Published by KnowBe4
CYBERHEISTNEWS
arming you with the facts

Scam of The Week: New Fileless, Code-Injecting Ransomware Bypasses Antivirus

Security researchers have discovered a new fileless ransomware in the wild, which injects malicious code into a legitimate system process on a targeted system and then self-destructs itself to evade detection by antivirus.

It has been called SOREBRECT and unlike more generic "spray-and-pray" ransomware, it has been designed to specifically target enterprise systems in various industries.

SOREBRECT also takes pains to delete the infected system's event logs and other artifacts that can provide forensic information such as files executed on the system, including their timestamps. These deletions deter analysis and prevent SOREBRECT's activities from being traced.

This malicious code, after it has taken control of the machine, uses Microsoft's Sysinternals PsExec command-line utility to encrypt files.

Why PsExec?

"PsExec can enable attackers to run remotely executed commands, instead of providing and using an entire interactive login session, or manually transferring the malware into a remote machine, like in RDPs," Trend Micro says.

SOREBRECT Also Encrypts Network Shares

SOREBRECT also scans the local network for other connected computers with open shares and locks files available on them as well. "If the share has been set up such that anyone connected to it has read-and-write access to it, the share will also be encrypted," researchers say.

In addition, SOREBRECT uses the Tor network protocol attempting to anonymize its communication with its command-and-control (C&C) server, just like almost every other malware.

What to Do About It

- Restrict user write permissions
- Back up files

- Keep the system and network updated
- Deploy multi-layered security mechanisms
- Foster a cybersecurity-aware workforce.

Trend Micro advised: "User education and awareness helps improve everyone’s security posture. Like other malware, ransomware’s points of entry is typically through email and malicious downloads or domains. Organizations should conduct regular training to ensure that employees have a solid understanding of company security policy, procedure, and best practices."

We could not agree more. GroupEleven offers Cyber Security Training for our clients. If you would like more information, email support@groupeleven.com.

GroupEleven