FINAL

HOUSE HOMELAND SECURITY COMMITTEE

Adam Meyers
Senior Vice President, Intelligence
CrowdStrike

Testimony on Securing Critical Infrastructure Against Russian Cyber Threats

March 30, 2022

I. Introduction

Chairman Thompson, Ranking Member Katko, and Members of the Committee, thank you for the opportunity to testify today. As the world watches the conflict in Ukraine unfold, cybersecurity professionals are on high alert. Colleagues from across Government and Industry are monitoring the use of cyber means within the conflict itself and preparing for the possibility of Russian attacks abroad–either for the purposes of retaliation or coercion. This hearing evaluating critical infrastructure security posture is particularly timely.

Since 2011 I have built and led the intelligence team at CrowdStrike, a commercial security technology company headquartered in the United States with offices around the globe. In my capacity as the head of Intelligence, I manage a team of more than 200 professionals who conduct research on threat actors operating for state interests like espionage; financially-motivated or criminal purposes; and to advance “Hacktivist” goals. This team tracks the technical, cultural, and behavioral aspects of these attacks to identify and attribute threat actors, extrapolate how they operate, and determine what can be done to mitigate these actions. Prior to CrowdStrike, I worked to secure the defense industrial base (DIB), where I supported numerous federal customers across the military, intelligence community, and various civilian agencies in information security matters.

The CrowdStrike Intelligence team has supported cybersecurity initiatives for the U.S. Government and key allied governments around the globe. We actively participate in public-private partnerships, such as the Cybersecurity and Infrastructure Agency’s (CISA) Joint Cyber Defense Collaborative (JCDC), through which we have worked over the past few weeks with select industry partners to disrupt malicious Russian cyber infrastructure. Previously, we facilitated botnet disruptions such as the coordinated take down of the Kelihos botnet in partnership with the Department of Justice (DoJ)/Federal Bureau of Investigation (FBI)--the careful timing of which enabled the arrest, extradition to the U.S., and successful prosecution of the operator. Through our research, technology, and partnership, it is CrowdStrike’s goal to raise the cost of doing business for threat actors across the spectrum of cyber adversaries.

II. Cyber Activity Associated with the Conflict in Ukraine[1]

In the immediate lead up to the 2022 military conflict in Ukraine, several Russian-state nexus threat actors engaged in espionage as well as disruptive and destructive attacks against government and commercial targets. The commencement of the conflict also activated Russian eCrime and "Hacktivist" actors. I will survey developments with each in turn, following a brief discussion of the recent history of Russian threat activity targeting Ukraine.

II.1. Background

Russia has a long history of leveraging cyber operations to effectuate political goals in Ukraine. Russian cyber operations against Ukraine began in earnest following the Euromaidan protests which began in late 2013. The Main Center for Special Technologies (GTsST), Unit 74455 of Russia's military intelligence organization,[2] which CrowdStrike tracks as *VOODOO BEAR*,[3] has been one of the major perpetrators of these offensive operations. The overarching motivation for *VOODOO BEAR* activities is to contribute to psychological operations seeking to degrade, delegitimize, or otherwise influence public trust in state institutions and industry sectors in target countries, including government, energy, transportation, and media organizations.

This adversary was behind notorious incidents such as disruptions to Ukrainian Critical Infrastructure resulting in power outages in both December 2015, and a year later, as well as campaigns targeting media, transportation, and electoral infrastructure. *VOODOO BEAR* operations created wider concern for the international community in June 2017 when a supply chain attack against a financial software update mechanism resulted in the deployment of *NotPetya*, a self-propagating destructive weapon masquerading as ransomware. The impact of the *NotPetya* incident by some estimates caused USD $10 Billion in total damage and impacted global companies and public services in a variety of sectors, including critical infrastructure providers.[4]

[1] I have endeavored to cite as much source material as possible for this testimony. In some instances, however, it was most prudent to redact details like URLs. In other instances, I've cited limited-distribution CrowdStrike research. Additional information and materials are available to Committee staff upon request.
[2] Redesignated the *Main Directorate of the General Staff of the Armed Forces of the Russian Federation*, researchers and analysts still widely refer to this organization by its former acronym, *GRU*.
[3] CrowdStrike uses a cryptonym-based system to designate threat actors we track. Names generally take the form of a community- or researcher-derived codeword with some significance, followed by an animal type based on the actor's geography or motivation. This naming scheme is designed to be somewhat more descriptive than others, and can simplify and disambiguate communication and information sharing with government and industry counterparts, as well as assist customers' threat modeling processes. *See* Adam Meyers, *Meet The Threat Actors: List of APTs and Adversary Groups*, CrowdStrike Blog (Feb. 24, 2019), https://www.crowdstrike.com/blog/meet-the-adversaries/. Most notably for the purposes of this discussion, we use *BEAR* for Russian state-nexus actors, *SPIDER* for criminal actors, and *JACKAL* for hacktivist actors.
[4] Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, WIRED (Aug. 22, 2018, 5:00 AM), https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Another threat actor, which CrowdStrike tracks as *PRIMITIVE BEAR*, has conducted widespread espionage against Ukrainian government targets since 2014. Believed to be operating from the city of Simferopol in Crimea, this actor represents an offensive cyber capability established specifically in a conflict region to facilitate rapid tasking and collection.

Numerous other adversaries[5] have contributed to the broader asymmetric campaign waged against Ukraine. One notable example observed in 2014 was a coordinated campaign targeting the Central Election Commission (CEC) and Ukrainian media sector which CrowdStrike attributes in part to *BERSERK BEAR, a component* of the Federal Security Service of the Russian Federation (FSB), and in part to the CyberBerkut hacktivist front.[6] Taken together, this campaign intended to deliver effects against strategic targets in the effort to undermine the democratic process within Ukraine.

II.2. Current Nation-State Activity

As Russia began to amass forces on the Ukrainian border, Russian cyber threat activity targeting the nation increased in kind. In mid-January 2022, a campaign of website defacement and data theft impacted numerous Ukrainian government entities contemporaneously with a wiper attack that the security industry has dubbed *Whispergate*.[7] The website defacements included messaging in Ukrainian, Russian, and Polish language that was of a threatening nature, and an image with metadata suggested the activity originated in Poland. The wiper attack and website defacements occurred immediately following a series of bilateral meetings between the U.S. and Russia regarding troop deployments near the Ukrainian border. Following the defacement and wiper attacks, several personas emerged in online underground forums offering data stolen in these incidents. CrowdStrike currently associates these activities with the Russian-nexus threat actor designated *EMBER BEAR*, an adversary group that has operated against government and military organizations in eastern Europe since early 2021.

In mid-February, various Ukrainian banking and governmental websites were targeted as part of a large-scale distributed denial-of-service (DDoS) attack.[8] This included the websites of Ukraine's Ministry of Defense and Armed Forces as well as the website of the State Savings Bank of Ukraine (Oschadbank) and the mobile application of Ukraine's largest commercial bank, PrivatBank. In concert with the DDoS attack, some banking customers were targeted with SMS messages falsely indicating ATM systems were not functioning, and bomb threats were made against several bank locations. The DDoS attacks were later attributed by various government

[5] *FANCY BEAR*, *COZY BEAR*, and *RepeatingUmbra* — which strongly overlaps with an adversary tracked as *UNC1151* in the broader information security industry — actively conducted espionage campaigns targeting Ukraine within the last year.
[6] Brian Yates, *CyberBerkut Attempt to Alter Ukrainian Election*, Guardianlv (May 25, 2014), https://guardianlv.com/2014/05/cyberberkut-attempt-to-alter-ukrainian-election/.
[7] CISA, *Alert (AA22-057A): Destructive Malware Targeting Organizations in Ukraine* (last revised Mar. 1, 2022), https://www.cisa.gov/uscert/ncas/alerts/aa22-057a.
[8] *Attention: There is No Threat to the Funds of Privatbank Depositors* (Feb. 15, 2022), https://spravdi.gov.ua/uvaga-zhodnoyi-zagrozy-dlya-koshtiv-vkladnykiv-pryvatbanku-nemaye/.

officials to the Main Intelligence Directorate of the General Staff of the Armed Forces of the Russian Federation ("GRU").

On 23 February 2022 a second wiper attack was identified, which CrowdStrike tracks as *DriveSlayer*. More technically sophisticated than the *WhisperGate/EMBER BEAR* activity from January, *DriveSlayer* is propagated by a worm the broader cybersecurity industry tracks under the name *HermeticWizard*. The technical complexity and overlap of tactics is consistent with previous operations attributed to *VOODOO BEAR*. In what might be construed as a lesson learned from *NotPetya's* rampant spread, *HermeticWizard* was intentionally designed to limit its spread to the local network, theoretically limiting infections primarily to networks in Ukraine.

On 24 February 2022, several Ukrainian government websites were displaying a defacement message before becoming unresponsive to visitor requests. The displayed message was almost identical to the one used in defacement activity against similar targets on 14 January 2022. Soon after the *DriveSlayer* wiper attack and website defacements, Russian troops attacked Ukraine. In the weeks since the commencement of military conflict numerous other incidents have been identified including additional wiper attacks, misinformation, and espionage against Ukrainian targets.

Although beyond the scope of this testimony, I would at least like to note two other forms of activity associated with this conflict. The first is reported destructive attacks targeting Ukrainian satellite communications capabilities.[9] The second is informational or psychological operations-type activities, likely including amplification through personas and propagation through social media. Elements of the researcher community are monitoring these types of operations, and information about their scope and effects is likely to become clearer over time.

II.3 eCrime

The conflict in Ukraine has also impacted–perhaps even reshaped–the criminal cyber threat ecosystem. This is notable because Russia has long harbored, and potentially leveraged for policy or political ends, eCrime threat actors. These adversaries now have the potential to act in support of Russian state goals, such as by acting as an irregular component, performing disruptive attacks around the globe and specifically in the United States.

In the immediate wake of the invasion of Ukraine, eCrime actors who are responsible for financially-motivated malicious cyber activity began responding to the conflict. Some actors appeared to directly support Russian state interests. *WIZARD SPIDER*,[10] an adversary that first surfaced in 2016 with their *Trickbot* malware, and is more recently associated with several ransomware operations including *Ryuk* and *Conti,* announced their full support of the Russian

[9] Ellen Makashima, *Russian Military Behind Hack of Satellite Communication Devices in Ukraine at War's Outset, U.S. Officials Say*, Washington Post (Mar. 24, 2022, 10:25 PM), https://www.washingtonpost.com/national-security/2022/03/24/russian-military-behind-hack-satellite-communication-devices-ukraine-wars-outset-us-officials-say/.

[10] *WIZARD SPIDER* is not associated with the *HermeticWizard* wiper malware described above; the naming overlap is coincidental.

government and their willingness to retaliate against critical infrastructure entities.[11] Other groups such as *SALTY SPIDER,* the operator of the *Sality* botnet, and *SCULLY SPIDER,* operator of the *Danabot* infrastructure, recently engaged in DDoS attacks uncharacteristic of their previous operations, against Ukrainian targets. It is unknown whether these incidents were motivated by patriotism, conducted at the direction of Russian security services, or followed some other motive such as financial gain.

In other cases, the criminal ecosystem broke with Russian members over the invasion. For example, some criminal forums–digital bazaars for buying and selling stolen information and tools for offensive cyber operations–began banning users associated with Russian Internet Protocol (IP) address space as a sort of criminal community-driven sanction in response to the Russian aggressions against Ukraine.[12] However, anti-Russian sentiment in the eCrime space was not widespread, and most of the criminal groups tracked by CrowdStrike signaled that they were apolitical and primarily focused on revenue generation, consistent with their general modus operandi. Some groups have actually used the conflict as fodder for conducting operations, inserting malicious components into varying participatory DDoS tools marketed at individuals who want to lend their computers to attacks against Russia in response to the conflict. Ever opportunistic, some criminally motivated actors have used the conflict in Ukraine as material for lures, or implanted information stealers in participatory DDoS tools designed for individuals who wish to engage in hacktivism against Russian targets but lack the technical sophistication to launch attacks on their own.

II.4 Hacktivism

The conflict catalyzed a significant level of both pro-Russian and pro-Ukrainian hacktivism. On the pro-Russian side, *Killnet*—a low-level Russian eCrime group—turned to hacktivism in response to Ukraine's coordinated effort to unite pro-Ukraine hacktivists, including the so-called *IT Army of Ukraine*.[13] *Killnet* claimed a series of DDoS attacks beyond Ukraine's borders and against websites controlled by the Polish and Latvian governments. Killnet also claimed a DDoS attack against the website of the National Bank of Poland. In a social media post, the group called the attack against the bank a "warning" and included links to the National Bank of Poland website as well as an online tool for checking website availability. The group threatened to target the Polish government if Warsaw escalated tensions between NATO and Russian forces in the region. Specifically, the group vowed to encrypt "all information systems with internet access" in Poland. In the warning, *Killnet* also issued a "reminder" about *REvil* (ransomware developed by the eCrime adversary *PINCHY SPIDER*) and a recent high-profile ransomware attack against a U.S. critical infrastructure operator.

[11] In response to this announcement, a security researcher released logs of internal communications of this group exposing their composition, internal structure, recruitment strategies, financial infrastructure, and future ambitions. These leaks provided an unprecedented view into the internal machinations of a several hundred person organization built for the express purpose of conducting extortion, theft, and other criminal enterprises against western organizations and critical infrastructures.
[12] CrowdStrike Intelligence Reporting, Feb. 25, 2022.
[13] *Russian Killnet Hackers Brought Down Anonymous Website*, Ren.TV, (Mar. 1, 2022), [*Source URL available to Committee Staff by request*.]

Pro-Ukrainian Hacktivism observed or reported to date includes:[14]

- *Anonymous*. Since at least mid-February 2022, affiliates of the hacktivist collective *Anonymous* advertised their intent to conduct cyber operations should tensions in Ukraine escalate. Self-identified *Anonymous* affiliates have claimed responsibility for dozens of incidents since late February, including DDoS attacks, website defacements, and leaks. *Anonymous* affiliate's claims are frequently exaggerated, however CrowdStrike has confirmed significant data leaks from Russian-state-owned energy company Rosneft, Russia's censorship agency Roskomnadzor, Russia's state-controlled oil pipeline company Transneft, and the Central Bank of Russia. Some affiliates have also claimed more disruptive attacks, including destroying back-up images of mobile phones and file directories from Rosneft and a brief take-over of multiple Russian State media organizations to broadcast footage of the war in Ukraine.
- *PARTISAN JACKAL*. *The Cyber Partisans*, which CrowdStrike tracks as *PARTISAN JACKAL*, signifying its hacktivist motivation, issued a statement on social media calling on "like-minded hackers" in Ukraine and Russia to join forces against the "fascist campaign" Russia has launched against "brotherly" Ukraine. This statement followed a 24 February 2022 post announcing the formation of the "Belarus Tactical Group" consisting of members of multiple other resistance groups that *PARTISAN JACKAL* supports. *PARTISAN JACKAL* previously responded to Russia's troop presence in Belarus by encrypting several systems controlled by state-owned railway operator Belarusian Railway.
- *CURIOUS JACKAL*. Personas associated with Spanish-speaking actor *KelvinSecTeam,* tracked as *CURIOUS JACKAL*, published several posts on forums and social media detailing recent targeting of the Russian government. This included posts with at least 668 seemingly legitimate government files, information on the state media outlet RT, and surveillance video purportedly from inside a nuclear power plant in Russia.
- *Ukrainian Government*. As the military conflict began, the Ukrainian government reportedly started recruiting a volunteer cyber force, the IT Army of Ukraine. Advertisements for volunteers began circulating on hacker forums, calling on Ukrainian forum members to "get involved in the cyber defense of our country." The forum posts reportedly directed users to an application asking volunteers for areas of specialty and professional references. The volunteers are reportedly divided into defensive and offensive units.[15] CrowdStrike has observed the offensive units use social media outlets to coordinate DDoS attacks against Russian government and private industry websites.
- *Unknown actors*. Unidentified hacktivists defaced the Russian Emergency Situations Ministry website. The hacktivists replaced a ministry hotline number with a number Russian soldiers could use to defect, changed news items on the front page to "Don't Believe Russian media–they lie", and posted a link offering "full information about the

[14] Except where otherwise noted, information in this subsection is derived from CrowdStrike Intelligence Reporting, Jan.-Feb. 2022.

[15] Joel Schectman and Christopher Bing, *EXCLUSIVE Ukraine Calls on Hacker Underground to Defend Against Russia*, Reuters (Feb. 24, 2022, 6:51 PM), https://www.reuters.com/world/exclusive-ukraine-calls-hacker-underground-defend-against-russia-2022-02-24/.

war in Ukraine." The same day, likely hacktivists posted insults aimed at President Putin and Russians on Russian judicial websites.[16]

- *Supply chain*. In one deeply concerning incident, the maintainer of 'node-ipc' a popular open source coding component altered it to effectuate a targeted supply chain attack to protest Russia's invasion of Ukraine. The maintainer released a sabotaged version of the software that included malicious code that would delete files or overwrite them with a heart emoji for users based in Russia and Belarus, as determined by the system's external IP address. The affected module is used as a dependency in many nodejs-based applications, which were also impacted by the malicious node-ipc versions. The unintended consequences of this supply chain attack have not been fully assessed, but it stands to erode trust in open source software and damage the credibility of such projects.[17]

III. U.S. Critical Infrastructure Readiness

Since long before the current conflict in Ukraine, U.S. national security officials and cybersecurity industry analysts have raised concerns about Russia's demonstrated capabilities and potential intentions to attack U.S. critical infrastructure. Periodic breaches of operators in this space, attributed to Russia-nexus actors, illustrate that U.S. infrastructure could at least be held at risk, and possibly attacked, degraded, and destroyed, during a time of heightened geopolitical tensions. As the war in Ukraine drags on without Russia achieving its political objectives, and as sanctions by the U.S. and allies mount in scope and impact, the risk of such attacks becomes more acute.

U.S. critical infrastructure operators, for their part, are increasingly focused on this threat. The U.S. government, through collective efforts of the White House, CISA, the Department of Energy, and other Sector Risk Management Agencies, have rolled out a variety of awareness and assistance campaigns over the years to help strengthen infrastructure entities' security posture. There have been improvements over the past decade, albeit from a sometimes low baseline of readiness. Defensive capabilities also differ significantly across sectors. For structural reasons, we see different resourcing and outcomes across sectors like financial services and water utilities, for example.

IV. U.S. Government Support and Coordination Mechanisms

White House public statements and reported notifications and offers of assistance to state government leadership; the CISA #ShieldsUp campaign; and well-timed DoJ indictments represent an unprecedented level of communications engagement on cybersecurity from Executive Branch leadership. These are all positive steps from an awareness perspective.

---

[16] Mary Ilyushina, *Russian Government Website Face 'Unprecedented' Wave of Hacking Attacks, Ministry Says*, Washington Post (Mar. 17, 2022, 8:29 AM), https://www.washingtonpost.com/world/2022/03/17/russia-government-hacking-wave-unprecedented/.

[17] Adam Bannister, *NPM Maintainer Targets Russian Users with Data-Wiping 'Protestware'*, Daily Swig (Mar. 21, 2022), https://portswigger.net/daily-swig/npm-maintainer-targets-russian-users-with-data-wiping-protestware.

The U.S. Government has made significant strides over the past few years in coordinating with industry against cyber threats. The establishment of JCDC in particular, where CrowdStrike participates as a plankholder organization, has helped strengthen cybersecurity and IT industry and government collaboration and information sharing. Parallel efforts by nongovernmental organizations as well as other agencies with different authorities and mandates also help the community. Many of these have formed organically over the years, and in my assessment, contribute to a healthy ecosystem. Mature entities like CrowdStrike and others in the cybersecurity industry can support participation in multiple groups organized around different themes, interests, and relationships so long as there is marginal value–and this ultimately promotes sharing.

Beyond the cybersecurity industry, businesses and critical infrastructure operators have significant limitations and constraints on time, attention, and resources. Those seeking support or fulfilling regulatory obligations presently collaborate through some or all of CISA, a different Sector Risk Management Agency, and the FBI. Views within the community differ about the extent to which the status quo “choose your partner”-style system is equal to the threats we face, and my co-panelists are better suited than me to address the efficacy for their respective sectors. I will just note here that the recent consolidation of Incident Reporting under CISA appears likely to promote rapid analysis and dissemination of threat indicators and trends, which can improve security posture across the board.

V. Conclusions and Recommendations

Russian state actors have used cyber means over the years to advance its political agenda, and that continues in the context of the ongoing war in Ukraine. Events there have also affected the shape of the broader eCrime ecosystem and activated both pro-Russia and pro-Ukraine hacktivism. Outside the immediate theater of conflict, Russian activity to date has been modest relative to early fears. However, this could change at any time and indeed there are indications that Russia may become more aggressive in retaliation for foreign support to Ukraine and significant sanctions on Russian personnel and entities. U.S. critical infrastructure operators must remain on high alert. With significant media coverage and the efforts of U.S. Government actions and warnings described above, it appears that private sector entities are increasingly taking note.

But even with awareness sufficiently raised, and new resources and support, critical infrastructure operators must still “do” cybersecurity well. This is a “last mile” problem that cannot be solved through policy initiatives alone. Though not an exhaustive list, entities should:

- Build relationships with law enforcement or homeland security staff that can help during an incident.
- Develop or maintain access to know-how and skilled workers or support staff. This includes having an incident response plan in place and, in many cases, a retainer with a qualified provider of incident response services.

- Levage measures identified in Executive Order 14028 on *Improving the Nation's Cybersecurity*. This includes use of modern IT enterprise security tools and concepts like Multi-Factor Authentication (MFA) and Endpoint Detection and Response (EDR); sufficient logging; migration where practical to cloud/Software-as-a-Service (SaaS) applications; implementation of Zero Trust Architectures; and proactive threat hunting for adversaries within their networks.
- Utilize, where appropriate, specialized tools and capabilities required for Operational Technology (OT) security.

For small and medium sized organizations–say, those with fewer than 6 or 8 dedicated cybersecurity staff–one of the biggest "needle movers" in recent years has probably been the increasing adoption of managed security service providers (MSSP)/managed Detection and Response (MDR) providers. This is a trend that should be encouraged and incentivized.

Congress' efforts in recent years implementing Cyberspace Solarium Commission recommendations and, most recently, Incident Reporting measures will absolutely help. In addition, consider:

- Ensuring CISA is sufficiently resourced to carry out both its Federal Civilian Executive Branch (FCEB) and private sector/infrastructure security mandate.
- Strengthening FCEB cybersecurity by modernizing the Federal Information Security Management Act (FISMA) to reduce compliance burdens and Federal Risk and Authorization Management Program (FedRAMP) to speed authorizations.
- Expanding the use of shared services procurement models for Federal IT to create operational efficiencies, particularly for cyber threat intelligence and adoption of state-of-the-art cybersecurity technologies.
- Working with CISA to guarantee that new Incident Reporting mandates do not become overly burdensome to victims and reduce focus on remediation during a cyber incident or event.
- Taking measures to expand national incident response capacity.

I'll close by briefly referencing efforts CrowdStrike has undertaken to support defensive efforts during this time of increased risk. As noted above, we have collaborated with organizations like JCDC to address active campaigns. As always, we endeavor to openly publish through our blog materials that might help the community understand emerging threats and threat actors, and we will continue to do that as appropriate. We have taken special measures to strengthen defenses of current customers, and in consultation with government partners we collaborated with industry counterparts Cloudflare and Ping Identity to launch a free Critical Infrastructure Defense Project for the Energy, Water, and Hospital sectors.[18] We encourage eligible entities to consider participating in this program.

Thank you for the opportunity to testify before you today. I look forward to your questions and our continued discussion.

###

[18] *Rapidly Improving Cyber Readiness for U.S. Critical Infrastructure*, Critical Infrastructure Defense Project, https://criticalinfrastructuredefense.org/.