Cyber-Intelligence Report

This cyber-intelligence product is produced by David Swan. Collection of information is in accordance with guidelines provided by clients. It contains 'observations', meaning headlines and links to information published online. It *MAY* contain comments and analysis. It is copyright ©David Swan 2022. It MAY be circulated.

If this report does not meet your requirements, is in error or if you need additional information and/or analysis, please contact David Swan at DSC.Ops.Vulcan@gmail.com

Cyberwarfare: Russia vs Ukraine (16)

This report contains selected cyber-security information from 3rd to 14th October 2022.

Synopsis

1. During the reporting period there were few reports of cyber attacks between Russia and Ukraine, but multiple warnings of cyber espionage and information operations. There have been attacks by pro-Russian hackers against several U.S. State government web sites and the UK's MI5 web site. Some hackers are getting creative with drones. There has been an unusual number of cyber attacks reported on Canadian organizations.

2. Russian 'Courses of Action' for cyber forces, including allies such as 'patriotic', mercenary, and domestic criminal hackers are *assessed* as:

> **Ongoing**: Russian cyber forces, including allied forces, are launching a new series of cyber attacks against strategic targets such as energy companies and weapons manufacturers as well as vulnerable governments.
>
> **Worst Case Scenario**: President Putin decides to focus Russia's cyber attacks on one country (such as Canada) or a small group of vulnerable countries. *Assessed as UNLIKELY.*

Best Case Scenario: Russia agrees to cease or is forced to cease offensive cyber operations. *Assessed as VERY UNLIKELY.*

Russia vs Ukraine

3. Analysts Summary: During the last few weeks few cyber attacks have been reported between Russia and Ukraine. For Ukraine this is not a change. Ukrainian operational security around its cyber operations remains tight. Short video clips showing missile, artillery and tank strikes are released daily. Information operations, such as reporting Russian prisoners and casualties to their Russian families are ongoing – but not reported to media. Russian cyber attacks on Ukraine are almost certainly ongoing, but without results those efforts are not published. There are warnings of new cyber espionage efforts, efforts by Russia and China to affect U.S. midterm elections and reports of new cyber attacks on both the UK and the U.S.

4. The Finnish Security Intelligence Service (SUPO) is warning the Russia is '*Highly Likely*' to intensify its cyber activity over the winter. The SUPO is concerned that Russia

will intensify its cyber espionage activities. According to the SUPO, "*future NATO membership will make the country a privileged target for Russian intelligence and influence operations. The intelligence agency states that cyber threats to Finland's critical infrastructure has increased in both the physical and cyber environments as a result of the Russian invasion of Ukraine. These malicious activities could potentially paralyze infrastructure operations with unpredictable consequences*." The Security Affairs report states: Russia's traditional intelligence gathering activity relied on spies with diplomatic cover, but this approach has become substantially more difficult since Russia invaded Ukraine, because many Russian diplomats have been expelled from the West.[1]

5. Senior FBI Officials are warning that "*Russian and Chinese government-affiliated operatives and organizations are promoting misinformation about the integrity of American elections ... ahead of November's midterms. recent Russian influence operations ... typically involve amplifying conversations that Americans have on social media ... rather than creating new content. Chinese operatives have shown signs of engaging in more "Russian-style influence activity" that stokes American divisions.*"[2] Analysts Comment: Although these campaigns are more 'information operations' than cyber operations, both Russian and Chinese campaigns involve creating fake or 'bot' accounts on social media such as Facebook, Instagram, LinkedIn, etc. The fake accounts are used to repeat, and promote narratives.

6. Russia's 'KillNet' hacker group took credit for attacks on three U.S. State governments. On 6th October some web sites run by the governments of Colorado, Connecticut, Kentucky and Mississippi were temporarily disabled. KillNet's Telegram Channel shows a target list including sites run by dozens of U.S. state governments. The group describes these hacks as *this week's operation "USA Offline*."[3] One analyst said: "*In the case of these state government websites, the disruption of service, while inconvenient, is far less of a problem than a data breach involving the theft of personally identifiable information, ... it [the attacks] erode public trust in the organizations that these websites represent*."[4] Followup reports indicate almost all web sites were back in service either the same day or by the following morning.

7. Russia has added 'Meta', specifically 'Facebook' and 'Instagram' to its list of "terrorist and extremist organizations." The platforms were banned for "Russophobia". *The listing came after Meta's announcement it would permit posts such as "death to Russian invaders" but not credible threats against civilians.* WhatsApp is also owned by Meta but has not been banned.[5]

8. On September 30th the web site of MI5, the UK internal security service, was knocked offline for a few hours. 'Anonymous Russia' a Russian hacker group claimed responsibility for the attack, disabling the web site at 9 am.[6] Apparently the attack was

1 Source: Security Affairs: Finnish intelligence warns of Russia's cyberespionage activities
2 Source: KYMA and CNN: Russia and China are promoting US voting misinformation ahead of midterms, FBI warns
3 Source: StateScoop: Russian hacking group targets state-government websites in DDoS campaign
4 Source: silicon ANGLE: Russian hackers take down state websites in politically motivated attack
5 Source: BBC: Russia confirms Meta's designation as extremist
6 Source: yahoo!finance: MI5 website briefly knocked offline by possible cyber attack

intended as a warning to Britain and other countries who are supporting Ukraine.[7] Analysts Comment: Most hackers have enough common sense not to attack an organization that can potentially retaliate. Since MI5 can retaliate this is an unusual attack, even allowing for the Russia – Ukraine conflict.

Drones Used in Network Attacks

9. Two technologies are being used together to attack computer networks. Reports describe drones being used to place wireless network-intrusion devices. A report in 'the Register' described an attack on a US East Coast financial firm. "*The company's security team responded and found that the user whose MAC address was used to gain partial access to the company Wi-Fi network was also logged in at home several miles away. The user was active off-site but someone within Wi-Fi range of the building was trying to wirelessly use that user's MAC address, which is a red flag. The team then took steps to trace the Wi-Fi signal and used a Fluke system to identify the Wi-Fi device. This led the team to the roof, where a 'modified DJI Matrice 600' and a 'modified DJI Phantom' series were discovered ... The Phantom drone was in fine condition and had a modified Wi-Fi Pineapple device, used for network penetration testing. The Matrice drone was carrying a case that contained a Raspberry Pi, several batteries, a GPD mini laptop, a 4G modem, and another Wi-Fi device".*[8]

10. The concept of using drones to place intercept devices has been well developed since initial trials in 2011 but there are few examples of it being used. The assessment of the attack reads in part: "*This was definitely a threat actor who likely did internal reconnaissance for several weeks, had physical proximity to the target environment, had a proper budget and knew their physical security limitations,"*[9] according to Cybersecurity researcher Greg Linares. *He explained this sort of drone exploit delivery attack probably cost no more than $15,000 to put together. "Attackers are spending this range of budget in order to target your internal devices and are ok with burning it," he cautioned. "This is the third real-world drone based attack I have encountered in two years."*[10]

Canada

11. Recently there has been mainstream media reporting on hacks on Canadian organizations. U.S. cybersecurity firm CrowdStrike said it discovered malicious software being distributed by Vancouver-based 'Comm100'. The company provides chat bots and social media management tools as customer service products to more than 15,000 clients across 80 countries.[11] According to CrowdStrike researchers, Chinese hackers hijacked the installer for Comm100 between 27th and 29th September. During this time the installer infected numerous businesses in healthcare, industrial, insurance, manufacturing, technology, and telecommunication sectors in Europe and North

7 Source: Independent (UK): Pro-Russian hackers temporarily take MI5 website offline with cyber attack
8 Source: The Register: How Wi-Fi spy drones snooped on financial firm
9 Source: Ibid
10 Source: DARKReading: Airborne Drones Are Dropping Cyber-Spy Exploits in the Wild
11 Source: Reuters: Suspected Chinese hackers tampered with widely used customer chat program, researchers say

America.[12] An updated Comm100 installer has been released to remove the malicious code. Security Week reports Comm100 appears to be investigating the incident, but has not shared any information on the attack.[13]

12. In 2019 media reports stated a U.S.-based third-party contractor used by both the Canadian and U.S. border agencies was hacked exposing as many as 1.38 million licence plate images and associated information. The Privacy Commissioner's Office investigated, completing its report in May 2022. The report was tabled Thursday 29th September as part of the Commissioners Annual Report. Approximately "*11,000 [images] were posted on the dark web. It also found the image files included metadata containing the relevant province or state associated with the licence plate, the date and time the image was taken, and the numerical code representing the border crossing site along with lane number.*"[14] The boarder agency said: it did not consider the licence plate images to be personal information.

13. On September 30th new details were released on the hack of Calgary's Parking Authority. "A *vulnerability on one of its servers exposed the information of 145,895 customers, despite an earlier statement saying that only 12 customers had their data compromised*." The breach was caused because a server was left without a password. Anyone who discovered the server address could login. Exposed was "*customers' information, such as their names, birthdates, phone numbers, email addresses, postal addresses, and even parking ticket/offences data was exposed. The parking details also gave out customers' license plate information and vehicle descriptions. ... Logs also contained partial card payment numbers and expiry dates.*" The Calgary Parking Authority does not know if any 'external parties' accessed the data.[15]

14. On September 29th the Waterloo Region District School Board confirmed the data of around 70,000 students was stolen during a cyberattack. During the June attack the hackers targeted data from 2006/2007 through 2012/2013 academic years. According to the School Board data taken "may have included" names, birthdates, whether the student had an individualized education plan, and historical education information like former teachers and schools. The board said they have received "assurances" that any copies of the stolen data have been deleted.[16]

---

12 Source: LatestHackingNews: Comm100 Chat Service Hacked In A Supply-Chain Attack
13 Source: SecurityWeek: Supply Chain Attack Targets Customer Engagement Firm Comm100
14 Source: AirdrieTODAY: Data breach at border agency contractor involved up to 1.38 million licence plates
15 Source: Insurance Business Magazine: Over 145,000 customers' data was exposed in agency data breach incident – report
16 Source: CTV News Kitchener: Data of 70,000 students stolen during hack: WRDSB