PICKING UP THE PIECES

Ed Williams *examines the correct procedure in the aftermath of a ransomware attack*

Ransomware is a nightmare for CISOs and security teams. It can topple an organisation and compromise its critical assets and systems in a matter of seconds. On average, it takes ransomware attacks only three seconds after execution to start encrypting critical files on a system or network and block organisational access. According to Microsoft, ransomware infections can take less than an hour to take over an entire system.

The fast and stealthy nature of this attack has made ransomware one of the most popular methods among cybercriminals. In 2021, almost 37 percent of all global organisations were victims of some form of ransomware attacks. There was an annual increase of 62 percent in such attacks last year, and the FBI reported receiving over 2,000 ransomware complaints in the first two quarters of 2021 alone.

What's more worrying is that more than half of the victim companies are paying ransoms, which is encouraging more cybercriminals to launch such attacks and target an organisation multiple times. For example, leading storage devices company QNAP Systems has already been targeted twice this year by the DeadBolt Ransomware group. So, there is evidently a gap in organisational response to such attacks, influencing criminals to carry on this vicious cycle. Even for the businesses that refuse to pay up, it's still a very costly operation to investigate and remediate such attacks. Not to mention that valuable time, resources, and assets are lost as a result. So, the big question that needs to be answered is, how can organisations develop a strong response mechanism to ransomware attacks and break the vicious cycle?

Before diving into the guidelines of ransomware response, it is important to know the type of ransomware groups that are currently most active across the industries. Although ransomware attacks can come from any threat actors, whether its novice attackers trying to test their skills or experienced cybercriminal gangs – some of the most active and known ransomware groups are Conti, REvil, Lapsus$ and DarkSide.

The focus immediately after an attack should be on digital forensics and incident response

The Lapsus$ group is currently dictating headlines, as this ransomware gang has attacked some of the biggest names in the tech industry within a short time span, including Microsoft, Nvidia, Samsung and Okta. In a very demonstrable case of taking advantage of the insider threat, Lapsus$ recruited employees to gain access to targeted organisations. Once in, the group's known methods for launching ransomware attacks are exploiting unpatched vulnerabilities on internal servers, deploying Redline password stealer, paying employees to leak credentials and purchasing session tokens and authenticator codes on the Dark Web.

While many ransomware groups like to remain in the shadows, Lapsus$ is a little less cautious about covering its tracks, indicating it is not only confident in its ability to not get caught but also maintains a permanent footprint. During this time all organisations, especially if a part of the digital supply chain, should remain hyper vigilant and carry out some of the basic cyber fundamentals, including proactive threat hunting, third-party vendor/supply chain assessments and conducting crisis simulations.

The first and immediate challenge in the aftermath of a ransomware attack is to get the business back on its feet and resume operations. However, this is where businesses make the first big mistake. Most immediate response plans focus on getting business operations back to the standard it was before the attack, without taking into account any long-term considerations. This leaves the business vulnerable to recurring attacks.

The focus immediately after an attack should be on digital forensics and incident response. The first action should be to track down the source of the attack, how it was initiated and how it gained access to the organisation's system or network. Identifying these aspects will help to close any existing security gaps by issuing the latest patches and ensuring there are adequate security measures in place.

Once the source and entry-point have been identified and the gaps have been closed, the next concern should be to find any hidden malware that is still inside the system. Most ransomware attacks are deployed using modular malware, such as Dridex, Emotet and Trickbot.

Modular malware is an advanced malicious software that attacks a system gradually in different stages, instead of trying to infect the entire system in one go. It starts with an initial payload and installs the essential components of the malicious software first to stay undetected. These malware stay hidden inside the system, disguised as normal attachments, files or browser extensions. This means attackers can trigger another infection at a later time.

Recurring attacks can be triggered even months after the initial strike if the malware is still present within the system. That's why it is critical for organisations to undertake an in-depth assessment of the entire system and network and identify any sophisticated and hidden malicious files. Automated scans can often miss advanced and well-disguised malware. A more proactive approach can be to employ threat hunters – security experts who can think like cybercriminals to identify attack paths, patterns and vulnerabilities. A combined approach of automated system scanning and threat hunting can help to quickly flush out the hidden malware from the internal systems.

It is also important that companies regularly carry out IT security audits, particularly in this era of hybrid working. It helps to whitelist applications and keep a comprehensive record of what 'normal' systems and applications look like. So, in the aftermath of a ransomware attack, security teams can easily compare the compromised system with its normal state to identify any unusual activity or vulnerabilities.

IT teams must also have visibility of all critical assets across the entire organisational network. It's imperative to have effective IAM solutions and frameworks in place, so security teams can constantly monitor and manage which user accounts have access to what applications and systems. This allows organisations to ensure that there are no over privileged or stale accounts within the network.

Once the security gaps of the initial attack have been plugged and the hidden infections have been eradicated, organisations should focus on mitigating the risks of any future attacks. With new threat groups emerging every day and millions of attacks being carried out every year, it is highly likely that an organisation will be targeted again by a different ransomware group or threat actors.

EVEN FOR THOSE THAT REFUSE TO PAY UP, IT'S STILL A COSTLY OPERATION TO INVESTIGATE ATTACKS

To start-off mitigation efforts, organisations should first understand how the attack unfolded. Every ransomware attack includes extensive planning and creating a sophisticated attack path. Executing the malware itself is the final step of the attack. Most attacks are carried out through phishing emails, breaching overprivileged access, exploiting ghost accounts or breaching weak remote access controls.

Disrupting any steps of the attack path can significantly slow down the adversary. Ransomware attacks thrive on fast execution so slowing down any steps takes the critical advantage away from the attackers and increases the chance of the attack being detected by security teams and automated solutions.

Ransomware attack paths can be disrupted by regularly patching the system vulnerabilities and updating security measures. A well-circulated and regular patching process can quickly detect and resolve software vulnerabilities before they can be exploited. A regular patching process can also assign risk-scores to system elements, identifying high-risk and low-risk applications.

The next measure is to implement strong security protocols and standards across the entire workforce. This means mandating a strong password process and implementing credential management solutions so that attackers cannot easily gain access to user accounts.

Organisations can significantly benefit from implementing multi-factor authentication for all users and incorporating highly secured authentication methods such as biometric log-in or third-party authenticators. It is also important to conduct

security awareness training from time to time. It helps to keep the employees aware of email-bound threats and social engineering-based attacks.

Also, every organisation should have an effective antivirus solution in place as an initial layer of defence. It's true that antivirus solutions cannot effectively detect sophisticated ransomware attacks, but they also help to detect and fend-off low-level attacks. Having a good antivirus in place can slow down ransomware attacks to some extent, although not significantly.

RANSOMWARE CAN TAKE LESS THAN AN HOUR TO TAKE OVER AN ENTIRE SYSTEM

Organisational networks should be configured in a way that doesn't allow ransomware to race through the entire system. Organisations should have an accurate understanding of what is on the network. When conducting penetration tests, we often find assets in the network that companies weren't aware of or that they thought had been disconnected. So, it's critical to know what assets are currently on the network, what should be there and what shouldn't.

Also, not every asset should be directly stored in the centralised system. For instance, if a company has all data stored on the central database, a single ransomware attack can compromise all critical data. Having assets stored in several different networks is a good way to cut off attack paths. For instance, if the central database is compromised, eliminating its connection to other distributed networks can save the entire system from getting breached. This approach helps to contain the attack in a limited area and restrict it from affecting the entire network. It also helps to quickly identify the source of the attack and provide faster threat response.

Security audits are critical to identifying the entire state of an organisational IT and security infrastructure. Cybersecurity is an evolving field and security tools and standards continuously need updates. So it is important to assess existing security infrastructure from time to time to ensure that all implemented solutions and measures are up to date.

Auditing helps to identify security vulnerabilities quickly and close down gaps before attackers can exploit them. It also helps to examine access privileges and ensure all users only have access to the systems relevant to their roles.

Following these steps and measures can help companies to mitigate the threats of ransomware attacks. Sophisticated and advanced attacks can still breach even the most secured defences, but implementing these mitigation measures can help organisations to reduce the damage and potentially avoid paying any ransom. It is important that organisations have a 'when, not if' perspective towards ransomware attacks, as it can help them to plan accordingly and bounce back quickly in the aftermath of an attack ●

Ed Williams is EMEA Director of SpiderLabs, Trustwave.

The Lapsus$ group has attacked some of the biggest names in the tech industry including Microsoft, Nvidia, Samsung and Okta