BEYOND SCATTERGUN: THE NEW FACE OF RANSOMWARE

Ransomware attacks are on the increase and the consequences are costly. Organisations must invest in multifaceted prevention measures to protect their data

The war on digital security is being fought on different fronts. Cyberattacks themselves are more common and the type and impact have changed. Viruses used to focus on system damage and data destruction, typically randomly infecting as many systems as possible. Now, ransomware attacks are more carefully considered to maximise the hackers' return.

CYBERCRIME IS BIG BUSINESS

So, while the complexity has increased, the potential profits driving each attack have also increased. Cybercriminals understand data is a company's biggest asset and denying access to that information can prevent it from functioning. The result is effectively data kidnapping, or ransomware.

Tools must constantly evolve to conduct ransomware attacks and criminals are more selective when choosing a target. The return may not meet the effort required to attack a "Mom-and-Pop" business, while enterprises have more to lose, so the potential for a big pay-out is real.

In 2019, ransomware was reported to have cost businesses $11.5 billion. A year later, that number was more than $20 billion[1]. Beyond the ransom itself, companies can expect to absorb costs in lost revenue, data, systems, and intellectual property; system restorations, re-establishment of operations; and reputational damage. The total cost of cybercrime could be more than $6 trillion annually by 2021[2].

Ransomware attacks are not "just" a business issue, but can easily become public emergencies affecting healthcare, communications, transport, and other critical infrastructure.

FOLLOW THE MONEY

But the top line masks the underlying shift in the profile of ransomware. Hackers are, very deliberately, taking aim at different ransomware targets. There seem to be two potential driving factors here. One is the potential financial return, and the other is around increasing the likelihood of attack success.

The United States and Europe have always been priority targets, but the scattergun approach hits everyone indiscriminately. This Sophos report[3] shows a marked shift to wealthier, more stable countries and those with poor cyber defences. Well-resourced countries are better prepared to combat ransomware and are therefore less likely to be targeted.

Their lower gross domestic product may have put South Africa, Poland, and the Philippines further down the list of organisations most recently hit by ransomware, with South Africa falling from a previous incidence rate of 54 per cent to 24 per cent in the most recent report. Public sector organisations are least likely to be targeted, with 45 per cent of respondents reporting an attack, however, this is only 6 per cent below the average of 51 per cent.

CONSEQUENCES AND THE COVID-19 EFFECT

No country or organisation can afford to be complacent. The threat is real, as the WannaCry ransomware attack on the United Kingdom's National Health Service (NHS) in 2017 proved. The government had to make up £19 million in lost output and £73 million in IT costs.

The DarkSide ransomware gang attack on the United States' Colonial Pipeline in May of 2021 shut down one of the East Coast's main oil supply lines, affecting multiple states for five days. Many garages ran out of fuel, sparking panic buying and triggering a state of emergency in several locations. News outlets report that the company paid $5 million in bitcoin to the hackers.

Both examples prove that ransomware attacks are not "just" a business issue, but can easily become public emergencies affecting healthcare, communications, transport, and other critical infrastructure. Despite increased protection, the attack froze the core operations of Colonial Pipeline. The initial, but unproven, belief is that hackers gained access through phishing emails and the personal equipment of home workers. The pandemic has created new hacking opportunities as workers access systems through less secure methods.

While electronic defenses will prevent many problems, the major attack route remains employee behaviour with 45 per cent of organisations reporting ransomware accessed their system either as a file download or via email.

RANSOMWARE RECOMMENDATIONS

Ransomware attack prevention is multifaceted; each element must be thorough and maintained. The first step is to ensure that systems and software are updated with the latest versions and all security patches are applied. The WannaCry worm exploited a Windows vulnerability for which a patch had already been issued, but not applied by many organisations.

Updated systems need defending by antivirus and anti-phishing software. Again, these must be updated regularly to keep up with constantly evolving hacker efforts to find and exploit new vulnerabilities. Deploying analysis software to monitor systems, data, and networks for unusual behaviour can indicate that an attack is in progress and then attempt to stop it.

While electronic defences will prevent many problems, the major attack route remains employee behaviour with 45 per cent of organisations reporting ransomware accessed their system either as a file download or via email, according to the Sophos report. Educating the workforce will reduce the incidence of ransomware ingress by increasing and maintaining awareness.

Ultimately, it is wise to assume an attack will occur, and organisations will be compromised. A robust backup process is needed. Hiding data in the cloud does not make it safe from attack and subsequent encryption, as almost six in 10 ransomware attacks encrypted data in the public cloud, the report reveals.

Micro Focus Data Protector is a comprehensive backup solution that supports the 3-2-1 rule for backup. The rule requires **three** backup copies of the data to be made and held on at least **two** different media types such as tape, disk, cloud, virtual, or physical, with at least **one** copy held in an off-site location, detached from the network. A comprehensive and integrated management and reporting capability ensures backups are completing on schedule and within their service level agreements.

A single backup software tool, protecting all data is the simplest and most cost-effective solution. It will back up everything from lower importance data on older servers to mission-critical applications and data running on the latest storage infrastructure or virtual machines. Being able to direct backup to different locations and media types, and move them when required, offers the best protection. Regularly testing restore operations will ensure quick and efficient data restoration should the worst happen.

Reverting to backups following an attack is not ideal. It takes time and causes disruption but is far less costly in money and resources than paying a ransom, hoping the data is unencrypted, and then rebuilding the systems to get them operational again. It is a lesson business would do well to not learn the hard way.

Footnotes

[1] Coveware 2020 Ransomware Marketplace Report
www.coveware.com/blog/q2-2020-ransomware-marketplace-report#1

[2] Cybersecurity Ventures: 2019 Official Annual Cybercrime Report
www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf

[3] Sophos: The State of Ransomware 2020
www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-ofransomware-2020-wp.pdf

For more information:
www.microfocus.com
www.microfocus.com/dataprotector