DigitalXRAID
CYBER SECURITY EXPERTS

RANSOMWARE

How to Stop the Spread of a Digital Pandemic

As COVID-19 swept the globe in 2020, organisations were simultaneously forced to confront a different type of pandemic. Corporate victims were struck out of the blue, with potentially devastating consequences for business owners. No organisation was safe.

Yet while mass vaccinations have now finally begun to slow the spread of the novel coronavirus in some countries, ransomware continues unabated.

Like the virus, ransomware will need more consistent tracking and tracing if we're to launch an effective response. Your most valuable digital assets will need to be quarantined. And Security Operations Centre (SOC) capabilities must be deployed en masse if organisations are to build-up an effective herd immunity.

Attacks increased by

151%

in the first six months of 2021

Have you profiled the threat, and do you understand the potential impact on your organisation?

Would you know how to manage and recover from a serious infection?

The story so far

Ransomware was around long before COVID-19. But despite the global disruption caused by WannaCry and NotPetya in 2017, these were relatively isolated events.

Ransomware today is arguably far more widespread and more dangerous. Attacks increased by 151% the first six months of 2021 alone, and the FBI has warned that there are now 100 different strains circulating around the world.

What can explain this spike in activity? A combination of factors. First, the rise of Ransomware-as-a-Service (RaaS) has effectively democratised the ability to launch these attacks. Today, countless affiliate groups effectively hire the use of a particular malware variant from its authors and then share the spoils of an attack. Access-as-a-service options on the cybercrime underground mean they even have a readymade selection of targets to aim for.

Second, organisations are failing to address deficiencies in their cybersecurity posture which are allowing the bad guys to thrive. The initial vector is most likely to be a phishing attack, an exploited vulnerability or an RDP endpoint hijacked because of weak or previously breached credentials. After gaining a foothold into networks, many use legitimate tools like Cobalt Strike and PSexec to move laterally without setting off any alarms.

Third, victim organisations keep on paying, despite pleas from the government not to. Quite rightly, it says that doing so does not guarantee a victim will get a working decryption key, or that stolen data is deleted. Instead, it only encourages copycat attacks and more affiliates to join in.

DigitalXRAID
CYBER SECURITY EXPERTS

A geopolitical response

Ransomware can strike from anywhere at any time, including via "trusted" third parties like Managed Service Providers (MSPs) and their software supply chains.

If organisations are breached, the focus must be on rapid threat detection and incident response. If they fail, their attackers may not simply encrypt key systems but are likely to also steal sensitive data and could even launch DDoS attacks to force a payment. The fallout isn't just the ransom cost itself, but downtime, IT overtime, lost productivity, customer churn, reputational damage, and potentially class action lawsuits in the event of a serious data breach.

Already we've seen serious attacks lead to fuel shortages and concerns over food supply chains in the US, school and university closures in the UK and hospital disruption in Europe and the US. It's no surprise that the White House has escalated its threat response to the same level as terror attacks. Washington says it will take unilateral action if Russia and other hostile nations don't take action to stop the criminal gangs operating with impunity from within their borders. The UK government has even been urged to consider banning ransom payments outright. Interpol has called for immediate cross-border action to stem the pandemic.

> "In the UK, ransomware has been described as the biggest online threat currently facing organisations and individuals."

Fighting back against ransomware

Just as COVID-19 is constantly evolving, so are the cyber-criminals. They have the advantage of surprise and the agility to respond and outwit defensive measures.

Yet there is hope. In reality, despite the existence of numerous variants and ransomware groups, threat actors have not changed their tactics, techniques and procedures (TTPs) much in recent years. This means that following a series of best practices outlined below should be an effective way of “vaccinating” your organisation against the impact of most attacks.

Let’s take a look at these countermeasures using the Five Functions of the NIST Cybersecurity Framework:

Identify

Visibility is the first pillar of effective defence. That means first understanding your risk appetite and tolerances before identifying and putting in place a comprehensive risk-based cybersecurity strategy for dealing with ransomware attacks. This should start with:

- Identifying where key hardware and software IT assets are located in the organisation and the wider supply chain
- Then it’s a case of understanding what the key threats are to these assets and where vulnerabilities are. **DigitalXRAID provides a continuous vulnerability monitoring service** as part of our SOC solution which will categorise the severity of any unpatched flaws and ensure all critical and high impact bugs are remediated as soon as possible

Protect

Next, it’s time to put in place the appropriate safeguards to limit and/or contain a ransomware attack:

- The first stop should be your employees. Turn them from a potential weak link in the security chain to a formidable first line of cyber-defence with security awareness training. Real-world simulation of phishing incidents works best, with lessons run in relatively short bursts but frequently. Our **HarpoonX** managed service offers customised simulations that could reduce the threat of phishing by up to 80%
- Data encryption and back-ups should come next. Scramble data to render it useless in the event it’s stolen by threat actors, and back-up regularly according to the **3-2-1 rule** so that it can be restored in the event of a serious compromise
- Set compliance standards for your supply chain partners. Put simply, there’s no point in applying best practice security to mitigate the risk of ransomware if your suppliers don’t, as attackers could compromise your networks via these third parties. Regular audits and clear standards are key
- Least privilege access and network separation. A lot of risk mitigation in cybersecurity boils down to reducing the attack surface and minimising the impact of a potential breach. In this way, ensure all accounts and endpoints, including remote desktop protocol (RDP), are protected with unique and strong passwords and multi-factor authentication (MFA). Enhance this further by applying the principle of least privilege, meaning users only get access to the resources they need to do their job and no more. Network segmentation will restrict attackers that do manage to penetrate your defences, preventing lateral movement and containing a compromise

Detect

Preventing a security breach is not always possible today, especially if attackers get hold of employee credentials. This makes rapid detection and response absolutely critical to minimise the impact of a ransomware attack. Focus on the following:

- Consistent penetration testing. This will allow you to understand where there are weaknesses in your security posture which attackers could exploit. **We run simulations** of genuine hacking techniques replicating insider threats, external attacks and attempted exploits of web applications. The results can help inform patch management strategies and changes to security policy
- Log monitoring and aggregation is the process of collecting data from across your IT environment and analysing it for suspicious behaviour which could indicate a compromise. DigitalXRAID analysts perform this resource-intensive and specialised activity using highly tuned SIEM software, to spot attacks early on in the kill chain
- 24/7/365 monitoring is essential for optimised detection of serious cyber-threats. We offer this from **an outsourced SOC**, providing not only SIEM and log management, but intrusion detection, proactive threat mining, dark web monitoring for indicators of compromise, file integrity monitoring and vulnerability management

Respond

Once you've detected threat actors in your environment, it's time for incident responders to take the helm. In this situation, we'd always urge victims not to pay their extorters. Instead, the focus should be on:

- Limiting the impact. This ties back to the detection piece. The sooner you know what's going on in your environment, the quicker you can spring into action to remediate
- Incident response plans should be comprehensive and thoroughly tested, with playbooks designed for the most common incident scenarios. **Our expert SOC team** will not only detect and analyse threats but respond to them in order to mitigate risk before attackers have had a chance to cause any damage. Working round-the-clock, every day of the year, means there's no downtime for attackers to target

Recover

Finally, it's time to restore any services or infrastructure that was impaired by in incident. This could encompass:

- Restoring from backups. If systems are backed up regularly, then the impact of any ransomware attack should be reduced
- Forensic analysis and disaster recovery processes, not only to understand which digital assets have been compromised, but also to analyse exactly where vulnerabilities were penetrated and how defence strategies can be bolstered to make sure it never occurs again
- Lessons learned—including what worked and what didn't from a team training perspective, and how staff can make better decisions next time around

With resources stretched to the limit by the pandemic, and a global shortage of cybersecurity talent, organisations are increasingly turning to expert third-party help. Providers like DigitalXRAID offer economies of scale, a wealth of in-house expertise, and the ability to spot threat trends across multiple customers, which enhances the service they're able to deliver. With an outsourced SOC at the centre of your cybersecurity strategy, it is possible to track and trace all threats and immunise your network to ensure complete protection. Knowing your business is secured 24/7/365 provides invaluable peace of mind, and your entire organisation will have the confidence to grow, free from the risk of the ransomware pandemic.

DigitalXRAID

CYBER SECURITY EXPERTS

Need the Best Defence Against Cyber Threats? Call us now on 0800 0903 734

Suite 9A Cavendish Court
South Parade, Doncaster
DN1 2DJ
UK

01302 639 470

32 Cubitt Street
London
WC1X 0LR
UK

0207 183 3795

12 Tithebarn Street
Liverpool
L2 2DT
UK

0151 329 0431

info@digitalxraid.com **digitalxraid.com**

ISO 27001 CERTIFIED British Assessment Bureau ISO 9001 CERTIFIED British Assessment Bureau CYBER ESSENTIALS PLUS IASME® Consortium CREST CHECK IT Health Check Service