404 Keylogger Campaigns | Infoblox

404 Keylogger Campaigns

Author: James Barnett

Overview

On October 11 and 15, Infoblox observed two related malicious spam (malspam) campaigns that used 7-Zip archive files to deliver the 404 Keylogger malware.

Customer Impact

404 Keylogger is an information stealer (infostealer) that can steal a victim's credentials and log their keyboard input. It was initially released on a Russian hacking forum in August 2019.[1] It is notable for its relatively unusual methods of data exfiltration, including via email messages, Pastebin file uploads and encrypted Telegram messages.

Campaign Analysis

All malspam emails in the two campaigns we observed came from the same SMTP server, but each campaign had different themes for the subject lines and attachments. The October 11 campaign used the subject line *RE: BANK TRANSFER SLIP* and had an attachment named *swift transfer copy 639082020.7z*. The October 15 campaign used the subject line *Re: T21 Orders - Quotation - MLM -309-Ref-284* and included an attachment named *T21 Orders - Quotation 309-Ref-284.7z*.

Attack Chain

When the victim extracts and executes the 404 Keylogger payload contained within the 7-Zip archive, the malware creates a copy of itself with a randomized name in the victim's *AppData* folder. It then creates a scheduled task that will periodically run this copy of the malware, allowing it to achieve a basic level of persistence on the victim's machine.

After establishing persistence, 404 Keylogger sets up a keyboard hook that allows it to log the victim's keystrokes so that the attacker can steal any credentials the victim types in. The malware then proceeds to search for saved credentials for a variety of different application types, including web browsers (e.g. Google Chrome), email clients (e.g. Microsoft Outlook), chat clients (e.g. Pidgin) and FTP clients (e.g. Filezilla).

Once 404 Keylogger has collected the victim's credentials, it contacts a legitimate IP lookup service to determine the IP address of the victim's machine. It also gathers various pieces of information about the system itself, including the system name and Windows version. It then combines all of this information along with the stolen credentials and saves it in the current user's *Documents* folder as a text file named *Results.txt*.

TLP: WHITE https://www.us-cert.gov/tlp

Enter the password to open this PDF file:

File name:

-

File size:
-

Title:
-

Author:
-

Subject:
-

Keywords:
-

Creation Date:
-

Modification Date:
-

Creator:
-

PDF Producer:
-

PDF Version:
-

Page Count:
-

Page Size:
-

Fast Web View:
-

Preparing document for printing…
0%