Zhadnost strikes again… this time in Finland.

securityscorecard.com/blog/zhadnost-strikes-again-this-time-in-finland

1. Blog

By Ryan Slaney, Staff, Threat Researcher

Posted on April 13th, 2022

Executive Summary

- SecurityScorecard (SSC) has identified a DDoS attack which targeted the websites of the Finnish Ministry of Foreign Affairs and Ministry of Defense.
- SSC discovered more than 350 bots, mainly located in Bangladesh and African countries, which are now considered to be part of the Zhadnost botnet, previously discovered by SSC in March.
- The majority of the bots are MikroTik routers, running various MikroTik services, or devices running Squid Proxy and vulnerable Apache web servers.
- The DDoS attack against the Finnish websites does not appear to have a lasting impact, as the sites were back online within hours of the attack.

- The attack was conducted at the same time as Ukrainian President Volodymyr Zelensky's virtual address to the Finnish parliament, and hours after a Russian aircraft is suspected of invading Finland's air space.
- The attack coincides with Finland's accelerated pursuit for NATO membership, a likely motivating factor for the DDoS attack.
- Attributing Zhadnost and the DDoS attacks to any one threat actor is difficult, however, SSC assesses with moderate confidence that Russia, or Russian-aligned actors, are likely behind this DDoS campaign.
- Based on prior history of Russian attacks, the next play in the Russian cyber threat actor playbook would be the deployment of wiper-style attacks, possibly against critical infrastructure and government targets.

Background

"Russia is not the neighbor we thought it was." Those were the words of Finland's Prime Minister, Sanna Marin, when she told the Finnish people that it was very likely Finland would join NATO during her time in office. This was seen as a sea change for Finland who, even after two wars with the former Soviet Union, kept its independence during the Cold War, and avoided joining alliances in the East or West. However, Russia's second invasion of Ukraine appears to be the tipping point. Finland is now rocketing through the political process to become a NATO member, with a final decision expected as early as May. If Finland is successful in its NATO bid, the length of the Russian - NATO border would double overnight.

Russia has made it clear it isn't keen on Finland's pursuit of NATO membership. On March 12, Russian foreign ministry spokesman Sergei Belyayev said that Finnish or Swedish NATO membership would have "serious military and political consequences, and would require changing the whole palette of relations with these countries and require retaliatory measures."

DDoS Attack

On April 8, as members of the Finnish parliament were listening intently to a virtual address by Ukrainian President Volodymyr Zelensky, reports emerged that the websites of Finland's Ministry of Foreign Affairs (um.fi) and Defense (defmin.fi) were knocked offline for several hours as a result of a DDoS attack.

SSC resolved the IP addresses of these domains and conducted netflow analysis for the period corresponding with the DDoS attack. Our data shows a sustained DDoS attack, lasting approximately four hours, launched by more than 350 unique IP addresses, spanning multiple countries and continents. The most active bots were located in Bangladesh and African countries. Of note, none of the IP addresses involved in any of the observed DDoS

attacks were located in Russia or Belarus. The attack itself 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.

SSC then used proprietary data enrichment techniques, as well as open and closed intelligence sources to conduct further research and analysis on the 50 most active bots involved in the attack. What we discovered was that the majority (82%) of the bots were MikroTik routers, running various MikroTik services. The remaining IP addresses were running Squid Proxy, Caddy Server, and vulnerable versions of Apache.

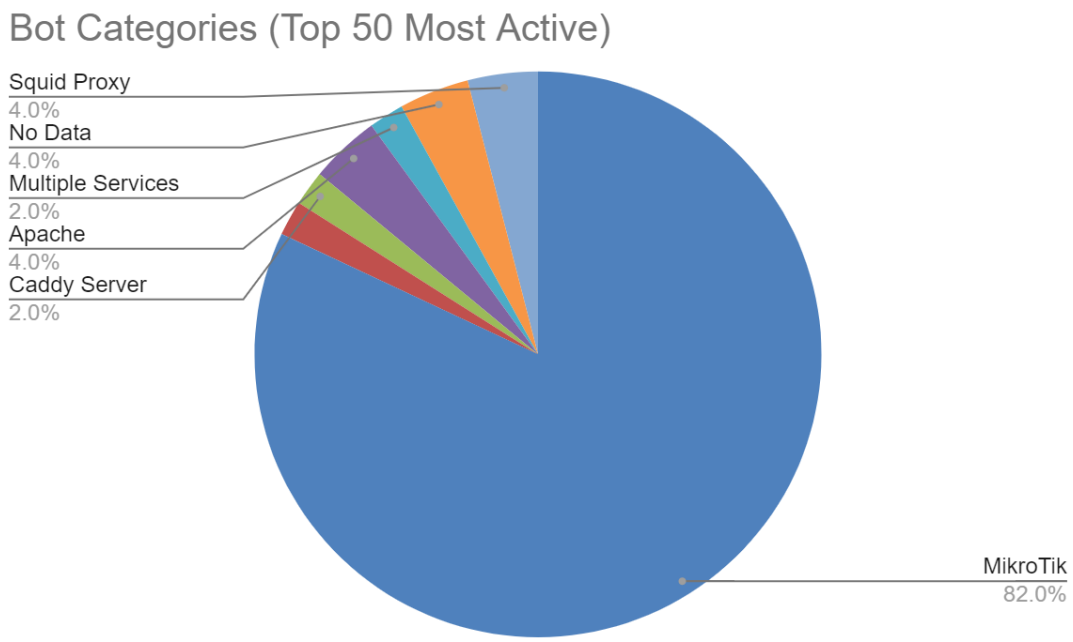

Image 1: Breakdown of Bot Types (Source: SSC Attack Surface Intelligence)

The makeup of these bots are nearly identical to that of the Zhadnost botnet, which was responsible for three separate DDoS attacks against Ukrainian government and financial websites before and shortly after the Russian invasion of Ukraine. The Finland attack is identical to the first Ukraine attack, which was conducted on February 15. Both attacks consisted of HTTPS flooding and relied on MikroTik, Squid Proxy, and Apache devices to conduct the attack. (Of note: the last two Ukraine attacks consisted of DNS amplification from misconfigured MikroTik routers.)

As we mentioned in our previous blog post on Zhadnost, MikroTik routers have a bevy of vulnerabilities that allow threat actors to use them for DDoS attacks and other malicious purposes. Although some patches have been deployed, multiple botnets, including Mēris, Dvinis, and Glupteba consist of vast numbers of compromised MikroTik routers. According to

our Attack Surface Intelligence Data, there are at least 875,000 MikroTik devices deployed all over the world. This could potentially represent a near infinite number of bots, provided they are vulnerable and DNS recursion is not properly configured on these devices.

Image 2. Location and density of MikroTik devices. (Source: SSC Attack Surface Intelligence)

With the addition of the more than 350 bots we identified in this campaign, SSC is now aware of nearly 3350 bots that make up the Zhadnost botnet.

Breach of Airspace - Innocent Mistake or Calculated Move?

The attack came several hours after Finland's Ministry of Defense announced Finnish air space had been breached by a Russian aircraft. According to a press release, a Russian Ilyushin IL-96-300 was suspected to have violated Finnish airspace for about three minutes, off the coast of the Gulf of Finland near the city of Porvoo in the morning of April 8. The press release did not specify if it was a Russian military, government, or civilian aircraft.

The Russian government is known to operate several IL-96-300s in various configurations. In 2013, the Kremlin announced that it would receive two brand new IL-96-300PU "command post" aircraft, fitted with VIP interiors and special communications equipment, in order to allow for confidential communications and management of nuclear forces.

It's unclear which IL-96-300 variant was involved in the suspected breach of Finnish airspace, who was operating it, or whether the breach was intentional or simply a navigational error. However, given the timing of the airspace breach and the cyber attacks, it's possible that Russia was conducting a coordinated flexing of both its air and cyber muscles as a warning to both Finland and Sweden.

Image 3: Iluskin IL-96-300PU (Source: jetlinemarvel.net)

Attribution

Attributing Zhadnost and the DDoS attack to any one threat actor is difficult, given that many botnets rely on compromised MikroTik devices, and that individual bots can be used by more than one botnet. Furthermore, it is difficult to identify the botnet's command and control infrastructure since the router's traffic is combined with the legitimate traffic of the devices behind them. However, taking into account the current geopolitical factors, and considering which country is likely to gain from such an attack, SSC can assess with moderate confidence that Russia-or Russian-aligned actors–are likely behind this latest DDoS campaign.

Outlook

The DDoS attack against the Finnish websites does not appear to have a lasting impact, as the sites were back online within hours of the attack. It's likely that the threat actor was aware that this attack would have a small impact, but still conducted it to achieve a different goal–to serve as a warning to Finland, and by extension, Sweden.

As Finland continues down the path of obtaining NATO membership, it is likely that cyber attacks will not only continue, but they will escalate. If history were to repeat itself, the next play in the Russian cyber threat actor playbook would be the deployment of wiper-style attacks, possibly against critical infrastructure and government targets.

Recommendations

> 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 during a Zhadnost DDoS attack.

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

Indicators of Compromise

Please contact for IoCs associated with the Zhadnost botnet, or with any questions or comments.

Return to Blog