SecurityScorecard Discovers new botnet, ‘Zhadnost,’ responsible for Ukraine DDoS attacks

securityscorecard.com/blog/securityscorecard-discovers-new-botnet-zhadnost-responsible-for-ukraine-ddos-attacks

SecurityScorecard Discovers new botnet, ‘Zhadnost,’ responsible for Ukraine DDoS attacks
SecurityScorecard

1. Blog

By Ryan Slaney, Staff, Threat Researcher

Posted on March 10th, 2022

Executive Summary

- SecurityScorecard (SSC) has identified three separate DDoS attacks which all targeted Ukrainian government and financial websites leading up to and during Russia’s invasion of Ukraine. Details of these DDoS attacks have not yet been publicly identified.

- SSC discovered a botnet of more than 3,000 unique IP addresses, across multiple countries and continents, that were the source of the DDoS attacks which consisted of HTTP floods and DNS amplification. SSC has named this botnet “Zhadnost” – Russian for “Greed.”

- Most Zhadnost bots are routers, the majority of them MikroTik, with misconfigured DNS recursion settings and other known vulnerabilities.

- The DDoS attacks appeared to have had a minimal, temporary impact on their targets. Government websites and banking services were quickly restored and customers' balances were not affected.
- We assess that the IP addresses used in the first DDoS attack were a combination of Zhadnost bots and other botnets possibly controlled by criminal actors, who partnered with or were hired by the same threat actor. The second and third DDoS attacks used only Zhadnost bots.
- Attributing Zhadnost and the DDoS attacks to any one threat actor is difficult, however, we assess with moderate confidence that Russia, or Russian-aligned actors, are likely behind this DDoS campaign.

Background

On November 10, 2021, reports emerged of unusual movement of Russian troops near the borders of Ukraine. By November 28, Ukraine reported a build up of 92,000 Russian troops. In January 2022, Russian troops began arriving in Belarus for military exercises. Throughout December 2021 and January 2022, a series of diplomatic talks took place between Russia, NATO, and Ukraine during which Russia proposed limits on NATO’s activities in eastern Europe, such as a prohibition on Ukraine ever joining NATO. NATO/Ukraine rejected these proposals and warned Russia of strong economic and other measures should it invade Ukraine. Russia continued to build up its forces along Ukraine’s border with Russia and Belarus, and in the Black Sea. NATO and Western countries pledged their support to Ukraine and began providing lethal and non-lethal military equipment, intelligence, and financial aid to help Ukraine defend itself from Russian aggression.

On February 24, Russian President Putin announced he had decided to launch a “special military operation” in Ukraine. Shortly thereafter, explosions were reported in several Ukrainian cities and Russian military vehicles began crossing Ukrainian borders on several fronts.

This whitepaper specifically discusses SecurityScorecard’s investigation into the use of DDoS attacks against Ukrainian infrastructure leading up to and during Russia’s invasion of Ukraine. We have identified three separate DDoS attacks which all targeted Ukrainian government and financial websites in a likely effort to take them offline, thereby denying and degrading access to news, information, and currency from official Ukrainian government and financial sources.

Methodology

According to various open sources and media reports, as well as SecurityScorecard’s own data, the following websites were targeted by DDoS attacks on three different occasions:

- **Ukrainian Ministry of Foreign Affairs** - mfa.gov.ua

- **Ukrainian Ministry of Defence** - mil.gov.ua
- **Ukrainian Ministry of Internal Affairs** - mvs.gov.ua
- **Security Service of Ukraine** - ssu.gov.ua
- **Ukrainian Cabinet of Ministers** - kmu.gov.ua
- **Oschadbank** - oschadbank.ua
- **Privatbank** - privatbank.ua

We resolved the IP addresses of these domains and conducted netflow analysis for the period corresponding with the DDoS attacks. From the available netflow results, we discovered more than 3,000 unique IP addresses–spanning multiple countries and continents–that were the source of the DDoS attacks. Of note, none of the IP addresses involved in any of the observed DDoS attacks were located in Russia or Belarus. We then conducted further research and analysis on the 50 most active IP addresses from each attack using proprietary data enrichment techniques and open and closed intelligence sources.

February 15 DDoS Attack

On February 15, 2022, Ukraine’s minister of digital transformation, Mykhailo Fedorov, announced that a cyberattack against the websites of Ukraine’s defense ministry and army, as well as the interfaces of the country’s two largest banks, was the largest assault of its kind in the country's history and “bore traces of foreign intelligence services.” Ilya Vityuk, the head of the Ukrainian Intelligence Agency’s Cyber Security Department, blamed Russia for the attack, citing as evidence that the attack likely cost “millions of dollars” to execute, far beyond the capabilities of individual hackers or groups. He asserted that Russia is the only country that is interested in such strikes on Ukraine.

From our analysis, SSC has identified more than 200 unique IP addresses that were involved in the February 15 DDoS attack. The attack consisted of HTTPS flooding on port 443. This type of attack is designed to overwhelm a targeted server with HTTP requests. Once the target has been saturated with requests and is unable to respond to normal traffic, a denial-of-service will occur for additional requests from actual users. Analysis of the 50 most active IP addresses revealed that approximately half of them appear to be MikroTik routers, or other devices running SquidProxy.

Our data also revealed that the majority of the IP addresses have previously been associated with activity from the following implants:

- Xorddos
- Cobaltstrike

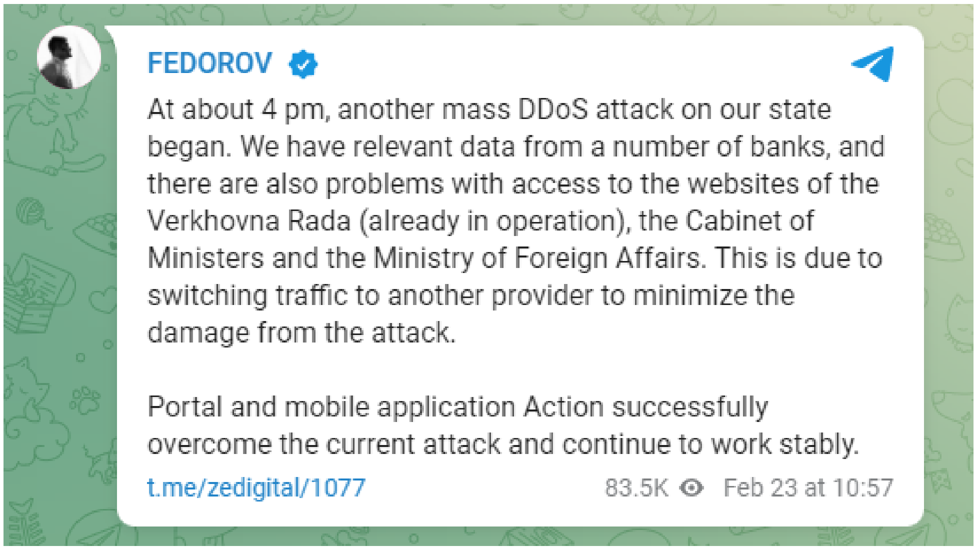
- Amadey
- Trickbot
- Qakbot
- Lokibot
- Jedobot
- Bluebot
- Betabot
- Gumblar
- Kasidet
- PonyLoader
- Smokeloader

Unfortunately, SSC is not able to determine from the available data if the malicious HTTP requests were sent from the router themselves, compromised hosts behind them, or a combination of both. This makes attributing this particular attack to any one threat actor extremely difficult. Our work here continues.

Fortunately, this attack appeared to have minimal impact on its targets. According to a statement from Victor Zhora of the Ukrainian Center for Strategic Communications and Information Security, Ukrainian cybersecurity officials managed to significantly reduce the amount of harmful traffic to the websites. Furthermore, while the targeted banks confirmed the attack, they indicated that users had only been temporarily unable to withdraw money from their accounts. Banking services were quickly restored and customers' balances were not affected.

February 23 and 28 DDoS Attacks

On February 23, another DDoS attack against Ukrainian websites was again reported by Mykhailo Fedorov.


FEDOROV

At about 4 pm, another mass DDoS attack on our state began. We have relevant data from a number of banks, and there are also problems with access to the websites of the Verkhovna Rada (already in operation), the Cabinet of Ministers and the Ministry of Foreign Affairs. This is due to switching traffic to another provider to minimize the damage from the attack.

Portal and mobile application Action successfully overcome the current attack and continue to work stably.

t.me/zedigital/1077 83.5K Feb 23 at 10:57

Image 1: Mykhailo Fedorov's Telegram

SSC discovered another DDoS attack that took place between February 27 - 28 that was largely unreported in the media, likely since such attacks were becoming commonplace at this point.

From our analysis, SSC has identified more than 3,000 unique IP addresses that were involved in DDoS attacks on February 23 and 27-28. Analysis of these IP addresses revealed that the vast majority of them are running "MikroTik Bandwidth-test server" on port 2000, with a connection signature of \x01\x00\x00\x00, recursion enabled on UDP/TCP port 53, and multiple versions of MikroTik RouterOS services on various ports. Analysis of the 50 most active IPs from the second and third attacks revealed that 76% and 92%, respectively, can be identified as MikroTik devices.

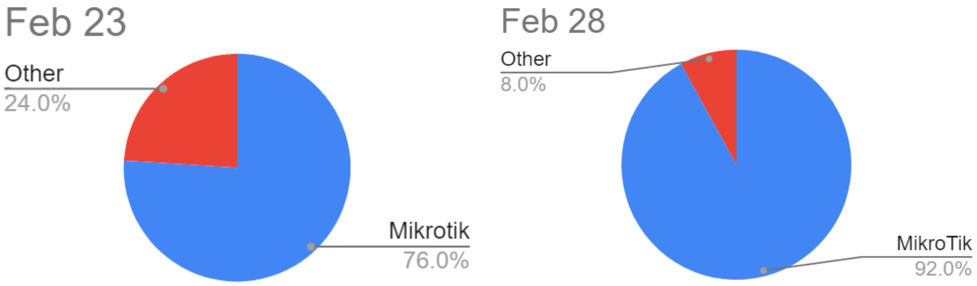


Image 2: Percentage of MikroTik Devices

100% of the IPs we identified had DNS recursion enabled on port 53. SSC assesses that the threat actor sent spoofed DNS requests to the MikroTik devices, which allowed DNS recursion. The requests were then processed as valid and returned to the spoofed recipients, in this case the targeted Ukrainian websites. This is known as an amplifier attack because this method takes advantage of misconfigured DNS servers to reflect the attack onto a target while amplifying the volume of packets. SSC has named the botnet used to conduct the second and third DDoS attacks "Zhadnost"--Russian for "Greed."

Zhadnost is somewhat similar to the Mēris botnet discovered by Russia-based companies Yandex and Qrator Labs in 2021. Yandex/Qrator Labs reported that 90 to 95% of the Mēris bots that had recently attacked Yandex with a DDoS attack had MikroTik Bandwidth Test running on port 2000 with a connection signature of \x01\x00\x00\x00. According to a different report released by NetScout on October 28, 2021, NetScout discovered that there are at least two distinct MikroTik-based IoT botnets inhabiting the same population of unpatched, exploitable MikroTik routers; Mēris, which uses HTTP Pipelining as a form of attack, and a botnet called Dvinis (Latvian for "twin"), which does not. Instead, Dvinis uses an apparent typo in the attack generator which appends an extra '/' character to the end of the URIs targeted in HTTP POST and GET floods.

In response to the Yandex/Qrator labs discovery, MikroTik released a report indicating

Mēris bots are MikroTik routers that were compromised in 2018, when MikroTik RouterOS had a vulnerability that was quickly patched. There was no new vulnerability in RouterOS and there was no malware hiding inside the RouterOS filesystem, rather the attacker was reconfiguring RouterOS devices for remote access, using commands and features of RouterOS itself. Unfortunately, closing the old vulnerability does not immediately protect these routers.

Although MikroTik provided mitigation advice in its statement, it did not mention anything about ensuring that DNS recursion was properly configured. But there is evidence that MikroTik is aware of this vulnerability. According to MikroTik's website, every MIkroTik that has the"Allow-Remote-Requests" feature turned on is a potential attack vector, representing a 1:179 bandwidth amplification factor.

Preliminary analysis using Qrator Labs' Mēris identification tool has revealed that none of the Zhadnost IP addresses are part of the Mēris botnet. No such identification tool for Dvinis nodes exists. However, only the first attack consisted of HTTP floods, which Dvinis is known for. Zhadnost bots don't require a compromised router, simply a router with misconfigured DNS recursion. Therefore, SSC assesses that it is also unlikely that Zhadnost IPs are part of Dvinis. Thus, we believe they are a new botnet, controlled by a different actor.

The analysis of the 50 most active Zhadnost bots/MikroTik routers used in the second and third attack has also revealed that several devices behind them have previously been associated with activity from the following implants:

- Amadey
- Betabot
- Gumblar
- Lokibot

- Ponyloader

We assess that the implant activity is incidental, and not connected to the deployment of Zhadnost bots.

To create Zhadnost, all the threat actor had to do was establish and maintain a list of MikroTik and other devices with misconfigured DNS recursion settings, which would forward spoofed requests to the targeted websites. This could be easily done using tools such as Shodan and Google Dorks. According to our Attack Surface Intelligence Data, there are at least 875,000 MikroTik devices located all over the world. This could potentially represent a near infinite number of bots, provided DNS recursion is not properly configured on these devices.

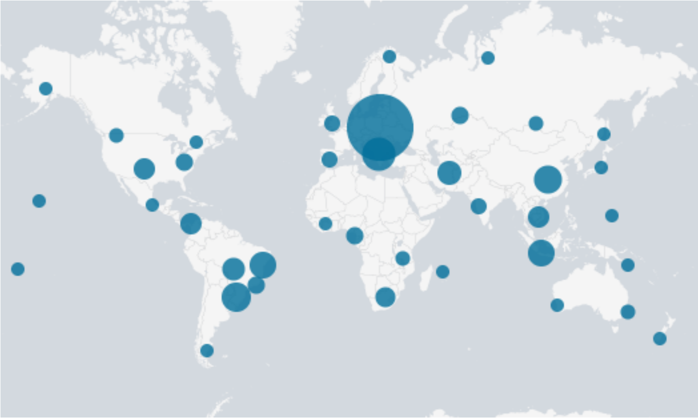


Image 3. Location and density of MikroTik devices. (Source: SSC Attack Surface Intelligence)

Attribution

Attributing Zhadnost and the DDoS attacks to any one threat actor is difficult, given that anyone could have taken advantage of this misconfiguration with little effort. Furthermore, it is difficult to differentiate the traffic from the router itself from the legitimate traffic of the devices behind it, making identification of the command and control infrastructure extremely difficult. However, taking into account the current geopolitical factors, and considering which country is likely to gain from such attacks, SSC can assess with moderate confidence that Russia, or Russian-aligned actors, are likely behind this DDoS campaign.

Key Insights

Despite the involvement of MikroTik devices in all three attacks, further comparison reveals that the first attack is quite different from the second or third:

Attack Date	**Feb 15th**	**Feb 23rd**	**February 28th**
% MikroTik	50%	76%	92%

DDoS Attack Type	HTTP Flood	DNS Amplification	DNS Amplification
# of unique IPs	200	1892	1958
% previously compromised	50%	4%	12%
DNS Recursion Enabled %	20%	100%	100%

Figure 1: Comparison of three attacks.

Based on these differences, SSC assesses with moderate confidence that the IP addresses used to conduct the second and third DDoS attacks against Ukrainian government and financial websites were solely Zhadnost bots, meaning MikroTik and other routers with misconfigured DNS recursion settings. We assess that the IP addresses used in the first attack were a combination of Zhadnost bots and other botnets possibly controlled by criminal actors, who partnered with or were hired by the same threat actor.

SSC also assesses with moderate confidence that the DDoS attacks had very limited impact on their targets. This is likely a result of Ukraine being adequately prepared to handle such attacks, since similar tactics had been used during previous attacks. Furthermore, various Ukrainian officials have made public statements regarding Ukraine’s success in minimizing the effects of attacks.

Outlook

So far, the DDoS attacks SSC has observed have been targeted towards government and financial websites, and do not appear to have much of an impact. This leads to the possibility that the threat actor will target more critical targets in the next attacks, such as networks used for power generation, communications, and by hospitals and military units.

As the Russian military’s efforts become more aggressive to overcome the stiff Ukrainian resistance, we expect the cyber attacks towards Ukraine to follow suit. We also expect to see attacks on NATO and Western countries, in retaliation for the sanctions placed on Russia and the aid provided to Ukraine.

Recommendations

SSC recommends that organizations check the DNS recursion settings in their routers, whether they are MikroTik or another vendor. It is recommended that DNS recursion is disabled if it is not required. If required, it should be configured to only conduct recursion for trusted domains/hosts.

It is critical to put DDoS mitigations in place, via a service like Cloudflare, Akamai, or AWS Cloudfront. Having a firewall will not stop the volume of traffic we have observed against Ukrainian targets via netflow analysis.

Furthermore, blocking Russian IPs will not stop DDoS attacks. The attacks are coming from across the world from neutral countries in Latin America, EU (not Russia or Belarus), and southeast Asia.

IoCs

Please contact [email protected] for IoCs associated with Zhadnost and the DDoS attacks on Ukrainian websites.

Standing up for Peace and Democracy

SecurityScorecard (SSC) stands with Ukraine during this difficult time in its history. We have always been a company of action (not words), which is why we are making significant efforts to support our customers with timely and relevant intelligence. We built our intelligence products with the goal of keeping our customers informed of changes in adversarial behaviors, data, tools, and attacks. Some of the actions we have taken:

We have donated to the UN Refugee Agency, and the Ukrainian Red Cross to assist in humanitarian efforts. We encourage the business community to make similar efforts.

We will match any SecurityScorecard employee donation, up to $100,000 (USD) in total.

Any Ukraine-based company, for the next six months, can get entirely free access to SecurityScorecard’s enterprise license to protect themselves from malware resilience in light of ongoing cyber attacks. We are also providing them free access to SecurityScorecard forensics remediation team to deal with ransomware issues or to recover from any outage. Simply email [email protected]

Our Threat Research & Intelligence team has been analyzing the scope, impact, and attribution of cyber attacks involving both Russia and Ukraine. We are partnering with U.S. authorities to further aid their efforts, and have posted our recommendations here.

Return to Blog