EternalBlue Exploit Used in Retefe Banking Trojan Campaign

By Tom Spring

Published: 2017-09-22 · Archived: 2026-04-06 00:18:22 UTC

Banking Trojan Retefe is adopting new WannaCry tricks, adding an EternalBlue module to propagate the malware.

Criminals behind the Retefe banking Trojan have added a new component to their malware that uses the NSA exploit EternalBlue.

The update makes Retefe the latest malware family to adopt the SMBv1 attack against a patched Windows vulnerability, and could signal an emerging trend, said researchers at Proofpoint. Earlier this year, researchers at Flashpoint observed the TrickBot banking Trojan had added an EternalBlue module as well.

While Retefe has never reached the scale or reputation of similar Trojans such as Dridex or Zeus, it is notable for its interesting implementations and consistent regional focus in Austria, Sweden, Switzerland, Japan and more recently the United Kingdom, researchers said.

“Unlike Dridex or other banking Trojans that rely on webinjects to hijack online banking sessions, Retefe operates by routing traffic to and from the targeted banks through various proxy servers, often hosted on the TOR network,” said Proofpoint in a technical post Thursday explaining its research.

Over the past several months, researchers have observed a wave of new Retefe campaigns consisting of unsolicited emails containing malicious Microsoft Office documents. Attachments contain embedded Package Shell Objects, or Object Linking and Embedding Objects, that are typically Windows Shortcut “.lnk” files, researchers said.

If the user opens the shortcut and accepts the security warning that appears, a PowerShell command initiates the download of a self-extracting Zip archive hosted on a remote server. The Zip archive contains an obfuscated JavaScript installer.

When researchers de-obfuscated the JavaScript installer they found several configuration session parameters. In recent weeks, researchers said, a “pseb:” parameter has been added which references a script that implements the EternalBlue exploit that can be used to spread laterally within targeted networks.

“We first observed the ‘pseb:’ parameter on Sept. 5. The ‘pseb:’ configuration implements the EternalBlue exploit, borrowing most of its code from a publicly available proof-of-concept,” researchers wrote.

Proofpoint said the ExternalBlue parameter used by the adversary also contains functionality to log the installation and victim configuration details and uploads data to an FTP server.

The payload configuration for this implementation of EternalBlue downloads a PowerShell script from a remote server, which includes an embedded executable that installs Retefe, researchers said.

“We are observing increasingly targeted attacks from this group, that, with the addition of the EternalBlue exploit, creates opportunities for effective propagation within networks once initial targets have been compromised,” Proofpoint wrote.

Researchers note, on Sept.20, the “pseb:” section had been replaced with a new “pslog:” section that contained only the EternalBlue logging functions. “This installation, however, lacks the the ‘pseb:’ module responsible for further lateral spread via EternalBlue, thus avoiding an infinite spreading loop,” they said.

Researchers urge companies to ensure that they are fully patched against the EternalBlue vulnerability (CVE-2017-0144). “Companies should also block associated traffic in IDS systems and firewalls and block malicious messages (the primary vector for Retefe) at the email gateway,” Proofpoint added.
