UKRAINE

LADEN SIE HIER DEN VOLLSTÄNDIGEN ENGLISCHEN BERICHT HERUNTER

Die kontinuierliche Unterstützung von Talos für die Ukraine war in diesem Jahr ein großer Schwerpunkt unserer operativen Bemühungen. Angetrieben von unserer Kernaufgabe, die ukrainische Bevölkerung und die Infrastruktur zu schützen, hat Talos eine Task Force mit mehr als 40 Freiwilligen ins Leben gerufen, die sich für den Schutz unserer Kunden und Partner im Land einsetzt. Dieses Expertenteam überwacht Kunden kritischer Infrastrukturen, um Bedrohungen zu identifizieren, Angriffe einzudämmen und Informationen zu sammeln.

DIE WICHTIGSTEN ANGREIFER UND BEDROHUNGEN

Die folgende Liste ist eine Momentaufnahme der Angreifer und Bedrohungen, die Talos 2022 gegenüber ukrainischen Organisationen und ihren Verbündeten beobachtet hat:

- Im Vorfeld des Angriffs und danach traten zahlreiche destruktive Wiper und andere Malware gegen ukrainische Ziele auf, darunter WhisperGate, HermeticWiper, CaddyWiper, DoubleZero und CyclopsBlink.
- Cyberkriminelle nutzten die Situation aus, indem sie offensive Cyber-Tools bewarben, bei denen es sich tatsächlich um Malware für Angriffe auf russische Organisationen handelte, und E-Mail-Köder mit Inhalten im Zusammenhang mit der Krise nutzten, um Finanzbetrug zu begehen und Remote-Access-Trojaner zu verbreiten.
- Die vom russischen Staat finanzierte Gruppe Gamaredon verbreitete Malware zum Informationsdiebstahl, und ein mutmaßlicher staatlich unterstützter Akteur versuchte einen Lieferkettenangriff mit dem Namen GoMet.
- Der in China ansässige Bedrohungsakteur Mustang Pandas führte Phishing-Kampagnen gegen Organisationen in Europa und Russland durch und nutzte dabei gefälschte „offizielle“ Dokumente als Lockmittel.
- Die mit Russland im Zusammenhang stehende Hacktivistengruppe Killnet startete Denial-of-Service-Angriffe auf Websites in Ländern, welche die Ukraine unterstützen.

VERHALTENSTRENDS

Basierend auf Daten, die wir seit Anfang 2022 gesammelt haben, haben wir die folgenden Trends beobachtet, die auf Angreiferverhalten in der Ukraine hindeuten:

- Weit verbreitete Dienstprogramme wie PowerShell und Windows Management Instrumentation (WMI) sind nach wie vor ein Hauptziel von Angreifern, die Computer-interne Ressourcen nutzen und die Erkennung umgehen möchten.

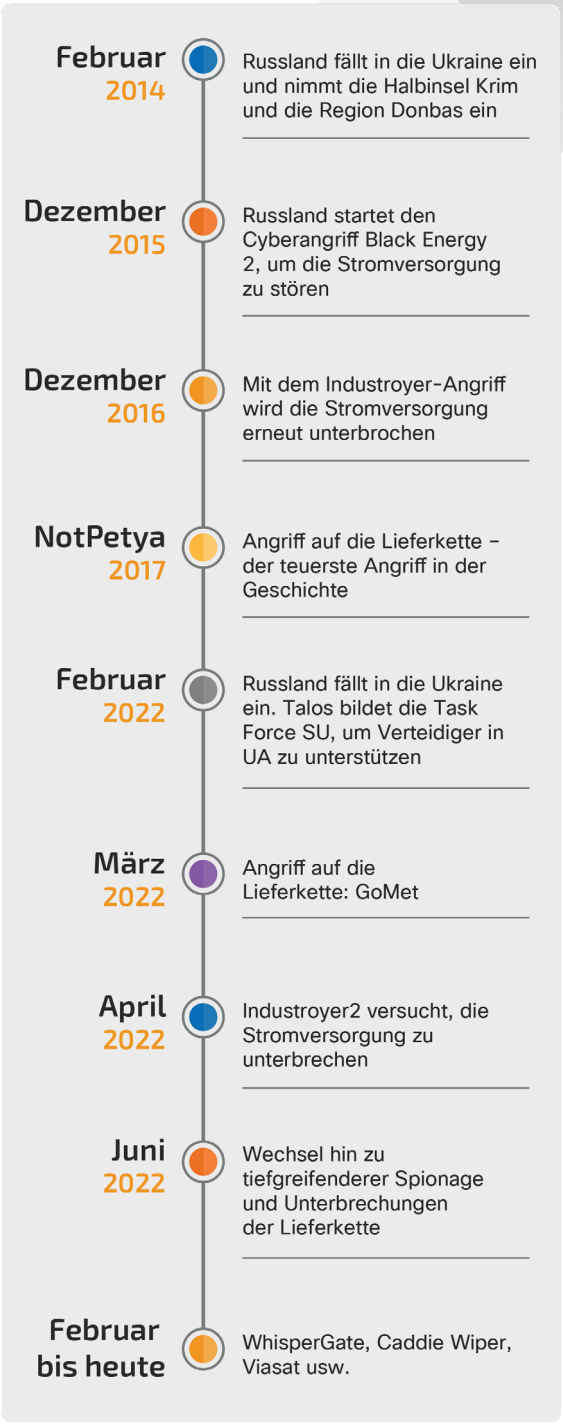

Abbildung 1: *Schwerwiegende Cyberangriffe auf die Ukraine.*

UKRAINE

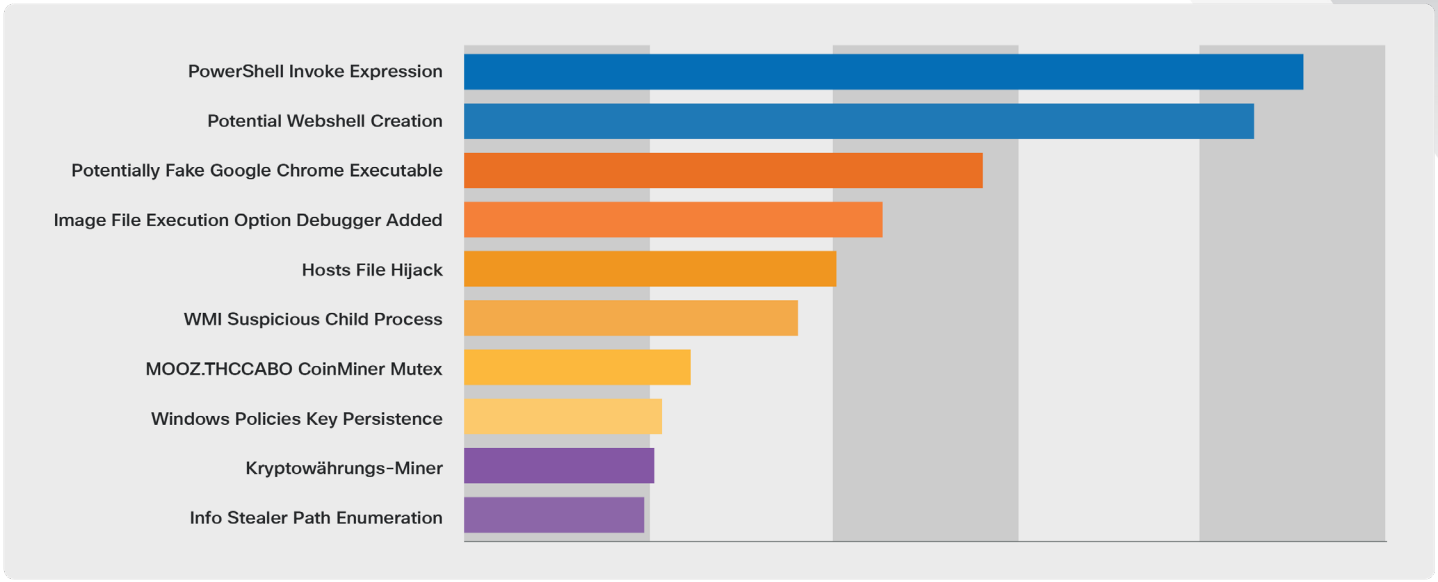

Abbildung 2: *Die aktivsten Behavioral Protection-Regeln von Cisco Secure Endpoint bei Kunden in der Ukraine, bei denen Cisco Secure Endpoint bereitgestellt wurde.*

- Techniken wie die Verwendung ausführbarer Dateien von Google Chrome und die Verwendung von Windows-Richtlinienschlüsseln zur Erreichung der Persistenz wurden häufiger beobachtet.
- Außerdem nahmen die Erkennungen von Information Stealern und Kryptowährungs-Minern zu. Allerdings erkennen wir Akteure aus dem gesamten Komplexitätsspektrum mit destruktiven Aktivitäten als Hauptziel.
- Wir haben in der Ukraine, aber auch auf globaler Ebene, einen Anstieg der Warnungen für die Ausführung eines signierten binären Proxys mit rundll32 beobachtet. Diese Technik missbraucht die Dynamic Link Library (DLL), um schädlichen Code auszuführen.

Trotz der verstärkten Aktivitäten gegen Ziele in der Ukraine beobachtete unser Incident-Response-Team im ersten Halbjahr 2022 im Allgemeinen weniger Bedrohungen für Cisco Kunden. Möglicherweise hat der Konflikt Bedrohungsakteure angezogen, die sonst an anderer Stelle Angriffe durchführen würden.

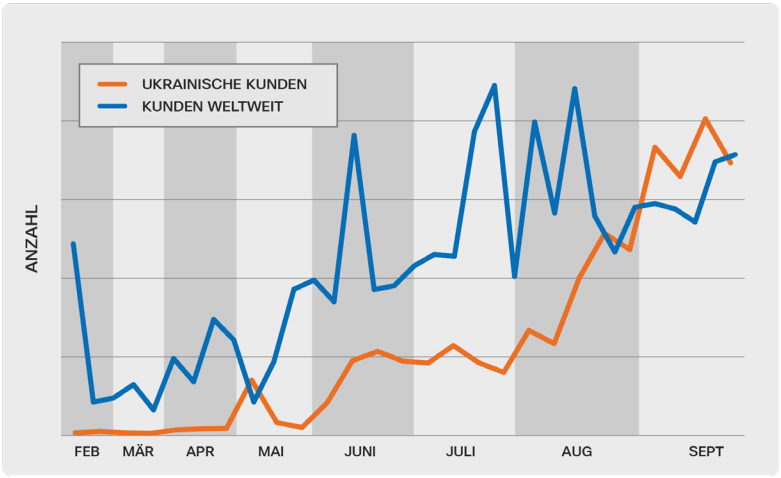

Abbildung 3: *Exploit-Präventions-Erkennungen für „Signed binary proxy execution using rundll32" bei Kunden in der Ukraine und weltweit, Feb. – Sept. 2022.*

FAZIT

Es gibt keine Anzeichen dafür, dass sich die Zahl der Cyberangriffe auf die Ukraine verlangsamt, noch wird der Cyberkonflikt zwangsläufig mit einer Einstellung der Kriegshandlungen enden. Regionale Spannungen und die Vielfalt der Bedrohungsakteure deuten darauf hin, dass die Angriffe auf die Ukraine wahrscheinlich weitergehen werden. Darüber hinaus gehen wir davon aus, dass die russischen Cyber-Bedrohungsakteure wahrscheinlich zerstörerische Angriffe durchführen werden, um den Ausgang des Krieges zu beeinflussen.

