Maple

maplenetworks.co.uk

What's your ransomware plan?

Ransomware attacks are not going away and for many, it's a matter of when, not if, a ransomware attack will happen. They are making headlines almost every day and causing more and more disruption to individuals as well as organisations. In a recent Sophos survey, 35% of UK organisations surveyed were targeted with ransomware in the past year. Therefore, it's important to understand some of the key attack techniques used, some of the common challenges faced when defending against ransomware and how your organisation can take steps to protect

The problem with ransomware

Ransomware can affect any organisation at any time and can cause multiple problems.

Attackers don't just use one point of entry when gaining initial access. Breaches are achieved via many different attack vectors such as unpatched VPN servers, Remote Desktop Protocol (RDP) access with weak or compromised user credentials aided by the rise of remote working, IoT systems, via email attachments or phishing links, and even zero-day exploits.

Once initial access has been achieved, the attacker moves to spread the malware internally. This is often done by leveraging active, insecure protocols within the environment. ExtraHop have recently conducted a survey that finds 67% of organisations still use the Server Message Block (SMB) v1 protocol, which is commonly used by threat actors to spread ransomware throughout a network. Notably, both WannaCry and NotPetya used SMB v1.

Once the malware is in place, and your data has been encrypted, extortion usually comes next. Threat actors are turning to double, and in some cases, triple extortion to increase their chances of the victim paying the ransom.

They are no longer just encrypting the data and hoping for the pay-out - they are now encrypting the data, demanding that the victim pay to decrypt their files, and, if the victim doesn't pay, then they threaten to leak the data.

But the financial demand isn't the only problem that needs immediate action. Severe operational disruption can happen very quickly, as demonstrated by the recent attacks on some national healthcare IT services. In some cases, their systems remained shut down for several days, impacting multiple activities, including X-rays and non-emergency surgery.

Be ransomware ready

There are several things you can do to improve your chances of preventing a ransomware attack. First and foremost, it's important to get the basics right. Keep patches up to date, apply remediation actions where patching is unavailable, such as in response to a zero-day, close down insecure protocols for more secure

alternatives and implement a cyber awareness program to educate users on phishing emails, the source of 94% of malware cases. While all of these can be time consuming and challenging for IT Teams to keep on top of, they are crucial in the fight against ransomware.

Secondly, having a thorough backup strategy is vital, and for several reasons. If you were subject to a successful attack, even if you might decide to pay the ransom, the Sophos survey reports the average amount of data returned is only 65% of the full amount, leaving a large hole if you don't have a backup available. In addition, even if you were lucky enough to get all of your data back, it could take weeks or even months to get up and running again properly. A good backup strategy would include a full recovery plan in the event of an incident that would provide a process and timeframe to get back to normal operations, even without data being returned.

Comprehensive protection

A comprehensive ransomware protection platform should make use of a variety of tools to prevent files being encrypted, such as signatures, which are used to block known malicious file types, and behaviour analytics, that can be applied to detect unknown, never seen before, file types and malicious user behaviour.

Maple offers this protection as part of our 'hardened' Security Operations Centre (SOC) offering, integrating a file-level ransomware detection and response suite into our hybrid security information and event management (SIEM) platform, providing a single pane of glass view. This integration enables us to correlate multiple log sources to rapidly determine the initial entry point and how the malware has spread throughout the organisation. This means we can rapidly increase the speed of our response and, importantly, reduce the Mean Time to Remediation (MTTR).

Supporting the foundations

We can also provide an automated AI Ops patching service to keep your critical IT infrastructure up to date on security and application patches to limit risk and reduce the attack surface – helping you get those basics right without the drain on time and resources.

And for complete peace of mind, we also offer a ransomware protected, immutable backup solution, also available as a service, so if the worst does occur, then files can be restored in an efficient and timely manner, keeping downtime and disruption to a minimum.

All-in-one service from Maple

We can offer ransomware protection, automated AI Ops patching, backup strategy, and more, through our 24/7, managed SOC service, which offers full visibility and the best protection against not only the encryption of files, but the detection of initial access and timely eradication of the threat.

Assess your protection and recovery

If you're concerned about your ability to protect your organisation against ransomware, or recover from an attack, we're offering a complimentary ransomware protection review. Get in touch today to book yours.

Book your complimentary ransomware protection review now

Maple

T: **020 3858 0048** | E: **info@maplenetworks.co.uk**

Maple Networks Limited - The Metal Box Factory, Great Guildford Street, Southwark, London, SE1 0HS