Ghostrat

New Campaign by Higaisa

June 12th, 2020

ATLAS CYBERSECURITY

www.atlas-cybersecurity.com

Infection

- Ghostrat uses an infection chain that begins once the victims receive an RAR file named "Project link and New copyright policy.rar"
- Once decompressed, the folder contains two Microsoft shortcut files and a PDF file
  - Zeplin Copyright Policy.pdf
  - ConversationsoiOS-Swipe Icons-Zeplin.lnk
  - Tokbox icon-Odds and Ends-iOS-Zeplin.lnk
- The PDF file "Zeplin Copyright Policy" is benign and was copied from the publicly accessible Zeplin website and is being used to act as a decoy, in case the PDF was examined by antivirus services
- If the victim clicks on one of the Microsoft shortcut files, a series of commands execute and the attack begins
  - These shortcuts also contained another decoy to distract the victim – the victim's web browser will open and be directed to the Zeplin page, zeplin.io

Examining the Links

- Examining the two Microsoft shortcut links yields no metadata information as almost all information has been stripped from the links by the attacker
  - The only information left in the two samples is the creation date of the file (May 11, 2020), the timestamp (8:03:01 UTC) and the date the C drive was created (March 18, 2019 21:37:44 UTC)
- When the file is executed, it will pull a block of data from the lnk file and save it as 'cSi1rouy.tmp'; it then base64 decodes this data, revealing a Microsoft Cabinet file (.cab).
  - Once this cabinet file is decompressed, it reveals an additional four files:
    - 34fDFkfSD32.js
    - Svchast.exe
    - 3t54dE3r.tmp
    - Conversations-iOS-Swipe Icons-Zeplin.url

The JavaScript File

- The JavaScript file, 34fDFkfSD32.js, is used to spawn a hidden command shell that runs ipconfig and redirects the output to a file named 'd3reEW.txt' that is then sent to a (presumed) threat actor hostname
  - hxxp://zeplin[.]atwebpages[.]com/inter.php
- Following this, the JavaScript file copies 'Svchast.exe' to the Windows Startup folder
  - The file path
    - %AppData%\\Microsoft\\Windows\\Start Menu\\Programs\\Startup\\officeupdate.exe
  - Copying this file fulfills two functions:
    - It allows for persistence on the infected host, as the programs inside the previous directory are automatically ran upon startup
    - It allows for 'blending into' the target environment by masking itself as the signed Microsoft program, officeupdate.exe
      - To allow for some redundancy, the loader file, Svchast.exe, is copied to the downloads folder and renamed officeupdate.exe
      - A schedule task is then created, named 'Driver Booster Update,' and set to run every two hours, at which point it will execute the officeupdate.exe file that was previously copied to the downloads folder

Loader and ShellCode

- The file Svchast.exe is the loader for the main payload in this campaign, a file named '3t54de.tmp'
  - The loader, Svchast.exe, has some built in protection against anti-malware analysis: it checks if it is being run in a debugger; if it is, the file will cease execution
- It will then decode a portion of the payload (XOR) and once complete it injects it into the running process
- The actual payload file, 3t54de.tmp, appears to be shellcode that contained the threat actor's command and control node. It performs some host-based enumeration upon the victim machine and the establishes a persisten connection between the infected host and the command and control node