CYBER ATTACKERS PREFER STEALTH

BY JAY BORDEN

Cyberattackers are relentless in their attacks and very clever. They prefer stealth mode, that is, attacking silently and remaining hidden until they are ready to spring. The amount of time compromises remain hidden is called dwell time. During this period, they may steal information such as user credentials, private information of employees and customers, or download and install more malware or ransomware, or spread to other systems within the organization. With all the third-parties that companies connect to, attackers may leverage those connections to spread to other organizations.

In the view of many, defenders have the more difficult position. They do their best and protect against many things. But they must be successful all the time. Not just in foiling known attack methods but also finding new ways to attack and creating protections. Attackers only have to be successful once. Attackers can also see what defenders know by examining their tools or trying different attack methods until they find one that works.

Attackers have gotten good at hiding their tracks. Once they are in, they may delete what got them in. This makes it harder for defenders to determine how they got it and the variety of malware left on the system.

One way cyberattackers succeed is by compromising a software vendor. SolarWinds is a good example of this. The attackers embedded malware in a SolarWinds software update. When customers installed the update, the malware was also installed.

Another method is by advertising free copies of legitimate software. Of course, the free copy is illegal. It will have malware installed and anyone who wants to avoid paying for the real package gets the malware. The illegal copy of the package may work or not, but the malware will work.

CYBER ATTACKERS PREFER STEALTH

CONTINUED

Phishing emails are one of the most successful methods. Clicking a link that leads to a fake site or downloads malware is often not caught by protective software. AI is helping make the phishing emails more believable.

The attackers are so thorough that their malware may look for antimalware packages on the compromised system before executing. If something is found that may interfere with their infection, it doesn't connect to its Command and Control Server, C2, and remains idle. By not connecting it is harder for tools and defenders to find and track or remove it.

Another method used is to create a number of application programming calls. Individually, they don't seem to do anything. But each one contains text from something. The exact material isn't important. What is important is that each one is different making it difficult to detect patterns or recognize known malware. When combined they do create a program or other material that does do something malicious.

All of these methods obscure the malware and make it difficult to detect.

When successful both methods typically create a backdoor into the system and are written directly to memory rather than onto the disk where it will be scanned by antimalware packages. Backdoors allow access by attackers even if passwords are changed. They may also work to steal session cookies. These will continue to allow access even if passwords are changed.

These methods elude most antimalware packages and also make forensics and analysis difficult.

Defending against attacks isn't easy. The old adage an ounce of prevention is worth a pound of cure is applicable here. Teaching users to not click suspicious links or not follow instructions in emails or from phone calls is helpful. Always check first using contact information you know. Never using contact information in the email or phone call.

With people responsible for 80% of breaches, it is imperative that users are kept up to date on attacks and know what to do. Despite best efforts breaches occur.

What is important is how long the attackers are in your systems before being discovered and evicted.

NOT REALLY TECH SUPPORT

CONTINUED

One of the best ways to stay safer is to get early warning of when malware has been installed or your information has been compromised, stolen and is for sale on the Dark Web.

That is why OneBrightlyCyber alerts you to compromised credentials and malware infected devices 12-18 months before other vendors and before they typically become a problem. That way you can change passwords and remediate the malware before it results in stolen information or more problems like ransomware.

Welcome to peace of mind.

To learn all the ways we can help make your company and family safer, visit onebrightlycyber.com, contact OneBrightlyCyber at info@onebrightlycyber.com, or call (888) 773-1920.