cisco | Talos

2023 HALF YEAR IN REVIEW

Here are the main threats we've covered on blog.talosintelligence.com up until the end of June 2023. The timeline is a blend of threat advisory articles, and long-term research.

January

Talos THREAT SPOTLIGHT

Following the LNK metadata trail

Talos observed threat actors moving away from malicious macros as an initial access method, in favor of other types of executable attachments, such as the Shell Link binary file format (LNK files).

Read more.

February

New MortalKombat ransomware and Laplas Clipper malware observed

Talos observed an unidentified actor deploying two new threats: The recently discovered MortalKombat ransomware and a GO variant of the Laplas Clipper malware. The nature of these threats is to steal cryptocurrency from victims.

Read more.

March

Talos THREAT SPOTLIGHT

Prometei botnet improves modules and exhibits new capabilities

Talos observed the Prometei botnet updating certain submodules of the execution chain to automate processes, and challenge forensic analysis methods.

Read more.

2023 HALF YEAR IN REVIEW

cisco | Talos

March

Talos uncovers espionage campaigns targeting CIS countries, embassies, and EU health care agency

Talos identified a new threat actor which we named, "YoroTrooper," that ran several successful espionage campaigns. The actor appears intent on exfiltrating documents and other information, for use in future operations.

Read more.

March

THREAT ADVISOR

Microsoft Outlook privilege escalation vulnerability being exploited in the wild

Talos urged all users to update Microsoft Outlook after the discovery of a critical vulnerability, CVE-2023-23397, in the email client that attackers were actively exploiting in the wild

Read more.

March

Emotet resumes spamming operations, targeting OneNote

Since returning, Emotet used several distinct infection chains, indicating that they are modifying their approach based on their perceived success in infecting new systems.

Read more.

March

3CX Softphone Supply Chain Compromise

A supply chain attack affecting Windows and MacOS users of the 3CX software-based phone application became known in March. This attack leveraged the legitimate update functionality of the 3CX application to deliver a set of malicious payloads to 3CX users.

Read more.

2023 HALF YEAR IN REVIEW

cisco | Talos

April

Typhon Reborn V2: Updated stealer features enhanced capabilities

In April, Talos wrote about our growing concerns over Version 2 of the information stealer Typhon. The latest version features additional anti-analysis and anti-virtual machine capabilities to evade detection and make analysis more difficult.

Read more.

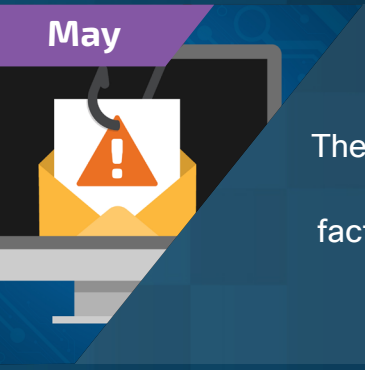
State-sponsored campaigns target global network infrastructure

Talos wrote about how we had become increasingly concerned with the increase in the rate of high-sophistication attacks on network infrastructure. While working with network infrastructure in various parts of the world, we observed both espionage and obvious targeting to support future destructive attacks.

Read more.

April

May



New phishing-as-a-service tool "Greatness"

The previously unreported phishing-as-a-service (PaaS) "Greatness" incorporates features seen in some of the most advanced PaaS offerings, such as multi-factor authentication (MFA) bypass, IP filtering and integration with Telegram bots.

Read more.

Newly identified RA Group compromises companies in U.S. and South Korea

Talos discovered a new ransomware actor called RA Group that has been operating since at least April 22, 2023. Since that date, the actor swiftly expanded its operations.

Read more.

May

2023 HALF YEAR IN REVIEW

cisco | Talos

May

Mercenary mayhem: A technical analysis of Intellexa's PREDATOR spyware

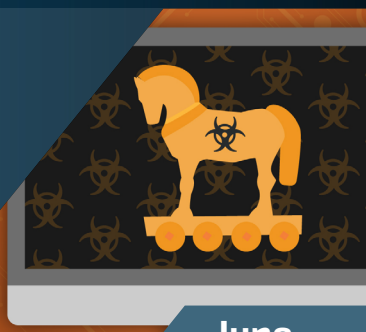
Commercial spyware use is on the rise, with actors leveraging these sophisticated tools to conduct surveillance operations against a growing number of targets. In May, Talos disclosed added details of a commercial spyware product sold by the spyware firm Intellexa (formerly known as Cytrox).

Read more.

New Horabot campaign targets the Americas

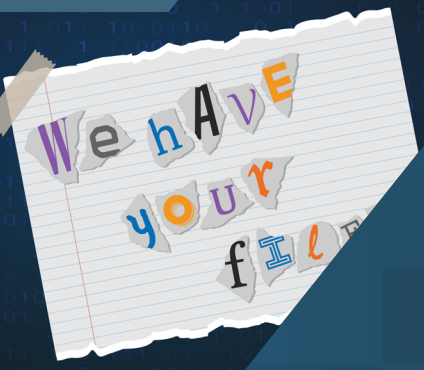
Talos observed a threat actor deploying a previously unidentified botnet program Talos is calling “Horabot,” which delivers a known banking trojan and spam tool onto victim machines in an ongoing campaign.

Read more.



June

June



Active exploitation of the MOVEIt Transfer vulnerability by Clop ransomware group

Talos is monitoring recent reports of exploitation attempts against CVE-2023-34362, a SQL injection zero-day vulnerability in the MOVEit Transfer managed file transfer (MFT) solution that has been actively targeted since late May 2023.

Read more.

Read the Talos blog

Follow us on Twitter, LinkedIn and Mastodon

Subscribe to the weekly Threat Source Newsletter