accenture

Global Incident Report: Russia Ukraine Crisis

Summary

A succession of events in January 2022, including a buildup of approximately 100,000 Russian troops on Ukraine's border, have raised fears that Russia plans to invade Ukraine during the first months of 2022. A kinetic offensive would probably also trigger a number of cyber and financial repercussions, potentially affecting parties in multiple locations, including Russia, Belarus, Ukraine, North Atlantic Treaty Organization (NATO) countries, and/or their allies, according to United States (US) and the United Kingdom government assessments.

Analysis

Within Ukraine, essential businesses and government services, such as those related to commerce, electricity, and transportation, could experience disruptions like those resulting from the CRASHOVERRIDE and Petya/NotPetya attacks of 2016-2017, should an invasion occur. Threat groups aligned with Russian government interests and Russia-sympathetic hacktivists could also use cyber threat activity to discredit the current Ukrainian government and undermine the population's will to fight. Other potential cyber activity could include purposeful oversight or omission of information to counter criminal ransomware or other disruptive attacks against governments or critical infrastructure. Depending upon how the crisis unfolds, malicious actors aligning themselves with Russian interests could remain the greatest threat; however, other malicious actors may attempt to take advantage of the situation by increasing their activities, which could potentially include conducting false-flag operations.

If diplomacy efforts fail and Russia actually invades Ukraine, there is possibility that Western countries may follow through on threats to cut Russia off from the SWIFT financial messaging service. If this were to happen, anyone doing business with Russia could also experience economic activity disruptions. Further, organizations in or doing business with Russia or its neighboring countries might see the invocation of emergency censorship and restrictions on Internet traffic.

Although this situation continues to evolve, several noteworthy cyber-related events have already occurred. On 15 January 2022, Microsoft published a blog stating it had identified a destructive malware, disguised as ransomware that Microsoft dubbed "WhisperGate," on dozens of Ukraine-based government, nonprofit, and IT organizations.[11] Outside of Ukraine, NATO members also incurred targeting: on 19 January 2022 a cyber attack disabled certain functions of Global Affairs Canada (GAC),

[1] https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/.

the country's diplomatic and external affairs agency, after Canadian officials extended their support to Ukraine.[2]

Meanwhile, mixed messages have come out of Russia, which continues to build up troops and conduct military exercises near Ukraine but which has also conducted negotiations with diplomats and businesspeople from Europe and the US.

Related Threat Groups and Capabilities

Several threat groups that align themselves with Russian interests are active against Ukraine and its supporters. Notably, some groups do carry out destructive attacks, primarily against Eastern Europe's critical infrastructure. Although these groups are highly regimented in their missions and target sets, the spillover from these events could affect organizations outside of the initial target sets, as seen with the NotPetya attacks in 2017, the fallout of which was partly due to the potency of ShadowBroker exploits that facilitated the extremely wormable wiper campaign. Likewise, threat groups that align themselves against Russian interests also exhibited the capacity to disrupt critical infrastructure. One such threat group disrupted Belarus railway system operations on 24 January 2022 with the claimed intent of slowing the movement of Russian troops through that country to Ukraine's borders.[3]

Primary State-Sponsored Groups

Accenture Cyber Threat Intelligence (ACTI) assesses the following groups are most active within Ukraine and Eastern Europe:

- SANDFISH (a.k.a. Sandworm, TeleBots, Quedagh, BlackEnergy, Voodoo Bear, TEMP.Noble, GreyEnergy): This threat group has carried out a wide variety of attacks, targeting political entities, the press, and critical infrastructure. These attacks include the 2015 and 2016 blackouts in Ukraine and the June 2017 NotPetya pseudo-ransomware campaign.
- WINTERFLOUNDER (a.k.a. Gamaredon Group, Calisto Group, Dancing Salome): This group's social engineering campaigns targeted the Ukrainian government, military, and law enforcement agencies during 2014 and 2015 (among other time), reaching peaks during the heaviest fighting between Ukrainian national forces and pro-Russian separatists. While more recent targeting by WINTERFLOUNDER suggests Ukrainian collection is still a priority, ACTI has also observed additional targeting in Eastern Europe, suggesting WINTERFLOUNDER's scope may widen as tensions increase.
- WALLEYE (a.k.a. Zebrocy, Earworm): Based on who its victims have been since as early as 2018, WALLEYE's traditional intelligence mission focuses on gathering intelligence against state institutions, security bodies, and military industries in Eastern Europe, the Middle East, and South and Central Asia. While WALLEYE may sometimes share infrastructure with other groups, WALLEYE's toolset and

[2] https://www.infosecurity-magazine.com/news/cyberattack-on-global-affairs/

[3] https://www.thedrive.com/the-war-zone/44066/cyberattack-targets-belarus-rail-network-to-slow-flood-of-russian-forces-into-the-country.

targeting remains distinct. There is little known WALLEYE targeting of Western European or North American countries.

Recent WhisperGate Activity

Based on ACTI analysis, there are a few similarities between the mid-January 2022 WhisperGate campaign and SANDFISH's June 2017 NotPetya campaign. Both campaigns masqueraded as ransomware campaigns and employed a chain of compromise that several cyber criminal groups have leveraged. In particular, artifacts from both campaigns suggest a victim can recover files by paying a ransom when in fact the malicious code runs a Master Boot Record (MBR) wiper and a file corrupter makes files on the victim system unrecoverable. Although there are similarities, ACTI assesses this general overlap in modus operandi across the WhisperGate and NotPetya campaigns is insufficient to draw any further conclusions, as such overlaps could occur across many wiper or corrupter campaigns.

Mitigation

To mitigate the threat of cyber threats stemming from fears of an escalation of hostilities between Russia and Ukraine, Accenture's Cyber Investigation and Forensics Response (CIFR) team suggests the following high-priority tactical mitigations and secondary strategic mitigations:

High-priority tactical mitigations:

- Patching externally facing infrastructure (VPN appliances, firewalls, web servers, load balancers, etc.) to the latest supported vendor releases, as threat actors often exploit vulnerabilities in externally facing infrastructure to gain initial access to an environment.
- Auditing domain controllers to log successful Kerberos TGS (ticket-granting service) requests and monitoring such events for anomalous activity.
- Having an adequate incidence response (IR) retainer in place to provide necessary surge support and domain-level IR expertise in the event of an incident.
- Treating malware detections for Cobalt Strike and webshells with high priority, as an attacker could use them for lateral movement and persistence.
- Testing and conducting backup procedures on a frequent, regular basis and isolating backups from network connections that could enable malware spreading.

Secondary strategic mitigations:

- Monitoring service accounts and administrator accounts for signs of credential misuse and abuse, especially for accounts that should not have interactive logon rights.
- Monitoring installation of file transfer tools such as FileZilla and rclone as well as the processes associated with compression or archival tools.

- Creating, maintaining, and periodically exercising a cyber incident response and continuity of operations plan.
- Identifying a resilience plan that addresses how to operate, given a loss of access to or control of an information technology (IT) and/or operational technology (OT) environment.
- Implementing network segmentation between IT and OT networks, where appropriate.
- Looking for processes and program execution command-line arguments that may indicate credential dumping, especially checking for attempts to access or copy the ntds.dit file from a domain controller.
- Monitoring network traffic for unusual spikes in outbound activity, especially to unusual networks such as VPS and VPN providers as well as the TOR network.
- Identifying, detecting, and investigating abnormal activity that may indicate lateral movement by a threat actor or malware, and using host-based logs and monitoring tools, such as an endpoint detection and response (EDR) tool, and network monitoring tools.

About Accenture

Accenture is a global professional services company with leading capabilities in digital, cloud and security. Combining unmatched experience and specialized skills across more than 40 industries, we offer Strategy and Consulting, Interactive, Technology and Operations services — all powered by the world's largest network of Advanced Technology and Intelligent Operations centers. Our 674,000 people deliver on the promise of technology and human ingenuity every day, serving clients in more than 120 countries. We embrace the power of change to create value and shared success for our clients, people, shareholders, partners and communities. Visit us at accenture.com.

Accenture Security is a leading provider of end-to-end cybersecurity services, including advanced cyber defense, applied cybersecurity solutions and managed security operations. We bring security innovation, coupled with global scale and a worldwide delivery capability through our network of Advanced Technology and Intelligent Operations centers. Helped by our team of highly skilled professionals, we enable clients to innovate safely, build cyber resilience and grow with confidence. Follow us @AccentureSecure on Twitter, LinkedIn or visit us at accenture.com/security.

Accenture Cyber Threat Intelligence, part of Accenture Security, has been creating relevant, timely and actionable threat intelligence for more than 20 years. Our cyber threat intelligence and incident response team is continually investigating numerous cases of financially motivated targeting and suspected cyber espionage. We have over 150 dedicated intelligence professionals spanning 11 countries, including those with backgrounds in the Intelligence Community and Law Enforcement. Accenture analysts are subject matter experts in malware reverse engineering, vulnerability analysis, threat actor reconnaissance and geopolitical threats.