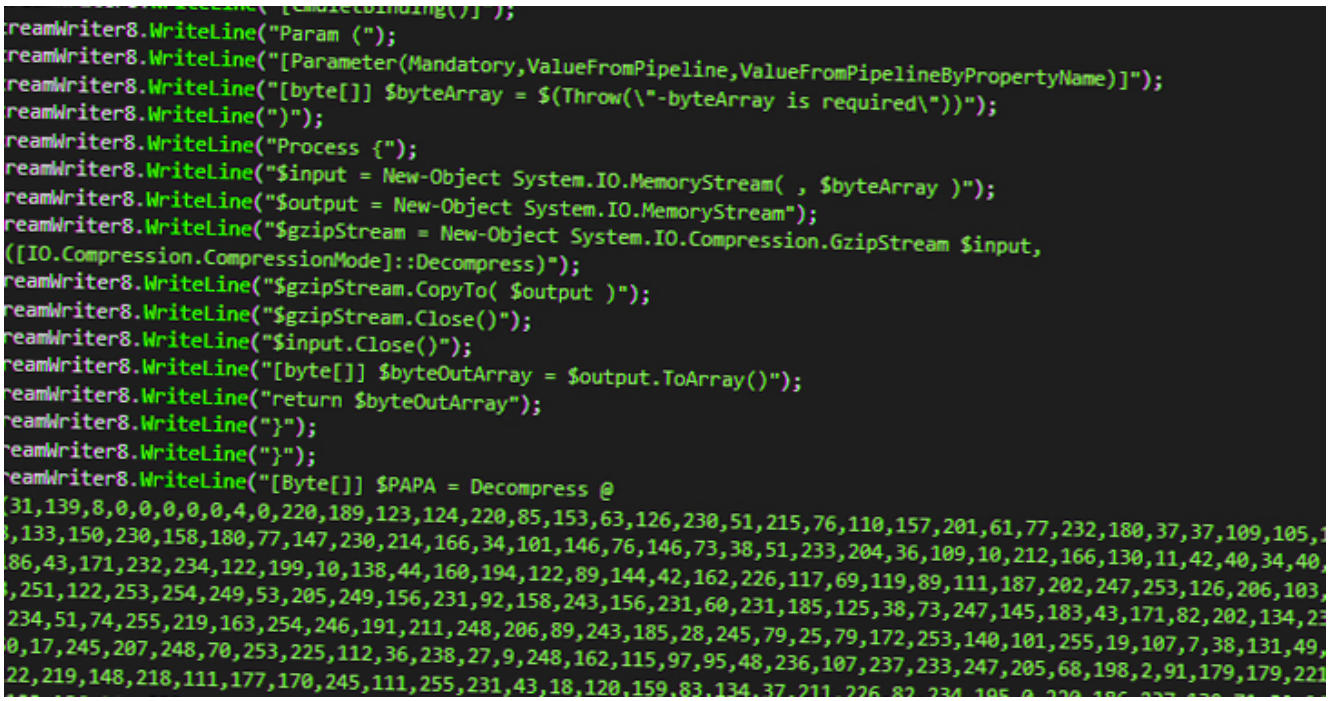
Hackers Using New Evasive Technique to Deliver AsyncRAT Malware

thehackernews.com/2022/01/hackers-using-new-evasive-technique-to.html

January 26, 2022

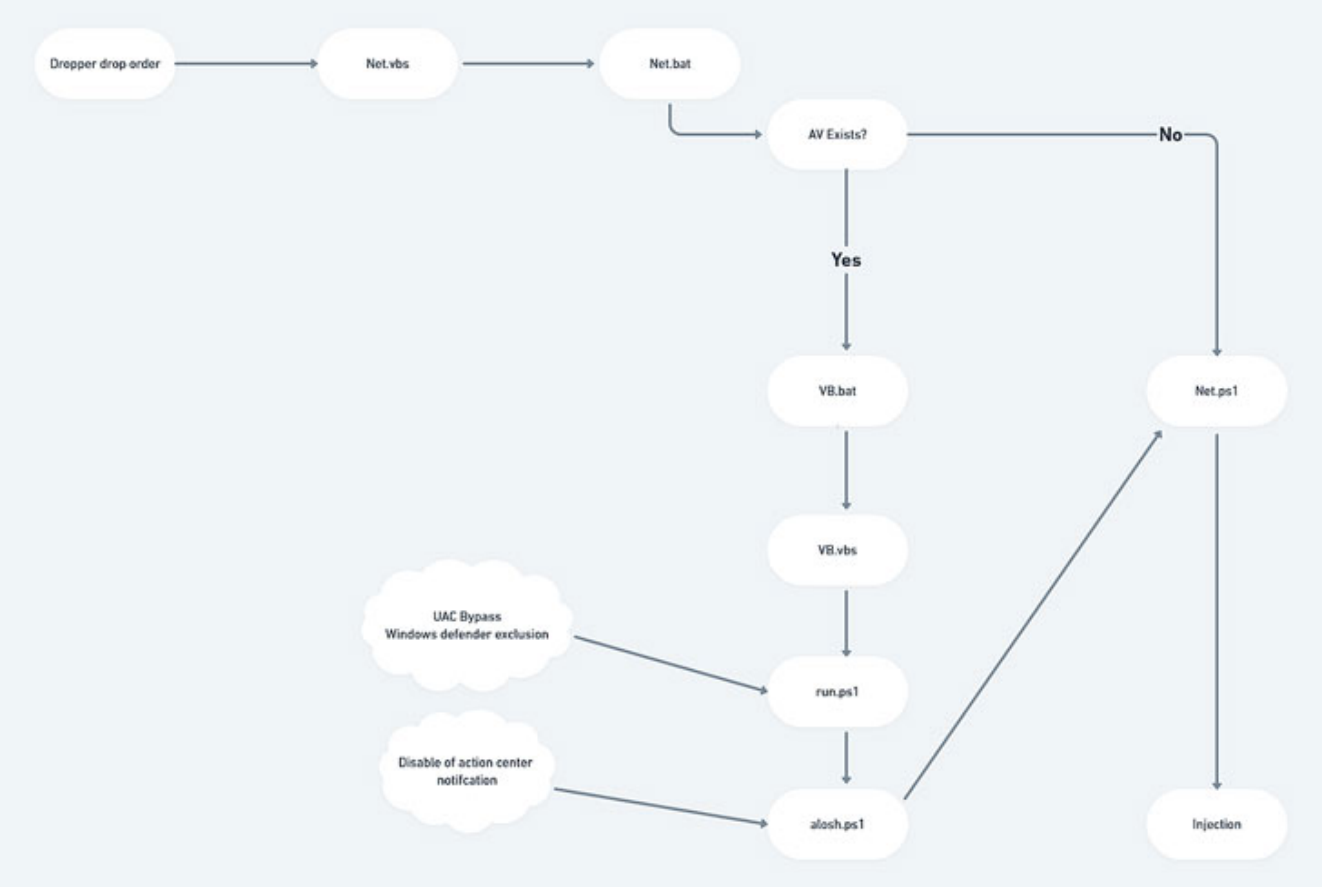


A new, sophisticated phishing attack has been observed delivering the AsyncRAT trojan as part of a malware campaign that's believed to have commenced in September 2021.

"Through a simple email phishing tactic with an HTML attachment, threat attackers are delivering AsyncRAT (a remote access trojan) designed to remotely monitor and control its infected computers through a secure, encrypted connection," Michael Dereviashkin, security researcher at enterprise breach prevention firm Morphisec, said in a report.

The intrusions commence with an email message containing an HTML attachment that's disguised as an order confirmation receipt (e.g., Receipt-<digits>.html). Opening the decoy file redirects the message recipient to a web page prompting the user to save an ISO file.

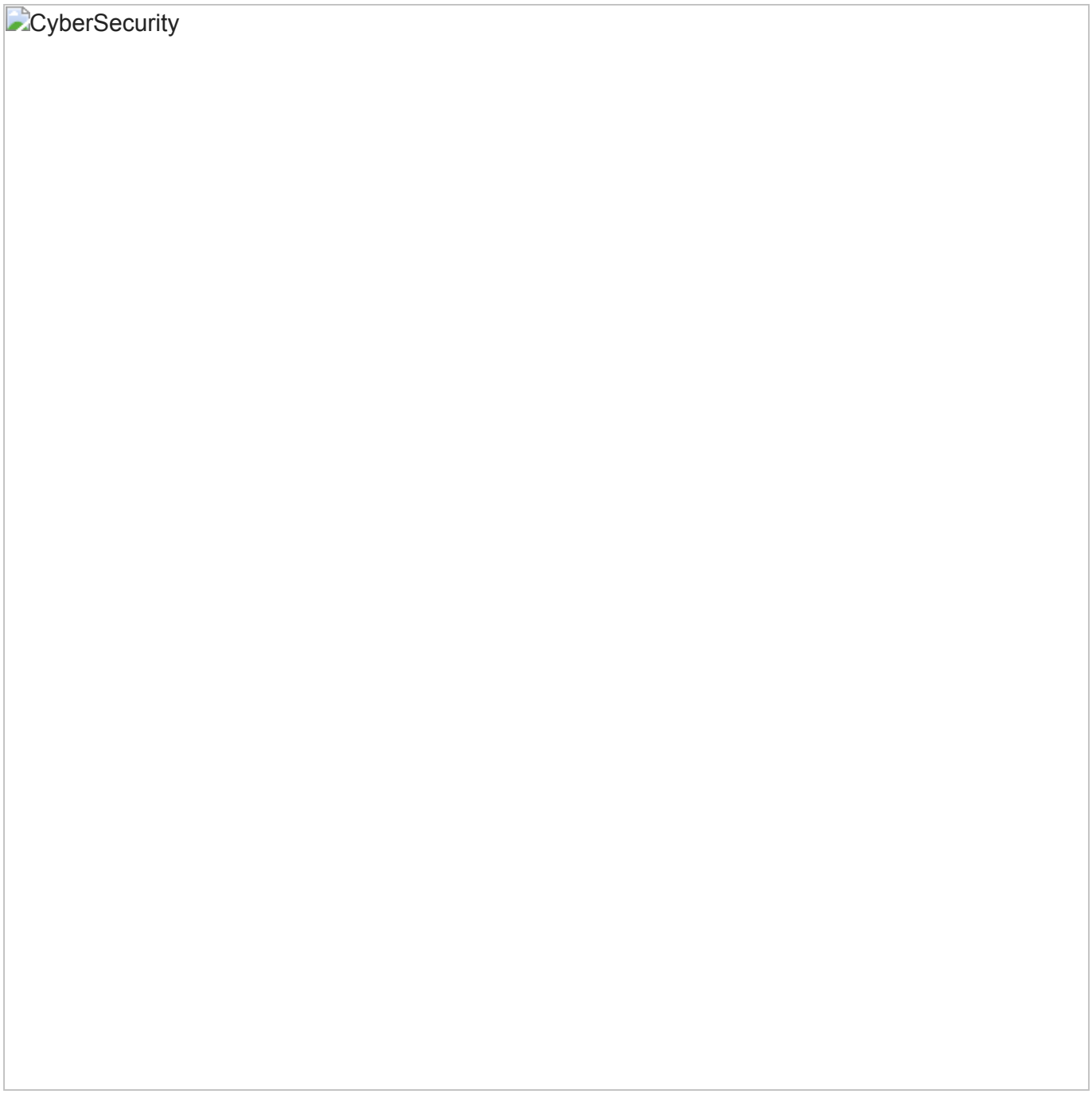
But unlike other attacks that route the victim to a phishing domain set up explicitly for downloading the next-stage malware, the latest RAT campaign cleverly uses JavaScript to locally create the ISO file from a Base64-encoded string and mimic the download process.



"The ISO download is not generated from a remote server but from within the victim's browser by a JavaScript code that's embedded inside the HTML receipt file," Dereviashkin explained.

When the victim opens the ISO file, it is automatically mounted as a DVD Drive on the Windows host and includes either a .BAT or a .VBS file, which continues the infection chain to retrieve a next-stage component via a PowerShell command execution.

This results in the execution of a .NET module in-memory that subsequently acts as a dropper for three files — one acting as a trigger for the next — to finally deliver AsyncRAT as the final payload, while also checking for antivirus software and setting up Windows Defender exclusions.



RATs such as AsyncRAT are typically used to forge a remote link between a threat actor and a victim device, steal information, and conduct surveillance through microphones and cameras. They provide an array of advanced capabilities that give the attackers the ability to fully monitor and control the compromised machines.

Morphisec also pointed out the campaign's advanced tactics, which it said allowed the malware to slip through virtually undetected by most antimalware engines despite the operation being in effect for close to five months.