SE Labs

INTELLIGENCE-LED TESTING

ANNUAL REPORT 2019

www.SELabs.uk info@SELabs.uk @SELabsUK www.facebook.com/selabsuk blog.selabs.uk

Contents

Document version 1.0 Written 16th August 2019

About SE Labs

Welcome to our first annual report! **SE Labs** was launched in 2016, immediately working with some of the best-known security companies in the world, as well as emerging 'next-generation' start-ups, all of which were attracted to our detailed and ethical approach to testing security products and services.

Initially focussing on endpoint security products, we also created new tests for services including email security and web security, as well as for firewalls and other security-focussed hardware appliances. Our 'hacking'-based testing, known as the Breach Response Test, has led the way in which endpoint and other products are tested in the face of effective and targeted attackers.

Our first blog post was published with the launch of our first public reports on endpoint security. The second article was about building a security lab, in terms of erecting walls, creating a server room and the challenges involved in starting up a business from scratch. The blog is the best place to find out what we're up to at any given time.

SE Labs is now located in the prestigious Wimbledon area of London.

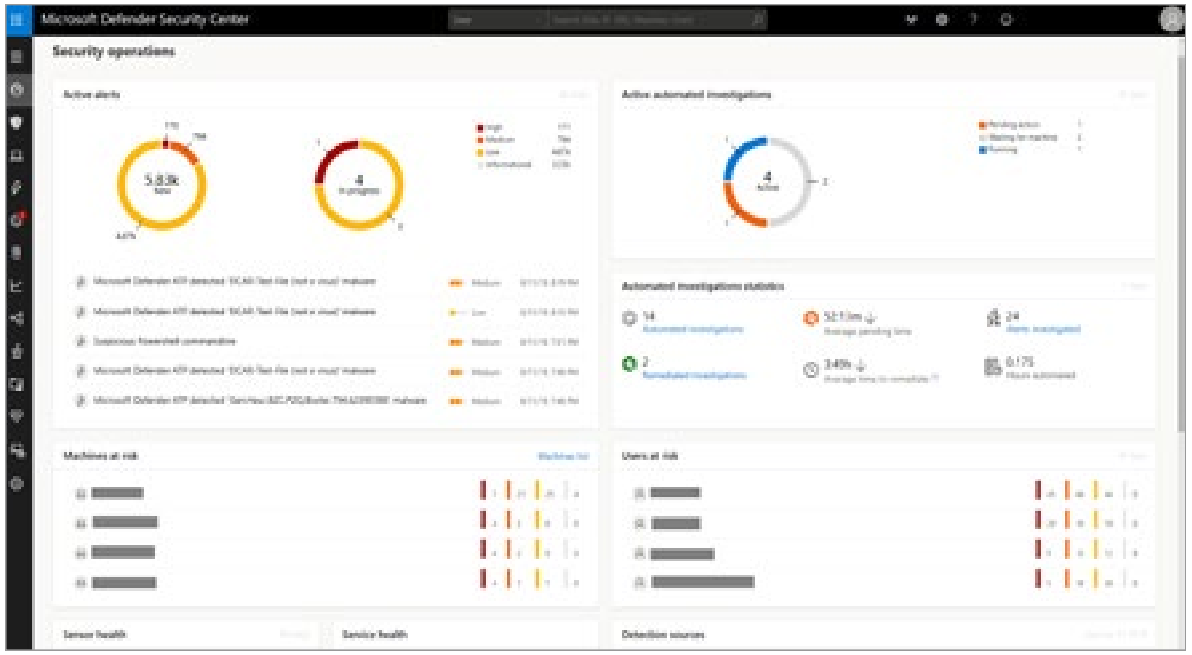
SE Labs uses state of the art equipment and facilities to run our world-leading security testing.

Over the last three and a half years the company has doubled in size and moved to larger, better-equipped offices in South West London. The new space accommodates a bespoke server room designed for the unique challenges involved in testing security products and services realistically, effectively and practically.

In September 2018 SE Labs was nominated by leading UK news outlet The Telegraph in its Trade Awards for Best Ethical Brand. We were also nominated for Best British International Brand; Best International Export; and Fastest Growing British Exports.

Seven months later business growth experts Tech Nation selected SE Labs as one of the 20 most promising cyber security companies in the UK.

While we continue to innovate in the computer security testing space, we have a keen sense of social responsibility and run a programme to introduce cyber security to young people at their schools and careers events like cyber Re:coded.



Our tests have expanded beyond endpoint testing and now includes threat response technologies on endpoints and in the cloud.

Social responsibility is core to our culture. We want to help improve IT security through testing and teaching the next generation of testers.

The Team

Management

Simon Edwards
Chief Executive Officer

Marc Briggs
Chief Operations Officer

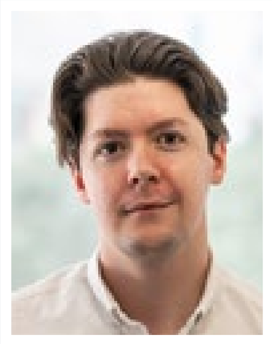
Magdalena Jurenko
Chief Human Resources Officer

Stefan Dumitrascu
Chief Technical Officer

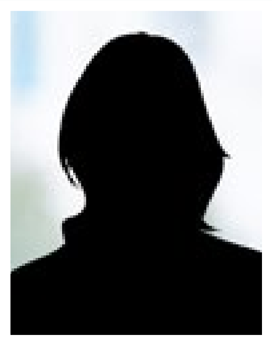
Testing Team

Thomas Bean
Tester

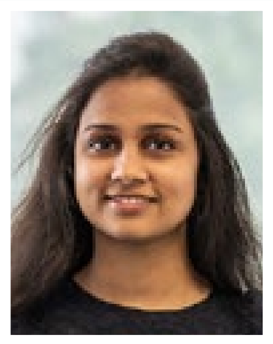
Dimitar Dobrev
Tester



Liam Fisher
Tester



Gia Gorbold
Tester



Pooja Jain
Tester

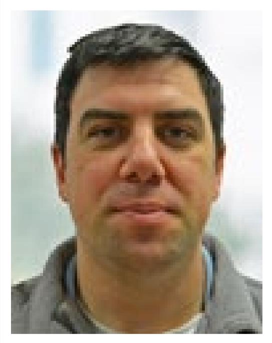
Jon Thompson
Email Testing Lead

Dave Togneri
Network Appliance
Testing Lead

Jake Warren
Tester

Stephen Withey
Development Ops

IT Support

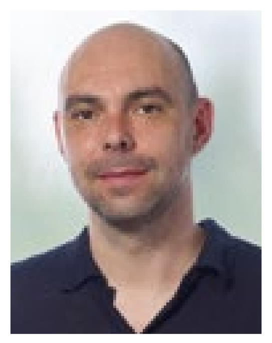


Danny King-Smith
IT Support Manager

Chris Short
IT Support Manager

Publication

Steve Haines
Production Manager



Colin Mackleworth
Design and Production

SE Labs

Website www.SELabs.uk
Twitter @SELabsUK
Email info@SELabs.uk
Facebook www.facebook.com/selabsuk
Blog blog.selabs.uk
Phone 0203 875 5000
Post SE Labs Ltd,
55A High Street, Wimbledon,
SW19 5BA, UK

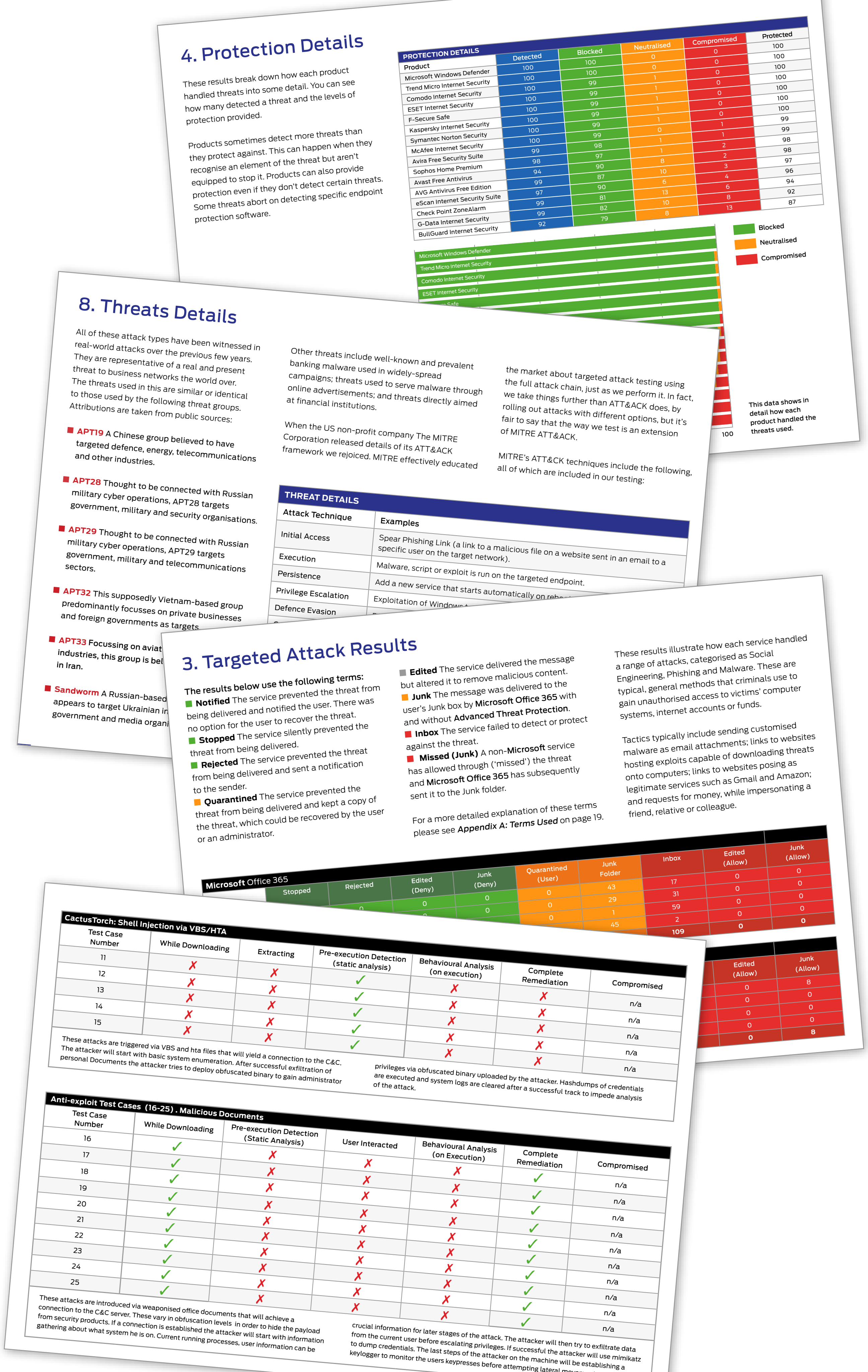
SE Labs is BS EN ISO 9001 : 2015 certified for The Provision of IT Security Product Testing.

SE Labs is a member of the Microsoft Virus Information Alliance (VIA); the Anti-Malware Testing Standards Organization (AMTSO); and the Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG).

Our Tests

Many of **SE Labs**' test reports are available for free from our website. We test a wide range of software, hardware and cloud-based services. The following list provides a few examples of our areas of expertise. In most cases we use both attacks found in the wild along with targeted attacks created in the lab. These targeted attacks can represent similar attacks that have occurred against real victims or may be more theoretical (but likely future) attacks.

- Endpoint Security Software
- Network Security Appliances
- Email Security Services
- Web Security Gateway Services
- Content Disarm and Reconstruction
- Endpoint Detection and Response/Incident Response
- Artificial Intelligence/ Machine Learning



Testing Standards

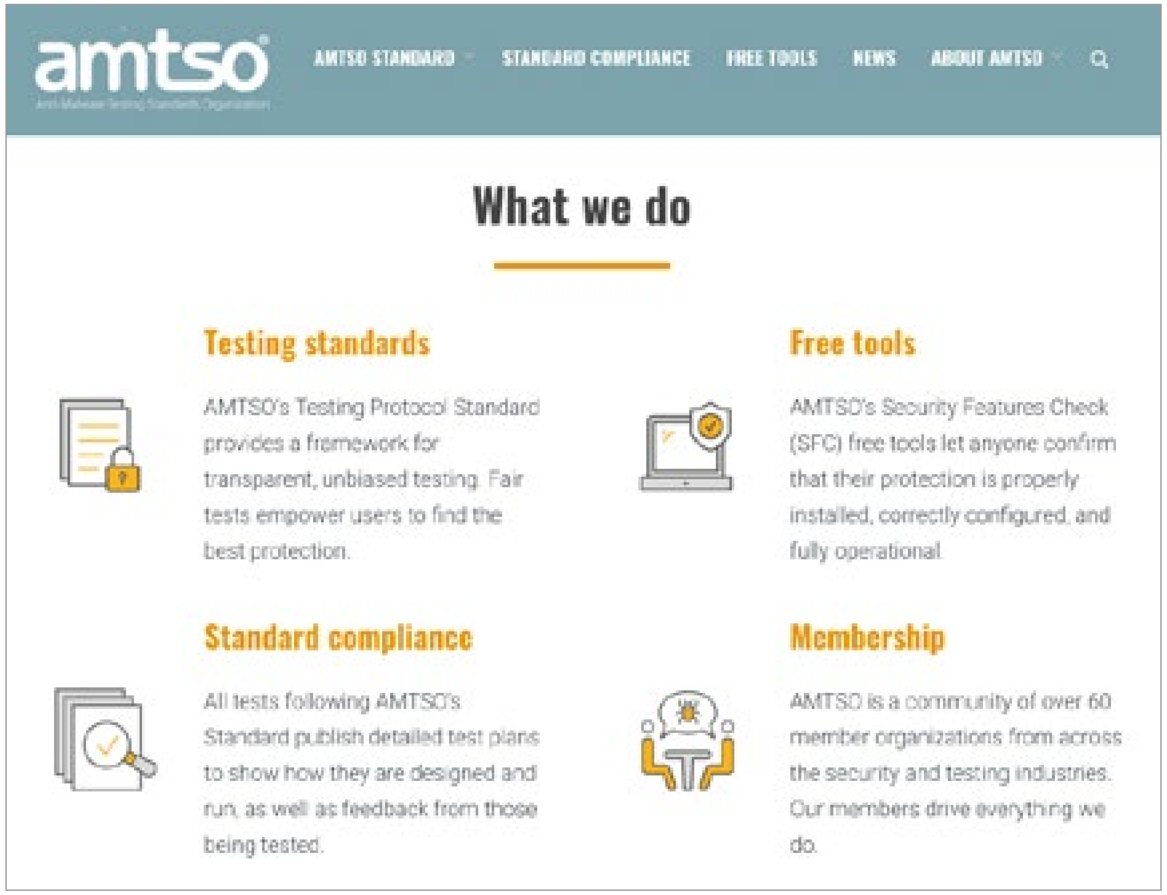
Security testing organisations make judgments on products and services, but how do you know if the tester is competent?

Testing computer security products and services comes with its own unique challenges and it is hard to assess the assessments. The industry is not known for its transparency in product effectiveness, and that extends to some testing. **SE Labs** has always prided itself on its ethical behaviour in terms of testing and business practices. That behaviour extends to maximum amounts of transparency. Unfortunately, until recently, there was no official way in which to demonstrate that we do what we say and are prepared to prove it to both validate test results and to help improve products.

In mid-2018 the Anti-Malware Standards Organization approved and adopted the AMTSO Testing Protocol Standard. A test that complies to this Standard has demonstrated that the testing has been conducted fairly and transparently. **SE Labs** was the first testing lab to engage with the Standard, running a private and then public pilot, before complying with the official Standard as soon as it was available.

To date all of **SE Labs**' public endpoint testing has complied with the AMTSO Standard, since its inception in 2018. We are committed to following the Standard so that readers of our reports can be assured that we've tested the way we said we did and that the results were checked by third parties.

Additionally, in 2017 **SE Labs** achived compliance with the ISO 9001:2015 Standard for Quality Management Systems, specifically relating to The Provision of IT Security Product Testing.



What we do

Testing standards

AMTSO's Testing Protocol Standard provides a framework for transparent, unbiased testing. Fair tests empower users to find the best protection.

Free tools

AMTSO's Security Features Check (SFC) free tools let anyone confirm that their protection is properly installed, correctly configured, and fully operational.

Standard compliance

All tests following AMTSO's Standard publish detailed test plans to show how they are designed and run, as well as feedback from those being tested.

Membership

AMTSO is a community of over 60 member organizations from across the security and testing industries. Our members drive everything we do.

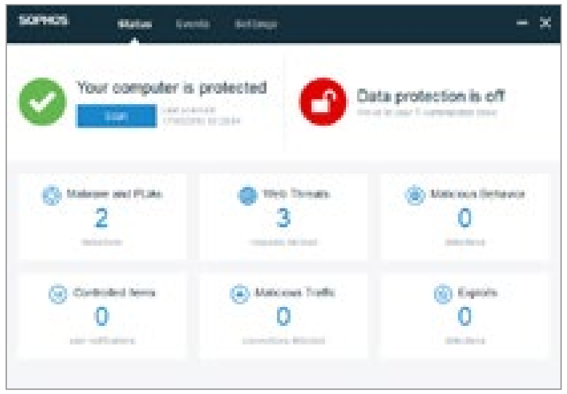
The Anti-Malware Testing Standards Organization supports transparency in testing, which encourages more accurate reports.

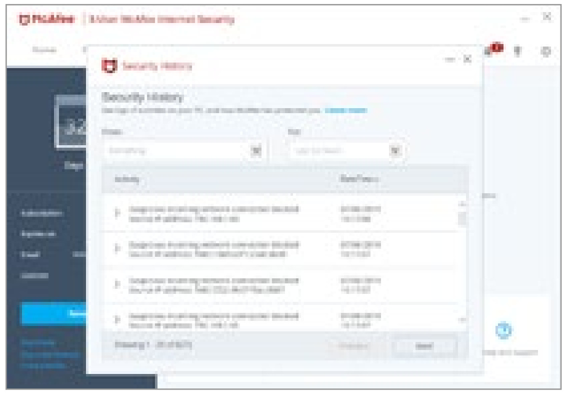
Targeted Attack Testing

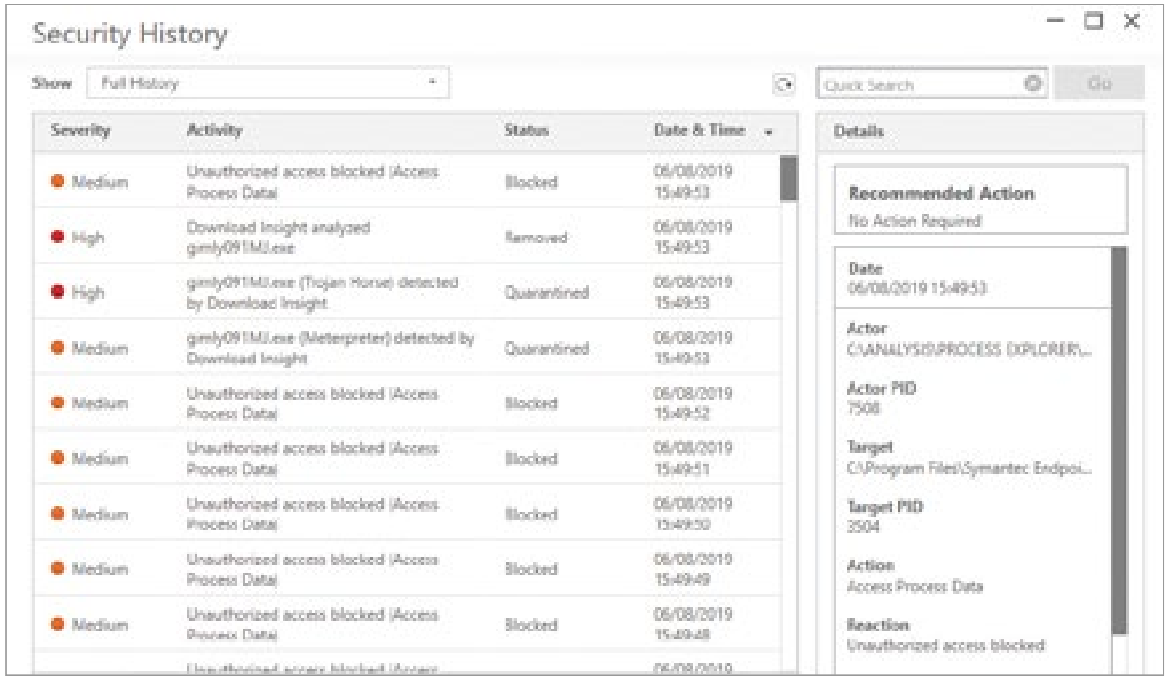
SE Labs has always specialised in target attack testing. While tests based around publicly available malware are valuable, they are limited in a number of ways, not least in that the tester usually doesn't have full control of the malware. This means that testing the full attack chain is virtually impossible.

For example, if the tester doesn't have control of a Trojan's controlling server then the test ends with an infection or a protection, but subsequent malicious behaviour that would happen in real life cannot be replicated for each tested product. This makes testing even one product hard and making comparisons impossible.

We have enjoyed great success in testing using publicly available tools and techniques. While some of tools are readily detected by anti-malware and other breach response products, it is often possible to evade detection using various common techniques. This allows our testers not only to help improve detection rates by consulting with security vendors, but also to run full attacks that further test products' abilities to detect and prevent specific malicious behaviour that occurs after an infection by malware.







Security History

Show Full History

Quick Search Go

Severity	Activity	Status	Date & Time
● Medium	Unauthorized access blocked (Access Process Data)	Blocked	06/08/2019 15:49:53
● High	Download Insight analyzed gimly091MJ.exe	Removed	06/08/2019 15:49:53
● High	gimly091MJ.exe (Trojan Horse) detected by Download Insight	Quarantined	06/08/2019 15:49:53
● Medium	gimly091MJ.exe (Meterpreter) detected by Download Insight	Quarantined	06/08/2019 15:49:53
● Medium	Unauthorized access blocked (Access Process Data)	Blocked	06/08/2019 15:49:52
● Medium	Unauthorized access blocked (Access Process Data)	Blocked	06/08/2019 15:49:51
● Medium	Unauthorized access blocked (Access Process Data)	Blocked	06/08/2019 15:49:50
● Medium	Unauthorized access blocked (Access Process Data)	Blocked	06/08/2019 15:49:49
● Medium	Unauthorized access blocked (Access Process Data)	Blocked	06/08/2019 15:49:48
	Unauthorized access blocked (Access		06/08/2019

Details

Recommended Action
No Action Required

Date
06/08/2019 15:49:53

Actor
C:\ANALYSIS\PROCESS EXPLORER\...

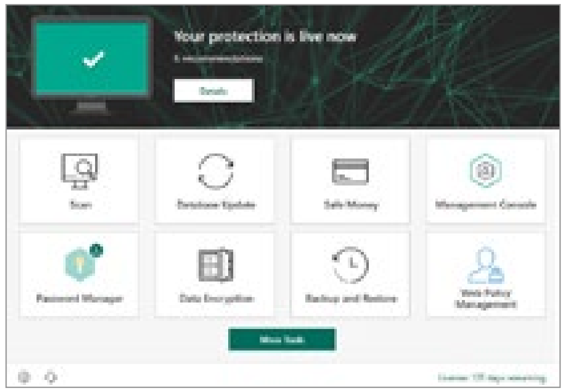
Actor PID
7508

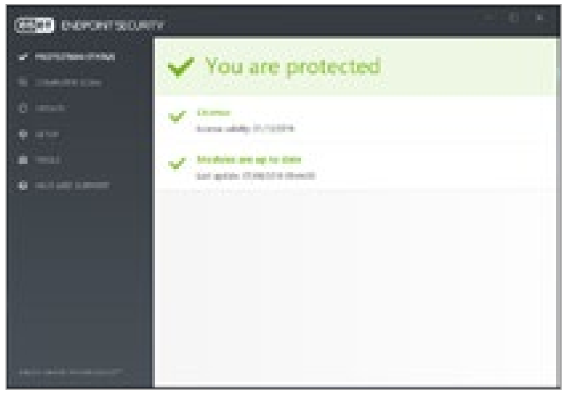
Target
C:\Program Files\Symantec Endpoi...

Target PID
3504

Action
Access Process Data

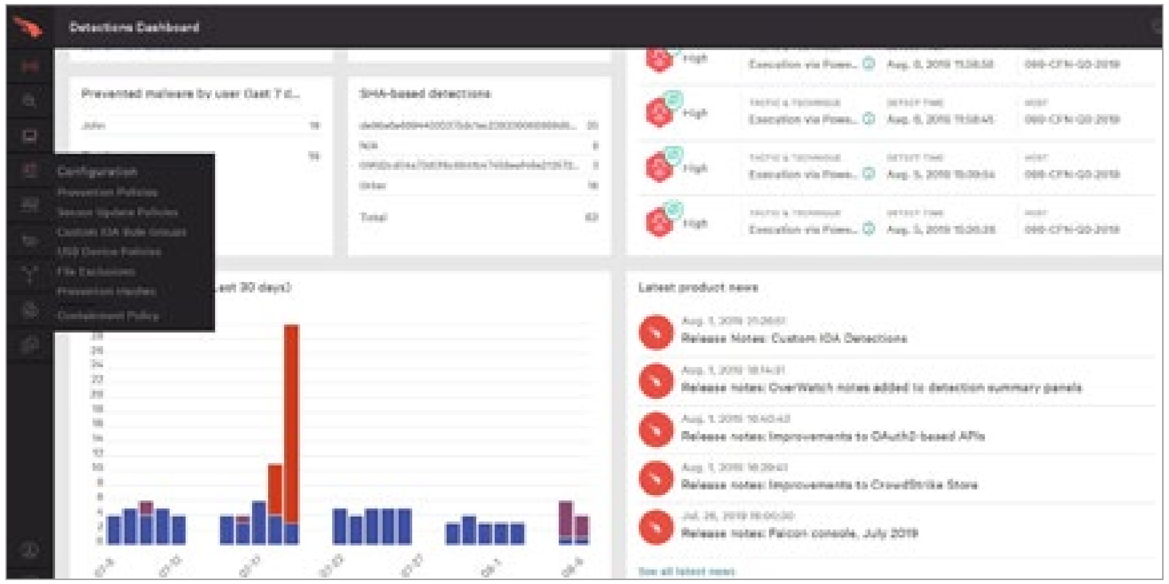
Reaction
Unauthorized access blocked

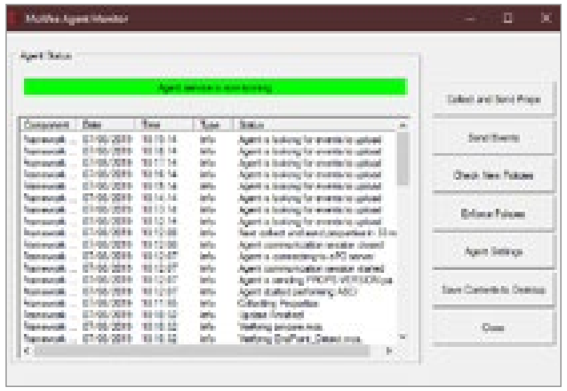




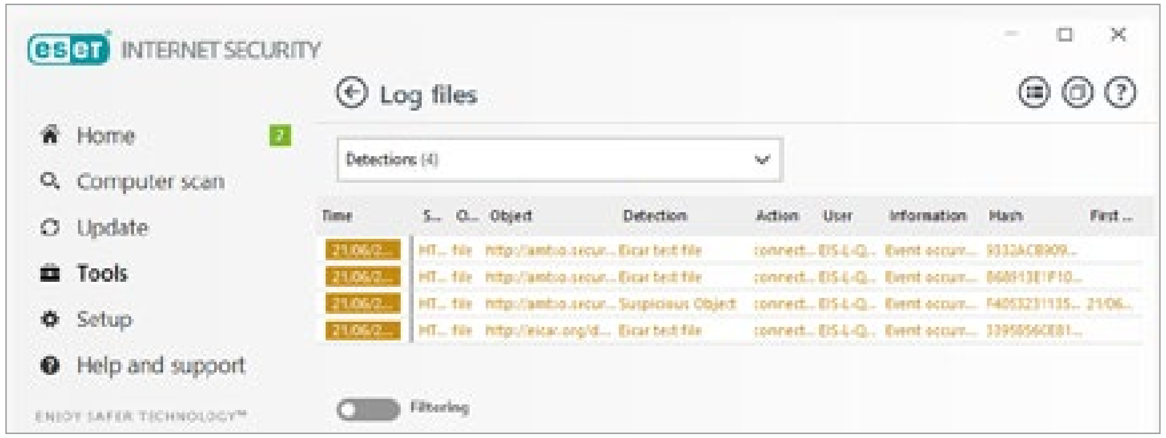
We don't rely solely on 'standard' malware, though, and often use so-called 'file-less' attacks, Macros and memory injection attacks. These are all used by real-world attackers so we believe a good test should include them also.

When the US non-profit company The MITRE Corporation released details of its ATT&ACK framework we rejoiced. We're good at hacking and testing, but marketing is not our strong point and MITRE effectively educated the market about targeted attack testing using the full attack chain, just as we perform it. In fact, we take things further than ATT&ACK does, by rolling out attacks with different options, but it's fair to say that the way we test is an extension of MITRE ATT&ACK.


Detections Dashboard
Prevented malware by user (last 7 d...
SHA-based detections
Configuration
Prevention Policies
Sensor Update Policies
Custom IOA Rule Groups
USB Device Policies
File Exclusions
Prevention Hashes
Containment Policy
High
Execution via Powe...
Latest product news
Release Notes: Custom IOA Detections
Release notes: OverWatch notes added to detection summary panels
Release notes: Improvements to OAuth2-based APIs
Release notes: Improvements to CrowdStrike Store
Release notes: Falcon console, July 2019
See all latest news



Windows Security
Virus & threat protection
Protection for your device against threats.
Current threats
Threats found. Start the recommended actions.
TrojanDropper:JS/Prolly.A
Severe
Start actions
Scan options
Threat history
Virus & threat protection settings
No action needed.
Manage settings
Windows Community videos
Learn more about Virus & threat protection
Do you have a question?
Get help
Who's protecting me?
Manage providers
Help improve Windows Security
Give us feedback
Change your privacy settings
View and change privacy settings for your Windows 10 device.
Privacy settings
Privacy dashboard

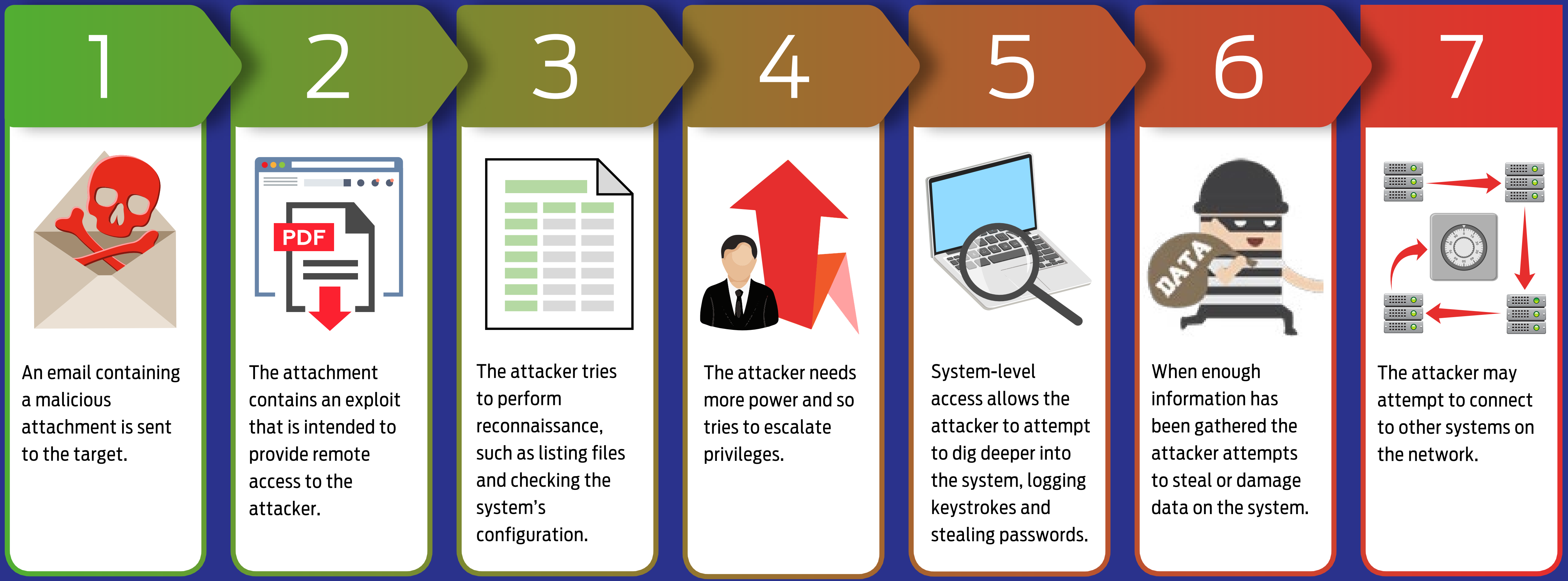


Time	S...	O...	Object	Detection	Action	User	Information	Hash	First ...
21/06/2...	HT...	file	http://amtso.secur...	Eicar test file	connect...	EIS-L-Q...	Event occurr...	5332ACB909...	
21/06/2...	HT...	file	http://amtso.secur...	Eicar test file	connect...	EIS-L-Q...	Event occurr...	B60513E1F10...	
21/06/2...	HT...	file	http://amtso.secur...	Suspicious Object	connect...	EIS-L-Q...	Event occurr...	F4053231135...	21/06...
21/06/2...	HT...	file	http://eicar.org/d...	Eicar test file	connect...	EIS-L-Q...	Event occurr...	3395056CE81...	

Full Attack Chain Testing Every Layer of 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.



1. An email containing a malicious attachment is sent to the target.
2. The attachment contains an exploit that is intended to provide remote access to the attacker.
3. The attacker tries to perform reconnaissance, such as listing files and checking the system's configuration.
4. The attacker needs more power and so tries to escalate privileges.
5. System-level access allows the attacker to attempt to dig deeper into the system, logging keystrokes and stealing passwords.
6. When enough information has been gathered the attacker attempts to steal or damage data on the system.
7. The attacker may attempt to connect to other systems on the network.

Targeted Attacks in Practice

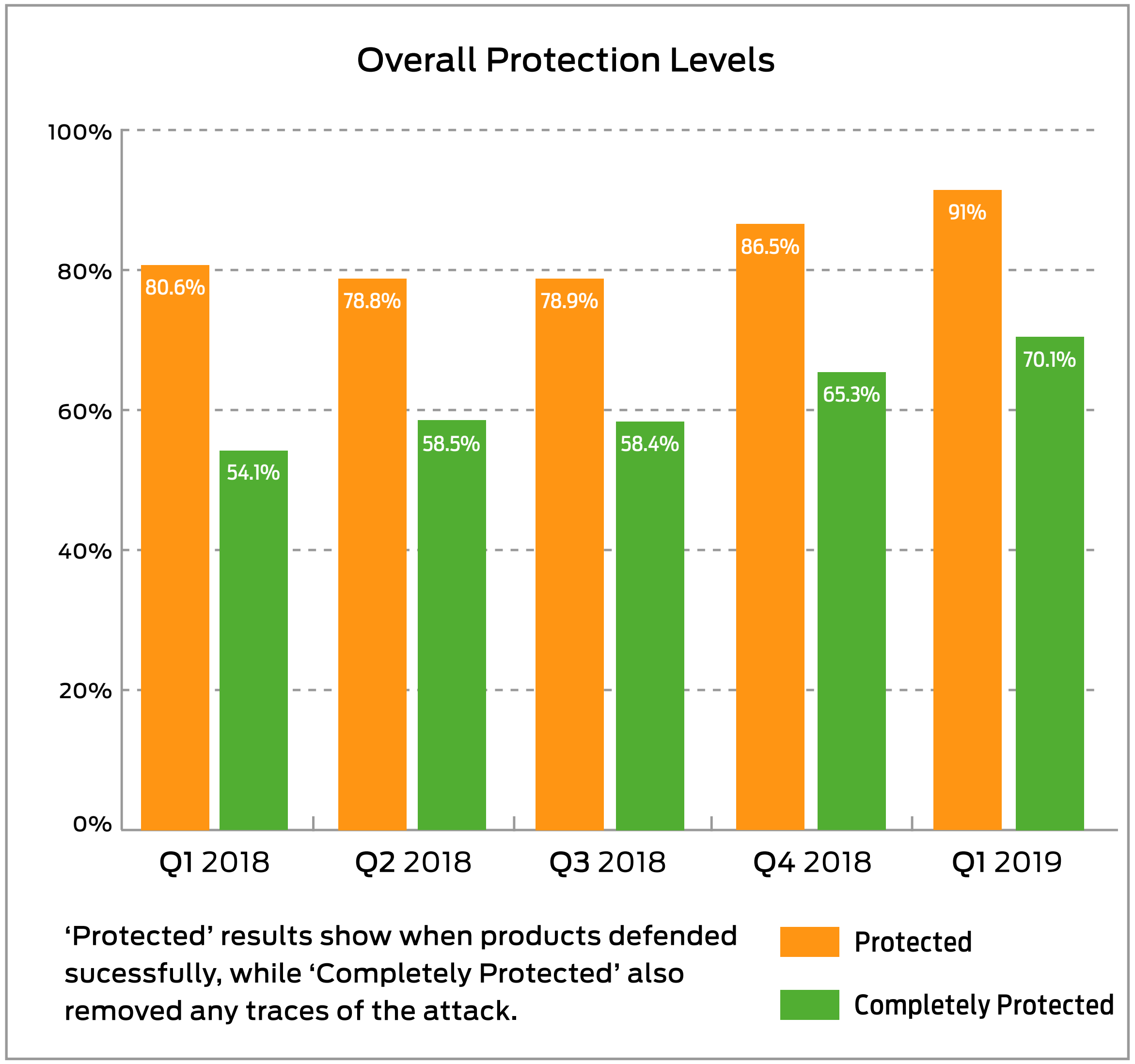
Over the last few years we have tested more than 50 different products using over 5,000 targeted attacks. These attacks were run in a realistic way using publicly available hacking tools. The results were surprising. As attackers, our success levels were far greater than we'd predicted. Using freely available tools that are widely distributed on the internet we were able to compromise large numbers of systems, often without detection.

The good news is that, as we work closely with the security vendors, their products have improved over time. However, it is interesting to see which hacking approaches were most effective. We used a combination of techniques including process and memory injection; anti-malware evasion; and file-less attacks including Microsoft PowerShell.

The results show that many endpoint products detect most of the attacks. However, while anti-malware evasion tools were mostly detected and prevented, injection techniques resulted in higher levels of compromise, while using PowerShell is currently an excellent way to break into systems, with far higher levels of compromise compared to the other methods. Products were generally poor at cleaning up after a detected attack.

We have also tested email security services with many of these attacks and our public reports show that email remains an effective route for attackers. Combined with a good endpoint product things don't look too hopeless, but you wouldn't want to rely solely on an email gateway right now.

If you are interested in diving more deeply into the details of our targeted attack research, please see our blog post at https://tinyurl.com/selar2019.



Annual Awards Winners

After months of in-depth testing we are proud to announce this year's Annual Awards winners. Each of the following companies or products has demonstrated to **SE Labs** its excellence in its category. We've based our conclusions on a combination of continual public testing, private assessments and feedback from corporate clients who use **SE Labs** to help choose security products and services.

SE Labs
INTELLIGENCE-LED TESTING
BEST
New Endpoint
WINNER 2019

Crowdstrike
Falcon

CROWDSTRIKE

SE Labs
INTELLIGENCE-LED TESTING
BEST
Innovator
WINNER 2019

Cylance
CylancePROTECT

BlackBerry
CYLANCE

SE Labs
INTELLIGENCE-LED TESTING
BEST
Enterprise Endpoint
WINNER 2019

Symantec
Endpoint Security

Symantec.

SE Labs
INTELLIGENCE-LED TESTING
BEST
Small Business Endpoint
WINNER 2019

Sophos
Intercept X Advanced

SOPHOS

SE Labs
INTELLIGENCE-LED TESTING
BEST
Consumer Anti-Malware
WINNER 2019

Kaspersky
Internet Security

kaspersky

SE Labs
INTELLIGENCE-LED TESTING
BEST
Free Anti-Malware
WINNER 2019

Microsoft
Windows Defender

Microsoft

SE Labs
INTELLIGENCE-LED TESTING
BEST
Email Security Service
WINNER 2019

Symantec
Email Security .cloud with ATP

Symantec.

SE Labs
INTELLIGENCE-LED TESTING
BEST
Network Security Appliance
WINNER 2019

Fortinet
FortiGate

FORTINET

A Word from Simon

To ensure our testing is as realistic and useful as possible, we monitor real-world breaches from a technical point of view. This allows us to adapt and change our testing in a similar way to how real attackers operate.

How do we know what the bad guys do? We gain insight from publicly available information and also direct contact with large businesses that use us for consultancy with incident response. We've seen many real-world hacks from their server rooms and security dashboards. We've logged into their email administration accounts and seen forwarding rules created by attackers. We've examined very targeted, malicious emails constructed with weird alphabets and containing advanced malware.

Predictions

As we watch the development of attacks, we are often asked to predict the future. How will tomorrow's attackers behave? Security predictions are highly predictable – they usually happen towards the end of the year and vendors will claim that the following year's threats will evolve in line with their own product developments.

If they market their products using Artificial Intelligence then the next logical step is that criminals will counter with evil AI. Similarly, vendors of signature-based products will predict that the bad guys will use morphing malware that will attempt to evade detection. In both cases the implication is that the world is facing a nearly insurmountable threat but that the good news is Vendor X has the solution.

It's clear from our testing that no single vendor has a unified and perfect answer to 'security'. We predict that this situation will continue indefinitely. Vendors that push their 'AI-based' solutions talk a good game but how many of their products have you seen in independent security tests? Precious few. You have to ask yourself why that might be…

At **SE Labs** we did prove that AI can work, though. In our Predictive Advantage test we've demonstrated how products can detect threats that were developed after the protection software was created, trained and deployed without the ability to update or check online resources.

Threat Intelligence

Threat intelligence, on which all of our testing is based, sounds exciting. It provides a view into the current criminal world of hacking. But we propose that development of attacks is not as fast and innovative as it could be, because it doesn't have to be.

When you look through our reports, reports from security vendors, leaked files from Wikileaks and books on hacking even from the start of the 21st century you'll see much the same thing. The hacking playbook is nearly identical, in fact. As software is patched so new exploits are discovered, but the general method in which hackers operate is quite established and predictable.

They try to gain access, perform some general reconnaissance, potentially steal some information and then move laterally through the network in search for further data or targets to damage. They may be some minor variations but that's essentially what you can expect to see in previous reports, today's news and for the foreseeable future.

Persistent Ransomware Attacks

That may sound disappointingly pedestrian so let's make an exciting prediction. We've seen a lot of ransomware over the last few years that encrypts an organisation's data quickly and then demands immediate payment for its decryption. One obvious and successful solution is to wipe the disks and restore from backups. We predict that the next evolution of ransomware will be a Persistent Ransomware Attack (PRA).

This new threat will sit quietly on systems slowly encrypting small numbers of files over a long period of time. These encrypted files will be absorbed into backups and will, after a period of months, replace many good files that had been backed up. As backup tapes are rotated back into service, or old backup sets abandoned, the backup will become corrupted. When the final demand for a ransom comes, the backups will no longer be a viable solution.

SE Labs
INTELLIGENCE-LED TESTING
PREDICTIVE MALWARE RESPONSE TEST
MARCH 2018

SE Labs
INTELLIGENCE-LED TESTING
Deep Instinct
THREAT PREVENTION EVALUATION:
Sophisticated, high-profile file-based and file-less targeted attacks
February 2019

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.