APT Campaign Leverages the Cueisfry Trojan and Microsoft Word Vulnerability CVE-2014-1761

secureworks.com/blog/apt-campaign-leverages-the-cueisfry-trojan-and-microsoft-word-vulnerability-cve-2014-1761

Param Singh

Dell SecureWorks Counter Threat Unit™ (CTU) researchers discovered the Cueisfry first-stage downloader trojan while analyzing a spearphishing message sent to an email account belonging to an intelligence-related group in Japan. The message was part of an Advanced Persistent Threat (APT) campaign targeting government officials and economic institutions in Southeast Asia.

Behavior

The attachment contained a Rich Text Format (RTF) file that exploited CVE-2014-1761, which affects multiple Microsoft Word releases and allows remote attackers to execute arbitrary code via crafted RTF data. Upon exploitation, the RTF file drops the Epdate.exe file (MD5: 1c29b24d4d4ef7568f519c470b51bbed) and executes it from the system's %TEMP% folder (see Figure 1). The compilation timestamp of the dropped Epdate.exe file was April 21, 2014, indicating that it was created the day before the email was sent.

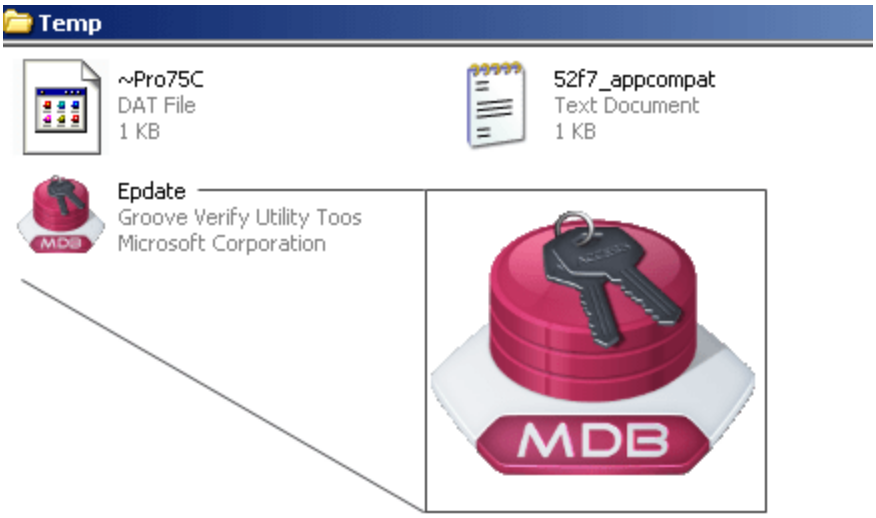

Figure 1. Cueisfry downloader trojan (Epdate.exe) disguised as Microsoft Access MDB file. (Source: Dell SecureWorks)

When executed for the first time on a victim's computer, Epdate.exe (the Cueisfry trojan) checks for the existence of “AntiVir_Update.URL” in the Startup folder. When that check fails, Cueisfry writes the file to the Startup folder to allow the malware to maintain persistence and automatically launch with a system restart and across logins. Cueisfry does not communicate with its command and control (C2) server during this initial run. When the victim logs back

onto the system, Windows automatically triggers the AntiVir_Update.URL file in the Startup folder. As with its initial run, Epdate.exe checks for the AntiVir_Update.URL file in the Startup folder. Confirming the file's existence, Cueisfry establishes a connection to the hard-coded C2 IP address 198.55.103.148. This IP address is still active as of this publication.

Upon execution, Cueisfry checks for proxy settings on the victim's systems by querying the HKCUSoftwareMicrosoftWindowsCurrentVersionInternet Settings registry key and reading values for ProxyEnable and ProxyServer. Then it writes information about processes running on the victim's system to %TEMP%~Proc75C.DAT. After gathering the system's process information, Cueisfry relays it to the C2 server (see Figure 2).

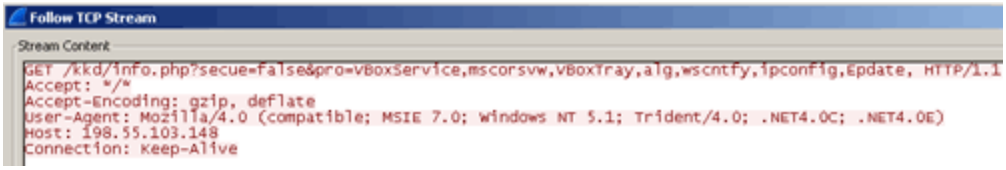

Figure 2. Cueisfry communicating to C2 server. (Source: Dell SecureWorks)

Conclusion

The details of the spearphishing email and dropped Cueisfry malware demonstrate attackers' sophistication when targeting high-value organizations. The use of CVE-2014-1761 reveals attackers' ability to exploit a newly disclosed vulnerability. Organizations can protect themselves from such attacks by applying security updates as they become available from vendors. Organizations should also invest in programs to educate and train employees in detecting and reporting spearphishing attempts.

Threat indicators

The threat indicators in Table 1 can be used to detect activity related to the Cueisfry downloader trojan. The IP addresses listed in the indicator table may contain malicious content, so consider the risks before opening them in a browser.

Indicator	Type	Context
1c29b24d4d4ef7568f519c470b51bbed	MD5 hash	Cueisfry downloader trojan
6ecfb8b802997c2198eb5ff5c87794b0	MD5 hash	Cueisfry downloader trojan
90dc549999ac89ca14ce4ef61fc93ae9	MD5 hash	Cueisfry downloader trojan
7480293644d041f5a969ab847bd12da4	MD5 hash	Cueisfry downloader trojan
ccb3fff7f699e881e3fddcaa2aadc8ba	MD5 hash	Cueisfry downloader trojan
198.55.103.148	IP address	C2 server
107.181.234.41	IP address	C2 server

198.74.114.231	IP address	C2 server

Table 1. Threat indicators for the Cueisfry trojan.