SE Labs

INTELLIGENCE-LED TESTING

Breach Response Test

Protection Mode

SentinelOne

August 2020

www.SELabs.uk info@SELabs.uk @SELabsUK www.facebook.com/selabsuk blog.selabs.uk

SE Labs tested **SentinelOne** 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
Dimitar Dobrev
Liam Fisher
Gia Gorbold
Joseph Pike
Dave Togneri
Jake Warren
Stephen Withey

IT SUPPORT
Danny King-Smith
Chris Short

PUBLICATION
Steve Haines
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 20th August 2020

INTRODUCTION

Testing Threat Detection, Protection and Response

Why it's possible to compare security products that work in very different ways

Testing breach response products is a complex business, which is why we now have two types of breach response test report. Some products focus primarily on detecting threats and enabling threat hunters, while others emphasise protection against the threats. For threat detection and hunting we produce reports in 'EDR mode' while, for products such as SentinelOne, we publish 'Protection mode' reports like this one.

In this report we explain the threats used and explore how the tested product interacts with them. You might notice a similarity between the way we present this information and the way that the MITRE ATT&CK framework illustrates threat chains. This is not a coincidence. Our goal is to share information in ways that are familiar and easily understandable by the security community and its customers.

Regardless of the report's format (EDR or Protection mode), we assess a product's efforts at handling each logical stage of an attack, those being:

- Detection
- Delivery
- Execution
- Action
- Escalation
- Post-escalation action
- Lateral Movement and
- Lateral Action.

In some cases, we might test a product on a system that has already been compromised. There is one such 'pre-infected' included in this report, that being the FIN4 APT group. When this happens we skip measuring a product's abilities to detect threat delivery and execution, because that happened before it was installed!

By using full attack chain testing with well-known ways of describing threats it is possible to test a wide range of endpoint security, 'EDR' and other anti-hacker security solutions and produce comparable results, in turn making purchasing (or change) decisions easier and better informed.

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

SentinelOne 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.

SentinelOne 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 (%)
SentinelOne	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:

SE Labs

AAA

AUGUST 2020

BREACH RESPONSE (PROTECT)

SentinelOne

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.

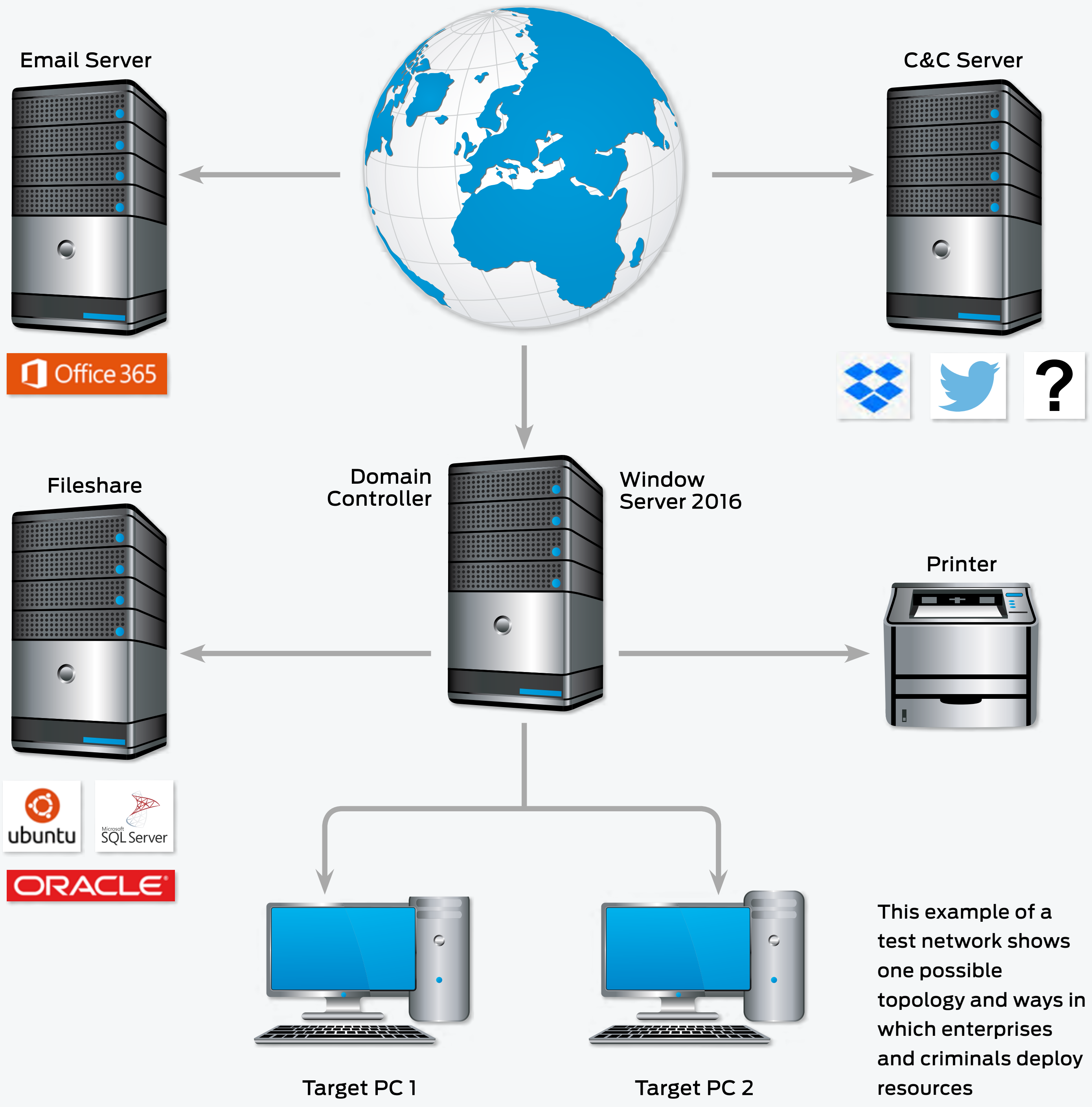
In the diagram on the right you will see an example network that contains workstations, some basic infrastructure such as file servers and a domain controller, as well as cloud-based email and a malicious command and control (C&C) server, which may be a conventional computer or a service such as Dropbox,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

ATTACK CHAIN STAGES

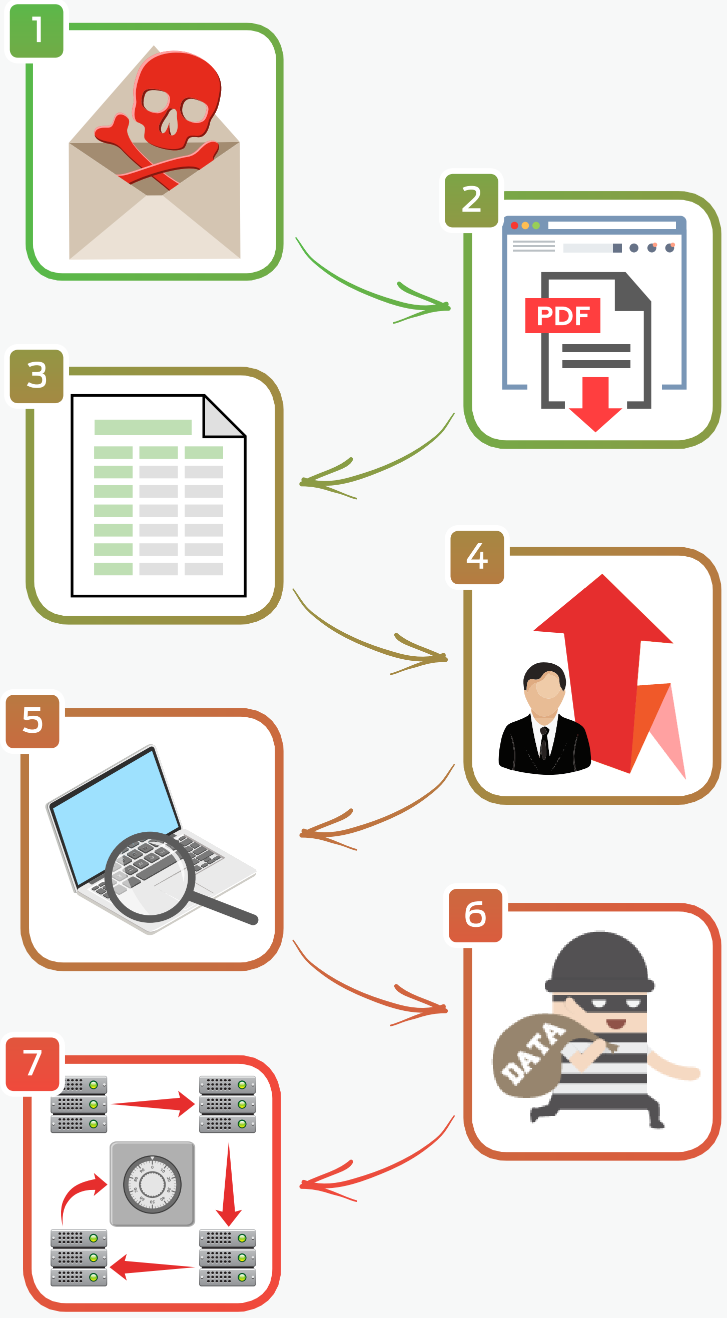


Figure 1. A typical attack starts with an initial contact and progresses through various stages, including reconnaissance, stealing data and causing damage.

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

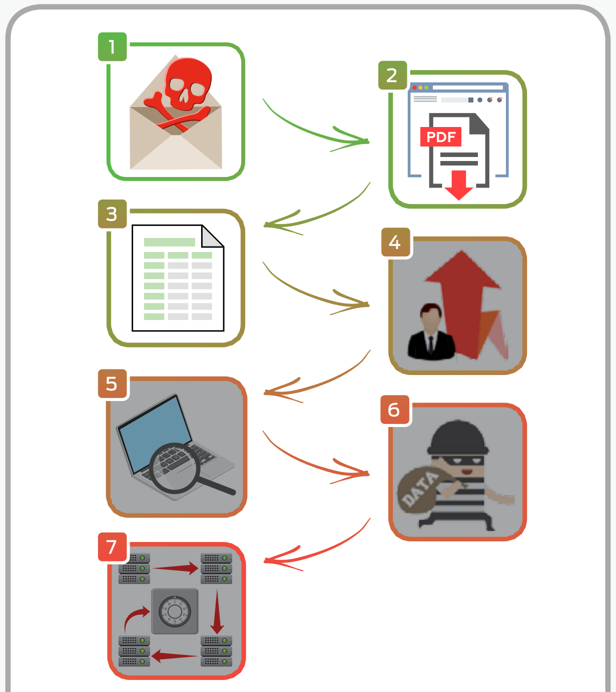


Figure 2. This attack was initially successful but only able to progress as far as the reconnaissance phase.

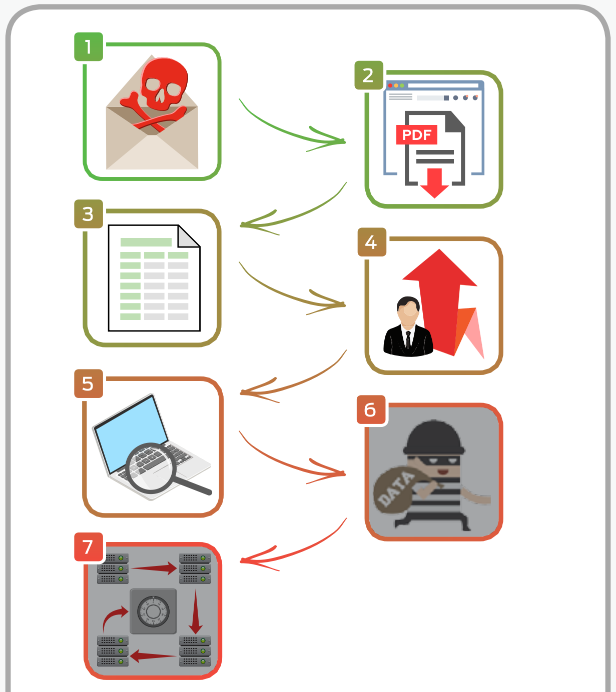


Figure 3. A more successful attack manages to steal passwords but wholesale data theft and destruction was blocked.

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	W	🛒	Documents containing hidden links to scripts
FIN4	X W X W	📈	Man-in-the-middle spear phishing
FIN10	⚙ M	🎲 🛢	Spear phishing emails combined with public attack tools
Silence	X W	🏦	Documents containing scripts, links and exploits

Key

✈ Aviation	🏦 Banking and ATMs	🏛 Democratic National Comittee
🏭 Energy	📈 Financial Market	🎲 Gambling
🏛 Government Espionage	🛢 Natural Resources	🛒 US Retail, Restaurant and Hospitality

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.

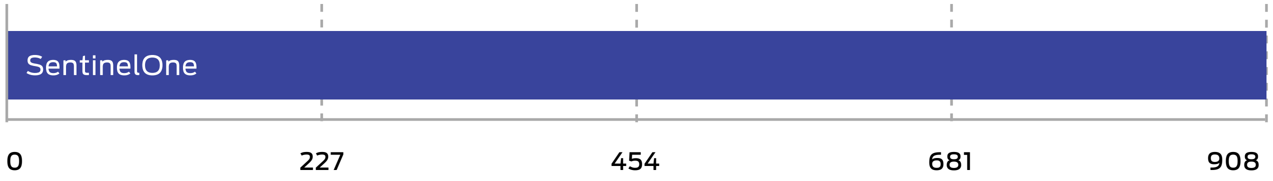
Not all protections, or detections for that matter, are equal. A product might completely block a URL, which stops the threat before it can even start its intended series of malicious events. Alternatively, the product might allow a web-based exploit to execute but prevent it from downloading any further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

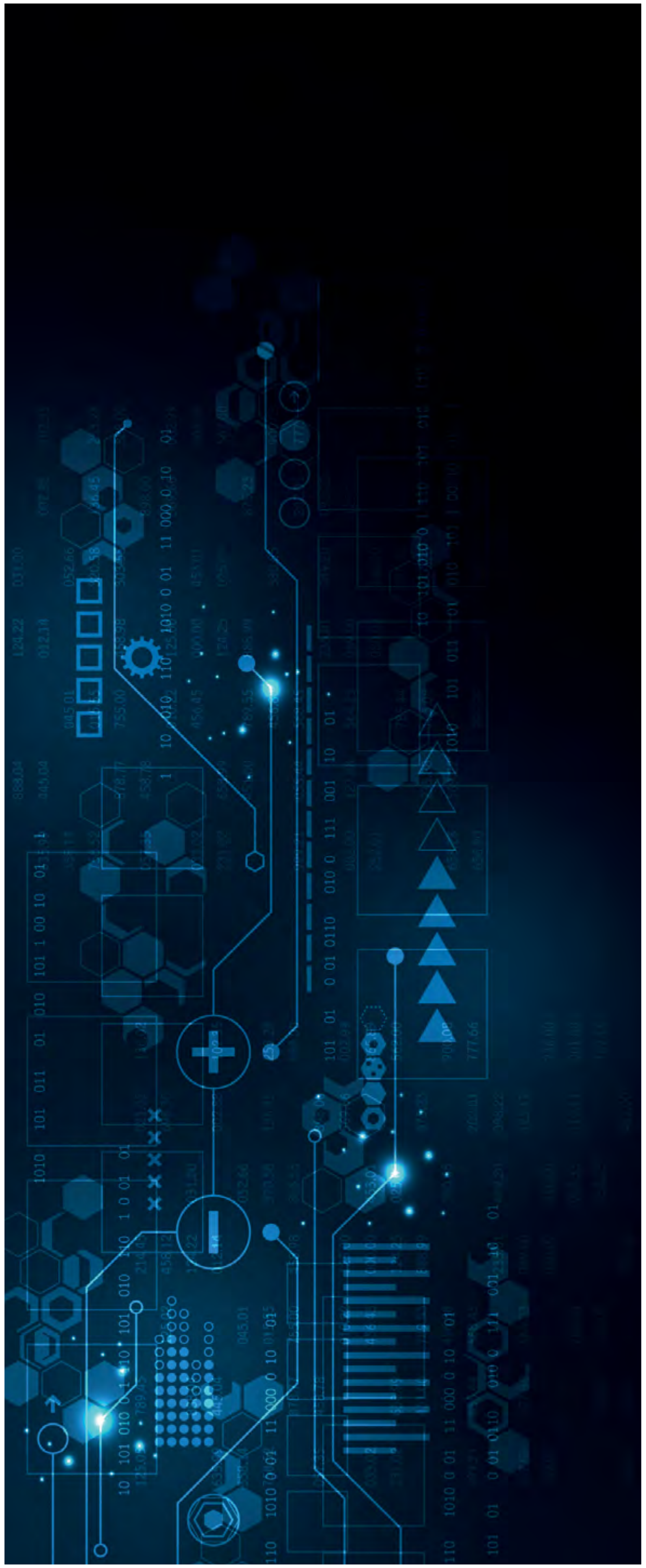
Scoring a product's response to a potential breach requires a granular method, which we outline in **3. Response Details** on page 11.

Total Accuracy Ratings

Product	Total Accuracy Rating	Total Accuracy (%)	Award
SentinelOne	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 (%)
SentinelOne	512	100%

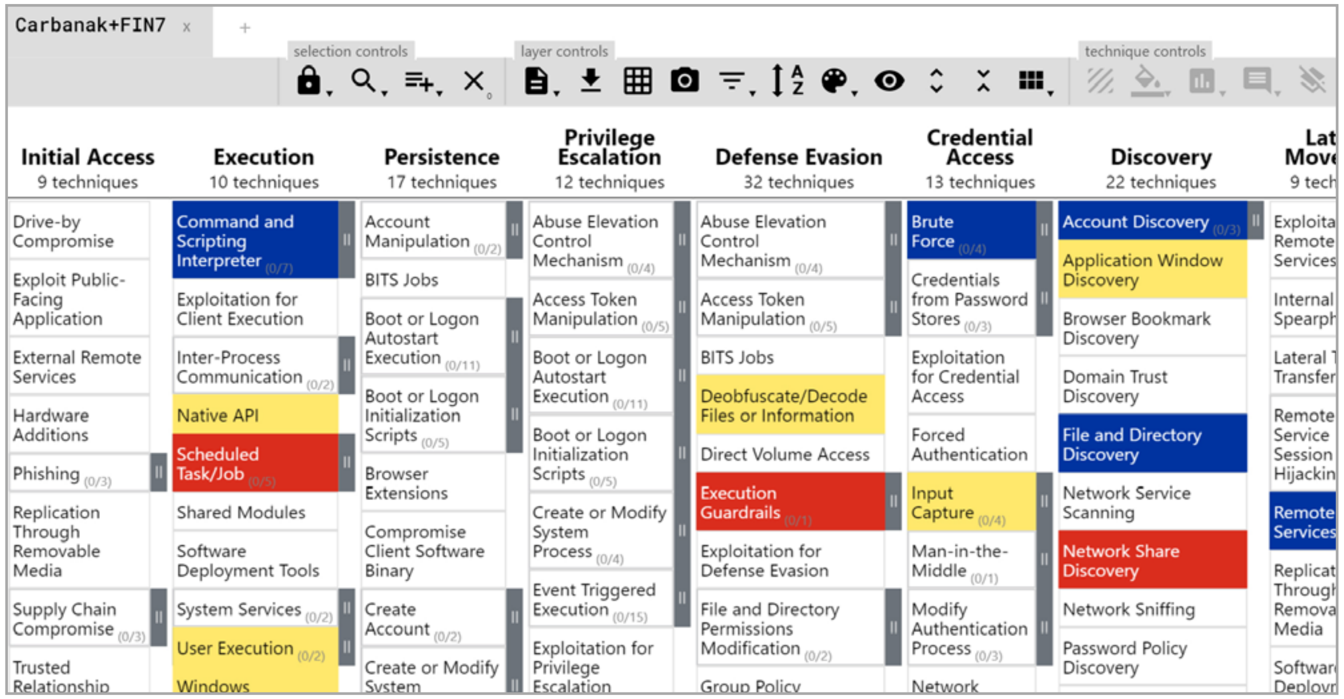
Protection Ratings are weighted to show that how products handle threats can be subtler than just ‘win’ or ‘lose’.

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/



Initial Access 9 techniques	Execution 10 techniques	Persistence 17 techniques	Privilege Escalation 12 techniques	Defense Evasion 32 techniques	Credential Access 13 techniques	Discovery 22 techniques	Lat Move 9 tech
Drive-by Compromise	Command and Scripting Interpreter (0/7)	Account Manipulation (0/2)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Brute Force (0/4)	Account Discovery (0/3)	Exploita Remote Services
Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Credentials from Password Stores (0/3)	Application Window Discovery	Internal Spearph
External Remote Services	Inter-Process Communication (0/2)	Boot or Logon Autostart Execution (0/11)	Boot or Logon Autostart Execution (0/11)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral T Transfer
Hardware Additions	Native API	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Deobfuscate/Decode Files or Information	Forced Authentication	Domain Trust Discovery	Remote Service Session Hijackin
Phishing (0/3)	Scheduled Task/Job (0/5)	Browser Extensions	Create or Modify System Process (0/4)	Direct Volume Access	Input Capture (0/4)	File and Directory Discovery	Remote Services
Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Event Triggered Execution (0/15)	Execution Guardrails (0/1)	Man-in-the-Middle (0/1)	Network Service Scanning	Replicat Through Remova Media
Supply Chain Compromise (0/3)	Software Deployment Tools	Create Account (0/2)	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Modify Authentication Process (0/3)	Network Share Discovery	Softwar Deployn
Trusted Relationship	System Services (0/2)	Create or Modify System		File and Directory Permissions Modification (0/2)	Network	Network Sniffing	
	User Execution (0/2)			Group Policy		Password Policy Discovery	
	Windows						

Attacker techniques documented by the MITRE ATT&CK framework

Example FIN7 Attack

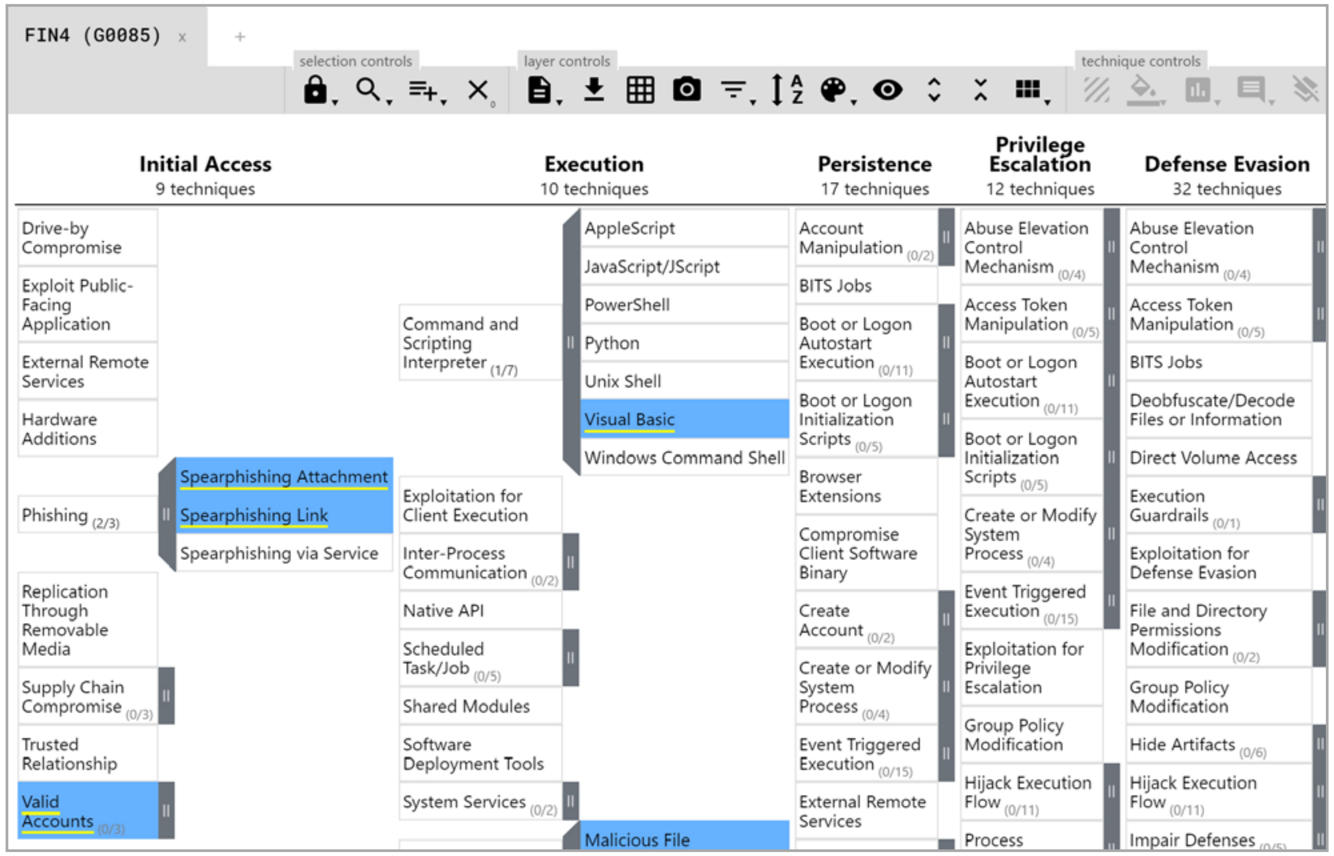
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration
Spearphishing Attachment	Command-Line Interface	Registry Run Keys / Startup Folder	Bypass UAC	Code Signing	Brute Force	File and Directory 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/



FIN4 (G0085)

selection controls · layer controls · technique controls

Initial Access (9 techniques): Drive-by Compromise; Exploit Public-Facing Application; External Remote Services; Hardware Additions; Phishing (2/3): Spearphishing Attachment, Spearphishing Link, Spearphishing via Service; Replication Through Removable Media; Supply Chain Compromise (0/3); Trusted Relationship; Valid Accounts (0/3)

Execution (10 techniques): Command and Scripting Interpreter (1/7): AppleScript, JavaScript/JScript, PowerShell, Python, Unix Shell, Visual Basic, Windows Command Shell; Exploitation for Client Execution; Inter-Process Communication (0/2); Native API; Scheduled Task/Job (0/5); Shared Modules; Software Deployment Tools; System Services (0/2); Malicious File

Persistence (17 techniques): Account Manipulation (0/2); BITS Jobs; Boot or Logon Autostart Execution (0/11); Boot or Logon Initialization Scripts (0/5); Browser Extensions; Compromise Client Software Binary; Create Account (0/2); Create or Modify System Process (0/4); Event Triggered Execution (0/15); External Remote Services

Privilege Escalation (12 techniques): Abuse Elevation Control Mechanism (0/4); Access Token Manipulation (0/5); Boot or Logon Autostart Execution (0/11); Boot or Logon Initialization Scripts (0/5); Create or Modify System Process (0/4); Event Triggered Execution (0/15); Exploitation for Privilege Escalation; Group Policy Modification; Hijack Execution Flow (0/11); Process

Defense Evasion (32 techniques): Abuse Elevation Control Mechanism (0/4); Access Token Manipulation (0/5); BITS Jobs; Deobfuscate/Decode Files or Information; Direct Volume Access; Execution Guardrails (0/1); Exploitation for Defense Evasion; File and Directory Permissions Modification (0/2); Group Policy Modification; Hide Artifacts (0/6); Hijack Execution Flow (0/11); Impair Defenses

Attacker techniques documented by the MITRE ATT&CK framework.

Example FIN4 Attack

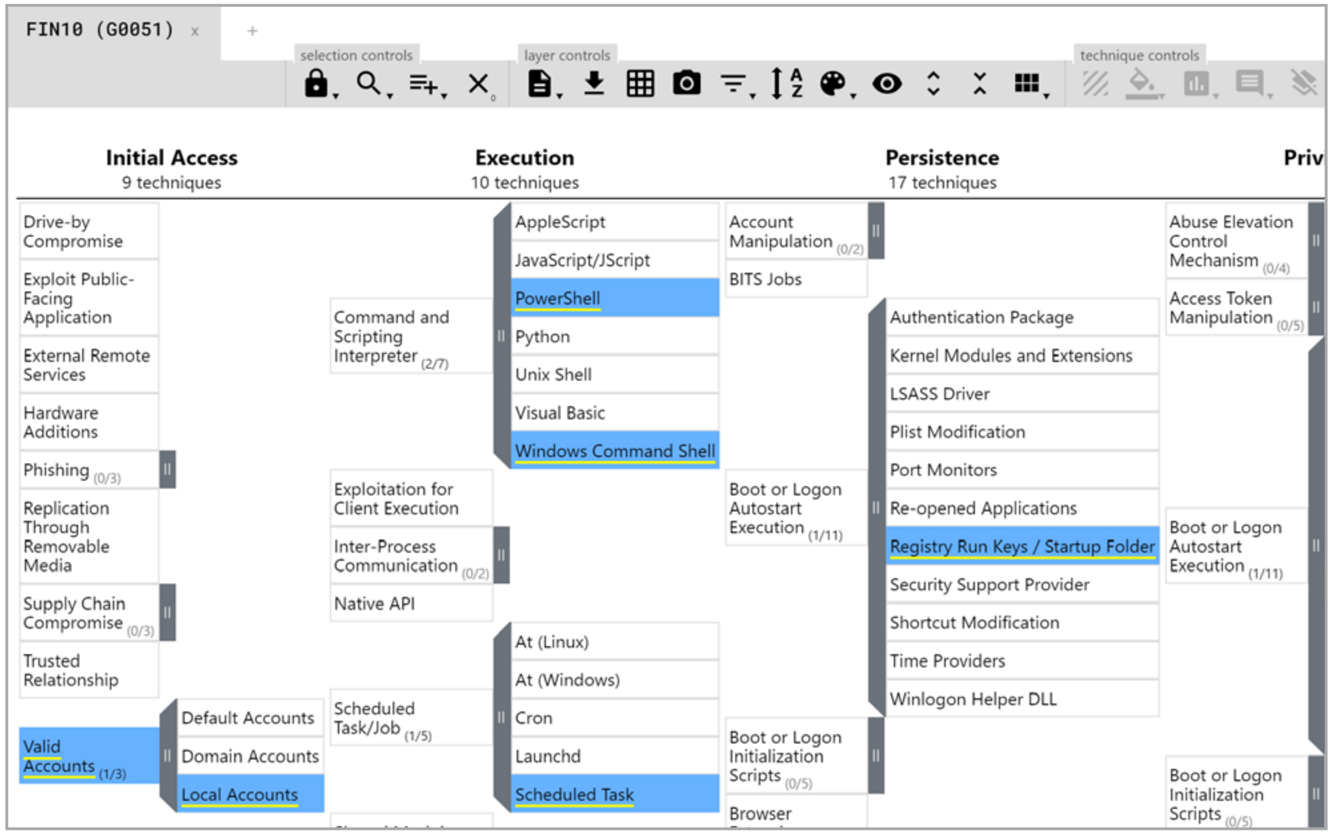
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration
Spearphishing Link	Scheduled Task	Scheduled Task	Valid Accounts	Software Packing	Input Capture	Account Discovery	Pass the Hash	Image Capture	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
						System Information Discovery				
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/



Initial Access 9 techniques

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (0/3)
- Replication Through Removable Media
- Supply Chain Compromise (0/3)
- Trusted Relationship
- Valid Accounts (1/3)
  - Default Accounts
  - Domain Accounts
  - Local Accounts

Execution 10 techniques

- Command and Scripting Interpreter (2/7)
  - AppleScript
  - JavaScript/JScript
  - PowerShell
  - Python
  - Unix Shell
  - Visual Basic
  - Windows Command Shell
- Exploitation for Client Execution
- Inter-Process Communication (0/2)
- Native API
- Scheduled Task/Job (1/5)
  - At (Linux)
  - At (Windows)
  - Cron
  - Launchd
  - Scheduled Task

Persistence 17 techniques

- Account Manipulation (0/2)
- BITS Jobs
- Boot or Logon Autostart Execution (1/11)
  - Authentication Package
  - Kernel Modules and Extensions
  - LSASS Driver
  - Plist Modification
  - Port Monitors
  - Re-opened Applications
  - Registry Run Keys / Startup Folder
  - Security Support Provider
  - Shortcut Modification
  - Time Providers
  - Winlogon Helper DLL
- Boot or Logon Initialization Scripts (0/5)
- Browser

Priv

- Abuse Elevation Control Mechanism (0/4)
- Access Token Manipulation (0/5)
- Boot or Logon Autostart Execution (1/11)
- Boot or Logon Initialization Scripts (0/5)

Attacker techniques documented by the MITRE ATT&CK framework.

Example FIN10 Attack

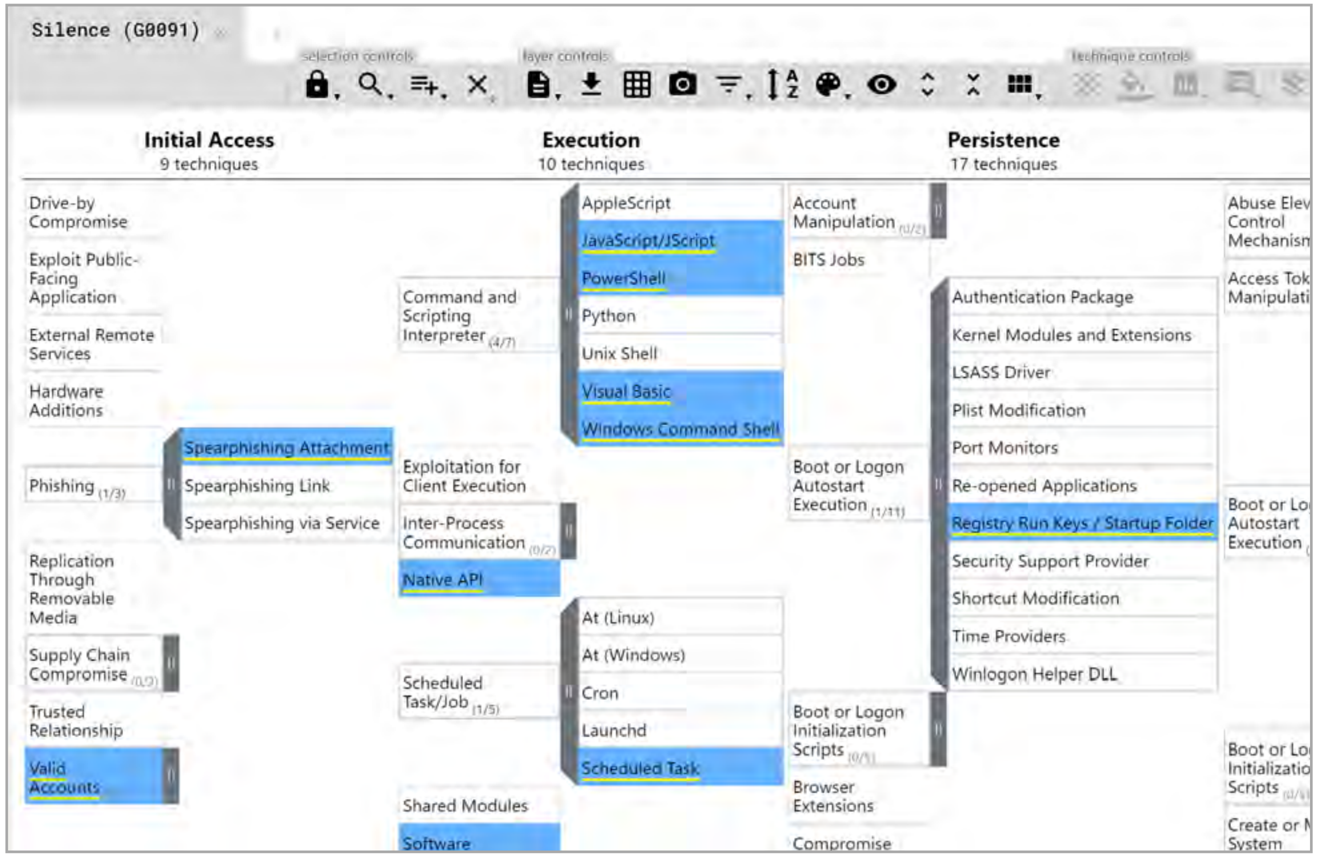
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration
Spearphishing Link	mshta Scripting User Execution	Registry Ru Key / Start Folder	Scheduled Tasks Valid Accounts	Scripting	No credential access 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
E-mail Link - Fileless Attack	mshta.exe mshta	Registry Ru Key/ Start Folder	Valid Accounts	Scripting		Process Discovery	Remote Desktop Protocol	Automated Collection	HTTPS DNS HTTP 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/



Silence (G0091)

Initial Access
9 techniques

Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing (1/3)
- Spearphishing Attachment
- Spearphishing Link
- Spearphishing via Service

Replication Through Removable Media
Supply Chain Compromise (0/3)
Trusted Relationship
Valid Accounts

Execution
10 techniques

Command and Scripting Interpreter (4/7)
- AppleScript
- JavaScript/JScript
- PowerShell
- Python
- Unix Shell
- Visual Basic
- Windows Command Shell

Exploitation for Client Execution
Inter-Process Communication (0/2)
Native API
Scheduled Task/Job (1/5)
- At (Linux)
- At (Windows)
- Cron
- Launchd
- Scheduled Task

Shared Modules
Software

Persistence
17 techniques

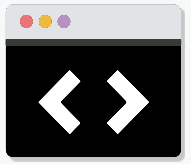
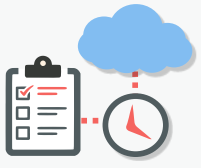
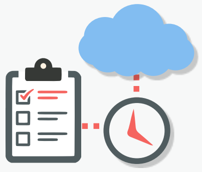
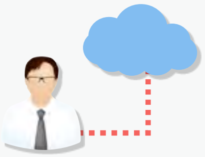
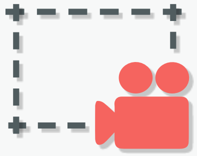
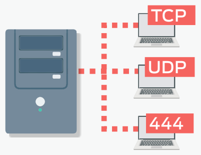
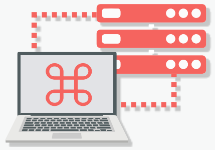
Account Manipulation (0/2)
BITS Jobs
Boot or Logon Autostart Execution (1/11)
- Authentication Package
- Kernel Modules and Extensions
- LSASS Driver
- Plist Modification
- Port Monitors
- Re-opened Applications
- Registry Run Keys / Startup Folder
- Security Support Provider
- Shortcut Modification
- Time Providers
- Winlogon Helper DLL

Boot or Logon Initialization Scripts (0/5)
Browser Extensions
Compromise

Abuse Elev
Control
Mechanism
Access Tok
Manipulati
Boot or Lo
Autostart
Execution
Boot or Lo
Initializatio
Scripts
Create or M
System

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 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
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

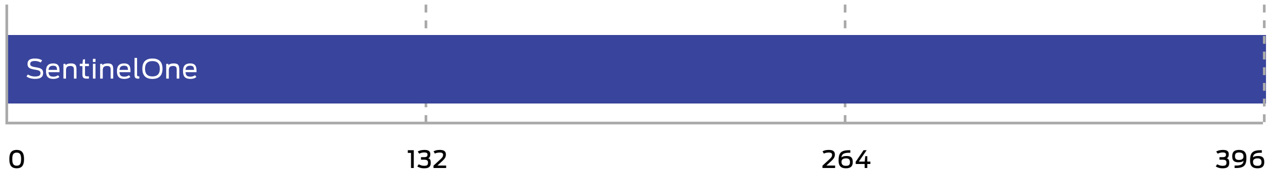
5. Legitimate Software Rating

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 (%)
SentinelOne	396	100%



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

6. Conclusions

This test exposed SentinelOne 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 SentinelOne generated no such false positive results, which is as hoped. SentinelOne 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 30th June and 19th July 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 Powershell Scripting Component Object Model and Distributed COM Execution through API	Hooking	DLL Search Order Hijacking	Indirect Command Execution [NEW] File Deletion Execution Guardrails	Hooking Input Capture	File and Directory Discovery Process Discovery System Information Discovery Application Windows Discovery Permission Groups Discovery Network Share Discovery	Windows Management Instrumentation [NEW]	Data from Local System Data Staged	Commonly Used Port Standard Application Layer Protocol Standard Cryptographic Protocol	Data Compressed Data Encrypted Exfiltration over Command and Control Channel

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 User Execution	New Service	Valid Accounts	Scripting	Input Capture Input Prompt	Account Discovery File and Directory Discovery Process Discovery System Information Discovery	Remote Desktop Protocol	Email Collection	Commonly Used Port Standard Application Layer Protocol	Automated Exfiltration Exfiltration Over Alternative Protocol Data Transfer Size Limits
6	Spearphishing Link	Scheduled Task User Execution	Scheduled Task	Valid Accounts	Software Packing	Input Capture Input Prompt	Account Discovery File and Directory Discovery Process Discovery System Information Discovery	Pass the Hash	Image Capture	Uncommonly used Port Data Encoding	Data Compressed Data Encrypted Exfiltration Over Command and Control Channel
7	Spearphishing Attachment	Regsvcs/Regasm User Execution	New Service	Valid Accounts	Process Injection	Input Capture Input Prompt	Account Discovery File and Directory Discovery Process Discovery System Information Discovery	Remote File Copy	Image Capture	Standard Application Layer Protocol Process Injection Commonly Used Port	Scheduled Transfer Exfiltration Over Alternative Protocol
8	Spearphishing Link	Scripting User Execution	Start Up Items	Valid Accounts	Scripting	Input Capture Input Prompt		Remote File Copy	Email Collection	Uncommonly used Port Web Service	Data Compressed 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.