Radware Advisory

Cyberattacks and Threats Admidst Russian Invasion of Ukraine

February 28, 2022

In this special advisory, Radware shares a collection of public information regarding threats and attacks surrounding the Kremlin's special military action against Ukraine. Information is based on recent developments online, influenced by, and in support of the offline conflict.

Background

The North Atlantic Treaty Organization (NATO) is an alliance of 30 member countries that promotes democratic values, is committed to a peaceful resolution of disputes, and relies on collective military power to undertake operations when diplomatic efforts fail. Article 5 of the NATO charter is the cornerstone of this military alliance. It talks of "the principle of collective defense," the very heart of NATO. This article binds NATO member countries to commit them "to protecting each other and setting a spirit of solidarity within the alliance." This means that if a member country is attacked by a non-member country, all members will consider it an attack on the individual countries, and respond militarily. But Article 5 does not apply to non-member countries such as Ukraine. Ukraine applied to be a Nato member in 2008 and its application for NATO membership is pending. Ukraine's President, Volodymyr Zelenskyy, has recently appealed again to expedite a membership decision. This is also what lies at the origin of the current conflict.

Although NATO fully supports Ukraine's sovereignty, territorial integrity, and Ukraine's right of self-defence and condemning Ukraine's invasion, the alliance can not and will not go to war with Russia unless one of its members is attacked. This applies both to online and offline conflicts.

NATO members agreed and imposed a package of unseen and severe sanctions on Russia, targeting its financial system and introducing export controls on dual-use and high-tech goods, with a particular focus on electronics, computers, telecom and information security, sensors and lasers and marine applications. The package also includes an export ban on aircraft, aircraft parts and related equipment, as well as a ban on the sale of equipment and technology needed to update Russian oil refineries to modern environmental standards.

In the Kremlin's best interest, it is not to expose itself by attacking targets outside of Ukraine. If they do, they could trigger a larger conflict through a NATO alliance member, at which point we can expect the worse.

There have been reports of DDoS attacks on both sides. Anonymous claimed responsibility for the attacks on Russia, while the attacks on Ukraine were attributed to Russia by the U.S. government and the NCSC (U.K.). The attribution is, as far as information is available, based on known and used Tactics, Techniques and Procedures (TTPs) during Russian military operations. Before the start of the invasion, Ukraine targets were assaulted by a wiper malware dubbed "HermeticWiper." The second deployment of a wiper malware against Ukrainian targets, with the first attacks taking place in the middle of January leveraging a malware named 'WhisperGate.'

Radware Advisory

Cyberattacks and Threats Admidst Russian Invasion of Ukraine

February 28, 2022

As the world started to take note of the horrendous situation on the ground in Ukraine, political hactivists and underground movements stepped in and took initiative targeting both sides of the dispute with online attacks. Nations and influencers are adding to the global confusion with disinformation campaigns and fake news surrounding offline and online events.

Wiper Malware Attacks

A wiper is a type of malware leveraged to wipe data or systems. Wipers can make systems inoperative by overwriting boot loaders. Wipers typically also have worming capabilities that allows them move from system to system through a local network or, in a worst case scenario, through the internet. Wipers leverage the most of the same techniques and tactics as ransomware. Some wipers disguise themselves as ransomware and leave a ransom note on the screen, only for the owner to find out that his system is wiped. Though leveraging much of the same initial access and propagation techniques, wipers are less sophisticated compared to their ransomware siblings. Ransomware encrypts data with a reversible algorithm and exfiltrates data while wiper do not concern themselves with an ability to recover the data or steal sensitive information. The objective of the wiper is to destroy systems and impact the availability and productivity of its victims. A good backup and restore strategy is most effective against wipers.

The Shamoon malware used in 2012 and 2016 attacks targeting Saudi energy organizations contained a disk wiping mechanism. The original variant overwrote files with portions of an image of a burning U.S. flag. The 2016 variant was nearly identical, except using an image of the body of Alan Kurdi instead.

In June 2017, a new variant of Petya, called NotPetya, was used for a global cyberattack, primarily targeting Ukraine. The new variant propagated via the EternalBlue exploit, an exploit that is generally believed to have been developed by the U.S. National Security Agency (NSA), and was used earlier in the year by the WannaCry ransomware. Although NotPetya purports to be ransomware, it was modified so that it is unable to actually revert its own changes. The NotPetya attacks have been attributed by security researchers, Google and several governments to the Russian government, specifically the Sandworm hacking group within the GRU Russian military intelligence organization.

DISK-WIPING ATTACKS PRECEDING RUSSIAN INVASION

Shortly before the Russian invasion started in the morning of February 24, a new form of disk-wiping malware dubbed HermeticWiper by ESET Research was used to attack organizations in Ukraine and impacted hundreds of systems in their networks. The attack came just hours after a series of distributed denial-of-service (DDoS) onslaughts knocked several important websites in the country offline.

The attackers appear to have used an exploit of a known vulnerability in Microsoft SQL Server (CVE-2021-1636) in order to compromise at least one of the targeted organisations. Once run, the wiper will damage the Master

Boot Record (MBR) of the infected computer, rendering it inoperable. The wiper does not appear to have any additional functionality beyond its destructive capabilities.

According to Symantec, the attacks may have been in preparation as early as November 2021 and targeting organizations in financial, defense, aviation and IT services.

In the middle of January, another data wiper swept through Ukraine. Called WhisperGate by Microsoft Threat Intelligence, the wiper overwrites the Master Boot Record to display a faked ransom note, masquerading as ransomware. WhisperGate wipes and corrupts a Windows system to the point where files and drives are no longer recoverable or usable. The threat actors deliberately deployed WhisperGate to targeted organizations. According to SecureWorks, one reported attack vector used to deploy WhisperGate was a supply chain attack against a technology service provider. Details are limited, but available evidence suggests that the supply chain attack involved a traditional compromise of the service provider. The threat actors then likely leveraged credentials and accesses from the provider's network to compromise its customers.

DDoS Attacks

On February 15, a campaign of moderate DDoS attacks began targeting Ukraine's Ministry of Defense, armed forces of Ukraine, and state-owned banks. While the DDoS attacks were ongoing, a series of spam text messages were sent to the customers of one of the state-owned banks about technical malfunctions at ATMs. The Ukrainian cyber police analyzed the content of the SMS and determined it was an information attack on the customers, not a phishing attempt. While the Ukrainian national police opened an investigation into the DDoS attacks at the request of a bank, these network outages came right as Russia staged over 130,000 troops outside of Ukraine.

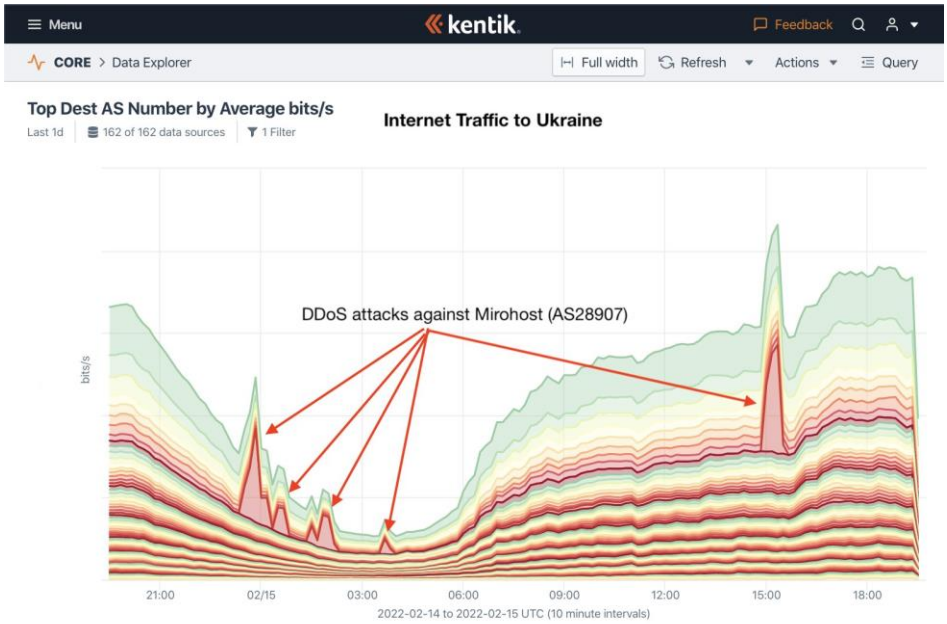

Figure 1: Evidence of DDoS attacks against Ukraine targets (source: Doug Madory - Kentik)

The following day, government agencies and security companies around the world began analyzing the events that had just unfolded on social media in real time. 360 Netlab was the first to report that the DDoS attacks originated from a Mirai botnet variant known as Katana, whose C2, 5.182.211[.]5, was located in the Netherlands. This botnet variant is associated with the threat group, VegaSec. The source code is freely available on GitHub but is also sold as a service via VegaSec's Telegram Channel, Katana Security. Sparking depart if the DDoS attacks seen on Tuesday were that of a VegaSec, patriotic hacktivist, or the Russian government.

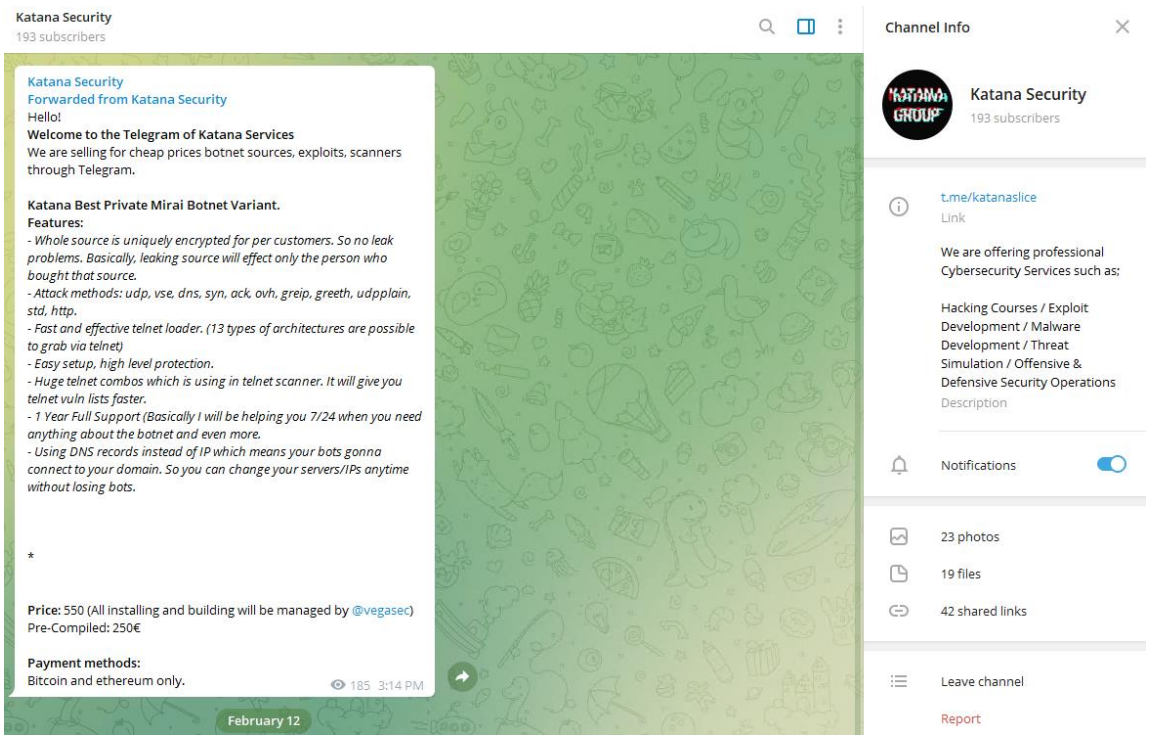

Figure 2: Katana botnet advertisement on Telegram (source: t.me/katanaslice)

On the morning of February 17,, the situation between Russia and Ukraine began to escalate as reports started to surface about government websites in Russia experiencing intermittent outages as well as a network outage impacting Vodafone in Luhansk, Ukraine. It was later determined that the outage in Luhansk was the result of sabotage and not a DDoS attack. Later that day, both the United Kingdom and the United States attributed the DDoS attack seen on Tuesday, February 15, to Russia's GRU.

On February 21, exactly one day after the closing ceremonies at the Beijing Winter Olympics, Putin recognized Ukraine territories as independent, setting the stage for further conflict. The following days would see a renewed round of DDoS attacks targeting the Ukrainian government, as well as U.K. and the U.S. publishing a joint report about Sandworm's new malware, Cyclops Blink, that replaces VPNfilter. A botnet that was taken down by the FBI in 2018. At the same time, ESET researchers discovered a new data wiper campaign that followed the DDoS earlier in the day.

On February 24, Russia invaded Ukraine. Along with the physical invasion, the world was exposed to modern hybrid warfare. As the troops entered Ukraine, regional DDoS attacks followed, causing disruption and panic across the country. In addition to Ukraine being targeted, the Russian government and banking websites also began experiencing several outages resulting in the Russian government deploying digital defenses.

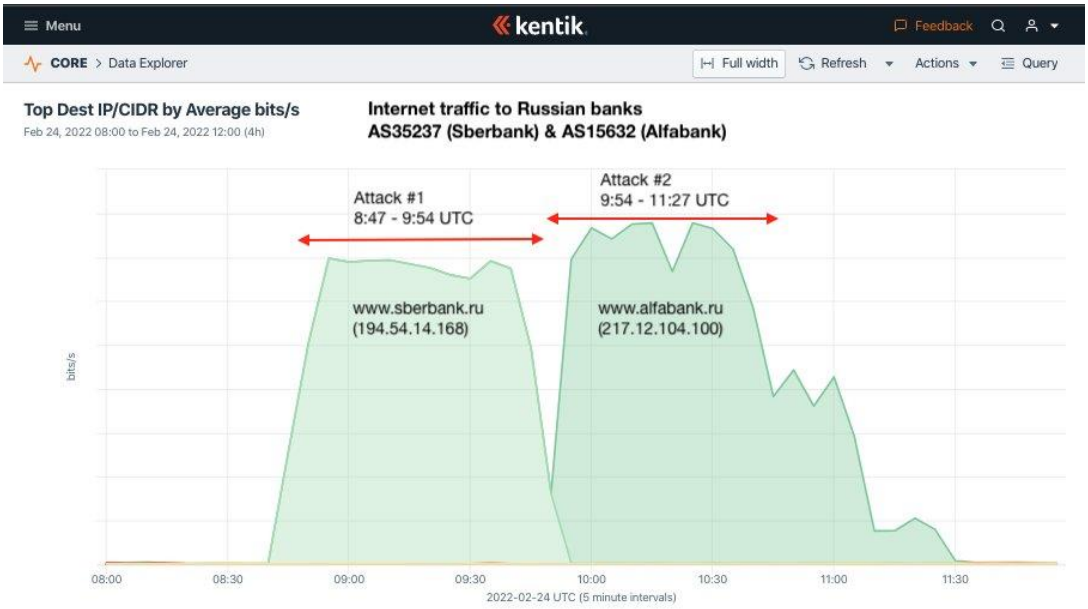

Figure 3: DDoS attacks targeting Russian banks (source: Doug Madory - Kentik)

As the invasion of Ukraine entered its second day, DDoS attacks between the two countries continued to escalate as additional threat actors began to show up. The Belarusian threat group, UNC1151, was linked to a phishing campaign that targeted Ukraine's military. In a surprise turn of events, hacktivists also returned, sparking concerns that their actions may trigger external aggression from Russian hacktivists and state-sponsored threat actors.

This concern was validated when Russian vigilante hackers and Anonymous joined the conflict. To make matters worse, the ransomware group Conti began posting statements related to the war, leading to other ransomware groups posting options and position of the conflict on their PR sites.

The addition of non-Russian or Ukraine threat actors had made it very difficult to determine what operations are run by patriotic hacktivists and what operations are run by intelligent services. As the conflict escalated and dissolved into war, DDoS attacks played and continue to play an instrumental role in modern hybrid warfare, such as the the significant disruption of Ukraine's internet backbone provider, GigaTrans. The provider supplies connectivity to other major networks in Ukraine, making it a prime target for the goal of disrupting news and communication. At the same time Netblock observed a number of DDoS attacks going the other direction, demonstrating that service providers and financial institutions were top targets among threat actors.

At the time of writing, the conflict and DDoS attacks between Russia and Ukraine is still ongoing. Hacktivists have shown up and taken sides leading many to believe that even if Russian and Ukraine agree on a cease-fire, the digital conflict will rage on at the hands of third-party threat actors. Fueling this underground war is the creation

of the IT Army of Ukraine. This is a group of over 180,000 pro-Ukrainian members who are willing to spread content and hack back at those attacking Ukraine. This group is supported by the Vice Prime Minister of Ukraine, Mykhailo Fedorov.

Figure 4: Mykhailo Fedorov announcing the creation of the "IT Army of Ukraine"

Inside of the channel, admins share information about DDoS targets such as Sberbank and Gazprom, as well as other military and enterprises in Russia. More recently, on February 27, the IT Army of Ukraine began listing and targeting government agencies and enterprises located in Belarus as a result of the country aiding Russian aggression.

Figure 5: First task posted to IT Army of Ukraine Telegram channel

Subsequent tasks were to shut down a list of Russian YouTube channels that "openly lie" about the war in Ukraine. A list of steps on how to report a channel in violation to YouTube is included in the message.

In another task, the IT Army of Ukraine is calling for targeted DDoS attacks on an API of one of the largest banks in Russia.

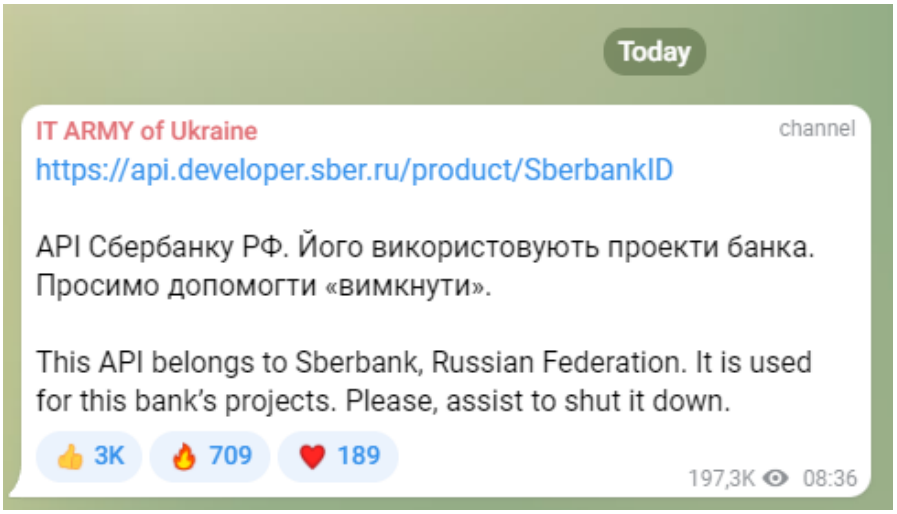

Figure 6: Task to perform DDoS attack on online API of a large Russian Bank, posted on IT Army of Ukraine telegram channel

Ransomware Operators "Warn" for Retaliation

On February 25, the Conti ransonware team posted a "warning" on their dark web site announcing their full Russian government support. They are warning that any cyber or war activities against Russia will result in them using all their resources "to strike back at the critical infrastructures of an enemy."

Figure 7: Conti Team's first version of "warning" (source: BleepingComputer)

One hour later, they changed their position, saying they do not ally with any government and they do condemn the ongoing war. But they will use their full capacity to strike back if American cyber aggression compromises the well-being and safety of peaceful citizens of the Russian Federation.

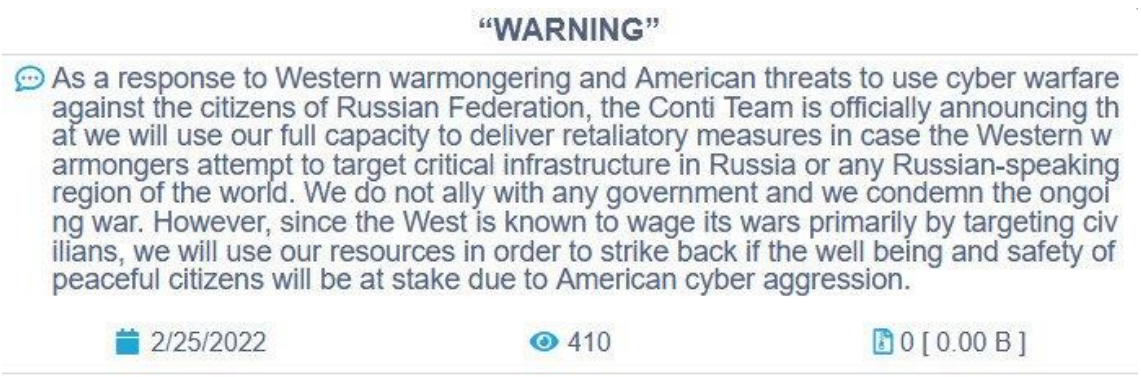

Figure 8: Conti Team's updated "warning" (source: BleepingComputer)

Conti is one of the most active ransomware actors are were responsible last year for breaching over 60 organizations operating industrial control systems (ICS).

The same day, CoomingProject, a lesser-known ransomware group, announced their support for the Russian government.

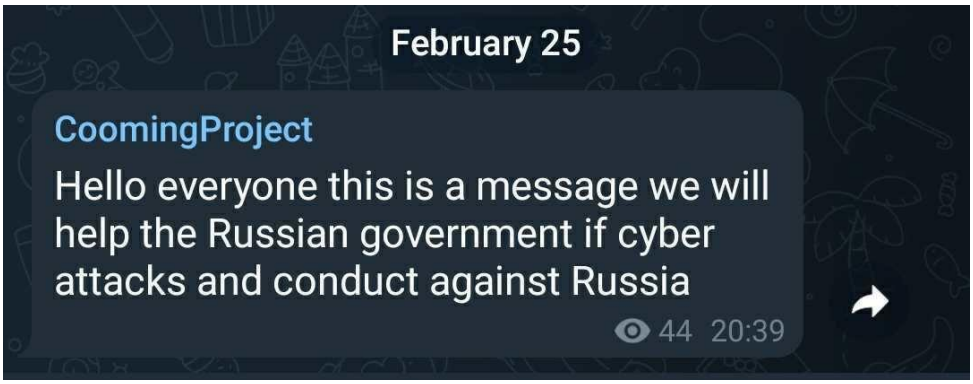

Figure 9: CoomingProject announcement (source: Valéry Rieß-Marchive on Twitter)

On Sunday, February 27, probably in reaction to Conti's "warning," Lockbit published in eight languages their "Official Statement on the Cyber Threat to Russia." Lockbit is not engaging in international conflicts and are "only interested in money for their harmless and useful work," calling their attacks "paid training to system administrators around the world on how to properly set up a corporate network."

> Many people ask us, will our international community of post-paid pentesters, threaten the west on critical infrastructure in response to cyber aggression against Russia?

Our community consists of many nationalities of the world, most of our pentesters are from the CIS including Russians and Ukrainians, but we also have Americans, Englishmen, Chinese, French, Arabs, Jews, and many others in our team. Our programmers developers live permanently around the world in China, the United States, Canada, Russia and Switzerland. Our servers are located in the Netherlands and the Seychelles, we are all simple and peaceful people, we are all Earthlings.

For us it is just business and we are all apolitical. We are only interested in money for our harmless and useful work. All we do is provide paid training to system administrators around the world on how to properly set up a corporate network. We will never, under any circumstances, take part in cyber-attacks on critical infrastructures of any country in the world or engage in any international conflicts.

Figure 10: Lockbit announcement following the Conti "Warning"

LockBit first emerged as the ABCD ransomware back in September 2019. It has honed it skills to become one of the most prolific ransomware groups today. Through professional operations and strong affiliate programs, LockBit operators show they were in it for the long haul. According to Trend Micro, LockBit has been detected all over the globe with the U.S. experiencing most the the attack attempts between June 2021 to January 20, 2022, followed by India and Brazil. Like many ransomware families, LockBit avoids the Commonwealth of Independent States (CIS) countries.

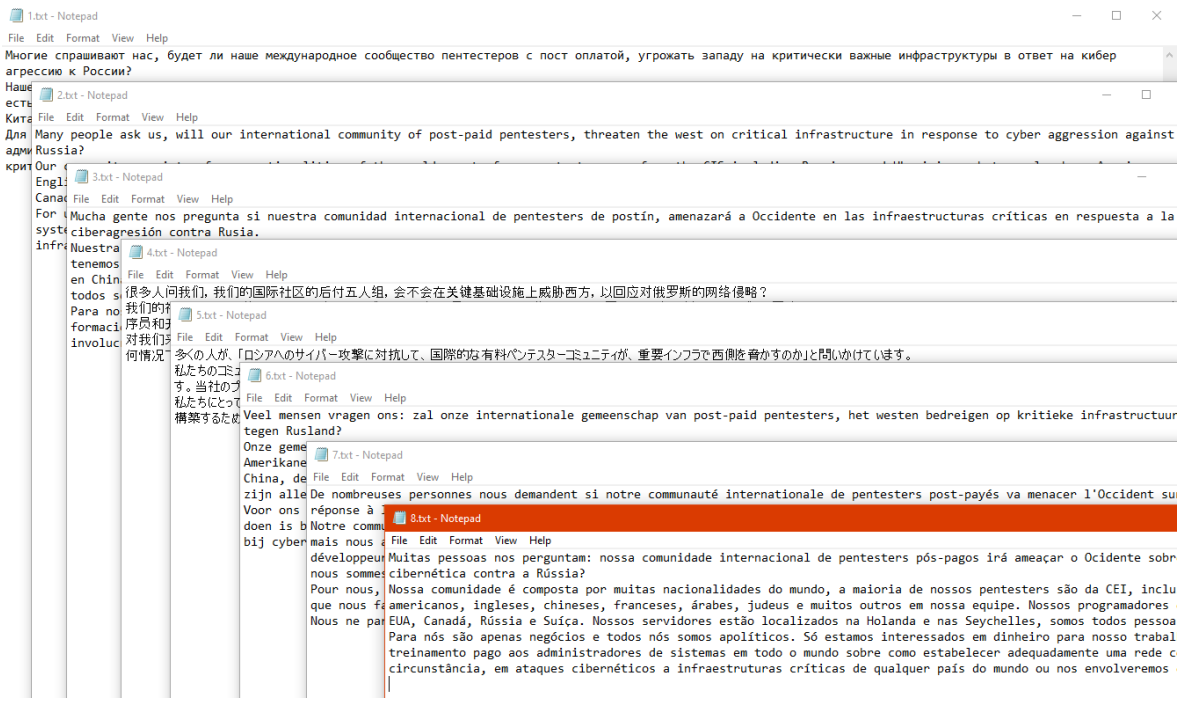

Figure 11: Lockbit announcement translated in seven languages (Russian, English, Spanish, Chinese, Japanese, Dutch, French and Portuguese)

Geoblocking and Ability To Resist Foreign DDoS Onslaughts

Geoblocking was reportedly deployed by Russia in an attempt to mitigate DDoS attacks. Geoblocking can provide quick and easy mitigation against application-level attacks, including application-level denial-of-service and targeted attacks such as exploits and breaches. Threat actors that perform targeted application-level attacks, however, have the option to rent HTTP- or SOCKS-based proxy services on the clear net and underground, such as SmartProxy. The success of geoblocking targeted attacks will also depend on how many bulletproof hosting services are within the country. Attackers will never initiate attacks from their local infrastructure but will rent infrastructure close to the targets they are attacking, preferably inside the country and from service providers that are more lenient to the activity on their servers. Geoblocking will provide an answer against global and random malicious attack campaigns, but not against most targeted attacks by experienced threat actors.

From a network DDoS perspective, geoblocking will typically provide limited success. Direct path attacks from hosts outside the country can leverage source spoofing by using target countries' IP address ranges to circumvent geoblocking. Many botnet operators and related booter/stresser services provide the ability to use only specific bots based on their geographic location to ensure the DDoS attacks are generated from in-country devices. Large volumetric attacks will leverage reflection and amplification services that are located in the country. By consequence, the success of geoblocking will largely depend on the penetration level of botnets in the country, its ability to prevent bulletproof and lenient hosting services in the country, and the ability to limit the number of exposed reflection and amplification services.

Russia, however, has the ability to disconnect itself from the global internet. Russia adopted legislation, known as "sovereign internet" law, in late 2019. It was put in place to shield the country against what Russia called the "aggressive nature" of the United State's national cybersecurity strategy. When this protocol is activated, Russia becomes a self-sustaining local network referred to as 'Runet.' The law stipulates that tests be carried out annually, and while tests in 2020 were called off due to complications with the pandemic, all of Russia's telecom providers ran successful tests in 2021.

Reasons for Concern

The most significant threat for organizations is collateral in a proxy war fought by patriotic hactivists. Hactivists typically target local and state governments and organizations they feel don't align with their political views, but any organization can become a target based on clients and partners they do business with.

Organizations across the globe should continue bolstering their cybersecurity resilience. The threats and potential attacks that might follow as conflicts could escalate between nations or between online communities

are not different than threats organizations have faced from hactivists and ransomware operators in previous years.

Radware strongly advises organizations:

- Keep patching and ensure no known vulnerabilities are left exposed
- Ensure access controls are adequate and use dual or multifactor authentication whenever possible
- Enforce good password hygiene, use and rotate complex passwords as often as possible
- Review and test your backups
- Ensure adequate DDoS protections protect critical and exposed assets
- Ensure adequate WAAP to protect web-facing applications and APIs
- Create awareness in the organization for phishing and smishing attacks
- Have an incident response plan
- Ensure coverage of logging and inspect logs for potential C2 communications and data exfiltration
- Audit and assess the risk from third parties that have access to data and systems