SE Labs

INTELLIGENCE-LED TESTING

Enterprise Advanced Security

Palo Alto Networks

VM-Series Virtual Firewall

NGFW DETECTION

May 2023

SE Labs tested **Palo Alto Networks VM-Series Virtual Next-Generation Firewalls** 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
Gia Gorbold
Anila Johny
Erica Marotta
Luca Menegazzo
Jeremiah Morgan
Julian Owusu-Abrokwa
Joseph Pike
Georgios Sakatzidi
Dimitrios Tsarouchas
Stephen Withey

Marketing
Sara Claridge
Janice Sheridan

Publication
Colin Mackleworth

IT Support
Danny King-Smith
Chris Short

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

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

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

Contents

Document version 1.0 Written 16th May 2023

Introduction

Detecting the Full Chain of Network Threats

Network security products detect threats at different security layers

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 detect and 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.

The Enterprise Advanced Security test assesses every security layer that products provide. In this report we look at how **Palo Alto Networks VM-Series Virtual Next-Generation Firewalls** handled full breach attempts. At which stages did it detect the threats as they attacked and moved through the network? 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.

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**.

Executive Summary

Palo Alto Networks VM-Series virtual firewall 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.

In this stand-alone test, we examined its abilities to:

- **Detect the delivery of targeted attacks**
- **Track different elements of the attack chain . . .**
- **...Including compromised beyond the endpoint and into the wider network**
- **Handle legitimate applications and other objects**

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

Palo Alto Networks VM-Series virtual firewall detected every targeted attack and tracked all the hostile activities that occurred during the attacks. Detection was wide, tracking malicious behaviour from the beginning to the end of the attack. In every case, the firewall also detected attackers moving from one target to another.

The product also takes prompt action against the execution and escalation of malicious attacks.

It only blocked a single legitimate object as malicious, so that it still achieved a high legitimate accuracy rating of 97%.

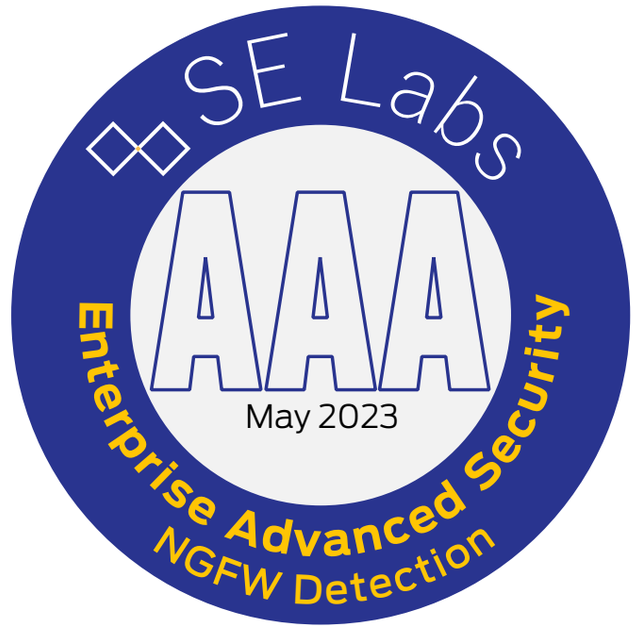
Executive Summary				
Product Tested	Attacks Detected (%)	Detection Accuracy (%)	Legitimate Accuracy Rating (%)	Total Accuracy Rating (%)
Palo Alto Networks VM-Series Virtual Firewall	100%	100%	97%	98%

Products highlighted in green were the most accurate, scoring 85 per cent or more for Total Accuracy. Those in yellow scored less than 85 but 75 or more. Products shown in red scored less than 75 per cent.

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

Next-Generation Firewall Detection Award

The following product wins the SE Labs award:



Palo Alto Networks
VM-Series Virtual
Next-Generation Firewall

1. How We Tested

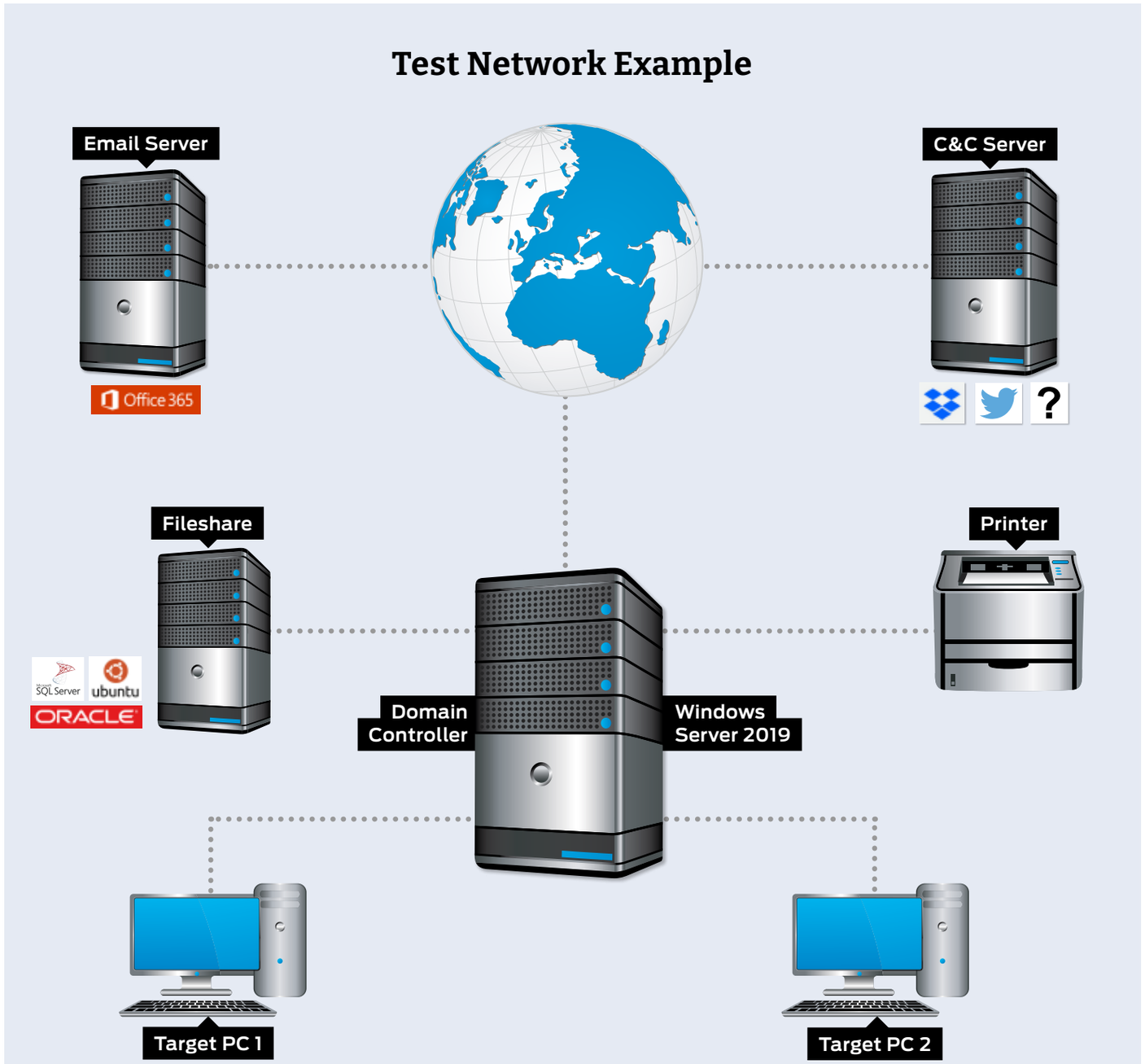
Testers can't assume that products will work a certain way, so running a realistic advanced security test means setting up real networks and hacking them in the same way that real adversaries behave.

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 to 16 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 contains them in a 'quarantine' or other safe holding mechanism for later analysis.

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

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

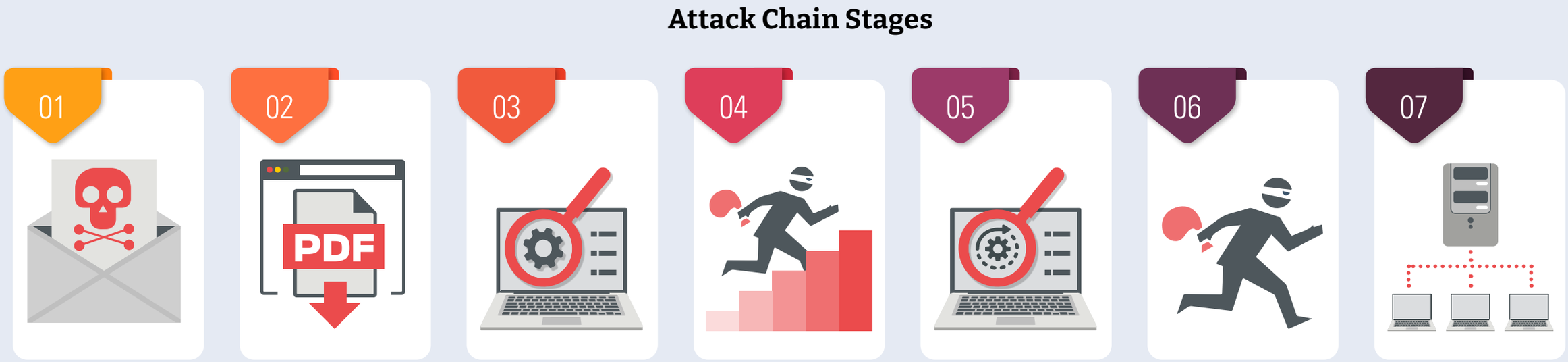


Figure 1. A typical attack starts with an initial contact and progresses through various stages, including reconnaissance, stealing data and causing damage.

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

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

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

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

Attack Chain: How Hackers Progress

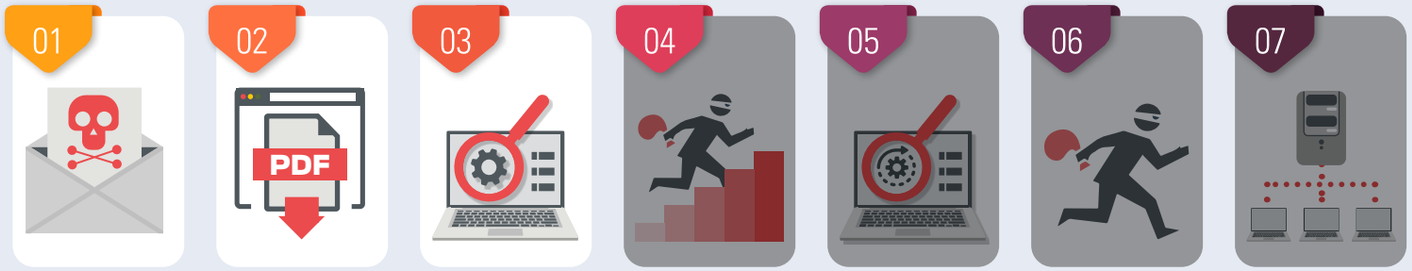


Figure 2. This attack was initially successful but only able to progress as far as the reconnaissance phase

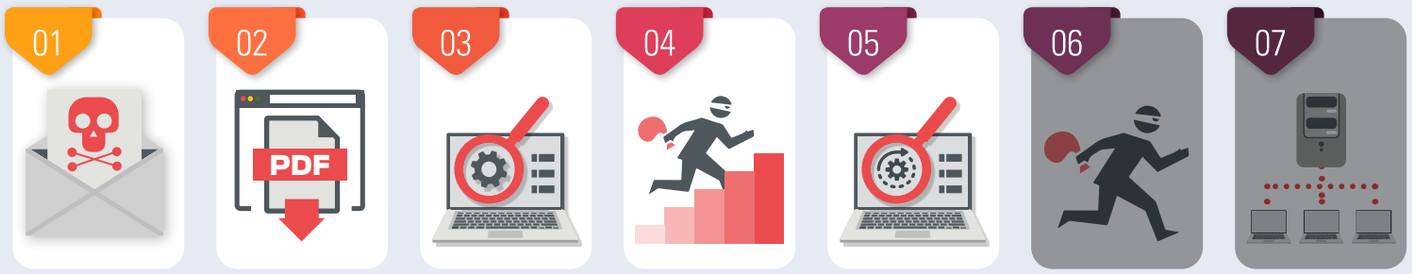


Figure 3. A more successful attack manages to steal passwords but wholesale data theft and destruction was blocked

Hackers vs. Targets

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

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

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

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

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

Hackers vs. Targets

Attacker/APT Group	Method	Target	Details
Wizard Spider			Credential harvesting, cryptomining and implementation of ransomware.
Sandworm			Obtain sensitive network data via encryption and system data wiping.
Dragonfly & Dragonfly 2.0			Phishing and supply chain methods used to gain access.

Key

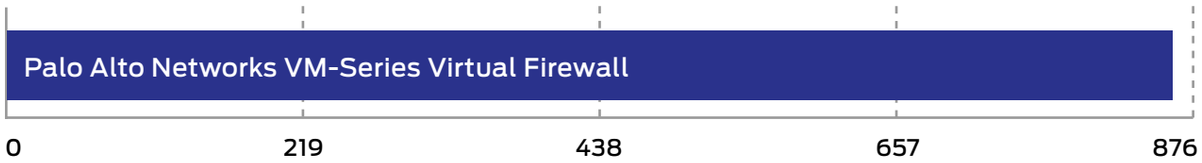
2. Total Accuracy Ratings

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

If you look at the results table in **3. Response Details** on page 11 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
Palo Alto Networks VM-Series Virtual Firewall	861	98%	AAA



Total Accuracy Ratings combine protection and false positives.

3. Response Details

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

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

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

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

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

Lateral movement/ action (+10)
The attacker may attempt to use the target as a launching system to other vulnerable systems.

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

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

Dragonfly & Dragonfly 2.0								
Incident No:	Detection	Delivery	Execution	Action	Escalation	PE Action	Lateral Movement	Lateral Action
9	✓	✓	✓	N/A	N/A	✓	✓	N/A
10	✓	✓	N/A	N/A	N/A	✓	✓	N/A
11	✓	✓	N/A	N/A	N/A	✓	✓	N/A
12	✓	✓	N/A	N/A	N/A	✓	✓	N/A

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.

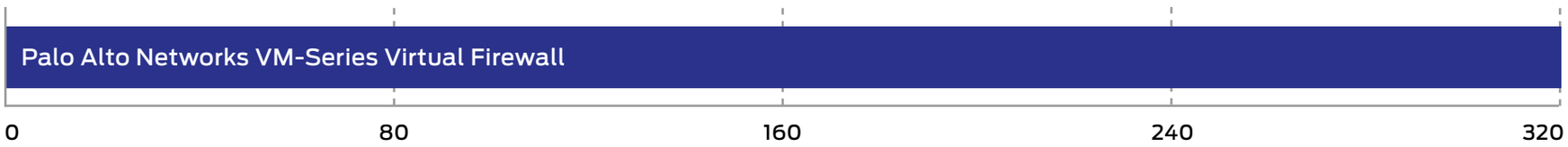
Response Details						
Attacker/APT Group	Number of Test Cases	Attacks Detected	Delivery/ Execution	Action	Privilege Escalation/Action	Lateral Movement/Action
Wizard Spider	4	4	4	N/A	2	4
Sandworm	4	4	4	N/A	2	4
Dragonfly & Dragonfly 2.0	4	4	4	N/A	4	4
Total	**12**	**12**	**12**	**N/A**	**8**	**12**

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

Detection Accuracy Rating Details				
Attacker/APT Group	Number of Test Cases	Attacks Detected	Group Detections	Detection Rating
Wizard Spider	4	4	10	100
Sandworm	4	4	10	100
Dragonfly & Dragonfly 2.0	4	4	12	120
Total	**12**	**12**	**32**	**320**

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 %
Palo Alto Networks VM-Series Virtual Firewall	320	100%



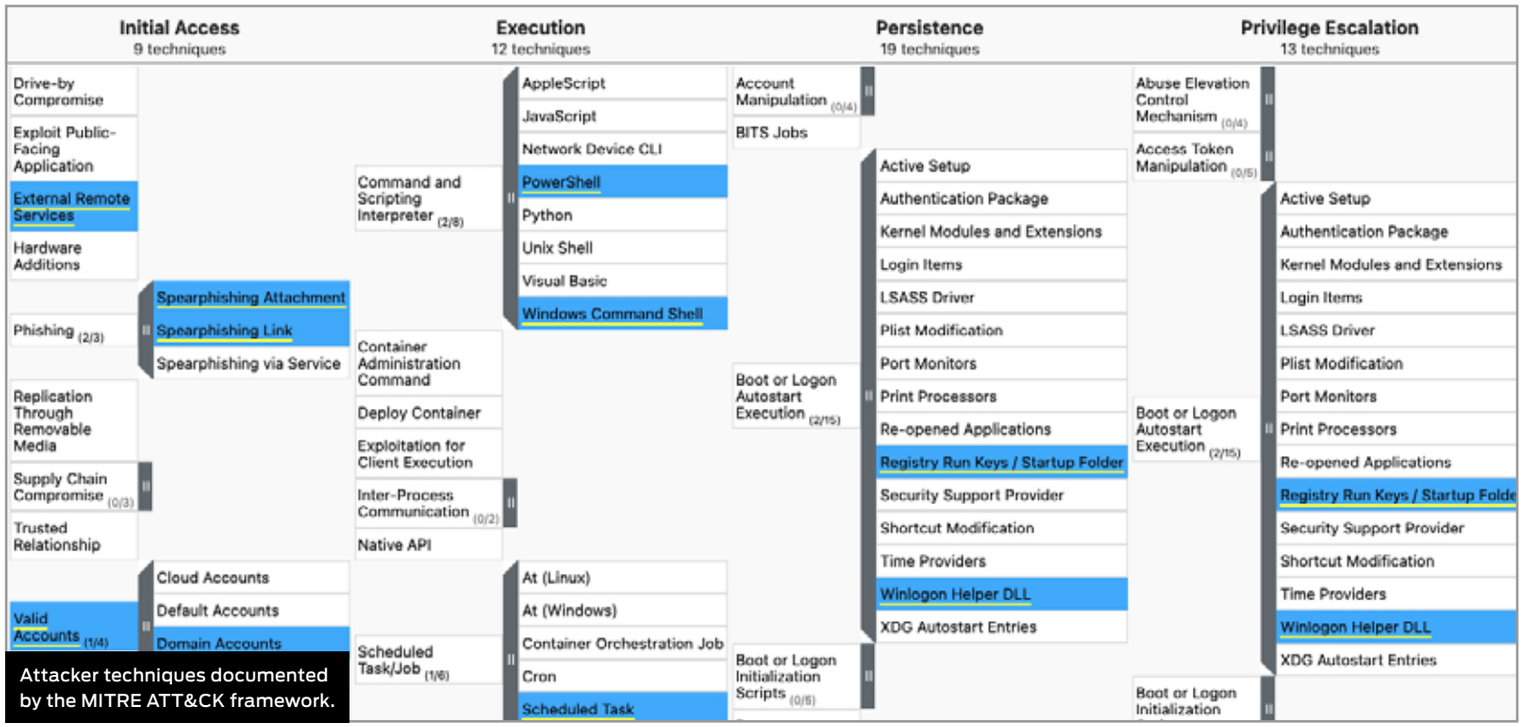
Detection Ratings are weighted to show that how products detect threats can be subtler than just ‘win’ or ‘lose’.

4. Threat Intelligence

Wizard Spider

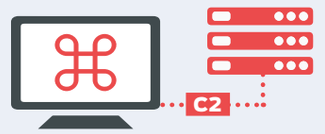
Known to have operated since at least 2016, Wizard Spider is considered to be a threat group based in and around St. Petersburg, Russia. It is most notable for developing the TrickBot banking malware. Wizard Spider has infected over a million systems worldwide predominantly by using this malware.

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



Attacker techniques documented by the MITRE ATT&CK framework.

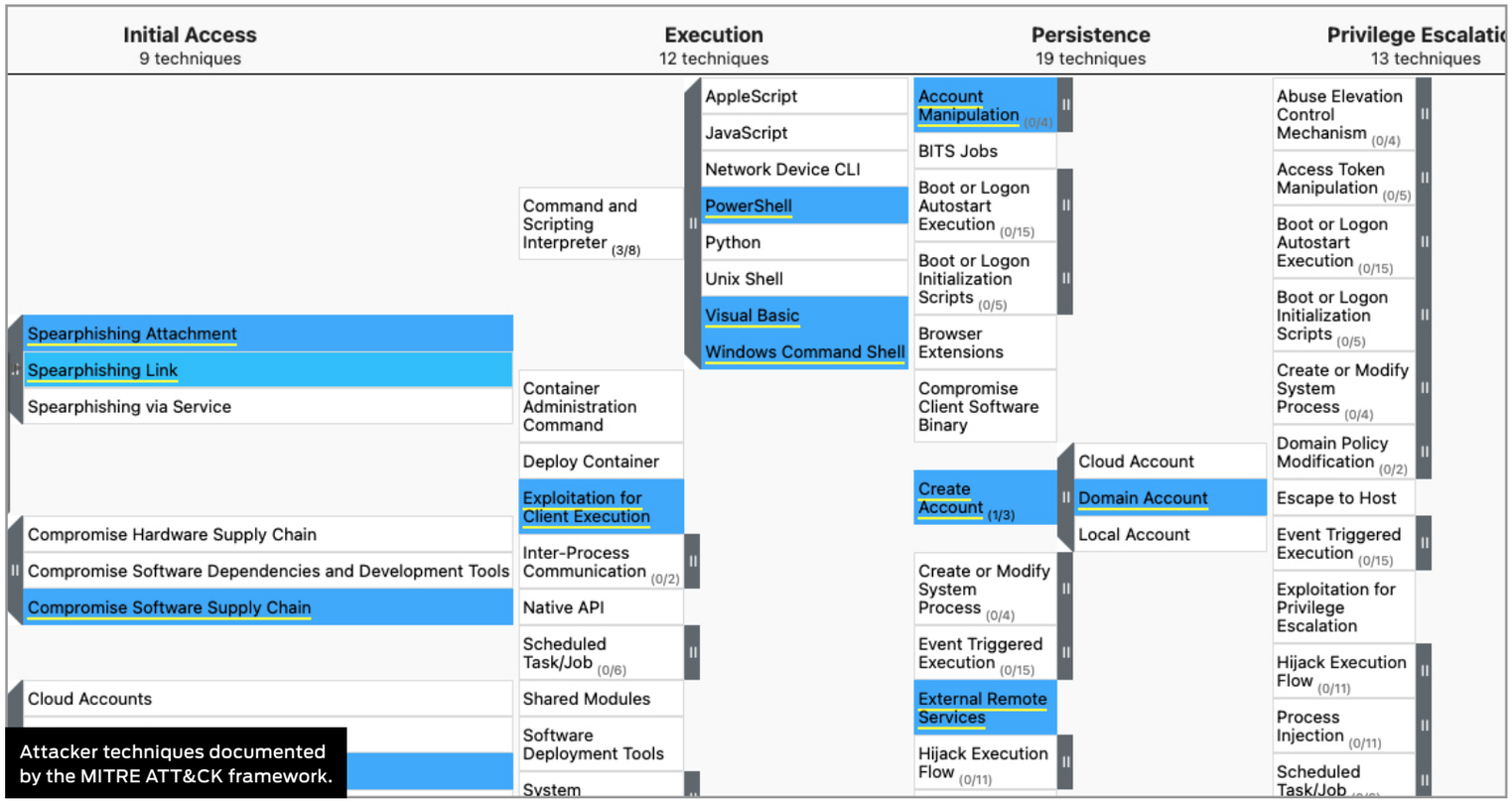
Example Wizard Spider Attack

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

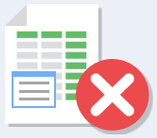
Sandworm

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

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



Example Sandworm Attack

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

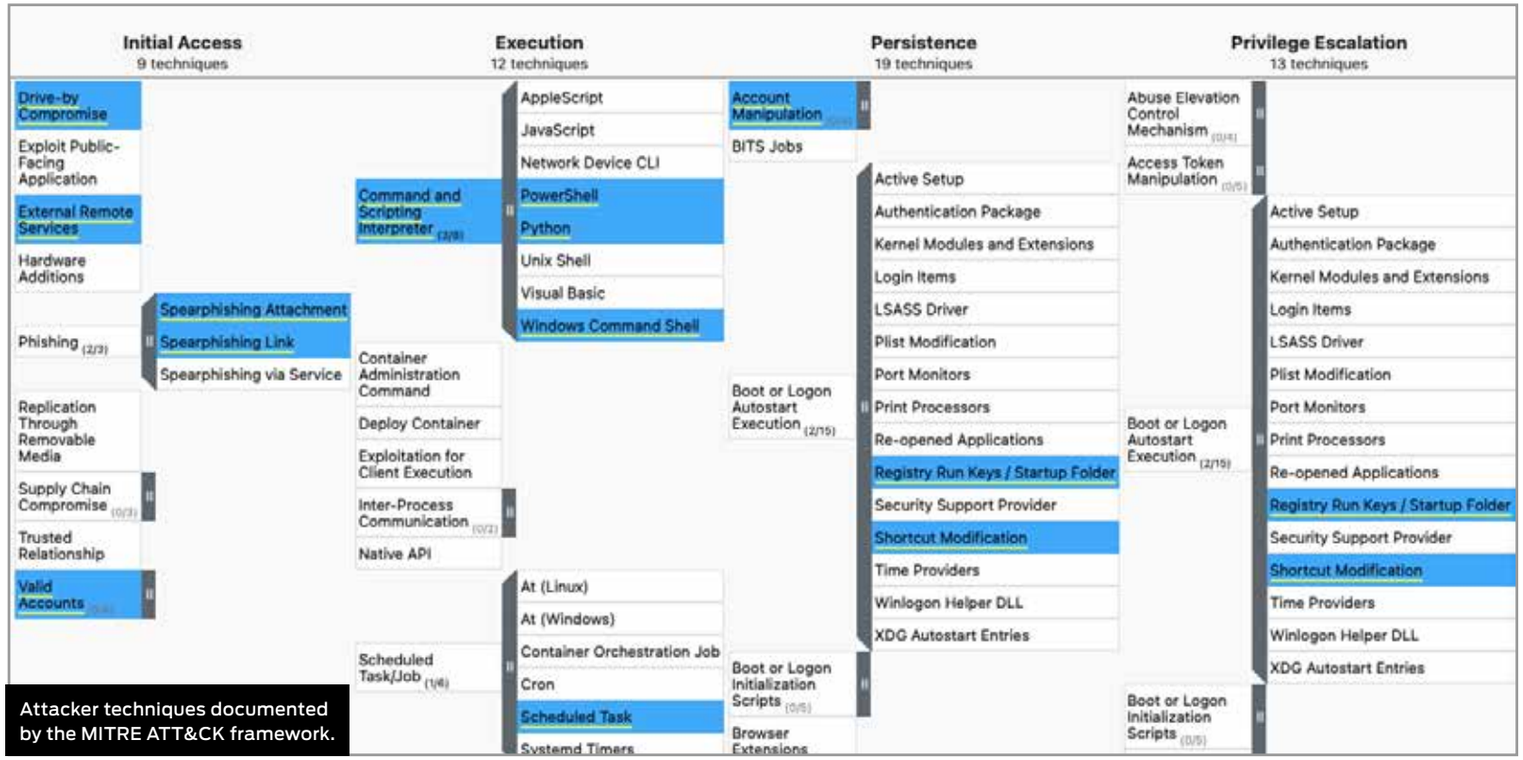
Dragonfly & Dragonfly 2.0

These two groups are sometimes tracked separately. Dragonfly has been active for approximately 10 years with their targets shifting from defense and aviation companies to the energy sector after 2013. Dragonfly 2.0 has kept the focus on the energy sector in its operations.

References:

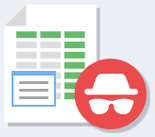
https://attack.mitre.org/groups/G0035/

https://attack.mitre.org/groups/G0074/



Attacker techniques documented by the MITRE ATT&CK framework.

Example Dragonfly & Dragonfly 2.0 Attack

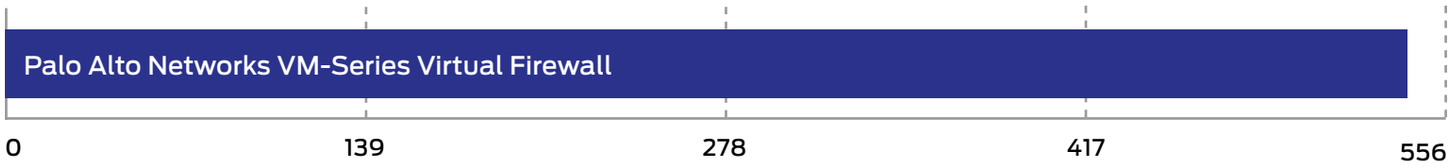
Delivery	Execution	Action	Privilege Escalation	Post-Escalation Action	Lateral Movement	Lateral Action
Spearphising Attachment	Application Layer Protocol	System Information Discovery	Valid Accounts	Scheduled Task	Remote Desktop Protocol	Automated Exfiltration
Malicious File	Command and Scripting Interpreter	Process Discovery		Clear Windows Event Logs		Screen Capture
	Windows Command Shell	System Owner/User Discovery		File deletion		Exfiltration Over C2 Channel
	Powershell			Ingress Tool Transfer		
				Local Account		
				Domain Account		
				Shortcut Modification		
 Malicious File	 Powershell	 System Owner/User Discovery	 Valid Accounts	 Scheduled Task	 Remote Desktop Protocol	 Screen Capture

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 (%)
Palo Alto Networks VM-Series Virtual Firewall	541	97%



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

6. Conclusions

This test exposed **Palo Alto Networks VM-Series virtual firewall** to a diverse set of exploits, file-less attacks and malware attachments, comprising a wide range of realistic threats.

All 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.

It is important to note that while the test used the same types of attacks, new files were used. This exercised the tested product's ability 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.

The product detected all the threats on a basic level, in that for each attack it detected at least some element of the attack chain. Almost all attacks were detected when they were delivered.

It's notable that the **Palo Alto Networks VM-Series virtual firewall** took prompt preventative action based on that detection. For example, because the initial attack was prevented from remotely controlling the target, any further attempt to perform one or more actions was pre-empted. It's quite stingy with granting system privileges and withdraws them when the attacker starts acting in a more powerful and insidious manner.

The firewall was also good at detecting movement between targets (lateral movement), scoring 11 out of the 12 test cases. In the one instance, when it initially missed a lateral movement, it rectified the situation by preventing the attack from running on the new target.

A firewall that's 'torqued too tight' will generate a lot of false positives, even as it prevents against damage from malicious attacks. Security operatives end up trading convenience for protection with such products. When they are forced to manually vet all flagged objects, they are basically having to second guess the firewall's classification of what's malicious or benign.

They will not have this problem with the **Palo Alto Networks VM-Series virtual firewall** with its high total accuracy rating of 98%. It took action against only one legitimate object even as it correctly identified and prevented all malicious attacks.

Palo Alto Networks VM-Series virtual firewall wins an AAA award for its excellent performance.

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 28th March to 13th April 2023.
- This test was conducted independently by SE Labs with similar testing made available to other vendors, at the same time, for their own standalone reports.
- The product was configured according to its vendor's recommendations.
- Targeted attacks were selected and verified by SE Labs.
- Malicious and legitimate data was provided to partner organisations once the test was complete.

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

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

Q We are a customer considering buying or changing part of our security infrastructure. Can you help?

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

Appendix C: Infrastructure Details

- Advanced Threat Prevention(AV, Vulnerability Protection Anti-spyware, File Blocking)
- Advanced URL Filtering
- Advanced Wildfire

Device Details	
Model	PA-VM
CPU	32 x Intel(R) Xeon(R) Gold 6342 CPU @ 2.80GHz
VM Cores	32
VM Memory	60GB
VM License	VM-SERIES-32
VM Capacity Tier	T3-56GB
VM Mode	VMware ESXi 7.0 Update 2
Software Version	11.0.0
Threat Prevention	Enabled
Antivirus	Enabled
WildFire	Enabled
Application Version	8699-7991
Threat Version	8699-7991
Antivirus Version	4425-4942
WildFire Version	761160-764620

Network Details			
	Management Interface	**Client Network**	**Server Interface**
Interface	MGMT	Ethernet 1/4	Ethernet 1/5
Physical interface	Copper 10/100/1000	Copper 10000	Copper 10000
Physical configuration	Auto	Auto	Auto
Zone	Management	Client	Server

Appendix D: Attack Details

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

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

Dragonfly & Dragonfly 2.0							
Incident no:	**Delivery**	**Execution**	**Action**	**Privilege Escalation**	**Post-Esclation Action**	**Lateral Movement**	**Lateral Action**
9	Spearphising Attachment	Application Layer Protocol	System Information Discovery	Valid Accounts	Scheduled Task	Remote Desktop Protocol	Automated Exfiltration
	Malicious File	Command and Scripting Interpreter	Process Discovery		Clear Windows Event Logs		Screen Capture
		Windows Command Shell	System Owner/User Discovery		File deletion		Exfiltration Over C2 Channel
		Powershell			Ingress Tool Transfer		
					Local Account		
					Domain Account		
					Shortcut Modification		
10	Spearphishing Link	Command and Scripting Interpreter	Domain Groups	Valid Accounts	Modify Registry	Remote Desktop Protocol	Archive Collected Data
	Malicious Link	Windows Command Shell	Remote System Discovery		Query Registry		Data from Local System
		Powershell	System Information Discovery		Registry Run Keys / Startup Folder		Local Data Staging
			Process Discovery		Disable or Modify System Firewall		Screen Capture
			System Owner/User Discovery		Forced Authentication		Exfiltration Over C2 Channel
11	Spearphishing Link	Command and Scripting Interpreter	System Information Discovery	Valid Accounts	System Network Configuration Discovery	Remote Desktop Protocol	Archive Collected Data
	Malicious Link	PowerShell	Process Discovery		Archive Collected Data		Automated Exfiltration
			System Owner/User Discovery		Data from Local System		Exfiltration Over C2 Channel
			File and Directory Discovery		Local Data Staging		
			Network Share Discovery		Exfiltration Over C2 Channel		
					Credentials from Password Stores		
					LSA Secrets		
12	Spearphising Attachment	Command and Scripting Interpreter	System Information Discovery	Valid Accounts	NTDS	Remote Desktop Protocol	Archive Collected Data
	Malicious File	Windows Command Shell	Process Discovery		Ingress Tool Transfer		Data from Local System
			System Owner/User Discovery		Security Account Manager		Local Data Staging
			Process Injection		Local Account		Screen Capture
			File and Directory Discovery		Domain Account		Exfiltration Over C2 Channel

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.