RAPID RESPONSE

Patrick Wragg *reports on the importance of responding to a ransomware resurgence*

The intensity of the ransomware landscape has reached unprecedented levels since the turn of the decade. In 2021, we experienced a record-breaking year totalling 623.3-million ransomware attacks, an increase of 105 percent over 2020 figures.

Come early 2022, however, and research shows there was actually a 23 percent drop in ransomware incidents globally in H1, dropping to 236.1-million attempted attacks and continuing the downward trend that had been observed for the previous four quarters.

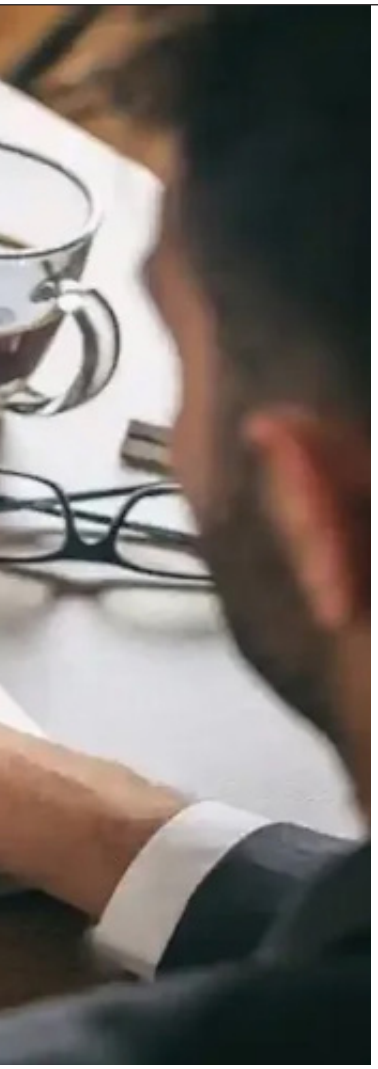
This was in large part down to the disappearance of some of the largest ransomware groups including Conti, REvil and PYSA, owing to the successful actions of law enforcement agencies.

The former, for example, was responsible for an incredibly impactful cyber-attack that paralysed the Costa Rican government in May 2022, disrupting the country's essential services, trade and healthcare systems. It marked the first time a nation declared a state of emergency in response to a cyber-attack.

In response, the US Department of State offered a $10-million bounty for information about the group's leaders, prompting the Conti group to go underground and cease operations.

In spite of successful outcomes such as this, ransomware again saw a resurgence in H2 2022, driven by the return of the LockBit ransomware operation.

Ransomware-as-a-service (RaaS) facilitators such as LockBit (currently estimated to account for over 40 percent



It is estimated that the total global cost of cyber crime will reach $10.5-trillion by 2025

of all global ransomware attacks) are particularly dangerous. Critically, they make sophisticated techniques available to the criminal masses, licensing out code to affiliates who then launch attacks on a broad scale in return for a fee.

The RaaS landscape is particularly worrisome in the current economic climate. As the cost-of-living crisis continues to take hold, more and more people will turn to cyber crime as a means of making money, with sophisticated outfits such as LockBit enabling these criminal opportunities.

Today, the ways in which exploitation gangs coercing victims into paying ransoms is changing. We're witnessing a growing trend towards double extortion techniques involving both the encryption and exfiltration of data, enabling threat actors to add pressure to targets by threatening to leak or sell sensitive information.

All these factors combined suggest that the ransomware resurgence will only continue in 2023 and beyond. In fact, come 2025, it is estimated that the total global cost of cyber crime will reach $10.5 trillion.

Staggeringly, if this were quantified in terms of economic output, cyber crime would be the world's third largest economy, only inferior to the USA ($25.03-trillion) and China ($18.32-trillion).

The statistics ultimately speak for themselves. Now, more than ever before, it is vital that organisations take steps to properly protect themselves in the face of intensifying threats.

So, how can companies make changes to improve their security posture? I believe there are three key areas firms should be focusing in on as a priority.

Improving prevention to combat encryption and leakage. First, organisations should look to rebalance their cybersecurity focus so that prevention plays just as central a role as detection and response.

Threat detection has been a huge focus of organisations and the wider security market, driven by the fear of advanced 'APT' threat actors. Resultantly, preventative controls have often fallen by the wayside – while they are often present in existing security platforms, they are typically underutilised or not properly configured.

While industry statistics tend to suggest that attacker dwell time is in the region of 200-plus days, my experience has shown that the initial stages, access and impacts of an attack can happen extremely quickly, and often in an automated manner. In such instances, those companies relying too heavily on detection are often too late to respond.

Such prevention techniques should be modernised to deal with new-age attacks. The need for capabilities around fileless malware and machine learning-based threat prevention is growing increasingly important and should be aligned with endpoint detection and response capabilities for a full prevention and detection strategy.

Modernising in this manner will aid organisations in preventing threats upfront and ensure you're not seen as an easy target.

Educating employees on phishing threats. Second, organisations shouldn't overlook the value of improving awareness and understanding of phishing among their employee base.

Today, threat actors view the human as the weakest link in the cybersecurity chain, and for good reason. The statistic stemming from IBM research that 95 percent of data breaches involve human error remains prevalent, making the individual a primary target for attackers.

When employees are left to their own devices, even the best technical efforts will fail. Therefore, any new security solutions need to be supplemented with an improved consciousness of the risks and implications associated with specific behaviours.

By far the most common way in which individuals are targeted is with phishing emails that are ultimately designed to infect an endpoint with malware to gain a foothold into their network. Education efforts should therefore centre around the detection of phishing emails with security awareness training, phishing simulations and behaviour change programmes.

If successful, these efforts will also bolster attack prevention, reducing the risk of employees inadvertently downloading a malicious email or attachment that spreads ransomware.

IBM RESEARCH REVEALS THAT 95 PERCENT OF DATA BREACHES INVOLVE HUMAN ERROR

Improving visibility. Thirdly, firms must focus on improving visibility of their networks in 2023.

It's vital for any organisation to regularly assess and reduce gaps and exposure in systems. Further, having clear oversight of your data and who has access to it is also crucial.

Without visibility, entities are operating blindly, putting themselves at much greater risk of being targeted by cyber criminals. By achieving holistic oversight of systems and vulnerabilities, organisations can better prevent threats in the first instance as well as detecting and responding to incidents quickly, before they can cause significant damage.

Further, greater transparency can also enable companies to track the effectiveness of their security measures and adjust them as needed to improve their overall security posture on a continuous basis.

The need to adapt in these various manners has never been more important. Keeping advanced cyber threats at bay is what many organisations aren't equipped to do. As the complexity of threats has increased, security teams have struggled to keep up, relying on legacy security controls that are ineffective at detecting and containing these dangers.

However, making the necessary adaptations to improve protection is unfortunately much easier said than done. A key reason why so many organisations continue to rely on ineffective solutions is because they lack the internal expertise or resources to orchestrate effective strategic improvements.

Enhancing visibility, education and prevention requires skills, technologies and mindsets that many simply don't have. Further, changing that typically requires investing in skilled staff and solutions that command high wages or fees – something that may not be realistic for many companies, particularly in the current economic climate.

So, what's the solution? How can organisations access market-leading expertise and solutions at speed, without breaking the bank? Here, Managed Security Service Providers (MSSP) and Managed Detection and Response (MDR) services can provide the answer. MSSPs are external providers that will supplement an organisation's

internal security team, offering market-leading solutions to provide services spanning detection, investigation, threat hunting, response and remediation. In other words, they can help companies to more quickly and effectively respond to incidents to minimise potential costs and impacts.

MORE PEOPLE ARE TURNING TO CYBER CRIME AS THE COST-OF-LIVING CRISIS TAKES HOLD

MDR services are also offered by external parties. Unlike MSSPs, these involve in-depth security monitoring and incident response supplemented with proactive security support. In this sense, MDR providers can work with you to undertake advanced threat testing to uncover hidden vulnerabilities and develop adequate defences and response plans.

The fact that both solutions are delivered by external providers is critical – it removes the need for organisations to invest in expensive and advanced expertise in-house through the provision of access to market-leading security support. In this sense, they can also help companies to bridge the cyber skills gaps in a cost-effective manner.

Here, we'll consider some of the core benefits of MSSPs and MDR solutions, starting with their ability to enable rapid incident response. When it comes to ransomware attacks, time is money. The more time between detection and containment, the more damage will likely be done.

MSSPs and MDRs can provide organisations with on-demand support from experienced security professionals to rapidly detect, analyse and contain security incidents, reducing the chance that ransomware attacks will materialise. This approach eases the load on the internal security teams, saving them hours that would have to be spent sifting through false positive alerts.

Secondly, external providers can help organisations to align with increasingly complex data privacy regulations and ensure that their security strategies are compliant. By providing complete visibility over the security of their environment through proactive reporting and auditing and remote support from 24/7/365 security professionals, MSSP and MDR solutions can help to maintain compliance posture.

MDR enables organisations to maintain their compliance posture by providing them with complete visibility over the security of their environment through proactive reporting and auditing, as well as remote support from 24/7/365 security professionals who can help prevent intruders from accessing sensitive data and also fill in general compliance gaps.

Thirdly, external support can be the difference in achieving continuous, dynamic security improvement. As threat actors continue to evolve their methods, static security strategies are becoming outdated and obsolete ever more quickly. To ensure that their customers' security strategies are moving in tandem, MDRs and MSSPs will use threat intelligence feeds to identify the types of exploits and attacks cyber criminals are using, and tweak and improve the security posture incrementally over time.

With the threat of ransomware expected to continue to grow over the course of the coming months, it is vital that organisations make the most of these resources and build effective, modern security strategies capable of defending against evolving threats. By working with a trusted and proven external security provider, they will be well placed to mitigate the most critical risks in their environments, and in turn stop ransomware attacks in their tracks ●

Patrick Wragg is Head of IR at Integrity360.

A cyber-attack that paralysed the Costa Rican government in May 2022 marked the first time a nation had declared a state of emergency in response