digital shadows_

Weekly Intelligence Summary

04 FEB 2022

In the spotlight this week: A recent attack showed the devastating potential of cyber-threat activity when used by a nation-state for coercion or, worse, escalating regional instability (hybrid warfare). The attack occurred amid mounting international tension after Russia deployed more than 100,000 troops to Ukraine-bordering Russian, Crimean, and Belarussian outskirts, and the US and NATO[1] reacted swiftly. Russia responded with its own set of demands. The cyber attack came on 13 Jan 2022, when threat actors defaced the websites of more than 70 Ukrainian government agencies and installed the "WhisperGate" wiper malware to disable government computer systems. Russia has employed such hybrid warfare tactics in the past, with fall-out including damage to multiple business sectors, the economy, and supply chains; the recent attack further demonstrates the state's capabilities.

Russia-Ukraine tension leaves door open for hybrid warfare

Affected sector	Government
Affected geographies	Ukraine, Russia, Crimea, Belarus, US, UK, Europe
Tactics, techniques, and procedures (TTPs)	Social engineering, wiper malware, information warfare

What happened?

In recent months, Ukraine has been the nexus of escalated rhetoric and military activity between Russian and Western states. This has largely been a reaction to the surge of 100,000-plus Russian troops along Ukraine's common borders with Belarus, Russia, and Crimea—a former territory of Ukraine annexed by Russia in 2014. Russia's strategic land grab was deemed illegal by NATO allies, and NATO still refuses to officially recognize the territory as part of Russia. Ukraine is in the crosshairs of a modern-day power struggle, making it vulnerable not only to a military attack but the constant threat of cyber attacks. The cyber element of modern warfare is often overlooked, but recent events in Ukraine and actions taken by Russia have highlighted how it can be used as a coercive or threatening tool.

On 13 Jan 2022, threat actors defaced the websites of more than 70 government agencies in Ukraine. They also installed the destructive wiper malware "WhisperGate" onto computer systems, affecting Ukraine's foreign ministry, its Ministry of Education and Science, and other state services. Although WhisperGate was designed to look like ransomware, its true purpose was to destroy Ukrainian government systems or render them inoperable. Russia has denied any involvement in the attack, but the Ukrainian Ministry of Digital Transformation and independent security researchers have stated that all evidence points to a probable link to the Russian government, if not government support.[2]

In the wake of this attack, Russia's cyber capabilities have once again been placed under a microscope. The Czech Republic, the UK, Canada, and the US have all warned of the likelihood of Russian cyber attacks. On 25 Jan 2022, the Cyber Security and Infrastructure Agency (CISA) released an alert to warn the US public of potential Russia-based cyber threats to US critical infrastructure. The alert provided an overview of Russian state-sponsored cyber operations, and claimed that although there "are not currently any specific credible threats to the U.S. homeland," officials are "mindful of the potential for Russia to consider escalating its destabilizing actions in ways that may impact others outside of Ukraine."[3]

[1] North Atlantic Treaty Organization

[2] hxxps://www.ft[.]com/content/0bdfafb8-a340-4e6a-a688-d878c45d1010

[3] hxxps://www.cisa[.]gov/uscert/ncas/alerts/aa22-011a

So what?

For months, the cyber-security world has been trying to anticipate and prepare for a potentially destructive cyber attack that might accompany or precede a Russian invasion of Ukraine. Some observers have described this position as alarmist, but Russia has previously used its sophisticated cyber capabilities in conjunction with military action. For example, when Russia invaded and annexed Crimea in 2014, one of its first actions was cutting a cable linking the peninsula to the outside world. This disrupted Internet connectivity and gave Russia additional leverage over the region; it limited the world's visibility of the early phases of the "grey zone"[4] conflict[5].

In the aftermath of the annexation, in 2015, the Russia-backed advanced persistent threat (APT) group "Sandworm" launched a devastating cyber attack on Ukraine's power grid. This attack created widespread power outages that affected hundreds of thousands of residents. In 2017, Sandworm deployed the "NotPetya" malware. By overwriting master boot records and a list of file types, NotPetya immobilized hundreds of Ukrainian organizations and critical infrastructure, including banks, ministries, newspapers, electricity firms, and hospitals.[6]

These previous attacks provide insight into Russia's cyber TTPs, such as persistence. Researchers at Cisco have suggested that the WhisperGate attackers may have initially infiltrated Ukrainian government systems as early as mid-2021,[7] suggesting that initial access preceded the attack by months. Before the 2015 cyber attack on Ukraine's power grid, Sandworm had established and maintained persistence in the networks of Ukrainian power companies for several months.

Russia has also been known to use information warfare and psychological warfare to control narratives. The Russian state-controlled media has already been amplifying the narrative that Ukraine is actively preparing a military offensive or provocation against Donetsk, Luhansk, or Crimea—areas controlled by Russia-backed separatists. In the past few weeks, the US and UK announced they were providing arms, and troops, to bolster Ukraine's defenses. The Russian state-controlled media claimed that the weapons would eventually end up in the hands of terrorists, militants, and neo-Nazis in Ukraine.[8]

Inflammatory, false, and misleading narratives are also circulating on social media and other communication platforms. On Russian social-media sites, such as VK (the Russian-language equivalent of Facebook), Russian volunteers are being sought to reinforce separatist forces in eastern Ukraine.[9] In addition, according to Symantec, the Russian APT group "Gameradon" is using eight novel payloads in a social-engineering campaign against Ukraine. The attacks are intended to influence Ukrainian society, sow mistrust, and exacerbate domestic issues[10]—a familiar tactic that was used before the US presidential election in 2016.

[4] A term used to denote a conflict that falls below the threshold of war

[5] hxxps://www.atlanticcouncil[.]org/blogs/new-atlanticist/cord-cutting-russian-style-could-the-kremlin-sever-global-internet-cables/

[6] hxxps://www.wired[.]com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

[7] hxxps://www.wsj[.]com/articles/ukraine-hacks-signal-broad-risks-of-cyberwar-even-as-limited-scope-confounds-experts-11642683723

[8] hxxps://www.atlanticcouncil[.]org/blogs/new-atlanticist/russian-hybrid-threats-report-kremlin-pushes-claims-about-ukrainian-offensive-junk-weapons-from-west/

[9] hxxps://www.aljazeera[.]com/news/2022/2/2/social-media-posts-call-on-russians-to-join-separatist-forces

[10] hxxps://thecyberwire[.]com/stories/3d5750a3b0aa40eabc80357c2ab8eb55/hybrid-war-across-the-spectrum-of-conflict

In a future cyber attack, Russia could probably disable Ukraine's power grid, turn off heat supplies in the middle of winter, and shut down Ukraine's military command centers and cellular communication systems. A communications blackout could provide opportunities for a massive disinformation campaign to undermine the Ukrainian government.[11] The Russian military could cut power to Internet service provider (ISP) facilities, which enable Internet access, and Internet exchange points, which enable traffic between ISPs. These physical elements enable global Internet traffic; disrupting them would have international effects, forcing some traffic to be routed around Ukraine, but the worst effects would be felt within the country.[12]

Although it seems likely that Ukraine would bear the brunt of Russian cyber attacks, activity could spill over globally, affecting greater Europe, the US, and NATO countries—as it did in the 2017 NotPetya campaign, causing USD 10 billion[13] worth of damage. The NotPetya attack serves as a reminder that a widespread cyber attack can inflict damage on multiple business sectors, disrupting economic activity and interconnected supply chains.

What's next?

In this dynamic Ukrainian situation, hostile (but sometimes hopeful) rhetoric and strategic military moves are occurring daily. In just the past seven days, Russia has reportedly deployed medical personnel and blood supplies to support military troops near the border of Ukraine. On 02 Feb 2022, the US announced it was deploying 3,000 troops to Eastern Europe to bolster NATO defenses. Diplomatic solutions on all sides are being explored, and it is not clear yet whether this territorial dispute can be resolved quickly or peacefully. If history is any indicator, there is a realistic possibility that tension, or provocations, could inflame a larger cyber warfare campaign.

It is also realistically possible that Russia will decide to withdraw its troops. Some diplomats have argued that President Vladimir Putin has "overplayed his hand" by miscalculating NATO's response, and he may be looking to save face. Russia knows that a full-scale invasion of Ukraine would be extremely costly, in terms of resources, inevitable casualties, and the swift economic sanctions from NATO members that would follow. A drawn-out conflict could also be very unpopular for Putin in Russia. In any case, robust Russian cyber capabilities remain available and stealthy cyber action may still be used.

On 01 Feb 2022, the US presidential administration announced it was working with Ukraine to harden the latter's cyber defenses and warned that cyber attacks could be part of a "broad-based Russian effort to destabilize" and further invade Ukraine. As part of the defensive effort, the US sent its top cyber-security official, Anne Neuburger, to NATO, to inform

[11] hxxps://www.politico[.]com/news/2022/01/28/russia-cyber-army-ukraine-00003051

[12] hxxps://www.atlanticcouncil[.]org/blogs/new-atlanticist/cord-cutting-russian-style-could-the-kremlin-sever-global-internet-cables/

[13] hxxps://www.wired[.]com/story/russia-ukraine-destructive-cyberattacks-ransomware-data-wiper/#intcid=_wired-bottom-recirc_2e4adffc-b6f4-4792-86a8-106bb3835e0b_similar2-3-reranked-by-vidi

its members that "that the kinds of disruptive or destructive cyberactions possible during a conflict are different in scope, kind and sophistication from the types of incidents we have seen during peacetime."[14]

Ukraine is scheduled to conduct some long-planned activities in the coming weeks that involve disconnecting from Russian electricity supply networks and linking to other European power grids. However, this effort is preliminary, and would not likely be much help in any confrontation with Russia over the next few weeks.[15]

Sources	The information in this article is primarily derived from the Atlantic Council and Wired.
External source reliability	**A (Reliable)** Limited doubt about the source's authenticity, trustworthiness, or competency; history of reliability.
External information reliability	**2 (Probably true)** Logical, consistent with other relevant information, not confirmed.

[14] hxxps://www.nytimes[.]com/2022/02/01/us/politics/russia-ukraine-cybersecurity-nato.html
[15] hxxps://www.nytimes[.]com/2022/02/01/us/politics/russia-ukraine-cybersecurity-nato.html

Weekly Intelligence Summary

04 FEB 2022

Weekly highlights in brief

Intelligence cut-off date: 1200 UTC, 03 Feb 2022

Newbie group Ransom Cartel smacks of REvil

On 24 Jan 2022, cyber-security researchers reported on the emergence of a new ransomware group called Ransom Cartel. The group reportedly bears similarities to the now-defunct "REvil" ransomware group. For instance, when viewed using hex editor[16] tools, files encrypted by Ransom Cartel featured footers that resembled files encrypted by REvil. In addition, the format used for ransom notes was similar to that used by REvil, although such files and formats are easy to imitate. Researchers believe that Ransom Cartel comprises core members of REvil, despite the arrest of 14 REvil members in Russia in January 2022.

Threat actors use Glitch coding platform in malware attacks

On 20 Jan 2022, researchers published their findings on an attack campaign that delivered malicious Web Page Archive files (MHT or MHTML files) and used the coding platform Glitch for communication with command-and-control infrastructure. Victims who enabled macros in a file triggered the execution of malicious code. The files also contained obfuscated Visual Basic Application code, which dropped a Dynamic Link Library (DLL) in the disk. As a backdoor, the DLL enabled the attackers to obtain data from the compromised system. Analysis in 2021, by other researchers, indicated the involvement of the Vietnam-linked "APT32" (aka OceanLotus), but the latest report suggests other threat actors/groups.

FBI links Diavol ransomware to Wizard Spider group

On 20 Jan 2022, security researchers reported that the US FBI had formally linked the "Diavol" ransomware to the "Wizard Spider" cybercrime group. This followed observations of researchers made in June 2021, when they first detected Diavol in use. The researchers found that the ransomware had been deployed on the same network as the "Conti" ransomware had. Additionally, the two ransomware types bore similarities, such as their use of asynchronous input/output (I/O) operations for file encryption queuing and similar command-line parameters. At the time, there was insufficient evidence to link both operations to the same threat actor/group. Previously the FBI had formally linked Diavol to the TrickBot group, after the 2001 arrest of Alla Witte, a woman involved in developing the "TrickBot" malware.

[16] A computer program used to manipulate the binary data that forms a computer file

Language of uncertainty

Throughout this intelligence summary, Digital Shadows assessed probability using qualitative statements from a defined matrix, known as "the uncertainty yardstick." To give the reader perspective, each of these statements is associated with a probability range.

Qualitative statement	Associated probability range
Remote or Highly unlikely	<10%
Improbable or Unlikely	15–20%
Realistic possibility	25–50%
Probable or Likely	55–70%
Highly/Very probable/likely	75–85%
Almost certain	>90%

Source evaluation

Digital Shadows evaluated sources using qualitative statements from two defined matrices, scoring the reliability of sources and that of the information gleaned from them.

	Source	Description
A	Reliable	Limited doubt about the source's authenticity, trustworthiness, or competency; history of reliability
B	Usually reliable	Minor doubts; history of mostly valid information
C	Fairly reliable	Doubts; provided valid information in the past
D	Not usually reliable	Significant doubts; provided valid information in the past
E	Unreliable	Lacks authenticity, trustworthiness, and competency; history of invalid information
F	Cannot be judged	Insufficient information to evaluate reliability; may or may not be reliable

	Information	Description
1	Confirmed	Logical, consistent with other relevant information, corroborated by independent sources
2	Probably true	Logical, consistent with other relevant information, not confirmed
3	Possibly true	Reasonably logical, agrees with some relevant information, not confirmed
4	Doubtfully true	Not logical but possible, no other information on the subject, not confirmed
5	Improbable	Not logical, contradicted by other relevant information
6	Cannot be judged	The validity of the information cannot be determined

Analytical techniques

To provide objective, robust and quality intelligence, Digital Shadows uses a variety of analytical techniques in our products. They include the Analysis of Competing Hypotheses (ACH), Devil's Advocacy, A & B Teaming and Key Assumption Checks. To guard against biases, such as groupthink, confirmation bias and mirror imaging, Digital Shadows' analysts are educated in how to avoid such pitfalls, and their work is subjected to rigorous peer reviews. To learn more about threat intelligence, see our blog article on intelligence tradecraft: https://www.digitalshadows.com/blog-and-research/threat-intelligence-a-deep-dive/