SE Labs

INTELLIGENCE-LED TESTING

Breach Response Test
Protection Mode

Crowdstrike Falcon

December 2020

SE Labs tested **Crowdstrike Falcon** 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
Zaynab Bawa
Thomas Bean
Solandra Brewster
Liam Fisher
Gia Gorbold
Joseph Pike
Dave Togneri
Jake Warren
Stephen Withey

IT SUPPORT
Danny King-Smith
Chris Short

PUBLICATION
Sara Claridge
Colin Mackleworth

Website selabs.uk
Twitter @SELabsUK
Email info@SELabs.uk
Facebook www.facebook.com/selabsuk
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 17th December 2020

INTRODUCTION

Protection with Detection

If you can spot a threat, why not block it too?

Any doubt that intrusion detection technology is necessary was shattered this month. Large companies and other organisations relying on compromised technology from IT management firm SolarWinds are racing to discover if they have been breached themselves, and to what extent.

And it's not like things have been quiet on the breach front more generally. Once security vendors and the press cast around desperately for examples of breaches. The vendors used rare known cases to sell their software. Journalists used them to write explosive articles. Now it's a case of Googling 'ransomware' and choosing from the dozens of recent reports, including attacks on major healthcare, technology and educational victims.

So-called endpoint detection and response (EDR) products are designed to spot a breach and document it. If something weird happens, like company data being leaked, you want to know what happened to avoid a similar problem. An EDR product or service can help, even when the specific malware used wasn't known about previously. Some of those companies reeling from the Solarwinds attack are probably digging through their EDR logs now, wishing they had monitored them more closely.

This poses a question, though. If an EDR solution can spot an attack, why doesn't it stop it too?

Increasingly vendors have been taking this approach, 'weaponising' the capability of their detection technology to enable protection. It's a bit like attaching a sniper rifle or (less lethally) a massive glue gun to a CCTV camera. Wouldn't it be better to neutralise the threat rather than quietly observe as it does damage or steals things?

In our Breach Response testing we have two different modes that we use to test products. The 'Detection' mode measures all the different ways in which a product can detect an attack, and at which stages it can do so. Our 'Protection' mode, as used in this report, shows its abilities to detect and stop a threat.

Understanding the capabilities of different security products is always better achieved before you need to use them in a live scenario. SE Labs' Breach Response 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 via our Twitter or Facebook accounts. 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

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

We examined its abilities to:

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

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

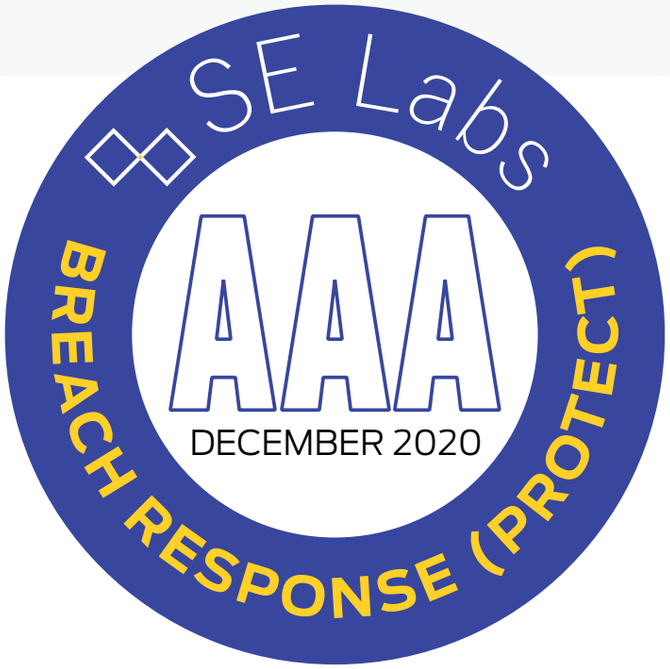
Crowdstrike Falcon performed admirably, providing complete detection and protection coverage against all attacks, while allowing all legitimate applications to operate. This is an exceptional result in a challenging test.

Executive Summary			
Product Tested	Protection Accuracy (%)	Legitimate Accuracy Rating (%)	Total Accuracy Rating (%)
Crowdstrike Falcon	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%.

Breach Response Award

The following product wins the SE Labs award:



Crowdstrike Falcon

1. How we Tested

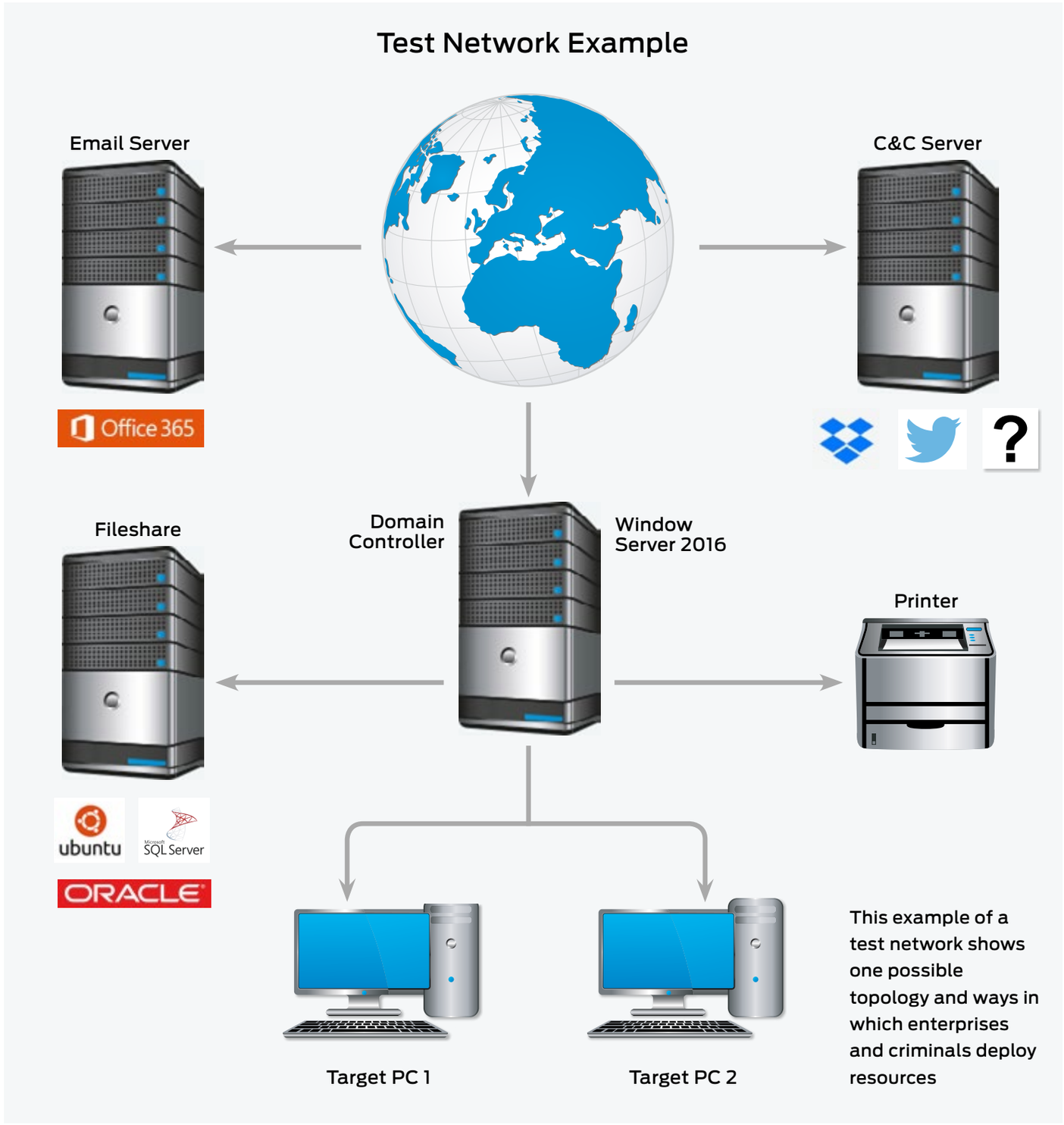
Testers can't assume that products will work a certain way, so running a realistic breach response test means setting up real networks and hacking them in the same way that real adversaries behave.

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.**



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 (right) 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.

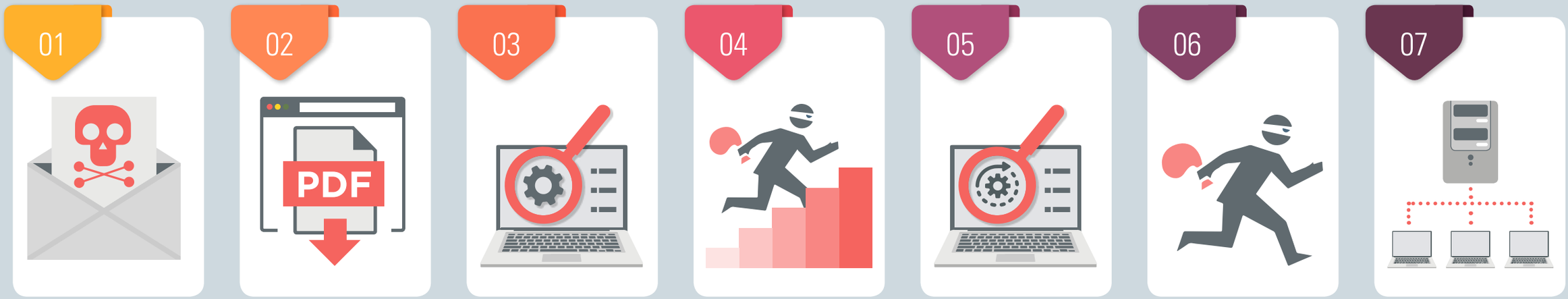


Figure 1. A typical attack starts with an initial contact and progresses through various stages, including reconnaissance, stealing data and causing damage.

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

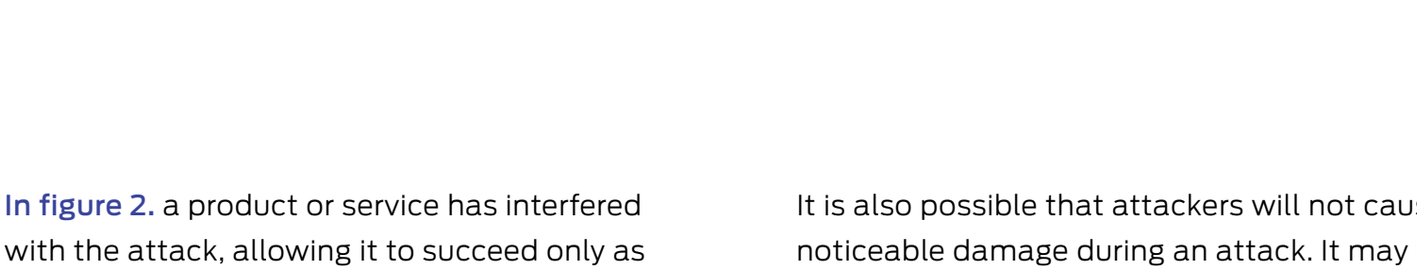


Figure 2. This attack was initially successful but only able to progress as far as the reconnaissance phase.

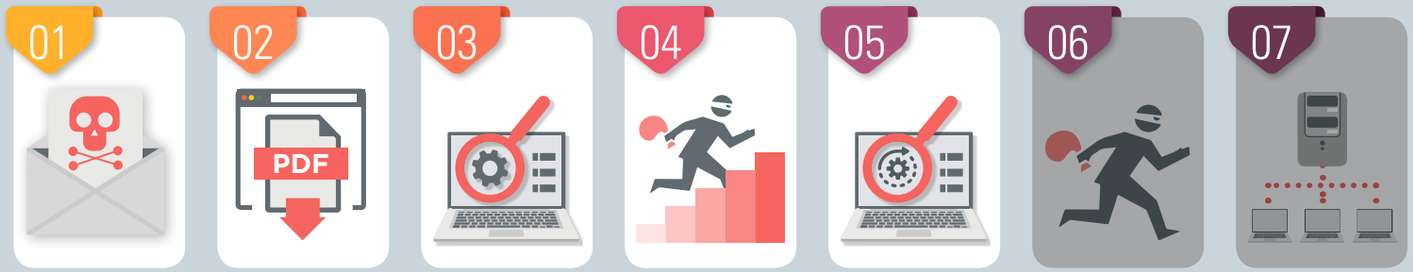


Figure 3. A more successful attack manages to steal passwords but wholesale data theft and destruction was blocked.

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
FIN7			Documents containing hidden links to scripts
FIN4			Man-in-the-middle spear phishing
FIN10			Spear phishing emails combined with public attack tools
Silence			Documents containing scripts, links and exploits

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.

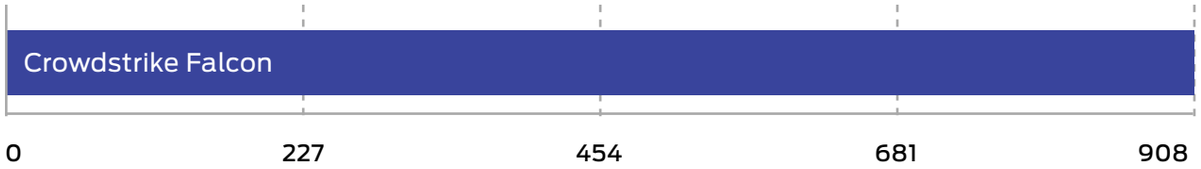
The chart below takes into account not only the product's ability to detect and protect against threats, but also its handling of non-malicious objects such as web addresses (URLs) and applications.

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 11.

Total Accuracy Ratings			
Product	Total Accuracy Rating	Total Accuracy (%)	Award
Crowdstrike Falcon	908	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 and protect against all relevant elements of an attack. The term 'relevant' is important, because if early stages of an attack are countered fully there is no need for later stages to be addressed.

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

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

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

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

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

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

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

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

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

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

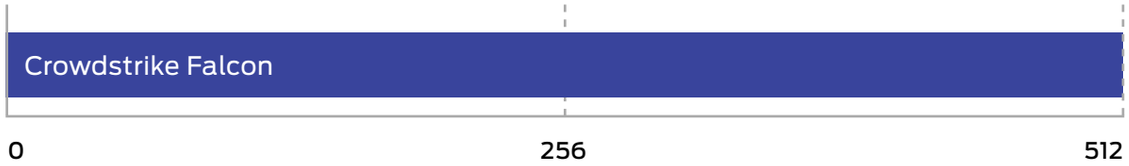
Response Details											
Attacker/ APT Group	Number of test cases	Detection	Delivery	Execution	Action	Privilege Escalation	Post Escalation Action	Lateral Movement	Lateral Action	Protected	Penalties
FIN7	13	13	0	0	0	0	0	0	0	13	0
FIN4	4	4	0	0	0	0	0	0	0	4	0
FIN10	9	9	0	0	0	0	0	0	0	9	0
Silence	6	6	0	0	0	0	0	0	0	6	0
TOTAL	**32**	**32**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**32**	**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 test cases	Protected	Penalties	Protection Score	Protection Rating
FIN7	13	13	0	52	208
FIN4	4	4	0	16	64
FIN10	9	9	0	36	144
Silence	6	6	0	24	96
TOTAL	**32**	**32**	**0**	**128**	**512**

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

Protection Accuracy Ratings		
Product	Protection Accuracy Rating	Protection Accuracy Rating (%)
Crowdstrike Falcon	512	100%



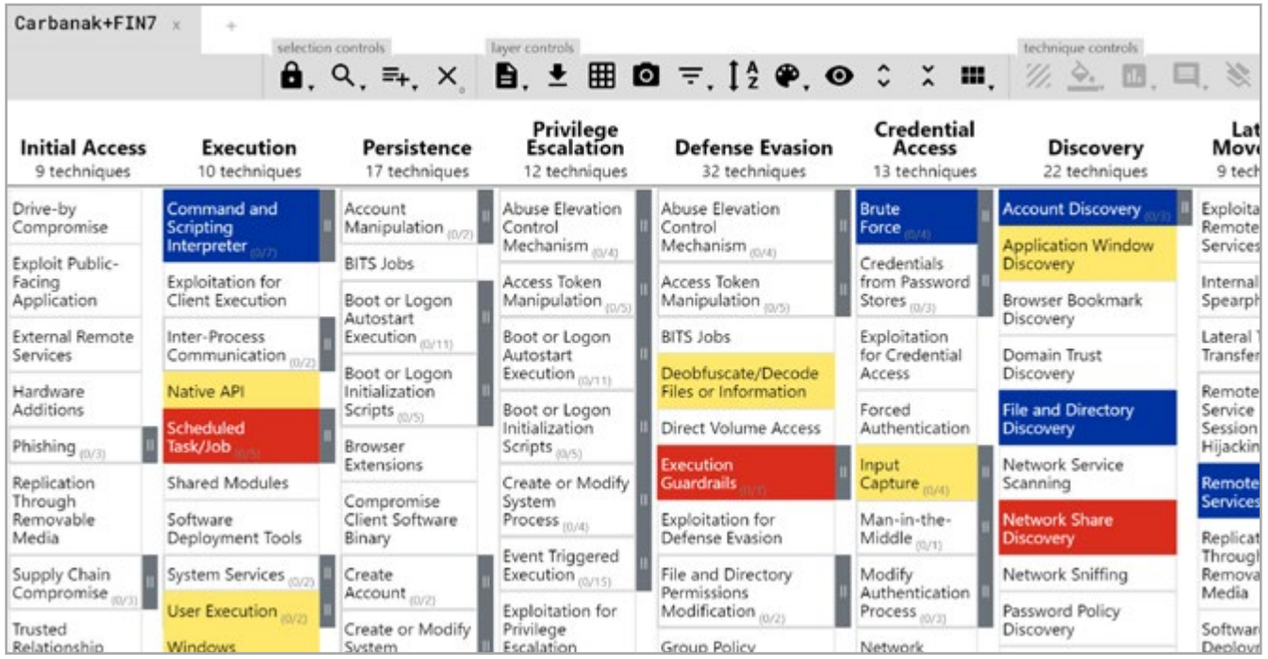
Protection Ratings are weighted to show that how products handle threats can be subtler than just 'win' or 'lose'.

4. Threat Intelligence

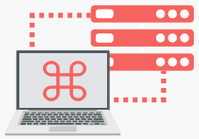
FIN7

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

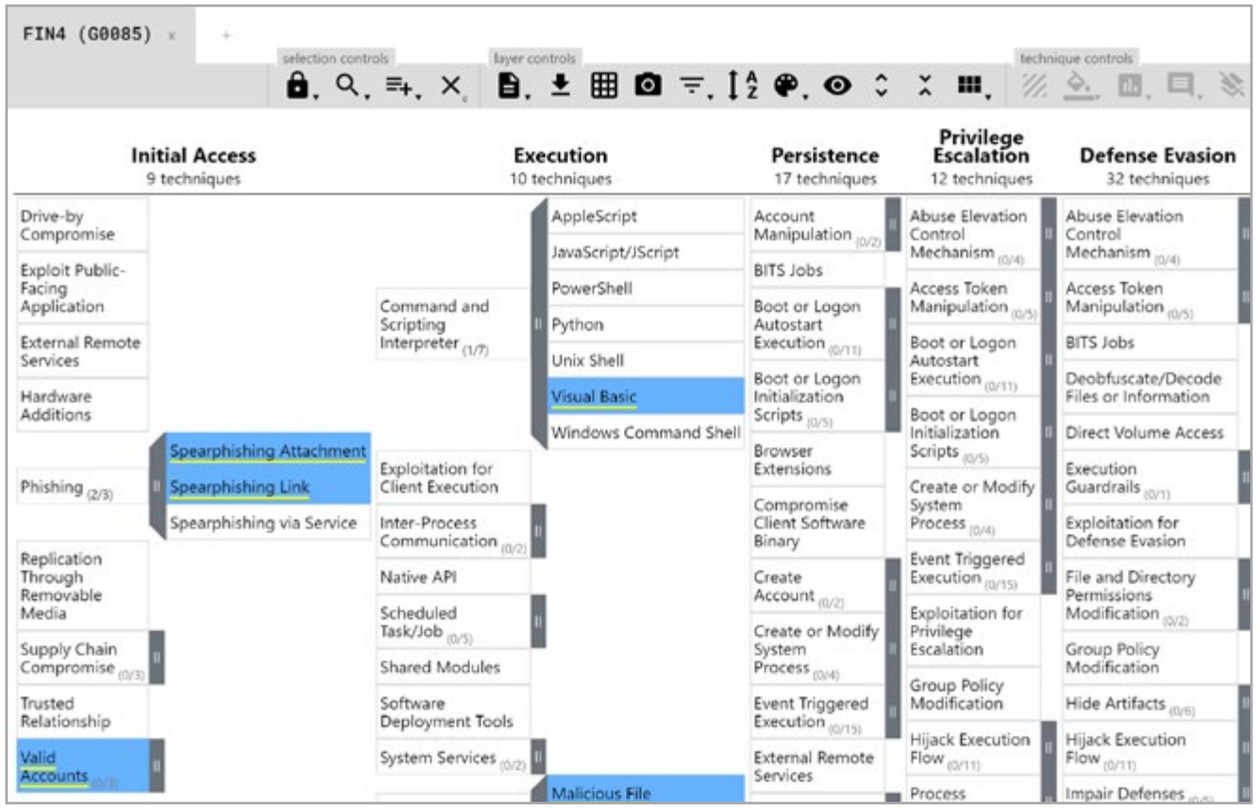
Example FIN7 Attack										
Initial Access	**Execution**	**Persistence**	**Privilege Escalation**	**Defense Evasion**	**Credential Access**	**Discovery**	**Lateral Movement**	**Collection**	**Command And Control**	**Exfiltration**
Spearphishing Attachment	Command-Line Interface	Registry Run Keys / 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

FIN4

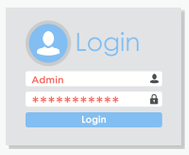
This group stole clean Office documents from the target and edited them, embedding malicious macros.

By using correctly formatted documents containing real information, stolen from compromised accounts, the attackers increased the likelihood that recipients would be tricked into opening the documents and allowing their own systems to be compromised.

References:
https://attack.mitre.org/groups/G0085/



Attacker techniques documented by the MITRE ATT&CK framework.

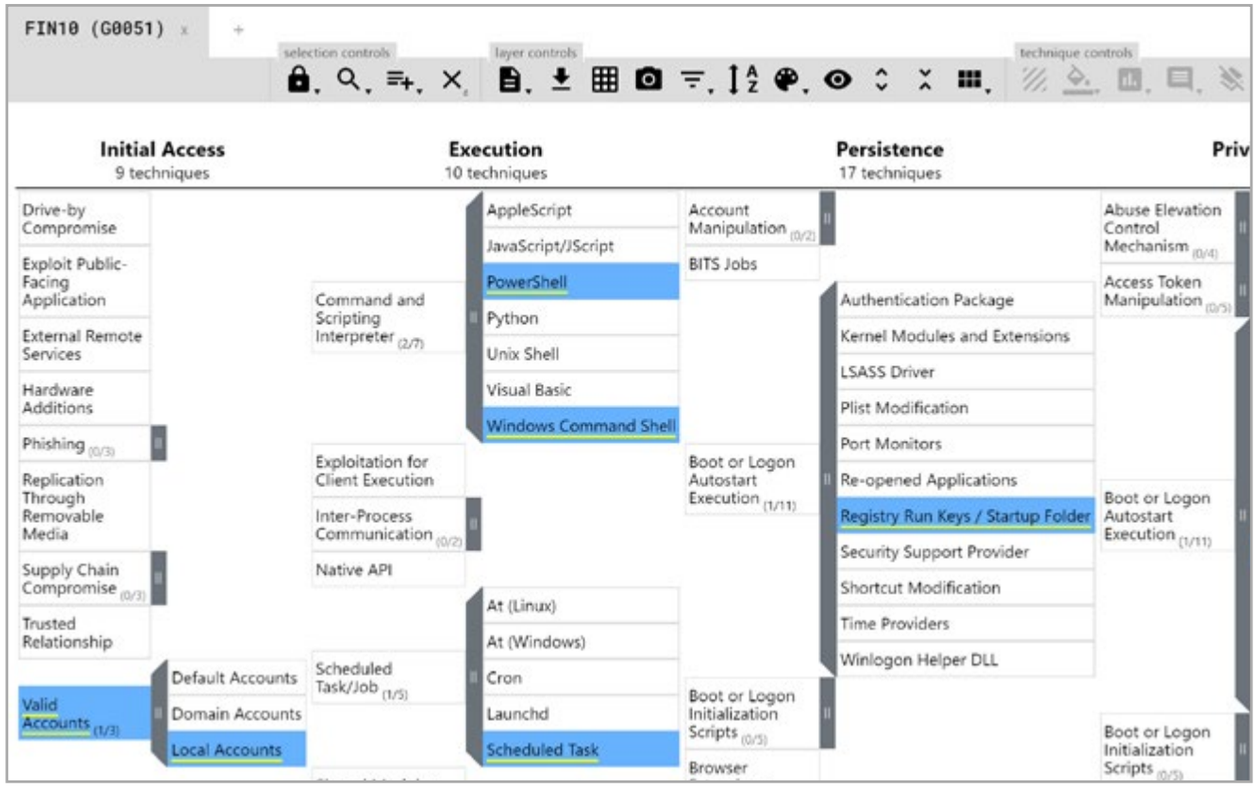
Example FIN4 Attack										
Initial Access	**Execution**	**Persistence**	**Privilege Escalation**	**Defense Evasion**	**Credential Access**	**Discovery**	**Lateral Movement**	**Collection**	**Command And Control**	**Exfiltration**
Spearphishing Link	Scheduled Task	Scheduled Task	Valid Accounts	Software Packing	Input Capture	Account Discovery	Pass the Hash	Image Capture	Uncommonly used Port	Data Compressed
	User Execution				Input Prompt	File and Directory Discovery			Data Encoding	Data Encrypted
						Process Discovery				Exfiltration Over Command and Control Channel
 **E-mail Link - Fileless Attack**	 **User Execution**	 **Scheduled Task**	 **Valid Accounts**	 **Software Packing**	 **Input Prompt**	 **System Information Discovery**	 **Pass the Hash**	 **Image Capture**	 **Data Encoding**	 **Data Encrypted**

FIN10

This group of attackers used publicly known tools and techniques to compromise Canadian-based casinos and natural resources companies, with a view to extorting funds by threatening to release stolen data publicly.

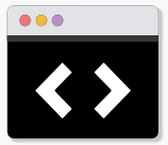
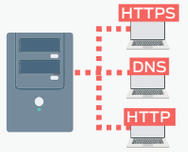
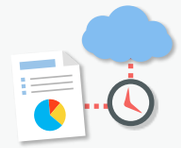
Spear phishing emails combined with Metasploit, PowerShell scripts and the SplinterRat remote access tool were used in combination.

References:
https://attack.mitre.org/groups/G0051/



Attacker techniques documented by the MITRE ATT&CK framework.

Example FIN10 Attack

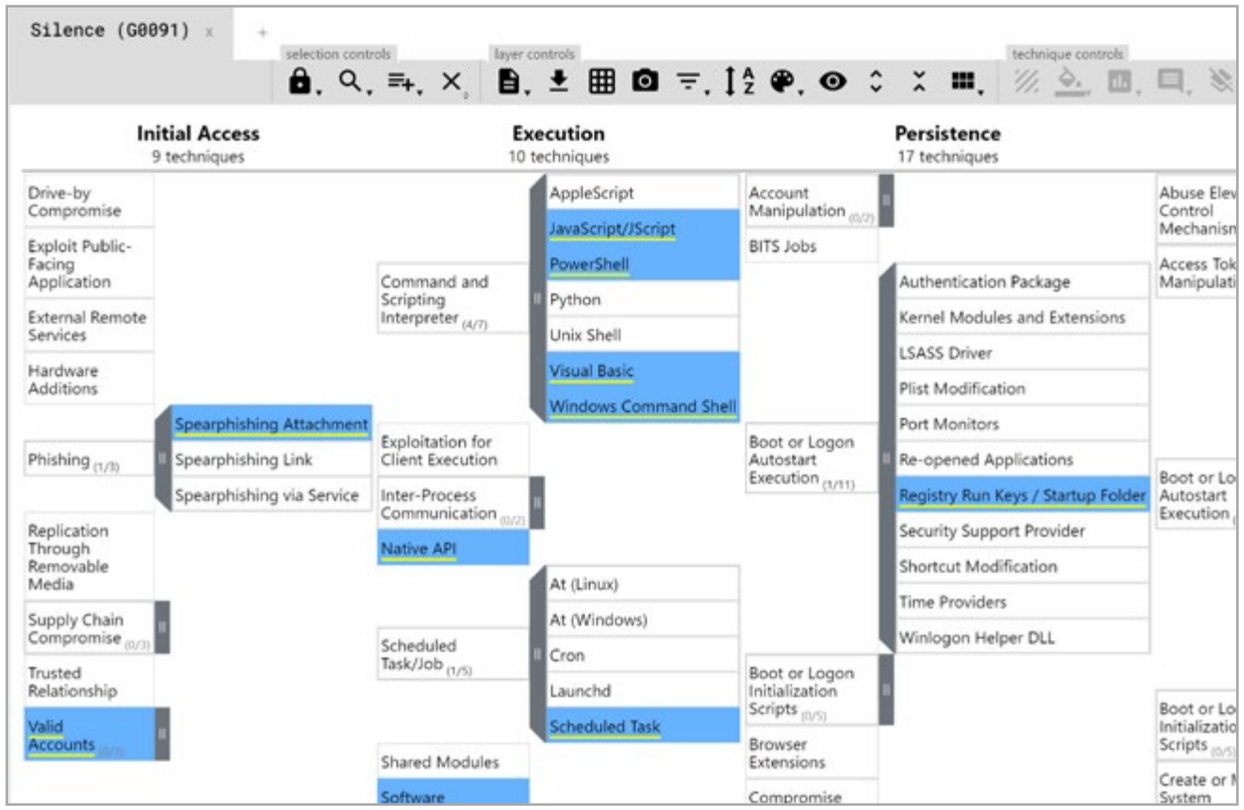
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration
Spearphishing Link	mshta	Registry Ru Key / Start Folder	Scheduled Tasks	Scripting	No credential access seen in research for FIN10.	Account Discovery	Remote Desktop Protocol	Automated Collection	Commonly Used Port	Scheduled Transfer
	Scripting		Valid Accounts			File and Directory Discovery				
	User Execution					Process Discovery				
						System Information Discovery				
						System Owner/User Discovery				
 E-mail Link - Fileless Attack	 mshta	 Registry Ru Key/ Start Folder	 Valid Accounts	 Scripting		 Process Discovery	 Remote Desktop Protocol	 Automated Collection	 Commonly Used Port	 Scheduled Transfer

Silence

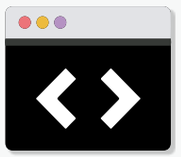
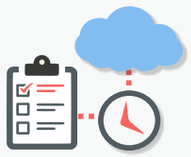
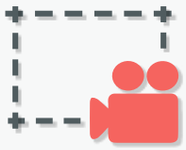
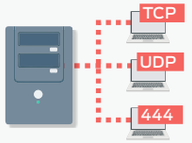
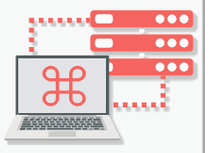
Largely focussed on script-based attacks using .CHM and .LNK files, as well as macros and other exploits, the Silence group targeted banking organisations with malicious Microsoft Office documents.

While targets have been distributed globally, the group has historically paid particular attention to Eastern European countries, with ATMs as specific targets.

References:
https://attack.mitre.org/groups/G0091/



Attacker techniques documented by the MITRE ATT&CK framework.

Example Silence Attack										
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration
Spearphishing Attachment	Scripting	Scheduled Task	Scheduled Task	File Deletion	No Credential Access techniques seen in research for Silence.	Network Share Discovery	Windows Admin Shares	Video Capture	Uncommonly Used Port	Exfiltration Over Command and Control Channel
	Service Execution			Obfuscated Files or Information		Remote Share Discovery				
	User Execution			Scripting						
 E-mail Link - Fileless Attack	 Scripting	 Scheduled Task	 Scheduled Task	 File Deletion		 Network Share Discovery	 Windows Admin Shares	 Video Capture	 Uncommonly Used Port	 Exfiltration Over Command and Control Channel

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 (%)
Crowdstrike Falcon	396	100%

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

6. Conclusions

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

All of these attack types have been witnessed in real-world attacks over the previous few years. They are representative of a real and present threat to business networks the world over. The threats used in this are similar or identical to those used by the threat groups listed in **Hackers vs. Targets** on page 9 and **4. Threat Intelligence** on pages 13 - 16.

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 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.

The product detected and protected fully against all of the threats. In every case the threats were unable to move beyond the earliest stages of the attack chain, meaning that as soon as the target systems were exposed to the threats, the attacks were detected immediately and were blocked from running. This prevented them from causing any damage, including data theft.

The results are strong and not one attack could progress far enough to the point at which the testers could start hacking through the targets. Sometimes products are overly aggressive and detect everything, including threats and legitimate objects. In this test **Crowdstrike Falcon** generated no such false positive results, which is as hoped. **Crowdstrike Falcon** 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 12th November and 3rd December 2020.
- 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 endpoint security testing on physical PCs, not virtual machines.

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

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

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

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

APPENDIX C: Attack Details

FIN7											
Incident No:	**Initial Access**	**Execution**	**Persistence**	**Privilege Escalation**	**Defense Evasion**	**Credential Access**	**Discovery**	**Lateral Movement**	**Collection**	**Command And Control**	**Exfiltration**
1	Spearphishing Attachment	Command-Line Interface	New Service	Bypass UAC	Obfuscated Files or Information	Credential Dumping	Account Discovery	Remote File Copy	Data from Local System	Commonly Used Port	Data Compressed
		Powershell	Scheduled Task	Valid Accounts	Modify Registry	Input Capture	File and Directory Discovery	Pass the Hash	Data Staged	Standard Application Layer Protocol	Data Encrypted
		Scripting			File Deletion		Process Discovery		Input Capture	Standard Cryptographic Protocol	Exfiltration over Command and Control Channel
		Remote File Copy			Process Hollowing		Query Registry				
		User Execution			Virtulisation/ Sandbox Evasion		System Information Discovery				
							System Owner/User Discovery				
2	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				
3	Spearphishing Attachment	Command-Line Interface	Application Shimming	Bypass UAC	Deobfuscate Files or Information	Brute Force	File and Directory Discovery	Remote File Copy	Data from Local System	Commonly Used Port	Data Compressed
		mshta			Execution Guardrails	Credential Dumping	Process Discovery	Pass the Hash	Data Staged	Connection Proxy	Data Encrypted
		User Execution			Software Packing		System Information Discovery	Windows Admin Shares		Standard Non-Application Layer Protocol	Exfiltration over Command and Control Channel
		Scripting					Network Share Discovery				
							System Network Configuration Discovery				
							System Owner/User Discovery				
							Account Discovery				

FIN7

Incident No:	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration
4	Spearphishing Attachment	Command-Line Interface	Hooking	DLL Search Order Hijacking	Indirect Command Execution [NEW]	Hooking	File and Directory Discovery	Windows Management Instrumentation [NEW]	Data from Local System	Commonly Used Port	Data Compressed
		Powershell			File Deletion	Input Capture	Process Discovery		Data Staged	Standard Application Layer Protocol	Data Encrypted
		Scripting			Execution Guardrails		System Information Discovery			Standard Cryptographic Protocol	Exfiltration over Command and Control Channel
		Component Object Model and Distributed COM					Application Windows Discovery				
		Execution through API					Permission Groups Discovery				
							Network Share Discovery				

FIN4

Incident No:	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration
5	Spearphishing Attachment	Scripting	New Service	Valid Accounts	Scripting	Input Capture	Account Discovery	Remote Desktop Protocol	Email Collection	Commonly Used Port	Automated Exfiltration
		User Execution				Input Prompt	File and Directory Discovery			Standard Application Layer Protocol	Exfiltration Over Alternative Protocol
							Process Discovery				Data Transfer Size Limits
							System Information Discovery				
6	Spearphishing Link	Scheduled Task	Scheduled Task	Valid Accounts	Software Packing	Input Capture	Account Discovery	Pass the Hash	Image Capture	Uncommonly used Port	Data Compressed
		User Execution				Input Prompt	File and Directory Discovery			Data Encoding	Data Encrypted
							Process Discovery				Exfiltration Over Command and Control Channel
							System Information Discovery				
7	Spearphishing Attachment	Regsvcs/Regasm	New Service	Valid Accounts	Process Injection	Input Capture	Account Discovery	Remote File Copy	Image Capture	Standard Application Layer Protocol	Scheduled Transfer
		User Execution				Input Prompt	File and Directory Discovery			Process Injection	Exfiltration Over Alternative Protocol
							Process Discovery			Commonly Used Port	
							System Information Discovery				
8	Spearphishing Link	Scripting	Start Up Items	Valid Accounts	Scripting	Input Capture		Remote File Copy	Email Collection	Uncommonly used Port	Data Compressed
		User Execution				Input Prompt				Web Service	Data Encrypted
											Exfiltration Command and Control Channel

FIN10											
Incident No:	**Initial Access**	**Execution**	**Persistence**	**Privilege Escalation**	**Defense Evasion**	**Credential Access**	**Discovery**	**Lateral Movement**	**Collection**	**Command And Control**	**Exfiltration**
9	Spearphishing Attachment	User Execution	Scheduled Tasks	Scheduled Tasks Valid Accounts	File Deletion	No credential access seen in research for FIN10.	Account Discovery File and Directory Discovery Process Discovery System Information Discovery System Owner/User Discovery	Remote File Copy	Data from Local System Data Staged	Commonly Used Port	Exfiltration Over Command and Control Channel
10	Spearphishing Link	mshta Scripting User Execution	Registry Ru Key / Start Folder	Scheduled Tasks Valid Accounts	Scripting	No credential access seen in research for FIN10.	Account Discovery File and Directory Discovery Process Discovery System Information Discovery System Owner/User Discovery	Remote Desktop Protocol	Automated Collection	Commonly Used Port	Scheduled Transfer
11	Spearphishing Link	Powershell Scripting Regsvcs/Regasm User Execution	Scheduled Tasks	Scheduled Tasks Valid Accounts	Regsvcs/Regasm Scripting	No credential access seen in research for FIN10.	Account Discovery File and Directory Discovery Process Discovery System Information Discovery System Owner/User Discovery	Remote File Copy	Automated Collection	Commonly Used Port	Scheduled Transfer

Silence											
Incident No:	**Initial Access**	**Execution**	**Persistence**	**Privilege Escalation**	**Defense Evasion**	**Credential Access**	**Discovery**	**Lateral Movement**	**Collection**	**Command And Control**	**Exfiltration**
12	Spearphishing Attachment	Command-Line Interface Compiled HTML File Execution through API User Execution	Scheduled Task	Scheduled Task	Compiled HTML File File Deletion	No Credential Access techniques seen in research for Silence.	Network Share Discovery Remote Share Discovery	Windows Admin Shares	Screen Capture	Commonly Used Port	Exfiltration Over Command and Control Channel
13	Spearphishing Attachment	Scripting Service Execution User Execution	Scheduled Task	Scheduled Task	File Deletion Obfuscated Files or Information Scripting	No Credential Access techniques seen in research for Silence.	Network Share Discovery Remote Share Discovery	Windows Admin Shares	Video Capture	Uncommonly Used Port	Exfiltration Over Command and Control Channel

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.