SE Labs

INTELLIGENCE-LED TESTING

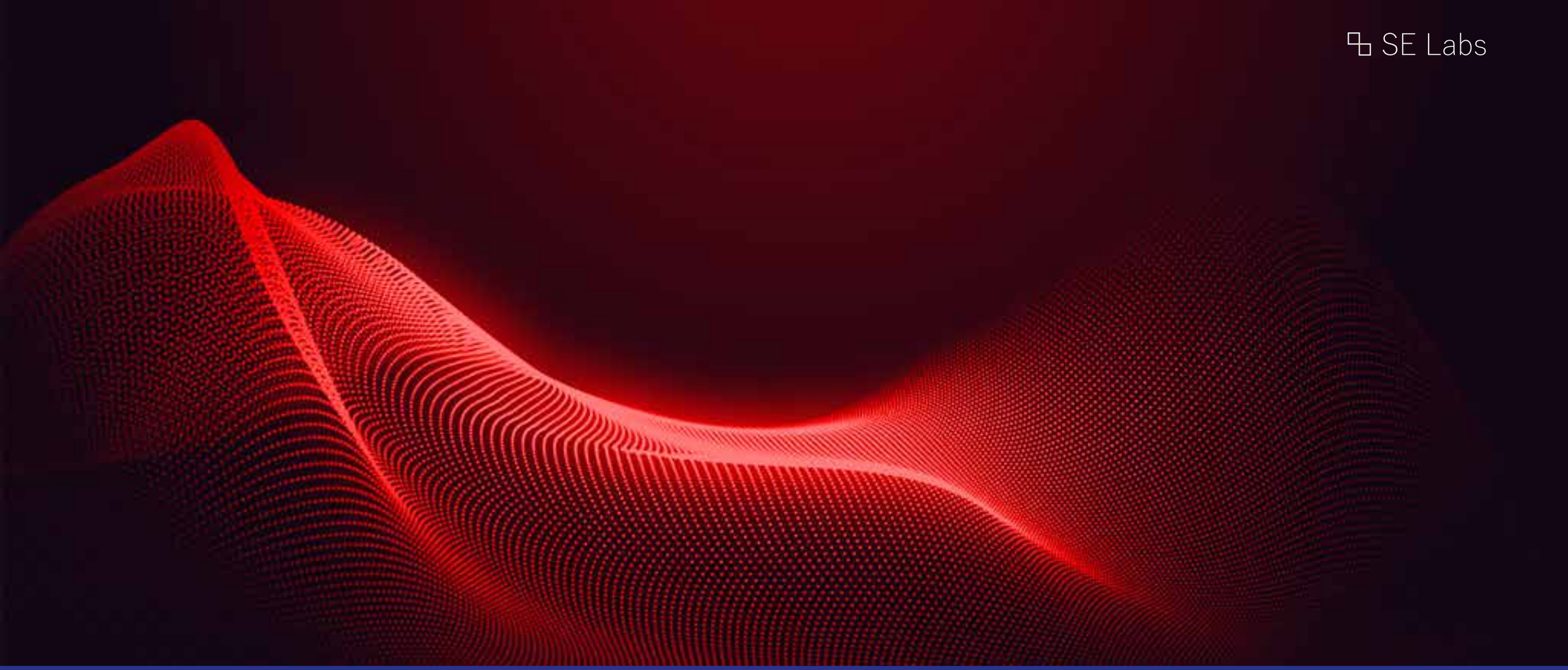
Enterprise Advanced Security

EDR DETECTION

Acronis

Cyber Protect Cloud with Advanced Security pack + EDR

May 2024



SE Labs ® tested **Acronis Cyber Protect Cloud with Advanced Security pack + EDR** against a range of hacking attacks designed to compromise systems and penetrate target networks in the same way as criminals and other attackers breach systems and networks.

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

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

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

Publication and Marketing
Colin Mackleworth
Sara Claridge
Janice Sheridan

IT Support
Danny King-Smith
Chris Short

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

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

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

© 2024 SE LABS LTD

Contents

Document version 1.0 Written 28th May 2024

Introduction

Endpoint Detection and Response is more than anti-virus

Understand cybersecurity testing with visible threat intelligence

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

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

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

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

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

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

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

Executive Summary

SE Labs tested **Acronis Cyber Protect Cloud With Advanced Security Pack + EDR** against targeted attacks based on Scattered Spider, ATP29 and Lapsus$.

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.

Acronis Cyber Protect Cloud With Advanced Security Pack + EDR scored an impressive 100% Detection Accuracy Rating for detecting every element of the attacks. It detected the delivery and initial executing of all the attacks, whether this be a spear phishing attachment or an attempt to exploit an Internet-facing application.

The product also detected all the subsequent malicious activities in the attack chain, tracking all of the hostile activities that occurred as the attacks progressed.

However, it misclassified several legitimate objects as malicious, bringing its Legitimate Accuracy Rating down to 77%.

Given its Total Accuracy Rating of 88%, the product can be described as very accurate and achieved an AA rating for enterprise advanced security.

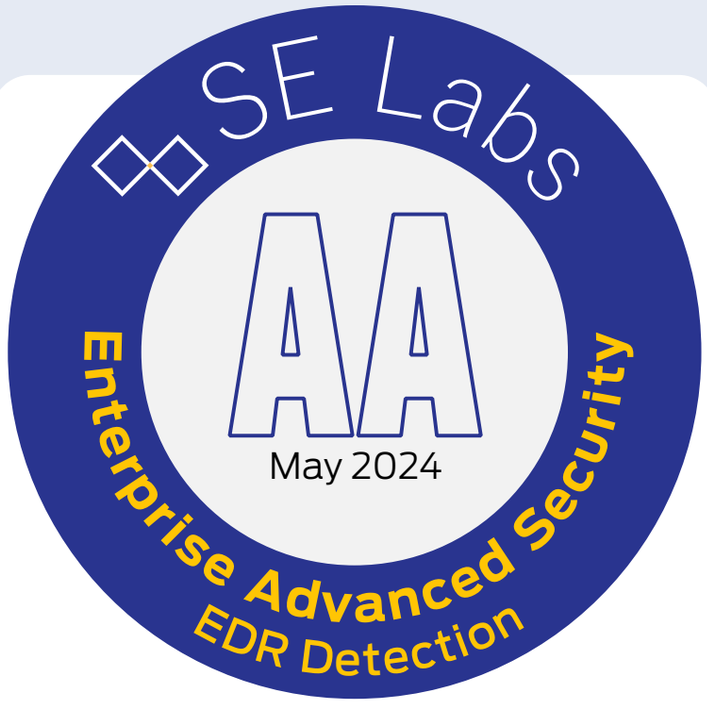
Executive Summary				
Product Tested	**Attacks Detected (%)**	**Detection Accuracy (%)**	**Legitimate Accuracy Rating (%)**	**Total Accuracy Rating (%)**
Acronis Cyber Protect Cloud with Advanced Security pack + EDR	100%	100%	77%	88%

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

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

Enterprise Advanced Security Award

The following product wins the SE Labs award:



Acronis
Cyber Protect Cloud with Advanced Security pack + EDR

1. How We Tested

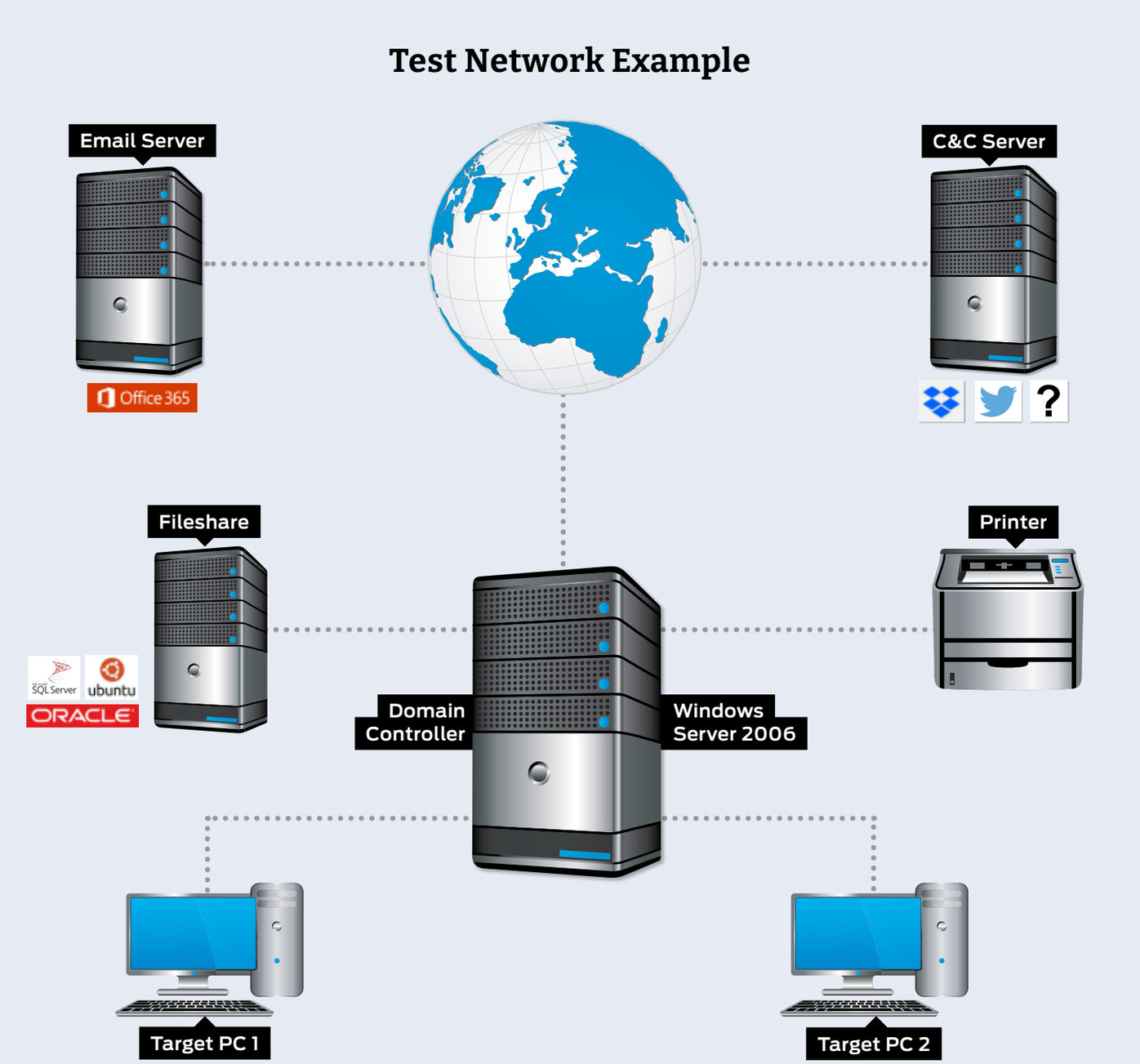
Testers can't assume that products will work a certain way, so running a realistic advanced security test means setting up real networks and hacking them in the same way that real adversaries behave.

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

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

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

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



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

Threat Responses

Full Attack Chain: Testing Every Layer of Detection and Protection

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

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

Attack Stages

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

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

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

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

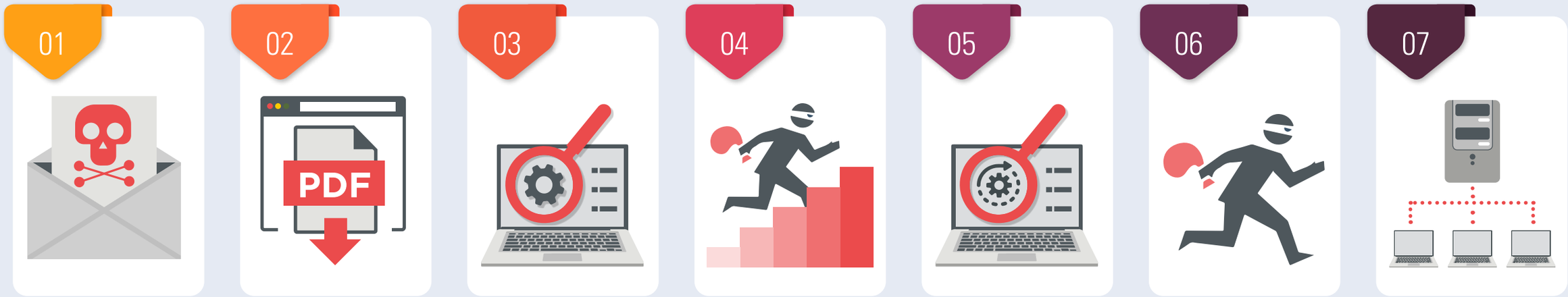


Figure 1. A typical attack starts with an initial contact and progresses through various stages, including reconnaissance, stealing data and causing damage.

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

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

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

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

Attack Chain: How Hackers Progress

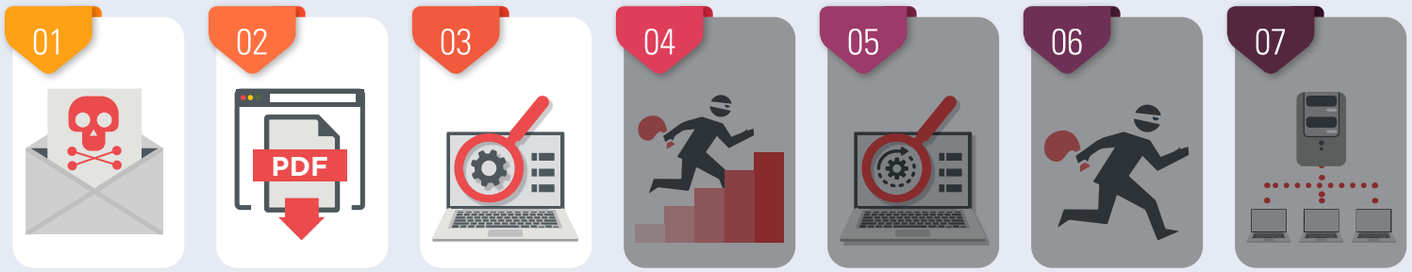


Figure 2. This attack was initially successful but only able to progress as far as the reconnaissance phase

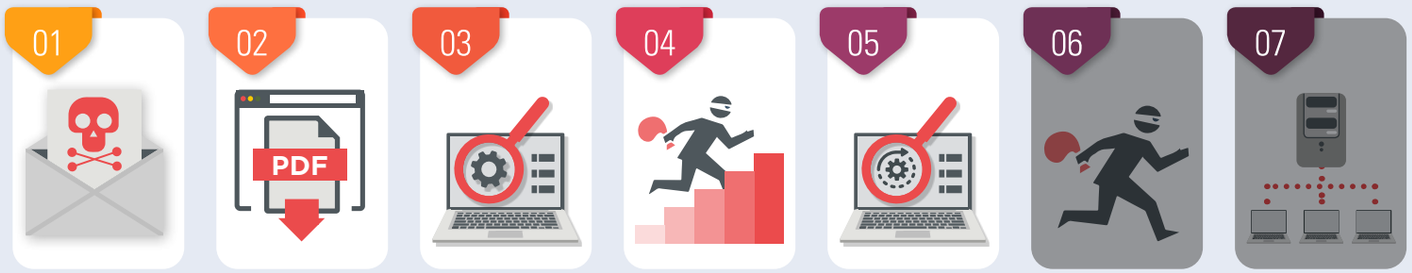


Figure 3. A more successful attack manages to steal passwords but wholesale data theft and destruction was blocked.

DE:CODED
Deciphering Cyber Security

Understand cybersecurity and other security issues. Practical and insightful, our experts have experience in attacking and defending in the physical and digital worlds.
Peek behind the curtain with the Cyber Security **DE:CODED** podcast.

Hackers vs. Targets

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

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

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

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

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

Attackers vs. Targets

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

Key

Aviation	Banking and ATMs	Defence	Energy	Education
Entertainment	Financial	Gambling	Government Espionage	Healthcare
Information Technology	Law	Manufacturing	Natural Resources	Private Sector Industries
Research Institutes	Telecommunication	Travel	US Retail, Restaurant and Hospitality	

2. Total Accuracy Ratings

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

If you look at the results tables in **Response Details** on page 12 you'll see that Delivery and Execution are grouped together into one chunk, while Action sits alone. Escalation and Post-Escalation (PE) Action are grouped, while Lateral Movement and Lateral Action are also grouped.

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

Total Accuracy Ratings			
Product	**Total Accuracy Rating**	**Total Accuracy (%)**	**Award**
Acronis Cyber Protect Cloud with Advanced Security pack + EDR	945.5	88%	**AA**

Total Accuracy Ratings combine protection and false positives.

Annual Report 2023

Our 4th Annual Report is now available

- Threat Intelligence Special
- Ransomware Focus
- Security Awards
- Advanced Email Testing

DOWNLOAD THE REPORT NOW!

(free – no registration)

selabs.uk/ar2023

3. Response Details

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

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

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

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

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

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

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

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

Understanding Detection Groups

First group | Second group | Third group | Fourth group

Dragonfly & Dragonfly 2.0

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

Response Details

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

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

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

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

Scattered Spider								
Incident No:	Detection	Delivery	Execution	Action	Escalation	PE Action	Lateral Movement	Lateral Action
1	✓	✓	✓	✓	✓	✓	—	✓
2	✓	✓	✓	✓	✓	✓	✓	✓
3	✓	✓	✓	✓	✓	✓	✓	✓
4	✓	✓	✓	✓	✓	✓	✓	✓
5	✓	✓	✓	✓	✓	✓	✓	✓
6	✓	✓	✓	✓	✓	✓	—	✓
7	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

APT29								
Incident No:	Detection	Delivery	Execution	Action	Escalation	PE Action	Lateral Movement	Lateral Action
8	✓	✓	✓	✓	✓	✓	✓	✓
9	✓	✓	✓	✓	✓	✓	—	✓
10	✓	✓	✓	✓	✓	✓	—	✓
11	✓	✓	✓	✓	✓	✓	—	✓
12	✓	✓	✓	✓	✓	✓	✓	✓
13	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

Lapsus$								
Incident No:	Detection	Delivery	Execution	Action	Escalation	PE Action	Lateral Movement	Lateral Action
14	✓	✓	✓	✓	✓	—	—	✓
15	✓	✓	✓	✓	✓	—	—	✓

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.

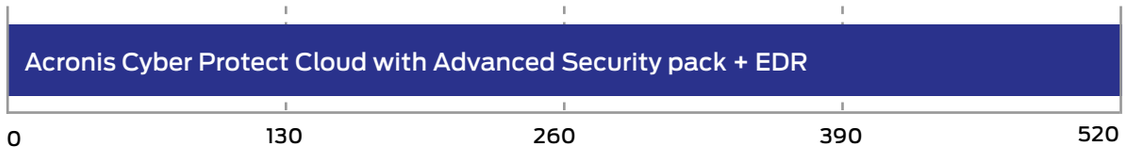
Response Details						
Attacker/ APT Group	Number of Incidents	Attacks Detected	Delivery/ Execution	Action	Privilege Escalation/ Action	Lateral Movement/ Action
Scattered Spider	6	6	6	6	6	6
APT29	5	5	5	5	5	5
Lapsus$	2	2	2	2	2	2
Total	**13**	**13**	**13**	**13**	**13**	**13**

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

Detection Accuracy Rating Details				
Attacker/ APT Group	Number of Incidents	Attacks Detected	Group Detections	Detection Rating
Scattered Spider	6	6	24	240
APT29	5	5	20	200
Lapsus$	2	2	8	80
Total	**13**	**13**	**52**	**520**

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

Detection Accuracy Ratings		
Product	Detection Accuracy Rating	Detection Accuracy Rating (%)
Acronis Cyber Protect Cloud with Advanced Security pack + EDR	520	100%



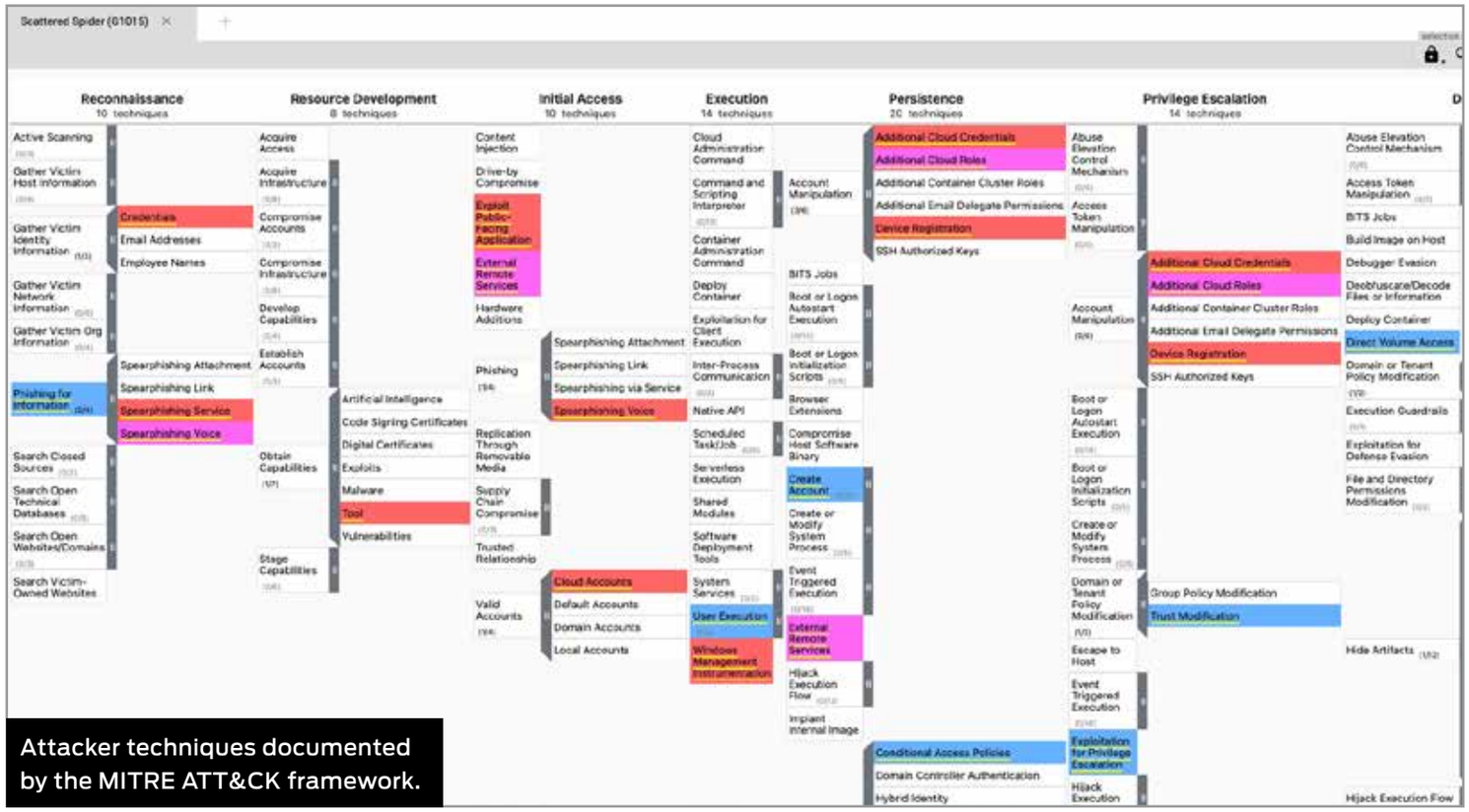
Detection Ratings are weighted to show that how products detect threats can be subtler than just 'win' or 'lose'.

4. Threat Intelligence

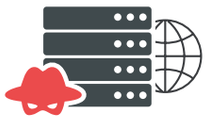
Scattered Spider

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/



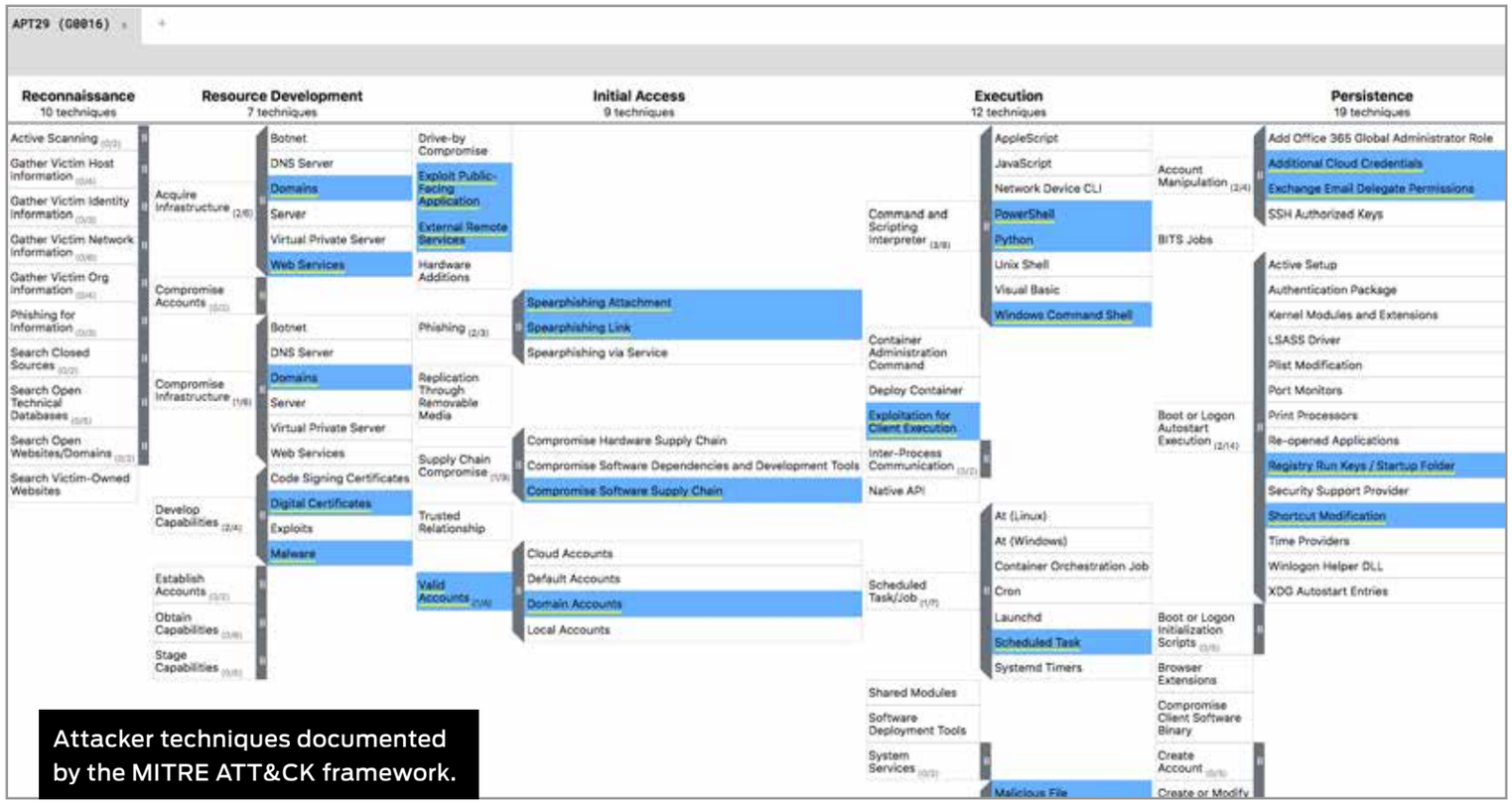
Attacker techniques documented by the MITRE ATT&CK framework.

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

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.

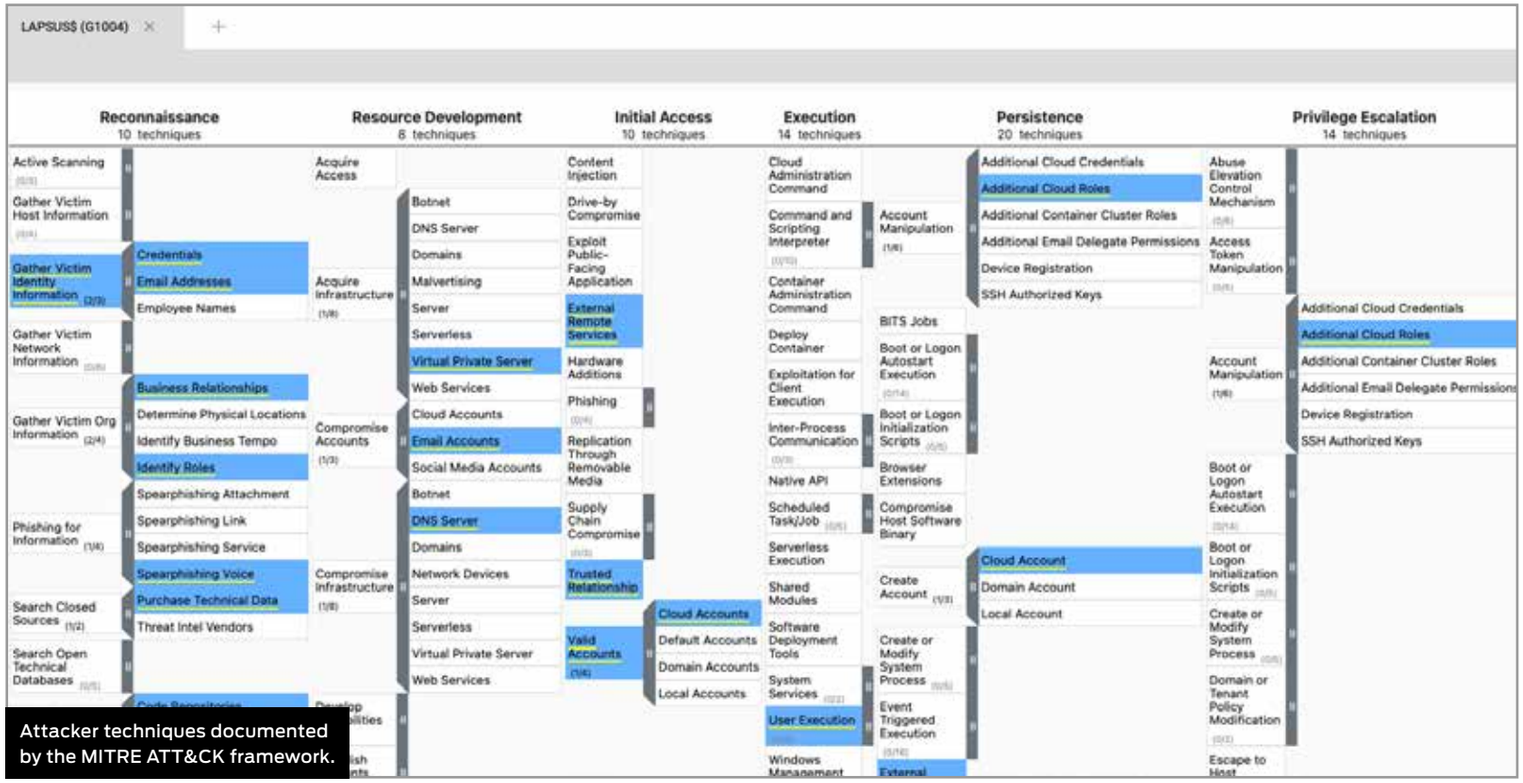
Example APT29 Attack

Delivery	Execution	Action	Privilege Escalation	Post-Escalation Action	Lateral Movement	Lateral Action
Spearphishing Attachment	Powershell	Cloud Account	Bypass User Account Control	Pass the Ticket	SMB/Windows Admin Shares	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
	Malicious File	Domain Account		Local Accounts		Archive via Utility
	Internal Proxy	Domain Groups		Disable Windows Event Logging		Code Repositories
	Bidirectional Communication	File and Directory Discovery		Disable or Modify Tools		Remote Data Staging
	Encrypted Channel	Domain Trust Discovery		DCSync		Remote Email Collection
				File Deletion		
 Spearphishing Attachment	 Malicious File	 Domain Groups	 Bypass User Account Control	 File Deletion	 SMB/Windows Admin Shares	 Remote Email Collection

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

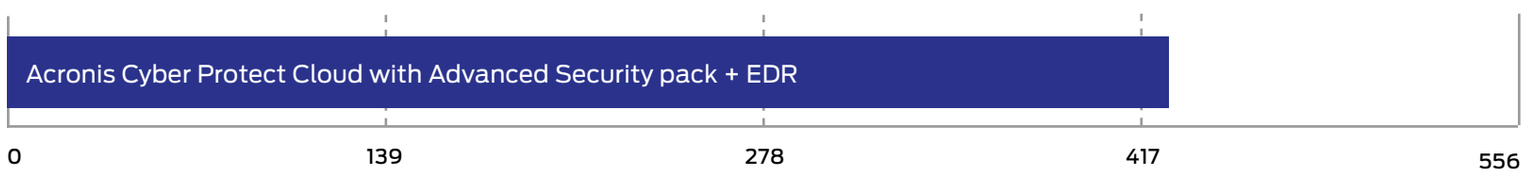
Delivery	Execution	Action	Privilege Escalation	Post-Escalation Action	Lateral Movement	Lateral Action
Spearphishing Link	User Execution	File and Directory Discovery	Exploitation for Privilege Escalation	Credentials from Web Browsers	External Remote Services	Sharepoint
Trusted Relationship	Malicious File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

5. Legitimate Software Rating

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

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

Legitimate Software Ratings		
Product	**Legitimate Accuracy Rating**	**Legitimate Accuracy (%)**
Acronis Cyber Protect Cloud with Advanced Security pack + EDR	425.5	77%



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

SE Labs
Monthly Newsletter
Don't miss our security articles and reports
- Test reports announced
- Blog posts reviewed
- Security testing analysed
- NEW: Podcast episodes

SUBSCRIBE NOW!

6. Conclusions

The test exposed **Acronis Cyber Protect Cloud with Advanced Security pack + 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 are similar or identical to those used by the threat groups listed in **Hackers vs. Targets** on page 9 and **4. Threat Intelligence** on pages 13-16. Scattered Spider and Lapsus$ are threat groups that have emerged fairly recently compared to APT29 which was first observed in 2008. However, APT29 has remained active since then and has been developing new attack techniques.

It is important to note that while the test used the same type 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 future performance rather than just a compliance check that the product can detect old attacks.

Acronis Cyber Protect Cloud with Advanced Security pack + EDR detected almost all of the threats on a basic level, in that for each attack it detected at least some element of the attack chain. It was not tested against Linux-based rounds 7 and 13 because the product was not configured with a Linux sensor.

The product detected all the other threats in depth, capturing details as each threat proceeded down the attack chain from the initial introduction to the system through to executing and subsequent behaviour by the attacker. This ability to detect every element of the attack chain was especially evident when the product was confronted with Scattered Spider-type threats that launched a wide variety of post-escalation actions. Its excellent performance earned it a 100% Detection Accuracy Rating.

Acronis Cyber Protect Cloud with Advanced Security pack + EDR did misclassify several legitimate objects as threats, bringing its Legitimate Accuracy Rating down to 77%. When a product wrongly detects legitimate software, it can hamper operations. Security operatives end up trading convenience for protection as they end up deciding what's malicious or benign.

Acronis claims to have fixed this issue with an update.

Given its Total Accuracy Rating of 88%, the product can be described as very accurate and achieved an AA rating for enterprise advanced security.

Enterprise Security Testing Services for CISOs

Elevate your cyber security strategy with SE Labs, the world's leading security testing organisation.

SE Labs works with large organisations to support CISOs and their security teams:

- Validate existing combination of security products and services.
- Provide expert partnership when choosing and deploying new security technologies.

SE Labs provides in-depth evaluations of the cyber security that you are considering, tailored to the exact, unique requirements of your business.

For an honest, objective and well-informed view of the cyber security industry contact us now at

selabs.uk/contact

Appendices

Appendix A: Terms Used

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

Appendix B: FAQs

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

- The test was conducted between 3rd and 4th April 2024.
- The product was configured according to its vendor's recommendations.
- Targeted attacks were selected and verified by SE Labs.
- Malicious and legitimate data was provided to partner organisations once the test was complete.

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

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

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

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

Appendix C: Product Versions

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

Product Versions			
Vendor	Product	Build Version (start)	Build Version (end)
Acronis	Cyber Protect Cloud with Advanced Security pack + EDR	23.12 37114	24.3.37587

SE Labs
INTELLIGENCE-LED TESTING

SE Labs helps advance the effectiveness of computer security through innovative, detailed and intelligence-led testing, run with integrity.

Enterprises
Reports for enterprise-level products supporting businesses when researching, buying and employing security solutions.
Download Now!

Small Businesses
Our product assessments help small businesses secure their assets without the purchasing budgets and manpower available to large corporations
Download Now!

Consumers
Download free reports on internet security products and find our how you can secure yourself online as effectively as a large company
Download Now!

selabs.uk

Appendix D: 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	Intial File Transfer
		Web Protocols	File and Directory Discovery		Disable or Modify System Firewall		Input Capture
		Windows Command Shell	Process Discovery		Scheduled Task/Job		Clipboard Data
			Query Registry		LSASS Memory		Email Collection
			Remote System Discovery		Cloud Infrastructure Discovery		Data from Local System
			Network Share Discovery		Cloud Service Discovery		Data from Cloud Storage Object
			Network Service Discovery		Sharepoint		Exfiltration to Cloud Storage
2	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		Data from Cloud Storage Object
		External Proxy	System Network Configuration Discovery		Cloud Service Discovery		Exfiltration to Cloud Storage
			System Network Connections Discovery		Cloud Storage Object Discovery		Account Access Removal
			Internet Connection Discovery		Browser Extensions		Data Encrypted for Impact
			Local Account		Hide Artifacts		System Shutdown/Reboot
3	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	Process Discovery		Cloud Accounts		System Shutdown/Reboot
		External Proxy	Local Account		Disable Cloud Logs		Safe Mode Boot
		Non-Standard Port	Domain Groups		Domain Trust Modification		Automatic Collection
		Indicator Removal From Tools	Domain Trust Discovery		Kernel Modules and Extensions		Data from Local System
			Remote System Discovery		BITS Jobs		Exfiltration to Cloud Storage
			Cloud Account		DCSync		Device Registration
			Group Policy Discovery		Impair Command History Logging		
					LSA Secrets		
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		Disable or Modify Tools		Clipboard Data
		Windows Command Shell	Process Discovery		Registry Run Keys / Startup Folder		Email Collection
		External Proxy	Remote System Discovery		Azure Account Creation		Data from Local System
		Non-Standard Port	Cloud Account		Match Legitimate Name or Location		Automatic Collection
		Compromise Software Supply Chain	Network Service Discovery		Rename System Utilities		Data from Cloud Storage Object
			Query Registry		Modify Authentication Process		Exfiltration to Cloud Storage
5	Spearphishing Attachment	Windows Command Shell	File and Directory Discovery	Access Token Manipulation	Create Cloud Instance	Windows Remote Management	Data from Cloud Storage Object
		External Proxy	System Information Discovery		Sharepoint	Initial File Transfer	Exfiltration to Cloud Storage
		Non-Standard Port	System Owner/User Discovery		Code Repositories		Data from Local System
		Indicator Removal From Tools	Network Share Discovery		Portable Executable Injection		Account Access Removal
		Trusted Relationship	Process Discovery		Rootkit		Data Encrypted for Impact
		Compromise Software Supply Chain	Query Registry		Web Session Cookie		Input Capture
			Domain Account		Cloud Instance Metadata API		Automatic Collection
			Internet Connection Discovery		Credentials In Files		System Shutdown/Reboot
			Domain Groups		External Remote Services		
			Cloud Account				
6	Exploit Public-Facing Application	Malicious File	File and Directory Discovery	Domain Trust Modification	Native API	Remote Access Software	Input Capture
		Web Protocols	System Information Discovery	Bypass User Account Control	Cloud Infrastructure Discovery	Protocol Tunneling	Clipboard Data
		Windows Command Shell	System Owner/User Discovery		Cloud Service Discovery		Automatic Collection
		External Proxy	Domain Account		Cloud Storage Object Discovery		Data from Cloud Storage Object
		Non-Standard Port	Internet Connection Discovery		Credentials from Password Stores		Exfiltration to Cloud Storage
		Indicator Removal From Tools	Domain Groups		Multi-Factor Authentication Interception		Account Access Removal
			Cloud Account		Multi-Factor Authentication Request Generation		Data Encrypted for Impact
			Process Discovery		Default Accounts		System Shutdown/Reboot
			Query Registry		Windows Management Instrumentation Event Subscription		Safe Mode Boot
			Permission Groups Discovery		Modify Authentication Process		
			Domain Trust Modification		Disable or Modify Tools		
					Registry Run Keys / Startup Folder		
					Azure Account Creation		
7	Spearphishing 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

APT29							
Incident No.	Delivery	Execution	Action	Privilege Escalation	Post-Escalation	Lateral Movement	Lateral Action
8	Exploit Public-Facing Application	Web Protocols	Cloud Account	Bypass User Account Control	Application Access Token	Cloud Services	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
	External Remote Services	Steganography	Domain Account	Additional Cloud Credentials	Pass the Ticket	Remote Desktop Protocol	Archive via Utility
		Malicious File	Domain Groups	Additional Cloud Roles	Web Session Cookie		Code Repositories
		Internal Proxy	Internet Connection Discovery		Cloud Accounts		Remote Data Staging
		Mark-of-the-Web Bypass	File and Directory Discovery		Local Accounts		Remote Email Collection
		Multi-hop Proxy	Domain Trust Discovery		Domain Accounts		
9	Trusted Relationship	Bidirectional Communication	File and Directory Discovery	Device Registration	Application Access Token	SMB/Windows Admin Shares	Deobfuscate/Decode Files or Information
	Spearphishing Attachment	Dynamic Resolution	Process Discovery	Bypass User Account Control	Domain Trust Modification		Archive via Utility
		Mshta	Remote System Discovery		Disable or Modify System Firewall		Code Repositories
		Software Packing	System Information Discovery		Disable or Modify Tools		Remote Data Staging
		Code Signing	Domain Trust Discovery		Disable Windows Event Logging		Remote Email Collection
		Windows Command Shell	Internet Connection Discovery		Accessibility Features		Data from Local System
		Malicious File	Cloud Account		Clear Mailbox Data		
10	Spearphishing Attachment	Encrypted Channel	File and Directory Discovery	Ingress Tool Transfer	File Deletion	Cloud Services	Archive via Utility
		Rundll32	Process Discovery	Exploitation for Privilege Escalation	Timestomp	Windows Remote Management	Code Repositories
		HTML Smuggling	Remote System Discovery		Masquerade Task or Service		Remote Data Staging
		Cloud API	System Information Discovery		Match Legitimate Name or Location		Remote Email Collection
		Visual Basic	Domain Trust Discovery		Hybrid Identity		Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
		Malicious File	Domain Groups		Windows Management Instrumentation Event Subscription		
11	Spearphishing via Service	Malicious File	File and Directory Discovery	Bypass User Account Control	Registry Run Keys / Startup Folder	Cloud Services	Deobfuscate/Decode Files or Information
	Compromise Software Supply Chain	Domain Fronting	Process Discovery		Disable or Modify System Firewall	Remote Desktop Protocol	Archive via Utility
		Python	Remote System Discovery		Scheduled Task		Code Repositories
		Cloud Administration Command	System Information Discovery		External Remote Services		Data from Local System
		Exploitation for Client Execution	Domain Account		Additional Email Delegate Permissions		
		Windows Management Instrumentation	Cloud Account		Device Registration		
					Timestomp		
12	Spearphishing Attachment	Powershell	Cloud Account	Bypass User Account Control	Pass the Ticket	SMB/Windows Admin Shares	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
		Malicious File	Domain Account		Local Accounts		Archive via Utility
		Internal Proxy	Domain Groups		Disable Windows Event Logging		Code Repositories
		Bidirectional Communication	File and Directory Discovery		Disable or Modify Tools		Remote Data Staging
		Encrypted Channel	Domain Trust Discovery		DCSync		Remote Email Collection
					File Deletion		
13	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		Code Repositories
		Internal Proxy	Process Discovery				Data from Local System
		Software Packing	System Information Discovery				
		Malicious Link					

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

Techniques in grey are either normally tested within test cases 7 and 13 or are cloud techniques. The product did not have coverage for cloud and Linux techniques, which is why these test cases and techniques were not covered or scored in this run.

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.