




INTELLIGENCE-LED TESTING

Enterprise Advanced Security

BlackBerry Protect and Optics

EDR
PROTECTION

January 2022



SE Labs tested **BlackBerry Protect and Optics** 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 Gorbald

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](https://twitter.com/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
Enterprise Advanced Security 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
Wizard Spider	13
Sandworm	14
Dragonfly & Dragonfly 2.0	15
5. Legitimate Software Rating	16
6. Conclusions	17
Appendicies	18
Appendix A: Terms Used	18
Appendix B: FAQs	18
Appendix C: Attack Details	19

Document version 1.0 Written 1st February 2022.
1.01 Corrected minor typo 28th March 2022.



INTRODUCTION

Preventive Endpoint Protection

Would you rather your security stopped the bad guys before they walk through the door?

There are many opportunities to spot and stop attackers. Products can detect them when attackers send phishing emails to targets. Or later, when other emails contain links to malicious code. Some kick into action when malware enters the system. Others sit up and notice when the attackers exhibit bad behaviour on the network.

Regardless of which stages your security takes effect, you probably want it to detect and prevent before the breach runs to its conclusion in the press.

Our Breach Response test is unique, in that we test products by running a full attack. We follow every step of a breach attempt to ensure that the test is as realistic as possible. This is important because different products can detect and prevent threats differently.

Ultimately you want your chosen security product to prevent a breach one way or another, but it's more ideal to stop a threat early, rather than watch as it wreaks havoc before stopping it and trying to clean up.

Some products are designed solely to watch and inform, while others can also get involved and remove threats either as soon as they appear or after they start causing damage.

For the 'watchers' we run the Breach Response test in Detection mode. For 'stoppers' like **BlackBerry Protect** we can demonstrate effectiveness by testing in Protection Mode.

In this report we look at how **BlackBerry Protect** handled full breach attempts. At which stages did it detect and protect? And did it allow business as usual, or mis-handle legitimate applications?

Understanding the capabilities of different security products is always better achieved before you need to use them in a live scenario. SE Labs' Breach Response test reports help you assess which are the best for your own organisation.

If you spot a detail in this report that you don't understand, or would like to discuss, please contact us via our [Twitter](#) 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

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

We examined its abilities to:

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

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

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

Executive Summary			
Product Tested	Protection Accuracy (%)	Legitimate Accuracy Rating (%)	Total Accuracy Rating (%)
BlackBerry Protect and Optics	100%	91%	97%

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%.

For exact percentages, see 2. Total Accuracy Ratings on page 10.

Enterprise Advanced Security Award

The following product wins the SE Labs award:



BlackBerry
Protect and Optics

1. How we Tested

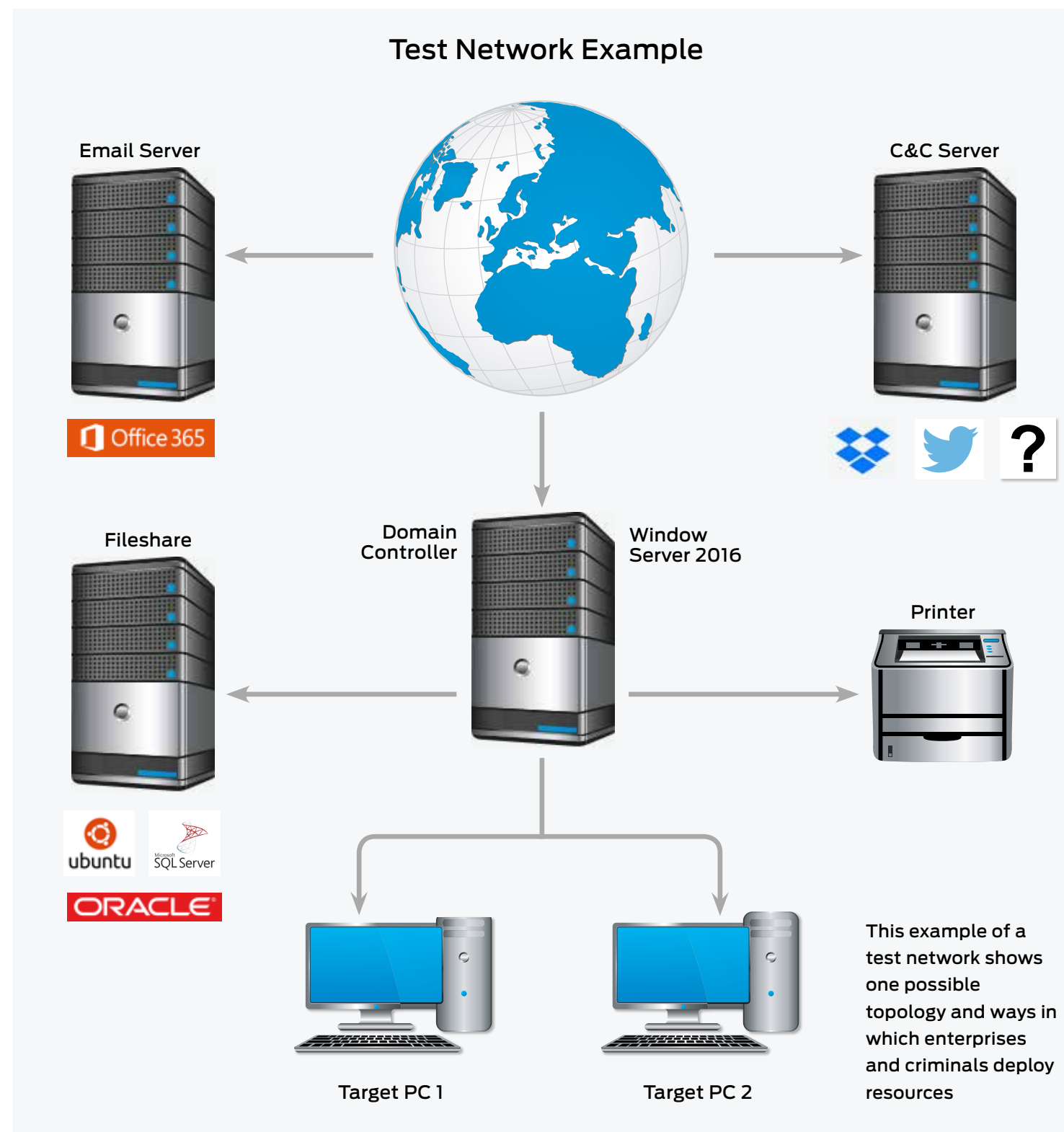
Testers can't assume that products will work a certain way, so running a realistic breach response test means setting up real networks and hacking them in the same way that real adversaries behave.

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

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

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

The techniques that we choose for each test case are largely dictated by the real-world behaviour of online criminals. We observe their tactics and replicate what they do in this test. To see more details about how the specific attackers behaved, and how we copied them, see **Hackers vs. Targets** on page 9 and, for a really detailed drill down on the details, **4. Threat Intelligence** on pages 13 to 15 and **Appendix C: Attack Details**.



Threat Responses

Full Attack Chain: Testing every layer of detection and protection

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

If the test starts too far into the attack chain, such as executing malware on an endpoint, then many products will be denied opportunities to use the full extent of their protection and detection

abilities. If the test concludes before any 'useful' damage or theft has been achieved, then similarly the product may be denied a chance to demonstrate its abilities in behavioural detection and so on.

Attack stages

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

We measure how a product responds to the first stages of the attack with a detection and/or protection rating. Sometimes products allow threats to run but detect them. Other times they

might allow the threat to run briefly before neutralising it. Ideally they detect and block the threat before it has a chance to run. Products may delete threats or automatically contain them in a 'quarantine' or other safe holding mechanism for later analysis.

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

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

ATTACK CHAIN STAGES

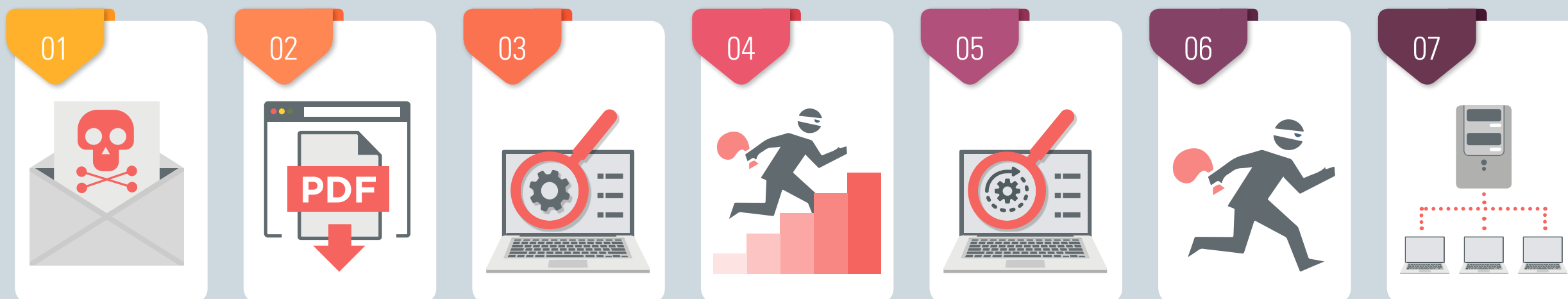


Figure 1. A typical attack starts with an initial contact and progresses through various stages, including reconnaissance, stealing data and causing damage.

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

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

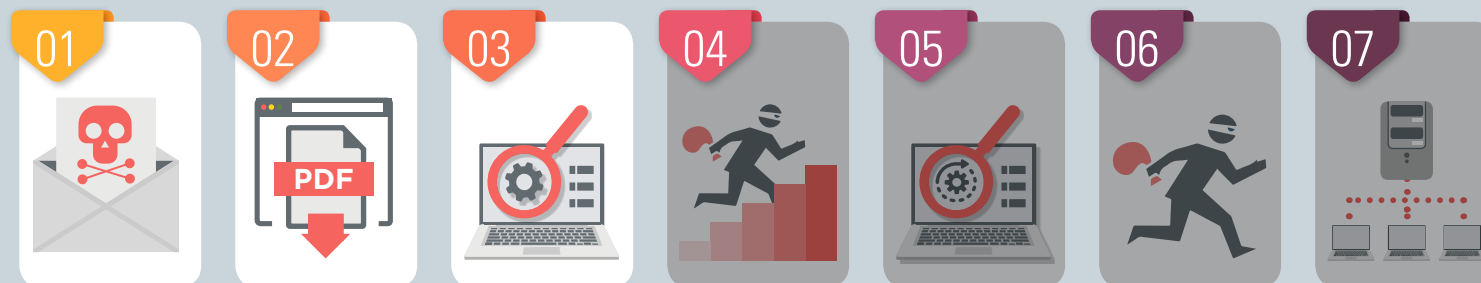


Figure 2. This attack was initially successful but only able to progress as far as the reconnaissance phase.

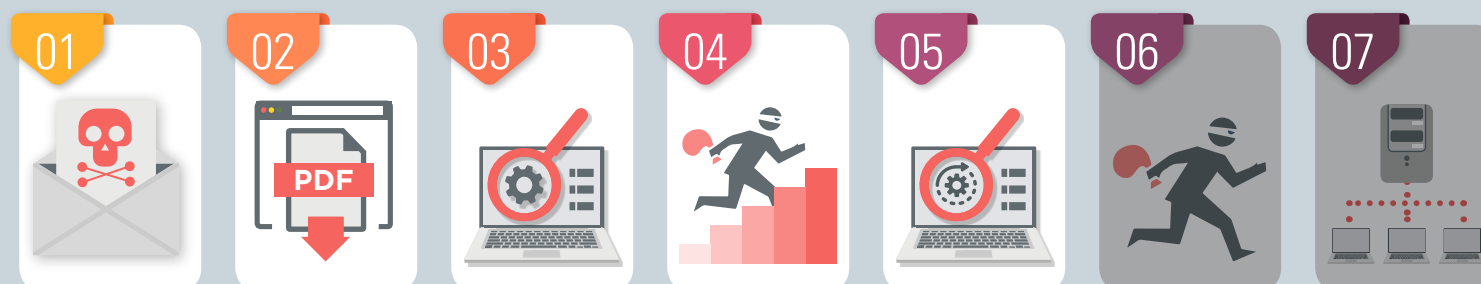


Figure 3. A more successful attack manages to steal passwords but wholesale data theft and destruction was blocked.



DOWNLOAD THE REPORT NOW!

(free – no registration)

selabs.uk/ar2021

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
Wizard Spider	 		Credential harvesting, cryptomining and implementation of ransomware.
Sandworm	 		Obtain sensitive network data via encryption and system data wiping.
Dragonfly & Dragonfly 2.0	 		Phishing & supply chain methods used to gain access.

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

2. Total Accuracy Ratings

Judging the effectiveness of an endpoint security product is a subtle art, and many factors are at play when assessing how well it performs. To make things easier we've combined all the different results from this report into one easy-to-understand chart.

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

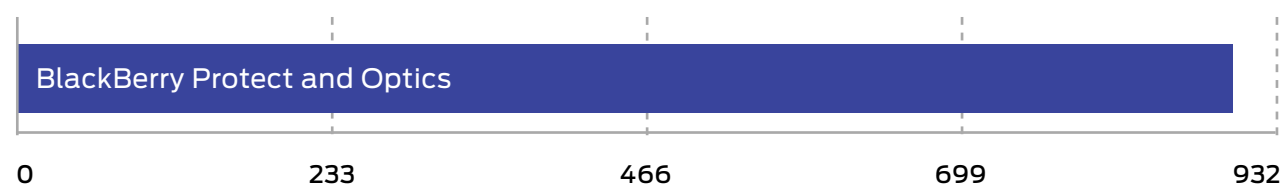
Not all protections, or detections for that matter, are equal. A product might completely block a URL, which stops the threat before it can even start its intended series of malicious events. Alternatively, the product might allow a web-based exploit to

execute but prevent it from downloading any further code to the target. In another case malware might run on the target for a short while before its behaviour is detected and its code is deleted or moved to a safe 'quarantine' area for future analysis. We take these outcomes into account when attributing points that form final ratings.

For example, a product that completely blocks a threat is rated more highly than one that allows a threat to run for a while before eventually evicting it. Products that allow all malware infections, or that block popular legitimate applications, are penalised heavily.

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

Total Accuracy Ratings			
Product	Total Accuracy Rating	Total Accuracy (%)	Award
BlackBerry Protect and Optics	900	97%	AAA



Total Accuracy Ratings combine protection and false positives.

SE Labs Monthly Newsletter

Don't miss our security articles and reports

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



SUBSCRIBE NOW!



3. Response Details

In this test security products are exposed to attacks, which comprise multiple stages. The perfect product will detect and protect against all relevant elements of an attack. The term 'relevant' is important, because if early stages of an attack are countered fully there is no need for later stages to be addressed.

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

Detection (-0.5)

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

Execution (-0.5)

Threats that are allowed to execute generate a penalty of 0.5 points.

Action (-1)

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

Privilege escalation (-2)

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

Post escalation action (-1)

New, more powerful and insidious actions are possible with escalated privileges. If these are successful, the product loses one more point.

Lateral movement (-2)

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

Lateral action (-2)

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

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

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

Response Details

Attacker/ APT Group	Number of Test Cases	Detection	Delivery	Execution	Action	Privilege Escalation	Post Escalation Action	Lateral Movement	Lateral Action	Protected	Penalties
Wizard Spider	12	12	0	0	0	0	0	0	0	12	0
Sandworm	12	12	0	0	0	0	0	0	0	12	0
Dragonfly & Dragonfly 2.0	12	12	0	0	0	0	0	0	0	12	0
Total	36	36	0	0	0	0	0	0	0	36	0

This data shows how the product handled different stages of each APT group. The columns labelled 'Delivery' through to 'Lateral Action' show how many times an attacker succeeded in achieving those goals. A 'zero' result is ideal.

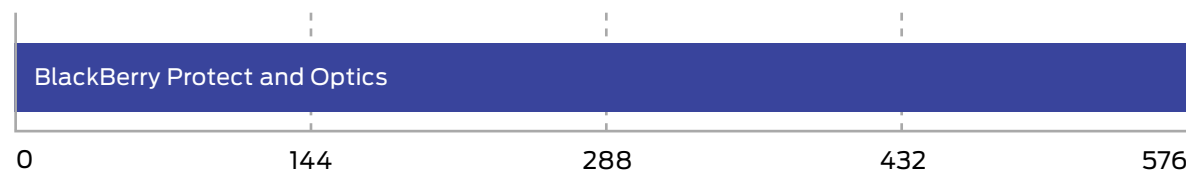
Protection Accuracy Rating Details

Attacker/ APT Group	Number of Test Cases	Protected	Penalties	Protection Score	Protection Rating
Wizard Spider	12	12	0	48	192
Sandworm	12	12	0	48	192
Dragonfly & Dragonfly 2.0	12	12	0	48	192
Grand Total	36	36	0	144	576

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

Protection Accuracy Ratings

Product	Protection Accuracy Rating	Protection Accuracy Rating (%)
BlackBerry Protect and Optics	576	100%



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

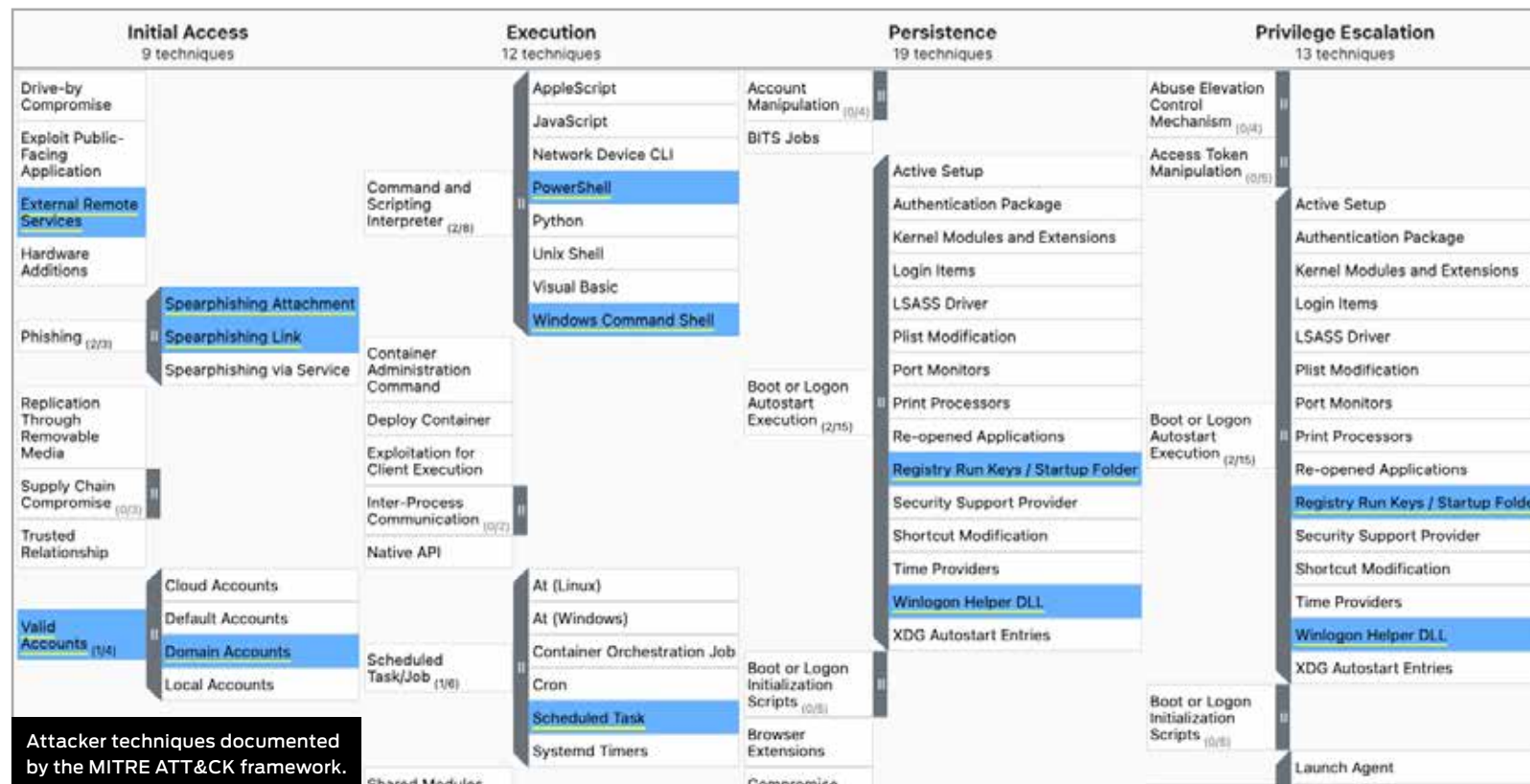
4. Threat Intelligence

Wizard Spider

Known to have operated since at least 2016, Wizard Spider is considered to be a threat group based in and around St. Petersburg, Russia. It is most notable for developing the TrickBot banking malware. Wizard Spider has infected over a million systems worldwide predominantly by using this malware.

Reference Link:

<https://attack.mitre.org/groups/G0102/>



Example Wizard Spider Attack						
Delivery	Execution	Action	Privilege Escalation	Post-Escalation Action	Lateral Movement	Lateral Action
Spearphishing Attachment	Windows Command Shell	File and Directory Discovery	Bypass User Account Control	Remote System Discovery	Service Execution	Archive Collected Data
	Malicious File	Process Discovery	Valid Accounts	Security Software Discovery	Domain Accounts	Data Staged
	Obfuscated Files or Information	System Information Discovery		LLMNR/NBT-NS Poisoning and SMB Relay		Data from Local System
	Powershell	System Network Configuration Discovery				Exfiltration Over C2 Channel
		System Owner/User Discovery				
Spearphishing Attachment	Obfuscated Files or Information	System Information Discovery	Valid Accounts	Security Software Discovery	Domain Accounts	Exfiltration over C2 Channel

Sandworm

In operation since around 2009, Sandworm Team is threat group that has been connected to Russia's Main Intelligence Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU). It is believed to be the GRU's Unit 74455. Notable campaigns include a targeted attack on the 2017 French Presidential campaign, as well as the worldwide NotPetya ransomware attack in the same year.

References:

<https://attack.mitre.org/groups/G0034/>

Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques
<ul style="list-style-type: none"> Spearphishing Attachment Spearphishing Link Spearphishing via Service 	<ul style="list-style-type: none"> AppleScript JavaScript Network Device CLI PowerShell Python Unix Shell Visual Basic Windows Command Shell 	<ul style="list-style-type: none"> Account Manipulation (0/4) BITS Jobs Boot or Logon Autostart Execution (0/15) Boot or Logon Initialization Scripts (0/5) Browser Extensions Compromise Client Software Binary Create Account (1/3) Create or Modify System Process (0/4) Event Triggered Execution (0/15) External Remote Services Hijack Execution Flow (0/11) 	<ul style="list-style-type: none"> Abuse Elevation Control Mechanism (0/4) Access Token Manipulation (0/5) Boot or Logon Autostart Execution (0/15) 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 (0/15) Exploitation for Privilege Escalation Hijack Execution Flow (0/11) Process Injection (0/11) Scheduled Task/Job
<ul style="list-style-type: none"> Compromise Hardware Supply Chain Compromise Software Dependencies and Development Tools Compromise Software Supply Chain 	<ul style="list-style-type: none"> Command and Scripting Interpreter (3/8) Container Administration Command Deploy Container Exploitation for Client Execution Inter-Process Communication (0/2) Native API Scheduled Task/Job (0/6) Shared Modules Software Deployment Tools System 	<ul style="list-style-type: none"> Cloud Account Domain Account Local Account 	
<ul style="list-style-type: none"> Cloud Accounts 	<ul style="list-style-type: none"> Attacker techniques documented by the MITRE ATT&CK framework. 		

Example Sandworm Attack						
Delivery	Execution	Action	Privilege Escalation	Post-Escalation Action	Lateral Movement	Lateral Action
Spearphishing Link	Windows Command Shell	File and Directory Discovery	Domain Accounts	Remote System Discovery	Lateral Tool Transfer	Data from Local System
	Powershell	System Information Discovery	Bypass UAC	LSASS Memory	SMB/Windows Admin Shares	Local Data Staging
	Malicious Link	System Owner/User Discovery				Exfiltration Over C2 Channel
	File Deletion	Data from Local System				Network Sniffing
	Obfuscated Files or Information	Local Data Staging				
		Exfiltration Over C2 Channel				

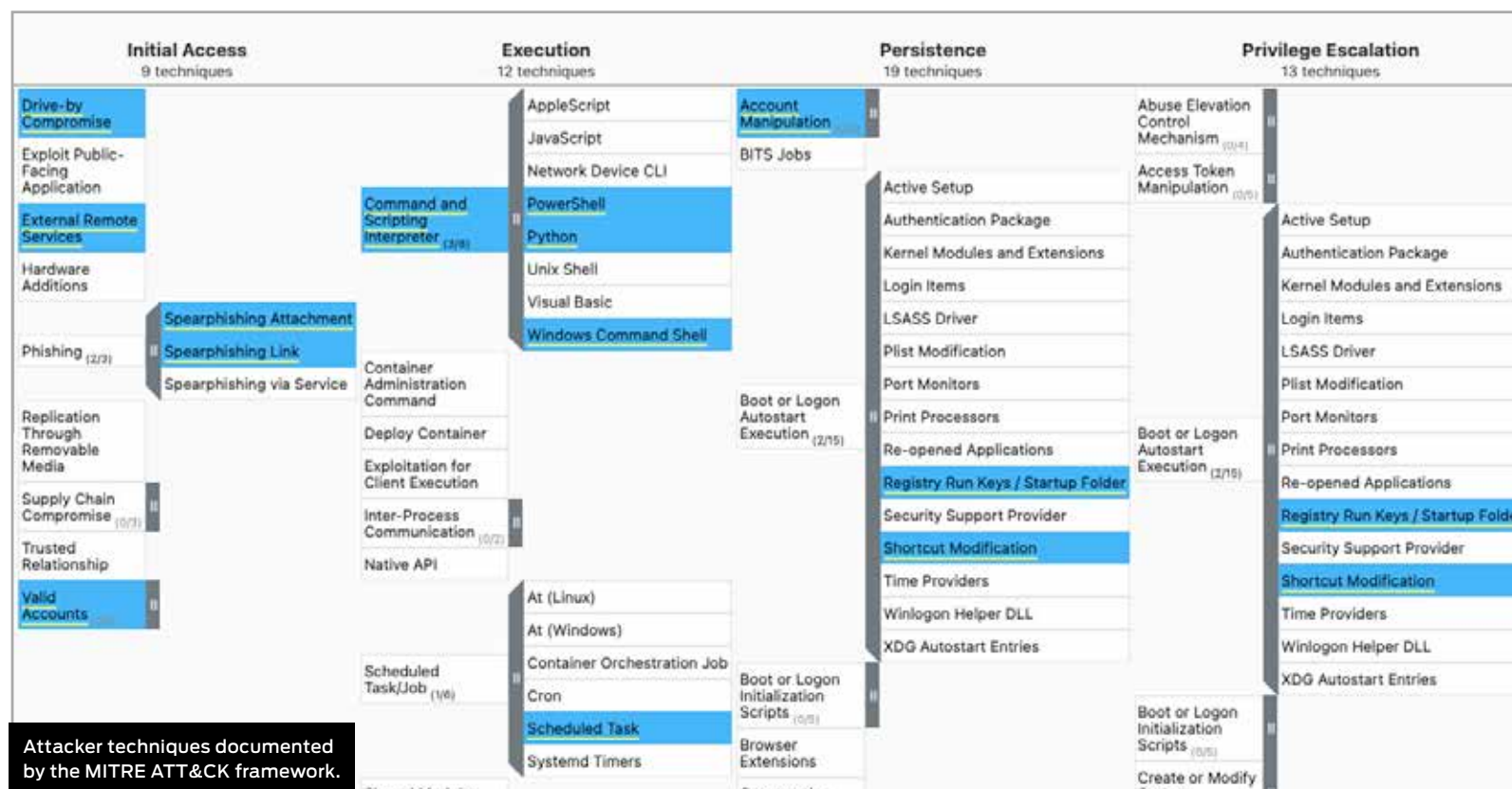
Dragonfly & Dragonfly 2.0

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

References:

<https://attack.mitre.org/groups/G0035/>

<https://attack.mitre.org/groups/G0074/>



Example Dragonfly & Dragonfly 2.0 Attack

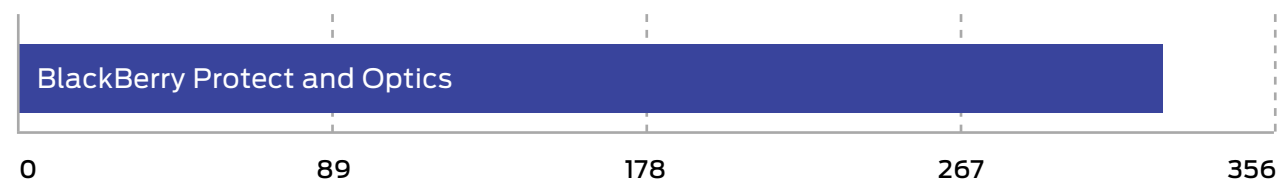
Delivery	Execution	Action	Privilege Escalation	Post-Escalation Action	Lateral Movement	Lateral Action
Spearphishing Attachment	Application Layer Protocol	System Information Discovery	Valid Accounts	Scheduled Task	Remote Desktop Protocol	Automated Exfiltration
Malicious File	Command and Scripting Interpreter	Process Discovery		Clear Windows Event Logs		Screen Capture
	Windows Command Shell	System Owner/User Discovery		File deletion		
	Powershell			Ingress Tool Transfer		
			Local Account			
			Domain Account			
			Shortcut Modification			
Malicious File	Powershell	System Owner/User Discovery	Valid Accounts	Scheduled Task	Remote Desktop Protocol	Screen Capture

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 (%)
BlackBerry Protect and Optics	324	91%



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

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



Enterprises

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

[Download Now!](#)

Small Businesses

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

[Download Now!](#)



Consumers

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

[Download Now!](#)

6. Conclusions

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

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

It is important to note that while the test used the same types of attacks, new files were used. This exercised the tested product's abilities to detect and protect against certain approaches to attacking systems rather than simply detecting malicious files that have become well-known over the previous few years. The results are an indicator of potential future performance rather than just a compliance check that the product can detect old attacks.

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

The results are strong and not one attack could progress far enough to the point at which the testers could start hacking through the targets. Sometimes products are overly aggressive and detect everything, including threats and legitimate objects. In this test BlackBerry Protect and Optics generated a low level of sub-optimal errors, misclassifying and blocking just one application.

BlackBerry Protect and Optics 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



SUBSCRIBE NOW!



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 A: FAQs

A [full methodology](#) for this test is available from our website.

- The test was conducted between 22nd and 31st November 2021.
- 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

Wizard Spider						
Delivery	Execution	Action	Privilege Escalation	Post-Esclation Action	Lateral Movement	Lateral Action
Spearphishing Attachment	Powershell	File and Directory Discovery	Bypass User Account Control	Remote System Discovery	External Remote Services	Archive Collected Data
Spearphishing Link	Windows Command Shell	Process Discovery	Valid Accounts	Security Software Discovery	Domain Accounts	Data from Local System
	Service Execution	System Information Discovery		Windows Service	Exploitation of Remote Services	Data Staged
	Malicious File	System Network Configuration Discovery		Scheduled Task	Lateral Tool Transfer	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol
	Malicious Link	System Owner/User Discovery		Winlogon Helper DLL	Remote Desktop Protocol	Exfiltration Over C2 Channel
	Obfuscated Files or Information	Permission Groups Discovery		Registry Run Keys / Startup Folder	SMB/Windows Admin Shares	Service Stop
	Code-Signing			Dynamic-link Library Injection	Windows Remote Management	
	Web Protocols			Windows File and Directory Permissions Modification	Windows Management Instrumentation	
	Non-Standard Port			Masquerade Task or Service		
				Modify Registry		
				LLMNR/NBT-NS Poisoning and SMB Relay		
NTDS						
		Security Account Manager				
		Kerberoasting				

Sandworm						
Delivery	Execution	Action	Privilege Escalation	Post-Esclation Action	Lateral Movement	Lateral Action
Spearphishing Attachment	Powershell	File and Directory Discovery	Domain Accounts	Credentials from Web Browsers	SSH	Cron
Spearphishing Link	Visual Basic	System Information Discovery	Bypass User Account Control	Keylogging	External Remote Services	Boot or Logon Initialization Scripts
	Windows Command Shell	System Owner/User Discovery	Setuid and Setgid	LSASS Memory	Remote Access Software	RC Scripts
	Unix Shell	System Network Configuration Discovery		Email Account (Discovery)		Systemd Service
	Malicious File	System Network Connections Discovery		Domain Account (Discovery)		Kernel Modules and Extension
	Malicious Link	Data from Local System		Remote System Discovery		SSH Authorized Keys
	Exploitation for Client Execution	Local Data Staging		Network Sniffing		/etc/passwd and /etc/shadow
	Valid Accounts	Exfiltration Over C2 Channel		Security Software Discovery		Bash History
	Web Shell			Ingress Tool Transfer		Clear Linux or Mac System Logs
	Deobfuscate/Decode Files or Information					
	File Deletion					
	Obfuscated Files or Information					
	Rundll32					
	Standard Encoding					
	Non-Standard Port					
	Proxy					
Web Protocols						
Bidirectional Communication						

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	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
3	Spearphishing 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

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.