SE LABS

EAS
PROTECTION

Advanced Security Test Report

[redacted]

[redacted]

JANUARY 2025

SE LABS ® tested [redacted] 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.

Contents

Document version 1.0 Written 6th January 2025

SE LABS

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
Jarred Earlington
Gia Gorbold
Anila Johny
Erica Marotta
Jeremiah Morgan
Julian Owusu-Abrokwa
Joseph Pike
Georgios Sakatzidi
Enejda Torba
Dimitrios Tsarouchas
Stephen Withey

Marketing
Sara Claridge
Janice Sheridan

Publication
Rahat Hussain
Colin Mackleworth

IT Support
Danny King-Smith
Chris Short

Website selabs.uk
Email info@SELabs.uk
LinkedIn www.linkedin.com/company/se-labs/
Blog blog.selabs.uk
Post SE Labs Ltd, 55A High Street, Wimbledon,
SW19 5BA, UK

SE Labs is ISO/IEC 27001 : 2022 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 Initiative (MVI);
the Anti-Malware Testing Standards Organization (AMTSO);
the Association of anti Virus Asia Researchers (AVAR);
and NetSecOPEN.

CEO
Simon Edwards

Resistance is not futile

Assessing endpoint resilience against advanced targeted and deep attacks

In this report the SE Labs testing team assessed [redacted] endpoint security configuration. The test used [redacted] hardware configured for normal use in the business and exposed these systems to advanced cyberattacks, the likes of which are known to have caused breaches in the real world in recent months.

We explored the configuration's resistance to attacks that seek to achieve low-level access to targets. The test focussed on advanced privilege escalation techniques and physical insider attacks using specialised hardware designed to help break into networks.

In the event that any of the attacks managed to penetrate the system fully, the testers were instructed to execute ransomware to determine the existence and extent of any special protections currently provided by the configuration.

The attacks themselves were based on criminal behaviour from a range of global adversaries. These included Russian, Chinese and Vietnamese groups believed to have targeted retail businesses, financial institutions, governmental organisations and national infrastructure. In addition, insider attacks were emulated using tools including customised USB devices designed to simplify hands-on endpoint attacks.

Attackers follow a process, from the initial stages of an attack through to the point at which they achieve their mission - or determine that they need a different approach to making a breach. The results from this test take into account the different stages of a typical cyberattack. These stages are illustrated in **1. Threat Responses**, on page 6, while the exact results are shown in **3. Response Details** on page 9. The results show how effective the security configuration was at detecting and protecting against each attack stage.

In addition we provide some general notes about how effective [redacted] approach is, compared to endpoint deployments at other organisations.

If you spot a detail in this report that you don't understand, or would like to discuss, please contact us. 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 LinkedIn.

Executive Summary

The [redacted] configuration was exposed to attacks similar to those launched by APT groups including FIN7; Dragonfly (and Dragonfly 2.0); APT29; APT32 and Sandworm. It also faced custom insider attacks designed for local, hands-on breach attempts.

- **The [redacted] security configuration tested was identical to that used within the [redacted] organisation.**

- **The testers tried to gain access, escalate privileges and perform significant damage to the system, including installing ransomware.**

- **Every attack was detected and all efforts to execute malicious code was prevented, meaning that protection was provided at the near-maximum level.**

- **After some attacks, malicious documents remained on the system. These remnants of the attack could pose a future risk to the organisation.**

Products Tested	Detection Accuracy Rating (%)	Protection Accuracy Rating (%)	Total Accuracy Rating (%)
[redacted]	100%	100%	93%

- 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 **1.3 Total Accuracy Ratings** on page 8.

1. 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 that, 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 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 yet still 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 5-6).

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.

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 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.

How Hackers Progress

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

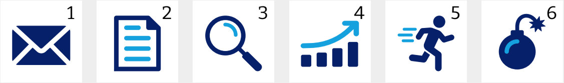
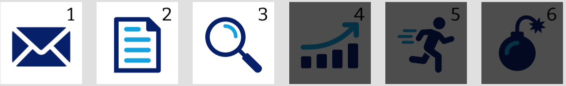


Figure 2. This attack was initially successful but only able to progress as far as the reconnaissance phase.



Attack Details

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.

Attacker/ APT Group	Targeted Nations	Target	Details
FIN7 & Carbanak	Russia, US, Germany	🛒	Documents containing scripts combined with public tools.
Dragonfly & Dragonfly 2.0	UAE, Saudi Arabia	💰 🏛 🏭	Phishing & supply chain methods used to gain access.
APT29	US , Hong Kong	🏛	Spear phishing emails containing scripts or links to malware.
APT32	Southeast Asia	🏛	Public tools used to obfuscate powershell and perform other code obfuscation.
Sandworm	Ukraine, France	🏛 🏭	Base64 encoding within their malware variants.
Custom	N/A	N/A	Custom USB, NET framework & Python based attacks.

KEY			
🏭	Energy	💰	Financial Industries
🏛	Government Espionage	🛒	US Retail, Restaurant and Hospitality

For more details about each APT group please see **4. Threat Intelligence on pages** 10-12.

2. Total Accuracy Rating

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.

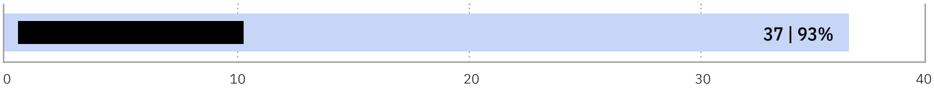
The chart below takes into account not only the product's ability to detect and protect against threats, but also its handling of non-malicious objects such as web addresses (URLs) and applications.

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 9.

Total Accuracy Rating



● Total Accuracy Ratings combine protection and false positives.

3. Response Details

In this test security products are exposed to attacks that comprise multiple stages. The perfect setup 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 4. Total Accuracy Ratings, these groups are as follows:

Delivery/Execution

If the configuration detects either the delivery or execution of the initial attack stage then a detection for this stage is recorded.

Protection

If the configuration subsequently protects the system by disallowing threats to run and correcting instantly any attempted changes to the target then the configuration has protected the system.

Action

When the attack performs one or more actions, while remotely controlling the target, the configuration should detect at least one of those actions.

Privilege Escalation/Action

As the attack progresses there will likely be an attempt to escalate system privileges and to perform more powerful and insidious actions. If the configuration can detect either the escalation process itself, or any resulting actions, then a detection is recorded.

Lateral movement/Action

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

Attacker/ APT Group	Incident No:	Detection	Complete Remediation	Delivery	Execution	Action	Escalation	PE Action
Fin7 & Carbanak	1	✓	✓	✓	✓	N/A	N/A	N/A
Dragonfly & Dragonfly 2.0	2	✓	✓	✓	✓	N/A	N/A	N/A
APT29	3	✓	✓	✓	✓	N/A	N/A	N/A
APT32	4	✓	✓	✓	✓	N/A	N/A	N/A
Sandworm	5	✓	✓	✓	✓	N/A	N/A	N/A
Dragonfly & Dragonfly 2.0	6	✓	✓	✓	✓	N/A	N/A	N/A
Custom	7	✓	✓	✓	✓	N/A	N/A	N/A
Custom	8	✓	✓	✓	✓	N/A	N/A	N/A
Custom	9	✓	✓	✓	✓	N/A	N/A	N/A
Custom	10	✓	✓	✓	✓	N/A	N/A	N/A

4. Threat Intelligence

FIN7 & 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.

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

Example FIN7 & Carbanak Attack

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

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.

Reference:
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
Spear phishing Link	Command and Scripting Interpreter	Domain Groups	Valid Accounts	Modify Registry
Malicious Link	Windows Command Shell	Remote System Discovery		Query Registry
	Powershell	System Information Discovery		Registry Run Keys / Startup Folder
		Process Discovery		Disable or Modify System Firewall
		System Owner/User Discovery		Forced Authentication

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.

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

Example APT29 Attack

Delivery	Execution	Action	Privilege Escalation	Post-Escalation Action
Spear phishing Attachment	Exploit Public-Facing Attachment	File and Directory Discovery	Bypass UAC	Registry Run Keys / Startup Folder
Digital Certificates	Software Packing	Process Discovery	Domain Accounts	Steal or Forge Kerberos Tickets
Malicious File	Non-Applcation Layer Protocol	System Information Discovery		Remote System Discovery
Masquerading	Windows Command Shell	Query Registry		Input Capture
Shortcut Modification		Permission Groups Discovery		Modify Registry
				OS Credential Dumping

APT32

This group has been active since at least 2014 and is known to target a variety of industries. Mostly focused in the private sector, targets such as foreign governments in Southeast Asian countries are also common.

Reference:
https://attack.mitre.org/groups/G0050/

Example APT32 Attack

Delivery	Execution	Action	Privilege Escalation	Post-Escalation Action
Spear phshing Attachment	User Execution	Account Discovery	Exploitation for Privilege Escalation	Exfiltration over Command and Control Channel
Ofuscated Files or Information	Powershell	Process Discovery		Indicator Removal
Malicious File	Command-Line Interface	File and Directory Discovery		Credential Dumping

Sandworm

This Russian-based group has been associated with worldwide attacks such as NotPetya and during the Winter Olympic games in 2018. It has been active since 2019 and has focused on a variety of different targets.

Reference:
https://attack.mitre.org/groups/G0034/

Example Sandworm Attack

Delivery	Execution	Action	Privilege Escalation	Post-Escalation Action
Spear phishing Attachment	Malicious File	File and Directory Discovery	Bypass User Account Control	Credentials from Web Browsers
Spear phishing Link	Malicious Link	System Information Discovery	Setuid and Setgid	Keylogging
	Standard Encoding	Data from Local System		LSASS Memory
	Non-Standard Port	Local Data Staging		Security Software Discovery
	Powershell	Exfiltration Over C2 Channel		Ingress Tool Transfer

Custom

We performed a variety of specialised attacks to simulate likely and imaginative attack vectors. For example, we used USB devices programmed to automate physical attacks on endpoints and used the latest Python-based attacks to assess protection.

Example Custom Attack

Delivery	Execution	Action	Privilege Escalation	Post-Escalation Action
Spear phishing attachment	Powershell	File and Directory Discovery	Bypass UAC	Automated Exfiltration
Spear phishing link	Visual Basic	System Information Discovery	Exploitation for Privilege Escalation	Screen Capture
Attack PC via USB Connection	Malicious File	Data from Local System		Exfiltration Over C2 Channel
	User Execution	Local Data Staging		
	Python	Exfiltration Over C2 Channel		

5. Conclusion

The threats in this test were all based on targeted attacks seen in the real world, as executed by skilled and professional opponents. We copy the tactics, techniques and procedures employed by cybercriminals and nation state actors to ensure that the test results are relevant. The more relevant the result, the more useful it is for a business hoping to validate or improve its security.

Threats are a process. An attack is a chain of events that starts with the initial contact, such as when you receive a malicious email or visit an infected website. We need to test using each stage of the attack to ensure that security measures have every opportunity to either succeed or fail. We explore attack chains in **1. Threat Responses** on page 6.

The [redacted] security configuration we tested in this report was exactly the same as is used within the [redacted] organisation. During the test we used [redacted] laptops configured as if we were genuine employees. We then tried to gain unauthorised levels of access to the systems that would allow attackers to perform powerful and often hidden malicious actions.

The common term for gaining these powerful levels of access is privilege escalation. An attacker who can use the system as a standard user can steal certain files and perform harmful actions, but an attacker that gains 'system-level' access can do much more. Examples include installing ransomware; running spying software to record strokes made on the keyboard; and activating microphones and cameras attached to the target system.

In this test our goal was to gain access, escalate privileges and perform significant damage to the system, including installing ransomware. We even used specialist hardware designed to gain unauthorised physical access. In other words, we emulated what could happen if we stood near a [redacted] laptop and had a few seconds to insert a specially programmed USB key capable to running automatic attacks.

The test results were very positive for [redacted] security stance (although disappointing from an attacker's point of view!) Each attempt to gain higher-level access was thwarted. Every attack was detected and all efforts to execute malicious code was prevented, meaning that protection was provided at the near-maximum level.

So why is the Total Accuracy Rating 93%, instead of 100%?

While the configuration protected the system against all attacks, our scoring penalises it for leaving some malicious documents on the system. These remnants of the attack could pose a future risk to the organisation, hence the scoring penalty. This is a common situation with certain security products in other organisations. They can detect some threats and delete them instantly. However, while they usually stop document-based attacks that involve malicious PDFs or Microsoft Office documents, they often fail to provide a thorough clean-up afterwards.

The problem with this scenario is that employees are usually diligent, want to do their work and will take extraordinary steps to achieve their goals when the computer appears to fail. If they believe that the Word document sent to them by their manager is necessary, they will try to open it. If the document doesn't open on their work laptop they may try it on another system (perhaps their home computer). Security products that don't delete malicious documents leave a dangerous weapon in a victim's hands. Only they don't know it's a weapon. This is why we recommend removing all malicious code during and after an attack and penalise products and configurations that leave significant elements of an attack in place.

All that said, in this test the [redacted] endpoint security configuration faced advanced attacks and detected all of them, preventing unauthorised access and denying any chance of the attacker gaining dangerously powerful levels of control over the target.

Appendices

Appendix A: Protection Ratings

The results below indicate how effectively the products dealt with threats. Points are earned for detecting the threat and for either blocking or neutralising it.

🟦 **Detected (+1)** If the product detects the threat with any degree of useful information, we award it one point.

🟩 **Blocked (+2)** Threats that are disallowed from even starting their malicious activities are blocked. Blocking products score two points.

🟩 **Complete Remediation (+1)** If, in addition to neutralising a threat, the product removes all significant traces of the attack, it gains an additional one point.

🟨 **Neutralised (+1)** Products that kill all running malicious processes 'neutralise' the threat and win one point.

🟧 **Persistent Neutralisation (-2)** This result occurs when a product continually blocks a persistent threat from achieving its aim, while not removing it from the system.

🟥 **Compromised (-5)** If the threat compromises the system, the product loses five points. This loss may be reduced to four points if it manages to detect the threat (see Detected, above), as this at least alerts the user, who may now take steps to secure the system.

Rating Calculations

We calculate the protection ratings using the following formula:

Protection Rating =
(1x number of Detected) +
(2x number of Blocked) +
(1x number of Neutralised) +
(1x number of Complete Remediation) +
(-5x number of Compromised)

The 'Complete Remediation' number relates to cases of neutralisation in which all significant traces of the attack were removed from the target.

These ratings are based on our opinion of how important these different outcomes are. You may have a different view on how seriously you treat a 'Compromise' or 'Neutralisation without complete remediation'.

Targeted Attack Scoring

The following scores apply only to targeted attacks and are cumulative, ranging from -1 to -5.

■ **Access (-1)** If any command that yields information about the target system is successful this score is applied. Examples of successful commands include listing current running processes, exploring the file system and so on. If the first command is attempted and the session is terminated by the product without the command being successful the score of Neutralised (see above) will be applied.

■ **Action (-1)** If the attacker is able to exfiltrate a document from the target's Desktop of the currently logged in user then an 'action' has been successfully taken.

■ **Escalation (-2)** The attacker attempts to escalate privileges to NT Authority/System. If successful, an additional two points are deducted.

■ **Post-Escalation Action (-1)** After escalation the attacker attempts actions that rely on escalated privileges. These include attempting to steal credentials, modifying the file system and recording keystrokes. If any of these actions are successful then a further penalty of one point deduction is applied.

Appendix B: Terms Used

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 C: FAQs

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 I am a security vendor and you tested my product without permission. May I access the threat data to verify that your results are accurate?

A We are willing to share a certain level of test data with non-partner participants for free. The intention is to provide sufficient data to demonstrate that the results are accurate. For more in-depth data suitable for product improvement purposes we recommend becoming a partner.

A full methodology for this test is available from our website.

- The product was configured according to its vendor's recommendations.
- The test was conducted between 6th and 27th October 2021.
- Targeted attacks were selected and verified by SE Labs.
- SE Labs conducted this endpoint test using physical systems.

Appendix D: Attack Details

FIN7 & Carbanak

Incident No:	Delivery	Execution	Action	Privilege Escalation	Post-Escalation Action
1	Spear phishing Attachment	Command-Line Interface	Account Discovery	Bypass UAC	Credential Dumping
	Obfuscated Files or Information	Commonly Used Port	File and Directory Discovery	Valid Accounts	Data Compressed
		Powershell	Process Discovery		Data Encrypted
		Scripting	System Information Discovery		Data from Local System
		Standard Application Layer Protocol	System Owner/User Discovery		Data Staged
		User Execution			Exfiltration over Command and Control Channel
					File Deletion
					Input Capture
					Modify Registry
					New Service
					Process Hollowing
					Query Registry
					Scheduled Task

Dragonfly & Dragonfly 2.0

Incident No:	Delivery	Execution	Action	Privilege Escalation	Post-Escalation Action
2	Spear phishing Link	Command and Scripting Interpreter	Domain Groups	Valid Accounts	Modify Registry
	Malicious Link	Windows Command Shell	Remote System Discovery		Query Registry
		Powershell	System Information Discovery		Registry Run Keys / Startup Folder
			Process Discovery		Disable or Modify System Firewall
			System Owner/User Discovery		Forced Authentication
3	Spear phishing Link	Command and Scripting Interpreter	System Information Discovery	Valid Accounts	System Network Configuration Discovery
	Malicious Link	PowerShell	Process Discovery		Archive Collected Data
			System Owner/User Discovery		Data from Local System
			File and Directory Discovery		Local Data Staging
			Network Share Discovery		Exfiltration Over C2 Channel
					Credentials from Password Stores
					LSA Secrets

APT29

Incident No:	Delivery	Execution	Action	Privilege Escalation	Post-Escalation Action
4	Web Services	PowerShell	File and Directory Discovery	Bypass UAC	Scheduled Task
	Spear phishing Link	Non-Application Layer Protocol	Process Discovery	Domain Accounts	Windows Management Intrumentation
	Obfuscated Files or Information	Windows Command Shell	System Information Discovery		Steal or Forge Kerberos Tickets
		Deobfuscate/Decode File or Information	System Network Confriguration Discovery		Remote System Discovery
		Python	System Owner/User Discovery		OS Credential Dumping

APT32

Incident No:	Delivery	Execution	Action	Privilege Escalation	Post-Escalation Action
5	Spear phshing Attachment	User Execution	Account Discovery	Exploitation for Privilege Escalation	Exfiltration over Command and Control Channel
	Ovfuscated Files or Information	Powershell	Process Discovery		Indicator Removal
	Malicious File	Command-Line Interface	File and Directory Discovery		Credential Dumping

Sandworm

Incident No:	Delivery	Execution	Action	Privilege Escalation	Post-Escalation Action
6	Spear phishing attachment	Malicious File	File and Directory Discovery	Bypass User Account Control	Credentials from Web Browsers
	Spear phishing link	Malicious Link	System Information Discovery	Setuid and Setgid	Keylogging
		Standard Encoding	Data from Local System		LSASS Memory
		Non-Standard Port	Local Data Staging		Security Software Discovery
		Powershell	Exfiltration Over C2 Channel		Ingress Tool Transfer

Custom

Incident No:	Delivery	Execution	Action	Privilege Escalation	Post-Escalation Action
7-10	Spear phishing attachment	Powershell	File and Directory Discovery	BypassUAC	Automated Exfiltration
	Spear phishing link	Visual Basic	System Information Discovery	Exploitation for Privilege Escalation	Screen Capture
	Attack PC via USB Connection	Malicious File	Data from Local System		Exfiltration Over C2 Channel
		User Execution	Local Data Staging		
		Python	Exfiltration Over C2 Channel		

SE LABS

SE Labs Report Disclaimer

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