Hacked Steam accounts spreading Remote Access Trojan

By Lawrence Abrams

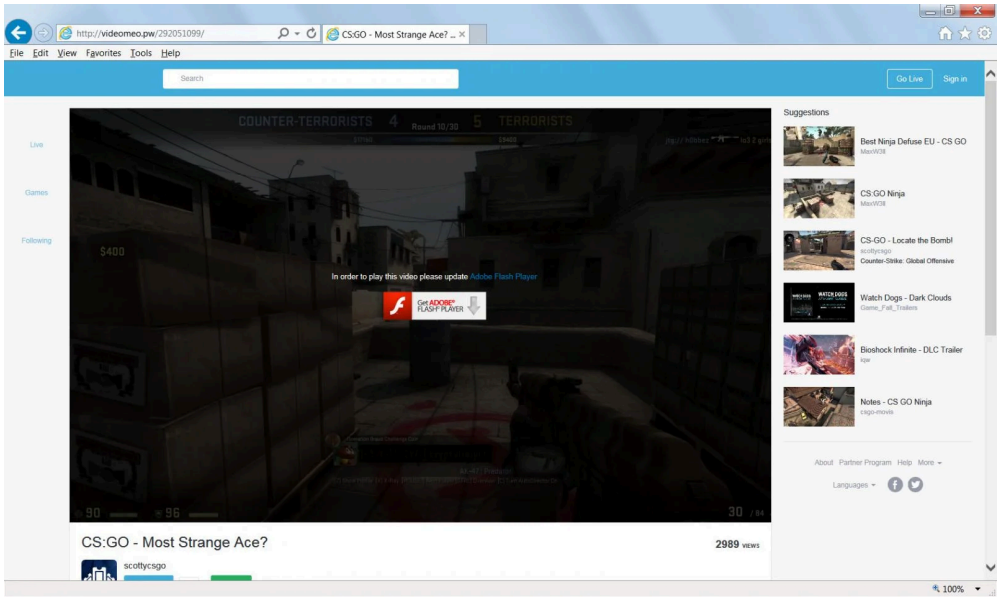
Published: 2016-10-01 · Archived: 2026-04-05 15:43:11 UTC

Yesterday, I stumbled on a post where a Reddit user named Haydaddict was alerting people about some hacked Steam accounts spreading malware. As I am always interested in new malware, I took a look to see what could be discovered.

According to the post, the hacked accounts were being used to SPAM suspicious links using Steam chat. These chat messages would tell the recipient to go to videomeo.pw to watch a video.

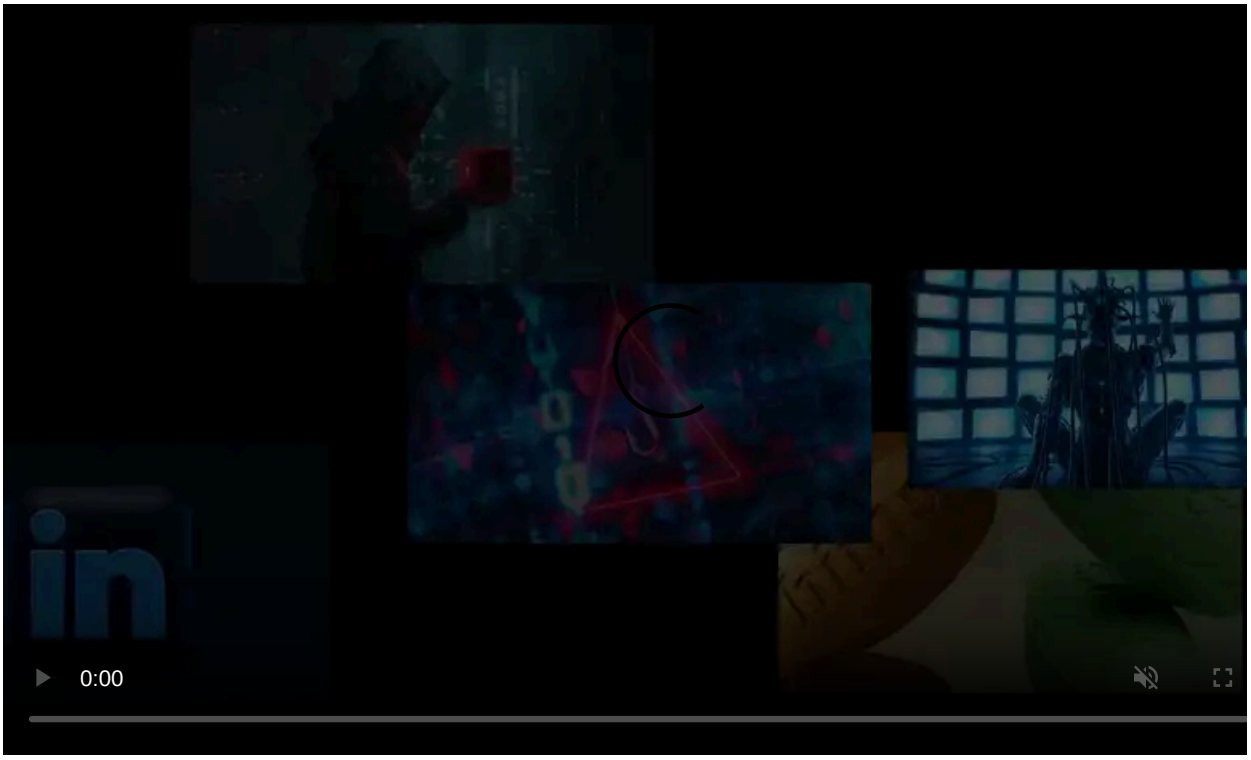
Steam Chats

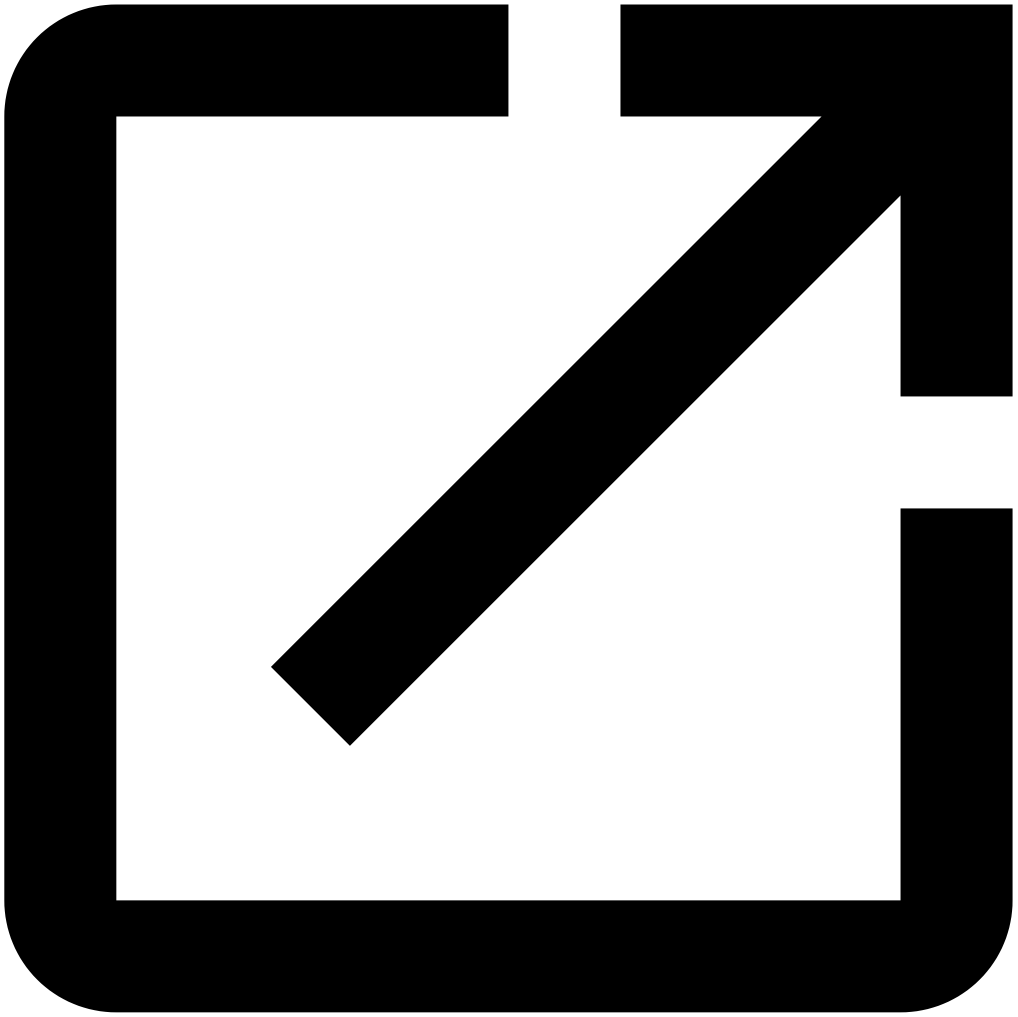
When the target went to the page, they would be greeted with a message stating that they needed to update Flash Player in order to watch the video.

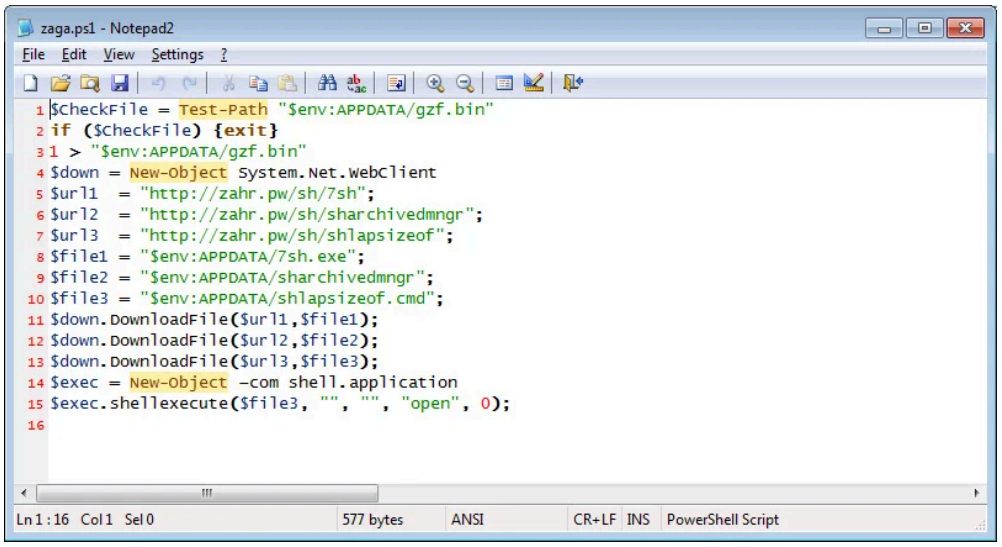


Fake Video Page

If a target downloads the installer and executes it, they will find that it does not appear to do anything. This is because the Flash Player installer is actually a Trojan that executes a PowerShell script called zaga.ps1, which will download a 7-zip archive, 7-zip extractor, and a CMD script from the zahr.pw server.


0:00

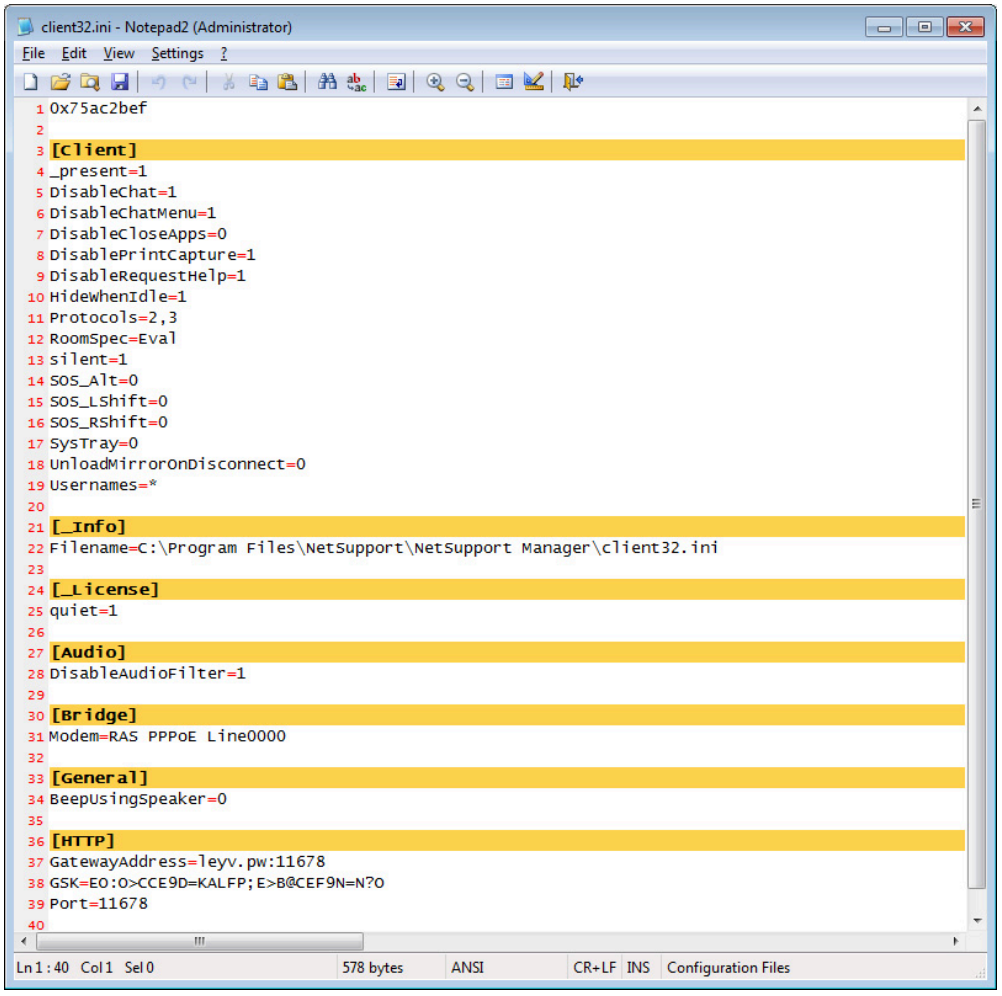




Zaga.ps1 PowerShell Script

Once the files are downloaded, the PowerShell script will then launch the CMD file, which will extract the **sharchivedmngr** to the **%AppData%\lappclimtfldr** folder and configure Windows to automatically start the **mcrtvclient.exe** program when a user logs in. This program is actually a renamed copy of the NetSupport Manager Remote Control Software.

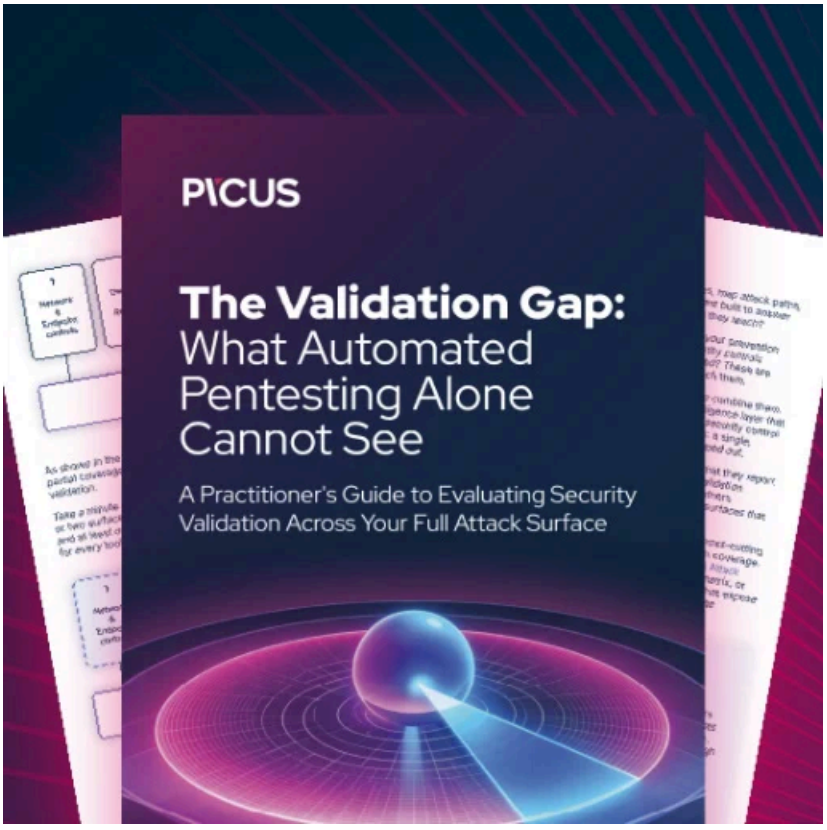
When the program is launched, it will connect to the NetSupport gateway at leyv.pw:11678 and await commands. This allows the attacker to remotely connect to the infected computer and take control over it.



NetManager Configuration File

For those who are concerned they are infected with this Steam Trojan, I suggest they check the %AppData% folder for the specified folders.

Furthermore, all users must be careful with what links they visit and what downloads they install. These days it is becoming more and more frequent for accounts to be hacked and then for attackers to use them to distribute malware. Stay vigilant, be careful, and make sure you have an antivirus software installed.



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/security/hacked-steam-accounts-spreading-remote-access-trojan/