TREND MICRO™

POWERED BY XGen™ SECURITY

No Silver Bullet: UK Firms Under Attack

How IT leaders are tooling up with advanced security to combat online threats

Introduction

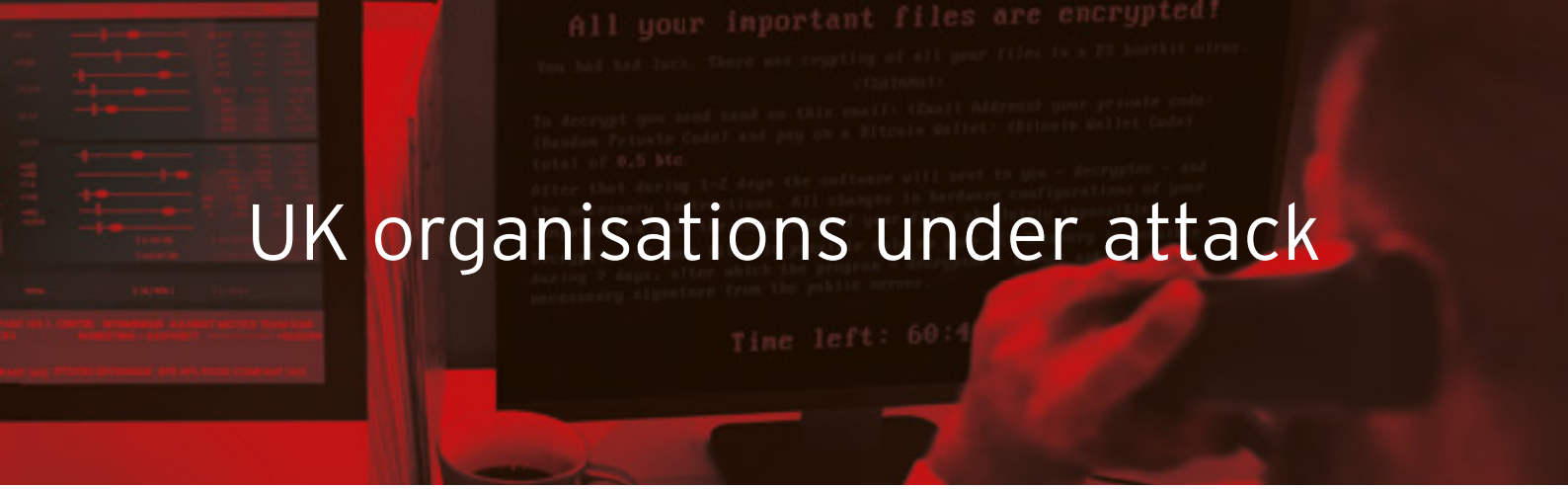
We live in extraordinary times. The internet has revolutionised the way we do business. And mobility, cloud computing, and the Internet of Things (IoT) are already enabling organisations to deliver innovative new services, and making them more productive, agile and cost efficient in the process. But the technologies that power our modern hospitals, schools, governments, factories and corporations are also more exposed than they've ever been to cyber threats.

This makes guarding your employee and customer data, company IP and systems more important than ever. As our latest predictions report, The Next Tier, reveals, the bad guys are getting ever more resourceful and determined – using the element of surprise and newly developed tools, tactics and procedures to circumvent our defences.

The impact of a breach could be devastating. Apart from the remediation and clean-up costs, firms need to consider the possible loss of customers and share price hit that might result from a damaged brand. Not only that, but additional legal costs and possibly regulatory fines might ensue. The latter is particularly pertinent considering the new European Union General Data Protection Regulation (GDPR) set to come into force in May 2018. It will levy fines of up to €20m or 4% of global annual turnover for serious transgressions around personal identifiable information (PII), and demands 72-hour breach notifications.

There's no doubt: cyber security is now a major board-level issue, but what do IT decision makers on the frontline think?

The report reveals current threat levels and what IT leaders think will comprise the biggest challenges and cyber threats to their organisation over the next twelve months. It also gauges their perception of newer advanced security tools, such as application behavioural analysis and machine learning. The report further discusses whether these tools are better off as part of a layered approach to security from a single integrated vendor, as there really is no silver bullet in cyber security.



UK organisations under attack

We asked just how extensive are the threats facing UK firms today? The bad news is that nearly half (48%) of respondents said they'd suffered a 'known' cyber attack over the past 12 months, with over a quarter (28%) saying they'd experienced more than 3 attacks.

This is particularly concerning as it takes just one simple malware infection, DDoS blitz, employee mistake or email-borne scam to cause widespread financial loss and reputation damage to an organisation.

Some 46% claimed not to have suffered an attack over the past year. However, given the stealthy nature of targeted and cyber espionage-type attacks, and the lack of visibility some IT teams have into key systems, it's likely that a large percentage of these organisations will also have been compromised without their knowledge.

How many 'known' cyber-attacks did your organisation experience over the last 12 months that disrupted your ability to carry out day to day business?

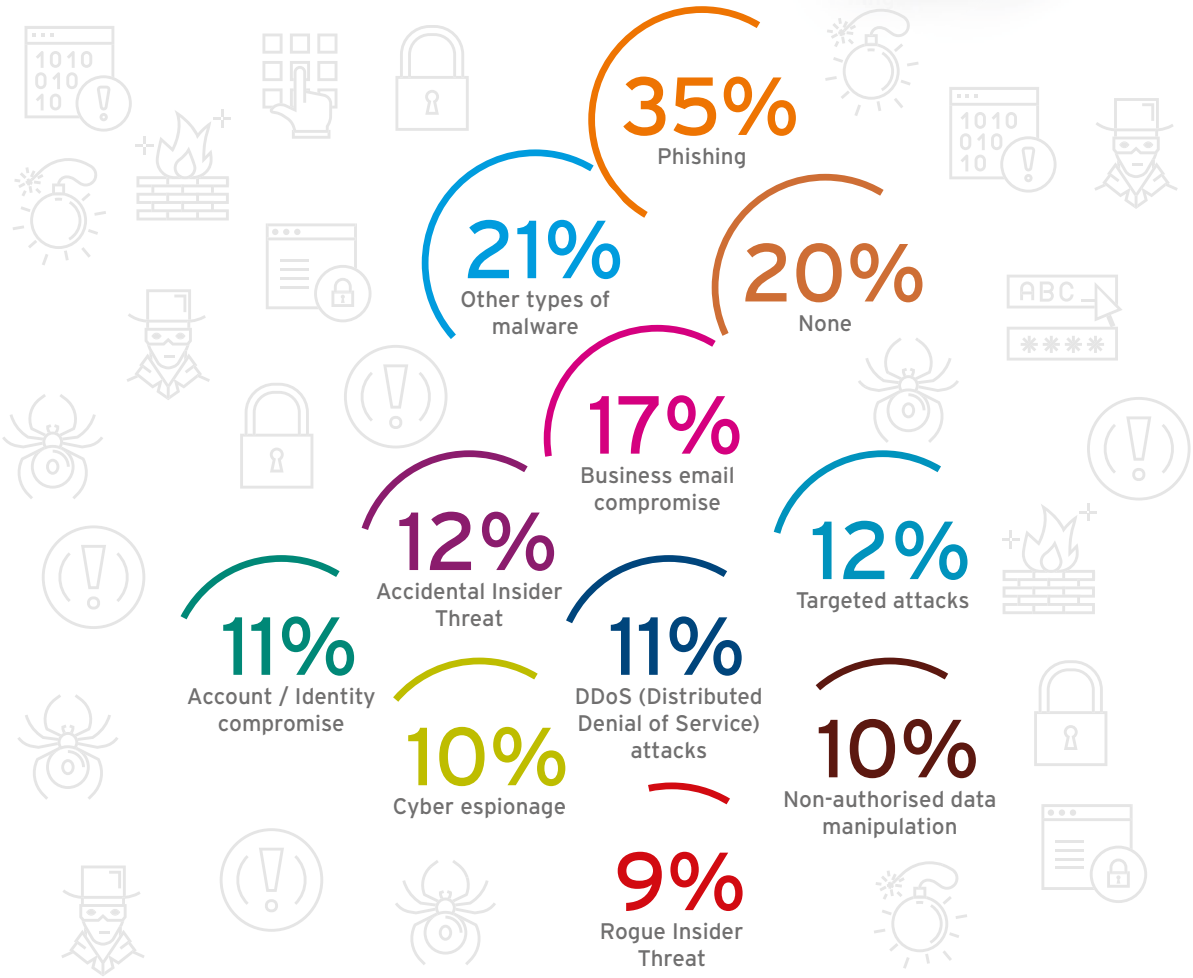
46%	No attacks
20%	1 - 2 attacks
12%	3 - 6 attacks
8%	7 - 10 attacks
4%	11 - 15 attacks
3%	16+ attacks
7%	Don't know

Ransomware was by far the most common threat type, with 69% of respondents claiming to have been attacked at least once in the period. In fact, only a quarter (27%) had not suffered a ransomware attack, highlighting the scale of this threat. Phishing (35%) was the next most common threat, followed by other malware (21%), Business Email Compromise or BEC (17%), targeted attacks (12%), accidental insider threats (12%) and DDoS (11%).

Of the 'known' cyber- attacks that disrupted your business last year, how many were ransomware attacks?

69%
Ransomware

What other security threats did you encounter last year?



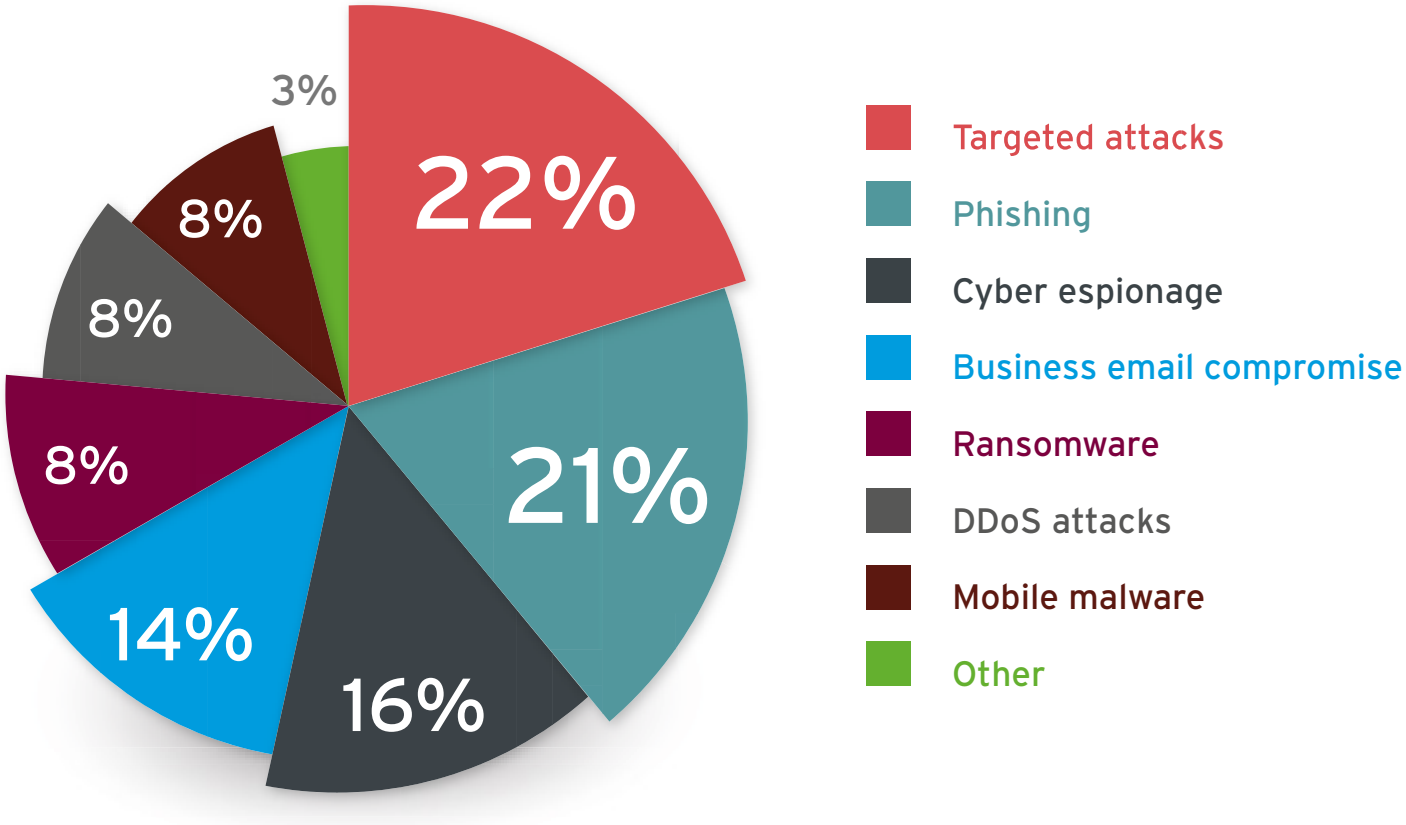
What are UK IT leaders most concerned about over the coming 12 months?

Number one was targeted attacks (22%). As mentioned, these insidious threats are specifically designed to fly under the radar of traditional defences and can be hard for employees to spot. Once inside the network, the attacker could lie hidden for days, weeks or even months, stealing valuable customer data or IP. Needless to say, the longer they go undetected the worse the impact.

Phishing (21%) came next. It can be a threat to organisations in two ways: spear-phishing attacks typically target a specific staff member or members, tricking them to click on a link or open an attachment as the first stage of a targeted attack. But broader phishing attempts on your customers, using emails spoofed to look like they came from your organisation, can serve to undermine brand and reputation.

Cyber espionage (16%) was also high on the watch list for UK IT decision makers, while the relatively new appearance of Business Email Compromise (BEC) – also known as CEO fraud or "whaling" – was pegged as the biggest threat for 14% of respondents. Interestingly, just 8% flagged ransomware, despite the havoc it has wreaked to date.

What do you believe will be the biggest security threat to your organisation in 2017?

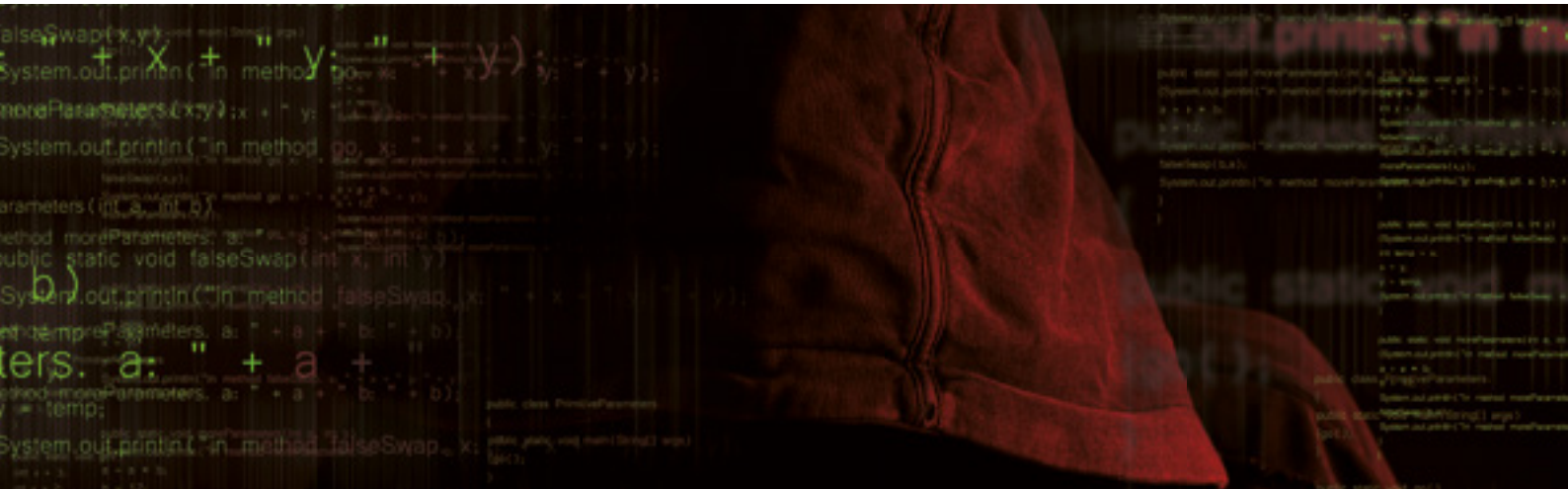


The data tallies nicely with Trend Micro's threat predictions report. In it, we flag the fact that ransomware will plateau as cybercriminals increasingly turn to BEC to gain a higher ROI from their attacks. The latter is particularly hard to spot as it relies not on malware but simple social engineering coupled with a spoofed domain to trick the recipient into transferring large sums to a third-party bank account.

We also predict in the report that the black hats (hackers) will continue to evolve their targeted attack tools and techniques to make them harder to detect with traditional security defences. Industrial IoT systems could be at major risk of targeted attacks as we go forward. We also warn of a rise in cyber propaganda, which includes nation states publicising sensitive data obtained via cyber espionage, for geopolitical purposes. UK IT decision makers are right to be concerned about the threat from state-sponsored hackers.

IT leaders are doing their best to protect themselves from the growing variety and volume of threats facing them. But many (38%) feel that a lack of understanding about cyber threats could be impeding their ability to do so. The sheer unpredictability of the black hats (36%) and the fast-moving nature of the threat landscape (27%) were also high on the list of challenges, as was legacy infrastructure (25%), which is more prone to attack than modern systems.

What do you think are the 3 biggest challenges organisations face when protecting themselves from cyber attacks?



Attack surface grows

So where are the threats likely to stem from going forward? Poorly secured networks (14%), use of unsecured public Wi-Fi (14%), and inadequate device security (12%) were flagged by respondents as the top causes.

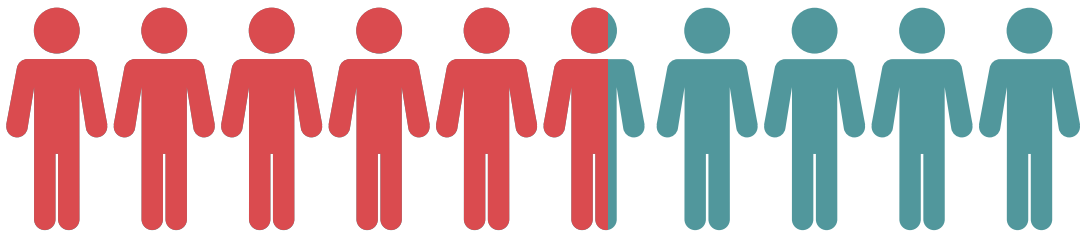
The latter two in particular are linked to the rise of mobile working and the increased attack surface created by mobile devices and the cloud, which organisations now have to defend against. In fact, 80% of respondents claimed the rise in endpoint devices would "significantly" or "slightly" increase risk. The problem with many of these devices is that they're owned by employees and therefore exposed to the risk of unsecured Wi-Fi, malware in third party app stores and online, and other threats, but not vetted before connecting to the corporate network. This can provide attackers with a ready-made incursion point into your IT systems. As wearables get smarter and more ubiquitous the threat will continue to grow.

IT leaders believe the best ways to reduce mobile risk are to educate staff (46%), enforce compulsory security such as default passwords (26%) and only allow staff to choose from a list of pre-approved devices (24%).

Tooling up with advanced security

The good news is that over three-quarters (77%) of IT leaders are confident they understand the cyber security challenges their organisation will face in the future. Is this confidence well placed given the scale of known and unknown threats facing them and the challenges described above?

The IT decision makers we spoke to appeared to have a pretty good grasp of advanced security techniques and are already implementing things like machine learning and behavioural analysis on a wide scale.



Over half (56%) of UK IT leaders are using advanced security techniques like machine learning and behavioural analysis in their current security solutions. 43% said they're considering integrating advanced security in the next 12-18 months.

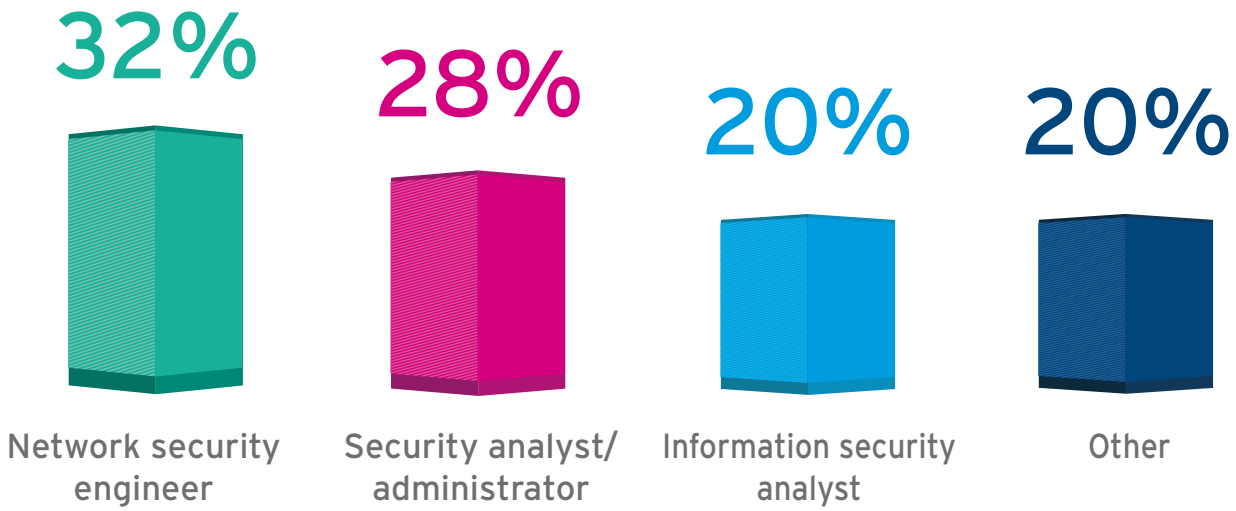
Nearly two-thirds (64%) believe machine learning and behavioural analysis are "very" or "quite" effective at preventing cyber attacks.

A plurality (42%) of IT leaders also believe these tools will ultimately make the job of security professionals easier, by filtering out stealthy threats more effectively.

In fact, nearly three-quarters (72%) think machine learning, artificial intelligence and other advanced techniques could one day replace the need for human expertise to pick through the subtle differences between anomalies. Network security engineers (32%), security analysts (28%), and security administrators (28%) are the top three roles that these technologies could fully replace.

Do you foresee advanced security such as machine learning replacing the need for human expertise in the future?

What job functions do you think would be most affected?



Layered threat protection

It's not all about investing in the latest and greatest technologies as a silver bullet to tackle modern-day threats. IT decision makers in the UK instead favour a layered approach, with 52% claiming: "we need to know that there are multiple hurdles for potential cyber-attacks to overcome."

They believe in security which features an integrated solution from a single vendor (46%) rather than a best-of-breed strategy (37%). And there was a definite rejection by IT buyers of newer vendors which hype their limited technology solutions as a cure-all for cyber security woes. Over half (56%) of respondents said they'd prefer to go with an experienced, stable vendor that understands the organisation.

Classic techniques like anti-malware and content filtering are still highly efficient techniques that remain critical for eliminating the high volume of known bad threats still active today. However, with the increase in stealthier and more sophisticated threats like targeted attacks, ransomware, and business email compromise, newer, more advanced threat defence techniques are also recommended. A multi-layered defence that covers endpoint, network, web, email and physical/hybrid cloud servers is required. Ideally one that can be managed from a single console.

Advanced security recommendations

Advanced security techniques to consider integrating into your existing threat defence include:

Signature-based detection: combined with file and web reputation and C&C blocking can stop most known threats. Note this is highly computationally efficient.

Application behavioural analysis: examines an item as it is unpacked, looking for suspicious or unusual behaviour in how it interacts with operating systems, applications and scripts — even if the item isn't on a blacklist. Helps block crypto-ransomware in this way. Also includes techniques such as script protection; injection protection; memory inspection; suspicious action monitoring; browser exploit protection.

Exploit prevention: prevents exploitation of app/OS flaws. Includes host-based firewalls; exploit protection; intrusion prevention; lateral movement detection.

Application control/whitelisting: highly effective in blocking the installation and execution of any executables that aren't approved applications or dynamic link libraries (DLLs).

Investigation and forensics/Endpoint detection and response (EDR): records and reports on system-level activities in great detail in order to appraise nature and scale of an attack.

Machine learning: A high fidelity machine learning approach can be used to extract and analyse a file's characteristics both before and during its execution. This helps improve accuracy and – in combination with 'noise cancellation' techniques such as census (file prevalence) and whitelist checking (known good applications) – reduces false positives.

Sandboxing: The above can be combined with sandboxing to run the potentially suspicious files in a secure virtual machine in order to ascertain exactly how they would behave if run on a client PC. Not only can the file be blocked but additional attributes like File Has, IP, URL and domain information used for C&C call back, downloading of additional malicious content etc can also be extracted and shared with the wider infrastructure in near real time.

Conclusion

The UK's IT leaders are confident about their ability to understand future security challenges. With the volume and variety of known and unknown threats growing all the time, they agree that the best approach is to seek a multi-layered, integrated solution from a single, stable vendor who understands their needs. Best of breed might sound good on the tin, but in reality it can result in a sometimes disjointed hotchpotch of tools and an increase in false positives. This creates gaps for the black hats to exploit and increases the management overheads for IT teams

As we face down the threat from organised crime groups, hacktivists and state-sponsored hackers, as well as growing insider-related risk, it pays to seek out a vendor which can offer that broad blend of multi-layered threat protection from a single console. This offers improved protection as it makes it harder for any one threat to bypass all layers. It also reduces admin overheads, provides better cross-platform integration and reduces support and acquisition costs.

In short, there is no silver bullet to combat the huge volume and variety of modern threats, despite what you might hear from some vendors. For maximum protection with minimum impact on performance, it's got to be an integrated, multi-layered approach to threat defence covering endpoint, network, web, email and physical/hybrid cloud servers.

TREND MICRO™

We surveyed 2,402 IT Decision Makers in the UK, US, France, Germany, Italy, Netherlands, Sweden, Norway, Austria and Switzerland. The survey was conducted by Opinium in February 2017. 307 of the responses were IT Decision Makers in the UK.

Trend Micro XGen™ security is a truly smart, optimised, and connected threat defence. The cross-generational blend of threat defence techniques protects against the ever-changing threat landscape, providing maximum security with minimum impact.

Read more at www.trendmicro.co.uk/XGen

POWERED BY XGen™ SECURITY