VIEW POINT

KNOW YOUR ENEMY: CYBER-ATTACKS THAT ARE STEALTHILY EDGING IN

Infosys®
Navigate your next

Cyber-attackers are almost pompous about their criminal activities and often claim responsibility with grandeur and pride. They obviously never share their methods and stratagem, but their actions prove that they are sophisticated and well-aware individuals or groups. Their acts usually result in devastating consequences for businesses across the globe. They infiltrate networks stealthily, exploit vulnerabilities, hijack computer systems for either monetary gains, to accentuate political or social agendas, for power, revenge, or publicity. In recent times, cyber-attacks are also state sponsored - which implies that a cybercrime could be as dangerous as a war. A well planned and executed attack could result in the shutting down of towns, cities, ruining people's lives or having economic breakdowns.

Since the past one year, we have been hit by this deadly pandemic – COVID 19. This novel virus has forced people to maintain social distance, stay indoors and lie low. In a way it had the power to compel the globe to standstill had it not been for advanced technologies and strategies. Remote working has become the new normal for industries and businesses to function. Cyber criminals have made most of this situation by increasing their criminal activities. This article examines in detail some of the deadly cyberattacks that have been edging in or have strengthened over the past few months due to unavoidable alterations across the globe.

Apart from the known lethal cyber-attacks like Phishing, Ransomware, Insider Threats and Web Attacks, the world also experienced the following attacks edging in slowly over the past one year.

Supply chain attacks

These attacks got a new paradigm after the recent Solarwinds attack, also touted as "Attack of the century". While there are several details around how it was orchestrated, the key aspect of this attack was that it used "Trusted software" and "good security practice of updated patching" as its core. Leveraging a compromised software application that is widely used, the attackers (expected to be nation state) used sophisticated techniques to carry out espionage, access the IP and confidential information.

Cryptojacking

Cryptojacking is a type of cyber-attack wherein cyber-criminals hack computers, systems, mobile devices to use them for cryptocurrency mining and stealing of crypto wallets. This is done by either getting the victim to click on a link that is malicious or by infecting a website that is usually used by the unsuspecting victim. Once victims engage with these links, the cryptomining code is loaded onto their computers and from there on run in the background without disrupting any functionalities. The only way a victim may notice something is off is when the performance and execution of the system becomes very slow

AI-powered Attacks

Although AI is an advanced and cutting-edge technology that is used to ensure robust cybersecurity solutions, it is turning out to be a double-edged sword as cyber-criminals too are resorting to it to attack systems and carry out malicious activities. It has the power to automate invasion methods and launch fast paced attacks. AI can be instrumental in deciphering various interaction patterns of the victim and then launch custom phishing attacks. It can also be used to gather insights and understand the technology environment of an organization, its patched vulnerabilities and the complete SDLC. Moreover, AI-powered malware could travel easily through an organization by using ML that could probe internal systems without being detected until it causes severe damage in an organization.

Whale Phishing attacks

Whale phishing attack is a type of attack that targets high profile employees managing sensitive functions by communicating with them as senior employees or C-level employees. These communications appear to be articulated in a manner wherein the reader would be tricked into feeling it has been sent by seniors of the organization requesting for sensitive information. C-level executives such as CEO, COO, CIO, CFO are also targets for cyber-attackers, and they choose them after intense profiling. These people are specifically victimized and made targets only to steal confidential information about an organization. Sometimes, attackers also try and manipulate their victims into unknowingly authorizing high value money transfers, providing approvals or access to sensitive data, and computer systems for conducting criminal activities.

Denial-of-service

Denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is the act of making servers, services, devices, networks, applications, unavailable to its users. The motive to carry out such criminal act usually trickles down to extortion. In this type of cyber-crime, the attackers interrupt or suspend services of hosts connected to the internet. In an increasingly digitized environment, wherein technologies have enabled various functions of organizations to be connected, such attacks result in major downtimes and disruptions resulting in disastrous repercussions. In the wake of the pandemic, the healthcare, education and financial industries have been badly hit among others by this attack wherein cyber-criminals deny services or make it impossible for a service to be delivered at random times rendering stakeholders anxious and clueless.

Recommendations

Cybersecurity is gradually becoming a business imperative with organizations across the globe recognizing its importance and wanting to implement it at every stage. Following are quick 7 recommendations you may want to consider to secure your businesses robustly.

1. Security awareness is a MUST. This should be run as a communication campaign in the Enterprise.
2. Security-first culture should be cultivated in the workplace
3. Enterprises need to follow basic IT Hygiene around patching and vulnerability management
4. Table-top exercise with CXO and Board should be done periodically and a detailed "Incident Response action plan" needs to created and signed off by the CEO
5. A well-thought out, designed and occasionally tested cyber resilience plan should be in place
6. Defense in Depth should be practiced with multiple technologies that have layers of control
7. It's imperative for the CISO organization to create "Frictionless Security" that balances control with user experience and agility

About the author

Mayank Agarwal

Head North America, Infosys CyberSecurity

Mayank Agarwal has been associated with Infosys for more than 15 years. In his current role, Mayank manages CyberSecurity business in North America. In his role, he is responsible for customer engagements, sales, analyst engagement, GTM partnerships with tech partners and start-ups in North America. He is proficient in building strategic plan for cybersecurity, managing strategic relationship with CIO, CISO's, Head of Cloud and Infrastructure etc. Mayank is an accomplished and astute professional with the prefect mix of sales acumen and technology expertise.

For more information, contact askus@infosys.com

Infosys®
Navigate your next