THREAT BULLETINS

Cisco Talos Releases Executive Guidance for Ongoing Cyberattacks in Ukraine as United States Increases Sanctions

TLP:WHITE

Feb 26, 2022

Cisco Talos has released strategic analysis for executives to respond and potentially prevent damages and fallout from the ongoing conflict in Ukraine. The report, Executive Guidance for Ongoing Cyberattacks in Ukraine, contains observed methodologies, techniques, tactics, and procedures being utilized by both military and pro-Russian entities online in order to disrupt and destroy critical online infrastructure in Ukraine. The report comes as the United States government imposes new sanctions aimed directly against Russian President Vladimir Putin.

Health-ISAC is releasing this intelligence report for your increased geopolitical and security awareness. The Cisco Talos report, which can be accessed here, and its subsequent analysis have been included in this alert for your reference. Health-ISAC continues to

follow the situation closely and will potentially release future intelligence reports when appropriate. Included in this report are several sections of strategic analysis, tactics observed, and additional information regarding previous alerts. Health-ISAC's previous Threat Bulletin, Russia Invades Ukraine; Cyberattacks Observed; Recommendations and Remediation Strategies Released, can be accessed here via the Health-ISAC Threat Intelligence Platform (HTIP)

Talos is observing a variety of threats targeting Ukraine, including disinformation, defacements, DDoS, wiper malware, and potential BGP manipulation. For the previous Talos information on WhisperGate see here.

Cisco continues to observe distributed denial-of-service (DDoS) attacks against Ukrainian entities amid heightened tensions. This activity represents a continued effort to disrupt services in Ukraine and sow discord among the population.

On February 15, 2022, several high-level Ukrainian targets, including their Ministry of Defense and two large national banks, were targeted with DDoS attacks. The banks' services were disrupted for several hours. Although the attacks did not affect the targets critically, it was still successful in alarming Ukrainian citizens as tensions increased. These attacks were attributed to Russia by Ukraine, the UK, and the US. They appeared to leverage a variant of the Mirai botnet, which has been previously associated with orchestrating disruptive DDoS attacks.

As recently as February 23, 2022, DDoS attacks were confirmed causing network disruptions and affecting high-profile government entities in Ukraine, such as Ukraine's Ministry of Foreign Affairs, Ministry of Defense, Ministry of Internal Affairs, and national banks, among others, illustrating that Russia will likely continue to rely on these types of attacks.

Around the same time of the DDoS attacks, the Ukrainian Computer Emergency Response Team (CERT-UA) asserted that there was a BGP hijacking attack against a Ukrainian bank. This potentially allowed traffic that was intended to reach the bank to reroute temporarily to another destination. BGP, or Border Gateway Protocol, is the primary traffic-routing mechanism on the internet.

CISA released a report on February 23, 2022, outlining a new malware dubbed Cyclops Blink, which appears to be a replacement

framework for the VPNFilter malware Talos discovered several years ago.

Looking Forward

The analysis provided below is based on Cisco's long-term work in Ukraine and Eastern Europe. This analysis represents Cisco's best-effort factual statements at the time of publication with the goal of preparing defenders to protect their networks and users. Keep in mind that organizations being targeted may not be directly tied to critical infrastructure or government but could be a partner/trusted organization used as a foothold or staging ground for malicious content to be used in further attacks.

Based on different objectives in each arena and the way adversaries perceive the capabilities of both targets, it is important to highlight that there will be differences in how Western nations and allies may be targeted and the level of conflict currently occurring in Ukraine.

Cyber operations in the West intended to erode popular support for sanctions against Russia and impose or highlight costs associated with those sanctions, are possible. These operations would likely come in forms that target critical infrastructure that are high-impact, but relatively easy to recover from. For example, looking at the lessons learned in the Colonial Pipeline ransomware incident, if an adversary disables key enterprise systems while leaving the operational technology (OT) systems fully intact, they can still cause an outage, though one that will not be overly destabilizing.

Cyber operations against Ukraine, by contrast, have escalated to include destructive malware attacks, DDoS attacks, BGP manipulation, and other operations designed to disrupt public order and everyday life for Ukrainian citizens.

We can expect to see adversaries use techniques consistent with past behavior, but technical indicators will be new and difficult to attribute. Cisco assess that these actors would likely abuse elements of complex systems to achieve their objectives on targeted environments. Past examples of this include the use of Ukrainian tax software to distribute NotPetya malware in 2017 and, more recently, the abuse of SolarWinds to gain access to high-priority targets.

It is also important to understand that any attacks will likely have elements that interfere with attribution and may have parallel disinformation campaigns to amplify the effect. For example, it may

be that a bank website experiences an outage from a DDoS attack, while false rumors of ATM outages are amplified on social media to maximize discomfort in the target country.

Organizations should understand that when looking at this particular set of concerns, they are not the target, they are the tool. The adversary in question will make choices to maximize the public impact of any outage, not to embarrass the affected organization, but to apply pressure to the government.

Reference(s)	Cisco Talos, Cisco Talos, ZDNet, Cisco Talos, Cisco Talos, CNN Money, Cisco Talos, Cisco Talos, Cisco Talos, Washington Post
Credibility	Multiple Sources
Vendors	Cisco

Recommendations
Cisco's current guidance continues to echo the recommendations from the US Cybersecurity and Infrastructure Security Agency (CISA) that global organizations with ties to Ukraine should carefully consider how to isolate and monitor those connections to protect themselves from potential collateral damage.

CISA released additional steps organizations could take to protect themselves. Cisco recommends organizations, especially those in critical infrastructure and government, review CISA's advisory, enable and carefully examine their logs, patch, develop a crisis plan, and implement multi-factor authentication where possible. Cisco also recommends following CISA guidance for safeguarding against foreign influence operations, which Russia previously used against US entities to disrupt critical infrastructure functions.

Sources
Talos: Current Executive Guidance for Ongoing Cyberattacks in Ukraine

CNN: US to Impose Sanctions on Putin Following Ukraine Invasion

Health-ISAC: Russia Invades Ukraine; Cyberattacks Observed; Recommendations and Remediation Strategies Released

Alert ID f61d5b93

View Alert

Tags Russian APT, Ukraine National Police, Russian origin, Sanctions, Russia, Ukraine, Russian

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Access the Health-ISAC Intelligence Portal Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Cyware.

For Questions or Comments Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.

For more update and alerts, visit: **https://health-isac.cyware.com**