10 Takeaways On Diplomacy, War, And Cyber Operations From The Microsoft Special Report On Ukraine

Susanna Cox | CX7
2022.05.01

On 27 April 2022, Microsoft released a special report on cyber operations in Ukraine, as the Russian military offensive in the region continued and the world's technologists braced for additional cyber incidents anticipated after a string of destructive cyber events in early 2022. The report is rich with forensic and anecdotal evidence around Russian-Ukrainian cyber operations, and how these correlate with critical events along the diplomatic and military timeline. Here are ten key takeaways:

1. Attacks have been tied to all three of Russia's main security services: GRU (ГРУ РФ), SVR (СВР РФ), and FSB (ФСБ РФ).

Russian security is officially handled by three agencies, each with its own area(s) of operations. These are the Foreign Intelligence Service / *Служба внешней разведки Российской Федерации* (SVR RF), which handles external intelligence gathering and espionage; the GRU RF, or *Гла́вное управле́ние Генера́льного шта́ба Вооружённых сил Росси́йской Федера́ции*, operating in the military intelligence domain; and the Federal Security Service (FSB RF), or *Федеральная служба безопасности Российской Федерации,* considered to be the successor agency to the KGB. All three agencies were listed in the Microsoft report as linked to attacks on Ukrainian targets (fig 1).

2. Attacks allowed both immediate access for damage and exfiltration, and persistence for longer term espionage and access.

The report notes that cyber attacks were not simply a one-time event; attackers had long-term designs for access to key Ukrainian systems:

Based on our observations, known and suspected Russian nation-state actors are working to compromise organizations in regions across Ukraine. These actors use a variety of techniques to gain initial access to their targets, including phishing campaigns, exploiting unpatched vulnerabilities in on-premises Exchange servers, and compromising upstream IT service providers. This initial access allows them to conduct operations for destruction, data exfiltration, and persistence for longer-term espionage and surveillance. (3)

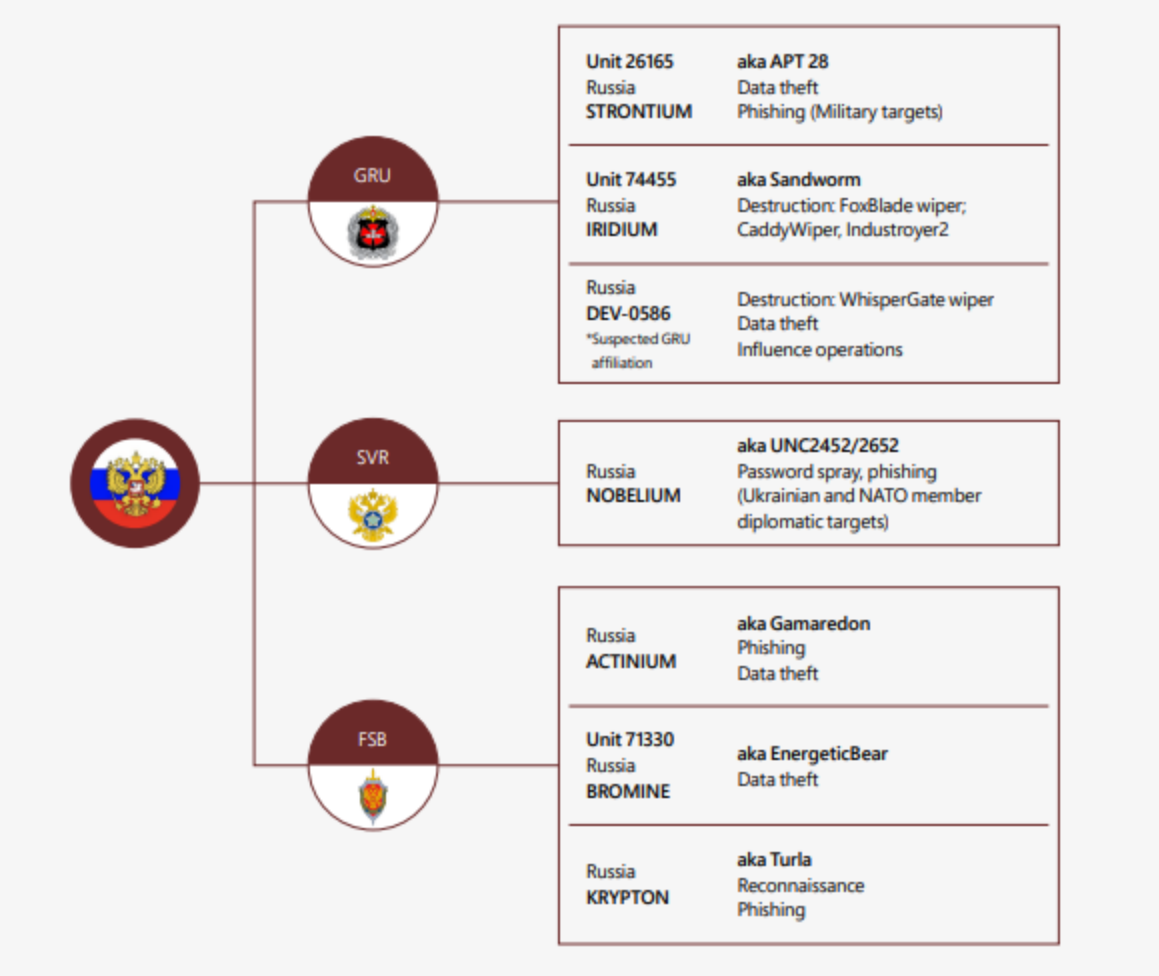

Figure 1. Image source: Microsoft. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

3. Not only did attackers use persistent tools, they also infiltrated Ukrainian IT providers to ensure mass spread and further destruction.

Attackers exploited a password reset vulnerability via a government IT contractor called Kitsoft to infiltrate and deface Ukrainian government systems:

Threat actors also established the access and persistence on networks for future destructive attacks. In late 2021, suspected Russian cyber actors positioned themselves in networks of Ukrainian energy and IT providers that were later targets of destructive attacks, including Kitsoft, the IT service provider that DEV-0586 compromised to facilitate destruction on the networks of several clients in January 2022. (6)

4. Attackers did not stop with IT providers: government and private sector were also targeted.

The original **Microsoft report** on the *DEV-0586* malware incident notes the targeting and successful infiltration of IT, non-profit, and even government systems. It also states that these likely do not represent the full extent of the attacks:

At present and based on Microsoft visibility, our investigation teams have identified the malware on dozens of impacted systems and that number could grow as our investigation continues. These systems span multiple government, non-profit, and information technology organizations, all based in Ukraine. We do not know the current stage of this attacker's operational cycle or how many other victim organizations may exist in Ukraine or other geographic locations. However, it is unlikely these impacted systems represent the full scope of impact as other organizations are reporting.

In fact the scale of infiltration was so great as of January 2022 that Microsoft (in its original malware report) advised a state of danger for all Ukrainian agencies and/or organizations with computer systems in Ukraine:

Given the scale of the observed intrusions, MSTIC is not able to assess intent of the identified destructive actions but does believe these actions represent an elevated risk to any government agency, non-profit or enterprise located or with systems in Ukraine.

5. Russian Information Warfare has been conducted in concert with kinetic, on-the-ground military actions.

The Microsoft report acknowledges that cyber offensives appear to directly correlate to kinetic military operations–and directly mentions the use of Information Warfare to "shake confidence" in Ukrainian leadership as a tactic:

…the activity we have observed has included attempts to destroy, disrupt, or infiltrate networks of government agencies, and a wide range of critical infrastructure organizations, which Russian military forces have in some cases targeted with ground attacks and missile strikes. These network operations have at times not only degraded the functions of the targeted organizations but sought to disrupt citizens' access to reliable information and critical life services, and to shake confidence in the country's leadership. Based on Russian military goals for information warfare, these actions are likely aimed at undermining Ukraine's political will and ability to continue the fight, while facilitating collection of intelligence that could provide tactical or strategic advantages to Russian forces. (2)

6. Military actions were preceded by phishing.

Early military actions were preceded by phishing attempts to gain access to sensitive military targets and data exfiltration, highlighting the role of such attacks in modern espionage:

In early 2021, when Russian troops first started to move en masse toward the border with Ukraine, we saw efforts to gain initial access to targets that could provide intelligence on Ukraine's military and foreign partnerships. Russian actor NOBELIUM launched a large-scale phishing campaign against Ukrainian interests involved in rallying international support against Russian actions. Similarly, DEV-0257 (publicly known as Ghostwriter) began phishing campaigns attempting to gain access to Ukrainian military email accounts and networks. (6)

7. The pace of attacks has been consistent–and relentless.

Attacks started immediately before the invasion began, and have continued at a pace of 2 - 3 per week during the conflict:

Threat groups with known or suspected ties to the GRU have continuously developed and used destructive wiper malware or similarly destructive tools on targeted Ukrainian networks at a pace of two to three incidents a week since the eve of invasion. From February 23 to April 8, we saw evidence of nearly 40 discrete destructive attacks that permanently destroyed files in hundreds of systems across dozens of organizations in Ukraine. (3)

8. By June 2021, Ukraine was the second most-attacked nation–behind only the United States.

The report documented more attacks against the United States than any other country by far, receiving 46% of cyber attacks. Ukraine ranked second, at 19% (fig 2).

9. Information Warfare and other cyber attacks are correlated with political events.

Initial deployment of the WhisperGate wiper began immediately after the failure of diplomatic talks January 13th, followed immediately January 14th by DEV-0586 defacements and still-unattributed DDoS attacks against Ukrainian government websites. Timeline analysis shows attacks are closely correlated to diplomatic failure points (fig 3).

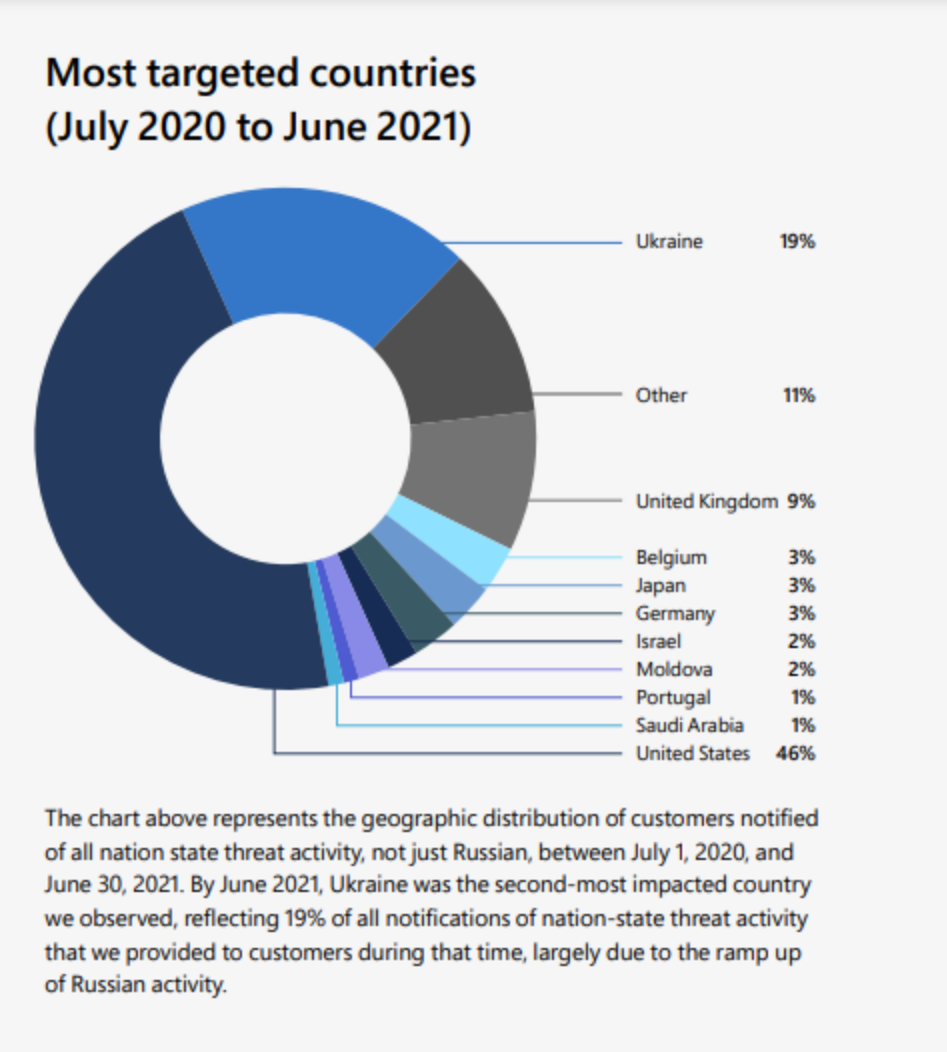

Figure 2. Image source: Microsoft. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

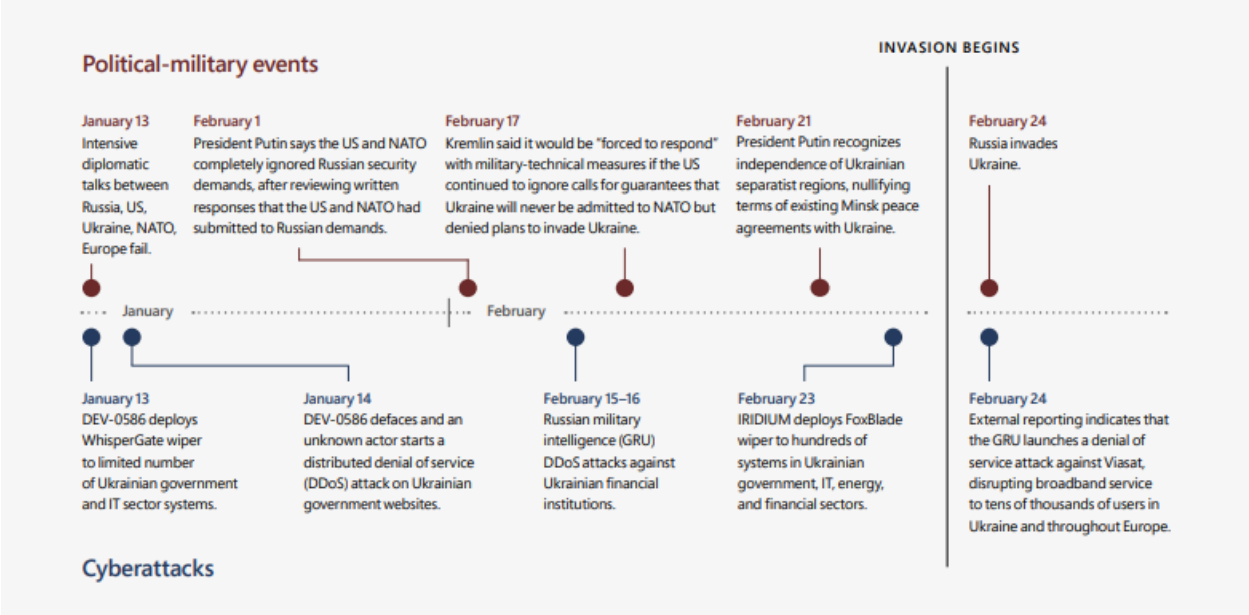

Figure 3. Image source: Microsoft. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

10. Attacks in early 2022 signaled the imminent invasion, and may have been intended to prompt diplomatic concessions.

The ramp up of cyber attacks against Ukraine not only correlated with key points in the diplomatic process, but also signaled the impending invasion–highlighting the importance of tracking hybrid warfare as a matter of national security:

In early 2022, when diplomatic efforts failed to de-escalate mounting tensions around Russia's military build-up along Ukraine's borders, Russian threat actors launched destructive wiper malware attacks against Ukrainian organizations with increasing intensity. These efforts signaled that Russian actions in Ukraine had entered a destructive phase that could escalate further. In early January, DEV-0586 launched WhisperGate5 malware which sought and deleted selected file extensions and then manipulated the Master Boot Record (MBR) to render targeted machines inoperable. This destructive malware impacted a limited number of government and IT sector systems, which coupled with the defacement of Ukrainian government websites in February, may have served as warnings intended to prompt Ukrainian concessions. (7)

Conclusion

Given the highly evolved nature of the Russian cyber offensive, its correlation with diplomatic efforts and breakdowns, and the rapid pace of deployment against Ukraine and its allies–combined with the raised stakes of any cyber actions within the context of wartime–organizations, investors, and AIML practitioners now face serious choices regarding their Information Warfare defense systems. Governments and industry alike should take notice:

the opportunity to tighten the OODA Loop in favor of AIML defenders has policy ramifications extending far beyond the Black Sea.

References

“An overview of Russia's cyberattack activity in Ukraine.” 2022. Microsoft AVIONEWS. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd.

“Destructive malware targeting Ukrainian organizations.” 2022. Microsoft. https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/.

At the intersections of AI, Security, Policy, & People

https://cx7.dev/