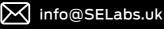
# BELADS INTELLIGENCE-LED TESTING

# **Enterprise Advanced Security**

# IronNet IronDefense











DETECTION



SE Labs tested **IronNet IronDefense** 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.

© 2022 SE Labs Ltd

# CONTENTS

Introduction	04
Executive Summary	05
Network Detection and 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
FIN7 & Carbanak	13
OilRig	14
APT3	15
APT29	16
5. Legitimate Software Rating	17
6. Conclusions	18
Appendicies	19
Appendix A: Terms Used	19
Appendix B: FAQs	19
Appendix C: Attack Details	20

Document version 1.0 Written: 3rd March 2022



### INTRODUCTION

# Network Threat Detection Assessment Full attack chain testing on the network

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

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

A very accurate sensor might not generate an alert when analysing such 'fake' test traffic. Ideally it would only alert on a real attack so that the team in the Security Operations Centre (SOC) focuses on significant events only. Parts of an exploit, malware or suspicious login are not a threat. Only a real attack looks like a real attack. A basic sensor might report problems with every packet that appears to be bad without looking at the context. For example, if a user logs into a system that they use regularly, an unsophisticated system might register that as a problem. A more intelligent one would recognise that all is well and hold back the alert. But it might sound the alarm if the same user logs in from an unusual part of the network. This could be a sign of an attacker moving between systems and using stolen login credentials.

In our tests we make no assumptions about how security products work and run full attacks, from the very first stages through to completing the final 'mission', which might be data damage, theft or the creation of a persistent presence. We replicate the behaviours of real-world attackers and use the MITRE ATT&CK framework to map out the attack chains used in every test case. We also perform benign activities to ensure that the product we are testing isn't just alerting without discrimination.

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

If you spot a detail in this report that you don't understand, or would like to discuss, please contact us via our Twitter account. SE Labs uses current threat intelligence to make our tests as realistic as possible. To learn more about how we test, how we define 'threat intelligence' and how we use it to improve our tests please visit our website and follow us on Twitter.

### ₲ SE Labs

# **Executive Summary**

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

We examined its abilities to:

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

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

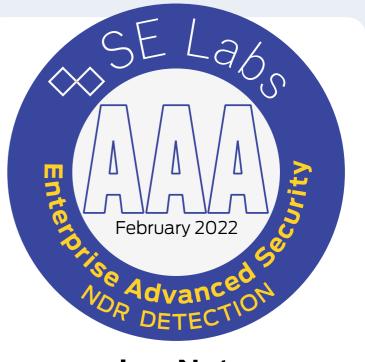
IronNet IronDefense was suspicious of some legitimate traffic but didn't block anything useful and was able to detect each targeted attack and track most of the hostile activities that occurred during the attacks.

Executive Summary			
Product Tested	Detection Accuracy Rating (%)	Legitimate Accuracy Rating (%)	Total Accuracy Rating (%)
IronNet IronDefense	100%	88%	94%

Green highlighting shows that the product was very accurate, scoring 85% or more for Total Accuracy. Yellow means between 75 and 85, while red is for scores of less than 75%.

# Network Detection and Response Award

The following product wins the SE Labs award:



### IronNet IronDefense

₲ SE Labs

# 1. How we Tested

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

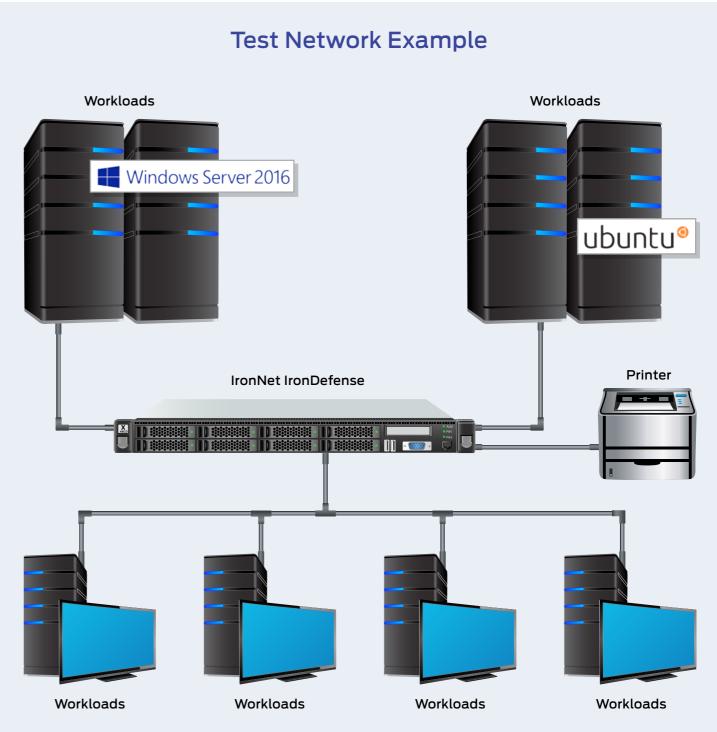
In the diagram on the right you will see an example network that contains workstations, some basic infrastructure such as file servers and a domain controller, as well as cloud-based email and a malicious command and control (C&C) server, which may be a conventional computer or a service such as Dropbox,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

6



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.

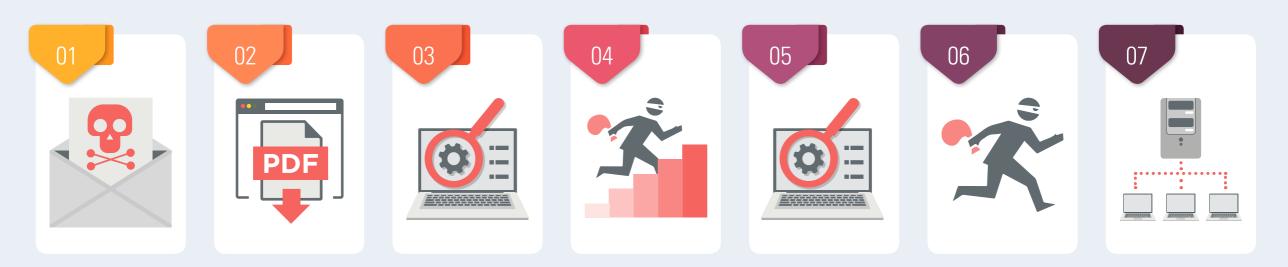
### Attack stages

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.

# Annual Report 2021

## Our 3rd Annual Report is now available

- Annual Awards Winners
- Ransomware in advanced security tests
- Security Testing DataBase
- Review: 6 years of endpoint protection





selabs.uk/ar2021

8

## 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.

9

Hackers vs. Targe	ets		
Attacker/APT Group	Method	Target	Details
FIN7 & Carbanak	W	الله الله	Documents containing scripts combined with public tools.
OilRig		\$ ∰ ∰	Phishing with email and other services, combined with public tools.
АРТЗ			Lateral movement focused on Windows Admin shares and RDP.
APT29			Spear phishing emails containing script or links to malware.



# 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 RatingsProductTotal Accuracy RatingTotal Accuracy (%)AwardIronNet IronDefense78594%AAA



# SE Labs Monthly Newsletter

### Don't miss our security articles and reports

- Test reports announced
- Blog posts reviewed
- Security testing analysed
- NEW: Podcast episodes



### 5 SF Labs

# **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)

11

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.

### PE 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 post-escalation 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.

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.



		First	group S	econd gi T	roup Thire	d group		Fourt	h group
Dragonf	ly & Dragor	nfly 2.0							
Incident No:	Detection	Delivery	Execution	Action	Escalatio	n PE Act	tion	Lateral Movement	Latera
1	1	1	1	(	1	1		1	1
2	1	12	1	1	1	1 1		1	1
з	1	-	1	1	1	1		1	1 1
4	1	1	1	-	1	1		1	1
Respons	se Details			<b>→</b>					
Attacker/ APT Grou		Number Inciden			Delivery/ Execution	Action	Escala	ilege ation/ tion	Lateral Movement Action
Dragonfly	& Dragonfly 2	4	4		4	2	4	4	4

Elements of the attack chain are put into groups. For example, the Delivery and Execution stages of an attack are in the same group. Similarly, we group the Post Escalation stage with the Post Escalation Action (PE Action) stage. When we count detections we look to see at least one detection (tick) in each group. One or two detections in a group is a success.

In this example we have four test cases, which we call 'incidents'. In Incident No. 1 there was a detection recorded for the delivery of the threat and when it was executed. These two results count as one detection. In Incident No. 2 the threat delivery was not detected, but its execution was. This also counts as one detection.

When no detection is registered in any part of a group the result will be a 'miss'. In Incident 1. there was no detection when the attacker performed the 'Action' stage of the attack. This is a miss for the product. In fact, this product only detected two of the four Action stages, which is why the Response Details table shows '2' in the Action column.

FIN7 & C	FIN7 & Carbanak									
Incident No:	Detection	Delivery	Execution	Action	Escalation	PE Action	Lateral Movement	Lateral Action		
1	1		1	n/a	n/a	1	1	<ul> <li>Image: A start of the start of</li></ul>		
2	1		1	n/a	n/a	1	1			
3	1		1	n/a	n/a	1	1	<ul> <li>Image: A second s</li></ul>		
4	1	_	1	n/a	n/a	1		1		

OilRig								
Incident No:	Detection	Delivery	Execution	Action	Escalation	PE Action	Lateral Movement	Lateral Action
5	1		1	n/a	n/a	1	1	1
6	1	1	1	n/a	n/a	1	1	n/a
7	1	1	1	n/a	n/a	n/a	1	1
8	1	1	1	n/a	n/a	1	1	n/a

АРТЗ								
Incident No:	Detection	Delivery	Execution	Action	Escalation	PE Action	Lateral Movement	Lateral Action
9	1	1	1	n/a	n/a	n/a	<ul> <li>Image: A second s</li></ul>	1
10	1	1	1	n/a	n/a	<ul> <li>Image: A second s</li></ul>	1	1
11	1	_	1	1	n/a	1	1	1

APT29								
Incident No:	Detection	Delivery	Execution	Action	Escalation	PE Action	Lateral Movement	Lateral Action
12	1	1	1	n/a	n/a	n/a	<ul> <li>Image: A second s</li></ul>	1
13	1	—	1	n/a	n/a	n/a	1	<ul> <li>Image: A second s</li></ul>
14	1		1	n/a	n/a	1	1	1
15	1	_	1	n/a	n/a	1	1	1

Response Details									
Attacker/ APT Group	Number of Incidents	Attacks Detected	Delivery/ Execution	Action	Privilege Escalation/ Action	Lateral Movement/ Action			
FIN7 & Carbanak	4	4	4	n/a	4	4			
Oilrig	4	4	4	n/a	3	4			
APT3	3	3	3	1	2	3			
APT29	4	4	4	n/a	2	4			
Total	15	15	15	1	11	15			

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

Detection Accuracy Rating Details									
Attacker/ APT Group	Number of Incidents	Attacks Detected	Group Detections	Detection Rating					
FIN7 & Carbanak	4	4	12	120					
Oilrig	4	4	11	110					
APT3	3	3	9	90					
APT29	4	4	10	100					
Total	15	15	42	420					

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

Detection Accuracy Ratings						
Product	Detection Accuracy Rating (%)					
IronNet IronDefense	420	100%				

1	I	I	1	1
IronNet Iro	onDefense			
	I.	I	1	
0	105	210	315	420

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

### **Group Detections**

We record detections in groups, as described above in Understanding Detection Groups. To get an overview of how a product handled the entire set of threats we then combine these detections into 'Group Detections'.

In a test with four incidents and four detection groups (Delivery/Execution; Action; Escalation/ PE Action; and Lateral Movement/ Lateral Action) the maximum score would be 16. This is because for each of the four threats a product that detects everything would score 4.

Our overall Detection Rating is based on the number of Detection Groups achieved.

# **4. Threat Intelligence** FIN7 and Carbanak

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

### References:

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

FIN7 (G0046) ×	÷1						), ± 🖩 O	≂,12,₽,⊗≎ 3 x m, ≝ <u>%</u>	
Reconnaissance 10 techniques		e Development techniques		itial Access 9 techniques		Execution 12 techniques		Persistence 19 techniques	
Active Scanning Gather Victim Host Information Gather Victim Identity Information Gather Victim Network Information Monte Victim Orig Information Information Search Closed Sources	Acquire infrastructure (1997) Campromise Accounts (1997) Compremise Infrastructure (1997) Develop Capabilities (1997) Establish Accounts (1997)	Code Signing Certificates     Exploit     Code Signing Certificates     Harlw     Digital Certificates     Malware     Phishie     Sector     Treton     Regis     Truste     Rediate     Valid	Drive-by Compromise Exploit Public Facing Application External Remote Services Hardware Additions	Spearphishing Attachment Spearphishing Link Spearphishing via Service	Command and Scripting Interpreter (Jam)	AppleScript JavaScript Network Device CLI PowerShell Python Unite Shell Visual Basic Windows Command Shell	Account Manipulation (1997) BITS Juba	Active Setup Authentication Package Kernel Modules and Extensions LSASS Driver Plist Modification Port Monitors Print Processors	Abuse Elevatio Control Mechanism (n Access Token Manipulation
Search Open Technical Databases mail Search Open Websites/Domains man Search Victim-Owned Websites	Obtain Capabilities <sub>(208)</sub> Stage Capabilities <sub>(208)</sub>		Replication Through Removable Media Supply Chain Companying Trusted Relationship Valid Accounts	0	Deploy Container Exploitation for Clevel Secution Inter-Process Communication (1) Native API	Component Object Model Dynamic Data Eschange At (Linux)	Execution (you)	Re-opened Applications Registry Run Keys / Startup Folder Security Support Provider Shortout Modification Time Providers Winlogon Helber DLL XDG Autostart Entries	Boot or Logo Autostart Execution <sub>(hit</sub> )
Attacker techr the MITRE ATT		nented by		-	Scheduled Task(Job <sub>rV/1</sub>	At (Windows) Container Orchestration Job Cron Launchd Scheduled Task	Boot or Logon Initialization Scripts Juli Browser Extensions Compromise Client Software		floot or Logon Initialization Scripta <sub>rang</sub> Create or Mod

Example FIN7 & Carb	oanak 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
	Commonly Used Port	File and Directory Discovery		Data Compressed		Data Encrypted
	Powershell	Process Discovery		Data Encrypted		Data from Local System
	Remote File Copy	System Information Discovery		Data from Local System	Pass the Hash	Data Staged
Obfuscated Files or Information	Scripting			Data Staged		
	Standard Application Layer Protocol		Valid Accounts	Exfiltration over Command and Control Channel		Exfiltration over Command and Control Channel
	Standard Cryptographic Protocol			Account Discovery		
		System Owner/User Discovery		Input Capture		
				Modify Registry		
				New Service		
	User Execution			Process Hollowing		
				Query Registry		
				Scheduled Task		
	<b>?</b> ?				f7ff9e8b7bb2e0d 9b70935a5d785b e0cc5d9d0abf0e	
Spearphishing Attachment	Standard Cryptographic Protocol	System Owner/User Discovery	Valid Accounts	Scheduled Task	Pass the Hash	Data Encrypted

# 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:

14

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

Reconnaissance 10 techniques	Resource Development 7 techniques		nitial Access 9 techniques		Execution 12 techniques		Persistence 19 techniques		ege Escalation 3 techniques	c									
Active Scanning <sub>cont</sub>	Acquire Infrastructure (1)(1)	Drive-by Compromise			AppleScript JavaScript	Account Manipulation mits		Abuse Elevation Control Mechanism (001)		Abuse Elevation Control Mechanism (1991)									
Information (1999) Gather Victim Identity	Compromise Accounts	Exploit Public- Facing Application		Second second	Network Device CLI	BITS Jobs Boot or Logon		Access Token Manipulation		Access Token Manipulation									
Information (5/3) Gather Victim Network S	Infrastructure (30)	External Remote		Command and Scripting	PowerShell	Autostart Execution (11947)	i i	Soot or Logon		BITS Jobs									
Information (UR)	Develop Capabilities (200)	Hardware		Interpreter (2.4)	Python Unix Shell	Boot or Logon Initialization		Autostart Execution (0/54)	1	Build Image on Host									
Gather Victim Org	Establish Accounts	Additions	Spearphishing Attachment		Visual Basic	Scripts (3/8) Browser	1	Boot or Logon Initialization Scripts (2011)		Deobfuscate/Decode Files or Information									
Phishing for Information	Obtain	Phishing (3/3)	Spearphishing Link		Windows Command Shell	Extensions		Create or Modify		Deploy Container									
Search Closed	Capabilities (1)(1) Stage	Contraction of Carlie	Spearphishing via Service	Container Administration Command		Compromise Client Software Binary		System Process (2(4)		Direct Volume Acces Domain Policy									
Sources <sub>(MIII</sub> Search Open	Capabilities (1.11)	Application Through		Deploy Container		Create		Domain Policy Modification		Modification (I)(T)									
Technical Databases <sub>midi</sub>		Removable Media		Exploitation for		Account	1	Escape to Host		Execution Guardralis (priv									
Search Open Websites/Domains (2+2)	2	Supply Chain Compromise		Client Execution	8	Create or Modify System Process (DM)		Event Triggered Execution (2018)		Exploitation for Defense Evasion									
Search Victim-Owned Websites		Trusted Relationship	Co	Communication (Int) Native API	the state of the s										Event Triggered Execution (11/10)		Exploitation for Privilege Escalation		File and Directory Permissions Modification (2010)
		Valid Accounts	-		At (Linux)	External Remote Services		Hijsck Execution	1	Hide Artifacts									
					At (Windows) Container Orchestration Job	Hijeck Execution Flow	5	Flow (1111) Process		Hijack Execution Flow (pro)									
				Scheduled	Cron	Implant Internal		Injection (1/11)		Impair Defenses									
				Task/Job (U7)	Launchd	image		1	At (Linux)										
					Scheduled Task	Modify Authentication			At (Windows)										
					Systemd Timers	Process (()(1)		Scheduled	Container Orchestration Job	Indicator Removal on									
Attacker techn	niques docum	nented		Shared Modules			Add-ins Office Template Macros	Task/Job (171	Cron	Host (1/0)									
by the MITRE A	ATT&CK fram	iework.		Software Deployment Tools		Office	Office Test	- T	Scheduled Task										

Example Oilrig Attac	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		Archive Collected Data: Archive via Utility				
	Windows Command Shell	Process Discovery		Scheduled Tasks						
		System Owner/User Discovery		Local Account	Remote Desktop Protocol	Screen Capture				
	Obfuscated File or Information	Local Groups	Valid Accounts	Domain Account						
Malicious Link			Valid Accounts	Password Policy Discovery						
		Domain Groups		Credentials in Files						
				Keylogging						
<b>@</b> 1				R						
Spearphishing Link	Powershell	System Information Discovery	Bypass UAC	Query Registry	Remote Desktop Protocol	Screen Capture				

# APT3

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

### References:

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

Reconnaissance	Resource Development 7 techniques		Access		Execution 12 techniques		Persistence 19 techniques		Privilege Escalation 13 techniques
Active Scenning (0/2)	Acquire	Drive-by			AppleScript	Account Manipulation		Abuse Elevation	
Gather Victim Host	Infrastructure (1/1)	Compromise			JavaScript		E	Control Mechanism	
Information USAC	Accounts (5/2)	Exploit Public- Facing			Network Device CLI	BITS Jobs	A	Access Token	
Oather Victim Identity Information	Compromise	Application		Command and	PowerShell		Active Setup	Manipulation volto	
Gather Victim Network	Infrastructure state	External Remote Services		Scripting Interpreter (3,9)	Python		Authentication Package		Active Setup
nformation (0.0)	Develop Capabilities	Hardware			Unix Shell		Kernel Modules and Extensions		Authentication Package
Bather Victim Org	Establish	Additions			Visual Basic		LSASS Driver		Kernel Modules and Extensions
Phishing for	Accounts (0.0)	Phishing (1:1) Replication			Windows Command Shell	Ê l	Plist Modification		LSASS Driver
information <sub>strill</sub>	Capabilities (MR) Stage Capabilities (MR) Stape Suppl	Replication Through		Container			Port Monitors		Plist Modification
Search Closed Sources mit:		Removable Media		Administration Command		Boot or Logon Autostart	Re-opened Applications Boot or Logon Autostart Print	Port Monitors	
Search Open		Supply Chain		Deploy Container		Execution (104)	Re-opened Applications		Print Processors
ichnical II atabases (cont)	Comprom(se (113)		Exploitation for			Registry Run Keys / Startup Folder	Execution (1/14)	Re-opened Applications	
Search Open	lpen	Trusted Relationship		Client Execution			Security Support Provider	(**5.b	Registry Run Keys / Startup Foi
Websites/Domains		manosamp	Cloud Accounts	Inter-Process Communication		Shortout Modification		Security Support Provider	
Search Victim-Owned		CHICAST	alid Default Accounts			Time Providers		Shortcut Modification	
Websites		Valid Accounts (100		NELVE AP.	A	· · · · ·	Winlogon Helper DLL		Time Providers
			Domain Accounts		At (Linux)		XDG Autostart Entries		Winlogon Helper DLL
			Local Accounta		At (Windows) Container Orchestration Job			Boot or Logon	XDG Autostart Entries
				Scheduled Task/Job cum	Cron	Scripts (said)		Initialization	
				1103070499	Launchd	Browser Extensions		Scripts (114)	
					Scheduled Task	Compromise		101101000000000000000000000000000000000	Launch Agent
					Systemd Timers	Client Software Binary		Create or Modify System	Launch Daemon
				Shared Modules	C. C. South Strengthere in the	1	Cloud Account	Process (1)40	Systemd Service
				Software		Create Account com	Domain Account	2-0200	Windows Service
				Deployment Tools		HOCODIN (1/3)	Local Account	Domain Policy Modification	u .
				System Services			Launch Agent	Escape to Host	
Attacker tech	niques docur	mented		User Execution			Launch Daemon	and a second	Accessibility Features
by the MITRE				Windows Management	-	System Process (1988)	Systemd Service		AppCert DLLs

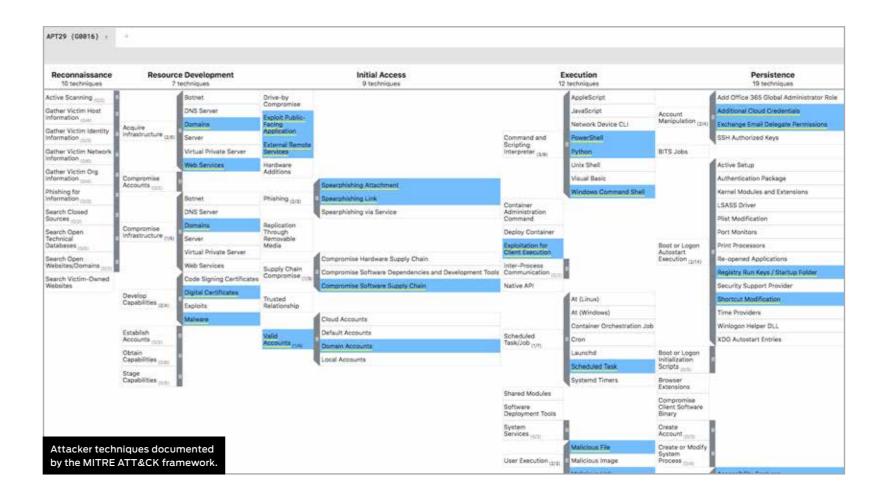
Example APT3 Attack	Example APT3 Attack								
Delivery	Execution	Action	Privilege Escalation	Post-Escalation Action	Lateral Movement	Lateral Action			
Spearphishing Link	PowerShell	File and Directory Discovery	Keylogging			Ingress Tool Transfer			
Obfuscated Files or Information	Windows Command Shell	Process Discovery	Domain Accounts	Registry Run Keys / Startup Folder	SMB/Windows Admin Shares	Archive via Utility			
	File Deletion	System Information Discovery	Domain Accounts	Data from Local System		Exfiltration Over C2 Channel			
	Hidden Window	System Owner/User Discovery				Local Data Staging			
Obfuscated Files or Information	File Deletion	System Information Discovery	Domain Accounts	Keylogging	SMB/Windows Admin Shares	Ingress Tool Transfer			

# APT29

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

### References:

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



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		Steal or Forge Kerberos Tickets		Exfiltration Over C2 Channel		
Malicious File	Non-Applcation Layer Protocol	System Information Discovery		Remote System Discovery	SMB/Windows Admin Shares	Data Compressed		
Masquerading		Query Registry	Domain Accounts	Input Capture		Data Encrypted		
Shortcut Modification	Windows Command Shell	Permission Groups Discovery		Modify Registry		Data Staged		
Shortcut Modification				OS Credential Dumping		Data from Local System		
Masquerading	C:\ 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 Rating	Legitimate Accuracy (%)
IronNet IronDefense	365	88%



# DELLADS

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 our how you can secure yourself online as effectively as a large company Download Now!

**⊻** selabs.uk

# ducts misclassify very popular software

# 6. Conclusions

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

The product detected all of the threats.

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

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

The results are strong and not one attack went undetected. IronNet IronDefense detected each attack at the execution stage, which is when it starts to run on a target. In two cases it also detected the threat as it was delivered to the target.

We don't expect every stage of an attack to be detected by a network detection system. This is because certain activities are not visible on the network. You would not expect a firewall, intrusion detection system or other network appliance to spot an attacker escalating privileges and installing a keylogger, for example. For this reason, in most test cases the Action and Escalation stages are marked as 'n/a'. Failure to detect these stages is not usually grounds to criticise a network security product.

In all but one case **IronNet IronDefense** detected the attackers moving through the network from one target to another. In nearly all appropriate cases it also detected the attackers' subsequent actions, once they had breached the next targets.

Sometimes products are overly aggressive and detect everything, including threats and legitimate objects. In this test **IronNet IronDefense** classified some legitimate traffic as being suspicious, which brings its scores down slightly. It didn't generate any full 'false positive' alerts, though, which is good.

**IronNet IronDefense** wins a AAA award for its excellent performance.

# SE Labs Monthly Newsletter

### Don't miss our security articles and reports

- Test reports announced
- Blog posts reviewed
- Security testing analysed
- NEW: Podcast episodes



# 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 February to 1st March 2022.
- The product was configured according to its vendor's recommendations.
- Targeted attacks were selected and verified by SE Labs.
- Malicious and legitimate data was provided to partner organisations once the test was complete.
- SE Labs conducted this network test using virtual systems.

# 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.

### We are a customer considering buying or changing our Network Detection and Response (NDR) product. Can you help?

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

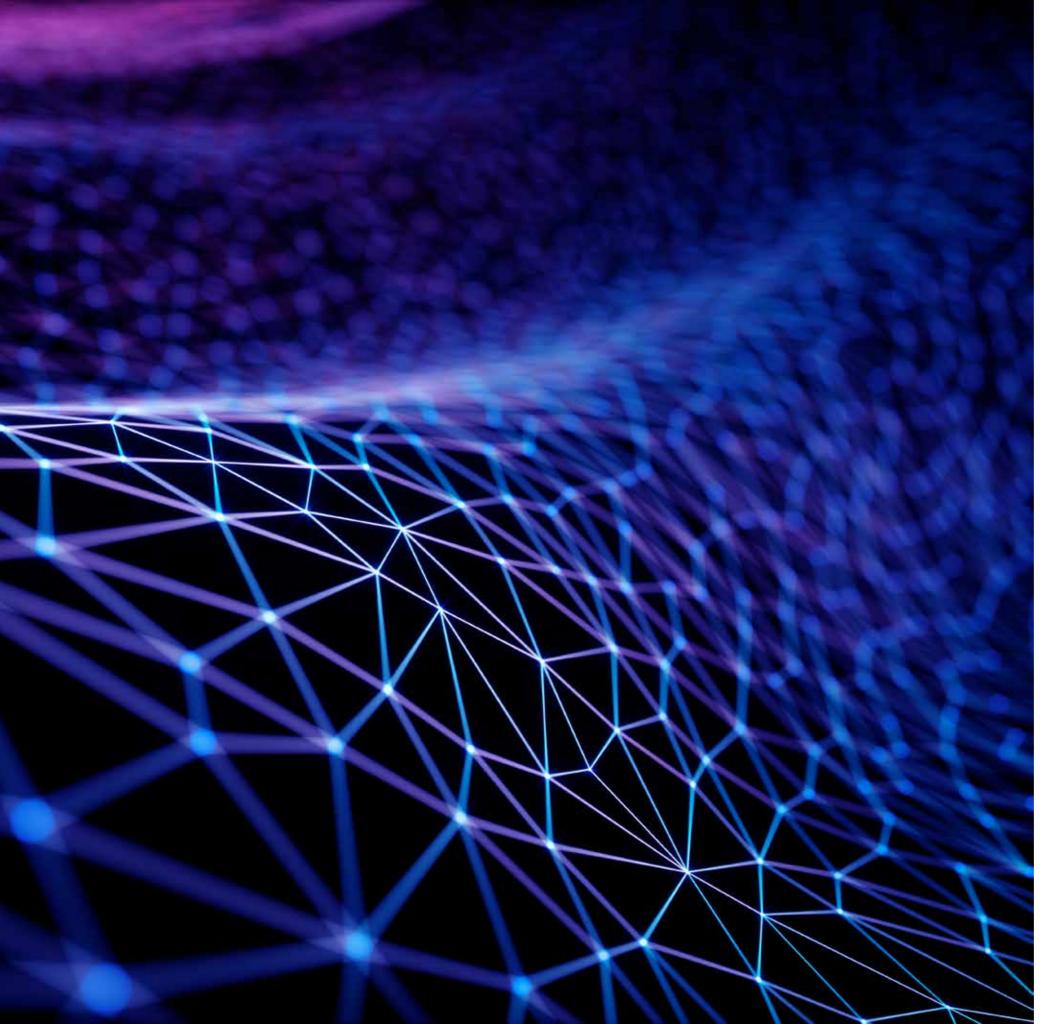
# Appendix C: Attack Details

FIN7 & Ca	rbanak						
Incident No:	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
		Commonly Used Port	File and Directory Discovery		Data Compressed		Data Encrypted
		Powershell	Process Discovery		Data Encrypted		Data from Local System
		Remote File Copy	System Information Discovery		Data from Local System		Data Staged
		Scripting			Data Staged		
,	Obfuscated Files or Information	Standard Application Layer Protocol			Exfiltration over Command and Control Channel		
1		Standard Cryptographic Protocol		Valid Accounts	Account Discovery	Pass the Hash	
					Input Capture		Exfiltration over Command
		User Execution	System Owner/User Discovery		Modify Registry		and Control Channel
					New Service		
					Process Hollowing		
					Query Registry		
					Scheduled Task		
		Command-Line Interface	Credentials from Web Browsers	Bypass UAC	Dll Search Order Hijacking		Data Compressed
		Code Signing	File and Directory Discovery		Data Compressed		Data Encrypted
		Commonly Used Port	Process Discovery		Data Encrypted		Data from Local System
		Masquerading	Process Injection		Data from Local System		Data Staged
2 Spearphishing A		Remote Access Tools	System Information Discovery		Data Staged		
		Service Execution			Disabling Security Tools		
	Spearphishing Attachment	Standard Non-Application Layer Protocol		Valid Accounts	Exfiltration over Command and Control Channel	Remote Desktop Protocol	
					Permission Groups Discovery		Exfiltration over Command and Control Channel
		User Execution	Valid Accounts		Query Registry		
					Registry Run Keys / Startup Folder		
					Screen Capture		
					System Network Configuration Discovery		
	Spearphishing Attachment	Command-Line Interface	Account Discovery	Bypass UAC	Application Shimming	Remote File Copy	Data Compressed
		Commonly Used Port	File and Directory Discovery		Credential Dumping	Pass the Hash	Data Encrypted
		Connection Proxy	Process Discovery		Data Compressed		Data from Local System
		mshta	System Information Discovery		Data Encrypted		Data Staged
3	Software Packing	Scripting	System Network Configuration Discovery	Valid Accounts	Data from Local System	Windows Admin Shares	
		Standard Non-Application Layer Protocol			Data Staged		Exfiltration over Command and Control Channel
		User Execution	- System Owner/User Discovery		Exfiltration over Command and Control Channel		
		Command-Line Interface	File and Directory Discovery	Bypass UAC	Application Window Discovery		Data from Local System
		Commonly Used Port	Process Discovery		Data Compressed		Data Compressed
		Component Object Model and Distributed COM			Data Encrypted		Data Encrypted
		Execution through API	1		Data from Local System		Data Staged
4	Spearphishing Attachment	Powershell	1		Data Staged	Windows Management	
•		Scripting	System Information Discovery	Valid Accounts	Hooking	Instrumentation	
		Standard Application Layer Protocol			Exfiltration over Command and Control Channel	_	Exfiltration over Command and Control Channel
			1		Hooking		
		Standard Cryptographic Protocol			Input Capture	1	

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

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

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



### ₲ SE Labs

### SE Labs Report Disclaimer

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