

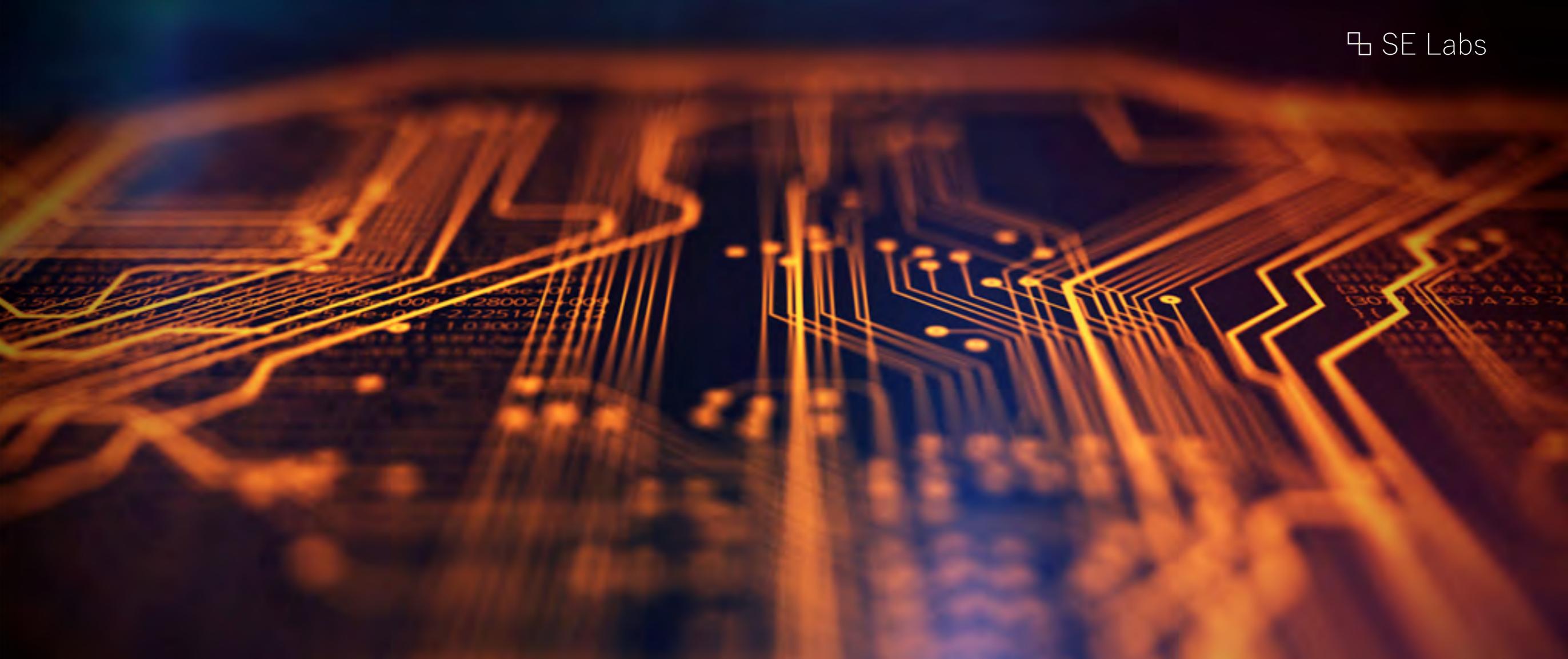


INTELLIGENCE-LED TESTING

Breach Response Test Detection Mode

CrowdStrike Falcon

August 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
 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 (M3AAG).

© 2020 SE Labs Ltd

CONTENTS

Introduction	04
Executive Summary	05
Breach Response Award	05
1. How We Tested	06
Threat Responses	07
Hackers vs. Targets	09
2. Total Accuracy Ratings	10
3. Response Details	11
4. Threat Intelligence	13
APT3	13
APT29	14
APT33	15
APT34	16
5. Legitimate Software Rating	17
6. Conclusions	18
Appendices	19
Appendix A: Terms Used	19
Appendix B: FAQs	19
Appendix C: Attack Details	20

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. Some can do both. To illustrate abilities in threat detection and hunting we produce Detection-mode (aka Endpoint Detection and Response (EDR)) reports like this one, while our 'Protection mode' reports focus on system protection.

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. When this happens we skip measuring a product's abilities to detect 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

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

CrowdStrike Falcon was able to detect every targeted attack and, in most cases, tracked each main element, particularly when the hostile activities occurred on the endpoint running the Falcon agent.

Executive Summary				
Product Tested	Attacks Detected	Detection Accuracy (%)	Legitimate Accuracy Rating (%)	Total Accuracy Rating (%)
CrowdStrike Falcon	100%	81%	100%	92%

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

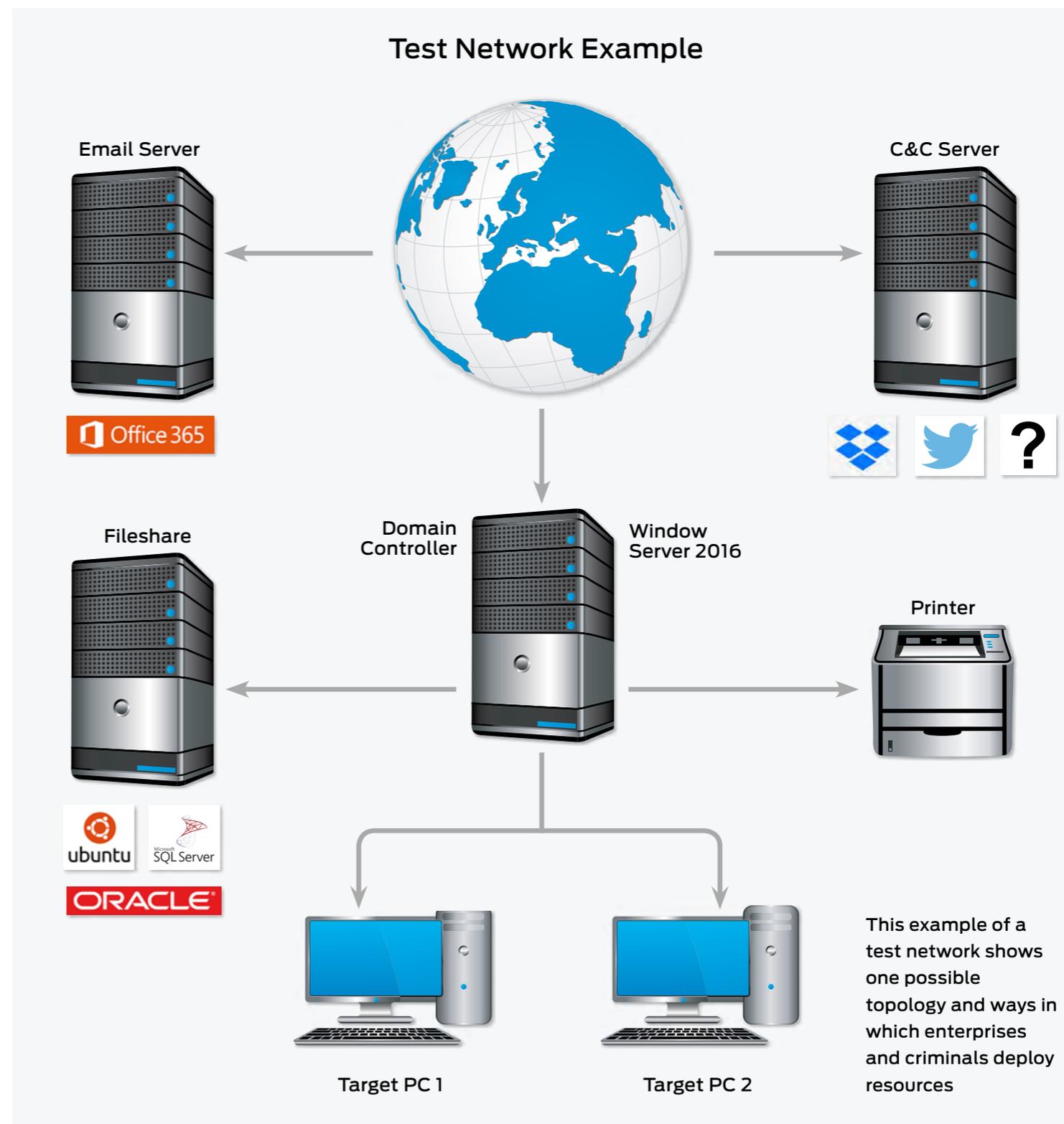
Testers can't assume that products will work a certain way, so running a realistic breach response test means setting up real networks and hacking them in the same way that real adversaries behave.

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 contain them in a 'quarantine' or other safe holding mechanism for later analysis.

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

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.

EMAIL SECURITY SERVICES PROTECTION

Which services from well-known vendors are the **most** effective?

SE Labs
INTELLIGENCE-LED TESTING

EMAIL SECURITY SERVICES PROTECTION
JAN - MAR 2020

www.SELabs.uk | info@SELabs.uk | @SELabsUK | www.facebook.com/selabsuk

DOWNLOAD NOW!

selabs.uk/essp2020

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
APT3	 		Spear phishing emails containing scripts
APT29	 		Spear phishing emails containing scripts or links to malware
APT33	 	 	Documents containing scripts combined with public tools
APT34	  	  	Phishing with email and other services, combined with public tools

Key					
	Aviation		Banking and ATMs		Energy
	Financial		Gambling		Government Espionage
	Natural Resources		US Retail, Restaurant and Hospitality		

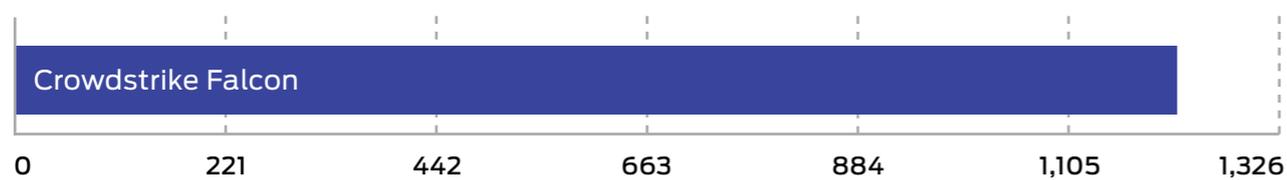
2. Total Accuracy Ratings

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.

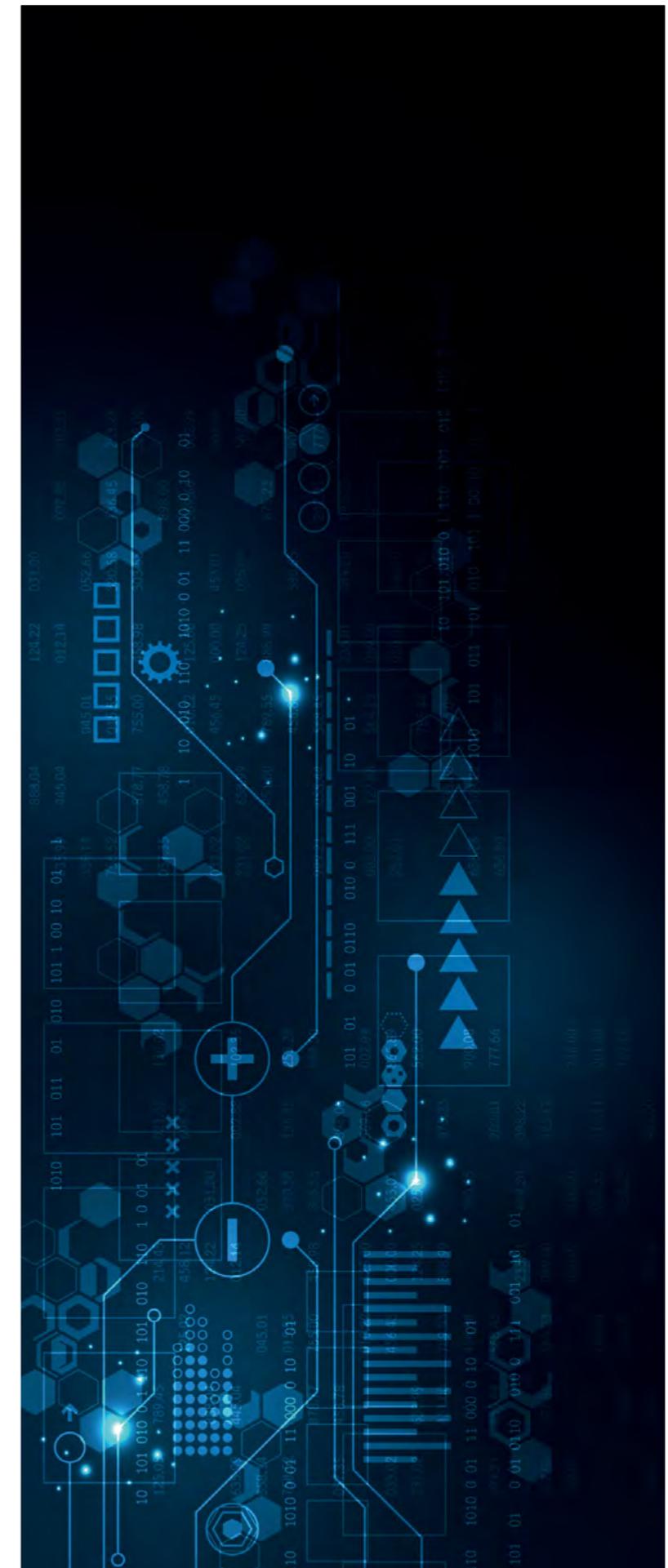
If you look at the results table in 3. Response Details on page 11 you'll see that Delivery and Execution are grouped together into one chunk, while Action sits alone. Escalation and Post-Escalation (PE) Action are grouped, while Lateral Movement and Lateral Action are also grouped.

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
CrowdStrike Falcon	1,216	92%	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.

APT3								
Incident No:	Detection	Delivery	Execution	Action	Escalation	PE Action	Lateral Movement	Lateral Action
1	✓	✓	✓	✓	✓	✓	✓	✓
2	✓	✓	✓	✓	✓	✓	✓	—
3	✓	✓	✓	✓	✓	✓	✓	✓
4	✓	✓	—	—	n/a	—	—	✓

APT29								
Incident No:	Detection	Delivery	Execution	Action	Escalation	PE Action	Lateral Movement	Lateral Action
5	✓	✓	—	n/a	✓	—	—	—
6	✓	✓	✓	✓	✓	✓	—	✓
7	✓	—	—	—	—	✓	✓	✓

APT33								
Incident No:	Detection	Delivery	Execution	Action	Escalation	PE Action	Lateral Movement	Lateral Action
8	✓	✓	—	✓	—	✓	✓	✓
9	✓	✓	✓	✓	—	✓	✓	—
10	✓	✓	—	✓	n/a	✓	✓	✓
11	✓	✓	✓	✓	n/a	✓	✓	✓

APT34								
Incident No:	Detection	Delivery	Execution	Action	Escalation	PE Action	Lateral Movement	Lateral Action
12	✓	—	✓	—	✓	—	—	—
13	✓	✓	✓	✓	✓	✓	✓	—
14	✓	—	✓	—	—	✓	—	—
15	✓	—	—	—	✓	✓	✓	—

If this attempt is discovered, or any subsequent action, a detection is reported.

The Detection Rating is calculated by adding points for each group in a threat chain that is detected. When at least one detection occurs in a single group, a 'group detection' is recorded and 10 points are awarded. Each test round contains one threat chain, which itself contains four groups

(as shown above), meaning that complete visibility of each attack adds 40 points to the total value.

A product that detects the delivery of a threat, but nothing subsequently to that, wins only 10 points, while a product that detects delivery and action, but not privilege escalation or lateral behaviours, is rated at 20 for that test round.

Response Details						
Attacker/ APT Group	Number of test cases	Attacks Detected	Delivery/ Execution	Action	Privilege Escalation/ Action	Lateral Movement/ Action
APT3	4	4	4	3	3	4
APT29	3	3	2	1	3	2
APT33	4	4	4	4	4	4
APT34	4	4	3	1	4	2
TOTAL	15	15	13	9	14	12

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

Detection Accuracy Rating Details				
Attacker/ APT Group	Number of test cases	Attacks Detected	Group Detections	Detection Rating
APT3	4	4	14	140
APT29	3	3	8	80
APT33	4	4	16	160
APT34	4	4	10	100
TOTAL	15	15	48	480

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

Detection Accuracy Ratings		
Product	Detection Accuracy Rating	Detection Accuracy Rating %
CrowdStrike Falcon	480	81%



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

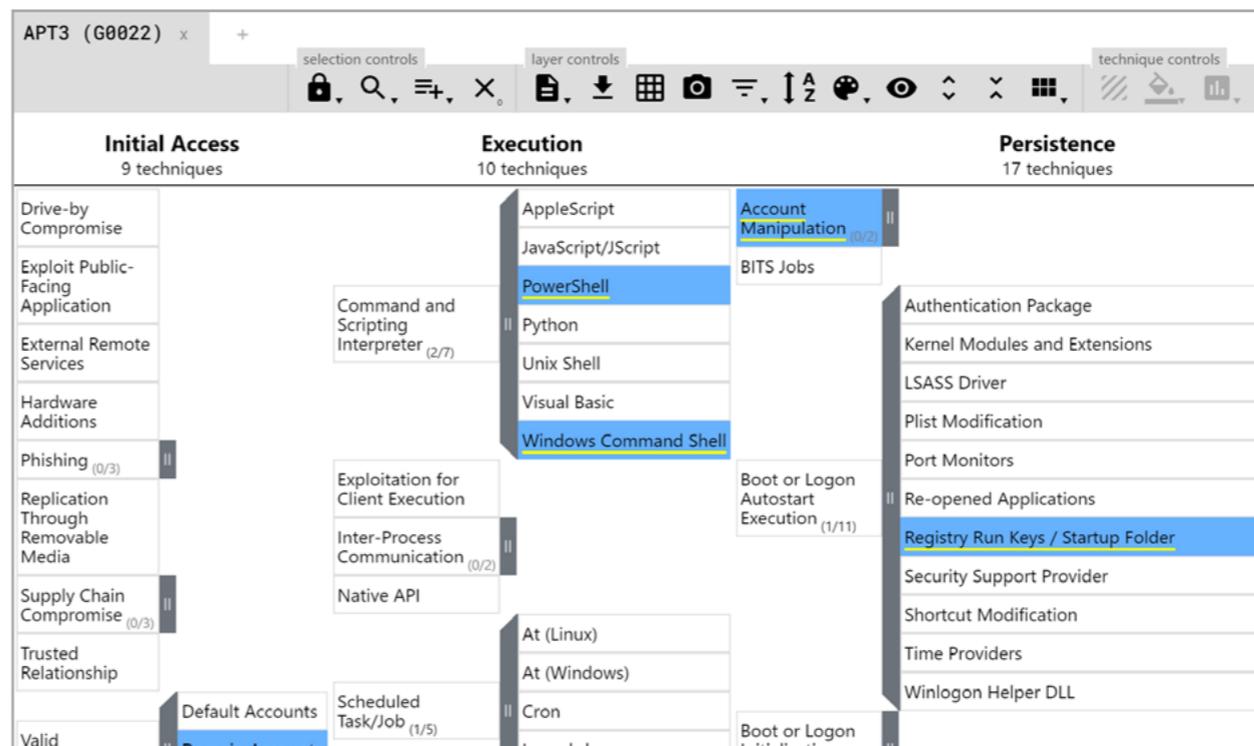
4. Threat Intelligence

APT3

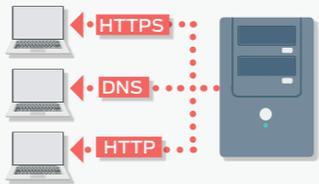
Primarily targeting political organisations in Hong Kong, APT3 uses a wide variety of initial attack techniques including phishing, web-based exploits and access via valid accounts. PowerShell and other scripting languages are used to gain further access, including control via Remote Desktop Access.

References:

<https://attack.mitre.org/groups/G0022/>



Attacker techniques documented by the MITRE ATT&CK framework.

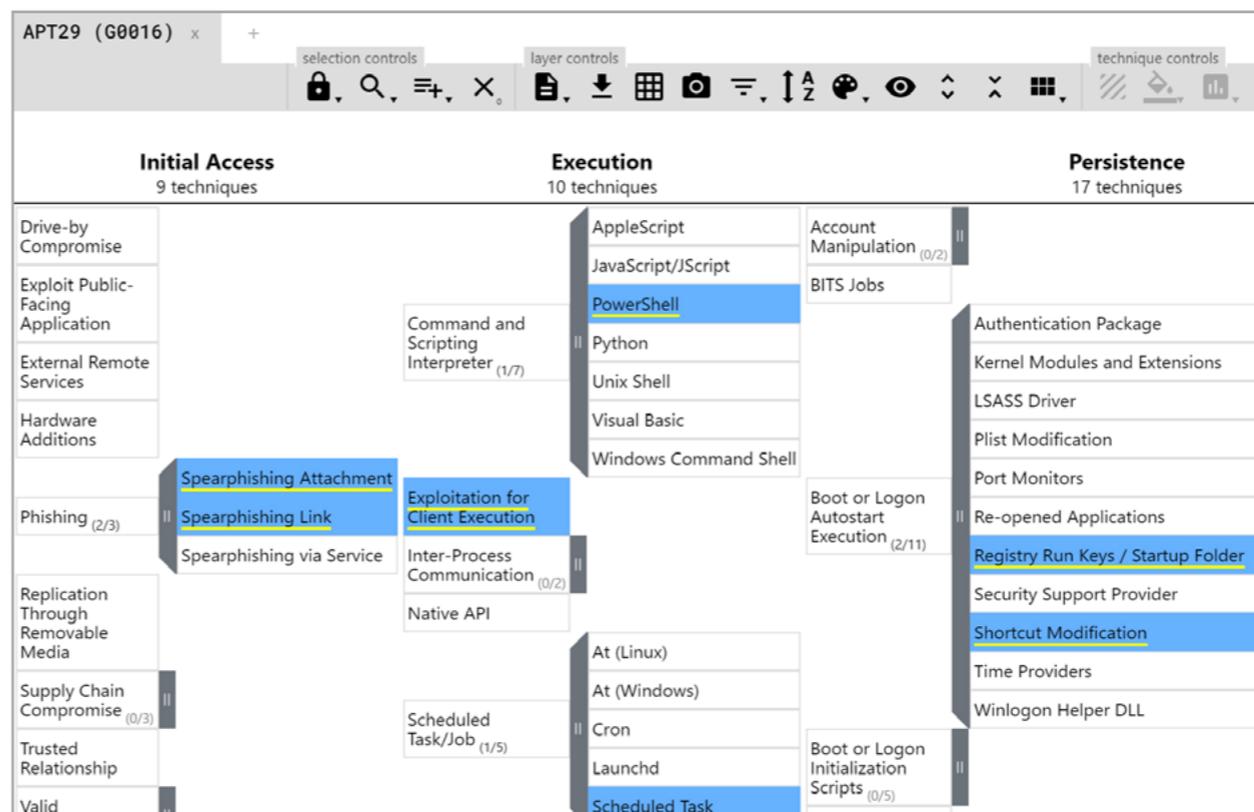
Example APT3 Attack						
Delivery	Execution	Action	Escalation	Post-Escalation Action	Lateral Movement	Lateral Action
Spearphishing Link	Command-Line Interface	Account Discovery	Bypass UAC	Credential Dumping	Remote Desktop Protocol	Data from Local System
	Commonly Used Port	File and Directory Discovery		Accessibility Features		Account Manipulation
	Connection Proxy	Process Discovery System Owner/User Discovery System Information Discovery Create Account				
 E-mail Link	 Commonly Used Port	 File and Directory Discovery	 Bypass UAC	 Accessibility Features	 Remote Desktop Protocol	 Data from Local System

APT29

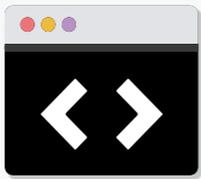
Thought to be connected with Russian military cyber operations, APT29 targets government, military and telecommunications sectors. It is believed to have been behind the Democratic National Committee hack in 2015, in which it used phishing emails with attached malware or links to malicious scripts.

References:

<https://attack.mitre.org/groups/G0016/>



Attacker techniques documented by the MITRE ATT&CK framework.

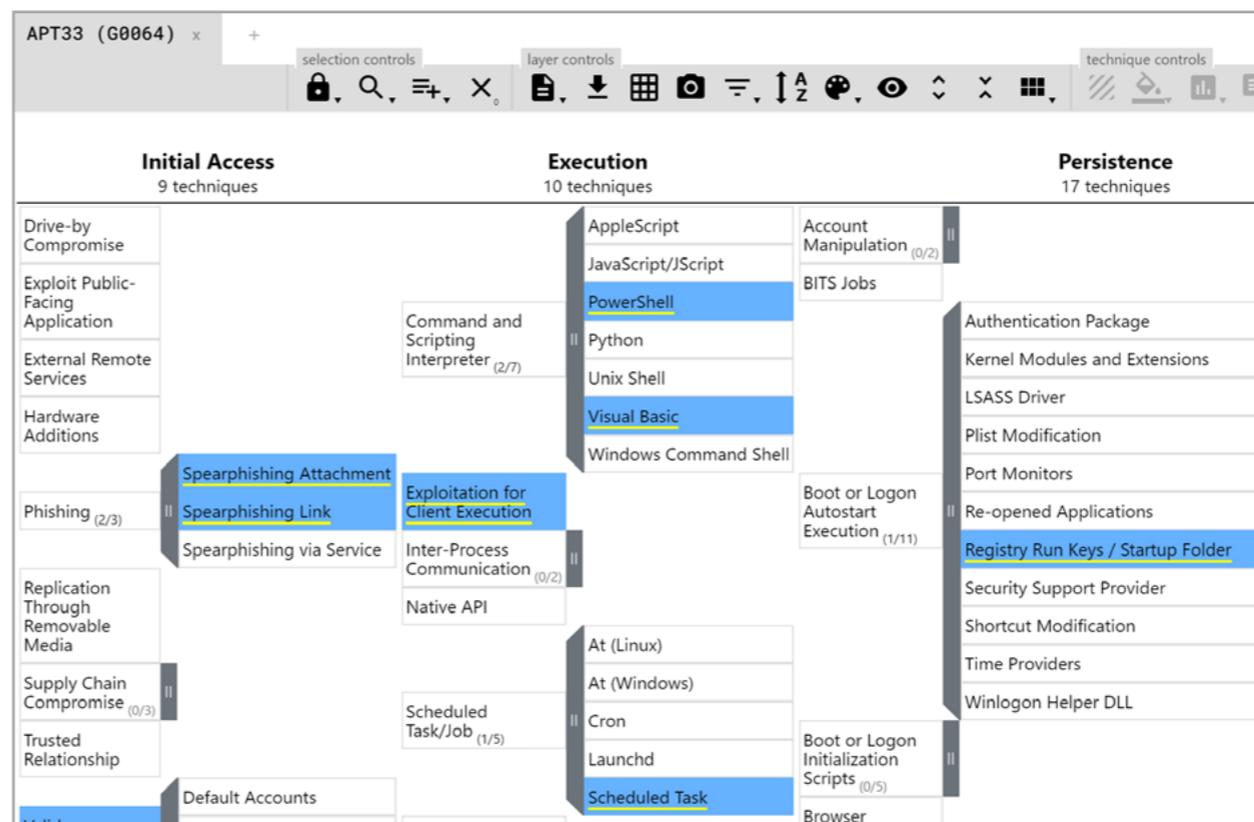
Example APT29 Attack						
Delivery	Execution	Action	Escalation	Post-Escalation Action	Lateral Movement	Lateral Action
Spearphishing Link	Powershell	Scheduled Task	Bypass UAC	Registry Run Keys / Startup Folder	Pass the Ticket	Scheduled Task
	Multi-Hop Proxy	File Deletion				Registry Run Keys / Startup Folder
	Scripting					Registry Run Keys / Startup Folder
	Obfuscated Files or Information					Registry Run Keys / Startup Folder
 E-mail Link - Fileless Attack	 Scripting	 Scheduled Task	 Bypass UAC	 Registry Run Keys / Startup Folder	 Pass the Ticket	 Scheduled Task

APT33

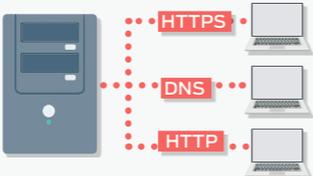
Focussing on aviation and energy industries, this group is believed to be based in Iran. It has used spear phishing emails containing links to scripts (including VBS and HTA) and exploits, some of which were used to escalate privileges. Public tools have been used to collect credentials.

References:

<https://attack.mitre.org/groups/G0064/>



Attacker techniques documented by the MITRE ATT&CK framework.

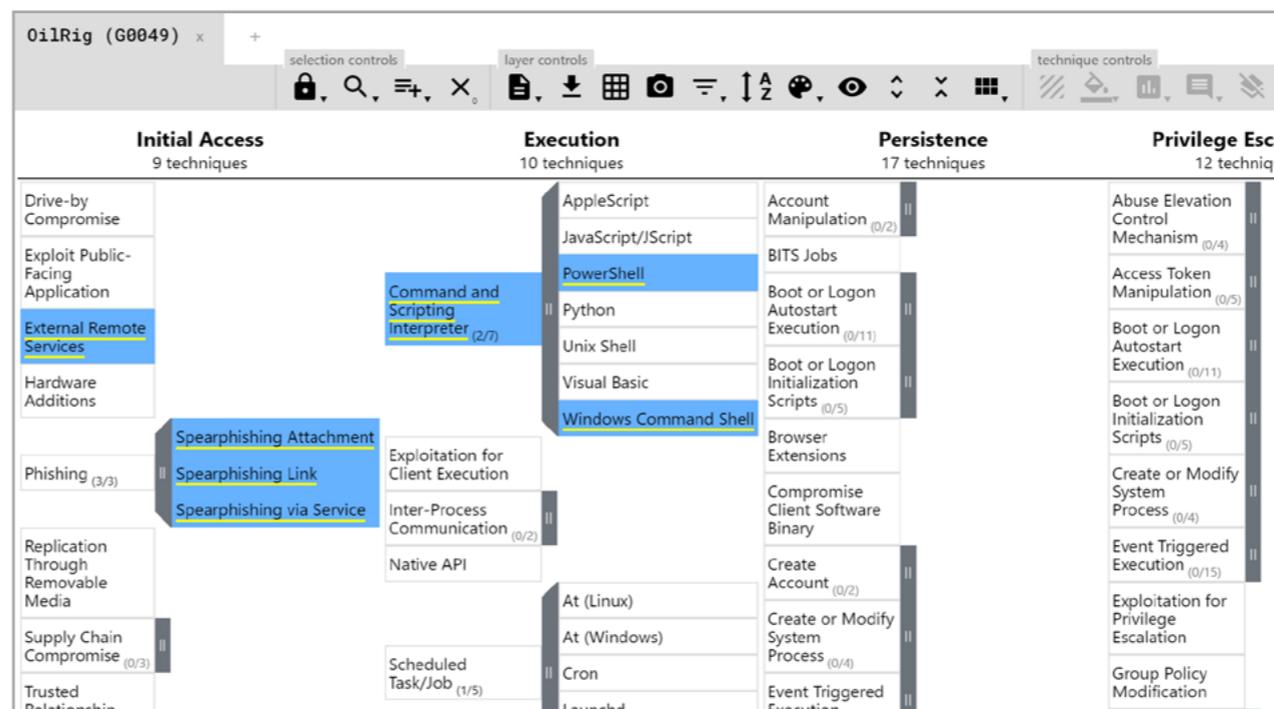
Example APT33 Attack						
Delivery	Execution	Action	Escalation	Post-Escalation Action	Lateral Movement	Lateral Action
Spearphishing Link	Exploitation for Client Execution	Scheduled Task	Exploitation for Privilege Escalation	Credential Dumping	Remote File Copy	Data Compressed
	User Execution			Brute Force		
	Commonly Used Port					
 E-mail Link - Fileless Attack	 Commonly Used Port	 Scheduled Task	 Exploitation for Privilege Escalation	 Credential Dumping	 Remote File Copy	 Data Compressed

APT34

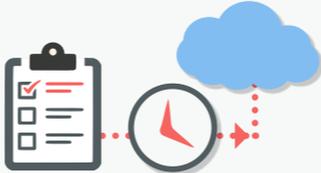
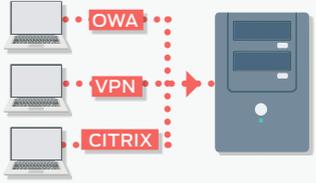
This Iranian APT has attacked a wide variety of targets, including financial, governmental and infrastructural organisations. Its techniques include using phishing via email and services such as LinkedIn, sending links to scripts, macros and other malware. It uses public tools to extract data and to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

References:

<https://attack.mitre.org/groups/G0049/>



Attacker techniques documented by the MITRE ATT&CK framework.

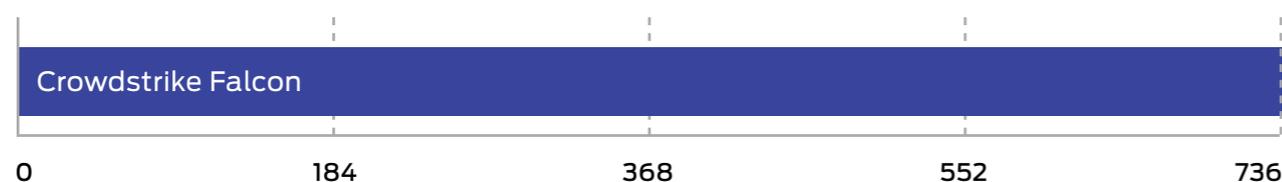
Example APT34 Attack						
Delivery	Execution	Action	Escalation	Post-Escalation Action	Lateral Movement	Lateral Action
Spearphishing via Service	Compiled HTML File	Process Discovery	Scheduled Task	System Network Configuration Discovery	Remote Services	Exfiltration Over Alternative Protocol
	Custom Command and Control Protocol	System Information Discovery		System Network Connections Discovery		
	Scripting	System Owner/User Discovery		Windows Management Instrumentation		
		Web Shell				
 Spearphishing Service LinkedIn Link	 Spearphishing Service LinkedIn Link	 Process Discovery	 Scheduled Task	 Windows Management Instrumentation	 Remote Services	 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 (%)
Crowdstrike Falcon	736	100%



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

SE Labs

INTELLIGENCE-LED TESTING

SE Labs helps advance the effectiveness of computer security through innovative, detailed and intelligence-led testing, run with integrity.



Enterprises

Reports for enterprise-level products supporting businesses when researching, buying and employing security solutions.

[Download Now!](#)

Small Businesses

Our product assessments help small businesses secure their assets without the purchasing budgets and manpower available to large corporations

[Download Now!](#)



Consumers

Download free reports on internet security products and find out how you can secure yourself online as effectively as a large company

[Download Now!](#)

SE Labs launches new security testing site

selabs.uk

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 all of the threats on a basic level, in that for each attack it detected at least some element of the attack chain. In most cases (11 out of 15) it detected the initial delivery made by each attack and in the remaining four cases, it detected execution of the threat twice. Only two threats went unnoticed past the initial stages, those being an APT29 attack and an APT34 attack. These were both detected in the escalation phase of the attack.

The results are strong and not one attack went completely undetected. 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 30th June and 19th July 2020.
- This test was conducted independently by SE Labs with similar testing made available to other vendors, at the same time, for their own standalone reports.
- The product was configured according to its vendor's recommendations.
- Targeted attacks were selected and verified by SE Labs.
- Malicious and legitimate data was provided to partner organisations once the test was complete.
- 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

APT3							
Incident No:	Delivery	Execution	Action	Escalation	Post-Escalation Action	Lateral Movement	Lateral Action
1	Spearphishing Link	Command-Line Interface	Account Discovery	Bypass UAC	Credential Dumping	Remote Desktop Protocol	Data from Local System
		Commonly Used Port	File and Directory Discovery		Accessibility Features		Account Manipulation
		Connection Proxy	Process Discovery System Owner/User Discovery System Information Discovery Create Account				
2	Spearphishing Link	Graphical User Interface	Account Discovery	Bypass UAC	Data Staged	Remote File Copy	Data Compressed
		Uncommonly Used Port	File and Directory Discovery		New Service		
		Software Packing	Process Discovery System Owner/User Discovery System Information Discovery Scheduled Task				
3	Spearphishing Link	PowerShell	Account Discovery	Bypass UAC	Input Capture	Windows Admin Shares	Exfiltration over Command and Control channel
		File Deletion	File and Directory Discovery		Registry Run Keys / Startup Folder		Data from Local System
		Obfuscated Files or Information	Process Discovery				
		Hidden Window	System Owner/User Discovery				
		Scripting	System Information Discovery System Network Configuration Discovery System Network Connections Discovery Remote System Discovery				
4	Scripting	Standard Non-Application Layer Protocol	Account Discovery	Bypass UAC	Credentials in Files	Remote Desktop Protocol	Data from Local System
	Rundll32	DLL Side-Loading	File and Directory Discovery Process Discovery System Owner/User Discovery System Information Discovery Redundant Access Permission Groups Discovery Indicator Removal from Tools		Scheduled Tasks		Scheduled Task

APT29									
Incident No:	Delivery	Execution	Action	Escalation	Post-Escalation Action	Lateral Movement	Lateral Action		
5	Spearphishing Attachment	User Execution		Bypass UAC	Windows Management Instrumentation Event Subscription	Pass the Ticket	File from Local system		
	Software Packing	Commonly Used Port			Persistence through Accessibility Features				
		Exploitation for Client Execution							
6	Spearphishing Link	Powershell	Scheduled Task	Bypass UAC	Registry Run Keys / Startup Folder	Pass the Ticket	Scheduled Task		
		Multi-Hop Proxy	File Deletion				Registry Run Keys / Startup Folder	Pass the Ticket	Registry Run Keys / Startup Folder
		Scripting							
		Obsfuscated Files or Information							
7	Spearphishing Attachment	Shortcut Modification	Indicator Removal on Host	Bypass UAC	Registry Run Keys / Startup Folder	Pass the Ticket	Scheduled Task		
		Rundll32							
		Domain Fronting							

APT33							
Incident No:	Delivery	Execution	Action	Escalation	Post-Escalation Action	Lateral Movement	Lateral Action
8	Spearphishing Link	Exploitation for Client Execution	Scheduled Task	Exploitation for Privilege Escalation	Credential Dumping	Remote File Copy	Data compressed
		User Execution			Brute Force		
		Commonly Used Port					
9	Spearphishing Link	PowerShell	Scheduled Task	Exploitation for Privilege Escalation	Registry Run Keys / Startup Folder	Remote File Copy	Exfiltration over Alternative Protocol
		Obsfuscated Files or Information			Network Sniffing		
		Data Encoding					
		Uncommonly Used Port					
10	Spearphishing Link	Exploitation for Client Execution	Scheduled Task	Bypass UAC	Network Sniffing	Remote File Copy	Exfiltration over Alternative Protocol
		User Execution					
		Standard Application Layer Protocol					
		Execution Guardrails					
11	Spearphishing Link	PowerShell	Scheduled Task	Bypass UAC	Credential Dumping	Remote File Copy	Data compressed
		Obsfuscated Files or Information			Brute Force		
		Data Encoding					
		Standard Cryptographic Protocol					

APT34							
Incident No:	Delivery	Execution	Action	Escalation	Post-Escalation Action	Lateral Movement	Lateral Action
12	Spearphishing Attachment	Command-Line Interface	Process Discovery	Scheduled Task	Indicator Removal from Tools	Remote Desktop Protocol	Exfiltration Over Alternative Protocol
		User Execution	System Information Discovery		Credentials in Files		
		Commonly Used Port	System Owner/User Discovery				
		Standard Application Layer Protocol	Screen Capture External Remote Services				
13	Spearphishing Link	PowerShell	Process Discovery	Scheduled Task	Credential Dumping	Remote File Copy	Automated Collection
		User Execution	System Information Discovery		Query Registry		
		Standard Cryptographic Protocol	System Owner/User Discovery		Account Discovery		
		File Deletion	System Service Discovery		Redundant Access		
14	Spearphishing via Service	Compiled HTML File	Process Discovery	Scheduled Task	System Network Configuration Discovery	Remote Services	Exfiltration Over Alternative Protocol
		Custom Command and Control Protocol	System Information Discovery		System Network Connections Discovery		
		Scripting	System Owner/User Discovery		Windows Management Instrumentation		
			Web Shell				
15	Spearphishing Attachment	User Execution	Process Discovery	Scheduled Task	Password Policy Discovery	Remote File Copy	Exfiltration Over Alternative Protocol
		Commonly Used Port	System Information Discovery		Permission Groups Discovery		
		Fallback Channels	System Owner/User Discovery		Credential Dumping		
			Deobfuscate/Decode Files or Information		Brute Force		

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.