

Advanced Security Test Report

Cisco Secure Firewall 4225



ONLINE REPORT

SE LABS ® tested **Cisco Secure Firewall 4225** 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 and APT29 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

Introduction	04
Executive Summary	05
Advanced Security Test Award	05
1. How We Tested	06
Threat Responses	07
Attack Details	08
2. Total Accuracy Ratings	09
3. Response Details	10
4. Threat Intelligence	12
5. Legitimate Accuracy Rating	14
6. Conclusion	15
Appendices	16
Appendix A: Terms Used	16
Appendix B: FAQs	16
Appendix C: Attack Details	17
Appendix D: Product Version	19

Document version 1.0 Written 14th February 2025



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 Johnny
Erica Marotta
Jeremiah Morgan
Julian Owusu-Abrokwa
Joseph Pike
Georgios Sakatzidi
Eneđa Torba
Dimitrios Tsarouchas
Stephen Withey

Marketing

Sara Claridge
Janice Sheridan

Publication

Rahat Hussain
Colin Mackleworth

IT Support

Danny King-Smith
Chris Short

Website [selabs.uk](https://www.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 : 2022 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.

© 2025 SE Labs Ltd

Introduction



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](#).

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 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 Advanced Security test in Detection mode. For 'stoppers' like **Cisco Secure Firewall 4225** we can demonstrate effectiveness by testing in Protection Mode.

In this report we look at how **Cisco Secure Firewall 4225** 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' Advanced Security test reports help you assess which are the best for your own organisation.

Executive Summary

Cisco Secure Firewall 4225 was tested against a range of hacking attacks designed to compromise systems and penetrate target networks in the same way 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.

Cisco Secure Firewall 4225 posted excellent results, detecting and protecting against all of the threats. However, the product blocked a few legitimate software from running when it misclassified them as either as malicious or unknown. This did not significantly affect the product's overall performance as it posted an impressive Total Accuracy Rating of 95%, thus achieving an AAA award.

Executive Summary

Product Tested	Protection Accuracy Rating (%)	Legitimate Accuracy Rating (%)	Total Accuracy Rating (%)
Cisco Secure Firewall 4225	100%	91%	95%

- 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.

Advanced Security Test Award

The following product wins the SE Labs award:



Cisco
Secure Firewall 4225

1. How We Tested

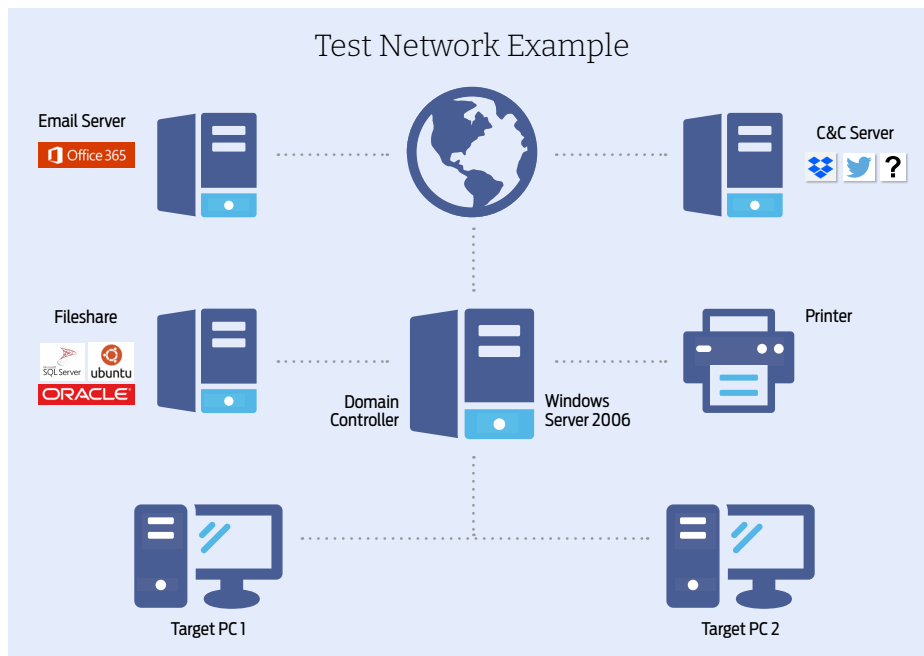
Testers can't assume that products will work a certain way, so running a realistic advanced security test means setting up real networks and hacking them in the same way that real adversaries behave.

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 12-13 and **Appendix C: Attack Details** on pages 17-18.

- 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 attacks

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.

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

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 12-13.

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.

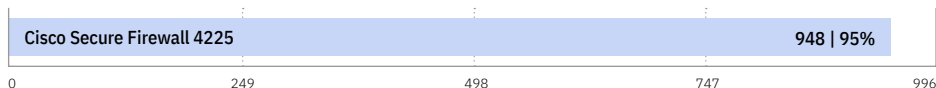
Not all protections, or detections for that matter, are equal. A product might completely block a URL, which stops the threat before it can even start its intended series of malicious events. Alternatively, the product might allow a web-based exploit to execute but prevent it from downloading any further 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



- Total Accuracy Ratings combine protection and false positives.

SE LABS PRESENTS THE - C2

TUESDAY 25TH AND
WEDNESDAY 26TH MARCH 2025

Connecting business with cyber security

The-C2 is an exclusive, invite-only threat intelligence event that connects multinational business executives with the cutting edge of the cyber security industry. The event enables frank and open discussion of the developing digital threat landscape among global security leaders.

The-C2 is hosted by SE Labs, the world's leading security testing lab. Its unique position in the industry provides a route to understanding both the developing threat landscape and the evolving security measures for defending against attackers.

REGISTER AT
THE - C2 . COM

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.

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	Lateral Movement	Lateral Action	Protected	Penalties
APT29	5	5	5	0	0	0	0	5	0
Scattered Spider	6	6	6	0	0	0	0	6	0
TOTAL	11	11	11	0	0	0	0	11	0

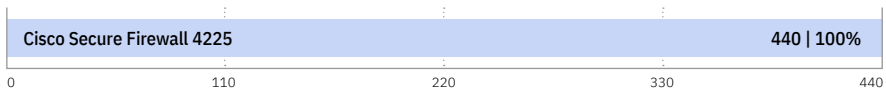
- This data shows how the product handled different stages of each APT group. The columns labelled 'Delivery' through to 'Lateral Action' show how many times an attacker succeeded in achieving those goals. A 'zero' result is ideal.

Protection Accuracy Rating Details

Attacker/ APT Group	Number of Incidents	Protected	Penalties	Protection Score	Protection Rating
APT29	5	5	0	20	200
Scattered Spider	6	6	0	24	240
TOTAL	11	11	0	44	440

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

Protection Accuracy Ratings



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

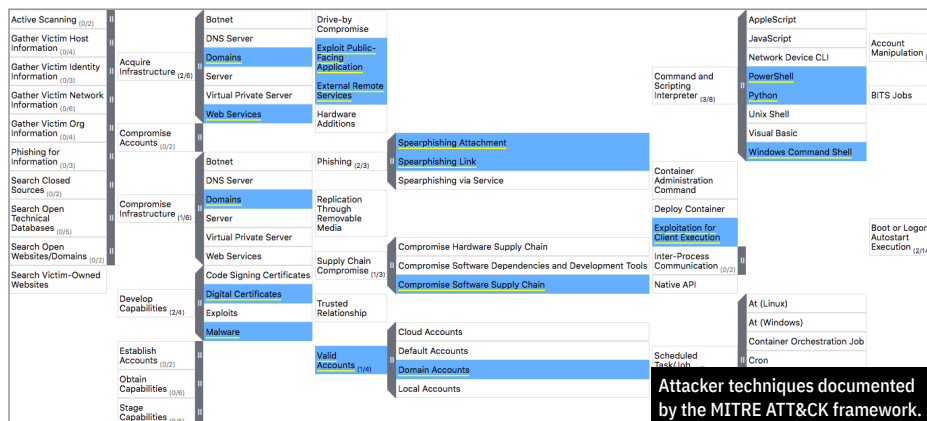
4. Threat Intelligence

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/>



Example APT29 Attack

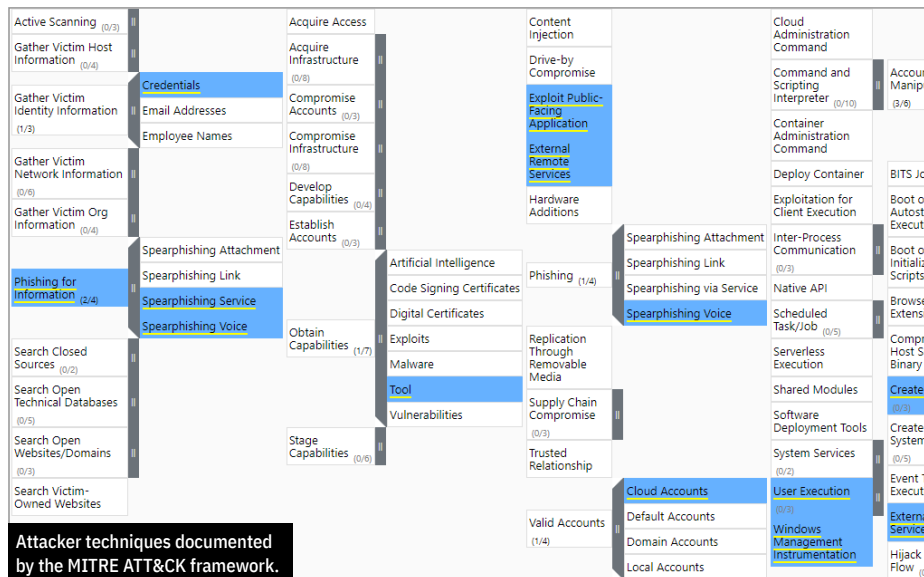
Delivery	Execution	Action	Lateral Movement	Lateral Action
T1190 Exploit Public-Facing Application	T1071.001 Web Protocols	T1087.002 Domain Account	T1021.001 Remote Desktop Protocol	T1048.002 Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
T1133 External Remote Services	T1090.001 Internal Proxy	T1069.002 Domain Groups	T1021.007 Cloud Services	T1213.003 Code Repositories T1140 Deobfuscate/Decode Files or Information
	T1568 Dynamic Resolution	T1057 Process Discovery	T1021.002 SMB/Windows Admin Shares	
	T1082 System Information Discovery	T1482 Domain Trust Discovery	T1021.001 Remote Desktop Protocol	
	T1016 System Network Configuration Discovery	T1016.001 Internet Connection Discovery		
	T1018 Remote System Discovery	T1083 File and Directory Discovery		
T1482 Domain Trust Discovery				
		T1550.003 Pass the Ticket		

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/>



Example Scattered Spider Attack

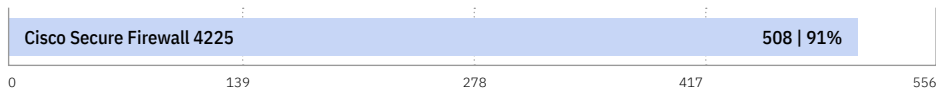
Delivery	Execution	Action	Lateral Movement	Lateral Action
T1190 Exploit Public-Facing Application	T1082 System Information Discovery	T1083 File and Directory Discovery	T1021.001 Remote Desktop Protocol	T1056 Input Capture
	T1016 System Network Configuration Discovery	T1033 System Owner/User Discovery	T1133 External Remote Services	T1114 Email Collection
	T1018 Remote System Discovery	T1082 System Information Discovery		T1005 Data from Local System
	T1071.001 Web Protocols			
	T1090.002 External Proxy			
T1571 Non-Standard Port				

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



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

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

6. Conclusion

This test exposed **Cisco Secure Firewall 4225** 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 on **page 8** and **4. Threat Intelligence** on pages 12 – 13.

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.

Cisco Secure Firewall 4225 provided excellent protection against attacks, as evidenced by its 100% Total Protection Accuracy Rating. It detected all five of the attacks based on APT29 type threats, and all six of those based on Scattered Spider.

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." The advantages of **Cisco Secure Firewall 4225's** early detection and prompt response can be seen in the **Response Details** on page 11. It shows that there were no malicious activities right after the testers/attackers introduced exploits and external remote services.

In all the cases, threats were unable to move beyond the earliest stage of the attack chain. The product detected the attacks as soon as the target systems were exposed to the threats and stopped them from running. The testers/attackers were unable to probe the target systems for vulnerabilities, much less gain external control over them. Further damage, including data theft,

was thus prevented. Moreover, the target system could not be used as a launch pad to attack other vulnerable systems in the network.

Cisco Secure Firewall 4225 did incur a few penalties for its treatment of legitimate applications. While it did not hamper access to all the non-malicious websites tested, it blocked one legitimate application that it had misclassified as malicious. Three other legitimate applications were "unknown" to the firewall which then erred on the side of caution by blocking them.

Despite this, **Cisco Secure Firewall 4225** posted excellent results and achieved a Total Accuracy Rating of 95%, making it deserving of its AAA award.

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 11th December and 18th December 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

APT29

Incident No.	Delivery	Execution	Action	Lateral Movement	Lateral Action
1	T1190 Exploit Public-Facing Application	T1071.001 Web Protocols	T1087.002 Domain Account	T1021.001 Remote Desktop Protocol	T1048.002 Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
	T1133 External Remote Services	T1090.001 Internal Proxy	T1069.002 Domain Groups	T1021.007 Cloud Services	T1213.003 Code Repositories
		T1568 Dynamic Resolution	T1057 Process Discovery	T1021.002 SMB/Windows Admin Shares	T1140 Deobfuscate/Decode Files or Information
		T1082 System Information Discovery	T1482 Domain Trust Discovery	T1021.001 Remote Desktop Protocol	
		T1016 System Network Configuration Discovery	T1016.001 Internet Connection Discovery		
		T1018 Remote System Discovery	T1083 File and Directory Discovery		
T1482 Domain Trust Discovery					
T1550.003 Pass the Ticket					
2	T1018 Remote System Discovery	T1007 System Service Discovery	T1016.001 Internet Connection Discovery	T1021.002 SMB/Windows Admin Shares	T1213.003 Code Repositories
	T1133 External Remote Services	T1059.003 Windows Command Shell	T1083 File and Directory Discovery	T1021.001 Remote Desktop Protocol	T1114.002 Remote Email Collection
		T1090.004 Domain Fronting	T1482 Domain Trust Discovery		T1005 Data from Local System
		T1049 System Network Connections Discovery	T1550.003 Pass the Ticket		
		T1573 Encrypted Channel			
T1018 Remote System Discovery	T1199 Trusted Relationship	T1057 Process Discovery	T1021.001 Remote Desktop Protocol	T1074.002 Remote Data Staging	
3	T1566.001 Spear phishing Attachment	T1595 Active Scanning	T1016.001 Internet Connection Discovery	T1021.007 Cloud Services	T1005 Data from Local System
		T1082 System Information Discovery		T1021.006 Windows Remote Management	T1140 Deobfuscate/Decode Files or Information
		T1133 External Remote Services			
		T1090.002 External Proxy			Domain groups
		T1573 Encrypted Channel			T1482 Domain Trust Discovery
		T1571 Non-Standard Port			
		T102.002 Bidirectional Communication			T1482 Domain Trust Discovery
T1573 Encrypted Channel	T1057 Process Discovery	T1219 Remote Access Software	T1529 System Shutdown/Reboot		
T1016 System Network Configuration Discovery	T1083 File and Directory Discovery		T1562 Safe Mode Boot		
T1595 Active Scanning	Pass the ticket				
T1018 Remote System Discovery					
4	T1566.002 Spear phishing Link	T102.002 Bidirectional Communication	T1482 Domain Trust Discovery	T1021.006 Windows Remote Management	T1531 Account Access Removal
	T1566.003 Spear phishing via Service	T1573 Encrypted Channel	T1057 Process Discovery	T1219 Remote Access Software	T1529 System Shutdown/Reboot
	T1204.001 Malicious Link	T1016 System Network Configuration Discovery	T1083 File and Directory Discovery		
		T1595 Active Scanning	Pass the ticket		
T1018 Remote System Discovery					
5	T1195.002 Compromise Software Supply Chain	T1573 Encrypted Channel	T1016.001 Internet Connection Discovery	T1021.006 Windows Remote Management	T1114.002 Remote Email Collection
	T1566.001 Spear phishing Attachment	T1102.002 Bidirectional Communication	T1057 Process Discovery	T1021.002 SMB/Windows Admin Shares	T1140 Deobfuscate/Decode Files or Information
		T1090.003 Multi-hop Proxy	T1069.002 Domain Groups		T1005 Data from Local System
	T1133 External Remote Services	T1049 System Network Connections Discovery	T1482 Domain Trust Discovery		T1560.001 Archive via Utility
		T1007 System Service Discovery			T1048.002 Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
		T1595 Active Scanning			

Scattered Spider

Incident No.	Delivery	Execution	Action	Lateral Movement	Lateral Action
6	T1190 Exploit Public-Facing Application	T1082 System Information Discovery	T1083 File and Directory Discovery	T1021.001 Remote Desktop Protocol	T1056 Input Capture
		T1016 System Network Configuration Discovery	T1033 System Owner/User Discovery	T1133 External Remote Services	T1114 Email Collection
		T1018 Remote System Discovery	T1082 System Information Discovery		T1005 Data from Local System
		T1071.001 Web Protocols			
		T1090.002 External Proxy			
	T1571 Non-Standard Port				
7	T1566.001 Spear phishing Attachment	T1049 System Network Connections Discovery	T1069.002 Domain Groups	T1021.002 SMB/Windows Admin Shares	T1213.003 Code Repositories
		T1007 System Service Discovery	T1087.002 Domain Account	T1021.001 Remote Desktop Protocol	T1114.002 Remote Email Collection
		T1595 Active Scanning	T1046 Network Service Discovery		T1005 Data from Local System
		T1059.003 Windows Command Shell	T1018 Remote System Discovery		
		T1199 Trusted Relationship			
	T1018 Remote System Discovery	T1033 System Owner/User Discovery	T1021.001 Remote Desktop Protocol	T1074.002 Remote Data Staging	
8	T1566.002 Spear phishing Link	T1016 System Network Configuration Discovery	T1016.001 Internet Connection Discovery	T1021.007 Cloud Services	T1005 Data from Local System
		T1090.002 External Proxy	T1087.001 Local Account	T1021.006 Windows Remote Management	T1140 Deobfuscate/Decode Files or Information
		T1571 Non-Standard Port			
		T1204.001 Malicious Link			
			T1082 System Information Discovery	T1083 File and Directory Discovery	T1021.001 Remote Desktop Protocol
9	T1566.001 Spear phishing Attachment	T1046 Network Service Discovery	T1012 Query Registry	T1021.002 SMB/Windows Admin Shares	T1119 Automatic Collection
		T1069 Permission Groups Discovery	T1482 Domain Trust Discovery	T1133 External Remote Services	T1567.002 Exfiltration to Cloud Storage
		T1071.001 Web Protocols			
		T1133 External Remote Services			
		T1090.002 External Proxy			
		T1199 Trusted Relationship			
	T1016 System Network Configuration Discovery	T1069.002 Domain Groups	T1021.006 Windows Remote Management	T1531 Account Access Removal	
10	T1566.001 Spear phishing Attachment	T1082 System Information Discovery	T1087.002 Domain Account	T1219 Remote Access Software	T1529 System Shutdown/Reboot
		T1595 Active Scanning	T1135 Network Share Discovery		T1562 Safe Mode Boot
		T1204.001 Malicious Link	T1069 Permission Groups Discovery		
		T1102.002 Bidirectional Communication			
		T1573 Encrypted Channel			
	T1007 System Service Discovery	T1083 File and Directory Discovery	T1021.001 Remote Desktop Protocol	T1119 Automatic Collection	
11	T1566.003 Spear phishing via Service	T1016 System Network Configuration Discovery	T1057 Process Discovery	T1133 External Remote Services	T1005 Data from Local System
		T1082 System Information Discovery	T1615 Group Policy Discovery		T1056 Input Capture
		T1059.003 Windows Command Shell			
		T1090.002 External Proxy			
		T1573 Encrypted Channel			

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)
Cisco	Secure Firewall 4225	7.6.0 (build 113)	7.6.0 (build 113)

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.