BIZCOMMUNITY

Many faces of malware: Are you protected?

By John Mc Loughlin

2 Mar 2021

Malware remains the biggest threat to corporate networks, more costly than any other threat including ransomware and trojans. A research study conducted by Deep Instinct reports on the hundreds of millions of attempted cyberattacks that occurred every day throughout 2020 showing malware increased by 358% overall.

© Igor Stevanovic – 123RF.com

Emotet - enemy #1

Emotet maintained its number one position in the Global Threat Index, highlighting the global impact of this malware. The highly destructive banking trojan remains the top malware as it has already impacted 6% of organisations globally.

This malicious spam campaign uses various delivery techniques to spread the malware, this includes phishing emails, embedded links, attachments and password protected zip files.

Emotet also collaborates with other campaigns where cybercriminals used it to drop ransomware and spyware onto systems that were already infected by this malware. Its worm-like capabilities enable it to spread to other devices within the same network.

Regardless of how it is spread, Emotet is persistent and avoids detection. This means victims are unaware that they have been compromised until it's too late.

Emotet is one of the most costly and destructive malware variants. It's critical for corporates to be aware of this threat; they need robust security systems to prevent data breaches. More importantly, employees need comprehensive training so they are able to identify and react to Emotet.

Other threats

Trickbot is another banking trojan that is used in various cyber-intrusion campaigns. Similar to Emotet, it is often installed on computers to provide a gateway to install ransomware. The third biggest malware is Formbook, a credential-harvesting trojan that is used by cyber-criminals to steal information like usernames and passwords.

Other malware includes Phorpiex, Hiddad Android malware, Dridex trojan and XMRig cryptocurrency mining malware. Phorpiex is a botnet known for distributing other malware families via spam campaigns as well as fuelling large scale sextortion campaigns.

App malware

Hiddad is an Android malware which repackages legitimate apps and then releases them to a third-party store. Its main function is to display ads, but it can also gain access to key security details built into the OS.

xHelper is a malicious application that is used for downloading other malicious apps and display advertisement. The application is capable of hiding itself from the user and reinstall itself in case it was uninstalled.

Security

To help prevent becoming a victim to malware attacks, businesses must ensure that they have a comprehensive cyber resilience program in place. This program will ensure a layered defence and provides visibility across the full environment, no matter where their users are.

It must incorporate all aspects of their operations including email, data, applications, internet and the people who are accessing these. The program will ensure that all software is up to date, users are well trained and anomalies can be rapidly detected and threats remediated.

One cannot manage what you cannot see. You cannot keep defending the same way and expecting different results. The threats and cyber criminals have evolved, so should your security.

ABOUT JOHN MC LOUGHLIN

John Mc Loughlin is a visionary entrepreneur that has been involved in the setup and management of a number of start-up businesses. For the past seven years, he has been working towards changing the security landscape for SMEs in South Africa through his company, J2 Software, which provides solutions around reducing risk and improving compliance. John is an industry specialist and thought leader in the security space, and his particular areas of expertise lie in planning and strategising.

- #BizTrends2023: Continued explosion of cyberattacks - 13 Jan 2023
- Many faces of malware: Are you protected? - 2 Mar 2021
- Data breaches becoming more common - 16 Oct 2020
- I've been hacked! What do I do? - 21 Feb 2020
- The complex and challenging world of cyber risks - 11 Dec 2019

View my profile and articles...