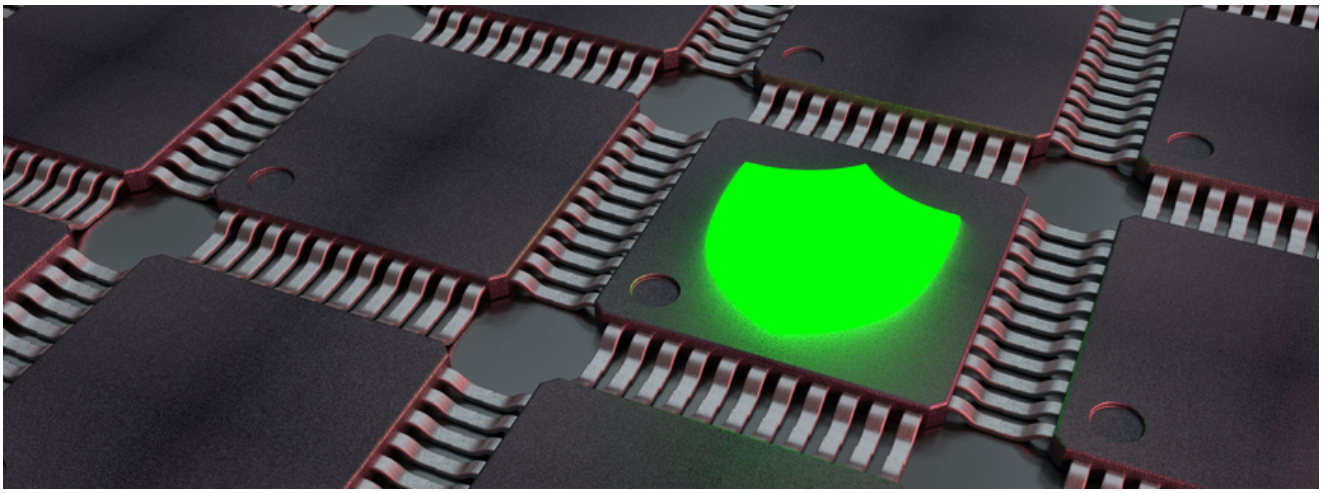
The Sysrv-hello Cryptojacking Botnet: Here's What's New

riskiq.com/blog/external-threat-management/sysrv-hello-cryptojacking-botnet/

June 4, 2021



External Threat Management Labs

June 04, 2021

By Team RiskIQ

Cryptojacking botnets can earn their operators millions by discretely stealing CPUs on infected machines to mine coins, especially with the sky-high value of today's cryptocurrencies. Sysrv-hello, a cryptojacking botnet first identified by Alibaba Cloud Security in late December 2020, is another of these money-making malware variants.

The Sysrv-hello botnet is deployed on both Windows and Linux systems by exploiting multiple vulnerabilities and deployed via shell scripts. Like many of the threat actor tools we've covered, it continuously evolves to fit the needs of its operators and stay ahead of security researchers and law enforcement.

Over time, there have been several slight changes in the shell scripts that install the Sysrv-hello implant on machines. There have also been incremental changes in how the executable gets deployed on host systems. In our latest threat intel analysis, RiskIQ researchers have identified one of its latest developments, including the use of drive-by downloads and two new Monero wallets.

Evolution of ldr.sh Shell Script

The latest iteration of Sysrv-hello is deployed via drive-by-downloads from an empty iframe that points to an executable that will download to the host system when a user visits that web page. The iframe was set up via a Python script.

Most observed versions of Sysrv-hello are deployed via shell script. On Linux systems, the host is initially infected with the bash script before downloading the second stage ELF binary. You can see the list of files as observed by RiskIQ, many not previously reported on in open source, by visiting our complete analysis article in the Threat IntelligencePortal.

The first shell scripting file had more basic functionality than later observed files. Its functions included killing prior versions of Sysrv, killing other miners, and, after they reported on Sysrv-hello in December 2020, removing Ali Baba (aka Aliyun) services. All of these samples specified a specific crypto wallet, which you can explore in the complete analysis.

RiskIQ also observed additional files about which we have less information than those mentioned above. However, from a shared IP address, MD5 hashes listed in the response banners collected by RiskIQ systems were found in VirusTotal—three out of the five were flagged as Linux Coinminers.

In April 2021, RiskIQ identified two more files on known Sysrv-hello C2 servers with much more extensive shell scripts than any previously observed. We are in the process of performing more analysis on these scripts, but both used a wallet that had never been reported in opensource.

As observed within the RiskIQ OSINT tab of our Threat Intelligence Portal, Palo Alto reported that one of these C2s is associated with the "WatchDog" mining operation. No further information is known about any relationships between the "WatchDog" and the "Sysrv-hello" mining operations. Still, a function of one of the Sysrv-hello scripts mentioned above included a function that killed processes called “watchdogs."

The scripting files obtained by RiskIQ include both a Sysrv IP reported on by Juniper Networks, and a WatchDog domain reported on by Palo Alto. More research is needed to determine the relationship between these two IOCs and compare the shell scrip[t deployed by both mining operations.

Say Goodbye to Sysrv-hello

RiskIQ's Internet Intelligence Graph gives security teams a universal view of the internet, enabling our customers to detect many of the CVE's that Sysrv-hello exploited reported on by Juniper and Laceworks. With RiskIQ's Enterprise Digital Footprint, customers can identify assets that may be vulnerable to many of these exploits.

Visit our Threat Intelligence Portal for our full technical analysis of **Sysrv-hello** and more information about its ties to other cryptojacking campaigns. To find out how RiskIQ can defend your organization's digital attack surface, get started today.

Subscribe to Our Newsletter

Subscribe to the RiskIQ newsletter to stay up-to-date on our latest content, headlines, research, events, and more.

Base Editor