SE Labs

INTELLIGENCE-LED TESTING

BREACH RESPONSE DETECTION TEST

NDR

VMware NSX Network Detection and Response

August 2021

SE Labs tested **VMware NSX Network Detection and Response** 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
Liam Fisher
Gia Gorbold
Jeremiah Morgan
Joseph Pike
Dave Togneri
Dimitrios Tsarouchas
Stephen Withey
Liangyi Zhen

IT SUPPORT
Danny King-Smith
Chris Short

PUBLICATION
Sara Claridge
Colin Mackleworth

Website selabs.uk
Twitter @SELabsUK
Email info@SELabs.uk
LinkedIn www.linkedin.com/company/se-labs/
Blog blog.selabs.uk
Phone +44 (0)203 875 5000
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 Information Alliance (VIA); the Anti-Malware Testing Standards Organization (AMTSO); and the Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG).

CONTENTS

Document version 1.0 Written: 31st August 2021

INTRODUCTION

NDR - Now Done Realistically

Network Detection and Response testing reaches new level

Network Detection and Response products are designed to recognise attacks as they pass through one or more networks. In other words, they are like CCTV systems monitoring the flow of information running through an organisation, data centre or other infrastructure.

There are a few different ways to test NDR solutions, many of which are so synthetic as to be misleading. You could run a tool that pushes network packets containing elements of an attack, for example. This might trigger a detection by the NDR sensors. Or it might not. It depends how those sensors are designed.

A very accurate sensor might not generate an alert when analysing such 'fake' test traffic. Ideally it would only alert on a real attack so that the team in the Security Operations Centre (SOC) focuses on significant events only. Parts of an exploit, malware or suspicious login are not a threat. Only a real attack looks like a real attack.

A basic sensor might report problems with every packet that appears to be bad without looking at the context. For example, if a user logs into a system that they use regularly, an unsophisticated system might register that as a problem. A more intelligent one would recognise that all is well and hold back the alert. But it might sound the alarm if the same user logs in from an unusual part of the network. This could be a sign of an attacker moving between systems and using stolen login credentials.

In our tests we make no assumptions about how security products work and run full attacks, from the very first stages through to completing the final 'mission', which might be data damage, theft or the creation of a persistent presence. We replicate the behaviours of real-world attackers and use the MITRE ATT&CK framework to map out the attack chains used in every test case.

We also perform benign activities to ensure that the product we are testing isn't just alerting without discrimination.

By running the most realistic set of attacks possible we put NDR products to a significant challenge. Can they detect real attacks in real-time, often using unique scripts and malware? If you want to know more about advanced persistent threats on the network please read past the initial graphs in this report and dig into the detail.

If you spot a detail in this report that you don't understand, or would like to discuss, please contact us via our Twitter account. 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 Twitter.

Executive Summary

VMware NSX Network Detection and Response was tested against a range of hacking attacks designed to compromise systems and penetrate target networks in the same way as criminals and other attackers breach systems and networks.

We examined its abilities to:

- Detect the delivery of targeted attacks
- Track different elements of the attack chain…
- …including compromises beyond the endpoint and into the wider network
- Handle legitimate applications and other objects

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

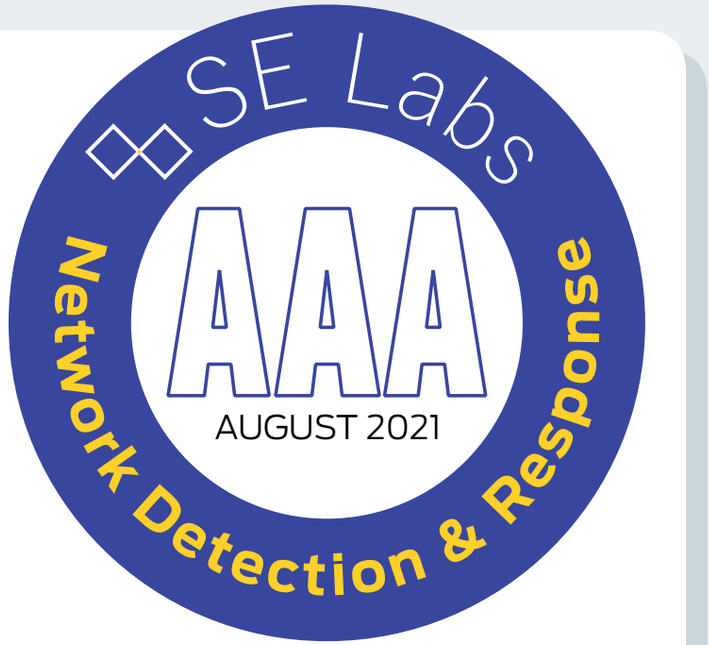
VMware NSX Network Detection and Response was able to detect every targeted attack and tracked each of the hostile activities that occurred during the attacks.

Executive Summary			
Product Tested	Protection Accuracy (%)	Legitimate Accuracy Rating (%)	Total Accuracy Rating (%)
VMware NSX Network Detection and Response	100%	100%	100%

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%.

Network Detection and Response Award

The following product wins the SE Labs award:



VMware
NSX Network
Detection and Response

1. How we Tested

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

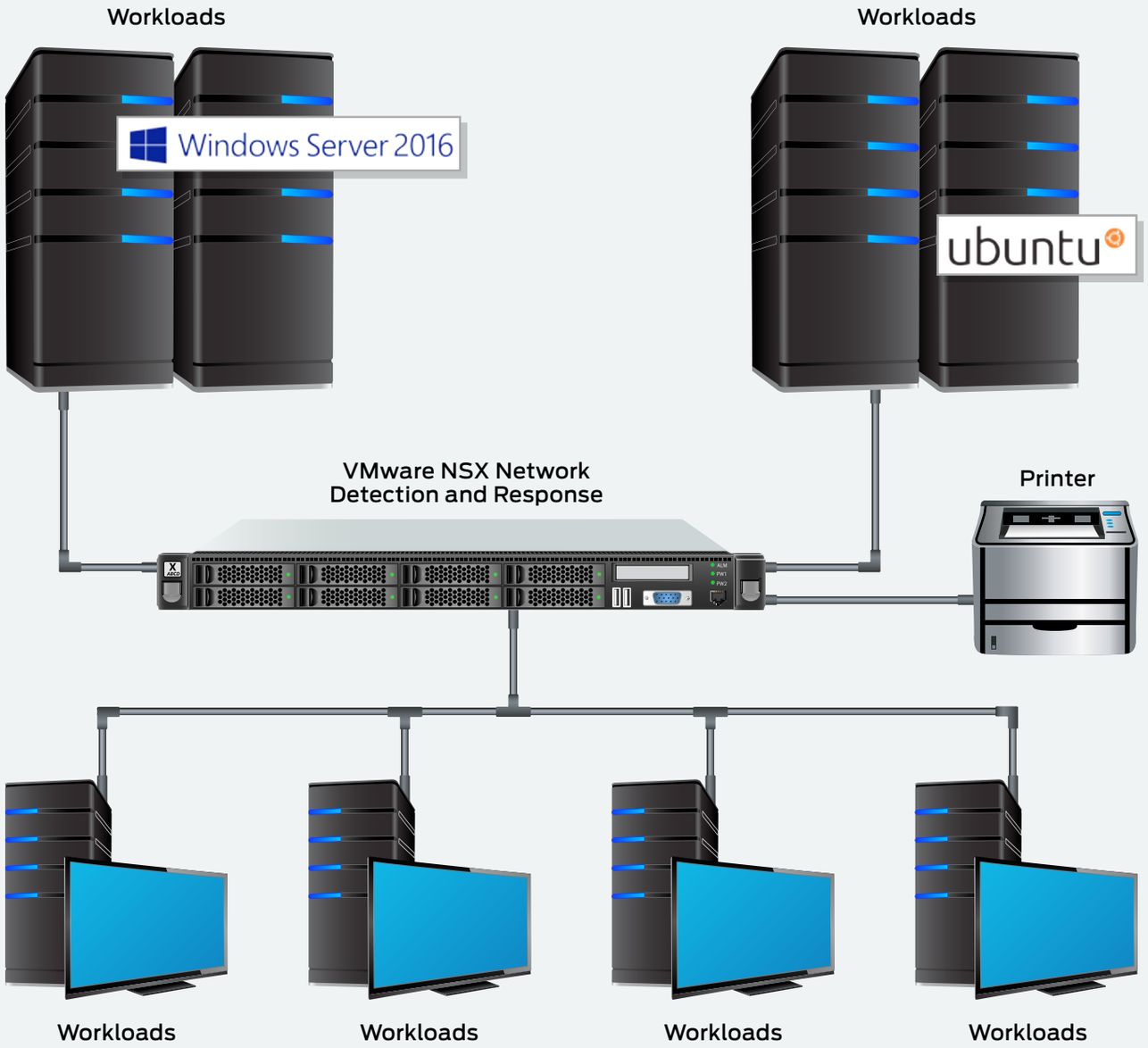
In the diagram on the right you will see an example network that contains workstations, some basic infrastructure such as file servers and a domain controller, as well as cloud-based email and a malicious command and control (C&C) server, which may be a conventional computer or a service such as Dropbox,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

Test Network Example



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.

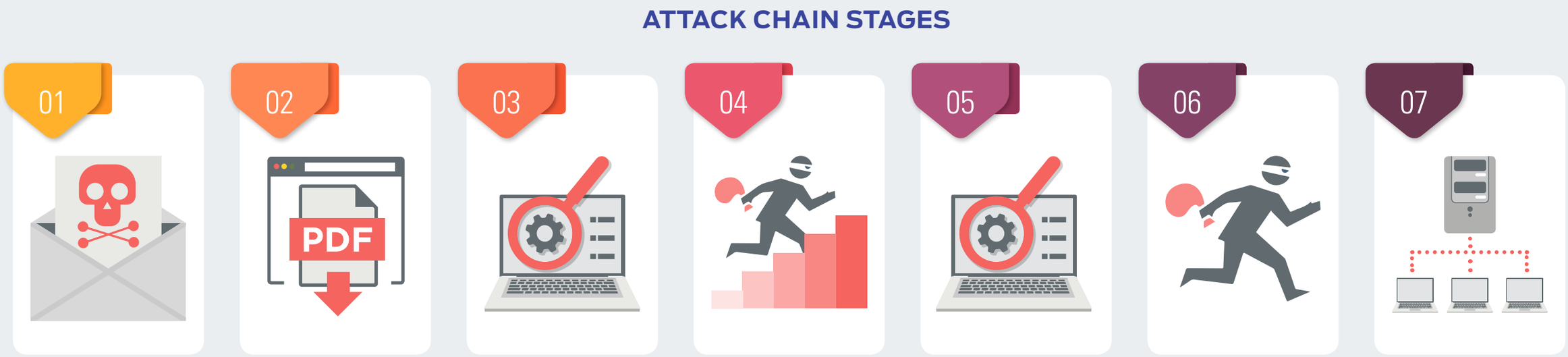


Figure 1. A typical attack starts with an initial contact and progresses through various stages, including reconnaissance, stealing data and causing damage.

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

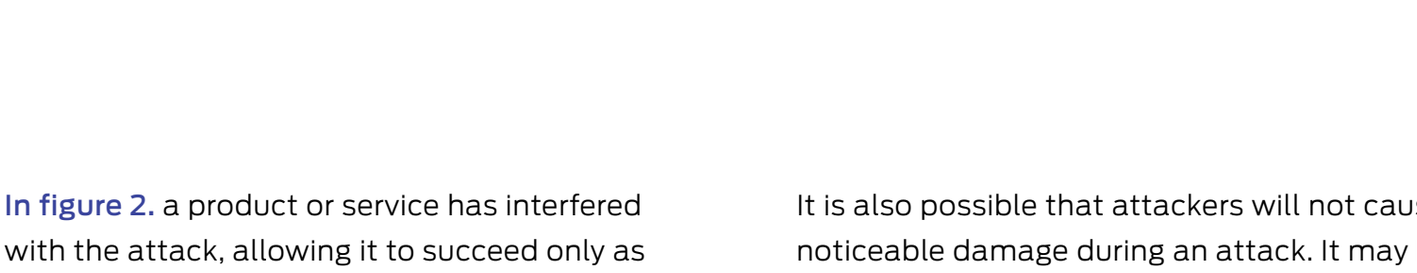


Figure 2. This attack was initially successful but only able to progress as far as the reconnaissance phase.

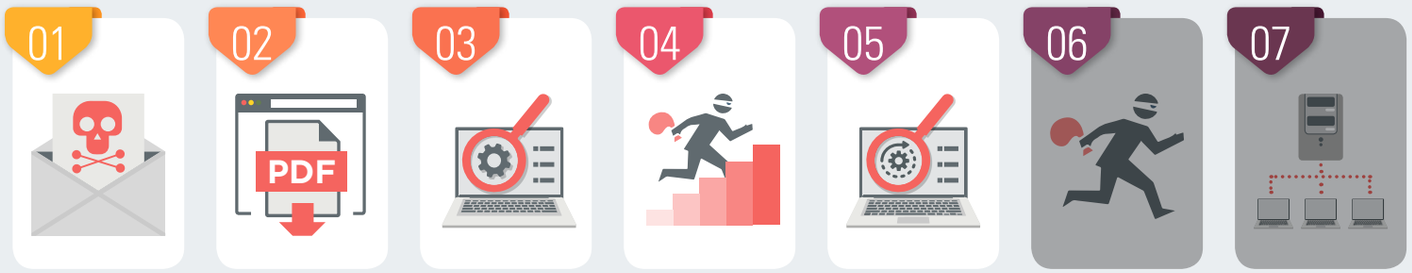


Figure 3. A more successful attack manages to steal passwords but wholesale data theft and destruction was blocked.

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.

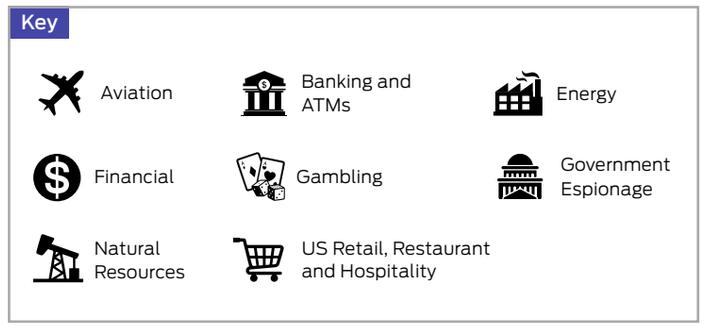
But we didn't just sit down and brainstorm how we would attack different companies. Instead we used current threat intelligence to look at what the bad guys have been doing over the last few years and copied them quite closely. This way we can test the services' abilities to handle similar threats to 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	Targeted Nations	Target	Details
FIN7 & Carbanak	Russia, US, Germany		Communication through Application Layer protocol to avoid detection.
OilRig	UAE, Saudi Arabia		Asymmetric cryptography to conceal C&C traffic.
APT3	US , Hong Kong		Lateral movement focused on Windows Admin shares and RDP.
APT29	US		Exfiltration of data over alternative protocols.



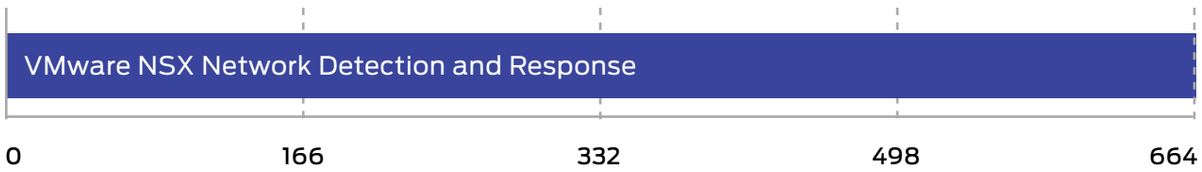
2. Total Accuracy Ratings

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
VMware NSX Network Detection and Response	664	100%	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.

FIN7 &Carbanak								
Incident No:	Detection	Delivery	Execution	Action	Escalation	PE Action	Lateral Movement	Lateral Action
1	✓	✓	✓	n/a	n/a	✓	✓	✓
2	✓	✓	✓	n/a	n/a	✓	✓	✓
3	✓	✓	✓	n/a	n/a	✓	✓	✓
4	✓	✓	✓	n/a	n/a	✓	✓	✓

OilRig								
Incident No:	Detection	Delivery	Execution	Action	Escalation	PE Action	Lateral Movement	Lateral Action
5	✓	✓	✓	n/a	n/a	✓	✓	✓
6	✓	✓	✓	n/a	n/a	✓	✓	✓
7	✓	✓	✓	n/a	n/a	✓	✓	✓
8	✓	✓	✓	n/a	n/a	✓	✓	✓

APT3								
Incident No:	Detection	Delivery	Execution	Action	Escalation	PE Action	Lateral Movement	Lateral Action
9	✓	✓	✓	n/a	n/a	✓	✓	✓
10	✓	✓	✓	n/a	n/a	✓	✓	✓
11	✓	✓	✓	n/a	n/a	✓	✓	✓

APT29								
Incident No:	Detection	Delivery	Execution	Action	Escalation	PE Action	Lateral Movement	Lateral Action
12	✓	✓	✓	n/a	n/a	✓	✓	✓
13	✓	✓	✓	✓	n/a	✓	✓	✓
14	✓	✓	✓	✓	n/a	✓	✓	✓
15	✓	✓	✓	✓	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.

This is a network security test so some endpoint-related parts of the attack chain are not relevant and are out of scope. These are marked as 'n/a'.

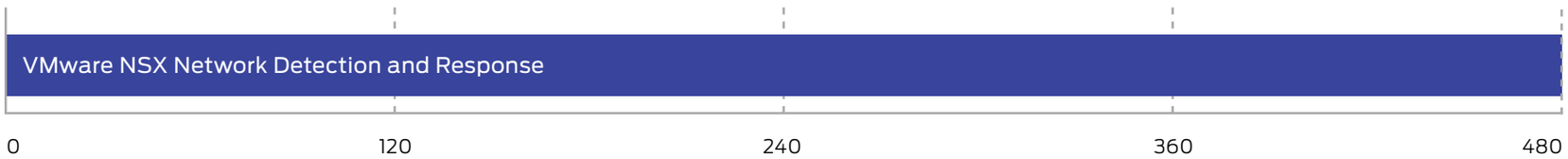
Response Details						
Attacker/ APT Group	Number of Test Cases	Attacks Detected	Delivery/Execution	Action	Privilege Escalation/ Action	Lateral Movement/ Action
FIN7 & Carbanak	4	4	4	n/a	n/a	4
OilRig	4	4	4	n/a	n/a	4
APT3	3	3	4	n/a	n/a	3
APT29	4	4	4	3	n/a	4
Total	**15**	**15**	**16**	**3**	n/a	**15**

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
FIN7 & Carbanak	4	4	12	120
OilRig	4	4	12	120
APT3	3	3	9	90
APT29	4	4	15	150
Total	**15**	**15**	**48**	**480**

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

Detection Accuracy Rating		
Product	Detection Accuracy Rating	Detection Accuracy Rating (%)
VMware NSX Network Detection and Response	480	100%



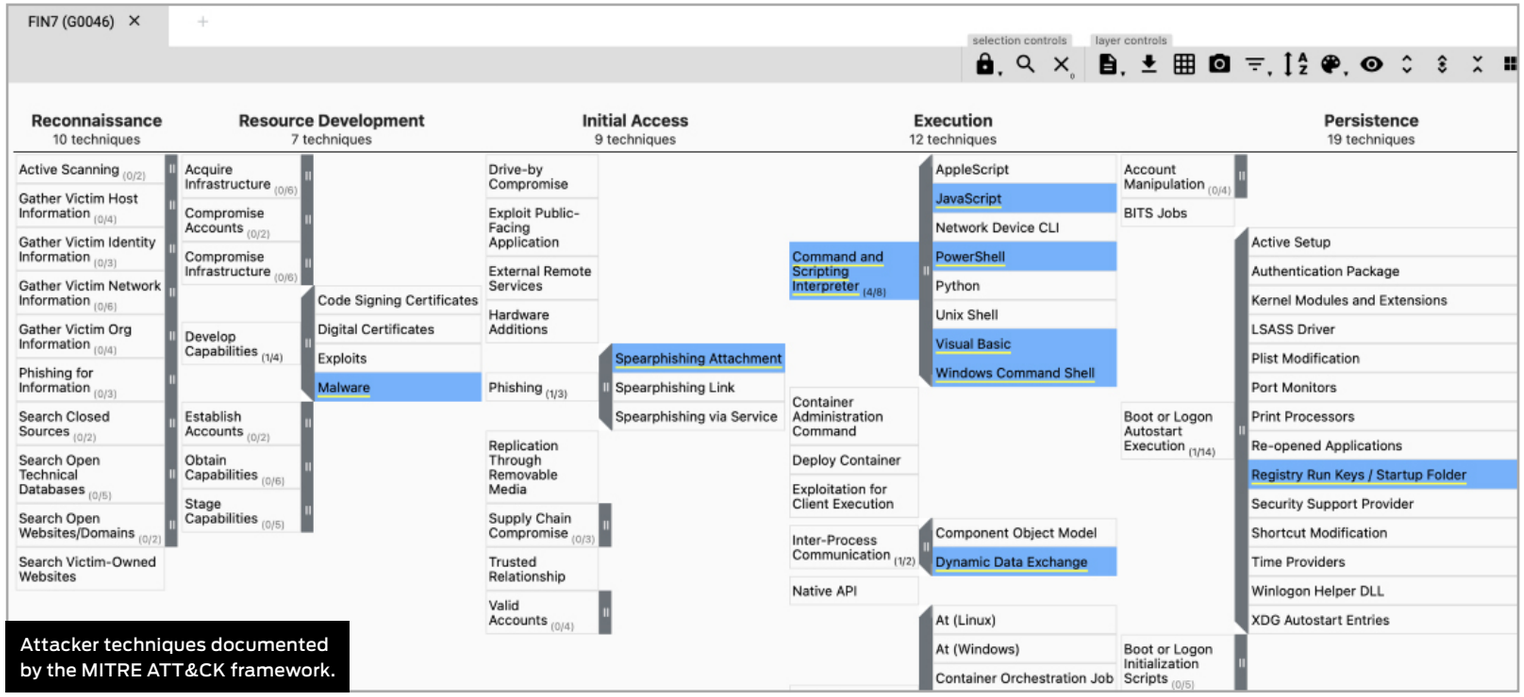
Detection Ratings are weighted to show that how products detect threats can be subtler than just ‘win’ or ‘lose’.

4. Threat Intelligence

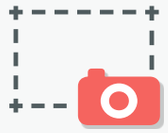
FIN7 and Carbanak

FIN7 used spear phishing attacks targeted at retail, restaurant and hospitality businesses. What appeared to be customer complaints, CVs (resumes) and food orders sent in Word and RTF formatted documents, were actually attacks that hid malicious (VBS) code behind hidden links.

References:
https://attack.mitre.org/groups/G0046/



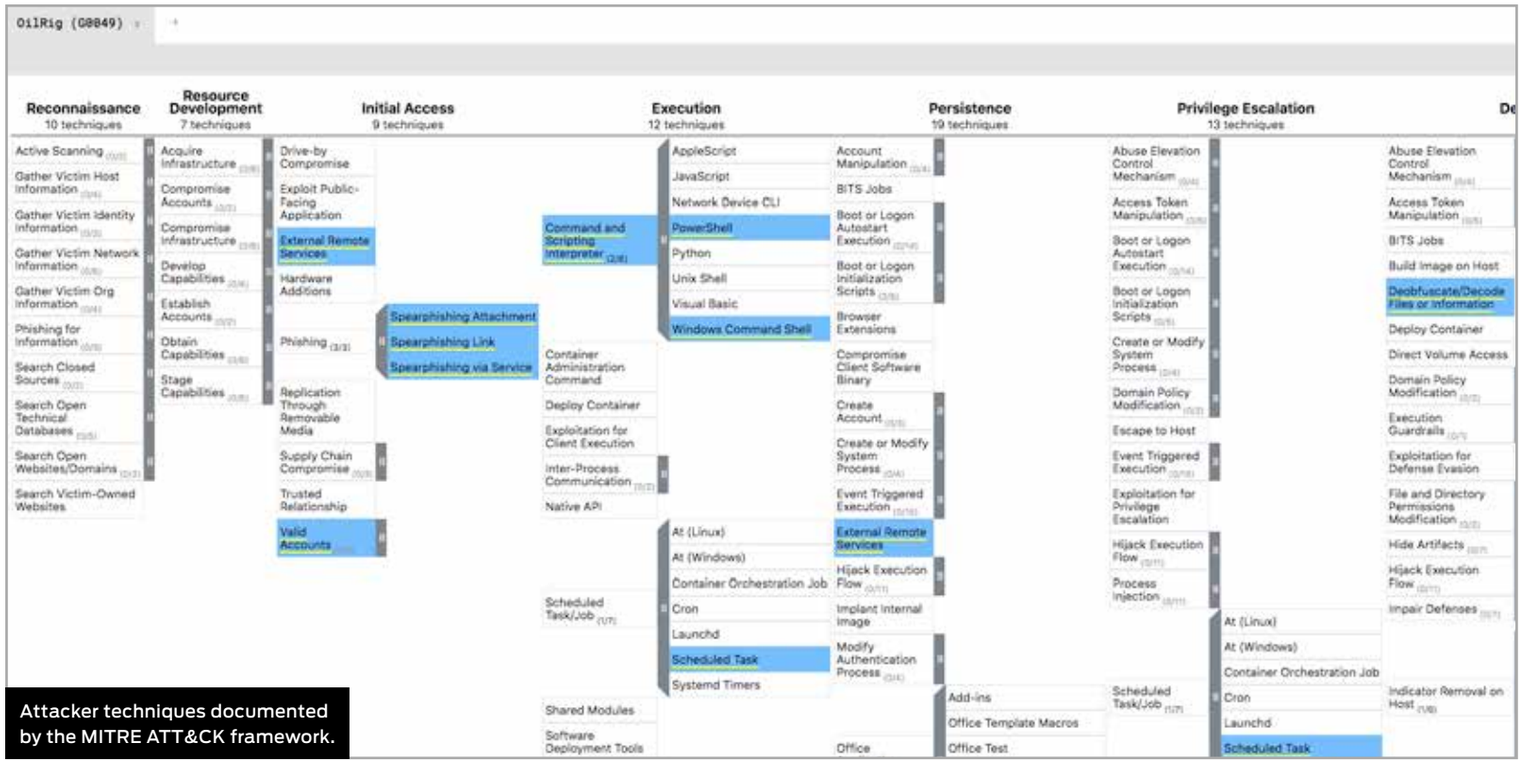
Attacker techniques documented by the MITRE ATT&CK framework.

Example FIN7 & Carbanak Attack									
Initial Access	**Execution**	**Persistence**	**Privilege Escalation**	**Defense Evasion**	**Credential Access**	**Discovery**	**Lateral Movement**	**Collection**	**Command And Control**	**Exfiltration**
Spearphishing Attachment	Command-Line Interface	Registry Run Keys / Startup Folder	Bypass UAC	Code Signing	Brute Force	File and Directory Discovery	Remote Desktop Protocol	Data from Local System	Commonly Used Port	Data Compressed
	Service Execution	Valid Accounts		Disabling Security Tools	Credentials from Web Browsers	Process Discovery		Data Staged	Standard Non-Application Layer Protocol	Data Encrypted
	User Execution			Masquerading		System Information Discovery		Screen Capture	Remote Access Tools	Exfiltration over Command and Control Channel
				Process Injection		Query Registry				
						Permission Groups Discovery				
						System Network Configuration Discovery				
 E-mail Link - Fileless Attack	 Service Execution	 Valid Accounts	 Bypass UAC	 Disabling Security Tools	 Credentials from Web Browsers	 System Information Discovery	 Remote Desktop Protocol	 Screen Capture	 Remote Access Tools	 Exfiltration over Command and Control Channel

OilRig

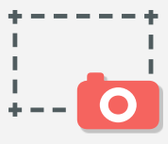
This Iranian APT has attacked a wide variety of targets, including financial, governmental and infrastructural organisations. Its techniques include using phishing via email and services such as LinkedIn, sending links to scripts, macros and other malware. It uses public tools to extract data and to establish and maintain connections to victims.

References:
https://attack.mitre.org/groups/G0049/



Attacker techniques documented by the MITRE ATT&CK framework.

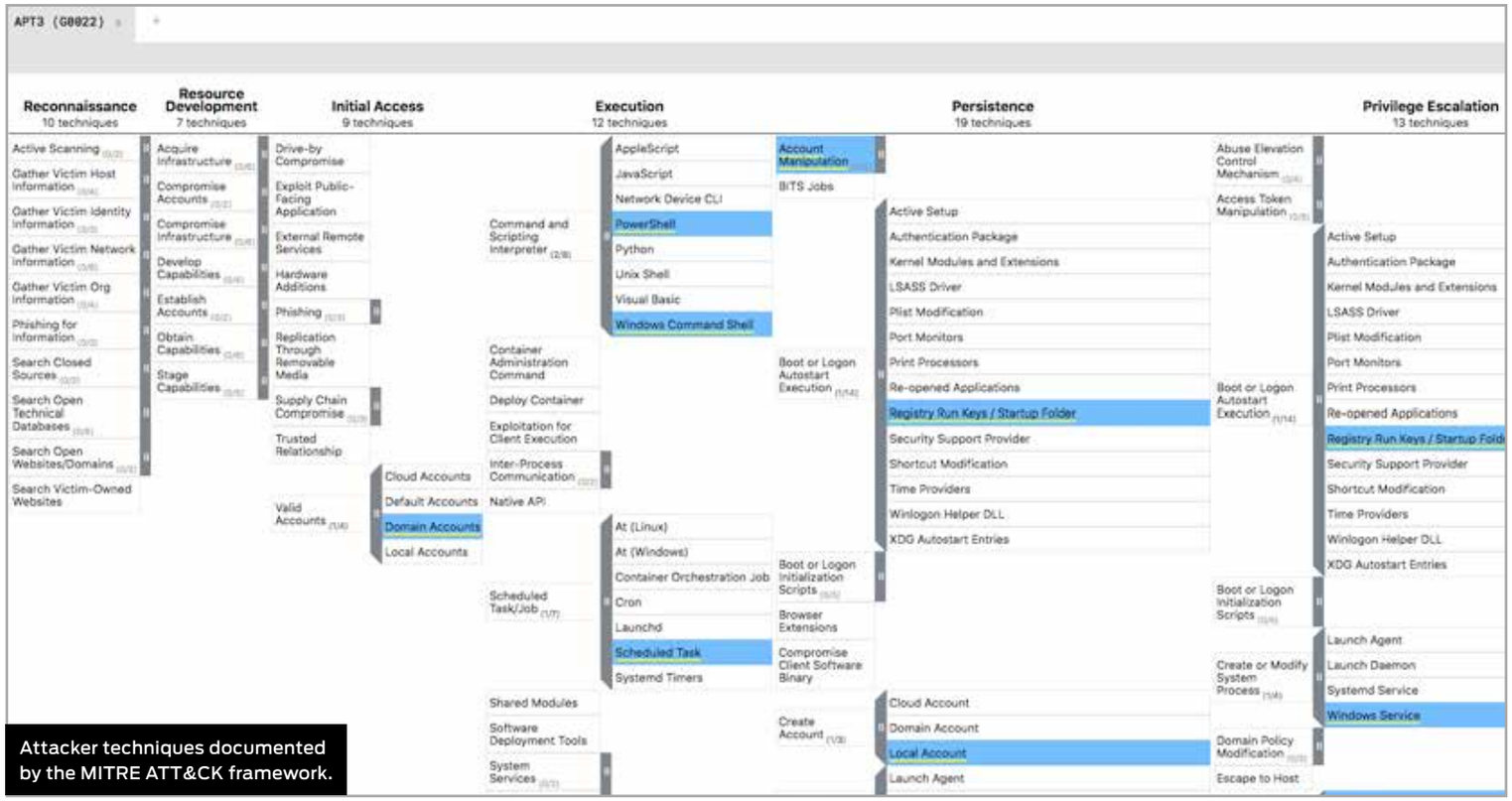
Example OilRig Attack

Delivery	Execution	Action	Privilege Escalation	Post-Escalation Action	Lateral Movement	Lateral Action
Spearphishing via Service	Powershell	System Information Discovery	Bypass UAC	Network Service Scanning	SSH	Keylogging
Compiled HTMl File	Mshta	Process Discovery	Valid Accounts	System Network Configuration Discovery		Screen Capture
	Windows Command Shell	System Owner/User Discovery		System Network Connections Discovery		
	Asymmetric Cryptography	Local Groups		Local Groups		
		Domain Groups		Domain Groups		
				Keylogging		
 Compiled HTMl File	 Asymmetric Cryptography	 Local Groups	 Valid Accounts	 Keylogging	 SSH	 Screen Capture

APT3

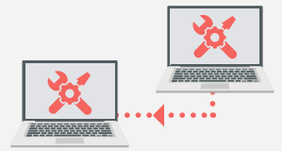
Primarily targeting political organisations in Hong Kong, APT3 uses a wide variety of initial attack techniques including phishing, web-based exploits and access via valid accounts. PowerShell and other scripting languages are used to gain further access, including control via Remote Desktop Access.

References:
https://attack.mitre.org/groups/G0022/



Attacker techniques documented by the MITRE ATT&CK framework.

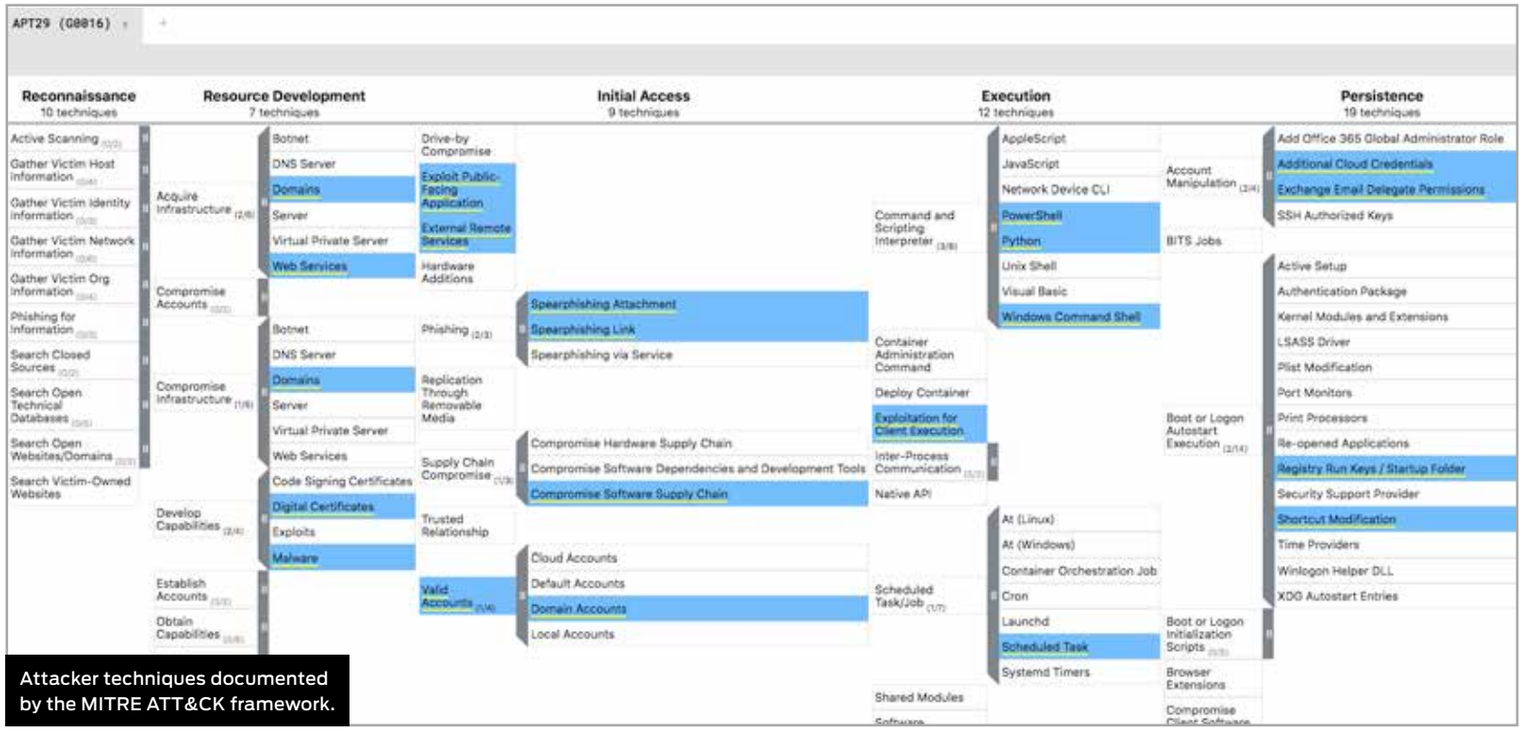
Example APT3 Attack

Delivery	Execution	Action	Privilege Escalation	Post-Escalation Action	Lateral Movement	Lateral Action
Spearphishing Link	PowerShell	File and Directory Discovery	Domain Accounts	Keylogging	SMB/Windows Admin Shares	Ingress Tool Transfer
Obfuscated Files or Information	Windows Command Shell	Process Discovery		Registry Run Keys / Startup Folder		Archive via Utility
	File Deletion	System Information Discovery		Data from Local System		Exfiltration Over C2 Channel
	Hidden Window	System Owner/User Discovery				Local Data Staging
 Obfuscated Files or Information	 File Deletion	 System Information Discovery	 Domain Accounts	 Keylogging	 SMB/Windows Admin Shares	 Ingress Tool Transfer

APT29

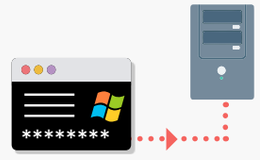
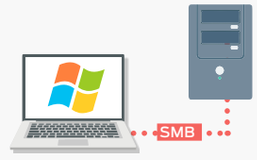
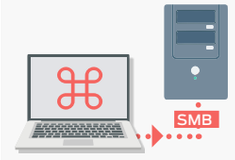
Thought to be connected with Russian military cyber operations, APT29 targets government, military and telecommunications sectors. It is believed to have been behind the Democratic National Committee hack in 2015, in which it used phishing emails with attached malware or links to malicious scripts.

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



Attacker techniques documented by the MITRE ATT&CK framework.

Example APT29 Attack

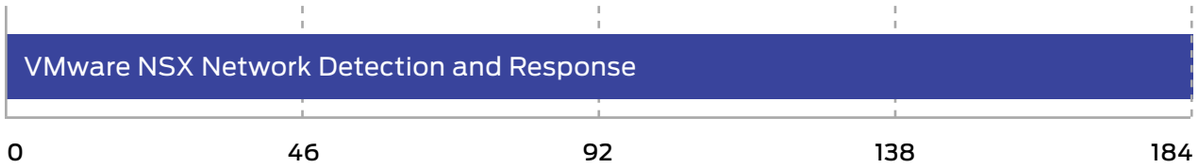
Delivery	Execution	Action	Privilege Escalation	Post-Escalation Action	Lateral Movement	Lateral Action
Web Services	PowerShell	File and Directory Discovery	Bypass UAC	Scheduled Task	SMB/Windows Admin Shares	Automated Collection
Spearphishing Link	File Deletion	Process Discovery	Domain Accounts	Windows Management Intrumentation		Data from Local System
Obfuscated Files or Information	Non-Applcation Layer Protocol	System Information Discovery		Steal or Forge Kerberos Tickets		Screen Capture
	Windows Command Shell	System Network Confirguration Discovery		Remote System Discovery		Exfiltration Over Alternative Protocol
	Deobfuscate/Decode File or Information	System Owner/User Discovery		OS Credential Dumping		
	Python					
 Obfuscated Files or Information	 PowerShell	 File and Directory Discovery	 Domain Accounts	 OS Credential Dumping	 SMB/Windows Admin Shares	 Exfiltration Over Alternative Protocol

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 (%)
VMware NSX Network Detection and Response	184	100%



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

6. Conclusions

This test exposed **VMware NSX Network Detection and Response** to a diverse set of exploits, file-less and malware attacks and reconnaissance ‘discovery’ techniques. The testers behaved as attackers, pivoting between systems (and generating lateral movement traffic), attempting to use credentials, exfiltrating data and creating command and control data flows.

The product detected all of the threats.

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.

An attack is made up of multiple stages and we record when a product detects malicious activity, including the initial ‘delivery’ stage of an attack, when a connection is first made and malicious code is sent to the target. We also watch out for code execution; behaviour by the attacker after their attempts to gain lower-level access (privilege escalation); and their movement across the network after the first stages of the attack (lateral movement).

The results are strong and not one attack stage went undetected. Sometimes products are overly aggressive and detect everything, including threats and legitimate objects. In this test **VMware NSX Network Detection and Response** generated no such false positive results, which is as hoped.

VMware NSX Network Detection and Response wins a 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 7th July and 15th July 2021.
- 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.
- SE Labs conducted this network test using virtual systems.

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 Network Detection and Response (NDR) 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: Attack Details

FIN7 & Carbanak							
Incident No:	Delivery	Execution	Action	Privilege Escalation	Post-Escalation Action	Lateral Movement	Lateral Action
1	Spearphishing Attachment	Command-Line Interface	Account Discovery	Bypass UAC	Credential Dumping	Remote File Copy	Data Compressed
	Obfuscated Files or Information	Commonly Used Port	File and Directory Discovery	Valid Accounts	Data Compressed	Pass the Hash	Data Encrypted
		Powershell	Process Discovery		Data Encrypted		Data from Local System
		Scripting	System Information Discovery		Data from Local System		Data Staged
		Standard Application Layer Protocol	System Owner/User Discovery		Data Staged		Exfiltration over Command and Control Channel
		User Execution			Exfiltration over Command and Control Channel		
					File Deletion		
					Input Capture		
					Modify Registry		
					New Service		
					Process Hollowing		
					Query Registry		
					Scheduled Task		
2	Spearphishing Attachment	Command-Line Interface	Credentials from Web Browsers	Bypass UAC	Data Compressed	Remote Desktop Protocol	Data Compressed
		Commonly Used Port	File and Directory Discovery	Valid Accounts	Data Encrypted		Data Encrypted
		Standard Non-Application Layer Protocol	Process Discovery		Data from Local System		Data from Local System
		User Execution	Process Injection		Data Staged		Data Staged
			System Information Discovery		Disabling Security Tools		Exfiltration over Command and Control Channel
			Valid Accounts		Exfiltration over Command and Control Channel		
					Permission Groups Discovery		
					Query Registry		
					Registry Run Keys / Startup Folder		
					Screen Capture		
					System Network Configuration Discovery		
3	Spearphishing Attachment	Command-Line Interface	Account Discovery	Bypass UAC	Deobfuscate Files or Information	Remote File Copy	Data Compressed
	Software Packing	Commonly Used Port	File and Directory Discovery	Valid Accounts	Application Shimming	Pass the Hash	Data Encrypted
		mshta	Network Share Discovery		Credential Dumping	Windows Admin Shares	Data from Local System
		Scripting	Process Discovery		Data Compressed		Data Staged
		Standard Non-Application Layer Protocol	System Information Discovery		Data Encrypted		Exfiltration over Command and Control Channel
		User Execution	System Network Configuration Discovery		Data from Local System		
			System Owner/User Discovery		Data Staged		
					Execution Guardrails		
					Exfiltration over Command and Control Channel		
4	Spearphishing Attachment	Command-Line Interface	Application Windows Discovery	Bypass UAC	Indirect Command Execution	Windows Management Instrumentation	Data from Local System
		Commonly Used Port	File and Directory Discovery	Valid Accounts	Data Compressed		Data Compressed
		Component Object Model and Distributed COM	Network Share Discovery		Data Encrypted		Data Encrypted
		Execution through API	Permission Groups Discovery		Data from Local System		Data Staged
		Powershell	Process Discovery		Data Staged		Exfiltration over Command and Control Channel
		Scripting	System Information Discovery		DLL Search Order Hijacking		
		Standard Application Layer Protocol			Execution Guardrails		
		Standard Cryptographic Protocol			Exfiltration over Command and Control Channel		
					File Deletion		
					Hooking		
					Input Capture		

OilRig							
Incident No:	Delivery	Execution	Action	Privilege Escalation	Post-Escalation Action	Lateral Movement	Lateral Action
5	Spearphishing Attachment	Windows Command Shell	System Information Discovery	Bypass UAC	Password Policy Discovery	Remote Desktop Protocol	Automated Collection
	Malicious File	Web Shell	Process Discovery	Valid Accounts	Local Groups		Screen Capture
		Deobfuscate/Decode Files or Information	System Owner/User Discovery		Domain Groups		Exfiltration Over Unencrypted/ Obfuscated Non-C2 Protocol
			Local Account		System Service Discovery		
			Domain Account		LSASS Memory		
					LSASS Secrets		
					Ingress Tool Transfer		
					Scheduled Task		
6	Spearphishing Link	Powershell	System Information Discovery	Bypass UAC	Query Registry	Remote Desktop Protocol	Archive Collected Data: Archive via Utility
	Malicious Link	Mshta	Process Discovery	Valid Accounts	System Service Discovery		Screen Capture
		Windows Command Shell	System Owner/User Discovery		Local Account		
		File Deletion	Local Groups		Domain Account		
		Obfuscated File or Information	Domain Groups		Password Policy Discovery		
					Cached Domain Credentials		
					Credentials in Files		
					Keylogging		
					Ingress Tool Transfer		
7	Spearphishing via Service	Windows Command Shell	System Information Discovery	Bypass UAC	System Network Configuration Discovery	SSH	Automated Collection
		Web Shell	Process Discovery	Valid Accounts	System Network Connections Discovery		Archive Collected Data: Archive via Utility
		Indicator Removal from Tools	System Owner/User Discovery		Local Account		Exfiltration Over Unencrypted/ Obfuscated Non-C2 Protocol
		Asymmetric Cryptography	Local Account		Domain Account		
			Domain Account		Query Registry		
			Credentials from Web Browsers		Credentials from Password Stores		
					Ingress Tool Transfer		
8	Spearphishing via Service	Powershell	System Information Discovery	Bypass UAC	Network Service Scanning	SSH	Keylogging
	Compiled HTMl File	Mshta	Process Discovery	Valid Accounts	System Network Configuration Discovery		Screen Capture
		Windows Command Shell	System Owner/User Discovery		System Network Connections Discovery		
		Asymmetric Cryptography	Local Groups		Local Groups		
			Domain Groups		Domain Groups		
					Keylogging		

APT3							
Incident No:	Delivery	Execution	Action	Privilege Escalation	Post-Escalation Action	Lateral Movement	Lateral Action
9	Spearphishing Link	Windows Command Shell	File and Directory Discovery	Domain Accounts	Scheduled Task	Remote Desktop Protocol	Ingress Tool Transfer
	Obfuscated Files or Information	PowerShell	Process Discovery		DLL-Sideloading		Archive via Utility
		File Deletion	System Information Discovery		Remote System Discovery		Exfiltration Over C2 Channel
		Hidden Window	System Owner/User Discovery		System Network Configuration Discovery		Local Data Staging
			Local Account		System Network Connections Discovery		
10	Spearphishing Link	PowerShell	File and Directory Discovery	Domain Accounts	Keylogging	SMB/Windows Admin Shares	Ingress Tool Transfer
	Obfuscated Files or Information	Windows Command Shell	Process Discovery		Registry Run Keys / Startup Folder		Archive via Utility
		File Deletion	System Information Discovery		Data from Local System		Exfiltration Over C2 Channel
		Hidden Window	System Owner/User Discovery				Local Data Staging
11	Spearphishing Attachment	Windows Command Shell	File and Directory Discovery	Domain Accounts	LSASS Memory	SMB/Windows Admin Shares	Ingress Tool Transfer
	Software Packing		Process Discovery		Windows Service		Archive via Utility
			System Information Discovery		Permission Group Discovery		Exfiltration Over C2 Channel
			System Owner/User Discovery		Data from Local System		Local Data Staging
			Credentials from Web Browsers				
			Credentials In Files				

APT29							
Incident No:	Delivery	Execution	Action	Privilege Escalation	Post-Escalation Action	Lateral Movement	Lateral Action
12	Web Services	PowerShell	File and Directory Discovery	Bypass UAC	Scheduled Task	SMB/Windows Admin Shares	Automated Collection
	Spearphishing Link	File Deletion	Process Discovery	Domain Accounts	Windows Management Intrumentation		Data from Local System
	Obfuscated Files or Information	Non-Applcation Layer Protocol	System Information Discovery		Steal or Forge Kerberos Tickets		Screen Capture
		Windows Command Shell	System Network Confirguration Discovery		Remote System Discovery		Exfiltration Over Alternative Protocol
		Deobfuscate/Decode File or Information	System Owner/User Discovery		OS Credential Dumping		
		Python					
13	Spearphishing Attachment	Exploit Public-Facing Attachment	File and Directory Discovery	Bypass UAC	Registry Run Keys / Startup Folder	Pass the Ticket	Email Collection
	Digital Certificates	Software Packing	Process Discovery	Domain Accounts	Steal or Forge Kerberos Tickets	SMB/Windows Admin Shares	Exfiltration Over C2 Channel
	Malicious File	Non-Applcation Layer Protocol	System Information Discovery		Remote System Discovery		Data Compressed
	Masquerading	Windows Command Shell	Query Registry		Input Capture		Data Encrypted
	Shortcut Modification		Permission Groups Discovery		Modify Registry		Data Staged
							Data from Local System
14	Spearphishing Attachment	Windows Command Shell	File and Directory Discovery	Bypass UAC	OS Credential Dumping	Windows Remote Management	Clipboard Data
	Malicious File		Process Discovery	Domain Accounts	Input Capture	Lateral Tool Transfer	Screen Capture
	Shortcut Modification		System Information Discovery		Modify Registry		Data from Local System
			Peripheral Device Discovery		Timestomp		Exfiltration Over C2 Channel
			Security Software Discovery		Steal or Forge Kerberos Tickets		OS Credential Dumping
					Registry Run Keys / Startup Folder		
15	Spearphishing Attachment	Exploitation for Client Execution	File and Directory Discovery	Bypass UAC	Hijack Execution Flow	SMB/Windows Admin Shares	Exfiltration Over Alternative Protocol
	Malicious File	Windows Command Shell	Process Discovery	Domain Accounts	Create Account		Clipboard Data
		Python	System Information Discovery		Unsecured Credentials		Data from Local System
			Query Registry		Permission Groups Discovery		Ingress Tool Transfer
			Security Software Discovery		Ingress Tool Transfer		Timestomp
							Automated Collection

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.