Elegant sLoad Carries Out Spying, Payload Delivery in BITS

By Tara Seals

Published: 2019-12-13 · Archived: 2026-04-05 19:12:47 UTC

The BITS file-transfer component of Windows as a key piece of sLoad's attack methodology.

A fresh analysis of the trojan sLoad sheds light on the growing trend of advanced malware "living off the land" of a targeted system and successfully evading detection and carrying out malicious activities.

SLoad is a PowerShell downloader type of malware and is known for its impressive reconnaissance tactics and targeting efforts. But what makes it unique to researchers is an almost exclusive use of a legitimate Windows file transfer utility for data exfiltration, payload fetching and command-and-control (C2) communications.

"SLoad is just one example of the increasingly more prevalent threats that can perform most of their malicious activities by simply living off the land," wrote Sujit Magar, an APT researcher with Microsoft, in an analysis of the malware posted on Thursday.

First spotted in May 2018, sLoad has been seen delivering a variety of payloads, including the Ramnit and Ursnif banking trojans, Gootkit, DarkVNC and PsiXBot, among others. According to Magar, it uses the Background Intelligent Transfer Service (BITS) component of Windows as a key piece of its attack methodology.

A hallmark of sLoad is its penchant for spying on system information and learning about a target before delivering its payload. According to a previous Proofpoint analysis, the malware gathers information about the infected system, including a list of running processes, the presence of Outlook, and the presence of Citrix-related files. It will also take screenshots of the target machine. By using loaders that can also assess infected systems, actors can select their targets wisely and improve the quality of infected hosts, Proofpoint noted.

In Microsoft's analysis, Magar said that sLoad abuses BITS as an alternative protocol to perform data exfiltration and most of its other malicious activities, "enabling the malware to evade defenders and protections that may not be inspecting this unconventional protocol."

A BITS Player

BITS allows the transfer of files using idle bandwidth, which increases the efficiency of a user's internet connection; legitimate users can thus make sure that certain services, such as VoIP calls or instant messaging, are prioritized in terms of bandwidth over file transfers. To carry out its functions, BITS creates self-contained "jobs" that can be prioritized and queued up, designated as either downloads or uploads. When a job is successfully sent, the receiving party sends back a file as a handshake response.

This process is perfect for sLoad, which infects victims using cascaded scripts, according to the Microsoft analysis.

"One script drops or downloads one or more scripts, passes control to one of these scripts, and repeats the process multiple times until the final component is installed," Magar explained. "In one campaign, the first-stage PowerShell code itself uses…a BITS job to download either the sLoad script and the C2 URL file, or the sLoad dropper PowerShell script [with the script and URL file embedded]."

Once installed, the sLoad PowerShell script (the final component) then continues to abuse BITS to carry out various nefarious activities. For instance, Magar said that it creates BITS download jobs to test its connections to C2 URLs to find one that's active – it sends out jobs until it gets a response from a server.

"It then saves the URL that responds in the form of a file…being downloaded as part of created BITS job," according to the research. "This ensures that the handshake is complete."

Once the C2 connection is established, sLoad proceeds to carry out its recon activities; it collects the system information mentioned earlier, then creates a BITS download job using the URL for the active C2 (in BITS, this goes into the "RemoteURL" parameter – i.e., the destination for the file transfer). sLoad also embeds the stolen system information into that same parameter.

"Creating a BITS job with an extremely large RemoteURL parameter that includes non-encrypted system information stands out and is relatively easy to detect," Magar said. "However, this malware's use of a download job instead of an upload job is a clever move to achieve stealth."

Once the malware sends off the BITS download job, it will receive a response in the form of a file downloaded back to the machine – and this is an opportunity for the C2 to send over additional payloads.

"The malware creates another BITS download job to download this payload, creates a copy of this newly downloaded encoded file, and uses another Windows utility, certutil.exe, to decode it into a portable executable (PE) file with .exe extension," according to the analysis. "Finally, it uses PowerShell.exe to run the decoded PE payload. One more BITS download job is created to download additional files."

For the screenshot function, sLoad uses a BITS upload job to send the stolen screenshots to the active C2.

"This is the only time that it uses an upload job, and these are the only files it uploads to the C2," Mager said. "Once uploaded, the screenshots are deleted from the machine."

In all, sLoad's use of BITS is an elegant way to evade detection, according to Magar.

"sLoad is…a dangerous threat that's equipped with notorious spyware capabilities, infiltrative payload delivery and data exfiltration capabilities," the analysis concluded. "While it drops some malware files during installation, its use of only BITS jobs to perform most of its harmful behaviors and scheduled tasks for persistence achieves an almost fileless presence on compromised machines."
