting Western targets.

KEY					
🏛	Education	🏢	Financial Industries	🎲	Gambling
🏛	Government Espionage	🏭	Manufacturing	🛢	Natural Resources
🏭	Private-sector Energy	🔍	Research Institutes	✈	Travel Industries

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.

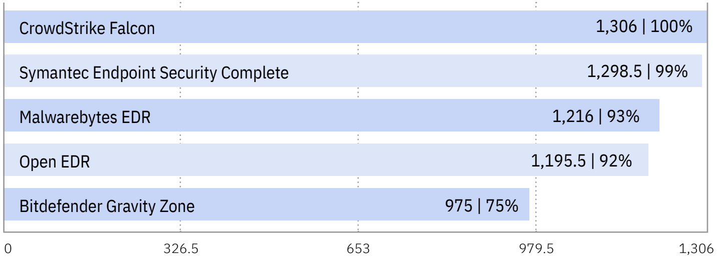
For more details about each APT group please see **AppendixA: Threat Intelligence** on pages 14-16.

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 17 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 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.

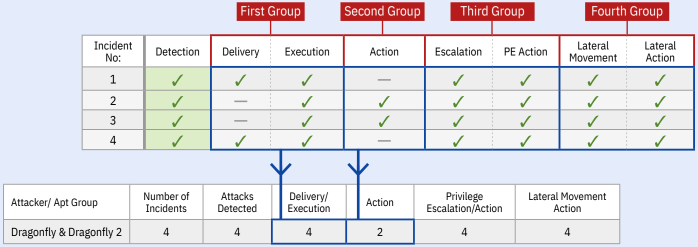
Lateral movement/ action (+10)

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

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

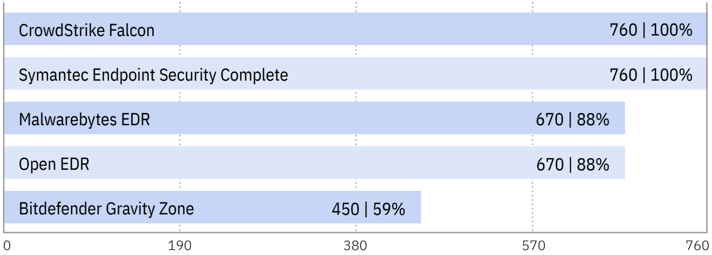
Elements of the attack chain are put into groups. For example, the Delivery and Execution stages of an attack are in the same group. Similarly, we group the Post Escalation stage with the Post Escalation Action (PE Action) stage. When we count detections we look to see at least one detection (tick) in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

3.1 Detection Accuracy Ratings

To understand how we calculate these ratings, see **Appendix B: Detailed Response** on page 17.

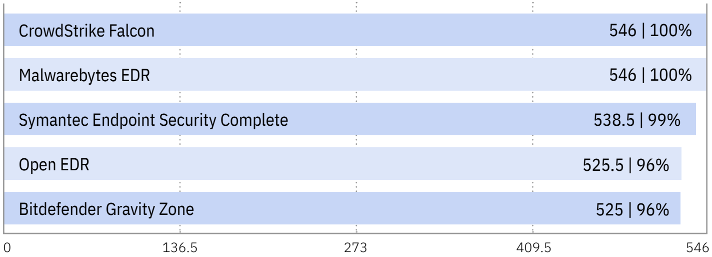


● Detection Ratings are weighted to show that how products detect threats can be subtler than just ‘win’ or ‘lose’.

3.2 Legitimate Accuracy Ratings

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

4. Conclusion

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 attacks have been witnessed in real-world attacks over the previous few years. They are representative of a real and persistent 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 **Attack Details** on page 9 and **Threat Intelligence** on pages 14-16.

It is important to note that while the test used the same type of attacks, new files were used. This exercised the tested products' 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 of the elements of every threat but only achieved a 59% Detection Accuracy Rating. It achieved perfect scores for each incident during the initial attack stage because, even if it only detected delivery about 40% of the time, it did detect every instance of execution. However, in all but three instances, it failed to detect the actions that an attacker can perform while he has remote control of the endpoint. It fared better with the later stages of the attacks when it displayed vigilance against the Scattered Spider and DPRK threats.

Malwarebytes EDR and **Open EDR** posted identical Detection Accuracy Ratings of 88%, as well as the for the totals of the response details. They even missed the same APT29, Scattered Spider and DPRK incidents, responding only when these particular threats were already using the target to launch attacks to other vulnerable systems in the network. Their overall strong performance did differ in the way they reported DPRK attacks. **Open EDR** mostly detected only the execution stage while **Malwarebytes EDR** responded to the delivery of the threat as well.

Speaking of identical Detection Accuracy scores, **CrowdStrike Falcon** and **Symantec Endpoint Security Complete** both achieved perfect results. Both products tracked the movement of every threat from delivery to lateral action, providing visibility at all times with their detection response.

CrowdStrike Falcon achieved perfect results in this test, detecting every element of each threat, and making no mistakes with legitimate applications. **Symantec Endpoint Security Complete** would have done the same except for one detection of a legitimate object. **Malwarebytes EDR's** and **Open EDR's** excellent coverage put them in the same running and all four products achieved AAA awards. **Bitdefender Gravity Zone** performed well enough to win an A rating.

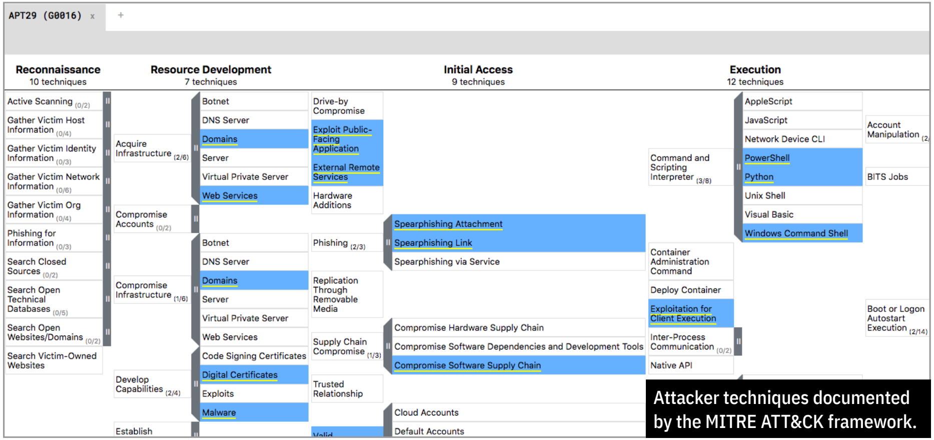
Appendices

Appendix A: Threat Intelligence

APT29

Thought to be connected with Russian military cyber operations, APT29 targets government, military and telecommunications sectors. It is believed to have been behind the Democratic National Committee hack in 2015, in which it used phishing emails with attached malware or links to malicious scripts.

Reference:
https://attack.mitre.org/groups/G0016/



APT29 (G0016) x +

Reconnaissance
10 techniques

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

Resource Development
7 techniques

- Acquire Infrastructure (2/6): Botnet, DNS Server, Domains, Server, Virtual Private Server, Web Services
- Compromise Accounts (0/2)
- Compromise Infrastructure (1/6): Botnet, DNS Server, Domains, Server, Virtual Private Server, Web Services
- Develop Capabilities (2/4): Code Signing Certificates, Digital Certificates, Exploits, Malware
- Establish

Initial Access
9 techniques

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (2/3): Spearphishing Attachment, Spearphishing Link, Spearphishing via Service
- Replication Through Removable Media
- Supply Chain Compromise (1/3): Compromise Hardware Supply Chain, Compromise Software Dependencies and Development Tools, Compromise Software Supply Chain
- Trusted Relationship
- Valid: Cloud Accounts, Default Accounts

Execution
12 techniques

- Command and Scripting Interpreter (3/8): AppleScript, JavaScript, Network Device CLI, PowerShell, Python, Unix Shell, Visual Basic, Windows Command Shell
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication (0/2)
- Native API

- Account Manipulation (2/
- BITS Jobs
- Boot or Logon Autostart Execution (2/14)

Attacker techniques documented by the MITRE ATT&CK framework.

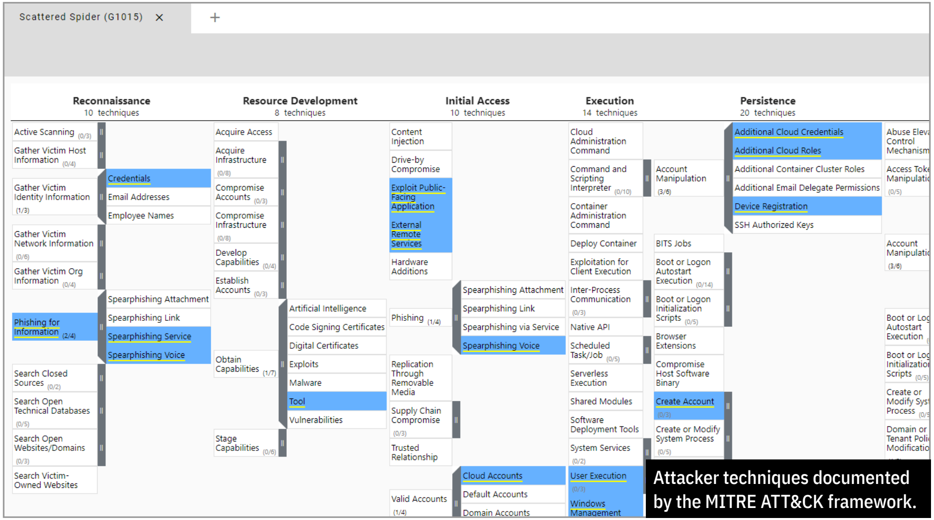
Example APT29 Attack

Delivery	Execution	Action	Privilege Escalation	Post-Escalation	Lateral Movement	Lateral Action
Exploit Public-Facing Application	Web Protocols	Domain Account	Bypass User Account Control	Pass the Ticket	Remote Desktop Protocol	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
External Remote Services	Steganography	Domain Groups		Web Session Cookie		Archive via Utility
	Malicious File	Internet Connection Discovery		Local Accounts		Remote Data Staging
	Internal Proxy	File and Directory Discovery		Domain Accounts		Remote Email Collection
	Mark-of-the-Web Bypass	Domain Trust Discovery				
	Multi-hop Proxy					

Scattered Spider

The Scattered Spider group has been active since at least 2022 and focussed on targets that provided customer relationship and business process solutions. It also attacks telecommunication and high-tech businesses.

Reference:
https://attack.mitre.org/groups/G1015/



Reconnaissance 10 techniques

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

Resource Development 8 techniques

- Acquire Access
- Acquire Infrastructure (0/8)
- Compromise Accounts (0/3)
- Compromise Infrastructure (0/8)
- Develop Capabilities (0/4)
- Establish Accounts (0/3)
- Obtain Capabilities (1/7)
  - Artificial Intelligence
  - Code Signing Certificates
  - Digital Certificates
  - Exploits
  - Malware
  - Tool
  - Vulnerabilities
- Stage Capabilities (0/6)

Initial Access 10 techniques

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

Execution 14 techniques

- Cloud Administration Command
- Command and Scripting Interpreter (0/10)
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication (0/3)
- Native API
- Scheduled Task/Job (0/5)
- Serverless Execution
- Shared Modules
- Software Deployment Tools
- System Services (0/2)
- User Execution (0/3)
- Windows Management

Persistence 20 techniques

- Account Manipulation (3/6)
  - Additional Cloud Credentials
  - Additional Cloud Roles
  - Additional Container Cluster Roles
  - Additional Email Delegate Permissions
  - Device Registration
  - SSH Authorized Keys
- BITS Jobs
- Boot or Logon Autostart Execution (0/14)
- Boot or Logon Initialization Scripts (0/5)
- Browser Extensions
- Compromise Host Software Binary
- Create Account (0/3)
- Create or Modify System Process (0/5)

- Abuse Eleva Control Mechanism
- Access Toke Manipulatio (0/5)
- Account Manipulatio (3/6)
- Boot or Log Autostart Execution
- Boot or Log Initializatio Scripts (0/5)
- Create or Modify Syst Process (0/5
- Domain or Tenant Poli Modificatio

Attacker techniques documented by the MITRE ATT&CK framework.

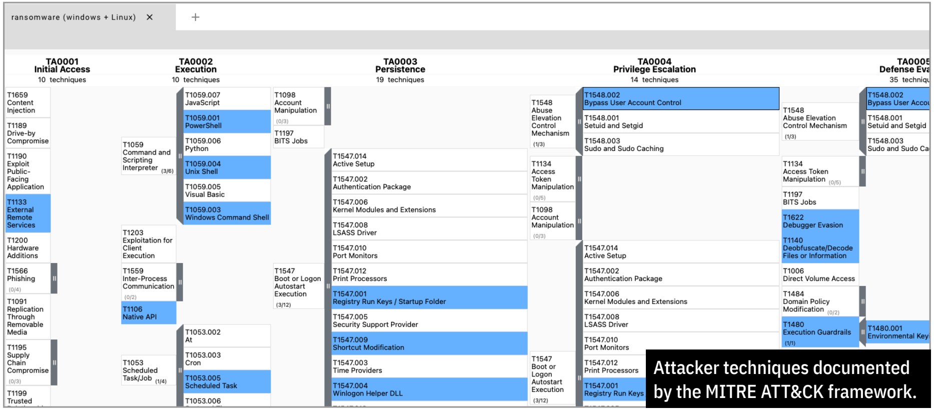
Example Scattered Spider Attack

Delivery	Execution	Action	Privilege Escalation	Post-Escalation	Lateral Movement	Lateral Action
Exploit Public-Facing Application	Malicious Link	System Information Discovery	Bypass User Account Control	Hide Artifacts	SSH	Clipboard Data
	Web Protocols	File and Directory Discovery		Disable or Modify System Firewall		Data from Local System
	Windows Command Shell	Process Discovery		Scheduled Task/Job		Email Collection
		Query Registry		LSASS Memory		Input Capture
		Remote System Discovery				
		Network Share Discovery				
		Network Service Discovery				

DPRK Ransomware

The DPRK Ransomware Group represent the common tactics and techniques attributed to groups originating from the Democratic People's Republic of Korea (North Korea). The main motive of these groups is financial and their main approach is to use Ransomware as a Service (RaaS), reducing the complexity for the attackers.

Reference:
Attack Evaluations: https://attackevals.mitre-engenuity.org/enterprise/er6/



ransomware (windows + Linux) ✕ +

TA0001 Initial Access
10 techniques

T1659 Content Injection
T1189 Drive-by Compromise
T1190 Exploit Public-Facing Application
T1133 External Remote Services
T1200 Hardware Additions
T1566 Phishing (0/4)
T1091 Replication Through Removable Media
T1195 Supply Chain Compromise (0/3)
T1199 Trusted

TA0002 Execution
10 techniques

T1059 Command and Scripting Interpreter (3/6)
T1059.007 JavaScript
T1059.001 PowerShell
T1059.006 Python
T1059.004 Unix Shell
T1059.005 Visual Basic
T1059.003 Windows Command Shell
T1203 Exploitation for Client Execution
T1559 Inter-Process Communication (0/2)
T1106 Native API
T1053 Scheduled Task/Job (1/4)
T1053.002 At
T1053.003 Cron
T1053.005 Scheduled Task
T1053.006

TA0003 Persistence
19 techniques

T1098 Account Manipulation (0/3)
T1197 BITS Jobs
T1547 Boot or Logon Autostart Execution (3/12)
T1547.014 Active Setup
T1547.002 Authentication Package
T1547.006 Kernel Modules and Extensions
T1547.008 LSASS Driver
T1547.010 Port Monitors
T1547.012 Print Processors
T1547.001 Registry Run Keys / Startup Folder
T1547.005 Security Support Provider
T1547.009 Shortcut Modification
T1547.003 Time Providers
T1547.004 Winlogon Helper DLL

TA0004 Privilege Escalation
14 techniques

T1548 Abuse Elevation Control Mechanism (1/3)
T1548.002 Bypass User Account Control
T1548.001 Setuid and Setgid
T1548.003 Sudo and Sudo Caching
T1134 Access Token Manipulation (0/5)
T1098 Account Manipulation (0/3)
T1547 Boot or Logon Autostart Execution (3/12)
T1547.014 Active Setup
T1547.002 Authentication Package
T1547.006 Kernel Modules and Extensions
T1547.008 LSASS Driver
T1547.010 Port Monitors
T1547.012 Print Processors
T1547.001 Registry Run Keys

TA0005 Defense Eva
35 techniqu

T1548 Abuse Elevation Control Mechanism (1/3)
T1548.002 Bypass User Accou
T1548.001 Setuid and Setgid
T1548.003 Sudo and Sudo Ca
T1134 Access Token Manipulation (0/5)
T1197 BITS Jobs
T1622 Debugger Evasion
T1140 Deobfuscate/Decode Files or Information
T1006 Direct Volume Access
T1484 Domain Policy Modification (0/2)
T1480 Execution Guardrails (1/1)
T1480.001 Environmental Key

Attacker techniques documented by the MITRE ATT&CK framework.

Example DPRK Ransomware Attack

Delivery	Execution	Action	Privilege Escalation	Post-Escalation	Lateral Movement	Lateral Action
External Remote Services	**T1059.003:** Windows Command Shell	**T1083:** File and Directory Discovery	**T1548.002:** Bypass User Account Control	**T1053.005:** Scheduled Task	**T1021.002:** SMB/Windows Admin Shares	**T1074.001:** Local Data Staging
	T1036.005: Match Legitimate Name or Location	**T1057:** Process Discovery		**T1055.001:** Dynamic-link Library Injection		**T1119:** Automated Collection
	T1218.010: Regsvr32	**T1033:** System Owner/User Discovery		**T1555.003:** Credentials from Web Browsers		**T1560:** Archive Collected Data
	T1571: Non-Standard Port	**T1614:** System Location Discovery		**T1564.001:** Hidden Files and Directories		**T1030:** Data Transfer Size Limits
	T1564.005: Hidden File System	**T1614.001:** System Language Discovery		**T1564.003:** Hidden Window		**T1041:** Exfiltration Over C2 Channel
	T1564: Hide Artifacts	**T1082:** System Information Discovery		**T1543.003:** Windows Service		**T1485:** Data Destruction
	T1027.002: Software Packing			**T1003.002:** Security Account Manager		**T1486:** Data Encrypted for Impact
	T1564.004: NTFS File Attributes			**T1055.012:** Process Hollowing		**T1489:** Service Stop

Appendix B: Detailed Response

Bitdefender Gravity Zone

APT29

Incident No:	Detection	Delivery	Execution	Action	Escalation	PE Action	Lateral Movement	Lateral Action
1	✓	—	✓	✓	—	—	—	—
2	✓	—	✓	—	—	—	—	—
3	✓	✓	✓	✓	✓	✓	—	—
4	✓	—	✓	—	—	—	—	—
5	✓	—	✓	—	—	—	—	—
6	✓	—	✓	—	✓	—	✓	—

Scattered Spider

Incident No:	Detection	Delivery	Execution	Action	Escalation	PE Action	Lateral Movement	Lateral Action
7	✓	✓	✓	—	✓	✓	—	—
8	✓	✓	✓	—	✓	—	✓	—
9	✓	—	✓	✓	✓	✓	—	—
10	✓	✓	✓	—	✓	✓	✓	—
11	✓	—	✓	—	—	✓	—	—
12	✓	✓	✓	—	✓	✓	—	—
13	✓	✓	✓	—	N/A	—	✓	—

DPRK Ransomware

Incident No:	Detection	Delivery	Execution	Action	Escalation	PE Action	Lateral Movement	Lateral Action
14	✓	—	✓	—	✓	✓	✓	✓
15	✓	—	✓	—	✓	✓	✓	✓
16	✓	✓	✓	—	N/A	—	✓	✓
17	✓	—	✓	—	✓	✓	—	✓
18	✓	—	✓	—	✓	✓	—	✓
19	✓	—	✓	—	✓	✓	✓	✓

Response Details

Attacker/ Apt Group	Number of Incidents	Attacks Detected	Delivery/ Execution	Action	Privilege Escalation/ Action	Lateral Movement Action
APT29	6	6	6	2	2	1
Scattered Spider	7	7	7	1	6	3
DPRK Ransomware	6	6	6	0	5	6
TOTAL	**19**	**19**	**19**	**3**	**13**	**10**

Detection Accuracy Rating Details

Attacker/ Apt Group	Number of Incidents	Attacks Detected	Group Detections	Detection Rating
APT29	6	6	11	110
Scattered Spider	7	7	17	170
DPRK Ransomware	6	6	17	170
TOTAL	**19**	**19**	**45**	**450**

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

APT29

Incident No:	Detection	Delivery	Execution	Action	Escalation	PE Action	Lateral Movement	Lateral Action
1	✓	✓	✓	✓	✓	✓	✓	✓
2	✓	✓	✓	✓	✓	✓	✓	✓
3	✓	✓	✓	✓	✓	✓	✓	✓
4	✓	✓	✓	✓	✓	✓	✓	✓
5	✓	✓	✓	✓	✓	✓	✓	✓
6	✓	✓	✓	✓	✓	✓	✓	✓

Scattered Spider

Incident No:	Detection	Delivery	Execution	Action	Escalation	PE Action	Lateral Movement	Lateral Action
7	✓	✓	✓	✓	✓	✓	✓	✓
8	✓	✓	✓	✓	✓	✓	✓	✓
9	✓	✓	✓	✓	✓	✓	✓	✓
10	✓	✓	✓	✓	✓	✓	✓	✓
11	✓	✓	✓	✓	✓	✓	✓	✓
12	✓	✓	✓	✓	✓	✓	✓	✓
13	✓	✓	✓	✓	N/A	✓	✓	✓

DPRK Ransomware

Incident No:	Detection	Delivery	Execution	Action	Escalation	PE Action	Lateral Movement	Lateral Action
14	✓	✓	✓	✓	✓	✓	✓	✓
15	✓	✓	✓	✓	✓	✓	✓	✓
16	✓	✓	✓	✓	N/A	✓	✓	✓
17	✓	✓	✓	✓	✓	✓	✓	✓
18	✓	✓	✓	✓	✓	✓	✓	✓
19	✓	✓	✓	✓	✓	✓	✓	✓

Response Details

Attacker/ Apt Group	Number of Incidents	Attacks Detected	Delivery/ Execution	Action	Privilege Escalation/ Action	Lateral Movement Action
APT29	6	6	6	6	6	6
Scattered Spider	7	7	7	7	7	7
DPRK Ransomware	6	6	6	2	6	6
TOTAL	**19**	**19**	**19**	**15**	**19**	**19**

Detection Accuracy Rating Details

Attacker/ Apt Group	Number of Incidents	Attacks Detected	Group Detections	Detection Rating
APT29	6	6	24	240
Scattered Spider	7	7	28	280
DPRK Ransomware	6	6	20	240
TOTAL	**19**	**19**	**72**	**760**

Malwarebytes EDR

APT29

Incident No:	Detection	Delivery	Execution	Action	Escalation	PE Action	Lateral Movement	Lateral Action
1	✓	✓	✓	✓	✓	✓	✓	✓
2	✓	✓	✓	✓	✓	✓	✓	✓
3	✓	✓	✓	✓	✓	✓	✓	✓
4	✓	✓	✓	✓	✓	✓	✓	✓
5	✓	✓	✓	✓	✓	✓	✓	✓
6	✓	—	—	—	—	—	✓	✓

Scattered Spider

Incident No:	Detection	Delivery	Execution	Action	Escalation	PE Action	Lateral Movement	Lateral Action
7	✓	✓	✓	✓	✓	✓	✓	✓
8	✓	✓	✓	✓	✓	✓	✓	✓
9	✓	✓	✓	✓	✓	✓	✓	✓
10	✓	✓	✓	✓	✓	✓	✓	✓
11	✓	✓	✓	✓	✓	✓	✓	✓
12	✓	✓	✓	✓	✓	✓	✓	✓
13	✓	—	—	—	N/A	—	✓	✓

DPRK Ransomware

Incident No:	Detection	Delivery	Execution	Action	Escalation	PE Action	Lateral Movement	Lateral Action
14	✓	✓	✓	✓	✓	✓	✓	✓
15	✓	✓	✓	✓	✓	✓	✓	✓
16	✓	—	—	—	N/A	—	✓	✓
17	✓	✓	✓	✓	✓	✓	✓	✓
18	✓	✓	✓	✓	✓	✓	✓	✓
19	✓	✓	✓	✓	✓	✓	✓	✓

Response Details

Attacker/ Apt Group	Number of Incidents	Attacks Detected	Delivery/ Execution	Action	Privilege Escalation/ Action	Lateral Movement Action
APT29	6	6	5	5	5	6
Scattered Spider	7	7	6	6	6	7
DPRK Ransomware	6	6	5	2	5	6
TOTAL	**19**	**19**	**16**	**13**	**16**	**19**

Detection Accuracy Rating Details

Attacker/ Apt Group	Number of Incidents	Attacks Detected	Group Detections	Detection Rating
APT29	6	6	21	210
Scattered Spider	7	7	25	250
DPRK Ransomware	6	6	18	210
TOTAL	**19**	**19**	**64**	**670**

Open EDR

APT29

Incident No:	Detection	Delivery	Execution	Action	Escalation	PE Action	Lateral Movement	Lateral Action
1	✓	✓	✓	✓	✓	✓	—	✓
2	✓	✓	✓	✓	✓	✓	✓	✓
3	✓	✓	✓	✓	✓	✓	—	✓
4	✓	✓	✓	✓	✓	✓	—	✓
5	✓	✓	✓	✓	✓	✓	✓	✓
6	✓	—	—	—	—	—	—	✓

Scattered Spider

Incident No:	Detection	Delivery	Execution	Action	Escalation	PE Action	Lateral Movement	Lateral Action
7	✓	✓	✓	✓	✓	✓	—	✓
8	✓	✓	✓	✓	—	✓	✓	✓
9	✓	✓	✓	✓	✓	✓	✓	✓
10	✓	✓	✓	✓	✓	✓	✓	✓
11	✓	✓	✓	✓	✓	✓	✓	✓
12	✓	✓	✓	✓	✓	✓	—	✓
13	✓	—	—	—	N/A	—	—	✓

DPRK Ransomware

Incident No:	Detection	Delivery	Execution	Action	Escalation	PE Action	Lateral Movement	Lateral Action
14	✓	—	✓	✓	✓	✓	✓	✓
15	✓	—	✓	✓	✓	✓	✓	✓
16	✓	—	—	—	N/A	—	—	✓
17	✓	—	✓	✓	✓	✓	✓	✓
18	✓	—	✓	✓	✓	✓	✓	✓
19	✓	✓	✓	✓	✓	✓	✓	✓

Response Details

Attacker/ Apt Group	Number of Incidents	Attacks Detected	Delivery/ Execution	Action	Privilege Escalation/ Action	Lateral Movement Action
APT29	6	6	5	5	5	6
Scattered Spider	7	7	6	6	6	7
DPRK Ransomware	6	6	5	2	5	6
TOTAL	**19**	**19**	**16**	**13**	**16**	**19**

Detection Accuracy Rating Details

Attacker/ Apt Group	Number of Incidents	Attacks Detected	Group Detections	Detection Rating
APT29	6	6	21	210
Scattered Spider	7	7	25	250
DPRK Ransomware	6	6	18	210
TOTAL	**19**	**19**	**64**	**670**

Symantec Endpoint Security Complete

APT29

Incident No:	Detection	Delivery	Execution	Action	Escalation	PE Action	Lateral Movement	Lateral Action
1	✓	✓	✓	✓	✓	✓	✓	✓
2	✓	✓	✓	✓	✓	✓	✓	✓
3	✓	✓	✓	✓	✓	✓	✓	✓
4	✓	✓	✓	✓	✓	✓	✓	✓
5	✓	✓	✓	✓	✓	✓	✓	✓
6	✓	✓	✓	✓	✓	✓	✓	✓

Scattered Spider

Incident No:	Detection	Delivery	Execution	Action	Escalation	PE Action	Lateral Movement	Lateral Action
7	✓	✓	✓	✓	✓	✓	✓	✓
8	✓	✓	✓	✓	✓	✓	✓	✓
9	✓	✓	✓	✓	✓	✓	✓	✓
10	✓	✓	✓	✓	✓	✓	✓	✓
11	✓	✓	✓	✓	✓	✓	✓	✓
12	✓	✓	✓	✓	✓	✓	✓	✓
13	✓	✓	✓	✓	N/A	✓	✓	✓

DPRK Ransomware

Incident No:	Detection	Delivery	Execution	Action	Escalation	PE Action	Lateral Movement	Lateral Action
14	✓	✓	✓	✓	✓	✓	✓	✓
15	✓	✓	✓	✓	✓	✓	✓	✓
16	✓	✓	✓	✓	N/A	✓	✓	✓
17	✓	✓	✓	✓	✓	✓	✓	✓
18	✓	✓	✓	✓	✓	✓	✓	✓
19	✓	✓	✓	✓	✓	✓	✓	✓

Response Details

Attacker/ Apt Group	Number of Incidents	Attacks Detected	Delivery/ Execution	Action	Privilege Escalation/ Action	Lateral Movement Action
APT29	6	6	6	6	6	6
Scattered Spider	7	7	7	7	7	7
DPRK Ransomware	6	6	6	2	6	6
TOTAL	**19**	**19**	**19**	**15**	**19**	**19**

Detection Accuracy Rating Details

Attacker/ Apt Group	Number of Incidents	Attacks Detected	Group Detections	Detection Rating
APT29	6	6	24	240
Scattered Spider	7	7	28	280
DPRK Ransomware	6	6	20	240
TOTAL	**19**	**19**	**72**	**760**

Appendix C: Legitimate Interaction Ratings

It's crucial that security products not only detect threats but also correctly handle legitimate objects, such as files and URLs. Incorrectly labelling legitimate objects as being ‘malware’ or ‘harmful’ is a false positive (FP) result.

In reality, genuine FPs are quite rare in good testing, with good products. In our experience it is unusual for a legitimate application to be classified as ‘malware’. More often it will be classified as ‘unknown’, ‘suspicious’ or ‘unwanted’ (or other terms that mean much the same thing).

Interaction Ratings

We use a subtle system to rate a product's approach to legitimate objects. This takes into account how it classifies them and how it presents that information.

Sometimes a product will pass the buck and demand that a user or administrator decide if something is safe or not. In such cases, the product may make a recommendation to allow or remove the object. In other cases the product will make no recommendation, which is possibly even less useful.

If a product reports that an application is safe, or doesn't recommend any action (such as to remove it), it has achieved an optimum result. Anything else is a Non-Optimal Classification/ Action (NOCA).

A product may be configured with a policy to restrict certain objects according to the business' objectives. A recommendation to remove a legitimate application could be the correct result if it matches a policy. For example, a policy to refuse all Microsoft Office applications would recommend the removal of Microsoft Word. As long as the alert is clear that this is a policy decision and not a mistake then the product will not face a penalty.

For example, an acceptable alert would be: ‘Word.exe is not permitted due to policy: NoMicrosoft’, whereas an unacceptable alert would be: “Word.exe is a threat that should be removed (Trojan.XYZ)”.

We think that measuring NOCAs is more useful than simply counting rarer FPs. The table below shows how we score different combinations of Classifications (the vertical axis) and Actions (the horizontal axis).

	Recommendation: None	Recommendation: Allow	Recommendation: Unclear	Recommendation: Remove	Action: Remove
Safe	2	1.5	1		
Unknown	2	1	0.5	0	-0.5
Not Classified	2	0.5	0	-0.5	-1
Suspicious	0.5	0	-0.5	-1	-1.5
Unwanted	0	-0.5	1	-1.5	-2
Malicious				2	-2

Legitimate Software Prevalence Rating Modifiers

Very High Impact	5
High Impact	4
Medium Impact	3
Low Impact	2
Very Low Impact	1

Prevalence Ratings

There is a significant difference between a product incorrectly alerting against a popular application like Microsoft Word and condemning a rare, obscure or outdated application such as Internet Explorer 6. One is very popular all over the world and its detection as malware (or something less serious, but still suspicious) is a big deal.

Conversely, the outdated web browser has not been in general use for years and in many cases should not be used in a business environment. Detecting this application as malware may be wrong (an FP) but the mistake is less impactful.

With this mind, we collected objects of varying popularity and sorted them into five separate categories, as follows:

1. Very High Impact
2. High Impact
3. Medium Impact
4. Low Impact
5. Very Low Impact

Incorrectly labelling any legitimate object invokes penalties, but classifying Microsoft Word as malware, and recommending its removal without providing any context, will bring far greater penalties than doing the same for an ancient, unsupported web browser.

In order to calculate these relative penalties, we assign each impact category with a rating modifier, as shown in the table above.

Objects are obtained from original sources in most cases, avoiding third-party download sites. This is due to the risk of third parties modifying the legitimate objects and potentially adding problematic elements that could be a threat to an organisation. We remove adware and other less obviously legitimate objects from the test set.

We base the prevalence for each object on publicly available data sources.

Accuracy Ratings

We calculate legitimate interaction ratings by multiplying together the interaction and prevalence ratings for each object:

Accuracy Rating = Interaction Rating x Prevalence Rating

If a product inspected one legitimate, Medium Impact application and gave no alert or recommendation, its Accuracy Rating would be calculated like this:

Accuracy Rating = 2 x 3 = 6

If it labelled the object as 'suspicious' its rating would be calculated like this:

Accuracy Rating = 0.5 x 3 = 1.5

This same calculation is made for each legitimate object in the test and the results are summed and used to populate the graph and table shown under **3.2 Legitimate Accuracy Ratings** in this report.

Distribution of Impact Categories

In this test there was a range of objects with different levels of prevalence. The table below shows the frequencies:

Legitimate Interaction Ratings

Product	None (allowed)	None (allowed)
Bitdefender Gravity Zone	75	100%
CrowdStrike Falcon	75	100%
Malwarebytes EDR	75	100%
Open EDR	75	100%
Symantec Endpoint Security Complete	75	100%

● **Products that do not bother users and classify most applications correctly earn more points than those that ask questions and condemn legitimate applications.**

Legitimate Software Category Frequency

Prevalence Rating	Frequency
Very High Impact	32
High Impact	32
Medium Impact	17
Low Impact	12
Very Low Impact	7

Appendix D: Terms Used

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 E: FAQs

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.

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

- The test was conducted between 4th August and 27th September 2024.
- All products were configured according to each vendor's recommendations, when such recommendations were provided.
- Targeted attacks were selected and verified by SE Labs.
- Malicious emails, URLs, attachments and legitimate messages were independently located and verified by SE Labs.
- Malicious and legitimate data was provided to partner organisations once the test was complete.

Appendix F: Attack Details

APT29

Incident No.	Delivery	Execution	Action	Privilege Escalation	Post-Escalation	Lateral Movement	Lateral Action
1	Exploit Public-Facing Application	Web Protocols	Domain Account	Bypass User Account Control	Pass the Ticket	Remote Desktop Protocol	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
	External Remote Services	Steganography	Domain Groups		Web Session Cookie		Archive via Utility
		Malicious File	Internet Connection Discovery		Local Accounts		Remote Data Staging
		Internal Proxy	File and Directory Discovery		Domain Accounts		Remote Email Collection
		Mark-of-the-Web Bypass	Domain Trust Discovery				
		Multi-hop Proxy					
2	Trusted Relationship	Bidirectional Communication	File and Directory Discovery	Bypass User Account Control	Disable or Modify System Firewall	SMB/Windows Admin Shares	Deobfuscate/Decode Files or Information
	Spearphishing Attachment	Dynamic Resolution	Process Discovery		Disable or Modify Tools		Archive via Utility
		Mshta	Remote System Discovery		Disable Windows Event Logging		Remote Data Staging
		Software Packing	System Information Discovery		Accessibility Features		Remote Email Collection
		Code Signing	Domain Trust Discovery		Clear Mailbox Data		Data from Local System
		Windows Command Shell	Internet Connection Discovery				
		Malicious File					
3	Spearphishing Attachment	Encrypted Channel	File and Directory Discovery	Ingress Tool Transfer	File Deletion	Windows Remote Management	Archive via Utility
		Rundll32	Remote System Discovery	Exploitation for Privilege Escalation	Timestomp		Remote Data Staging
		HTML Smuggling	System Information Discovery		Masquerade Task or Service		Remote Email Collection
		Visual Basic	Domain Trust Discovery		Match Legitimate Name or Location		Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
		Malicious File	Domain Groups		Windows Management Instrumentation Event Subscription		
4	Spearphishing via Service	Malicious File	File and Directory Discovery	Bypass User Account Control	Registry Run Keys / Startup Folder	Remote Desktop Protocol	Deobfuscate/Decode Files or Information
	Compromise Software Supply Chain	Domain Fronting	Process Discovery		Disable or Modify System Firewall		Archive via Utility
		Python	Remote System Discovery		Scheduled Task		Exfiltration Over C2 Channel
		Exploitation for Client Execution	System Information Discovery		External Remote Services		Data from Local System
			Domain Account		Timestomp		
5	Spearphishing Attachment	Powershell	Domain Account	Bypass User Account Control	Pass the Ticket	SMB/Windows Admin Shares	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
		Malicious File	Domain Groups		Local Accounts		Archive via Utility
		Internal Proxy	File and Directory Discovery		Disable Windows Event Logging		Remote Data Staging
		Bidirectional Communication	Domain Trust Discovery		Disable or Modify Tools		Remote Email Collection
		Encrypted Channel			DCSync		
					File Deletion		

Incident No.	Delivery	Execution	Action	Privilege Escalation	Post-Escalation	Lateral Movement	Lateral Action
6	Spearphishing Link	Web Protocols	Internet Connection Discovery	Ingress Tool Transfer	Binary Padding	Remote Desktop Protocol	Archive via Utility
		Domain Fronting	File and Directory Discovery		RC Scripts		Data from Local System
		Internal Proxy	Process Discovery				
		Software Packing	System Information Discovery				
		Malicious Link					

Scattered Spider

Incident No.	Delivery	Execution	Action	Privilege Escalation	Post-Escalation	Lateral Movement	Lateral Action
7	Exploit Public-Facing Application	Malicious Link	System Information Discovery	Bypass User Account Control	Hide Artifacts	SSH	Clipboard Data
		Web Protocols	File and Directory Discovery		Disable or Modify System Firewall		Data from Local System
		Windows Command Shell	Process Discovery		Scheduled Task/Job		Email Collection
			Query Registry		LSASS Memory		Input Capture
			Remote System Discovery				
			Network Share Discovery				
			Network Service Discovery				
8	Spearphishing Link	Malicious Link	System Information Discovery	Create Process with Token	Security Software Discovery	Service Execution	Email Collection
		Web Protocols	File and Directory Discovery	Token Impersonation/Theft	Dynamic-link Library Injection		Data from Local System
		Windows Command Shell	Process Discovery		Winlog Helper DLL		Account Access Removal
		External Proxy	System Network Configuration Discovery		Browser Extensions		Data Encrypted for Impact
			System Network Connections Discovery		Hide Artifacts		System Shutdown/Reboot
			Internet Connection Discovery				
			Local Account				
9	Spearphishing Attachment	Malicious File	System Information Discovery	Bypass User Account Control	Domain Accounts	SMB/Windows Admin Shares	Account Access Removal
		Web Protocols	File and Directory Discovery		Local Accounts		Data Encrypted for Impact
		Windows Command Shell	Local Account		Kernel Modules and Extensions		System Shutdown/Reboot
		External Proxy	Domain Groups		BITS Jobs		Safe Mode Boot
		Non-Standard Port	Domain Trust Discovery		DCSync		Automatic Collection
		Indicator Removal From Tools	Remote System Discovery		Impair Command History Logging		Data from Local System
			Group Policy Discovery		LSA Secrets		

Incident No.	Delivery	Execution	Action	Privilege Escalation	Post-Escalation	Lateral Movement	Lateral Action
10	Exploit Public-Facing Application	Malicious Link	System Information Discovery	Exploitation for Privilege Escalation	NTDS	SMB/Windows Admin Shares	Input Capture
		Web Protocols	File and Directory Discovery		Registry Run Keys / Startup Folder		Clipboard Data
		Windows Command Shell	Process Discovery		Match Legitimate Name or Location		Data from Local System
		External Proxy	Remote System Discovery		Rename System Utilities		Automatic Collection
		Non-Standard Port	Network Service Discovery		Modify Authentication Process		
		Compromise Software Supply Chain	Query Registry				
11	Spearphishing Attachment	Windows Command Shell	File and Directory Discovery	Access Token Manipulation	Portable Executable Injection	Windows Remote Management	Data from Local System
		External Proxy	System Information Discovery		Rootkit	Initial File Transfer	Account Access Removal
		Non-Standard Port	System Owner/User Discovery		Web Session Cookie		Data Encrypted for Impact
		Indicator Removal From Tools	Network Share Discovery		Credentials In Files		Input Capture
		Trusted Relationship	Process Discovery		External Remote Services		Automatic Collection
		Compromise Software Supply Chain	Query Registry				System Shutdown/Reboot
			Domain Account				
			Internet Connection Discovery				
			Domain Groups				
12	Exploit Public-Facing Application	Malicious File	File and Directory Discovery	Bypass User Account Control	Native API	Remote Access Software	Input Capture
		Web Protocols	System Information Discovery		Credentials from Password Stores	Protocol Tunneling	Clipboard Data
		Windows Command Shell	System Owner/User Discovery		Default Accounts		Automatic Collection
		External Proxy	Domain Account		Windows Management Instrumentation Event Subscription		Account Access Removal
		Non-Standard Port	Internet Connection Discovery		Modify Authentication Process		Data Encrypted for Impact
		Indicator Removal From Tools	Domain Groups		Disable or Modify Tools		System Shutdown/Reboot
			Process Discovery		Registry Run Keys / Startup Folder		Safe Mode Boot
			Query Registry				
			Permission Groups Discovery				
13	Spearphishing Link	Malicious Link	File and Directory Discovery	N/A	Binary Padding	External Remote Services / SSH	Input Capture
		Web Protocols	System Information Discovery		File Deletion		Clipboard Data
		Non-Standard Port	System Owner/User Discovery		Match Legitimate name or Location		Email Collection
			Internet Connection Discovery				Data from Local System

DPRK Ransomware

Incident No.	Delivery	Execution	Action	Privilege Escalation	Post-Escalation	Lateral Movement	Lateral Action
14	External Remote Services	**T1059.003**: Windows Command Shell	**T1083:** File and Directory Discovery	**T1548.002: B**ypass User Account Control	**T1053.005:** Scheduled Task	**T1021.002:** SMB/Windows Admin Shares	**T1074.001:** Local Data Staging
		T1036.005: Match Legitimate Name or Location	**T1057:** Process Discovery		**T1055.001:** Dynamic-link Library Injection		**T1119:** Automated Collection
		T1218.010: Regsvr32	**T1033:** System Owner/User Discovery		**T1555.003:** Credentials from Web Browsers		**T1560:** Archive Collected Data
		T1571: Non-Standard Port	**T1614:** System Location Discovery		**T1564.001:** Hidden Files and Directories		**T1030:** Data Transfer Size Limits
		T1564.005: Hidden File System	**T1614.001**: System Language Discovery		**T1564.003:** Hidden Window		**T1041:** Exfiltration Over C2 Channel
		T1564: Hide Artifacts	**T1082:** System Information Discovery		**T1543.003:** Windows Service		
		T1027.002: Software Packing			**T1003.002:** Security Account Manager		
		T1564.004: NTFS File Attributes			**T1055.012:** Process Hollowing		
15	External Remote Services	**T1059.003:** Windows Command Shell	**T1083:** File and Directory Discovery	**T1548.002:** Bypass User Account Control	**T1070.004:** File Deletion	**T1080:** Taint Shared Content	**T1074:** Data Staged
		T1059.001: PowerShell	**T1057:** Process Discovery		**T1547.004:** Winlogon Helper DLL	**T1072:** Software Deployment Tools	**T1119:** Automated Collection
		T1036.004: Masquerade Task or Service	**T1082:** System Information Discovery		**T1055.001:** Dynamic-link Library Injection		**T1560.001:** Archive via Utility
		T1036.008: Masquerade File Type	**T1016:** System Network Configuration Discovery		**T1562.002:** Disable Windows Event Logging		**T1048.001:** Exfiltration Over Symmetric Encrypted Non-C2 Protocol
		T1027.002: Software Packing	**T1007:** System Service Discovery		**T1562.004:** Disable or Modify System Firewall		
		T1027.008: Stripped Payloads	**T1069:** Permission Groups Discovery				
		T1071.001: Web Protocols					
		T1569.002: Service Execution					
16	External Remote Services	**T1059.004:** Unix Shell	**T1083:** File and Directory Discovery	N/A	**T1070.001:** Clear Windows Event Logs	**T1021.002:** SMB/Windows Admin Shares	**T1048.003:** Exfiltration Over Unencrypted Non-C2 Protocol
		T1095: Non-Application Layer Protocol	**T1057:** Process Discovery		**T1070.004:** File Deletion		**T1074:** Data Staged
		T1571: Non-Standard Port	**T1033:** System Owner/User Discovery		**T1552.003:** Bash History		**T1119:** Automated Collection
		T1564.005: Hidden File System	**T1007:** System Service Discovery		**T1562.006:** Indicator Blocking		**T1020:** Automated Exfiltration
		T1564: Hide Artifacts	**T1016.002:** Wi-Fi Discovery				**T1048:** Exfiltration Over Alternative Protocol
		T1219: Remote Access Software	**T1069.002:** Domain Groups				**T1485:** Data Destruction
			T1069: Permission Groups Discovery				**T1486:** Data Encrypted for Impact
			T1016.001: Internet Connection Discovery				**T1489:** Service Stop
							T1490: Inhibit System Recovery
							T1491.001: Internal Defacement

Incident No.	Delivery	Execution	Action	Privilege Escalation	Post-Escalation	Lateral Movement	Lateral Action
17	External Remote Services	**T1059.003:** Windows Command Shell	**T1083:** File and Directory Discovery	**T1546.012:** Image File Execution Options Injection	**T1562.002:** Disable Windows Event Logging	**T1570:** Lateral Tool Transfer	**T1074:** Data Staged
		T1622: Debugger Evasion	**T1057:** Process Discovery		**T1562.004:** Disable or Modify System Firewall	**T1072:** Software Deployment Tools	**T1119:** Automated Collection
		T1480: Execution Guardrails	**T1497.001:** System Checks		**T1112:** Modify Registry		**T1560.001:** Archive via Utility
		T1218.011: Rundll32	**T1497:** Virtualization/Sandbox Evasion		**T1055.001:** Dynamic-link Library Injection		**T1030:** Data Transfer Size Limits
		T1071.002: File Transfer Protocols	**T1518.001:** Security Software Discovery		**T1552.002:** Credentials in Registry		**T1048.002:** Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
			T1518: Software Discovery		**T1003.002:** Security Account Manager		**T1485:** Data Destruction
			T1016.002: Wi-Fi Discovery		**T1003.001:** LSASS Memory		**T1486:** Data Encrypted for Impact
					T1003.004: LSA Secrets		**T1489:** Service Stop
					T1564.001: Hidden Files and Directories		**T1490:** Inhibit System Recovery
					T1055.012: Process Hollowing		**T1491.001:** Internal Defacement
18	External Remote Services	**T1059.003:** Windows Command Shell	**T1083:** File and Directory Discovery	**T1546.012:** Image File Execution Options Injection	**T1564.001:** Hidden Files and Directories	**T1072:** Software Deployment Tools	**T1074:** Data Staged
		T1059.001: PowerShell	**T1057:** Process Discovery		**T1003.002:** Security Account Manager		**T1039:** Data from Network Shared Drive
		T1218.007: Msiexec	**T1033:** System Owner/User Discovery		**T1003.001:** LSASS Memory		**T1074.002:** Remote Data Staging
		T1106: Native API	**T1135:** Network Share Discovery		**T1003.004:** LSA Secrets		**T1560.003:** Archive via Custom Method
		T1620: Reflective Code Loading	**T1018:** Remote System Discovery		**T1003.005:** Cached Domain Credentials		**T1041:** Exfiltration Over C2 Channel
		T1480.001: Environmental Keying	**T1497.002:** User Activity Based Checks		**T1552.001:** Credentials In Files		
			T1497.003: Time Based Evasion		**T1555.003:** Credentials from Web Browsers		
			T1007: System Service Discovery		**T1055.002:** Portable Executable Injection		
			T1016.001: Internet Connection Discovery		**T1037.001:** Logon Script (Windows)		
			T1069.002: Domain Groups		**T1564.003:** Hidden Window		
			T1482: Domain Trust Discovery				
			T1069.001: Local Group				

Incident No.	Delivery	Execution	Action	Privilege Escalation	Post-Escalation	Lateral Movement	Lateral Action
19	External Remote Services	**T1059.003:** Windows Command Shell	**T1033:** System Owner/User Discovery	**T1548.002:** Bypass User Account Control	**T1070.004:** File Deletion	**T1570:** Lateral Tool Transfer	**T1005:** Data from Local System
		T1027.007: Dynamic API Resolution	**T1069:** Permission Groups Discovery		**T1053.005:** Scheduled Task		**T1119:** Automated Collection
		T1027.009: Embedded Payloads	**T1069.001:** Local Groups		**T1564.002:** Hidden Users		**T1560.002:** Archive via Library
		T1569: System Services	**T1016.001:** Internet Connection Discovery		**T1140:** Deobfuscate/Decode Files or Information		**T1048:** Exfiltration Over C2 Channel
		T1547.009: Shortcut Modification	**T1135:** Network Share Discovery		**T1562.002:** Disable Windows Event Logging		**T1485:** Data Destruction
		T1047: Windows Management Instrumentation	**T1518.001:** Security Software Discovery		**T1562.004:** Disable or Modify System Firewall		**T1486:** Data Encrypted for Impact
			T1518: Software Discovery		**T1547.001:** Registry Run Keys / Startup Folder		**T1489:** Service Stop
			T1018: Remote System Discovery		**T1543.003:** Windows Service		**T1490:** Inhibit System Recovery
			T1069.002: Domain Groups		**T1552.001:** Credentials In Files		**T1491.001:** Internal Defacement

Appendix G: Product Versions

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

Vendor	Product	Build Version (start)	Build Version (end)
Bitdefender	Gravity Zone	PC: 7.9.13.423 DC: 7.9.14.430	PC: 7.9.13.423 DC: 7.9.14.430
CrowdStrike	Falcon	PC: 7.16.18608.0 DC: 7.16.18609.0	PC: 7.16.18609.0 DC: 7.16.18609.0
Malwarebytes	EDR	1.2.0.1125	1.2.0.1125
Symantec	Endpoint Security Complete	Version: 14 (14.9 RU9) Build: 11216 (14.3.11216.9000)	Version: 14 (14.9 RU9) Build: 11216 (14.3.11216.9000)
Open EDR	——	9.1.48792.24030	9.1.48792.24030

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.