Octal0g1k
ANSWERING YOUR CYBER CHALLENGES

Ransomware: the new cyber organized crime syndicate

Ransomware attacks globally surged in the first half of 2021, with 304.7 million, surpassing 2020's full- year total (304.6 million), says a new report. The ransomware showed massive year-to-date spikes in the US (185 per cent) and the UK (144 per cent). The top five regions most impacted by ransomware in the first half of 2021 were the US, the UK, Germany, South Africa and Brazil. The spikes in ransomware have been seen most likely in sectors such as government, education, healthcare and retail organizations. For example, in June 2021, meat producer JBS, which supplies over a fifth of all the beef in the US, paid a £7.8m ransom to regain access to its computer systems.

The same month, the US's largest national fuel pipeline, Colonial Pipeline, paid £3.1m to ransomware hackers after they locked the company's systems, causing days of fuel shortages and paralyzing the east coast. This showcases that effective and complex these ransomware attacks really have been.

The year 2020 had been badly hit by COVID19 and had made the use of cyberspace more open and prevalent as more and more organizations started to provide the work from home option.

The fear and anxiety had grown multifold with businesses as there has been a huge rise in the two – fold risk – health risk and cyber risk. Cyber criminals took advantage of this anxiety and continued to accelerate against innocent people and vulnerable organizations. Ransomware business started to boom.

So, what is Ransomware? Ransomware is a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. In simple terms, the cyber criminals that hack into internet-connected computer systems, lock access to them, and then sell a decryption key in exchange for payment in bitcoin. In recent years, ransomware incidents have become increasingly prevalent among the Nation's state, local, tribal, and territorial (SLTT) government entities and critical infrastructure organizations.

The primary purpose of ransomware primary purpose is typically financial gain. No matter what a victim chooses to do, once they receive the ransom note, the cybercriminal has the opportunity to make money in some way. If the ransom is paid, they get money without having to do any more work. If they aren't paid, most strains of ransomware enable attackers to steal the data they are holding hostage. From there, they can sell the data, and make their money that way.

Ransomware is also used as a decoy. The power of ransomware as a tool for distraction is unique. A large number of targeted attack groups began adopting these methods of using ransomware as a tool to get IT and security teams chasing potential infections, allowing them to infiltrate the network and get what they are truly seeking. This approach causes considerable damage, as it causes so much confusion among victims and often delays effective responses. While attackers are entering the system in another area, IT response teams are preoccupied trying to recover from the initial ransomware attack—performing backup activities, shutting down offending systems, identifying internal ransomware procedures, and determining if they should pay the ransom.

Ransomware incidents can severely impact business processes and leave organizations without the data they need to operate and deliver mission-critical services. Malicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen customer or high-value data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion. The monetary value of ransom demands has also increased, with some demands exceeding US $1 million.

Ransomware can be deployed in several ways. According to the 2020 Malware Report, 83% of security professionals consider phishing emails to be the most dangerous attack vector. In fact, according to the Verizon Data Breach Investigations Report, 94% of malware deliveries

are completed through a phishing email of some type. Other potential entry points are email attachments, users visiting malicious or compromised websites, and exploit kits.

Ransomware incidents have become more destructive and impactful in nature and scope. Malicious actors engage in lateral movement to target critical data and propagate ransomware across entire networks. These actors also increasingly use tactics, such as deleting system backups, that make restoration and recovery more difficult or infeasible for impacted organizations. The economic and reputational impacts of ransomware incidents, throughout the initial disruption and, at times, extended recovery, have also proven challenging for organizations large and small.

There are two types of Ransomware:

1.Encrypting ransomware (crypto-ransomware) converts files into cipher text, rendering them unreadable. Attackers will deliver a decryption key upon payment, and threaten to delete the encryption key if the ransom goes unpaid, which effectively destroys the data by making it unusable. 2.Non-encrypting ransomware uses lock screens that take up the entire screen and display a ransom note in some form. These strains are often less successful, since once the lock screen is removed, which is possible to achieve without paying the threat actors, the files remain unaltered.

With remote working still widespread, businesses continue to be highly exposed to risk, and criminals are acutely aware of uncertainty across the cyber landscape. It is becoming highly recommended that organizations start to move toward a modern Boundless Cybersecurity approach to protect against both known and unknown threats, particularly when everyone is more remote, more mobile and less secure than ever. All organizations are vulnerable, although a sweet spot is mid-size businesses that have enough revenue but aren't large enough to have dedicated cybersecurity teams make them a lucrative target for cyber criminals.

The best way to be prepared for a ransomware is to create, maintain and exercise an incident response plan and an associated communications plan that includes response and notification procedures for a ransomware incident. The Ransomware Response Checklist, as part of the Ransomware Guide, serves as an adaptable, ransomware specific annex to organizational cyber incident response or disruption plans.

It is also recommended to Conduct regular vulnerability scanning to identify and address vulnerabilities, especially those on internet-facing devices, to limit the attack surface. For example the Cybersecurity and Infrastructure Security Agency (CISA) of the United States offers a no-cost Vulnerability Scanning service and other no-cost assessments. In addition, prioritizing timely patching of internet-facing servers—as well as software processing internet data, such as web browsers, browser plugins, and document readers —for known vulnerabilities helps minimize ransomware attacks.

Mutation of ransomware attacks shall continue and for each and every sector, it shall take-up a different form with new incidents being reported on a monthly basis. The best way for businesses to stop ransomware attacks is to be proactive in their security approach and ensure that one has strong protections in place before ransomware can infect one's systems, for example a strong, reputable endpoint antivirus security is a good start to prevent ransomware originating out of phishing emails.

In conclusion ransomware attacks, has proved that in the 'new normal' their impact can be devastating to small business owners and organization who have limited resources and means to invent is in-depth cybersecurity solutions. It should also be stated that ransomware is not only threats to small business and organization, but it has an impact on people as well. It's always good to keep monitoring ones IT systems for potential breaches and inculcate good practices and cyber services

which either minimize the ransomware attacks or reduces the damage induced by such an attack. As a policy, it is advised not to pay for ransomware; but this is easier said then done.

Best practices:

- Develop a clear, actionable framework for ransomware mitigation, response, and recovery;
- Update cyber hygiene regulations and standards;
- Perform and verify the effectiveness of protective measures that include network, personnel activity, malicious code, external service provider activity, connections, devices, and software;
- Employ backup systems to restore data if attacked. Backup systems should not be attached or connected to the main network;
- Use multi-factor authentication and be careful when opening email attachments or clicking on embedded links.
- Consider the implementation of real-time DDoS protection.
- Deploy a complex threat management strategy combined with vulnerability and risk mitigation processes.
- When contemplating ransomware worst-case scenarios, disaster recovery planning and business continuity must be positioned as important considerations.
- Organizations must choose not to make the required payments but instead focus on remediating the ransomware attack.