UKRAINE

DOWNLOAD THE FULL REPORT HERE

Talos' ongoing support for Ukraine has been a large focus of our operational efforts this year. Driven by our core mission of protecting the Ukrainian people and infrastructure, Talos launched a task force of 40+ volunteers dedicated to defending our customers and partners within. This team of experts monitors critical infrastructure customers to identify threats, remediate attacks, and gather information.

TOP ADVERSARIES AND THREATS

The following list represents a snapshot of the adversaries and threats Talos observed targeting Ukranian entities and their allies in 2022:

- Leading up to and following the invasion, we saw a variety of destructive wipers and other malware against Ukrainian targets, including WhisperGate, HermeticWiper, CaddyWiper, DoubleZero, and CyclopsBlink.
- Cybercriminals exploited the situation by advertising offensive cyber tools that were actually malware to target Russian entities and used email lures with themes relating to the crisis to conduct financial scams and deliver remote access trojans.
- Russian state-sponsored group Gamaredon distributed information-stealing malware, and a suspected state-sponsored actor attempted a supply chain attack attempt dubbed GoMet.
- The China-based threat actor Mustang Panda conducted phishing campaigns against entities in Europe and Russia using fake " official" documents as lures.
- The Russia-aligned hacktivist group Killnet launched denial-of-service attacks against websites within pro-Ukraine countries.

BEHAVIOR TRENDS

Based on data we have collected since the beginning of 2022, we have seen the following trends indicative of adversary behaviors that are active in Ukraine:

- Common utilities like PowerShell and Windows Management Instrumentation (WMI) remain a top target of adversaries looking to "live off the land" and evade detection.
- Techniques like utilizing Google Chrome executables and using Windows Policies Keys to establish persistence were seen in greater numbers.
- An observed increase in information stealer and cryptocurrency miner detections. However, we see actors across the sophistication

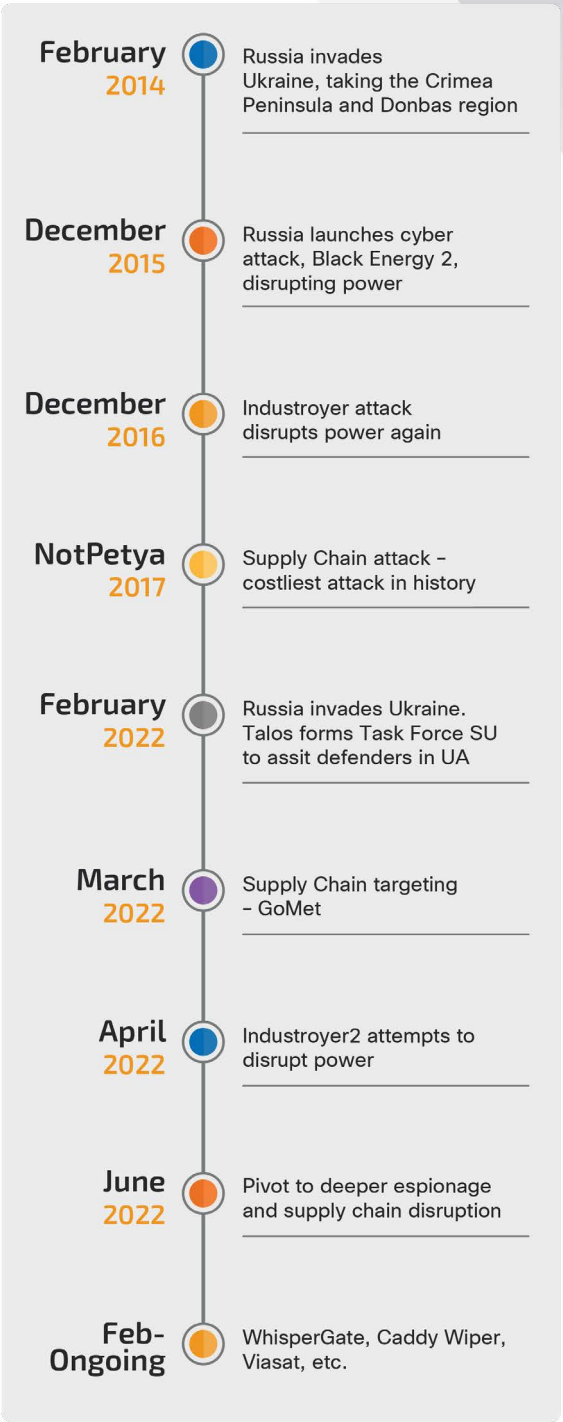

Figure 1: *Major cyber attacks against Ukraine.*

UKRAINE

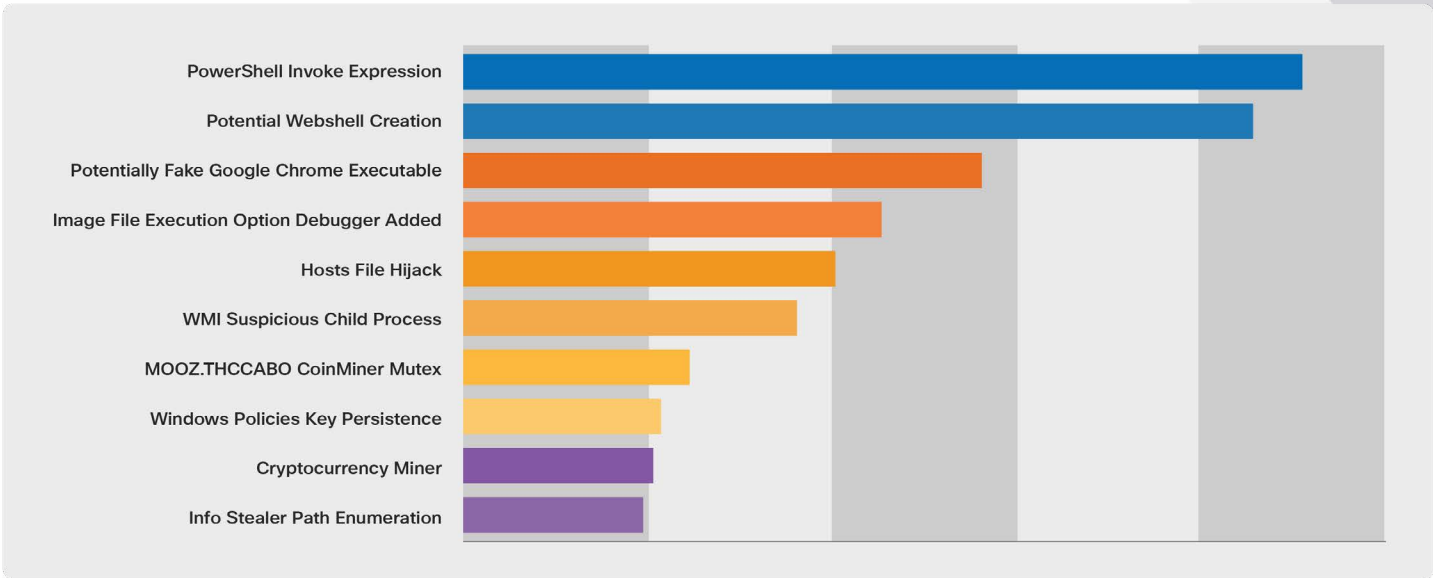

Figure 2: *Most active Behavioral Protections rules from Cisco Secure Endpoint across Ukrainian customers where Cisco Secure Endpoint has been deployed.*

spectrum with destructive activity as the main objective.

- We have observed a spike in alerts for "Signed binary proxy execution using rundll32" within Ukraine, but also on a global level. This technique abuses the dynamic link library (DLL) to run malicious code.

Despite the increased activity against targets in Ukraine, our incident response team observed fewer threats against Cisco customers in general during the first half of 2022. It is possible that the conflict has drawn in threat actors that would otherwise be conducting attacks elsewhere.

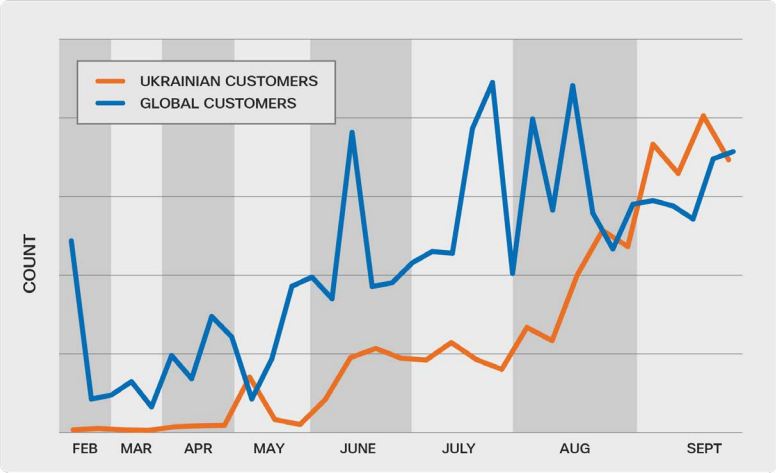

Figure 3: *Exploit Prevention detections for "Signed binary proxy execution using rundll32" across Ukrainian customers and global customers, Feb.–Sept. 2022*

CONCLUSION

There is no indication that the cadence of cyber attacks against Ukraine is slowing, nor will the cyber conflict necessarily end with any cessation of hostilities. Regional tensions and the diversity of the threat actors embroiled in the conflict suggests that attacks against Ukraine will probably continue. Furthermore, we assess Russian cyber threat actors will likely conduct destructive attacks as necessary to affect the outcome of the war.