Arechclient2 -

Published: 2022-11-30 · Archived: 2026-04-05 22:00:25 UTC

I. Targeted Entities

- Opportunistic organizations

II. Introduction

Arechclient2 is a .NET remote access trojan (RAT) that has numerous capabilities. The RAT can profile victim systems, steal information like browser and crypto-wallet data, and launch a hidden secondary desktop to control browser sessions.

III. Cyber Florida SOC Observations

Cyber Florida has observed network payload data obfuscated via Base64 encoding and sent to what appears to be a command control server. The command and control server appears to be utilizing Google cloud services (googleusercontent.com). Within the Base64 data, exfiltrated usernames and passwords were observed. Based on observations, the exfiltrated data appears to be from cached browser credentials (Google Chrome profiles, Firefox profiles, Microsoft Edge profiles, etc.) In reviewing logs and network traffic there were parameters of interest within the data payload that would aid in identifying this activity. The following payload parameters were observed the network traffic: *ConnectionType*, *Client*, *SessionID*, *BotName*, *Computer*, *BuildID*, *BotOS*, *URLData*, *UIP*.

Based on observing network traffic for the command control communication, there may be similarities associated to the Redline Stealer malware. See CERT Italy article. https://cert-agid.gov.it/news/scoperto-il-malware-redline-stealer-veicolato-come-lastpass/

Screenshot samples of log and network traffic have been provided in the appendix of this report.

Some of the interesting evasion tactics Cyber Florida observed were the utilization of “sleep” functions and the usage of .NET Framework’s InstallUtil.exe binary to communicate with the command and control server. The “sleep” functionality appeared to delay the usage of InstallUtil.exe. In testing, the Installutil.exe appeared to run in perpetuity regularly communicating with the command and control server. In reviewing a few of the automated sandboxes, the Installutil.exe activity was not identified. This may be due to the “sleep” activity being utilized.

Another evasion tactic appears to be attempting to modify Windows Defender settings via the second observed PowerShell instance. The cmdlet Set-MpPreference with the options –ExclusionPath ‘C:’ was employed. This command appears to create a malware scan exclusion, which would prevent Windows Defender from scanning the entire C: volume.

The following links provide examples and context of InstallUtil.exe malware usage and abuse.

https://gbhackers.com/hiding-malware-legitimate-tool/ (not directly related to observed activity)

https://www.ired.team/offensive-security/code-execution/t1118-installutil (not directly related to observed activity)

https://attack.mitre.org/techniques/T1218/004/

During initial malicious binary execution, a persistence mechanism was observed via the common HKCUSoftwareMicrosoftWindowsCurrentVersionRun location.

IV. Additional Background Information

Blackpoint Cyber discovered an ISO file that contained a malicious Windows executable that was downloaded to a victim's computer and was not detected by an antivirus program. A malicious executable, named *Setup.exe*, was observed using various defense evasion techniques including obfuscation, injection, and uncommon automation tools. These tools were used to drop a RAT named *Arechclient2* (Blackpoint Cyber). The size of *Setup.exe* is over 300 megabytes (Blackpoint Cyber).

The initial attack vector that was used to send *Setup.exe* to the victim is unknown. This is the execution step. When *Setup.iso* is double-clicked, the ISO file can be mounted like a CD and, oftentimes, the contents of the file are automatically executed (Blackpoint Cyber). Running *Setup.exe* will start the extraction of three files and execute multiple child processes (Blackpoint Cyber). A new folder, *IXP000.TMP*, is made in the victim's *AppDataLocalTemp* directory and three files are created into the newly created directory: *Funding.mpeg*, *Mali.mpeg*, and *Dns.mpeg* (Blackpoint Cyber).

The *Dns.mpeg* script is heavily obfuscated. The script searches for *AvastUI.exe* and *AVGUI.exe* running on the victim's computer. The two executables are found in the Avast antivirus product line (Blackpoint Cyber). If those two executables are not found, *Dns.mpeg* sets *Hole.exe.pif* to the name *AutoIT3.exe*. In the script *.au3* (or *d.au3*) there are over 3,000 references to a function named *Xspci()*. This function takes a string as its first argument and a number as its second argument. The function is responsible for decoding strings (Blackpoint Cyber).

The *.au3* script accomplishes three things through injection: 1. establishing persistence using a URL file in the victim's startup folder. 2. copying the *ntdll.dll* file from the *C:WindowsSysWOW64* folder to avoid antivirus hooks. 3. injecting the embedded payload into *jsc.exe* (Blackpoint Cyber). The function that is responsible for the above tasks is *KXsObHGILZNaOurxqSUainCYU()* which takes a pointer to the binary to be injected, a string argument, and a string argument with the path to the binary that would be executed and injected into as arguments (Blackpoint Cyber). The script establishes persistence by adding a URL file to the victim's startup folder that will execute a Microsoft Visual Basic Script (VBS) on every login (Blackpoint Cyber).

Arechclient2 has a decompilation phase. *Test.exe*, a C# binary, can be loaded into tools that statically and dynamically analyze code. One such tool is DnSpy (Blackpoint Cyber). The class names in *Test.exe* were minimized to single and double characters to add an additional layer of confusion for reverse engineers (Blackpoint Cyber). The actual name of *Test.exe* is *2qbarx12tqm.exe* (Blackpoint Cyber). Arechclient2 also contains a command and control (C2) phase. When Arechclient2 is executed, it connects to *https[:]//pastebin.com/raw/nJqnWX3u* to collect C2 information (Blackpoint Cyber). The requested file,

nJqnWX3u, contains the IP address *34[.]141[.]198[.]105* as a string. It also connects to *http[:]//eth0.me* to get its public IP address (Blackpoint Cyber). Arechclient2 connects to its C2 server on port 15647 to receive commands. The server responds with information to control the encryption status ("On" or "Off") in JSON format (Blackpoint Cyber). If the communications are intercepted and the encryption is set to "Off," further communications will be in plaintext (Blackpoint Cyber).

V. MITRE ATT&CK

- **T1059.001 – Command and Scripting Interpreter: PowerShell**
  Adversaries may abuse PowerShell commands and scripts for execution. PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system. Adversaries can use PowerShell to perform a number of actions, including discovery of information and execution of code.
- **T1555.003 – Credentials From Web Browsers**
  Adversaries may acquire credentials from web browsers by reading files specific to the target browser. Web browsers commonly save credentials such as website usernames and passwords so that they do not need to be entered manually in the future. Web browsers typically store the credentials in an encrypted format within a credential store; however, methods exist to extract plaintext credentials from web browsers.
- **T1547.001 – Registry Run Keys / Startup Folder**
  Adversaries may achieve persistence by adding a program to a startup folder or referencing it with a Registry run key. Adding an entry to the "run keys" in the Registry or startup folder will cause the program referenced to be executed when a user logs in. These programs will be executed under the context of the user and will have the account's associated permissions level.
- **T1562.001 – Impair Defenses: Disable or Modify Tools**
  Adversaries may modify and/or disable security tools to avoid possible detection of their malware, tools, and activities. Adversaries may also tamper with artifacts deployed and utilized by security tools. Security tools may make dynamic changes to system components in order to maintain visibility into specific events.
- **T1218.004 – System Binary Proxy Execution: InstallUtil**
  Adversaries may use InstallUtil to proxy execution of code through a trusted Windows utility. InstallUtil is a command-line utility that allows for installation and uninstallation of resources by executing specific installer components specified in .NET binaries. The InstallUtil binary may also be digitally signed by Microsoft and located in the .NET directories on a Windows system: C:WindowsMicrosoft.NETFramework vInstallUtil.exe and C:WindowsMicrosoft.NETFramework64 vInstallUtil.exe.
- **T1095 –Non-Application Layer Protocol**
  Adversaries may use a non-application layer protocol for communication between host and C2 server or among infected hosts within a network. The list of possible protocols is extensive.
- **T1132.001 –Standard Encoding**
  Adversaries may encode data with a standard data encoding system to make the content of command and control traffic more difficult to detect. Command and control (C2) information can be encoded using a standard data encoding system that adheres to existing protocol specifications. Common data encoding schemes include ASCII, Unicode, hexadecimal, Base64, and MIME.

VI. Recommendations

- **Phishing awareness training**
  Users should be informed and educated about new kinds of phishing scams currently being used and ones that have been used in the past. Awareness training should instruct users to avoid suspicious emails, links, websites, attachments, etc. Users should also be educated about new types of attacks and schemes to mitigate risk. **Recommended link**: https://www.us-cert.gov/ncas/tips/ST04-014
- **Set antivirus programs to conduct regular scans**
  Ensure that antivirus and antimalware programs are scanning assets using up-to-date signatures
- **Malware monitoring**
  Continuously monitor current and new types of malware. Stay up to date on intel and advancements to prevent, defend, and mitigate these types of threats.
- **Strong cyber hygiene**
  Enforce a strong password policy across all networks and subsystems. Remind users to be wary of any messages asking for immediate attention, links, downloads, etc. All sources should be verified. **Recommended link**: https://us-cert.cisa.gov/ncas/alerts/aa21-131a
- **Turn on endpoint protection**
  Enable endpoint detection and response (EDR) to stop unknown malware in the product you're using.
- **Network Monitoring**
  Review network logs, payload, etc. for related IP address and associated network parameters.

VII. Indicators of Compromise (IOCs)

This screenshot shows the payload sent to a victim, as seen by Cyber Florida. A portion of the Base64 and UIP fields have been redacted.

The following screenshot is similar from the log above but was acquired via network packet capture.

X. References

Blackpoint Cyber. "Ratting out arechclient2 – Blackpoint Whitepaper." Blackpoint Cyber. Accessed November 15, 2022. https://blackpointcyber.com/lp/ratting-out-arechclient2/?utm_campaign=ratting_out_arechclient2_whitepaper&utm_source=resource_library.

Threat Advisory created by **The Cyber Florida Security Operations Center**. *Contributing Security Analysts: Dorian Pope, Sreten Dedic, EJ Bulut, Uday Bilakhiya.*
