Fidelis Cybersecurity

Cyber Effects | Russo-Ukrainian Conflict

Threat Activity and Fidelis Cybersecurity Threat Intelligence

Overview

The Ukrainian region has suffered a string of cyber-attacks against government agencies, the banking community, and defense industries. On 24 February 2022, the situation escalated when Russia employed both physical and cyber force against Ukraine.

As outlined in a US **Cybersecurity & Infrastructure Security Agency** (CISA) advisory, this attack on the Ukrainian government and its critical infrastructure may have far-reaching consequences both within and beyond the region. The **U.S. CISA, Federal Bureau of Investigation (FBI), and National Security Agency (NSA)** (and others) encourage the cybersecurity community – especially critical infrastructure network defenders – to adopt a heightened state of awareness and to conduct proactive threat hunting. Every organization must be prepared to respond to disruptive cyber activity.

What We Are Doing

Fidelis Cybersecurity is dedicated to helping our customers defend their networks against these escalating attacks and emerge stronger and more secure. We are in this together.

To ensure that our customers have the latest information and the most up to date protections for their networks, Fidelis Cybersecurity has established a crisis response team. The focus of this team will be on:

- Tracking and assessing the evolving cyber situation
- Keeping our customers informed of new developments, and
- Ensuring that our detection and response capabilities remain up to date as new threats emerge

Our latest protections are automatically deployed to all customers through our Fidelis Insight Threat Intelligence feed. Information related to evolving threats and our cyber assessments will be shared through our Threat Research pages and our customer support portal.

At this time, the dominant headlines focus on a number of Distributed Denial of Service (DDoS) attacks launched against Ukrainian banks, government agencies, and critical infrastructure. We have seen instances of destructive wiper malware (e.g., WhisperGate) deployed as well. While DDoS attacks will temporarily take websites and networks down, destructive malware can permanently destroy endpoints and servers.

Fidelis Elevate and CloudPassage Halo platforms safeguard data, assets, and services – no matter where they are on your networks or cloud. Based on the observed attacks, the following capabilities can help our customers:

- Fidelis Network Insight Feed DPI rules, which include limited DDoS mitigation support capabilities for customers that do not have upstream mitigation capabilities. These rules include Emerging Threat signatures for detecting Denial of Service threats such as BIND (CVE-2015-5477), Industroyer, Perl IRC DDoS, Apple ICMP (CVE-2019-16928), CallStranger, UpnP Reflected Amplified TCP attacks, and denial of service attacks against OpenSSL TLSv1.2.
- Fidelis Network MDE (Malware Detection Engine) and Fidelis Endpoint AV (Antivirus) detect known variants of WhisperGate and can protect against other forms of destructive malware.
- Fidelis Deception that can provide an early warning of an attack as well as attempts of an attacker to move laterally inside an organization.

We will continue to monitor this situation so we can best help our customers stop threats before they impact business operations. We value our role in helping cyber defenders worldwide shift to proactive cyber defense and become stronger and more secure.

Key Developments

The cyber-attacks in Ukraine have included large scale Distributed Denial of Service (DDoS) attacks against Ukrainian critical infrastructure systems, web site defacement, and the deployment of multiple strains of destructive wiper malware disguised as Ransomware. Fidelis Network MDE and Fidelis Endpoint AV currently detect known iterations of this ransomware. Preliminary analysis of the wiper malware being deployed within the region indicates that MDE is effective at detecting this malware; however, a full assessment is still underway. It is important to note that Fidelis Cybersecurity does not specialize in DDoS mitigation, and we strongly recommend clients seek services and technology that provide upstream DDoS protection to mitigate the DDoS attacks outlined in this advisory.

DOI: 24 February 2022 - Coinciding with the Russian invasion of Ukraine, at approximately 3am local time on Thursday the 24th of February, several key Ukrainian websites were disrupted through a DDoS attack (Figures 1 and 2 below). Among those reported to be impacted were Ukrainian Foreign Ministry, Interior Ministry and Security Services. We are unable to attribute the platform responsible for this DDoS attack at this time; however, we are actively investigating.

Shortly after public reports of the latest DDoS campaign, came additional reporting from multiple sources signaling that these most-recent disruptive attacks likely coincided with the deployment of **HermeticWiper**. Initial analysis indicates that, similar to WhisperGate, the intent of this malware was destruction and not extortion. We are currently analyzing this malware in greater detail to discover additional mitigation opportunities. Fidelis Network MDE and Fidelis Endpoint AV currently detect known iterations of HermeticWiper.

DOI: 15 February 2022 – Ukrainian websites for the Ministry of Defense, and state-affiliated banks were disrupted through a substantial DDoS attack.

Figure 1.

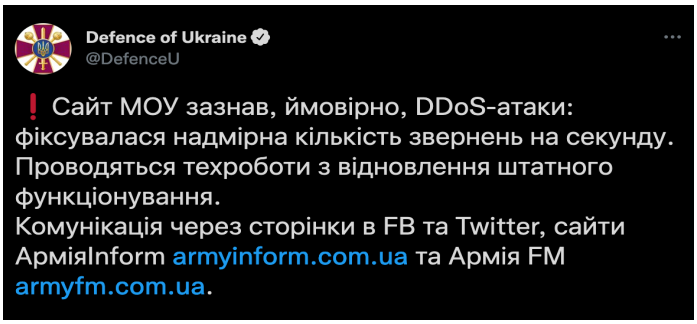

Figure 2.

Disruptive traffic reportedly consisted of a combination of TCP Syn and UDP Flood with a smaller amount of NTP reflection from non-spoofed sources. According to a **single source** claiming direct observation, the observed SYN-flood attack throughput reached a maximum of 1.2 million packets-per-second (mpps), while large-packet UDP flooding attacks reached a maximum of 5.3 Gbps.

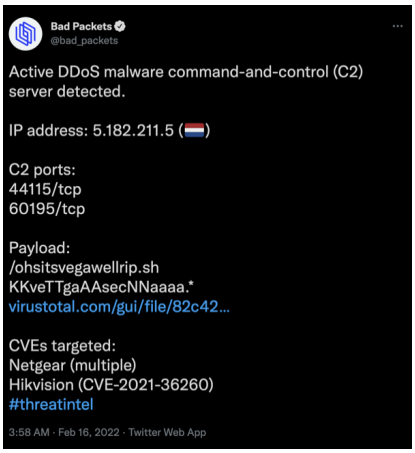

Figure 3.

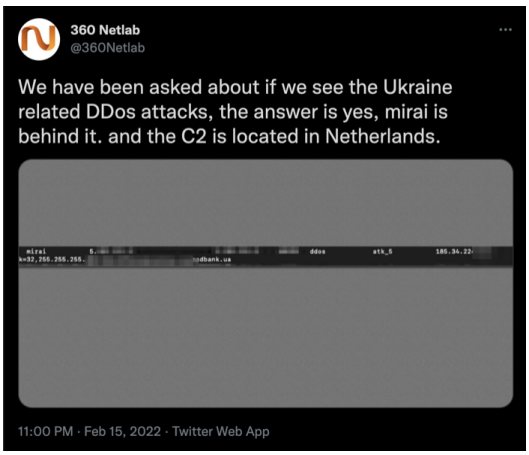

Figure 4.

Multiple sources (Figures 3 and 4 above) report that this attack instance was likely powered by a Mirai variant known as Katana. Additionally, the US National Security Council has attributed the attacks to infrastructure operated by the Russian Foreign Intelligence Service - GRU (Figure 5 below).

Figure 5.

The Mirai source code is publicly available. Katana is not likely applicable to all DDoS instances past and present concerning this conflict, as individual actors can invoke a myriad of options (e.g., criminal botnet infrastructure) towards executing a DDoS campaign. Mirai is a popular choice and most prevalent as of late because it primarily infects SOHO (Small Office/Home Office) routers making its sheer volume of attack power all the more attractive. While the US National Security Council has primarily implicated the mid-February attacks to the GRU, it's important to note that historically Russia has benefitted from the participation of cybercriminal and partisan threat actors.

DOI: 15 January 2022 – Over 70 Ukrainian public sector websites were disrupted through a DDoS attack. Reports of these attacks coincided with reporting released from Microsoft signaling the discovery of WhisperGate – a multi-stage Wiper malware disguised as ransomware. Public details of how the attacks were carried out are scant, and somewhat inconsistent.

Serhiy Demedyuk, Deputy Secretary of the National Security and Defence Council (NSDC-Ukraine) asserts that a group tied to Belarusian Intelligence services (UNC1151) defaced government websites with threatening messages and that it was cover for the more destructive actions behind the scenes.

Fidelis Cybersecurity analyzed several stages of the WhisperGate malware to affirm that appropriate mitigations were in place, illustrating how we effectively approached neutralization of the threat for our customer. Our detailed analysis of the WhisperGate malware is contained in our January 2022 **Threat Intelligence Summary** report.