New Remcos RAT Campaign Uses Simplified Delivery Tactic

Author: Bryce Schimon

Overview

From mid-June to July, Infoblox observed a campaign distributing the Remcos remote access trojan (RAT). We previously wrote about Remcos in December 2018, regarding a campaign in which Microsoft Word files with embedded dynamic data exchange (DDE) protocol prompted the recipient to update the file. It then downloaded a Rich Text Format (RTF) file designed to exploit Microsoft's Equation Editor.[1]

In this campaign, RTFs were sent directly to the recipients rather than requiring a download via Word. However, the campaign still exploits the Equation Editor remote code execution vulnerability.[2]

Customer Impact

Unlike exploits that require someone to enable macros, this particular RTF exploit needs no additional user interaction to run after the user opens the file. Once a machine is infected with the Remcos binary and the keepalive session is successful, the threat actor gains complete control of the device over an encrypted connection.

Remcos has advanced surveillance and capabilities that include ScreenLogger, audio capture, and webcam capture.[3] It is easy for threat actors to use and control, which makes it a popular choice among RATs for targeting Windows operating systems.

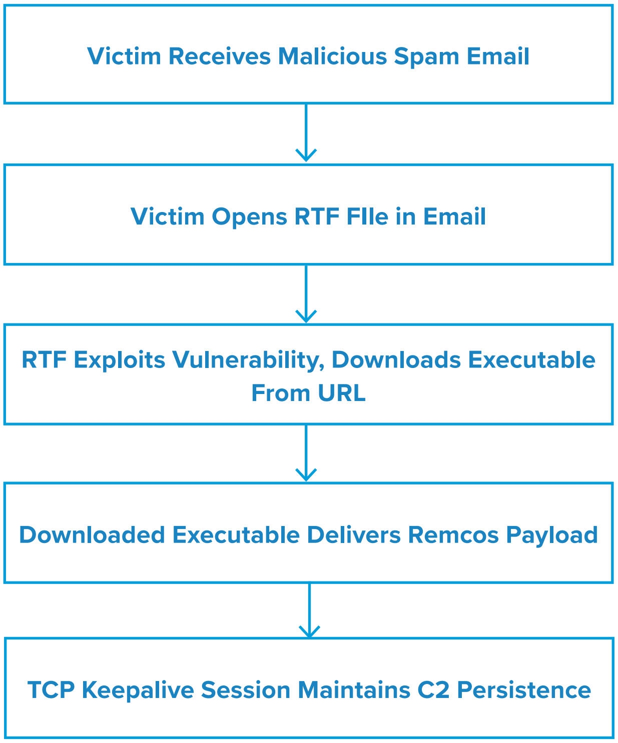
Campaign Analysis

The emails in this campaign had the same subject line, filename, and sender name, and contained nothing in the body. We did, however, find two different file hashes that were used over the course of the campaign.

Threat actors can have Remcos install itself into the User Profile, AppData, Temp, Root, Windows, system32, or Program Files directory of a victim's computer. Threat actors can also specify a custom folder name different than the default path AppData/remcos/remcos.exe, as well as specify a different location for an offline keylogger than the default path AppData/remcos/logs.dat.

Attack Chain

When the recipient opens the RTF, it silently exploits eqnedt32.exe to download a payload. The payload drops and automatically runs leclome.exe, which executes a Visual Basic 6 script, delivering the Remcos RAT hpsupport.exe and then deleting itself. For persistence, Remcos creates an encrypted session and adds hpsupport.exe startup method as HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\hpsupport.



Victim Receives Malicious Spam Email

Victim Opens RTF FIle in Email

RTF Exploits Vulnerability, Downloads Executable From URL

Downloaded Executable Delivers Remcos Payload

TCP Keepalive Session Maintains C2 Persistence

Vulnerabilities & Mitigation

This campaign exploited a widespread Microsoft Office vulnerability to deliver Remcos RAT via spam email. Infoblox recommends the following actions to reduce the risk of becoming infected by Remcos.

- Keep Microsoft Office security patches up to date.
- Do not open attachments from unfamiliar or unknown senders.
- Verify suspicious documents over the phone or in person.
- Filter attachments to reduce the likelihood of malicious content reaching a user's workstation.

Endnotes

1. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11882
2. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11882
3. https://breaking-security.net/remcos/

Infoblox is leading the way to next-level DDI with its Secure Cloud-Managed Network Services. Infoblox brings next-level security, reliability and automation to on-premises, cloud and hybrid networks, setting customers on a path to a single pane of glass for network management. Infoblox is a recognized leader with 50 percent market share comprised of 8,000 customers, including 350 of the Fortune 500.

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com