Latest Trends in Malware Attacks

Kaukab Jamal Zuberi
Chief Editor

Increased in cyber attacks on government infrastructure calls for an immediate effort on increasing end user awareness about the potential techniques used in latest malware attacks.

Some of the malware attack trends to watch out for in 2022 are described as follows:

Use of Artificial Intelligence in Hacking:
Artificial Intelligence is a double edged sword which can be used by hackers as a weapon to design advance attacks on complex networks. White hat hackers have successfully demonstrated real-world attacks against AI-powered autonomous driving systems such as those used by Tesla cars. Researchers from Chinese e-commerce giant Tencent managed to get the car's autopilot feature to switch lanes into oncoming traffic using inconspicuous stickers on the roadway. Even without gaining the access hackers can poison data and sabotage the algorithms. "There hasn't been enough policymaker attention on the risks of AI being hacked," says Andrew Lohn, a senior fellow at the Center for Security and Emerging Technology—or CSET—a nonpartisan think tank attached to Georgetown University's Walsh School of Foreign Service. "There are people pushing for adoption of AI without fully understanding the risks that they are going to have to accept along the way.

Mobile is the new target
Cyber security trends show an increased attacks on the handheld devices. Increase in usage of mobile banking through handheld devices, reliance of various communication applications to communicate and storage of private information on the mobile device has resulted in making handheld devices a lucrative target for malware developers. Smart phones malwares will be a big challenge in 2022 for cyber security professionals.

Clouds are Vulnerable
As more organizations are moving their data to clouds, their security has become a big concern for cyber security professionals. Security measures should be taken to continuously monitor and update the software to prevent data leakages or sabotage.

Data is the prime target for hackers
Data breaches are expected to increase specially in developing countries where the quality of the software and hardware are obsolete. Safe guarding the data is prime responsibility of the cyber security teams. There is an urgent need for analyzing the existing infrastructure and take measures to close the security gaps found in this process of analyzing infrastructure. There has been several data breaches during last nine months in Pakistan. The data of very important government organizations and banks was breached, hacked, and placed on dark web.

The process of Automation and Integration
As the data grows in size and the demand for efficient and automated operations increase every day. Modern day hectic schedules pressurize professionals and engineers to deliver quick and proficient solutions. Large and complex web applications are further hard to safeguard making automation as well as cyber security to be a key concept of the software development process.

Targeted Ransomware
Critical infrastructure of organizations is being targeted with customized ransomware written for those organizations. These attacks will grow in 2022. In Pakistan, the number of such attacks have grown significantly, some of them were reported and others were kept secret by the organizations. These attacks can leak the information on dark web or encrypted critical data. Organization should develop effective Disaster Recovery Infrastructure and take steps to safeguard the critical data of the organization.

State-Sponsored Cyber Warfare
Cyber space was declared as fifth domain of war in the year 2010 by US government. Since then, state sponsored cyber warfare continues to take place discreetly and effectively. These attacks are planned and are conducted by expert operators. These attackers have all the resources available, which are required to achieve their targets.

Often, these operators collaborate with the

employees of the target organizations by giving them material favors. The attacks which are supported by internal employees are hard to detect and investigate.

Measures should be taken in the critical infrastructure to have security checks on the important members of the information technology team. Periodical credit checks and background checks should be made and the management should very carefully watch the red flags in the spending patterns of these employees. In 2022, we will have redesign the cyber security policy and change the carelessness observed by the decision makers of the critical infrastructure in Pakistan. In 2022 following trends are picking up pace in global cyber security practices:

User Awareness:
As the cyber security threats have become more aggressive the organization are working to increase user awareness through seminars and trainings. What drives cybersecurity awareness forward is the growing number of people unaware of most cyberattack methods. A report by Infosec indicates that about 97% of the people in the world cannot identify a phishing email, while 1 in 25 people click such emails, thus, falling prey to cyberattacks (Infosec). Aside from this, cybercriminals now resort to more advanced and high-tech forms of phishing and malware infections. Cyber awareness among end users can prevent cyber attempts to attack the infrastructure. Organizations need to take immediate steps to create cyber awareness among employees.

Zero Trust
The zero trust model restricts network access to only those who need it. Access is granted to authorized users using patterns based on identity, time, and device based on contextual awareness, and default access is eliminated. Everything must now pass security protocols such as access control steps and user identity verification.

Security as Service
More and more companies are moving towards Managed Security Service Providers (MSSP) to ensure the cost efficient and timely availability of sisecurity solutions for the organizations. This trend is increasing and have its pros and cons.

Machine Learning:
Role of Machine Learning is growing in the field of Cyber Security. Machine Learning enables cyber security systems to analyze the threat patterns and learn the behavior of the cyber criminals. This prevents the organizations from future attacks.

GDPR Compliance
he general data protection regulation is one of the most important tools of the European Union in managing data privacy. In fact, it is extrapolated not only for inhabitants in any member state but for all companies marketing goods or services to EU residents. Therefore, the GDPR has a significant impact on global data protection requirements.

It imposes a uniform and consistent data security law, eliminating the need for each state to write its own law on personal data, which further protects consumers.

Distributed Decisions:
In the face of a potential cyberattack scenario, business cybersecurity needs, and expectations are maturing and shifting towards a more agile security model. Therefore, the scope, scale, and complexity of digital business require that cybersecurity decisions, responsibility, and accountability be distributed across organizational units, departing from a centralized function.

Therefore, the role of the CISO (Chief Information Security Officer) has shifted from that of a technical subject matter expert to that of an executive risk manager. But, as we said above, a single centralized cybersecurity function is not agile enough to meet today's business needs. CISOs must reconceptualize their roles to empower business leaders, making it easier to make their own informed risk decisions.

No one knows the future of cyber security. New risks are emerging every day. Some organizations are still trying to figure out the means and ways to secure their data, Pakistan is way behind in cyber security and intensity of the recent cyber attacks call for an immediate action to come up with a comprehensive strategy to safeguard our critical infrastructure from potential cyber attacks which may cause significant damage.