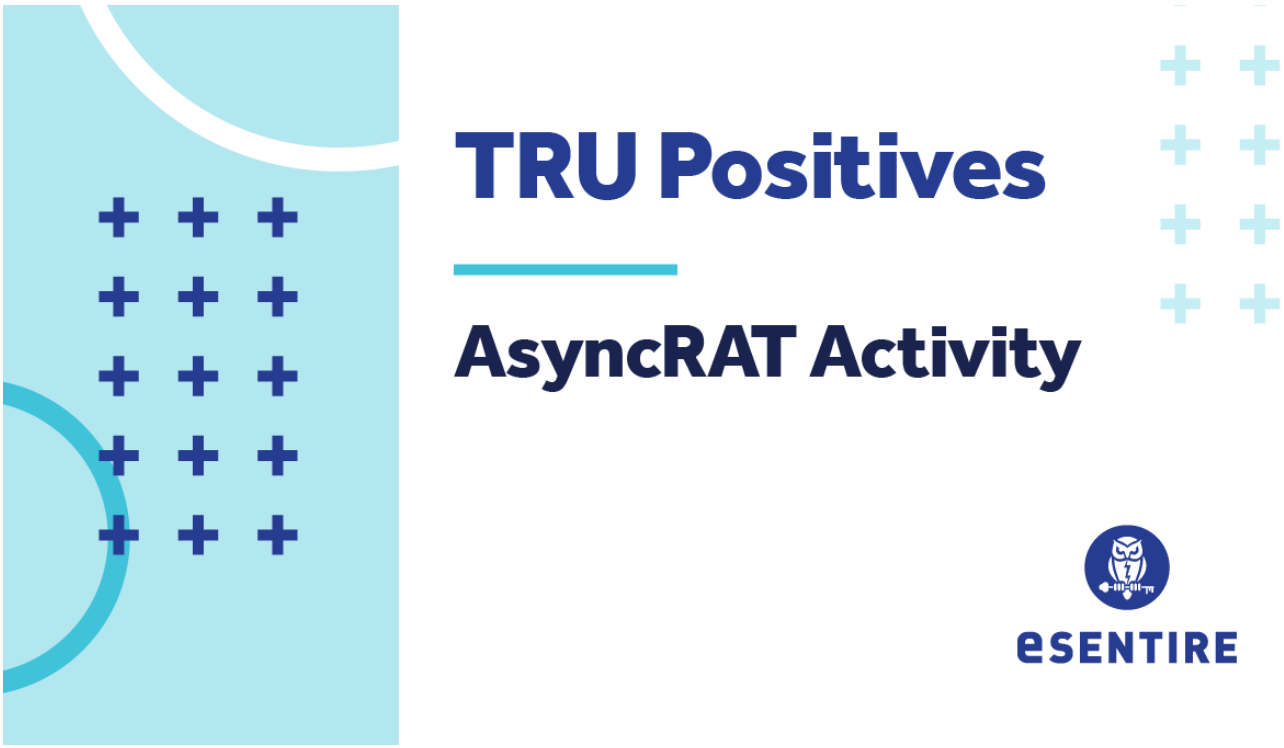
AsyncRAT Activity

esentire.com/blog/asyncrat-activity



Adversaries don't work 9-5 and neither do we. At eSentire, our 24/7 SOCs are staffed with Elite Threat Hunters and Cyber Analysts who hunt, investigate, contain and respond to threats within minutes.

We have discovered some of the most dangerous threats and nation state attacks in our space – including the Kaseya MSP breach and the more_eggs malware.

Our Security Operations Centers are supported with Threat Intelligence, Tactical Threat Response and Advanced Threat Analytics driven by our Threat Response Unit – the TRU team.

In TRU Positives, eSentire's Threat Response Unit (TRU) provides a summary of a recent threat investigation. We outline how we responded to the confirmed threat and what recommendations we have going forward.

Here's the latest from our TRU Team…

What did we find?

- AsyncRAT impacting a customer in the insurance industry.

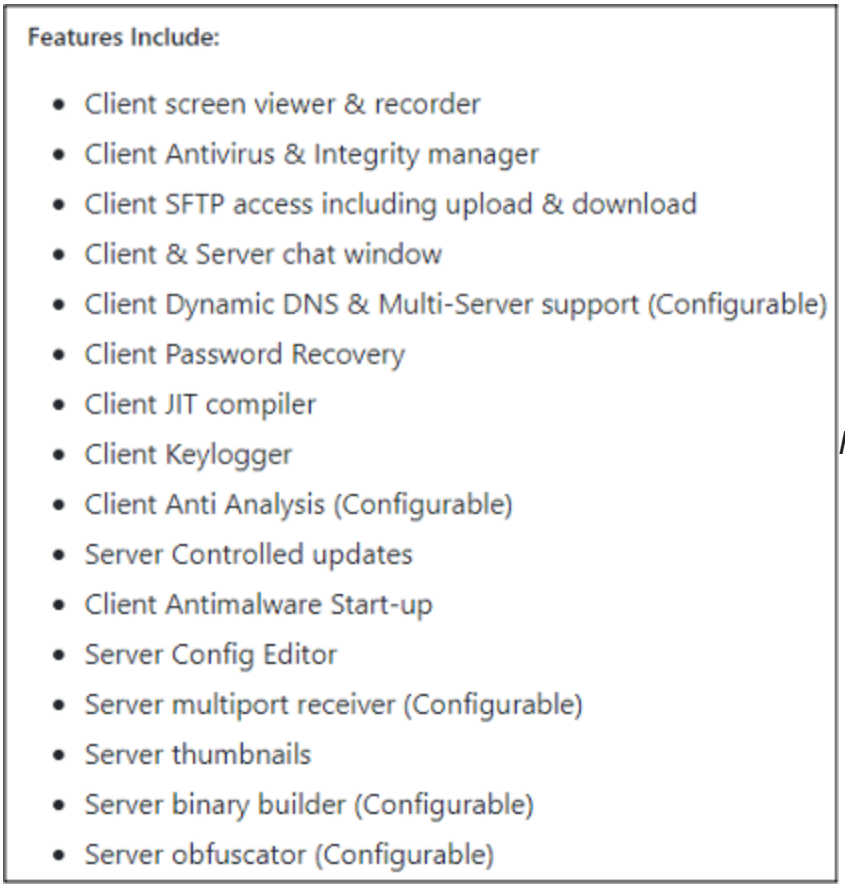
- AsyncRAT is an open-source remote access trojan with varying capabilities including remote access, file exfiltration, and keylogging.
- eSentire has observed an increase in this threat throughout March and April 2022.
- 

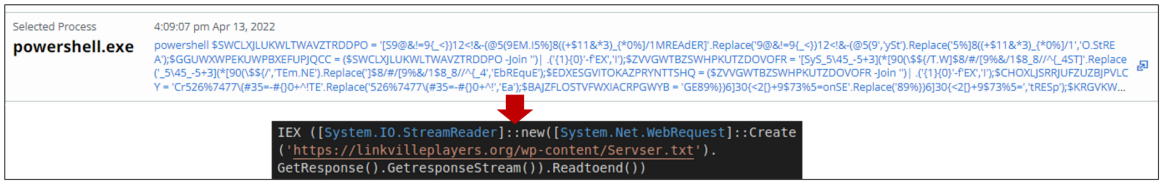
Figure 1 AsyncRAT's features. Source: GitHub
- In this incident, AsyncRAT was delivered via an email containing several layers of files to evade email filtering defenses.
  - The first layer, a randomly named HTML file was retrieved by the user and opened in their browser. The user was prompted to download an embedded ISO file, a defense evasion technique known as HTML smuggling.
  - The ISO file was mounted by the victim, revealing an embedded VBS script file.
  - The VBS file was clicked by the user, resulting in PowerShell execution to retrieve a script from a remote host.
  - 

Figure 2 PowerShell Dropper

- The PowerShell script functionality is similar to what is described here. In summary, the script:
    - Creates a working directory under C:\ProgramData\BQIZGZEFZTIRALVAQROZSD\.
    - Writes helper scripts to the working directory, most named after the directory itself.
    - Creates a scheduled task called 'BQIZGZEFZTIRALVAQROZSD' to persist on the device.
    - Decodes two embedded binaries. The files are hex encoded and interlaced with "+" symbols.
    - Injects the AsyncRAT payload into aspnet_compiler.exe.

How did we find it?

- Our Machine Learning PowerShell classifier detected the attempt to retrieve the second stage PowerShell script.
- Our 24/7 SOC cyber analysts were alerted and investigated.

What did we do?

- Our SOC cyber analysts investigated and confirmed that the activity is malicious.
- Isolated the host on the customer's behalf to contain this incident in accordance with the customer's business policies.

What can you learn from this TRU positive?

- AsyncRAT is an open-source project. Successful delivery and infection of AsyncRAT requires layers of obfuscation and code injection.
    We covered this infection chain previously.
- The infection chain requires the user to follow several steps to grant the adversary code execution capabilities. Unfortunately, mounting ISOs or executing scripting files in Windows is trivial and similar infection chains are increasingly common.
- Layers of embedded files may thwart email filtering. The malicious payload is only retrieved when the user has completed several manual steps.

Recommendations from our Threat Response Unit (TRU) Team:

- Attacks such as this rely on user execution. Using phishing and security awareness training, increase your employees' awareness of:
    - Email-based attacks (e.g., business email compromise (BEC) attacks), particularly those delivering HTML or ISO files.
    - Unknown ISO or script files (VBS, JS). These file types pose a risk and shouldn't be opened.

- Create new “Open With” parameters for script files (.js, .jse, .hta, .vbs) so they open with notepad.exe. This setting is found in the Group Policy Management Console under User Configuration > Preferences > Control Panel Settings > Folder Options.
    By default, these script files are executed automatically using Windows Script Host (wscript.exe) or Microsoft HTML Application host (mshta.exe) when double-clicked by a user.
- ISO files are mounted as a drive when double-clicked by users by default, consider deregistering this file extension in Windows File Explorer.

Ask Yourself...

1. Are your users sufficiently aware of techniques bypassing email filtering?
2. What level of visibility do you have across your network, endpoint, and overall environment to detect malicious behavior at scale?
3. Can you respond to remote access malware in a timely manner?