SE Labs

INTELLIGENCE-LED TESTING

Enterprise Advanced Security

EDR PROTECTION

Cisco Secure Endpoint

September 2023

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

SE Labs tested **Cisco Secure Endpoint** against targeted attacks based on the Turla threat.

These attacks are designed to compromise systems and penetrate target networks in the same way as the advanced persistent hacking group known as Turla operates to 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
Gia Gorbold
Anila Johny
Erica Marotta
Luca Menegazzo
Jeremiah Morgan
Julian Owusu-Abrokwa
Joseph Pike
Georgios Sakatzidi
Dimitrios Tsarouchas
Stephen Withey

Publication and Marketing
Colin Mackleworth
Sara Claridge
Janice Sheridan

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 : 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 Initiative (MVI);
the Anti-Malware Testing Standards Organization (AMTSO);
the Association of anti Virus Asia Researchers (AVAR);
and NetSecOPEN.

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
Turla 13
5. Legitimate Software Rating 14
6. Conclusions 15
Appendicies 16
Appendix A: Terms Used 16
Appendix B: FAQs 16
Appendix C: Product Versions 17
Appendix D: Attack Details 17

Document version 1.0 Written 15th September 2023

Introduction

Early Protection Systems

Testing protection against fully featured attacks

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 Enterprise Advanced Security 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 Enterprise Advanced Security test in Detection mode. For 'stoppers' like **Cisco Secure Endpoint** we can demonstrate effectiveness by testing in Protection Mode.

In this report we look at how **Cisco Secure Endpoint** 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' Enterprise Advanced Security 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**. 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

SE Labs tested **Cisco Secure Endpoint** against targeted attacks based on the Turla threat.

These attacks are designed to compromise systems and penetrate target networks in the same way as the advanced persistent hacking group known as Turla operates to 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-optimal interactions.

Cisco Secure Endpoint scored a 100% Protection Accuracy Rating for blocking every threat at the initial delivery stage. The product did not generate any false positives, meaning that it didn't wrongly detect or hamper harmless, legitimate software.

It also prevented all of the malicious activities from running, incurring no penalties for allowing the full or partial execution of targeted attacks.

The product did not generate false positives, meaning that it didn't wrongly detect or hamper harmless, legitimate software.

Executive Summary

Product Tested	Detection Accuracy Rating (%)	Protection Accuracy Rating (%)	Legitimate Accuracy Rating (%)	Total Accuracy Rating (%)
Cisco Secure Endpoint	100%	100%	100%	100%

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:

Cisco Secure Endpoint

1. How We Tested

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

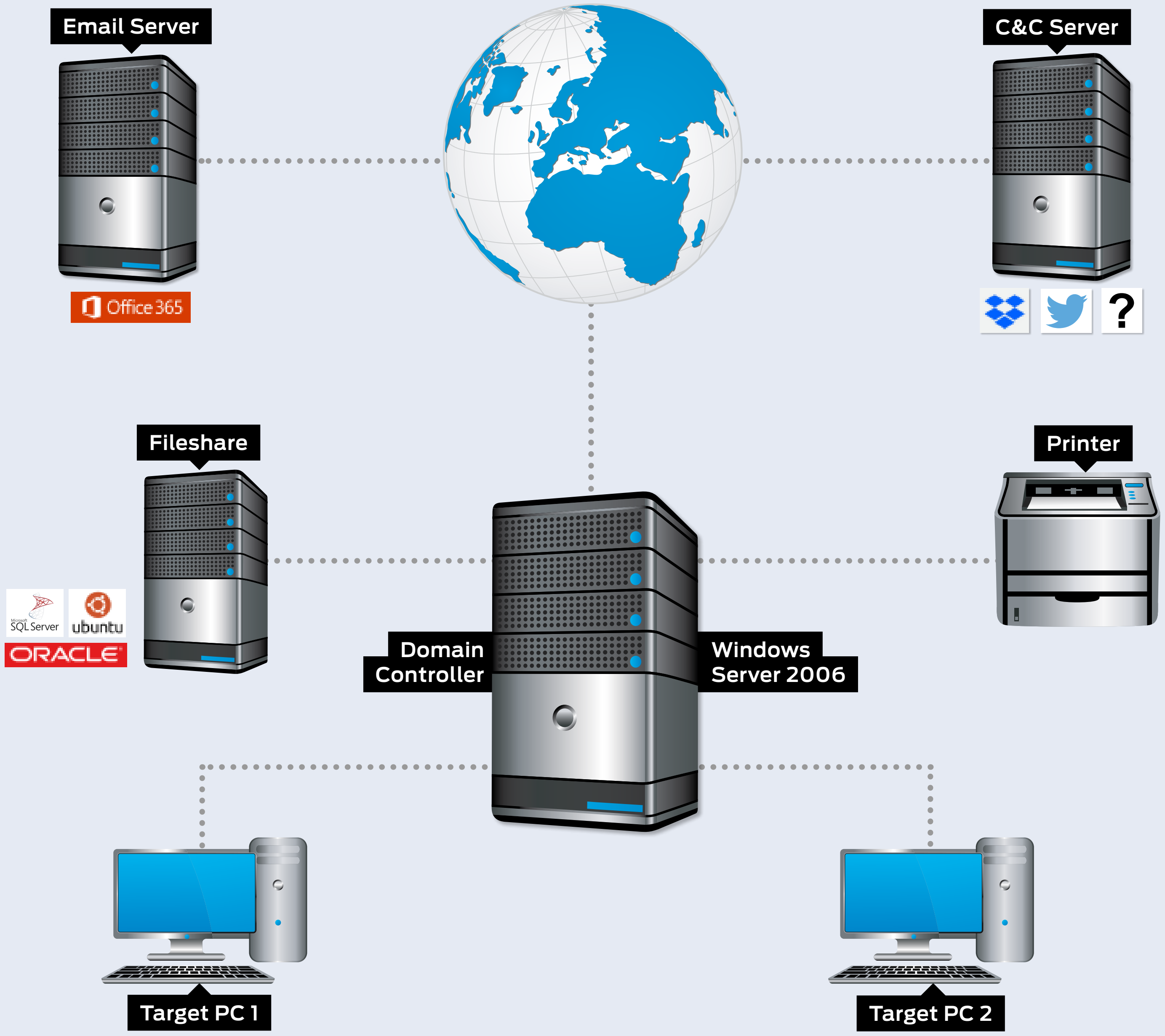
In the diagram on the right you will see an example network that contains workstations, some basic infrastructure such as file servers and a domain controller, as well as cloud-based email and a malicious command and control (C&C) server, which may be a conventional computer or a service such as Dropbox,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

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

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

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

Test Network Example



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

Threat Responses

Full Attack Chain: Testing Every Layer of Detection and Protection

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

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

Attack Stages

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

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

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

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

Attack Chain Stages

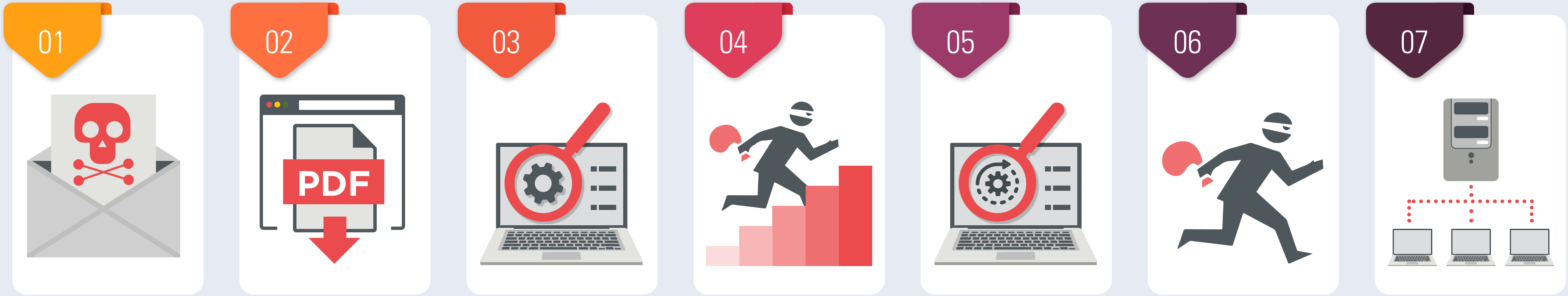


Figure 1. A typical attack starts with an initial contact and progresses through various stages, including reconnaissance, stealing data and causing damage.

In figure 2. a product or service has interfered with the attack, allowing it to succeed only as far as stage 3, after which it was detected and neutralised. The attacker was unable to progress through stages 4 and onwards.

It is possible for an attack to run in a different order with, for example, the attacker attempting to connect to other systems without needing to escalate privileges. However, it is common for password theft (see step 5) to occur before using stolen credentials to move further through the network.

It is also possible that attackers will not cause noticeable damage during an attack. It may be that their goal is persistent presence on the systems to monitor for activities, slowly steal information and other more subtle missions.

In figure 3. the attacker has managed to progress as far as stage five. This means that the system has been seriously compromised. The attacker has a high level of access and has stolen passwords. However, attempts to exfiltrate data from the target were blocked, as were attempts to damage the system.

Attack Chain: How Hackers Progress

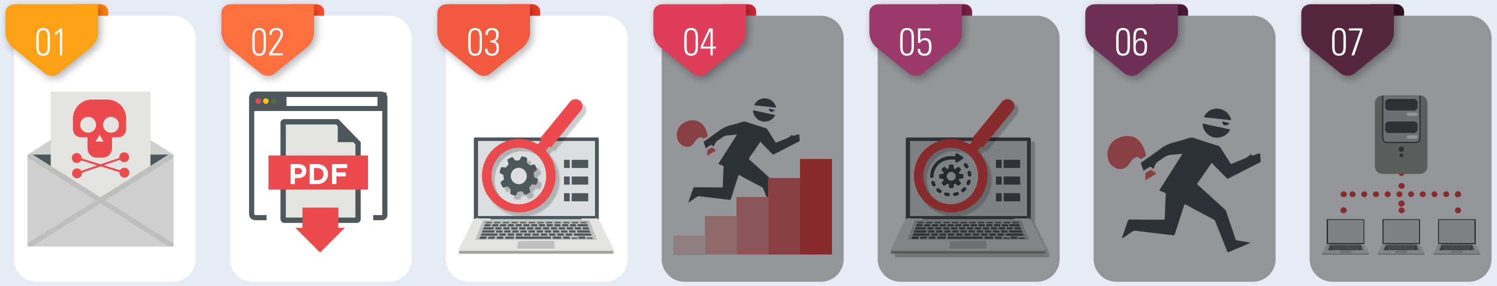


Figure 2. This attack was initially successful but only able to progress as far as the reconnaissance phase

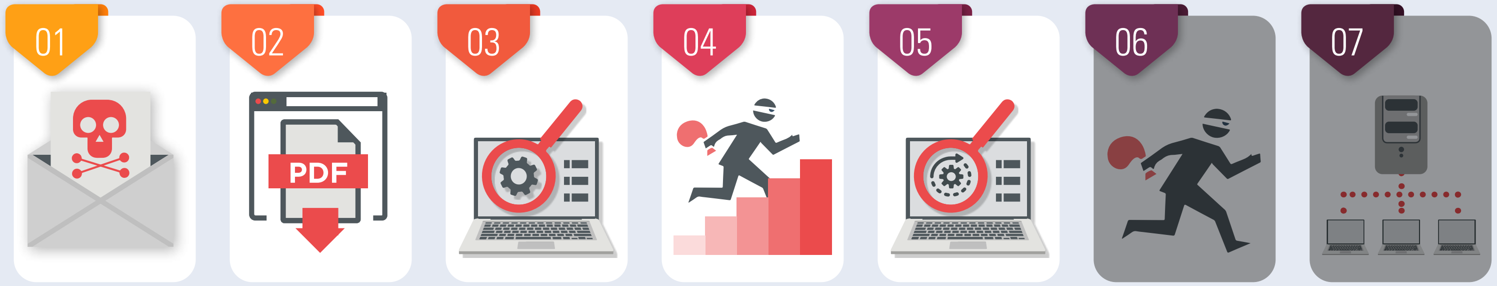


Figure 3. A more successful attack manages to steal passwords but wholesale data theft and destruction was blocked

SE Labs
INTELLIGENCE-LED TESTING
News from the security lab
FREE
Security opportunities for Managed Service Providers
Most popular reports of 2022
Your

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
Turla	🎣	🏛	Spear phishing campaigns and in-house espionage tools.

Key

✈ Aviation	🏦 Banking and ATMs	🏭 Energy	🎭 Entertainment
$ Financial	🃏 Gambling	🏛 Government Espionage	⊕ Healthcare
IT	⚖ Law	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.

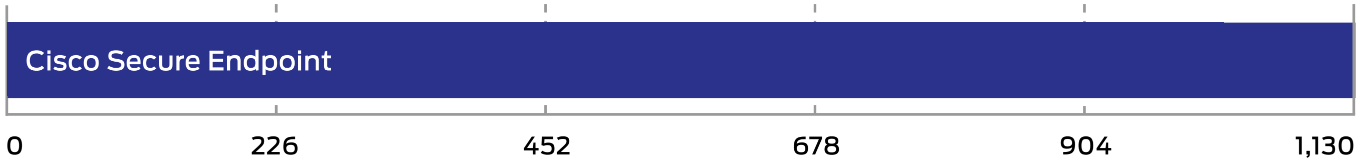
Not all protections, or detections for that matter, are equal. A product might completely block a URL, which stops the threat before it can even start its intended series of malicious events. Alternatively, the product might allow a web-based exploit to execute but prevent it from downloading any further 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
Cisco Secure Endpoint	1,130	100%	AAA



Total Accuracy Ratings combine protection and false positives.

3. Response Details

In this test security products are exposed to attacks, which comprise multiple stages. The perfect product will detect 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
Turla	12	12	0	0	0	0	0	0	0	12	0
Total	**12**	**12**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**12**	**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.

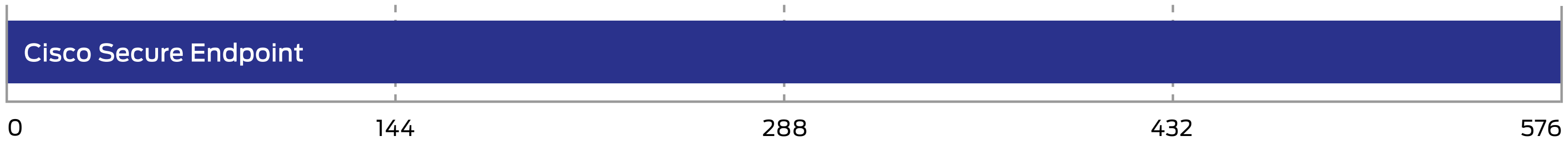
Protection Accuracy Rating Details

Attacker/ APT Group	Number of Test Cases	Protected	Penalties	Protection Score	Protection Rating
Turla	12	12	0	48	192
Grand Total	**12**	**12**	**0**	**48**	**192**

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 (%)
Cisco Secure Endpoint	576	100%



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

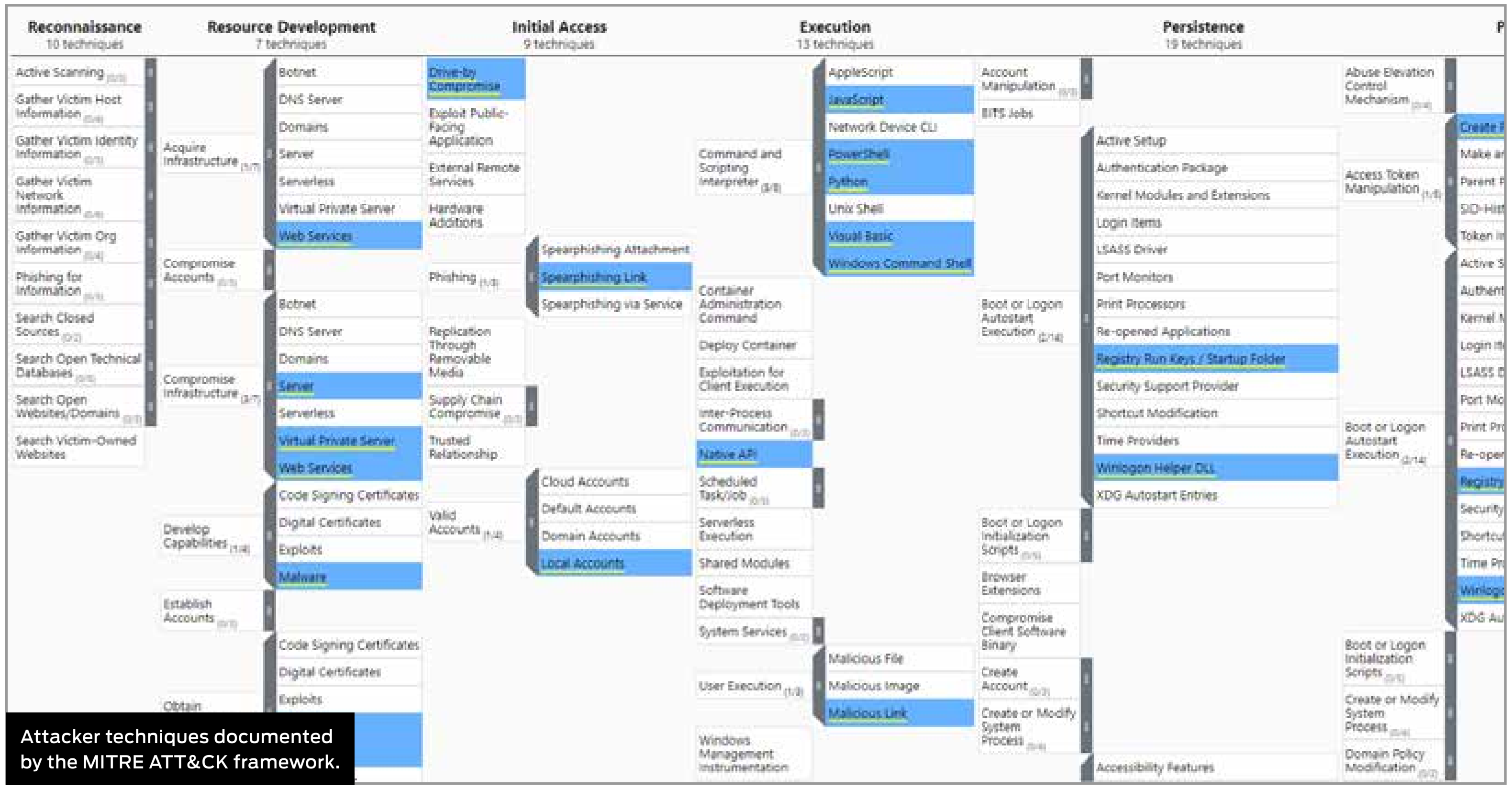
4. Threat Intelligence

Turla

This Russia-based threat group targets victims in different countries and across a wide range of industries. These include governmental organisations, notably including embassies and the military. Its main purpose is gathering intelligence.

Reference:
https://attack.mitre.org/groups/G0010/

Threat Visualisation:
https://selabs.uk/eas23cis
Use this JSON file to visualise the attack chain using a tool such as the **MITRE ATT&CK Navigator**. Download the file from the SE Labs site and upload to the tool.



Reconnaissance 10 techniques
- Active Scanning (0/3)
- Gather Victim Host Information (0/4)
- Gather Victim Identity Information (0/3)
- Gather Victim Network Information (0/6)
- Gather Victim Org Information (0/4)
- Phishing for Information (0/4)
- Search Closed Sources (0/2)
- Search Open Technical Databases (0/5)
- Search Open Websites/Domains (0/3)
- Search Victim-Owned Websites

Resource Development 7 techniques
- Acquire Infrastructure (1/7): Botnet, DNS Server, Domains, Server, Serverless, Virtual Private Server, Web Services
- Compromise Accounts (0/3)
- Compromise Infrastructure (3/7): Botnet, DNS Server, Domains, Server, Serverless, Virtual Private Server, Web Services
- Develop Capabilities (1/4): Code Signing Certificates, Digital Certificates, Exploits, Malware
- Establish Accounts (0/3)
- Obtain: Code Signing Certificates, Digital Certificates, Exploits

Initial Access 9 techniques
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (1/3): Spearphishing Attachment, Spearphishing Link, Spearphishing via Service
- Replication Through Removable Media
- Supply Chain Compromise (0/3)
- Trusted Relationship
- Valid Accounts (1/4): Cloud Accounts, Default Accounts, Domain Accounts, Local Accounts

Execution 13 techniques
- Command and Scripting Interpreter (5/8): AppleScript, JavaScript, Network Device CLI, PowerShell, Python, Unix Shell, Visual Basic, Windows Command Shell
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication (0/3)
- Native API
- Scheduled Task/Job (0/5)
- Serverless Execution
- Shared Modules
- Software Deployment Tools
- System Services (0/2)
- User Execution (1/3): Malicious File, Malicious Image, Malicious Link
- Windows Management Instrumentation

Persistence 19 techniques
- Account Manipulation (0/5)
- BITS Jobs
- Boot or Logon Autostart Execution (2/14): Active Setup, Authentication Package, Kernel Modules and Extensions, Login Items, LSASS Driver, Port Monitors, Print Processors, Re-opened Applications, Registry Run Keys / Startup Folder, Security Support Provider, Shortcut Modification, Time Providers, Winlogon Helper DLL, XDG Autostart Entries
- Boot or Logon Initialization Scripts (0/5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (0/3)
- Create or Modify System Process (0/4)
- Accessibility Features

- Abuse Elevation Control Mechanism (0/4)
- Access Token Manipulation (1/5)
- Boot or Logon Autostart Execution (2/14)
- Boot or Logon Initialization Scripts (0/5)
- Create or Modify System Process (0/4)
- Domain Policy Modification (0/2)

Attacker techniques documented by the MITRE ATT&CK framework.

Example Turla Attack

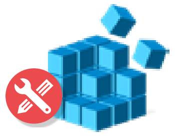
Delivery	Execution	Action	Privilege Escalation	Post-Escalation Action	Lateral Movement	Lateral Action
Spearphishing Attachment	Windows Command Shell	System Information Discovery	Bypass UAC	Registry Run Keys / Startup Folder	SSH	Archive via Utility
	Malicious File	File and Directory Discovery		Modify Registry	SSH Hijacking	Exfiltration over C2 Channel
	Masquerade Task or Service	Process Discovery		Disable or Modify Tools		Deobfuscate/Decode Files or Information
	Match Legitimate Name or Location	Query Registry				
	PowerShell	Remote System Discovery		Powershell Profile		
	Service Execution					
	Steganography					

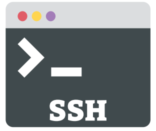
Spearphishing Attachment

Malicious File

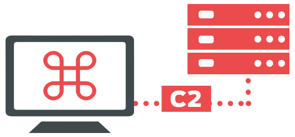
System Information Discovery

Bypass UAC


Modify Registry



SSH



Exfiltration over C2 Channel

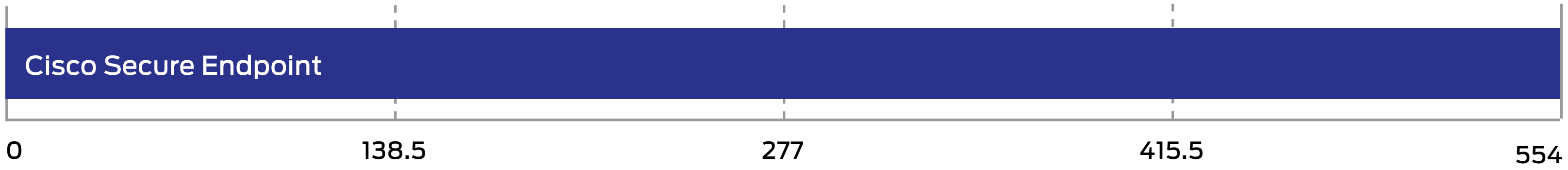
5. Legitimate Software Rating

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 (%)
Cisco Secure Endpoint	554	100%



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

6. Conclusions

The test exposed **Cisco Secure Endpoint** to a diverse set of exploits, file attacks and malware, comprising the Turla threat. Turla was launched by a Russian-based threat group in 2004 that has conducted espionage primarily against governments but has also attacked big businesses. Surging in 2015, Turla attacks are still a real and present threat to business networks worldwide, with reports that it has infected organisations in over 45 countries.

The attacks used in this test are similar or identical to those used by the Turla threat group described in **Hackers vs. Targets** on page 9 and **Threat Intelligence** on page 13

It is important to note that while the test used the same attack type, 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.

Two versions of **Cisco Secure Endpoint** were used in this test, Windows Version 8.1.7.21417 and Linux Version 1.22.0.950. While Turla's espionage platform has been deployed primarily against Windows systems, it has also been used against systems running Linux and macOS.

Both versions performed well against the Turla attacks. **Cisco Secure Endpoint** detected all the threats and provided an effective response against them. In four out of the four cases, it detected and stopped the threat at the very initial stages of the attack, scoring a 100% Protection Accuracy Rating.

The product achieved its 100% Protection Accuracy Rating by blocking the early stage of the attack. By recognising and rejecting the spear phishing emails that initiate the full attack chain, it did not have to address the later stages of the threat. No malicious files ran, system information was not compromised, user accounts were not bypassed and registries were not modified. Turla was also prevented from spreading to other systems and devices in the network.

Cisco Secure Endpoint also scored a 100% Legitimacy Accuracy Rating, meaning that it correctly identified harmless and legitimate software and allowed them to run without engaging administrators or end-users in sub-optimum interactions. This is noteworthy in the context of the Turla attack type which exploits in-house tools and software. **Cisco Secure Endpoint** was quick to disallow web-based exploits and malware because it recognised them as such. By also correctly identifying what would have been false positives, the product achieved a 100% Total Accuracy Rating.

Cisco Secure Endpoint wins a AAA award for its great performance against Turla-style advanced persistent threats.

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 18th and 24th August 2023.
- 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.

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: Product Versions

The table below shows the service's name as it was being marketed at the time of the test.

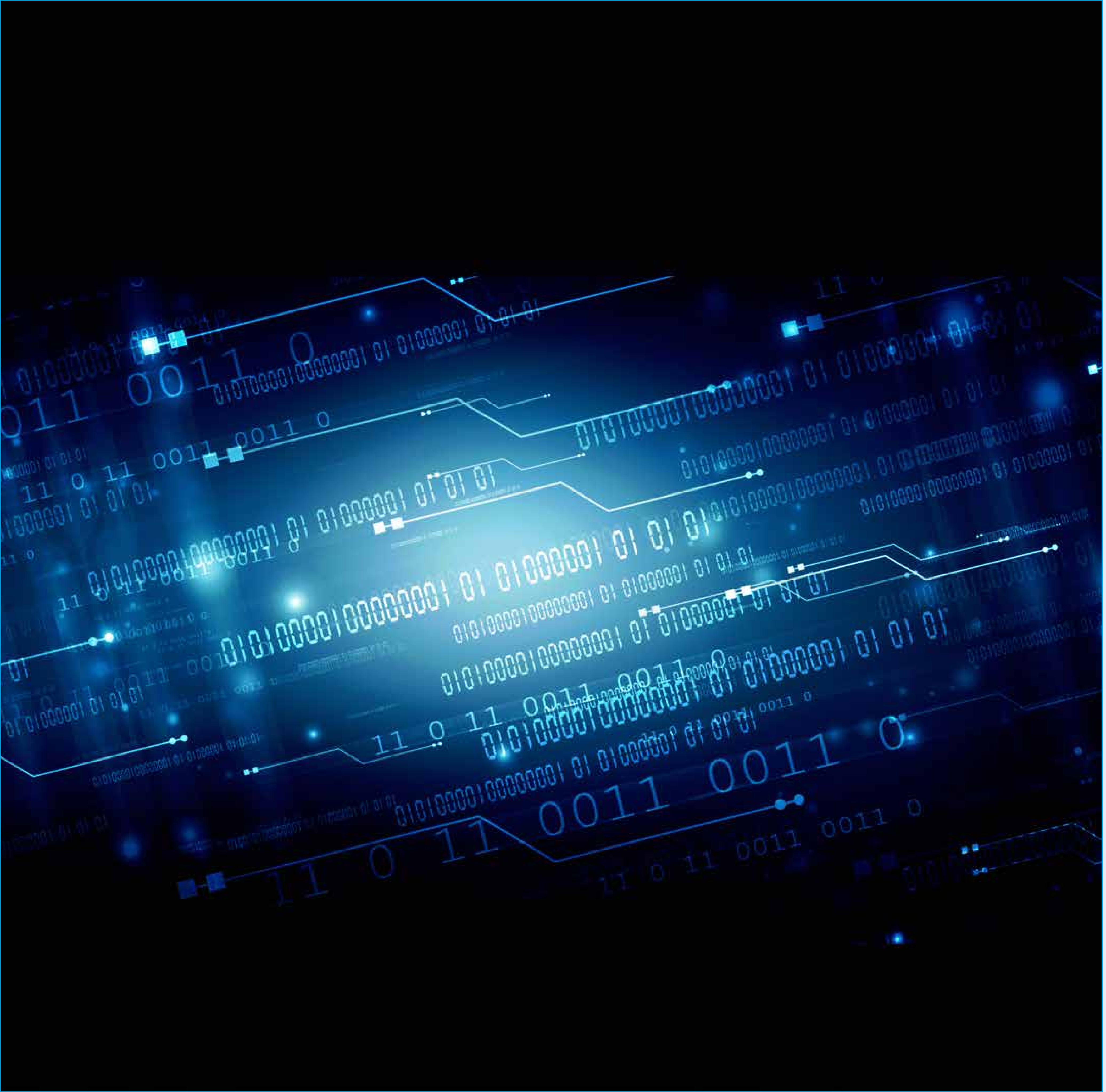
Product Versions

Vendor	Product	Build Version (start)	Build Version (end)
Cisco	Secure Endpoint (Windows)	8.1.7.21417	8.1.7.21417
Cisco	Secure Endpoint (Linux)	1.22.0.950	1.22.0.950

Appendix D: Attack Details

Turla

Delivery	Execution	Action	Post-Esclation Action	Post-Escalation Action	Lateral Movement	Lateral Action
Spear Phishing Attachment	Asymmetric Cryptography	Domain Groups	Bypass User Account Control	Code Signing Policy Modification	Lateral Tool Transfer	Archive via Utility
Spear Phishing Link	Bidirectional Communication	File and Directory Discovery	Create Process with Token	Disable or Modify Tools	SMB/Windows Admin Shares	Automated Collection
	Indicator Removal from Tools	Internet Connection Discovery	Token Impersonation/Theft	Disable Windows Event Logging	SSH	Automated Exfiltration
	JavaScript	Local Account		Domain Account	SSH Hijacking	Data from Local System
	Mail Protocols	Local Groups		Dynamic-link Library Injection		Data Transfer Size Limits
	Malicious File	Process Discovery		Email Hiding Rules		Deobfuscate/Decode Files or Information
	Malicious Link	Query Registry		Modify Registry		Exfiltration Over Alternative Protocol
	Masquerade Task or Service	Remote System Discovery		PowerShell Profile		Exfiltration Over C2 Channel
	Match Legitimate Name or Location	System Information Discovery		Registry Run Keys / Startup Folder		Ingress Tool Transfer
	PowerShell	System Network Configuration Discovery		Security Software Discovery		Local Data Staging
	Python	System Network Connections Discovery		Windows Credential Manager		Scheduled Transfer
	Service Execution	System Owner/User Discovery		Windows File and Directory Permissions Modification		
	Steganography	System Service Discovery		Windows Management Instrumentation Event Subscription		
	Visual Basic	System Time Discovery		Winlogon Helper DLL		
	Web Protocols					
	Windows Command Shell					
	Windows Service					



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.