RAT Gone Rogue: Meet ARS VBS Loader

flashpoint-intel.com/blog/meet-ars-vbs-loader/

April 16, 2018

Blogs

Blog

Malicious VBScript has long been a fixture of spam and phishing campaigns, but until recently its functionality has been limited to downloading malware from an attacker-controlled server and executing it on a compromised computer.

Malicious VBScript has long been a fixture of spam and phishing campaigns, but until recently its functionality has been limited to downloading malware from an attacker-controlled server and executing it on a compromised computer.

Researchers at Flashpoint have seen and analyzed a unique departure from this norm in ARS VBS Loader, a spin-off of a popular downloader called SafeLoader VBS that was sold and eventually leaked in 2015 on Russian crimeware forums.

ARS VBS Loader not only downloads and executes malicious code, but also includes a command and control application written in PHP that allows a botmaster to issue commands to a victim's machine. This behavior likens ARS VBS Loader to a remote access Trojan (RAT), giving it behavior and capabilities rarely seen in malicious "loaders", i.e. initial infection vector malware families used to install subsequent payloads.

Image 1: ARS VBS Loader's administrative login portal.***Image 1:*** *ARS VBS Loader's administrative login portal.*
The new loader has been spammed out in email attachments enticing victims with lures in subject lines related to personal banking, package shipments, and toll road notifications. Should a victim interact with the attachment and launch it, analysts say numerous types of commodity malware could be installed, including the AZORult information-stealing malware. AZORult was also used in campaigns targeting more than 1,000 Magento admin panels; in those attacks, the malware was used to scrape payment card information from sites running the popular free and open source ecommerce platform.

ARS VBS Loader targets only Windows machines and supports Windows 10, according to posts to a Russian-speaking forum going back to December. Previously, another loader called FUD ASPC Loader, first advertised in May 2017, contained similar functionality but not Windows 10 support.

The loader is also likely to side-step detection by signature-based antivirus and intrusion detection systems because of the relative ease in which attackers can obfuscate VBScript, Flashpoint analysts said. Obfuscation through a variety of means allows attackers to hide malware; if the malware is obfuscated with encryption or packing, it's exponentially more difficult for antivirus to sniff out malicious code, for example.

Once the ARS VBS Loader executes on a victim's computer, it immediately creates a number of entries in nearly a dozen autorun locations, including registry, scheduled tasks, and the startup folder, ensuring persistence through reboots. ARS VBS Loader will connect to the attacker's server, sending it system information such as the operating system version name, computer user name, RAM, processor and graphics card information, a randomly generated ID for infection tracking, and machine architecture information.

Image 2: ARS VBS Loader submits check in information to the C2 in GET and POST parameters.
Image 2: *ARS VBS Loader submits check in information to the C2 in GET and POST parameters.*
The botmaster, meanwhile, can remotely administer commands to bots through the PHP command-and-control application. Communication with the command-and-control server is carried out in plaintext over HTTP, making it easy to spot, Flashpoint analysts said.

The malicious code that runs on the victim's machine is written entirely in VBScript and contains functionality for updating and deleting itself, and deploying plugins such as a credentials stealer, or launching application-layer denial-of-service (DoS) attacks against websites, and loading additional malware from external websites.

The most common command spotted by analysts is download, which instructs bots to download and execute malware from a supplied URL. There is also the plugin command where plugins that steal passwords or capture desktop screenshots can be pushed to

compromised computers.

The DDoS command is also noteworthy because it's a unique capability; analysts said they have not seen this command used in the wild. The command tells bots to send a specified amount of HTTP POST requests to a particular URL. Since this is a simple application layer flooding attack, it is currently unknown how successful this attack would be against targets in the wild, analysts said, adding that it would be easy to spot such traffic because the same hardcoded POST values are sent in the HTTP flood.

 Image 3: Example DDoS HTTP flooding traffic from an infected bot.***Image 3:*** *Example DDoS HTTP flooding traffic from an infected bot.*

Analysts caution that users should be vigilant about not opening email attachments from unknown sources, and that it's likely ARS VBS Loader will continue to be an effective initial infection vector for spam campaigns.

To download the indicators of compromise (IOCs) for the ARS VBS Loader, click here.

To download the Yara rule for the ARS VBS Loader, click here.