Enterprise Advanced Security

Coro
Endpoint Detection and Response

SE LABS ® tested **Coro – EDR** against against
targeted attacks based on Threat Series: 9

These attacks are designed to compromise systems and penetrate
target networks in the same way as the advanced persistent
hacking groups known as Scattered Spider, APT29 and Lapsus$
operate to 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 6th November 2024

Introduction

**CEO
Simon Edwards**

Early Protection Systems

Testing protection against fully featured attacks

There are many opportunities to spot and stop attackers. Products can detect them when attackers send phishing emails to targets. Or later, when other emails contain links to malicious code. Some kick into action when malware enters the system. Others sit up and notice when the attackers exhibit bad behaviour on the network.

Regardless of which stages your security takes effect, you probably want it to detect and prevent before the breach runs to its conclusion in the press.

Our Enterprise Advanced Security test is unique, in that we test products by running a full attack. We follow every step of a breach attempt to ensure that the test is as realistic as possible.

This is important because different products can detect and prevent threats differently.

Ultimately you want your chosen security product to prevent a breach one way or another, but it's more ideal to stop a threat early, rather than watch as it wreaks havoc before stopping it and trying to clean up.

Some products are designed solely to watch and inform, while others can also get involved and remove threats either as soon as they appear or after they start causing damage.

For the 'watchers' we run the Enterprise Advanced Security test in Detection mode. For 'stoppers' like **Coro – EDR** we can demonstrate effectiveness by testing in Protection Mode.

In this report we look at how **Coro – EDR** handled full breach attempts. At which stages did it detect and protect? And did it allow business as usual, or mis-handle legitimate applications?

Understanding the capabilities of different security products is always better achieved before you need to use them in a live scenario. SE Labs' Enterprise Advanced Security test reports help you assess which are the best for your own organisation.

Executive Summary

Coro – EDR was tested against a range of hacking attacks designed to compromise systems and penetrate target networks in the same way as criminals and other attackers breach systems and networks.

We examined its abilities to:
- Detect highly targeted attacks
- Protect against the actions of highly targeted attacks
- Provide remediation to damage and other risks posed by the threats
- Handle legitimate applications and other objects

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

Coro – EDR posted excellent results, detecting all of the threats and protecting against almost all of them. It generated no false positives, meaning that it didn't wrongly detect or hamper harmless, legitimate software. One percent shy of a perfect Total Accuracy Rating is a great result in a challenging test.

Enterprise Advanced Security Protection Award

The following product wins the SE Labs award:

SE LABS

AAA

NOVEMBER 2024

ENTERPRISE ADVANCED SECURITY

Coro
EDR

Executive Summary

Product Tested	Protection Accuracy Rating (%)	Legitimate Accuracy Rating (%)	Total Accuracy Rating (%)
Coro – EDR	99%	100%	99%

● 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 9.

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

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

The techniques that we choose for each test case are largely dictated by the real-world behaviour of online criminals. We observe their tactics and replicate what they do in this test. To see more
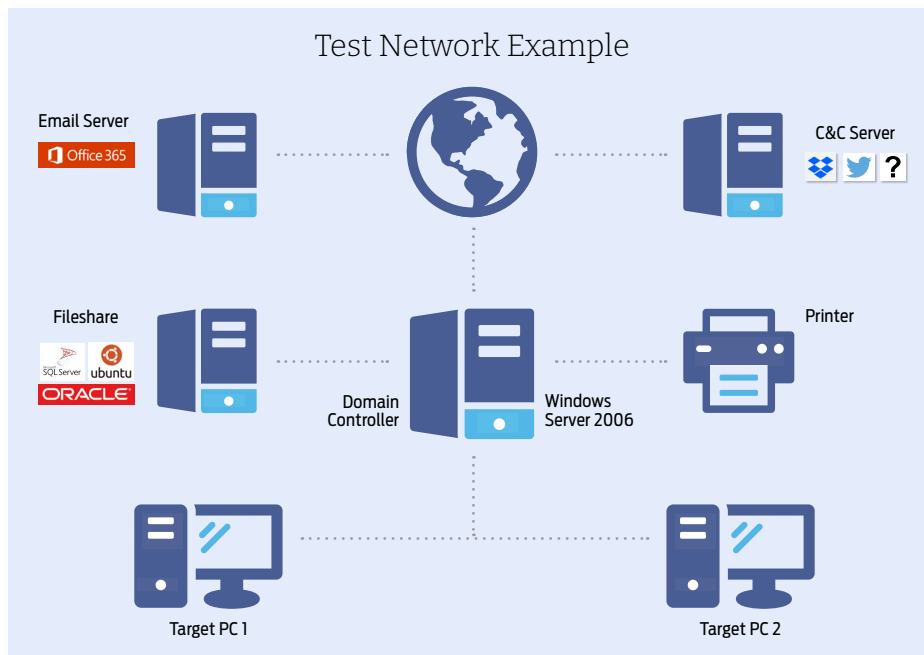
details about how the specific attackers behaved, and how we copied them, see **Attack Details** on page 8 and, for a really detailed drill down on the details, **4. Threat Intelligence** on pages 12-14 and **Appendix C: Attack Details** on pages 18-21

Test Network Example

Email Server
Office 365

Fileshare
SQL Server ubuntu
ORACLE

Domain Controller

Windows Server 2006

C&C Server

Printer

Target PC 1

Target PC 2

● 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

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

Attacker/ APT Group	Method	Target	Details
Scattered Spider	Exploiting Applications/ Valid Accounts		Financially motivated group most famous for the MGM Resorts International attack.
APT29	Compromised Credentials/ VPN Access		A common tactic of this group is to embed ransomware inside PDF documents.
Lapsus$	Compromised Credentials/ VPN Access		Social engineering for credential harvesting, SIM swapping and destructive behaviour even without deploying ransomware.

KEY					
	Education		Financial Industries		Gambling
	Government Espionage		Manufacturing		Natural Resources
	Private-sector Energy		Research Institutes		Travel Industries

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

For more details about each APT group please see **4. Threat Intelligence** on pages 12-14.

2. Total Accuracy Ratings

Judging the effectiveness of an endpoint security product is a subtle art, and many factors are at play when assessing how well it performs. To make things easier we've combined all the different results from this report into one easy-to-understand chart.

The chart below takes into account not only the product's ability to detect and protect against threats, but also its handling of non-malicious objects such as web addresses (URLs) and applications.
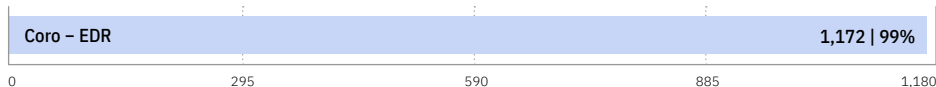
Not all protections, or detections for that matter, are equal. A product might completely block a URL, which stops the threat before it can even start its intended series of malicious events. Alternatively, the product might allow a web-based exploit to execute but prevent it from downloading any further code to

the target. In another case malware might run on the target for a short while before its behaviour is detected and its code is deleted or moved to a safe 'quarantine' area for future analysis. We take these outcomes into account when attributing points that form final ratings.

For example, a product that completely blocks a threat is rated more highly than one that allows a threat to run for a while before eventually evicting it. Products that allow all malware infections, or that block popular legitimate applications, are penalised heavily.

Scoring a product's response to a potential breach requires a granular method, which we outline in **3. Response Details** on page 10.

Total Accuracy Ratings

Coro – EDR	**1,172 | 99%**

0　　　　　　295　　　　　　590　　　　　　885　　　　　　1,180

● 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 and protect against all relevant elements of an attack. The term 'relevant' is important, because if early stages of an attack are countered fully there is no need for later stages to be addressed.

In each test case the product can score a maximum of four points for successfully detecting the attack and protecting the system from ill effects. If it fails to act optimally in any number of ways it is penalised, to a maximum extent of -9 (so -5 points in total). The level of penalisation is according to the following rules, which illustrate the compound penalties imposed when a product fails to prevent each of the stages of an attack.

Detection (-0.5)
If the product fails to detect the threat with any degree of useful information, it is penalised by 0.5 points.

Execution (-0.5)
Threats that are allowed to execute generate a penalty of 0.5 points.

Action (-1)
If the attack is permitted to perform one or more actions, remotely controlling the target, then a further penalty of 1 point is imposed.

Privilege escalation (-2)
As the attack impact increases in seriousness, so do the penalties. If the attacker can escalate system privileges then an additional penalty of 2 points is added to the total.

Post-escalation action (-1)
New, more powerful and insidious actions are possible with escalated privileges. If these are successful, the product loses one more point.

Lateral movement (-2)
The attacker may attempt to use the target as a launching system to other vulnerable systems. If successful, two more points are deducted from the total.

Lateral action (-2)
If able to perform actions on the new target, the attacker expands his/ her influence on the network and the product loses two more points.

The Protection Rating is calculated by multiplying the resulting values by 4. The weighting system that we've used can be adjusted by readers of this report, according to their own attitude to risk and how much they value different levels of protection. By changing the penalisation levels and the overall protection weighting, it's possible to apply your own individual rating system.

The Total Protection Rating is calculated by multiplying the number of Protected cases by four (the default maximum score), then applying any penalties. Finally, the total is multiplied by four (the weighting value for Protection Ratings) to create the Total Protection Rating.

Response Details

Attacker/APT Group	Number of Incidents	Detection	Delivery	Execution	Action	Privilege Escalation	Post-Escalation Action	Lateral Movement	Lateral Action	Protected	Penalties
Scattered Spider	18	18	16	2	0	0	0	0	0	18	2
APT29	18	18	16	2	0	0	0	0	0	18	2
Lapsus$	6	6	6	0	0	0	0	0	0	6	0
TOTAL	42	42	38	4	0	0	0	0	0	42	4

● This data shows how the product handled different stages of each APT group. The columns labelled 'Delivery' through to 'Lateral Action' show how many times an attacker succeeded in achieving those goals. A 'zero' result is ideal.

Protection Accuracy Rating Details

Attacker/ APT Group	Number of Incidents	Protected	Penalties	Protection Score	Protection Rating
Scattered Spider	18	18	2	71	284
APT29	18	18	2	59	236
Lapsus$	6	6	0	24	96
TOTAL	42	42	4	154	616

● Different levels of protection, and failure to protect, are used to calculate the Protection Rating.
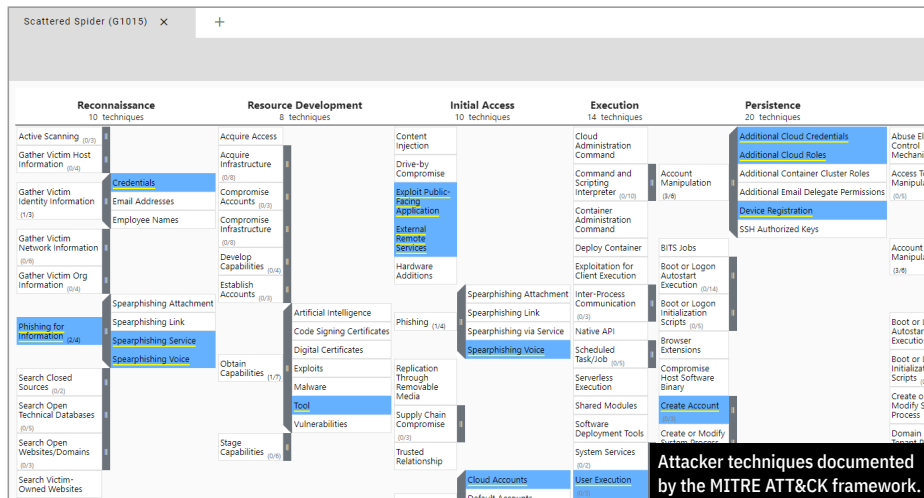
Protection Accuracy Ratings

Coro – EDR	616	99%

| 0 | 156 | 312 | 468 | 624 |

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

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/

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		Pass the Ticket		Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
	Steganography	Domain Groups		Web Session Cookie		Archive via Utility
External Remote Services	Malicious File	Internet Connection Discovery	Bypass User Account Control	Local Accounts	Remote Desktop Protocol	Remote Data Staging
	Internal Proxy	File and Directory Discovery				
	Mark-of-the-Web Bypass	Domain Trust Discovery		Domain Accounts		Remote Email Collection
	Multi-hop Proxy					

Lapsus$

Relying largely on social engineering to begin its attacks, Lapsus$ has operated since mid-2021. Its approach often needs destructive attacks to extort ransoms from victims, although without using ransomware.

Reference:
https://attack.mitre.org/groups/G1004/

Attacker techniques documented by the MITRE ATT&CK framework.
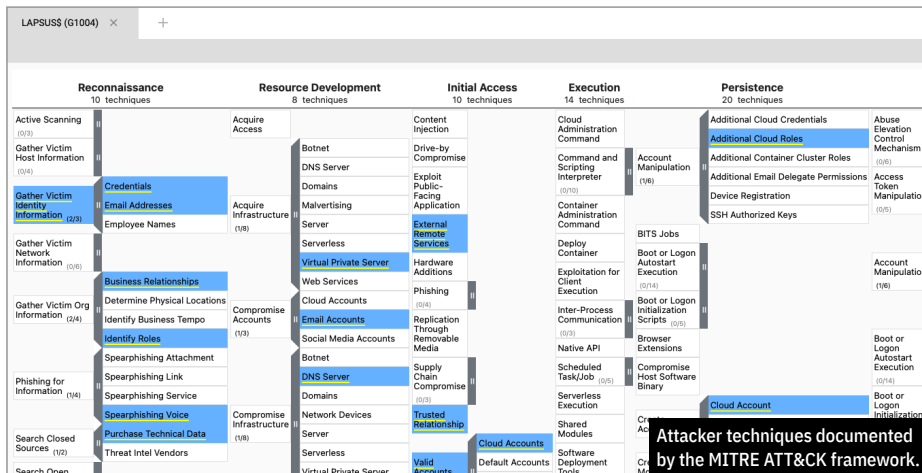
Example Lapsus$ Attack

Delivery	Execution	Action	Privilege Escalation	Post-Escalation	Lateral Movement	Lateral Action
Spear phishing Attachment	User Execution	File and Directory Discovery		Credentials from Web Browsers		Sharepoint
Trusted Relationship		Process Discovery		Password Managers		Data from Information Repositories
		Domain Groups		DCSync		Confluence
Proxy	Malicious File		Exploitation for Privilege Escalation	NTDS	External Remote Services	Chat Messages
		Domain Accounts		Cloud Accounts		Email Forwarding Rule
				Create Cloud Instance		Account Access Removal Data Destruction
				Delete Cloud Instance		Service Stop
				Additional Cloud Roles		

5. Legitimate Accuracy 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 Accuracy Rating

Coro – EDR	556 | 100%

0   139   278   417   556
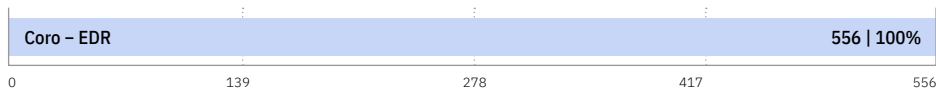
● **Legitimate Accuracy Ratings can indicate how well a vendor has tuned its detection engine.**

6. Conclusion

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

All of these attack types have been witnessed in real-world attacks over the previous few years. They are representative of a real and present threat to business networks the world over.

The threats used in this test are similar or identical to those used by the threat groups listed in **Attack Details** on page 8 and **4. Threat Intelligence** on pages 12 - 14. It was not tested against Linux-based rounds 7 and 13 because the product was not configured with a Linux sensor.

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

Coro – EDR provided excellent protection against attacks that are not just different from those used in last year's test, but from attacks typically deployed by a completely different set of threat groups. Despite the novelty of the threat groups, the product upped its Protection Accuracy Rating by a couple of percentage points, from last year's 94% to 99% in this test.

As we've said in previous reports, "it's more ideal to stop a threat early, rather than watch as it wreaks havoc before stopping it and trying to clean up." **Coro – EDR** behaved this way, stopping the vast majority of the threats as soon as it detected the delivery of the initial element of each attack.

In 38 out of 42 cases, threats were unable to move beyond the earliest stage of the attack chain, meaning that, as soon as the target systems were exposed to the threats, the attacks were detected immediately and were stopped from running. This prevented them from causing any damage, including data theft.

Coro – EDR only incurred half a penalty point each for the remaining four cases when it caught and stopped the attacks during the execution rather than the delivery stage. As can be seen from the row of 'zeros' thereafter in the **Response Details** on page 11, none of the attacks progressed after this point. So, the attacker/tester was unable to reconnoitre the target system nor gain remote control over it. Neither could they instigate an attack from the target system to other vulnerable systems in the network.

As in the previous **Coro – EDR** test, the product achieved a 100% Total Legitimacy Rating. Sometimes, in a bid to provide protection, products can be configured in such a way as to detect and block everything, including legitimate objects. **Coro – EDR** generated no sub-optimal errors and correctly handled all harmless, legitimate files.

Coro – EDR wins an AAA award for its near perfect performance.

Appendices

Appendix A: 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 B: 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 30th September and 14th October 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 C: Attack Details

Scattered Spider

Incident No.	Delivery	Execution	Action	Privilege Escalation	Post-Escalation	Lateral Movement	Lateral Action
1	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				
2	Spear phishing 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				
3	Spear phishing 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	Process Discovery		Kernel Modules and Extensions		System Shutdown/Reboot
		External Proxy	Local Account		BITS Jobs		Safe Mode Boot
		Non-Standard Port	Domain Groups		DCSync		Automatic Collection
		Indicator Removal From Tools	Domain Trust Discovery		Impair Command History Logging		Data from Local System
			Remote System Discovery		LSA Secrets		
			Group Policy Discovery				
4	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				

Incident No.	Delivery	Execution	Action	Privilege Escalation	Post-Escalation	Lateral Movement	Lateral Action
5	Spear phishing Attachment	Windows Command Shell	File and Directory Discovery	Access Token Manipulation	Portable Executable Injection	Windows Remote Management	Windows Remote Management
		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				Automatic Collection
		Compromise Software Supply Chain	Query Registry		External Remote Services		System Shutdown/Reboot
			Domain Account				Clipboard Data
			Internet Connection Discovery				Email Collection
			Domain Groups				Data from Local System
6	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		Modify Authentication Process		Automatic Collection
		External Proxy	Domain Account		Default Accounts		Account Access Removal
		Non-Standard Port	Internet Connection Discovery		Windows Management Instrumentation Event Subscription		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				
7	Spear phishing Link	Malicious Link	File and Directory Discovery		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
							Automatic Collection

● Incident number 7 is a Linux technique.

APT29

Incident No.	Delivery	Execution	Action	Privilege Escalation	Post-Escalation	Lateral Movement	Lateral Action
8	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					
9	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
	Spear phishing 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					
10	Spear phishing 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		
11	Spear phishing 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		Data from Local System
		Exploitation for Client Execution	System Information Discovery		External Remote Services		
		Windows Management Instrumentation	Domain Account		Timestomp		
12	Spear phishing 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		Deobfuscate/Decode Files or Information
					File Deletion		

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

● Incident number 13 is a Linux technique.

Lapsus$

Incident No.	Delivery	Execution	Action	Privilege Escalation	Post-Escalation	Lateral Movement	Lateral Action
14	Spear phishing Attachment	User Execution	File and Directory Discovery	Exploitation for Privilege Escalation	Credentials from Web Browsers	External Remote Services	Sharepoint
		Malicious File	Process Discovery		Password Managers		Data from Information Repositories
		Trusted Relationship	Domain Groups		DCSync		Confluence
					NTDS		Chat Messages
		Proxy	Domain Accounts		Cloud Accounts		Email Forwarding Rule
					Create Cloud Instance		Account Access Removal Data Destruction
					Delete Cloud Instance		Service Stop
					Additional Cloud Roles		
15	Spear phishing Link	User Execution	File and Directory Discovery	Exploitation for Privilege Escalation	Credentials from Web Browsers	External Remote Services	Sharepoint
		Malicious File	Process Discovery		Password Managers		Data from Information Repositories
		Trusted Relationship	Domain Groups		DCSync		Confluence
					NTDS		Chat Messages
		Proxy	Domain Accounts		Cloud Accounts		Email Forwarding Rule
					Create Cloud Instance		Account Access Removal Data Destruction
					Delete Cloud Instance		Service Stop
					Additional Cloud Roles		

Appendix D: Product Version

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)
Coro	EDR	**DC:** 2.5.65.1 (3.2) **PCs:** 2.5.65.1 (3.2)	**DC:** 2.5.65.1 (3.2) **PCs:** 2.5.65.1 (3.2)

SE LABS