Suspected AsyncRAT Delivered via ISO Files Using HTML Smuggling Technique

By eSentire Threat Response Unit (TRU)

Archived: 2026-04-05 19:27:06 UTC

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?

How did we find it?

- Our Machine Learning PowerShell classifier detected malicious code execution resulting from the victim manually executing the malicious VBS file.

What did we do?

- Our 24/7 SOC cyber analysts alerted the customer and responded on the client's behalf by successfully isolating the host.

What can you learn from this TRU positive?

- The HTML smuggling technique makes detection through content filters difficult since payloads are embedded within a local HTML file and not retrieved over the network.
- Further complicating detection is the use of an .iso file within the HTML to hide the payload until mounted by the victim. Figure 5 shows a visual representation of this file structure.
    - Note that only the email and final payload are transmitted over the network layer.

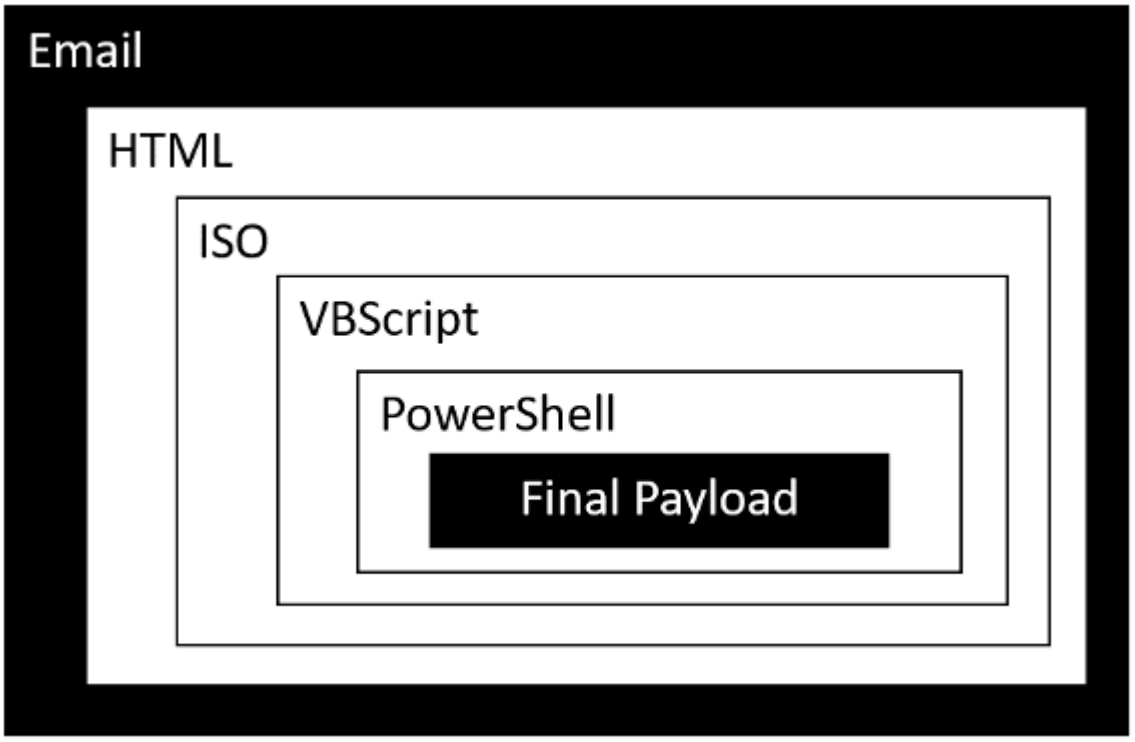

Figure 5 Visual representation of nested files.

- Our observations of adversaries using disk image files for code delivery is increasingly common. In February TRU identified an IcedID campaign delivered using .iso images.
- Malware embedded inside of .iso files may evade security controls and is a known technique for bypassing the Mark-of-the-Web trust control.
- Early detection of this evasive malware delivery method will be crucial to limiting impact.

Recommendations from our Threat Response Unit (TRU) Team:

- Display file extensions for known file types and consider showing hidden files to users by default.
- Conduct Phishing and Security Awareness Training (PSAT) on a regular basis with your employees, placing a special emphasis on spotting business email compromise (BEC) attacks. Warn users about the threat posed by .html and image files (.iso) attached or hyperlinked in emails.
- 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.
- Since .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. What level of visibility do you have across your network, endpoint, and overall environment to detect malicious behavior at scale?
2. What tools are you employing for email filtering and how is that activity monitored?

3. What level of managed endpoint support do you have in place?
4. Are you monitoring your endpoints 24/7 and what degree of control do you have to initiate a kill switch when required?

Indicators of Compromise

dca4d47ed0714d3ab9e4ef17192f7f1d	“Order_Receipt.html”
https://www[.]asterglobal[.]com/.Fainl.txt	Location for payload retrieved by PowerShell command

If you’re not currently engaged with a Managed Detection and Response provider, we highly recommend you partner with us for security services in order to disrupt threats before they impact your business.

Want to learn more? Connect with an eSentire Security Specialist.

To learn how your organization can build cyber resilience and prevent business disruption with eSentire’s Next Level MDR, connect with an eSentire Security Specialist now.

GET STARTED

ABOUT ESENTIRE'S THREAT RESPONSE UNIT (TRU)

The eSentire Threat Response Unit (TRU) is an industry-leading threat research team committed to helping your organization become more resilient. TRU is an elite team of threat hunters and researchers that supports our 24/7 Security Operations Centers (SOCs), builds threat detection models across the eSentire XDR Cloud Platform, and works as an extension of your security team to continuously improve our Managed Detection and Response service. By providing complete visibility across your attack surface and performing global threat sweeps and proactive hypothesis-driven threat hunts augmented by original threat research, we are laser-focused on defending your organization against known and unknown threats.

Back to blog

Take Your Cybersecurity Program to the Next Level with eSentire MDR.

BUILD A QUOTE

in this blog
