CIRT.GY Guyana National Computer Incident Response Team

AL2021_51 New Stealthy JavaScript Loader Infecting Computers with Malware (1st November 2021)

Description

Threat actors have been discovered employing a previously unknown JavaScript malware variant as a loader to spread a variety of remote access Trojans (RATs) and information stealers.

Summary

The new evasive loader, called "RATDispenser" by HP Threat Research, with the malware liable for delivering at least eight (8) different malware families in 2021. A total of 155 samples of this new malware have been identified, with three different variations, indicating that it is still in development.

How it works

"RATDispenser is used to get ahead of the system before unleashing secondary malware that takes control of the compromised device," said security researcher Patrick Schläpfer. "All of the payloads were remote access Trojans (RATs), which were designed to steal information and allow attackers to control targeted devices."

The infection begins with a phishing email that contains a malicious attachment that appears to be in the form of a text file but is obfuscated JavaScript code programmed to write and run a VBScript file, which then downloads the final-stage malware payload on the affected machine.

RATDispenser has been seen dropping a variety of malware, along with STRRAT, WSHRAT (Houdini or Hworm), AdWind (AlienSpy or Sockrat), Formbook (xLoader), Remcos (Socmer), Panda Stealer, CloudEyE (GuLoader), and Ratty, all of which can steal sensitive information from infected devices and targeting cryptocurrency wallets.

"The range of malware families can be purchased or downloaded for free from underground marketplaces," Schläpfer added, "that the creators of RATDispenser may be operating under a malware-as-a-service business model."

Remediation

At this moment there is no fixed patch to remedy this new malware. However, PC users should ensure they implement the following security measures.

- Keep your computer and software updated.
- Install antivirus
- Install firewall and configure it according to network requirements

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- New stealthy javascript loader infecting computers with malware (25th November 2021). Retrieved from thehackernews.

  https://thehackernews.com/2021/11/this-new-stealthy-javascript-loader.html

- New stealthy javascript loader infecting computers with malware (23rd November 2021). Retrieved from HP.

  https://threatresearch.ext.hp.com/javascript-malware-dispensing-rats-into-the-wild/

- New stealthy javascript loader infecting computers with malware (25th November 2021). Retrieved from The Cybersecurity News.

  https://thecybersecurity.news/general-cyber-security-news/this-new-stealthy-javascript-loader-infecting-computers-with-malware-2-14814/