Botnets are making a comeback

PARTNER UPDATE – August 4th, 2020

Dear reader,

I wanted to take a moment to remind people that some of the most aggressive cyber-attack methods are through self-propagating botnets. These typically fly in invisible through normal methods such as infected links, downloads or attachments, and other more aggressive approaches. With improper or ineffective defenses, these can be quietly deployed. Once deployed, they sit idle while quietly gathering information to harm you, your finances, and/or encrypting your data for ransom.

According to SANS.org and other security watchdogs, Botnets are on the rise again. New botnets are popping up with the latest approaches, such as using a multi-modular approach with multiple ways to spread their payloads. These methods could be simple SMB, psexec, WMI, or others like IPC$. The botnets appear to be using crypto-mining pools to spread themselves and use multiple methods to steal passwords with tools such as the Prometei or launch broader campaigns. Then they attack with other payloads from the C2 systems (in some cases) to run banking theft, ransomware, and other attacks.

We have seen similar attacks and have successfully prepared our clients to protect against botnets. We want the opportunity to help you confirm you are not at risk from these attacks. We are offering to do a free 1-hour review with your CISO or cybersecurity contact to discuss botnets, other new threats, and your cybersecurity readiness to defeat them. If nothing else, it is a good "sanity check" to go through for the security of your organization.

Please contact us by phone or chat online for a free 1-hour review.

Keep IT Simple, and Keep IT Safe.

Craig

Craig Miller
Director of Infrastructure & Security Practices
KIS - Keep IT Simple | Professional IT Solutions Experts Since 1988
E: miller@kiscc.com
O: (510) 403-7500