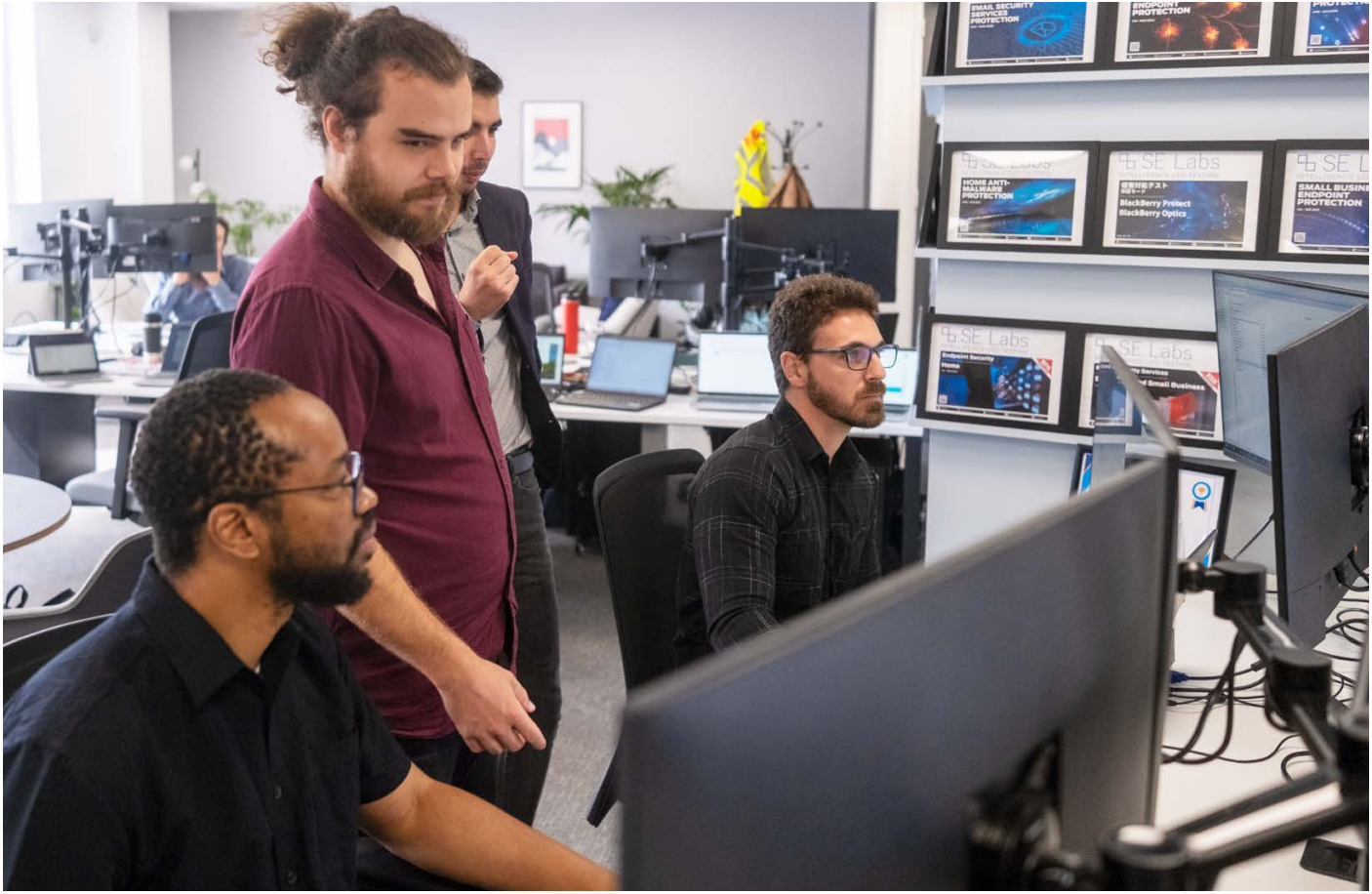
SE Labs

ANNUAL REPORT

Cyber Threat Intelligence 2023


EMAIL SECURITY SERVICES PROTECTION
ENDPOINT PROTECTION
HOME ANTI-MALWARE PROTECTION
BlackBerry Protect
BlackBerry Optics
SE Labs

Contents

Document version 1.0 Written 27th February 2023

Foreword

Welcome to the fourth annual report from SE Labs. This edition focusses on threat intelligence. Understanding threats is crucial when trying to defend against them. Knowing your enemy's tactics helps clarify security planning.

We use threat intelligence when testing security products, to ensure our results are useful to companies facing real threats in the real world. We're sharing our insights here to help you build a strategy for success in the face of the global cyber threat.

Criminal Profits Vastly Outstrip Security Spending

For every $1 we spend on protection, cyber criminals make $40. But there is hope

There's good news and there's bad news. You want the bad news first, I expect. The bad news is that we're not winning the war against cyber criminals. Global organisations and even tiny one-person businesses are buying cyber security solutions and yet cybercrime is still raking in the equivalent of trillions of US dollars. Some estimate that criminal hackers will cost the legitimate world as much as $10tn a year, within the next few years.

This rather puts into perspective the otherwise impressive amounts businesses are supposedly spending on cyber security. Headlines report that the cyber security industry, the companies that produce products to save us, will be worth one quarter of a trillion US dollars in around four years.

Even if these numbers are overstated by a factor of 10, we're still looking at defensive spending of $25Bn and losses to crime of $1tn. That's a forty to one disparity.

If this is the arms race that some analysts talk about, then there's a clear leader. And it's not the good guys.

Cyber safety is not all about buying products, though. Careful, intelligent planning can go a long way to protecting organisations. Unfortunately, the bad news continues. As we see in **What are the threats?** on page 6, large percentages of companies in the western world simply aren't paying attention to the cybercrime threat. It's probably safe to assume the same or worse for less well-resourced countries.

> "If this is the arms race that some analysts talk about, then there's a clear leader. And it's not the good guys"

This situation is nearly unbelievable. We live in a world where not a month passes without a major organisation suffering public humiliation and probably vast losses at the hands of ransomware gangs. As I write this, the UK's postal service suffered a ransomware attack that prevented it from sending parcels overseas for at least a week. A major Norwegian shipping company lost communication with 1,000 container ships and Taco Bell shut down systems (and a load of restaurants) following a ransomware attack. These aren't isolated incidents. Just the very latest ones in a regular rollcall of similar events.

So the bad news, in short, is that despite some companies spending huge amounts on security, too few are paying proper attention. And in a way, that's the good news too. Because we can fix that. If you're not yet prepared, it shouldn't be too hard to improve and rise above the average. If 25-50% of organisations have a cyber security plan, there's plenty of scope for improvement. And planning doesn't have to be rocket science. Even a basic plan is better than nothing.

Hackers, for it is they who are responsible for 50% of breaches today, generally follow the same process of reconnaissance, initial access, establishing a persistent foothold and then movement through the target network with the ultimate goal of stealing or damaging data (or both).

This is not news. Or if it is, it's good news because it means that the hacker playbook has remained pretty stable over the last few decades. Readers of the original and popular Hacking Exposed books, which started to appear in 1999, will not be shocked to hear that the NSA followed exactly the same general processes for breaching systems. And it is how hackers work today. If we know what to expect, we can plan for it.

I'd like to say that the move to using ransomware as a payload is relatively new but encrypting malware has been with us since the late 1980s. In some respects, ransomware has existed for 30 years. But it hit the mainstream consciousness about 10 years ago and today it's just another piece of malware released onto compromised systems. A particularly impactful type of malware, but still just code you don't want to run on your network.

Companies that exercise good cyber hygiene are much more resilient to ransomware attacks than those who pay a bit for cyber security solutions and spend the next 364 days of the year thinking about something else.

Attackers might use basic techniques to hack into businesses, but they only do that because they don't need to be more advanced. They are not stupid and learn constantly. As we improve our planning and shore up our defences, they will exercise greater ingenuity. At a bare minimum targets should make them work for their money and try not to be in the 50% of clueless organisations that are easy to breach. There is so much room for improvement. At the moment it feels less like an arms race between equals and more like bewildered sheep wandering into an abattoir.

Section 01

What are the Threats?

A basic lack of understanding and planning means half of all businesses are easy targets for hackers. Their largely simplistic tactics reflect this low bar of care. But talented security teams still face an increasing threat from more advanced attack methods. We look at this year's threats and predict what's around the corner.

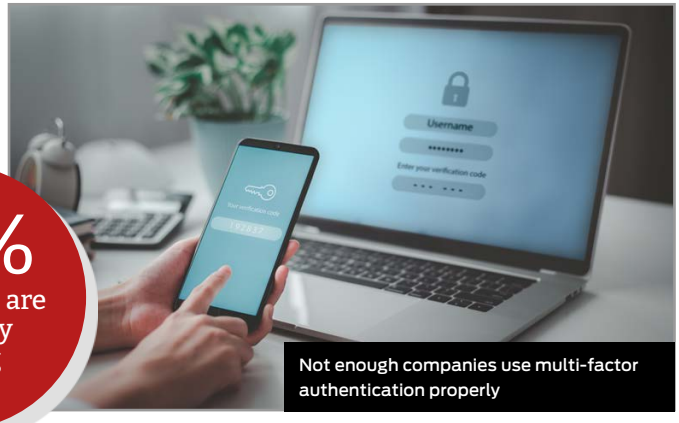
All Business are Targets. Is Yours an Easy One?

Attackers evolve, but they don't need to if businesses aren't paying attention.

This year's statistic is 50%. Is your business hackable? Flip a coin. There's a 50/50 chance that it is an easy target. Unfortunately, there's a 90% chance that someone can break in with more than a basic effort.

In the US only half of all businesses, large and small, take cybersecurity seriously. It's worse in the UK – only 25% are paying attention. The problem comes from the top: 50% of company boards don't understand cybersecurity. This is probably why half of all businesses don't have an IT security plan. So it should be no surprise, then, that 50% of breaches are caused by hacking, rather than tricking users or making silly configuration mistakes. If businesses aren't on the ball, attackers will win by doing what they've always done.

50%
of breaches are caused by hacking



Not enough companies use multi-factor authentication properly

Stolen 'Logins'

Can we be more specific? Hacking can mean exploiting vulnerable software, breaking into web servers and using remote desktop software to control systems. Some of that sounds highly technical but 50% of hacking involves using stolen credentials. The bad guys don't need to use secret hacks like exploits to break in. They just use valid usernames and passwords. These usernames and passwords are traded online, often for as little as $1.

The obvious solution is to add a layer of security called Multi-Factor Authentication (MFA), which can be free or certainly very inexpensive. If you have to enter a code generated by a free app, or sent to you by text message, that username and password combination isn't much use. Not enough companies have adopted this solution. One in five hacking victims don't use MFA.

Bypassing Multi-Factor Authentication

Even those that do use MFA are not immune from attack, though. This year hackers have been attempting to log in multiple times,

causing legitimate users to receive repetitive notifications on their devices, asking for access. Time this right (or just be lucky) and the user will click 'Allow' to get some peace. Multi Factor Annoyance works and is a growing threat.

31%
of organisations who paid the ransom still could not recover their data

Ransomware

Ransomware is on the rise, at rates never seen before. In the vast majority of cases the attackers target backups. Paying is expensive and could put you at risk of legal action. Besides which, nearly a third of organisations that paid were still unable to recover their data.

Over the last year every client we've spoken to has listed ransomware as their top concern. Unlike many cyberthreats, it's an easy concept for Boards to understand. Business stops until you pay. This is why we've devoted a large part of this report to ransomware and ways to protect against it.

Email as a Target

Email remains a primary attack vector. Phishing attacks over email power 20% of all successful breaches. Business Email Compromise (BEC) attacks, where attackers log into real accounts and send fraudulent emails, are common. In nearly half of cases they abuse stolen credentials.

The good news is that your employees are mostly trustworthy. 75% of breaches were executed by outsiders. While the insider threat exists, it's not as common as some believe. Partner organisations, on the other hand, are a more significant risk. Supply chain attacks can have much wider reaching impacts than other types, because they can affect larger numbers of targets.

Insider threats are real but rare. Businesses are **75%** more likely to be hacked by an outsider

Malware

While social engineering is popular with attackers, malware remains a significant problem. At least one third of all breaches involve the use of malicious code. Hackers don't need to create their own tools though. They are increasingly abusing legitimate software available on the network. Scripting systems like PowerShell can help the bad guys as much as real systems administrators.

Exploits

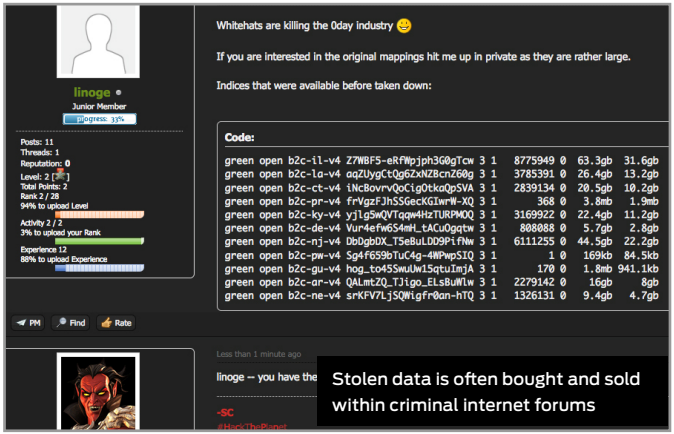
Hackers still exploit vulnerabilities in software, but that's relatively rare. Attackers used exploits in less than 10% of breaches over the last few months. However, this is an increase of 100% since last year, so we're expecting more of this type of attack in the near future, particularly during times of international conflict. Relatively rare, 'unknown' zero day exploits became more commonly used during the Russian invasion of Ukraine.

Zero day exploits have always been expensive and, therefore, uncommon. Known only to the researchers who discovered them, and a restricted number of associates, they are mainly used by nation states that can either afford to run their own research or pay for their exclusive use.

Are you Hacked Already?

43% of BEC involves stolen credentials (log in and send email from a real account)

In 50% of cases the attacker will let you know that you have been hacked. This could be in the form of a ransom note or a public announcement. If you keep an eye on criminal forums, such as on the so-called 'dark web', you might even see your data for sale. If we go back to the start of this section, it's not hard to realise that half of businesses aren't paying enough attention to prevent, handle or even notice data breaches until it's too late. And yet nothing the criminals are doing is particularly innovative. If there is any good news, it's that it should be relatively easy to reach the top 10% of most secure businesses in the world. The bar is so low.



Stolen data is often bought and sold within criminal internet forums

96% of breaches are financially motivated

Criminals sell access to targets for less than **$1**

27% of all email attacks are targeted against businesses (BEC)

ONE THIRD
of Breaches Involve Malware

95% of ransomware attacks target Backups

EMAIL PHISHING IS BEHIND **20%** OF ALL BREACHES

50% OF BREACHES ARE CAUSED BY HACKING

Data shown here is representative of that reported to us by clients and found in reports such as the Verizon Data Breach Report 2022, UK government statistics and other, smaller surveys from reputable sources

Section 02

Ransomware

Ransomware is the most visible, most easily understood cyber threat affecting businesses today

Paralysed computer systems mean stalled business and loss of earnings. On top of that, a ransom demand provides a clear, countable value to a threat. A demand for "one million dollars!" is easier to quantify than the possible leak of intellectual property to a competitor.

SE Labs takes some truly innovative approaches to testing anti-ransomware technologies.

Deep and Direct Ransomware Testing

300 ways to run a ransomware attack!

Our new ransomware test takes a sophisticated approach to assessing security solutions. It uses new adaptations of attacks alongside known, historical attacks. We test using the full attack chain, so products can demonstrate not only their abilities to block ransomware malware but also to detect the attack at earlier stages. We published the first test report of its kind in October 2022.

Testing security usually involves seeing if a product can handle threats from the past. If you're lucky, this might be recent history. But it is often the case that tests look back to ancient times. In the case of a physical lock, you'd hope a test would use state of the art picking techniques, not the methods used by Egyptian tomb robbers from a thousand years ago.

Realistic Ransomware

With anti-ransomware solutions you might expect testers to scan or run a collection of ransomware malware files. These might have been in use by criminals over the last few weeks, months or even a couple of years. But you'd hope that the focus would be on the most modern, most likely attack methods. And not fake anti-virus extortion software from a decade ago.

The Enterprise Advanced Security Ransomware test combines recent historical attacks with realistic variations, as well as brand new attacks designed to copy the usual modus operandi (MO) of the usual suspects. In other words, we copy the bad guys and behave in the same way that they did when they ran their attacking campaigns in the past.

Ransomware is Just a Payload

Ransomware attacks are standard hacking attacks that deploy ransomware as a payload. This means that anti-ransomware products would do well to monitor the full scope of an attack, rather than just the end bit, where malware encrypts files.

For this reason, our test also includes a detection part, where we monitor how effectively security products track the attack from start to end. This is useful because it's unlikely that every product will detect every ransomware malware file. But if it is able to track the attack, much like a CCTV camera can stand witness to a burglary, your security team stands a chance of preparing to avoid future successful attacks.

Read the first full report, featuring CrowdStrike Falcon, on our **website**.

Anatomy of a Ransomware Attack

How do attackers break in and extort ransoms

Defending against a ransomware attack is only possible if you know how the attackers work. The good news is that they tend to follow the same methods time and time again. You can massively increase your chances of staying safe if you mitigate against these threats.

How does it Start?

The most likely way that ransomware attackers will begin their campaign against your organisation is by sending an email. This will almost certainly be one of the following:

- A request for your log in details, either
  (a) in the email itself (phishing) or
  (b) on a webpage that you reach by clicking a link in the email (phishing).
- A link to something that sounds useful but is actually harmful software that:
  (a) you need to run manually (social engineering) or
  (b) will run itself automatically (exploit).
- An email that claims falsely you have been successfully attacked and demands a ransom (social engineering).

You might receive an SMS message to your mobile phone containing phishing or other social engineering links, as above. Attackers used automated phone calls to achieve the same goals.

These attacks might require that you visit links using your main computer so the attackers can gain remote access.

Some attackers infect websites with pop-up messages that direct visitors to download malicious software. More advanced attackers, with no sense of urgency, can set up websites that they believe you will find useful and allow you to find them independently. These 'waterhole' attacks use automatic exploits against specific targets, and don't infect everyone.

Finally, there is the insider attack, where a contractor or member of staff installs remote access or ransomware software directly onto a network.

The rise in ransomware attacks is higher than in previous five years

Next Steps

Attackers that target organisations need to gain access to many systems on the network, not just the computer owned by the initial victim. This is why we refer to ransomware as a payload. The attacker might gain initial access, run some reconnaissance to find out what types of systems are available and then move through the network, seeking out the best targets. The classic stages of a hack apply just as much

to ransomware attacks as anything else. These usually involve finding out about a target, getting a foothold onto the network and then digging in deeper to find the best data to damage or steal. You can summarise it simply like this:

- Initial reconnaissance (open-source research, scanning the outer network)
- Initial contact (email, web query, SMS)
- Exploitation (technical or social engineering)
- Internal reconnaissance (scanning the inner network)
- Achieve main goals (persistence, damage, data theft)

Ransomware attackers are likely to return to previous victims

Release the Ransomware!

Once the attackers have control of the target systems, they will deploy the ransomware software that encrypts files and possibly leaves information about how to pay the ransom. They might also steal copies of the data first, to further extort the organisation with threats of leaking.

Statistics suggest that ransomware attackers will return to previous victims, particularly if they receive a ransom payment. It's highly likely that they will attempt to set up a persistent presence on the network, hiding on systems unaffected by the ransomware. This allows them to run another attack in the future without having to worry about the initial attack stages. And by avoiding affected systems they reduce the risk of being 'cleaned' out of the network.

Ransomware Detection on a Chip

Modern processors can help defend against the ransomware threat

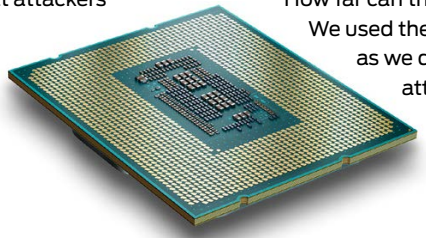
The security industry can't claim that it's winning the war on ransomware. And even if it did, public breach statistics would make a strong counterargument. Everyone, from security vendors to their biggest, richest customers, need all the help they can get. Hardware manufacturers are starting to get involved.

Attackers are often experienced in evading detection. They learn how security software works and develop ways to either hide from it or even disable it. Doing the same to physical hardware microprocessors is much harder. This presents an opportunity for defenders, and one major chip maker has announced its intention to take it.

Intel has developed security features in its latest processors that aim to improve ransomware detection. While some security companies focus on watching out for threats as they arrive, Intel's Threat Detection Technology (TDT) takes a different approach.

Watch all Layers

Ransomware is a payload – the software that attackers run after they have penetrated the network. The good news is that attackers can't just insert it into a target system magically. It has to get there somehow, which presents multiple avenues for detection.



Cloud services can spot incoming threats before they hit the network. Endpoint Detection and Response (EDR) software can detect and block threats after they arrive. Intel's TDT sits at the bottom of these security layers, watching out for malicious behaviour from the hardware level. It can potentially see things that the operating system and the software that runs on it cannot see.

The basic concept is that the hardware feed information about detections to the EDR software products from other companies, such as Microsoft and CrowdStrike.

Intel hopes that TDT will bring advantages, such as improved performance by using the in-built graphics chip (GPU) to do some of the heavy lifting. And by giving a deeper view on the threats, TDT aims to make it more challenging for attackers to bypass detection. Intel also claims that TDT can help with recovering from a ransomware attack.

We put Intel's claims to the test in our leading ransomware test. How far can the technology help EDR software detect ransomware? We used the same advanced method of testing anti-ransomware as we described on **page 11**. We used well-known ransomware attacks and many variations. We also ran full hacking attacks in exactly the same way as cyber criminals. Check out the special report on our **website**.

SE Labs

Test Guide

EAS
Enterprise Advanced Security

Red team test with full attack chains

EDR
Endpoint Detection and Response
Protection
Detection

NDR
Network Detection and Response
Protection
Detection

NGFW
Next-Generation Firewall
Protection
Detection

Others
Bespoke Detection / Protection

EAP
Enterprise Advanced Performance

Realistic and repeatable performance test

EDR
Endpoint Detection and Response
Performance

NGFW
Next-Generation Firewall
Performance

NDR
Network Detection and Response
Performance

ESS
Email Security Services

Red team test with full attack chains

Email Security Services
Protection
Detection

EPS
Endpoint Security

Anti-virus and targeted attack test

Endpoint Security
Protection

Certification

Verify the functionality of a product

EPS
Endpoint Security
Protection

ODMD
On-Demand Malware Detection
Detection

Section 03

Annual Security Awards

After months of in-depth testing and analysis we are proud to announce this year's Annual Security Awards winners.

Each of the following companies and products have 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.

Annual Security Awards Winners

Our role as security testers is to assess and monitor the state of computer security solutions. We use realistic hacking techniques to check that security products do what their manufacturers and developers claim.

We also work directly with large organisations, which need to know how effective their choice of security products is. They also need advice when it comes time to make a change, such as buying new firewalls, switching anti-virus and considering different cloud services.

Some of our testing results appear in public reports, which are freely available on our website. Most of it stays private, aiding security vendors to improve their products and their customers to make informed buying decisions.

With this unique perspective on the security world, we know the truth behind the marketing of security. We also understand the needs of businesses, as well as their success stories and disappointing experiences with technology that promises a lot and underdelivers.

Our Annual Security Awards recognises security vendors that not only do well in our tests, but perform well in the real world with real customers. These awards are the only in the industry that recognise strong lab work combined with practical success. It is not possible to buy an SE Labs award – each is allocated entirely on merit. We are pleased to announce this year's winners!

Email Security Service

Email is the primary vector for cyber threats. As such, there is much opportunity for email security services to stop cyber attacks at their earliest stages. As the threat of targeted attacks, including advanced social engineering, grows so must email security services adapt to block the unwanted and allow the necessary emails through. This year's winner has demonstrated time and time again its abilities to sort the evil from the good.

Enterprise Endpoint

When malware reaches its target it's up to endpoint security solutions to make the last stand. A robust solution will make low impact on system performance and be easily manageable. It should also be adaptable enough to detect and protect against the latest targeted attacks as well as the general commodity threats that affect victims indiscriminately.

New Endpoint

Entering the SE Labs testing programme is not to be undertaken lightly. The tests are the toughest in the industry and only top-grade products achieve A, AA or AAA awards. We always welcome new entrants to our tests and it's incredibly satisfying to work with partners who work to solve problems as well as to celebrate victories.

Endpoint Detection & Response

The best security involves having a good understanding of your enemy and the extent of the impact they could make (or have already made) on your IT infrastructure. Endpoint Detection and Response are the boots on the ground when it comes to seeing, stopping and investigating cyber threats on the network. A great solution makes it easier for security teams to be more effective.

Next Generation Firewall

When we assess firewalls we put their data sheets to the test. How fast can the data move through these devices when security rules are in place to a realistic degree? How good is the security when the device is under pressure from attacks and heavy legitimate traffic? And how easy is it to manage all of these things? Our award winner excelled in all areas.

Innovator

Attackers are constantly finding new ways to attack, so security vendors need to keep inventing ways to detect and prevent them from gaining ground. It's not enough to tag marketing phrases such as 'machine learning' onto a product to win our Innovator award. The products need to work extremely well and provide vast added value to the items in your security toolbox.

Intel

intel

Product Development

Our testing engagements, whether public or private, provide vast amounts of information that can be used to improve and strengthen security products. Our award winner has taken our work and run with it, improving the security of their customers and making life significantly harder for attackers. We recognise their efficiency and effectiveness with this award.

CrowdStrike

CROWDSTRIKE

Network Detection & Response

When threats bypass cloud security, firewalls and endpoint detection, their presence can still be spotted as they move through the network. A good Network Detection and Response service can monitor network traffic and sound the alert and stop the threats. By adding further context they help security teams investigate full security incidents. Our winner helps these teams to an exceptional degree.

Small Business Endpoint

Small businesses face the same level of threat as global 500 organisations, but with a fraction of the budget and expertise available for defence. They need good security measures that don't require large teams to manage them. Our Small Business Endpoint winner supports small businesses by providing an effective and easily used endpoint protection product.

Home Anti-Malware

Everyone deserves good security, including home users. Attackers often do not discriminate between targets. Automated attacks have been running on the internet for decades, and phishing and other social engineering attacks appear in our inboxes on a daily basis. Home computers are also often used for small business purposes. Our Home Anti-Malware winner provides world-beating security without requiring users to become security experts.

Free Anti-Malware

Not everyone can afford to pay to protect their home computers. We recognise the need for free anti-virus options but require that these products stand up to the threats just as well as the expensive business options. There may be less need for easy management, but we won't compromise on protection. The winner of this award makes your computing life safer without a fee.

DE:CODED

PODCAST

Deciphering Cyber Security

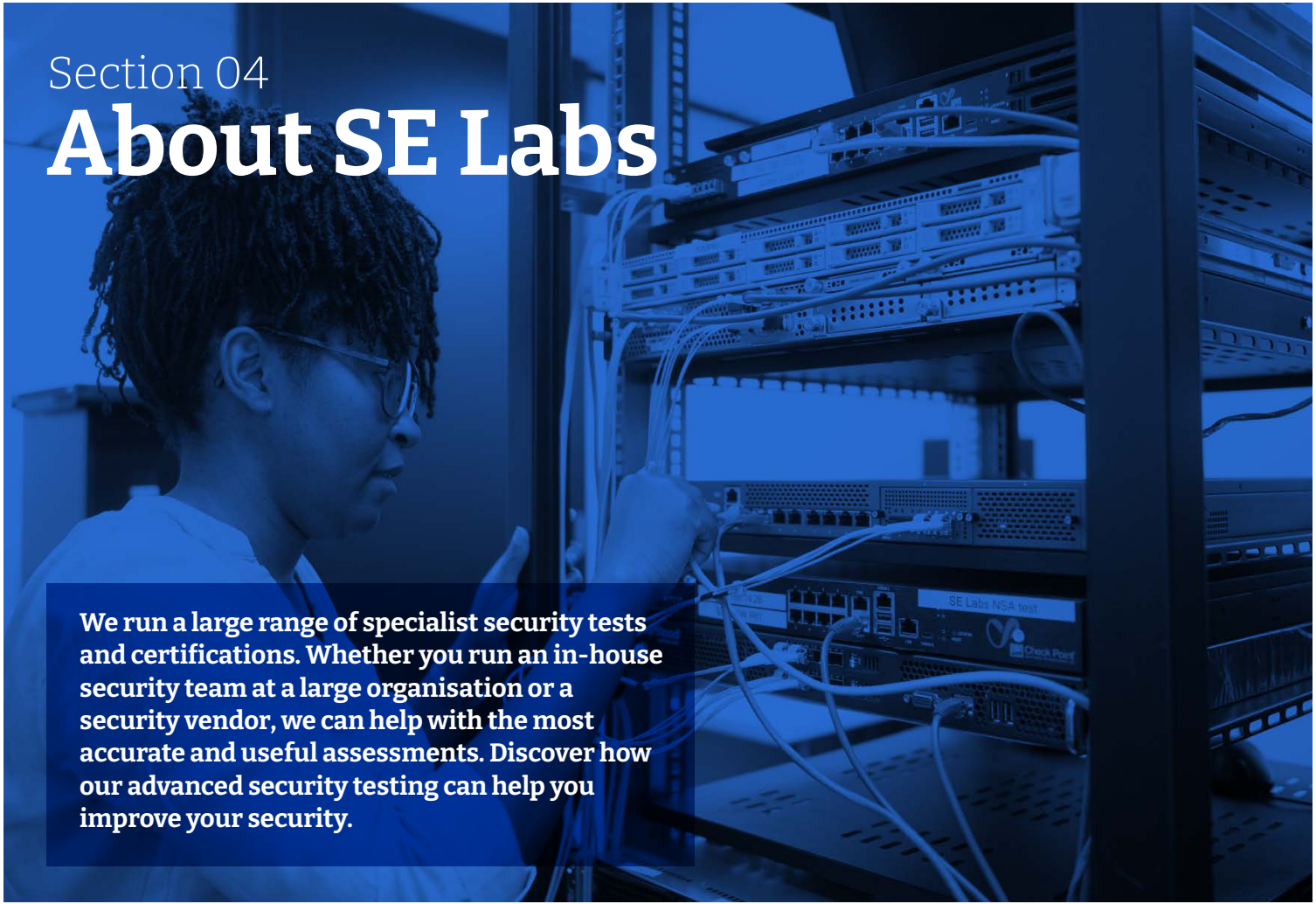
DE:CODED
SE Labs
Deciphering cyber security

Understand cybersecurity and other security issues. Practical and insightful, our experts have experience in attacking and defending in the physical and digital worlds. Peek behind the curtain with the Cyber Security **DE:CODED** podcast.

Listen on Apple Podcasts

Section 04

About SE Labs



We run a large range of specialist security tests and certifications. Whether you run an in-house security team at a large organisation or a security vendor, we can help with the most accurate and useful assessments. Discover how our advanced security testing can help you improve your security.

Our Tests

Security companies and their customers use our testing services to validate and improve security products. Large public and private companies use our tests to help make decisions when considering a change to their security infrastructures. Sometimes they want to verify or make changes to their configurations. Our realistic testing helps improve security in ways that technical teams and Board members can understand.

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. Our testing assesses the effectiveness of security features and the impact these have on performance. We explore how products handle significant threats including ransomware.

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 solutions**
  E.g., anti-virus; endpoint detection and response (EDR)
- **Network security appliances**
  E.g., firewalls; network detection and response (NDR)
- **Cloud security services**
  E.g., email and web security gateways
- **Incident response integrations**
  E.g., extended detection and response (XDR)

Certifications

We run two certification programmes. Both provide certificates acknowledging a product's performance in our tests. There are three main reasons to use SE Labs certification:

- **Demonstrate to customers or investors that your product works.**
- **Join the Microsoft Virus Initiative and then gain access to the Windows ELAM system.**
- **Join VirusTotal's detection scanner community.**

Consider the Endpoint Security (EPS) certification for MVI applications and the On-Demand Anti-Malware Detection (ODAMD) certification for VirusTotal.

Find out more about **public and private testing** and **get in touch** to start testing with us.

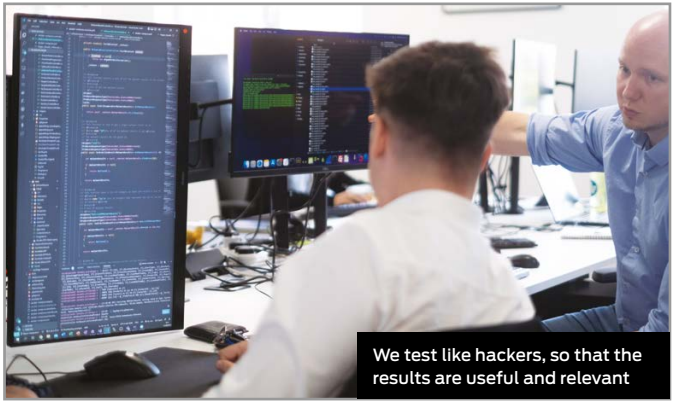
Test Developments

Just as cyber criminals change their behaviour to succeed, security testing needs to evolve to keep pace with the latest developments in offensive and defensive security. SE Labs has always taken a realistic approach to testing, avoiding simulations in preference to real attacks against targets set up in real-world configurations. Throughout 2022 we've continued with this approach and applied it to a new range of security products.

Endpoint Testing

SE Labs is probably best known for its endpoint testing. We run the most advanced anti-virus and endpoint detection and response (EDR) tests publicly available. Top-tier security vendors use our MITRE-compatible Enterprise Advanced Security (EAS) tests to improve their EDR products. Newer vendors can use our Endpoint Security (EPS) tests to assess their endpoint security ('anti-virus') products publicly or privately, and potentially gain access to Microsoft's Windows ELAM system.

Any security vendor can test their beta products privately, alongside existing releases, for internal comparison.



We test like hackers, so that the results are useful and relevant

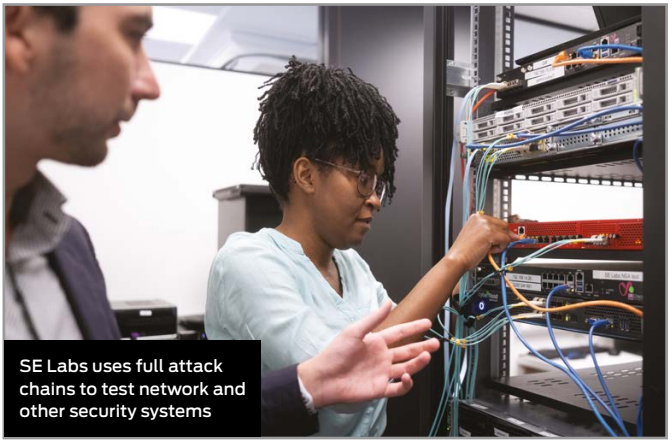
> "SE Labs has always taken a realistic approach to testing"

Ransomware Testing

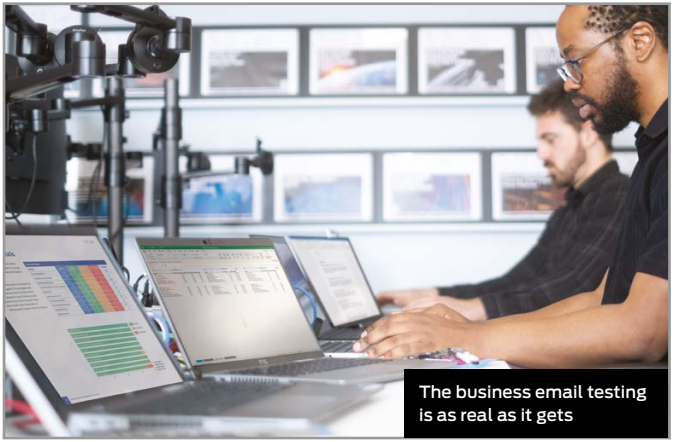
The ransomware threat is so significant that it demands its own special tests. As you can see in **2. Ransomware** on page 10, we've developed new ransomware-focussed tests to assess anti-virus, EDR and even hardware-assisted detection and mitigation of the threats. Ransomware attacks can be indiscriminatory or targeted, and we take both approaches into account in our tests, using real-world attacks and creating realistic variations.

Network Testing

Increasing interest in network security products such as Network Detection and Response (NDR) and Next-Generation Firewalls (NGFW) led us in 2022 to announce our security and performance



SE Labs uses full attack chains to test network and other security systems



The business email testing is as real as it gets

testing programme for these types of products, as well as combinations of network and endpoint security – known as Extended Detection and Response (XDR).

Our network performance testing is compatible with the NetSecOPEN testing Standard and our network security testing adopts the challenging and thorough approach we take with the flexible Enterprise Advanced Security test.

We use full attack chains to assess the detection and protection abilities of network devices and combinations of network and endpoint solutions.

Cloud Services Testing

We continue to develop cloud-based security tests and our Email Security Services (ESS) test reached new strengths in 2022, with rigorous attacks against targets that appear in nearly every way to be real target organisations. Our Business Email Compromise (BEC) testing is as close to the real thing as possible.

We continue to develop tests for other types of cloud security services, including mobile security and assessments of 'Internet of Things' (IoT) devices.

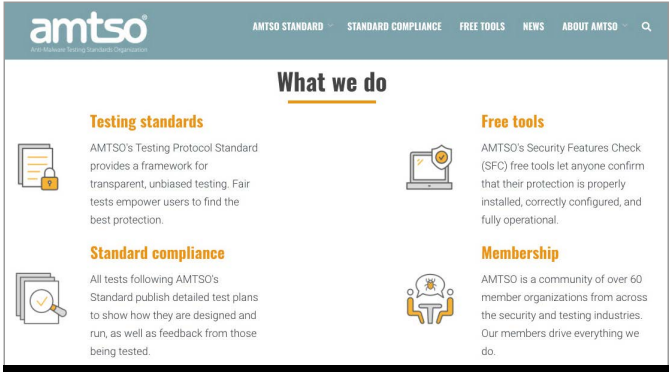
Testing in the Real World

As attackers change their attacks to avoid detection, vendors and other organisations take new approaches to the problem of security. These all need to be tested and it's rare to find a solution that can't be tested in a useful way. As cybercrime continues to evolve, so will the tests conducted by the SE Labs team.

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 relatively, there was no official way in which to demonstrate that we do what we say.



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

A reliable tester states in advance what it's going to do; follows its own rules; and then has the data to prove it has done what it said it would.

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. The Standard means, say what you're going to do. Do it! Then be prepared to prove it.

SE Labs was the first testing lab to engage with the Standard, running private and public pilots, before complying with the official Standard immediately. No other testing organisation has engaged so thoroughly and successfully with the AMTSO Standard.

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, SE labs complies with the ISO 9001 : 2015 Standard for Quality Management Systems, specifically relating to the Provision of IT Security Product Testing. We are also ISO/IEC 27001 : 2013 certified.

Test Like Hackers

To test a security product properly, you have to behave like a real attacker. There are countless clever ways to simulate attacks, automate testing and so on, but at the end of the day nothing beats sitting down and manually hacking away at a target for realism, which is why we do it that way. That said, to ensure that testing keeps abreast of the latest developments, we were the first testers to use machine learning to help power our tests.

Advanced Security Testing

Over the course of 2022 we used our full attack chain testing on a range of products. Historically the most common choice by the vendors was their endpoint protection products. This is why most of the 'breach response' reports on our website contain results for endpoint or 'EDR' products.

However, the way we test also works perfectly with firewalls, intrusion detection systems and cloud services. Starting in 2022, we migrated our 'breach response' testing to the Enterprise Advanced Security (EAS) test programme. EAS testing is available for endpoints; network appliances; and cloud services. This means that we're already producing EAS reports for EDR, next-generation firewalls, network detection and response systems and email security services.

As before we have worked with The MITRE Corporation and others on how to score products in a way that is compatible with the MITRE ATT&CK framework so, if you're familiar with that system, you'll find it extremely easy to understand our EAS test reports. Subsequently, it will also be simpler to assess which products you might choose to deploy.

Hackers vs. Targets

Attacker/APT Group	Method	Target	Details
Dragonfly & Dragonfly 2.0			Phishing & supply chain methods used to gain access
APT34			Phishing with email and other services, combined with public tools
FIN7 & Carbanak			Documents containing scripts combined with public tools
APT29			Spear phishing emails containing scripts or links to malware

Regardless of the product type, we can produce EAS reports in one of two modes: Detection or Protection. The Protection mode reports look at how fully a product (or combination of products) can protect the target, while the Detection mode approach assesses how thoroughly a product can detect different elements of an attack. You can read about these reports on **page 15**.

Computer Viruses are Still a Thing?

SE Labs is probably best known for its world-leading anti-malware testing, in the shape of our Endpoint Security (EPS) test. In 2022 we tested more products than ever before and have welcomed some of the best-known products from the newer, so-called 'next-gen' companies like SentinelOne, FireEye, BlackBerry and CrowdStrike. Our EPS reports are the best place to find such

a wide variety of business and consumer products tested to such an in-depth degree.

Threats in the Mail

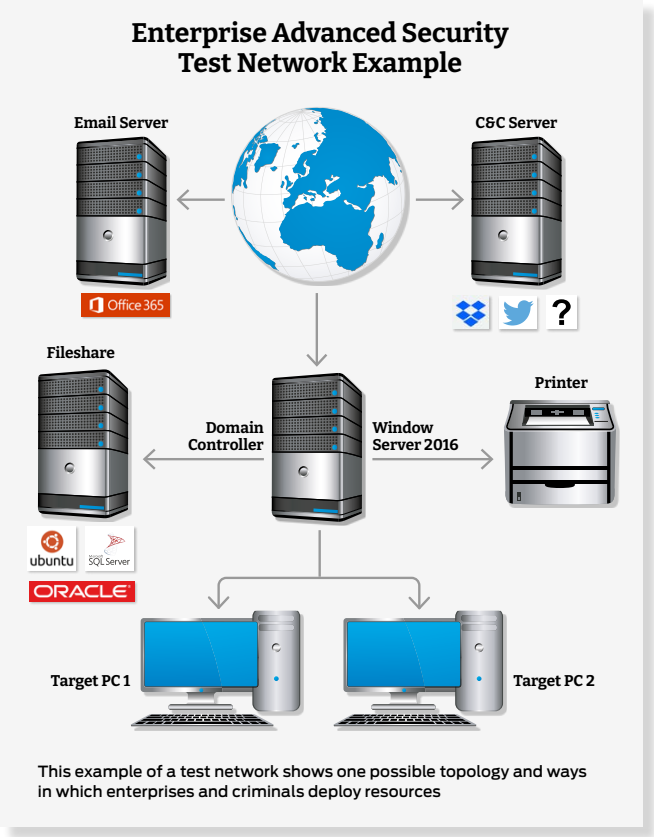
Our Email Security Services test also reached new strengths in 2022. The way we test has expanded to include business email compromise threats, to the extent that our test framework includes the ability to replicate a real target organisation and its attackers and legitimate suppliers.

We also run a baselining process during which next-generation email security products can learn what a clean network looks like. This helps some technologies detect malicious anomalies.

The development of this test has attracted the attention of all the major email vendors, who are now testing privately with us on a regular basis. Public reports, along with important details of the configurations used, are available on our website. You can see how the test is structured on **page 31**.

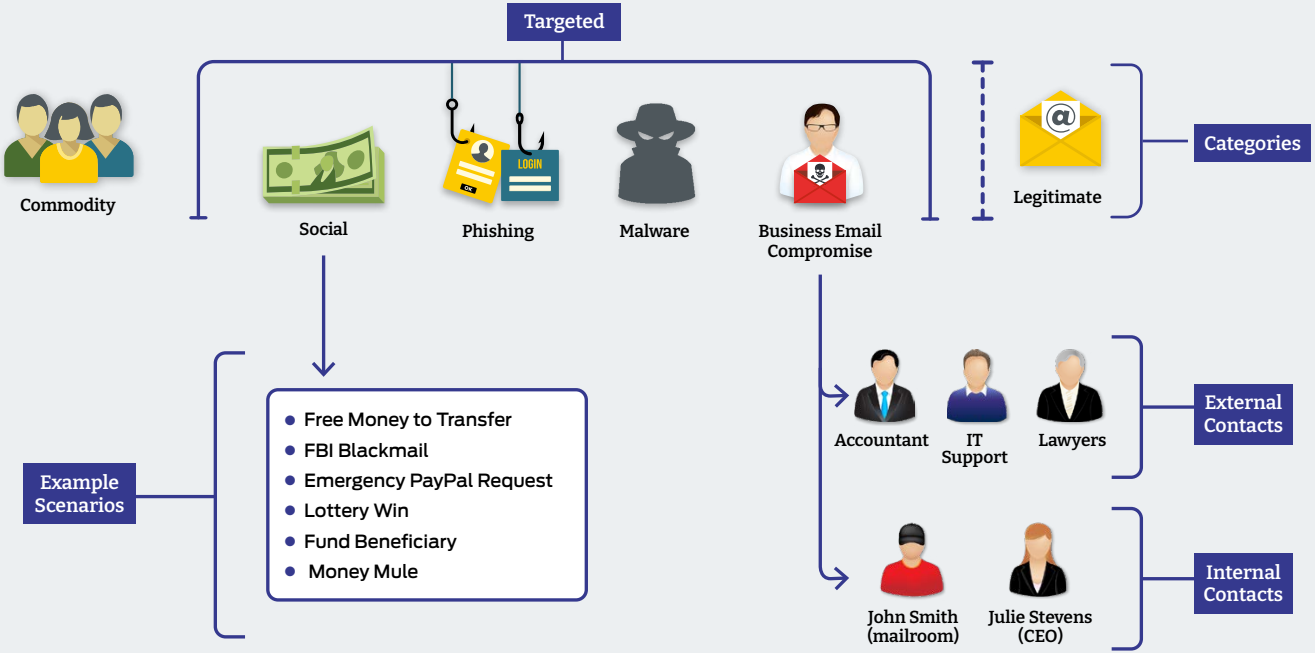
Threats Mobilise

Finally, we have created a new mobile security test that covers both Android and iOS. All of our testing must produce useful, meaningful data, which is why we have previously resisted running anti-malware tests for Android and iOS platforms – there isn't really much in the way of true malware in the wild. We are focussed on assessing mobile products' abilities to protect users from significant threats that pose real-world issues for users such as phishing.



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

Email Security Services Test Case Structure



Threats used in the Advanced Email Security test vary in type and include targeted business attacks

Stay in Touch

Don't miss out on the latest in the world of cyber security testing

Newsletter

The Best Way

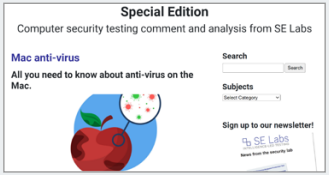
Our monthly newsletter provides a compact summary of all our reports, blog posts and other analysis that we provide publicly. Subscribe to this free newsletter and you won't miss out on a thing.

Don't rely on catching our social media posts as they fly by. All the best stuff ends up in the newsletter! We have options for enterprises, consumers and security vendors. Sign up now for free.

Link: https://selabs.uk/newsletter

Visit

Blog



Our blog gives a behind-the-scenes view on cybersecurity testing. Learn how we work and how you can improve your own personal and business security.

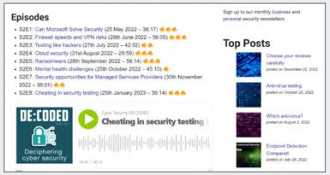
The blog adds extra context to all of our public reports. Understand what the security reports can mean to you, and how to use their results.

Our team monitors the threat landscape and writes about what we see. Stay informed about the latest attacks and learn how to stay safe.

Link: https://blog.selabs.uk/

Visit

Podcast



The security testers at SE Labs help decode the notoriously opaque world of cyber security. Practical and insightful, our experts have experience in attacking and defending in the physical and digital worlds.

In-depth discussions with expert guests will help you develop your own strategies for protecting yourself and your business. No marketing. Just solid, valuable advice from the best in the business.

Peek behind the curtain with Cyber Security DE:CODED, the award-winning podcast.

Link: http://decodedcyber.com/

Visit

The C2

The C2 is an event that bridges the knowledge gap of leading global security vendors and enterprise level businesses.

It combines open and frank discussions with talks by international leaders in threat intelligence.

The intimate gathering provides a bespoke experience for leaders in security and threat intelligence.

For more information speak to your SE Labs contact or visit ***the-c2.com***

Management

Chief Executive Officer
Simon Edwards

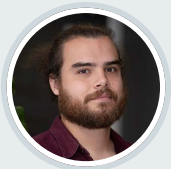
Chief Operations Officer
Marc Briggs

Chief Human Resources Officer
Magdalena Jurenko

Chief Technical Officer
Stefan Dumitrascu

SE Labs Team

EPS Project Lead
Nikki Albesa



EAS Project Lead
Thomas Bean

NSA Project Lead
Solandra Brewster

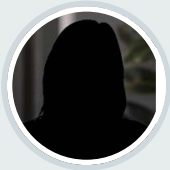
ESS Project Lead
Joseph Pike

Threat Engineer
Erica Marotta

Senior Security Analyst
Jeremiah Morgan

Senior Security Analyst
Julian Owusu-Abrokwa

Senior Security Analyst
Dimitrios Tsarouchas



Security Analyst
Gia Gorbold

Security Analyst
Anila Johny

Security Analyst
Luca Menegazzo

Security Analyst
Georgios Sakatzidi

Development Ops
Stephen Withey

Marketing
Sara Clarridge

Art Director
Colin Mackleworth

SE Labs

Website selabs.uk
Email info@SELabs.uk
Blog blog.selabs.uk
LinkedIn linkedin.com/se-labs/
Phone +44 (0)203 875 5000
Post SE Labs Ltd,
55A High Street,
Wimbledon,
SW19 5BA,
UK

SE Labs is ISO/IEC 27001 : 2013 certified and BS EN ISO 9001 : 2015 certified for The Provision of IT Security Product Testing.

SE Labs is a member of the Microsoft Virus Information Alliance (VIA); the Anti-Malware Testing Standards Organization (AMTSO); and NetSecOPEN.