SE Labs

INTELLIGENCE-LED TESTING

EDR

Advanced Security Test

Crowdstrike Falcon

November 2021

selabs.uk info@SELabs.uk @SELabsUK selabs.uk/newsletter blog.selabs.uk

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
Thomas Bean
Solandra Brewster
Rory Brown
Liam Fisher
Gia Gorbold
Erica Marotta
Jeremiah Morgan
Joseph Pike
Dave Togneri
Dimitrios Tsarouchas
Stephen Withey
Liangyi Zhen

IT SUPPORT
Danny King-Smith
Chris Short

PUBLICATION
Sara Claridge
Colin Mackleworth

Website selabs.uk
Twitter @SELabsUK
Email info@SELabs.uk
LinkedIn linkedin.com/company/se-labs/
Blog blog.selabs.uk
Phone +44 (0)203 875 5000
Post SE Labs Ltd,
55A High Street, Wimbledon, SW19 5BA, UK

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

SE Labs is a member of the Microsoft Virus Information Alliance (VIA); the Anti-Malware Testing Standards Organization (AMTSO); and NetSecOPEN.

CONTENTS

Document version 1.0 Written 22nd November 2021

INTRODUCTION

Testing Threat Detection, Protection and Response

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

Testing advanced security products is a complex business, which is why we now have two types of advanced security 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
- 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 account. SE Labs uses current threat intelligence to make our tests as realistic as possible. To learn more about how we test, how we define 'threat intelligence' and how we use it to improve our tests please visit our website and follow us on Twitter.

Executive Summary

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 tracked each of the hostile activities that occurred during the attacks. With one minor exception, detection was complete and deep, tracking malicious behaviour from the beginning to the end of the attack. It generated no false positives, which should lighten the load on security operatives using the product.

EXECUTIVE SUMMARY

Products Tested	Attacks Detected (%)	Detection Accuracy (%)	Legitimate Accuracy Rating (%)	Total Accuracy Rating (%)
Crowdstrike Falcon	100%	98%	100%	99%

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

For exact percentages, see **1. Total Accuracy Ratings** on page 10.

Advanced Security Test 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 advanced security test means setting up real networks and hacking them in the same way that real adversaries behave.

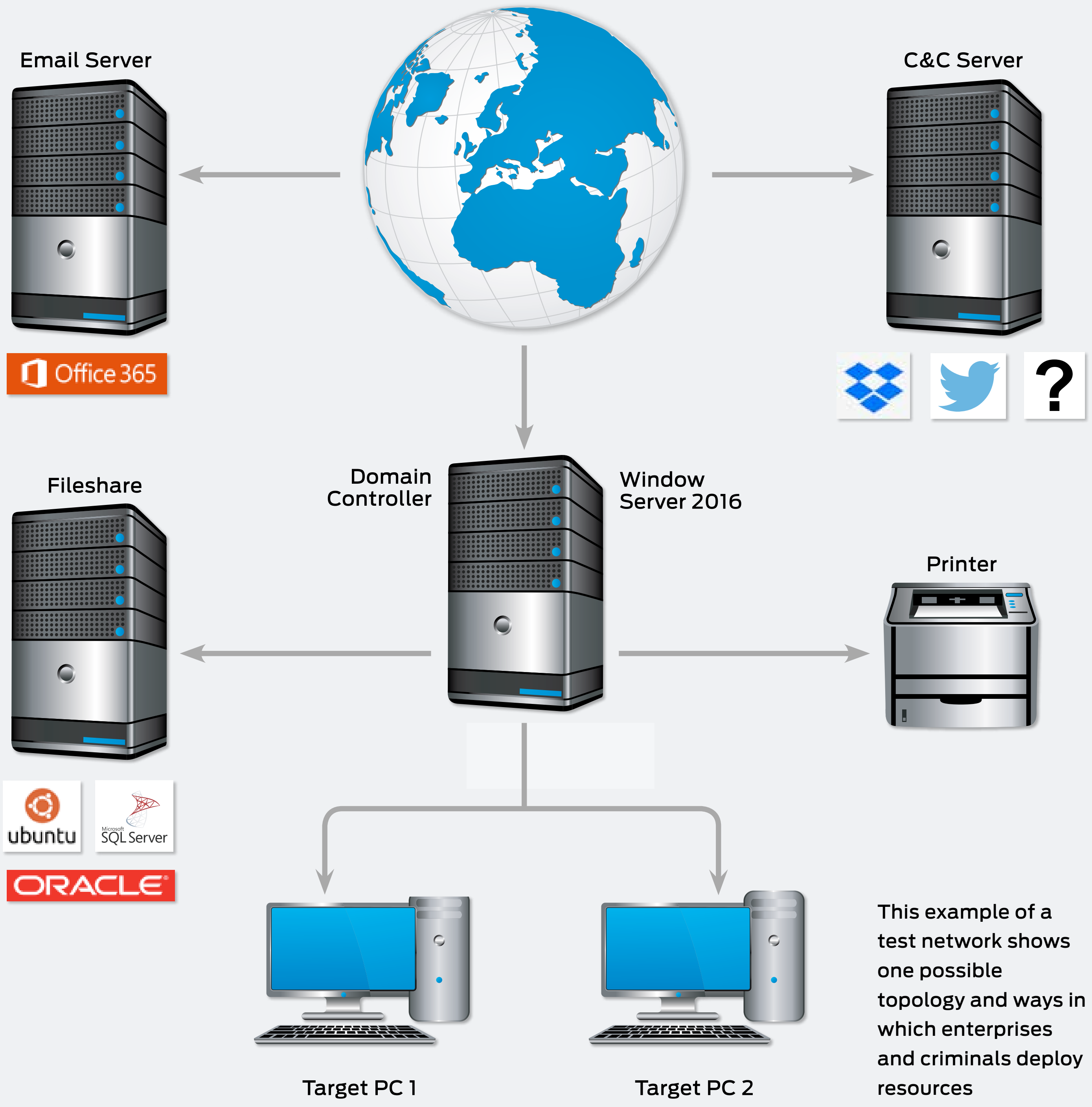
In the diagram on the right you will see an example network that contains workstations, some basic infrastructure such as file servers and a domain controller, as well as cloud-based email and a malicious command and control (C&C) server, which may be a conventional computer or a service such as Dropbox,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

As you will see in the **Threat Responses section** on page 7, attackers often jump from one compromised system to another in so-called 'lateral movement'. To allow products to detect this type of behaviour the network needs to be built realistically, with systems available, vulnerable and worth compromising.

It is possible to compromise devices such as enterprise printers and other so-called 'IoT' (internet of things) machines, which is why we've included a representative printer in the diagram.

The techniques that we choose for each test case are largely dictated by the real-world behaviour of online criminals. We observe their tactics and replicate what they do in this test. To see more details about how the specific attackers behaved, and how we copied them, see **Hackers vs. Targets** on page 9 and, for a really detailed drill down on the details, **4. Threat Intelligence** on pages 13 to 16 and **Appendix C: Attack Details.**

Test Network Example



This example of a test network shows one possible topology and ways in which enterprises and criminals deploy resources

Threat Responses

Full Attack Chain: Testing every layer of detection and protection

Attackers start from a certain point and don't stop until they have either achieved their goal or have reached the end of their resources (which could be a deadline or the limit of their abilities). This means, in a test, the tester needs to begin the attack from a realistic first position, such as sending a phishing email or setting up an infected website, and moving through many of the likely steps leading to actually stealing data or causing some other form of damage to the network.

If the test starts too far into the attack chain, such as executing malware on an endpoint, then many products will be denied opportunities to use the full extent of their protection and detection abilities. If the test concludes before any 'useful' damage or theft has been achieved, then similarly the product may be denied a chance to demonstrate its abilities in behavioural detection and so on.

Attack stages

The illustration (below) shows some typical stages of an attack. In a test each of these should be attempted to determine the security solution's effectiveness. This test's results record detection and protection for each of these stages.

We measure how a product responds to the first stages of the attack with a detection and/ or protection rating. Sometimes products allow threats to run but detect them. Other times they might allow the threat to run briefly before neutralising it. Ideally they detect and block the threat before it has a chance to run. Products may delete threats or automatically contains them in a 'quarantine' or other safe holding mechanism for later analysis.

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

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

ATTACK CHAIN STAGES

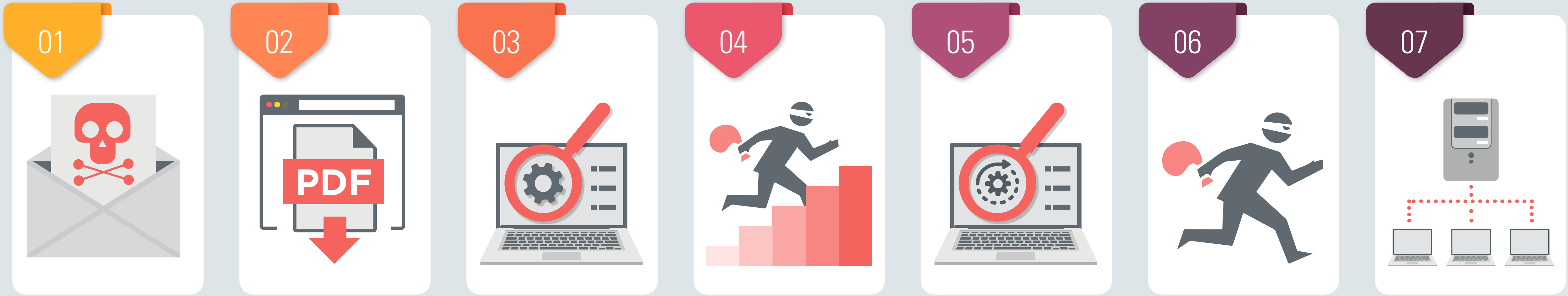


Figure 1. A typical attack starts with an initial contact and progresses through various stages, including reconnaissance, stealing data and causing damage.

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

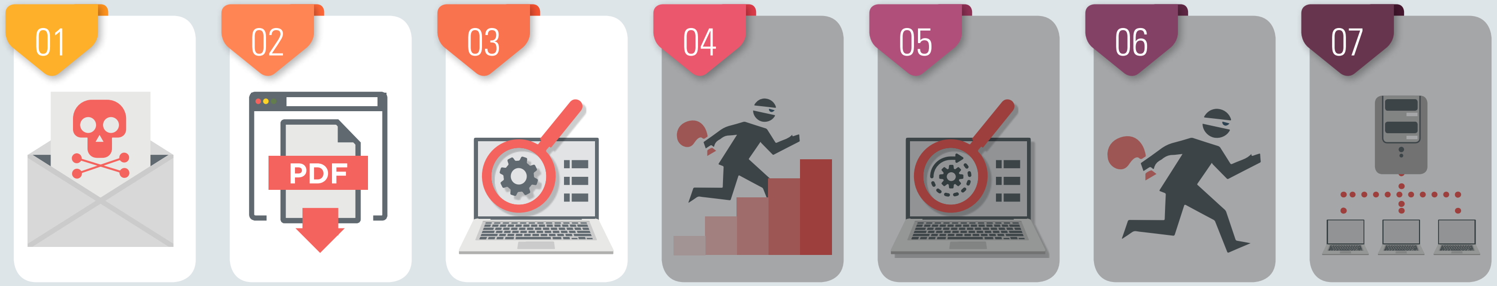


Figure 2. This attack was initially successful but only able to progress as far as the reconnaissance phase

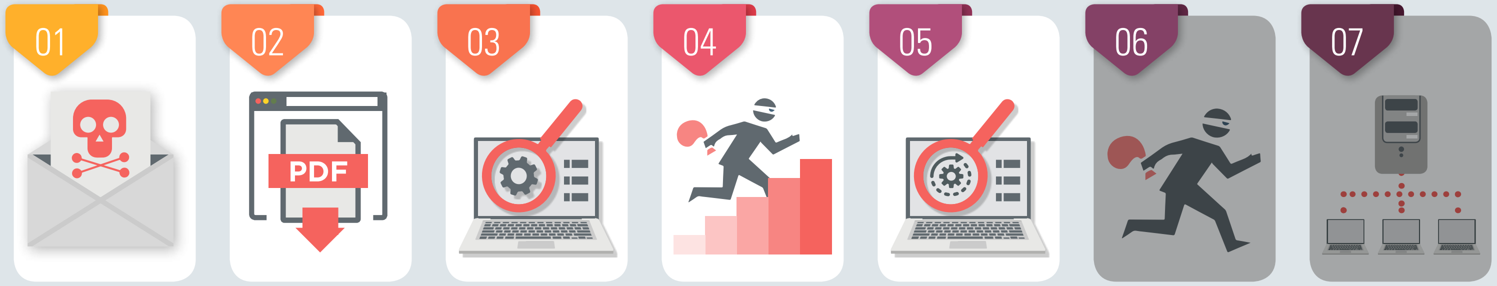


Figure 3. A more successful attack manages to steal passwords but wholesale data theft and destruction was blocked

Hackers
CYBER CRIME: 'WE'RE ALL TARGETS'
Only 13% cybercrime solved in two years
Cyber crime surges in Co
CYBER HACKERS CRIPPLE THE NHS
ransomware
English h
divert
ambulan
ransom
cyber at
Three U.S. Hospitals Hit in String of Ransomware Attacks
Ransomware attack hits
highlights dilemma for fight against malware
UK rail network hit by multiple cyber attacks
DON'T BE HELD TO RANSOM
Banks to face 10 attacks experts

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
Dragonfly & Dragonfly 2.0	✉ W	🏭	Phishing & supply chain methods used to gain access
Oilrig	✉ W <>	$ 🏛 🏭	Phishing with email and other services, combined with public tools
FIN7 & Carbanak	W	🛒	Documents containing scripts combined with public tools
APT29	✉ <>	🏛	Spear phishing emails containing scripts or links to malware

Key

✈ Aviation	🏦 Banking and ATMs	🏭 Energy
$ Financial	🃏 Gambling	🏛 Government Espionage
⛽ Natural Resources	🛒 US Retail, Restaurant and Hospitality	

2. Total Accuracy Ratings

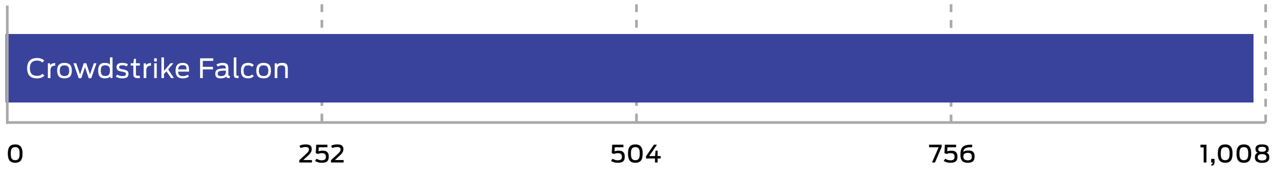
This test examines the total insight a product has, or can provide, into a specific set of attacking actions. We've divided the attack chain into chunks of one or more related actions. To provide sufficient insight, a product must detect at least one action in each chunk.

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	998	99%	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. If this attempt is discovered, or any subsequent action, a detection is reported.

Dragonfly & Dragonfly 2.0

Incident No:	Delivery	Execution	Action	Escalation	PE Action	Lateral Movement	Lateral Action
1	✓	✓	✓	✓	✓	✓	✓
2	—	✓	✓	✓	✓	✓	✓
3	—	✓	✓	✓	✓	✓	✓
4	✓	✓	—	✓	✓	✓	✓

Oilrig

Incident No:	Delivery	Execution	Action	Escalation	PE Action	Lateral Movement	Lateral Action
5	✓	✓	✓	✓	✓	✓	✓
6	✓	✓	✓	✓	✓	—	✓
7	—	✓	✓	✓	✓	✓	✓
8	—	✓	✓	✓	✓	✓	—

FIN7 & Carbanak

Incident No:	Delivery	Execution	Action	Escalation	PE Action	Lateral Movement	Lateral Action
9	✓	✓	✓	✓	✓	✓	✓
10	✓	✓	✓	✓	✓	✓	✓
11	—	✓	✓	✓	✓	✓	✓
12	—	✓	✓	✓	✓	✓	✓

APT29

Incident No:	Delivery	Execution	Action	Escalation	PE Action	Lateral Movement	Lateral Action
13	—	✓	✓	✓	✓	✓	✓
14	✓	✓	✓	✓	✓	✓	✓
15	✓	✓	✓	✓	✓	✓	✓
16	✓	✓	✓	✓	✓	✓	✓

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.

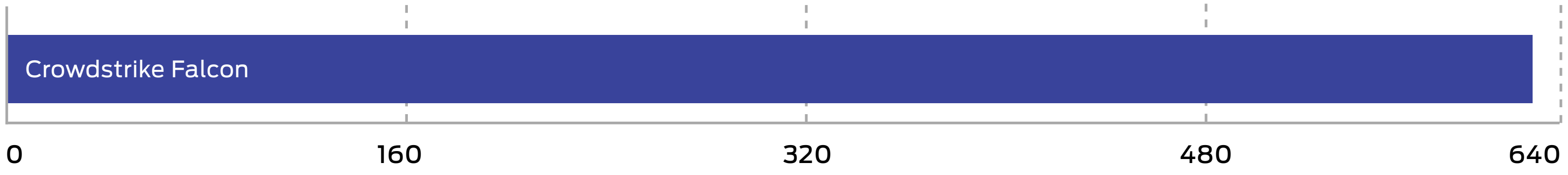
Response Details						
Attacker/APT Group	Number of Test Cases	Attacks Detected	Delivery/ Execution	Action	Privilege Escalation/ Action	Lateral Movement/Action
Dragonfly & Dragonfly 2.0	4	4	4	3	4	4
Oilrig	4	4	4	4	4	4
FIN7 & Carbanak	4	4	4	4	4	4
APT29	4	4	4	4	4	4
Total	16	16	16	15	16	16

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
Dragonfly & Dragonfly 2.0	4	4	15	150
Oilrig	4	4	16	160
FIN7 & Carbanak	4	4	16	160
APT29	4	4	16	160
Total	16	16	63	630

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	630	98%



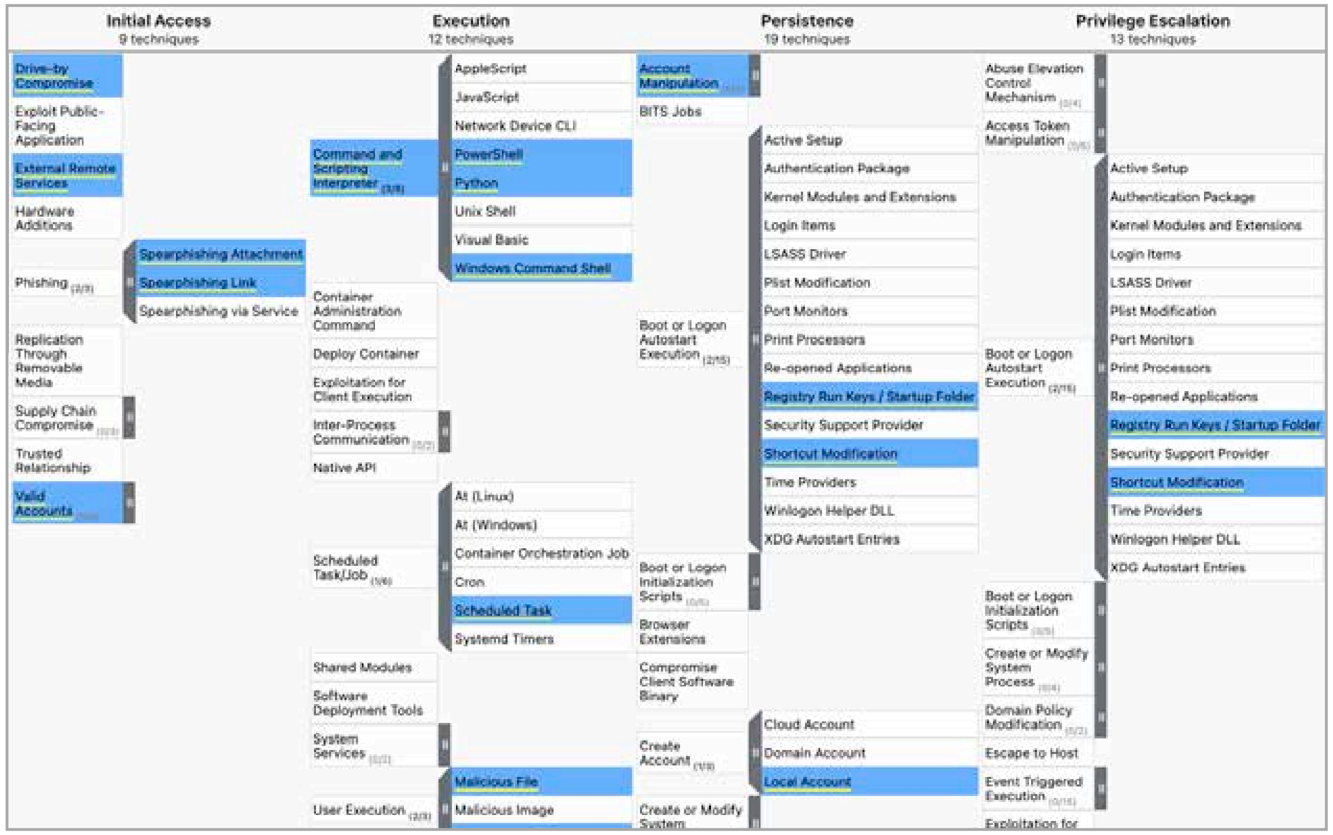
Detection Ratings are weighted to show that how products detect threats can be subtler than just ‘win’ or ‘lose’.

4. Threat Intelligence

Dragonfly & Dragonfly 2.0

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

References:
https://attack.mitre.org/groups/G0035/
https://attack.mitre.org/groups/G0074/



Initial Access
9 techniques

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

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

Execution
12 techniques

Command and Scripting Interpreter (3/8)
- AppleScript
- JavaScript
- Network Device CLI
- PowerShell
- Python
- Unix Shell
- Visual Basic
- Windows Command Shell

Container Administration Command
Deploy Container
Exploitation for Client Execution
Inter-Process Communication (0/2)
Native API
Scheduled Task/Job (1/6)
- At (Linux)
- At (Windows)
- Container Orchestration Job
- Cron
- Scheduled Task
- Systemd Timers

Shared Modules
Software Deployment Tools
System Services (0/2)
User Execution (2/3)
- Malicious File
- Malicious Image

Persistence
19 techniques

Account Manipulation
BITS Jobs
Boot or Logon Autostart Execution (2/15)
- Active Setup
- Authentication Package
- Kernel Modules and Extensions
- Login Items
- LSASS Driver
- Plist Modification
- Port Monitors
- Print Processors
- Re-opened Applications
- Registry Run Keys / Startup Folder
- Security Support Provider
- Shortcut Modification
- Time Providers
- Winlogon Helper DLL
- XDG Autostart Entries

Boot or Logon Initialization Scripts (0/5)
Browser Extensions
Compromise Client Software Binary
Create Account (1/3)
- Cloud Account
- Domain Account
- Local Account

Create or Modify System

Privilege Escalation
13 techniques

Abuse Elevation Control Mechanism (0/4)
Access Token Manipulation (0/5)
Boot or Logon Autostart Execution (2/15)
- Active Setup
- Authentication Package
- Kernel Modules and Extensions
- Login Items
- LSASS Driver
- Plist Modification
- Port Monitors
- Print Processors
- Re-opened Applications
- Registry Run Keys / Startup Folder
- Security Support Provider
- Shortcut Modification
- Time Providers
- Winlogon Helper DLL
- XDG Autostart Entries

Boot or Logon Initialization Scripts (0/5)
Create or Modify System Process (0/4)
Domain Policy Modification (0/2)
Escape to Host
Event Triggered Execution (0/16)
Exploitation for

Attacker techniques documented by the MITRE ATT&CK framework.

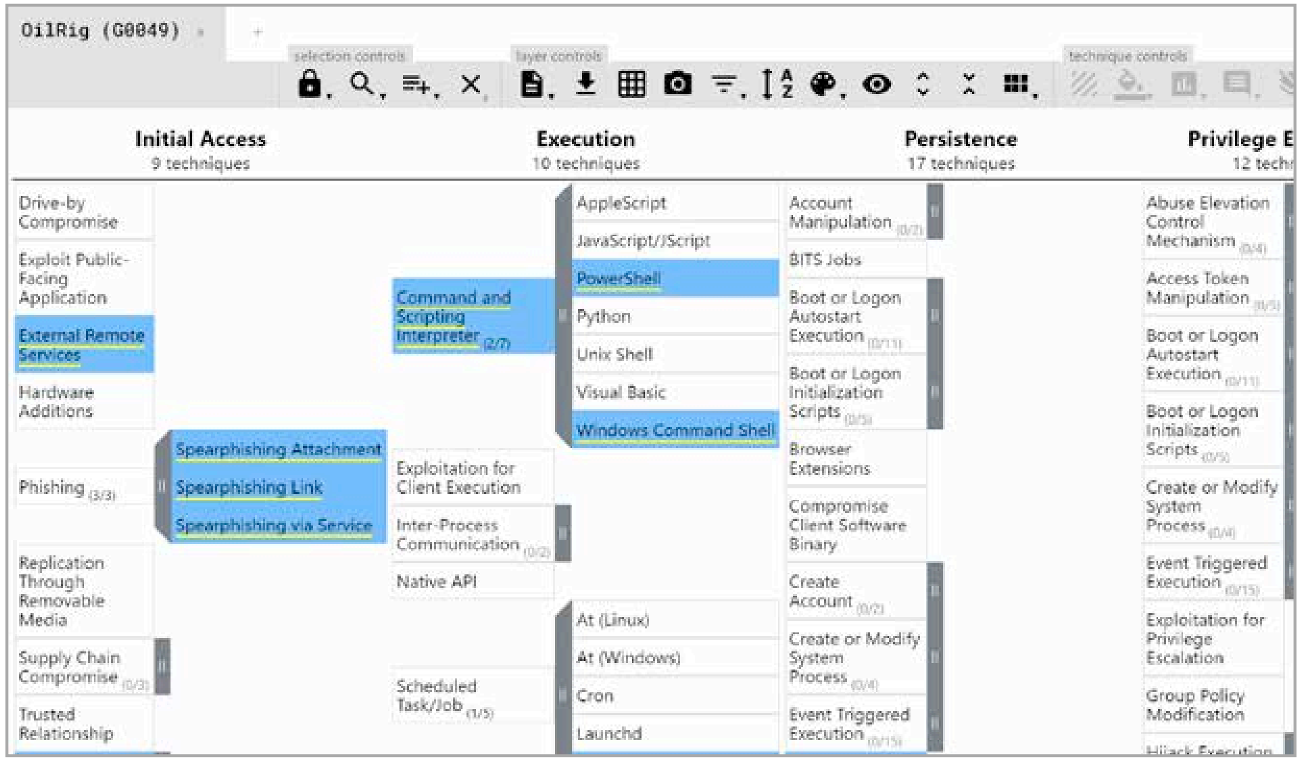
Example **Dragonfly & Dragonfly 2.0**

Delivery	Execution	Action	Privilege Escalation	Post-Escalation Action	Lateral Movement	Lateral Action
Spearphishing Link	Command and Scripting Interpreter	Domain Groups	Valid Accounts	Modify Registry	Remote Desktop Protocol	Archive Collected Data
Malicious Link	Windows Command Shell	Remote System Discovery		Query Registry		Data from Local System
	Powershell	System Information Discovery		Registry Run Keys / Startup Folder		Local Data Staging
		Process Discovery		Disable or Modify System Firewall		Screen Capture
		System Owner/User Discovery		Forced Authentication		Exfiltration Over C2 Channel
Malicious Link	Powershell	Process Discovery	Valid Accounts	Query Registry	Remote Desktop Protocol	Archive Collected Data

Oilrig

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

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



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

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

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)

Privilege E 12 techn
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

Attacker techniques documented by the MITRE ATT&CK framework.

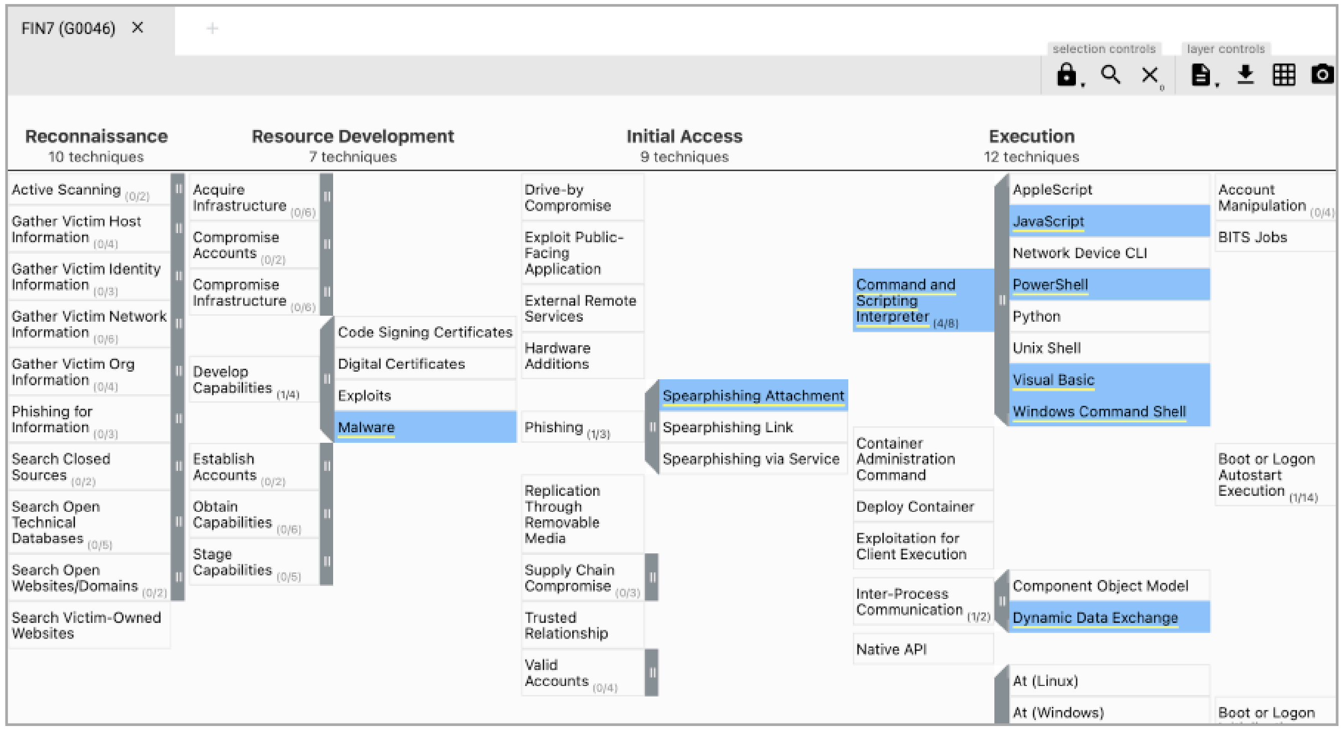
Example **Oilrig Attack**

Delivery	Execution	Action	Privilege Escalation	Post-Escalation Action	Lateral Movement	Lateral Action
Spearphishing Link	Powershell	System Information Discovery	Bypass UAC	Query Registry	Remote Desktop Protocol	Archive Collected Data: Archive via Utility
Malicious Link	Windows Command Shell	Process Discovery	Valid Accounts	Scheduled Tasks		Screen Capture
	Obfuscated File or Information	System Owner/User Discovery		Local Account		
		Local Groups		Domain Account		
		Domain Groups		Password Policy Discovery		
				Credentials in Files		
				Keylogging		
Spearphishing Link	Powershell	System Information Discovery	Bypass UAC	Query Registry	Remote Desktop Protocol	Screen Capture

FIN7 & Carbanak

FIN7 & Carbanak 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/



Reconnaissance
10 techniques

- Active Scanning (0/2)
- Gather Victim Host Information (0/4)
- Gather Victim Identity Information (0/3)
- Gather Victim Network Information (0/6)
- Gather Victim Org Information (0/4)
- Phishing for Information (0/3)
- Search Closed Sources (0/2)
- Search Open Technical Databases (0/5)
- Search Open Websites/Domains (0/2)
- Search Victim-Owned Websites

Resource Development
7 techniques

- Acquire Infrastructure (0/6)
- Compromise Accounts (0/2)
- Compromise Infrastructure (0/6)
- Develop Capabilities (1/4)
  - Code Signing Certificates
  - Digital Certificates
  - Exploits
  - Malware
- Establish Accounts (0/2)
- Obtain Capabilities (0/6)
- Stage Capabilities (0/5)

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 (0/4)

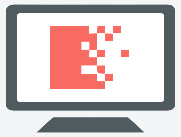
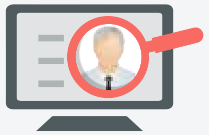
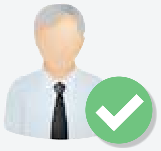
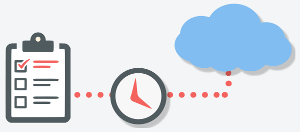
Execution
12 techniques

- Command and Scripting Interpreter (4/8)
  - AppleScript
  - JavaScript
  - Network Device CLI
  - PowerShell
  - Python
  - Unix Shell
  - Visual Basic
  - Windows Command Shell
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication (1/2)
  - Component Object Model
  - Dynamic Data Exchange
- Native API
  - At (Linux)
  - At (Windows)

- Account Manipulation (0/4)
- BITS Jobs
- Boot or Logon Autostart Execution (1/14)
- Boot or Logon

Attacker techniques documented by the MITRE ATT&CK framework

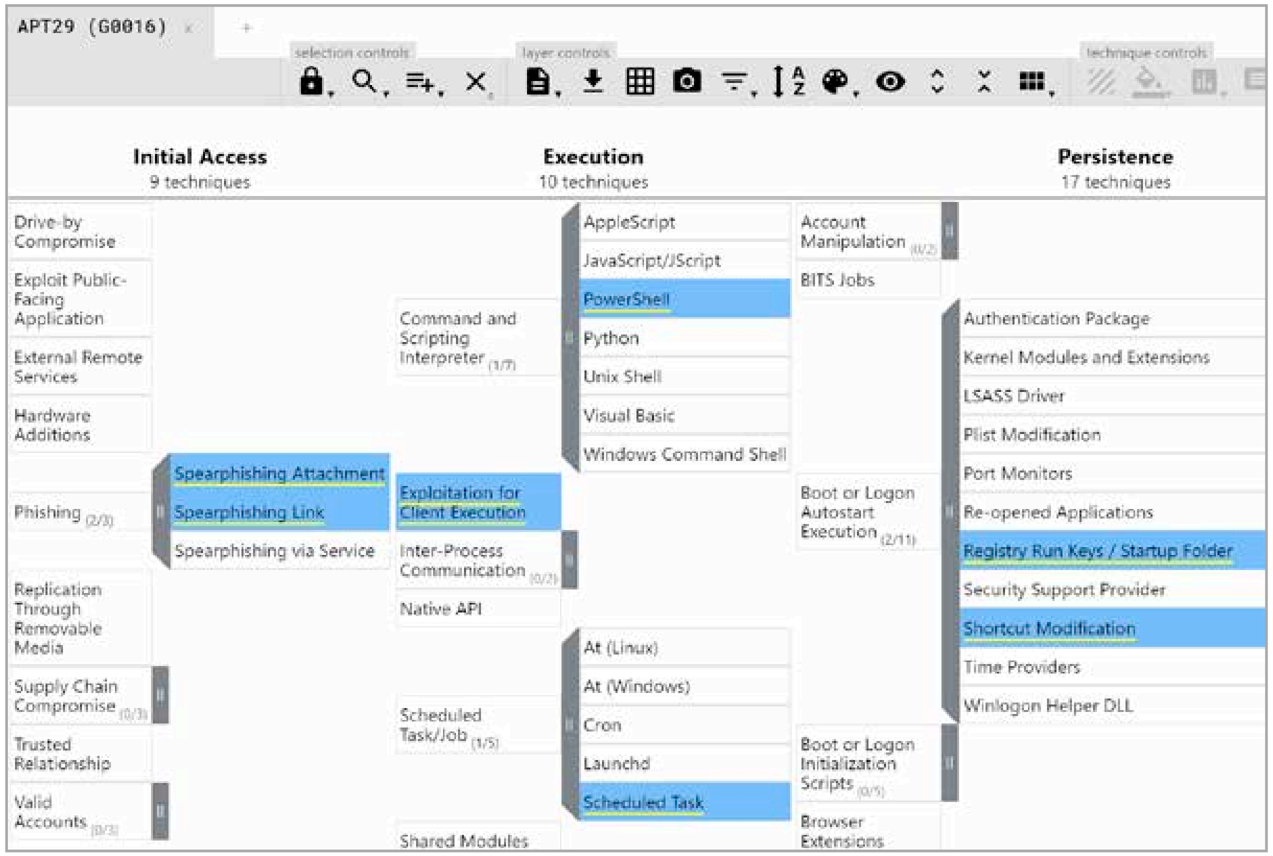
Example **FIN7 & Carbanak Attack**

Delivery	Execution	Action	Privilege Escalation	Post-Escalation Action	Lateral Movement	Lateral Action
Spearphishing Attachment	Command-Line Interface	Account Discovery	Bypass UAC	Credential Dumping	Remote File Copy	Data Compressed
Obfuscated Files or Information	Commonly Used Port	File and Directory Discovery	Valid Accounts	Data Compressed	Pass the Hash	Data Encrypted
	Powershell	Process Discovery		Data Encrypted		Data from Local System
	Remote File Copy	System Information Discovery		Data from Local System		Data Staged
	Scripting	System Owner/User Discovery		Data Staged		Exfiltration over Command and Control Channel
	Standard Application Layer Protocol			Exfiltration over Command and Control Channel		
	Standard Cryptographic Protocol			Account Discovery		
	User Execution			Input Capture		
				Modify Registry		
				New Service		
				Process Hollowing		
				Query Registry		
				Scheduled Task		
 Obfuscated Files or Information	Standard Cryptographic Protocol	 System Owner/User Discovery	 Valid Accounts	 Scheduled Task	Remote File Copy	Data Compressed

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/



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 (1/5)
  - At (Linux)
  - At (Windows)
  - Cron
  - Launchd
  - Scheduled Task
- Shared Modules

Persistence
17 techniques

- Account Manipulation (0/2)
- BITS Jobs
- Boot or Logon Autostart Execution (2/11)
  - 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

Attacker techniques documented by the MITRE ATT&CK framework.

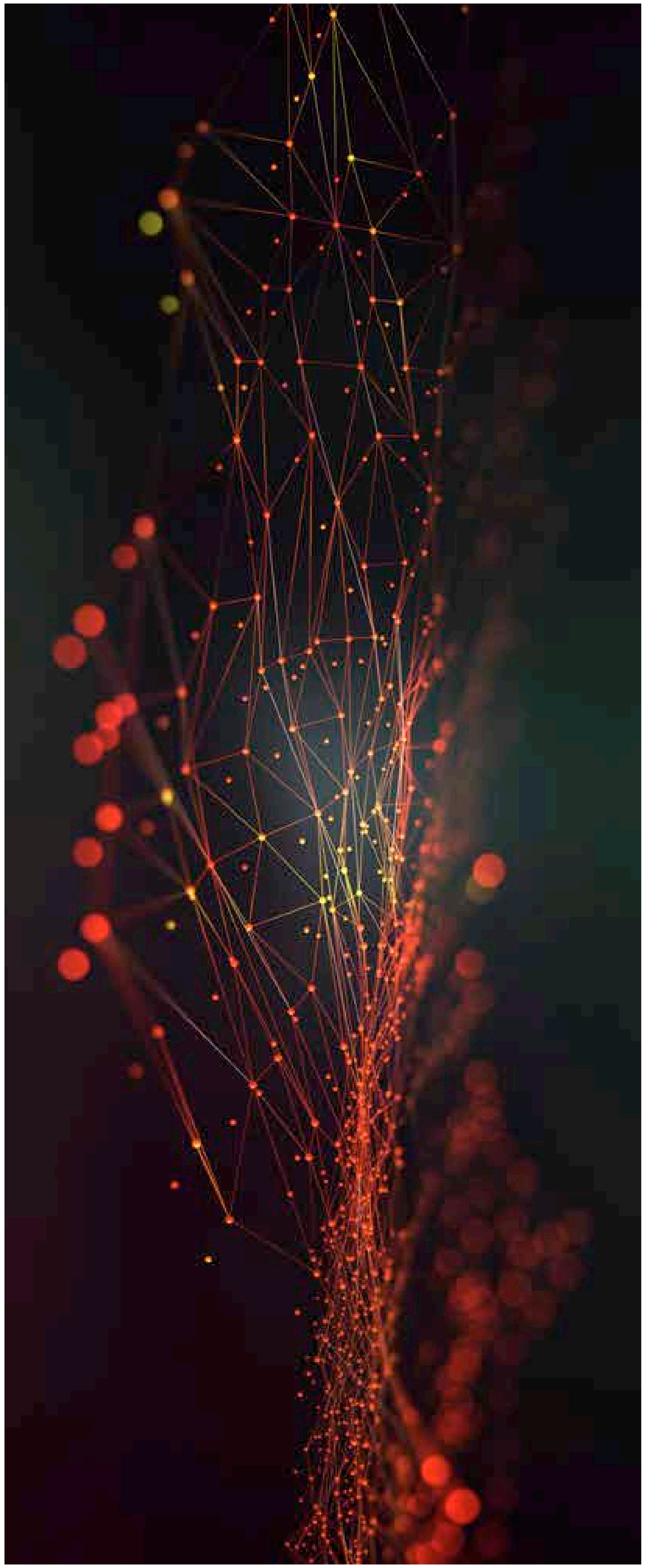
Example **APT29 Attack**

Delivery	Execution	Action	Privilege Escalation	Post-Escalation Action	Lateral Movement	Lateral Action
Spearphishing Attachment	Exploit Public-Facing Attachment	File and Directory Discovery	Bypass UAC	Registry Run Keys / Startup Folder	Pass the Ticket	Email Collection
Digital Certificates	Software Packing	Process Discovery	Domain Accounts	Steal or Forge Kerberos Tickets	SMB/Windows Admin Shares	Exfiltration Over C2 Channel
Malicious File	Non-Applcation Layer Protocol	System Information Discovery		Remote System Discovery		Data Compressed
Masquerading	Windows Command Shell	Query Registry		Input Capture		Data Encrypted
Shortcut Modification		Permission Groups Discovery		Modify Registry		Data Staged
				OS Credential Dumping		Data from Local System
Masquerading	Windows Command Shell	Query Registry	Domain Accounts	OS Credential Dumping	SMB/Windows Admin Shares	Data Encrypted

5. Legitimate Software Rating

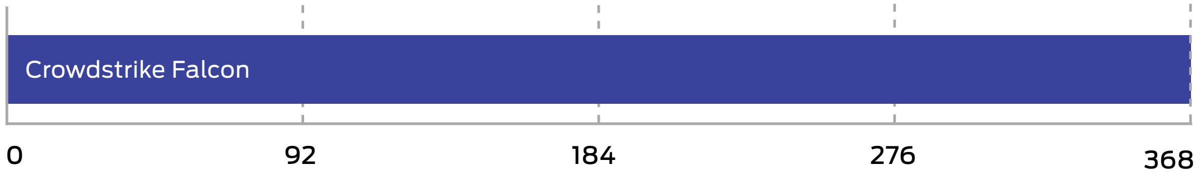
These ratings indicate how accurately the product classifies legitimate applications and URLs, while also taking into account the interactions that the product has with the user. Ideally a product will either not classify a legitimate object or will classify it as safe. In neither case should it bother 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 Ratings	Legitimate Accuracy (%)
Crowdstrike Falcon	368	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 all of the threats on a basic level, in that for each attack it detected at least some element of the attack chain. Even better, it also detected in depth, capturing details as each threat proceeded down the attack chain from the initial introduction to the system through to execution and subsequent behaviour by the attacker. In just one case it failed to detect one action by the attacker. However, in that specific test case it detected every other event, including the attack starting, running and continuing through to its conclusion. In the real world the attack would be detected at multiple stages.

The results are strong, and all attacks were detected to a near-perfect and full degree. 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 2nd August to 20th September 2021.
- 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

Dragonfly & Dragonfly 2.0

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

Oilrig

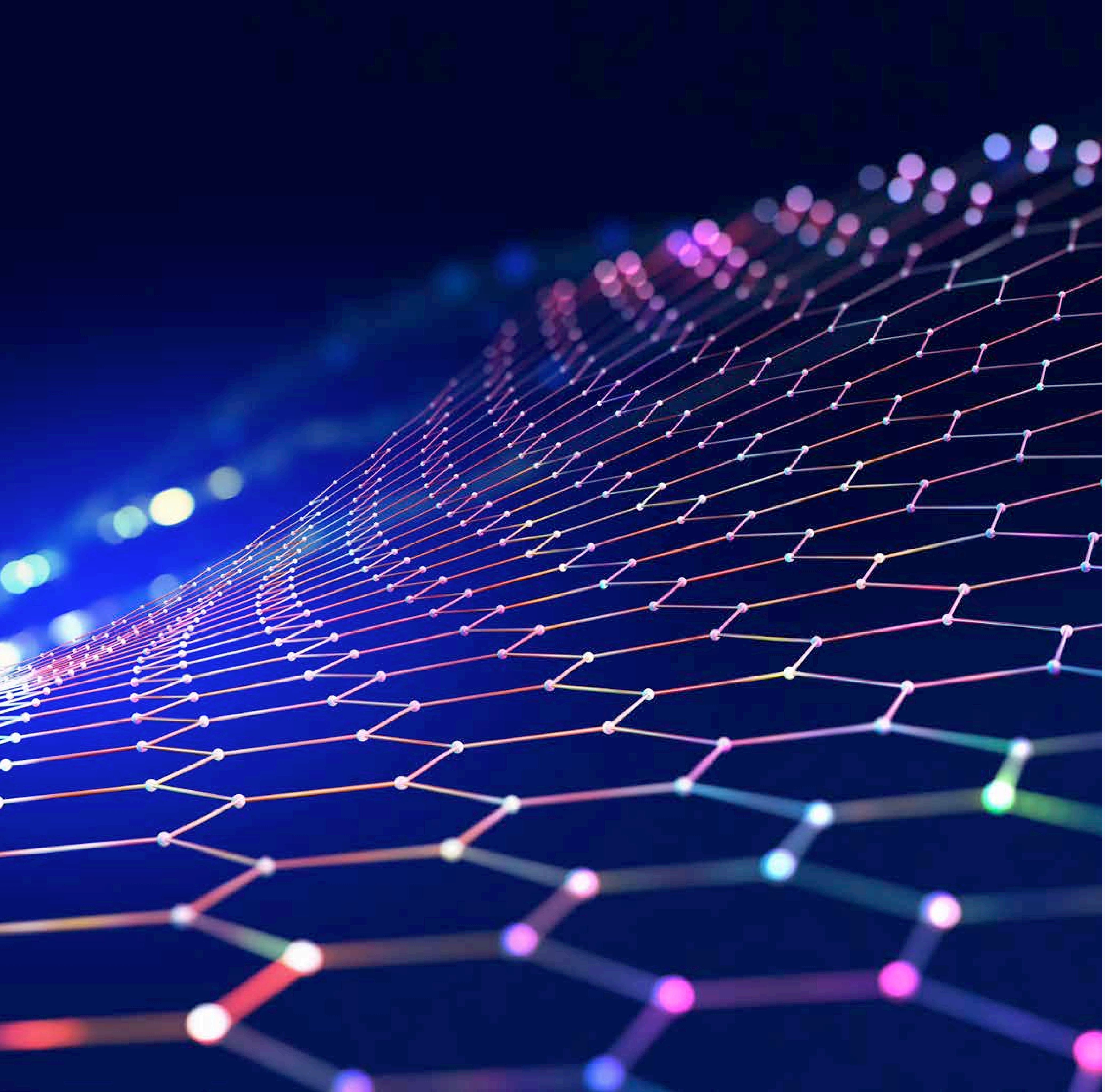
Incident No:	Delivery	Execution	Action	Privilege Escalation	Post-Escalation Action	Lateral Movement	Lateral Action
5	Spearphishing Attachment	Windows Command Shell	System Information Discovery	Bypass UAC	Password Policy Discovery	Remote Desktop Protocol	Automated Collection
	Malicious File	Deobfuscate/Decode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

FIN7 & Carbanak

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

APT29

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



SE Labs

SE Labs Report Disclaimer

1. The information contained in this report is subject to change and revision by SE Labs without notice.
2. SE Labs is under no obligation to update this report at any time.
3. SE Labs believes that the information contained within this report is accurate and reliable at the time of its publication, which can be found at the bottom of the contents page, but SE Labs does not guarantee this in any way.
4. All use of and any reliance on this report, or any information contained within this report, is solely at your own risk. SE Labs shall not be liable or responsible for any loss of profit (whether incurred directly or indirectly), any loss of goodwill or business reputation, any loss of data suffered, pure economic loss, cost of procurement of substitute goods or services, or other intangible loss, or any indirect, incidental, special or consequential loss, costs, damages, charges or expenses or exemplary damages arising his report in any way whatsoever.
5. The contents of this report does not constitute a recommendation, guarantee, endorsement or otherwise of any of the products listed, mentioned or tested.
6. The testing and subsequent results do not guarantee that there are no errors in the products, or that you will achieve the same or similar results. SE Labs does not guarantee in any way that the products will meet your expectations, requirements, specifications or needs.
7. Any trade marks, trade names, logos or images used in this report are the trade marks, trade names, logos or images of their respective owners.
8. The contents of this report are provided on an “AS IS” basis and accordingly SE Labs does not make any express or implied warranty or representation concerning its accuracy or completeness.