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 2023. This report 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 (35) And MOVEit! Continues

This report contains selected cyber-security information from 8th to 21st July 2023.

Synopsis

1. The MOVEit! hack has passed the SolarWinds hack in size. Russian hackers target the Ukrainian and Eastern European defense Industry. Russian hackers attacked: the NATO Summit, the Bulgarian parliament, PayPal, New Zealand, and London airports. Ukrainian police seized a massive Russian 'information operation'. Ukrainian hackers briefly hack Russian medical lab 'Helix'. The Internet is going to change. What should be done with 'veteran' hackers – after the war in Ukraine ends?

2. Russia appears to be committed to the following ongoing 'Course of Action' for its cyber forces:

> **Updated:** Russian cyber forces, including allied and supporting hackers, continue to launch campaigns against Ukrainian targets and their allies, including perceived Ukrainian allies. Targeting Includes: infrastructure, political, and media organizations as well as targets of opportunity. The number, scope and quality of Russian cyber attacks continues to increase.

MOVEit!

3. The MOVEit! hack continues to grow in scope. On July 14th Charles Schwab Corp, parent company of TD Ameritrade Inc, warned that "***tens of thousands of clients could have been affected***" as "*customer data stored on Ameritrade's MOVEit server was compromised.*"[1] Other financial organizations that have had their client information compromised include: 1st Source Bank, First Merchants Bank, Deutsche Bank, ING, and Commerzbank. This follows the July 11th announcement by Ernst & Young in Canada that 62 of their clients were compromised by the same attack including: "*Air Canada, Altus, Amdocs, Constellation Software, EY-Continental Transition, Laurentian Bank of Canada, LendLease, Sierra Wireless, SSC Fraud Risk Assessment, St. Mary's General Hospital Surgical Services Review, Staples Canada, Sun Life Assurance of Canada, United Parcel Service Canada Ltd.*"[2] Three of the largest law firms in the United States, Kirkland & Ellis, K&L Gates and Proskauer Rose have also been compromised by the MOVEit! Hack. In their case, a new group calling themselves "Lance Tempest" is demanding the ransom.[3] The hackers, the Cl0p Ransomware group, based principally in

1 Source: Investment News. Charles Schwab announces TD Ameritrade data breach
2 Source: Ban Info Security. Clop Crime Group Adds 62 Ernst & Young Clients to Leak Site

Russia, continues to name its victims and threaten to publish sensitive data on its website.

4. Analysts Comments: The MOVEit! hack is now so large that additional criminals and criminal groups are being recruited to process the victims. Worse, 'Progress Software', creators of the compromised application, continue to identify vulnerabilities.[4] This suggests its possible that the hackers have not yet been completely locked out of the software still installed in thousands of organizations.

Russian Cyber Operations

5. Microsoft's threat intelligence team and the Computer Emergency Response Team of Ukraine (CERT-UA) identified cyber attacks against the defense industry in Ukraine and Eastern Europe. The campaign has been mounted by 'Turla'[5], a known Russian Federal Security Service (FSB) hacking group. The attack is conducted using 'DeliveryCheck' malware which is "*distributed via email as documents with malicious macros. ... The ultimate goal of the attacks is to exfiltrate messages from the Signal messaging app for Windows, enabling ... access sensitive conversations, documents, and images on targeted systems.*"[6] Analysts Comment: The report did not say what (if anything) had been compromised nor how widespread the attack is.

6. Russian cyber attacks outside Ukraine

- 10 July. Russian hacking group 'NoName057(16)' attempted to disrupt the NATO summit in Vilnius, attacking several transport and tourism websites. Results were limited with the GoVilnius tourism promotion website, the 'stops.lt' website, a streaming music service and a local radio station briefly affected. Lithuania's national cybersecurity center (NKSC) has confirmed the DDoS attack. Analysts Comment: Lithuania has been working with NATO to improve its cyber defenses. It should be considered 'well prepared' for cyber attacks.[7]

- 10 July. The BlackBerry 'Threat Research and Intelligence Team' published a warning of two targeted threats. One was an emailed document to NATO Summit guests while two more emailed documents were 'lures' sent to an organization supporting Ukraine abroad. Blackberry's threat team attributes the attacks to 'RomCom' a known Russian threat group.[8]

- 15 July. NoName057(16) "*announced that they blocked access to the website of the Bulgarian Parliament, as well as to the port of Varna."* On its Telegram channel NoName057(16) said: "*Bulgaria has prepared for Ukraine a*

3 Source: New York Post. Massive cybersecurity breach hits biggest US law firms
4 Source: The Hacker News. Another Critical Unauthenticated SQLi Flaw Discovered in MOVEit Transfer Software
5 Turla is also known as: Iron Hunter, Secret Blizzard (formerly Krypton), Uroburos, Venomous Bear, and Waterbug.
6 Source: The Hacker News. Turla's New DeliveryCheck Backdoor Breaches Ukrainian Defense Sector
7 Source: Cybernews. Russia sends in cyber attack dogs as NATO summit looms
8 Source: Blackberry. RomCom Threat Actor Suspected of Targeting Ukraine's NATO Membership Talks at the NATO Summit

pact with 100 units of armored vehicles. Therefore, the website of the Bulgarian National Assembly received several hundred thousand DDoS missiles from us."[9]

- 18 July. Anonymous Sudan said it launched a "test attack" against PayPal. The 'attack' only lasted 30 seconds but it did lead to "*an error message appearing on the online payment service, saying user reports indicate problems at PayPal.*" The group promised to launch a series of attacks on UAE-based organizations, and subsequently claimed "*attacks on websites in the region, including the Dubai Electricity and Water Authority and the UAE government portal.*"[10]

- 19 July. Russian hacking group NoName057(16) claimed to be "*behind an attack on the Parliament website and another on the "New Zealand Legal Commission", possibly intended to refer to the Law Commission."* The attack was a Denial of Service (DoS) attack "*carried out as retribution for the Government's support of Ukraine".* New Zealand's "*National Cyber Security Centre said it was aware of attacks which it said affected a range of websites overnight."*[11]

- 19 July. UK airports are facing Distributed Denial of Service (DDoS) attacks from Russian hacker groups. "*London City Airport's website went down shortly before 3pm on Wednesday afternoon, coinciding with an apparent claim of a hack by pro-Russia UserSec. A short while later Anonymous Russia claimed to have launched a similar attack on Birmingham Airport's website".* A spokesman for Birmingham's airport said "*Some people have reported our website has been loading slowly this afternoon. We are investigating.*"[12]

Ukrainian Cyber Operations

7. The Cyber Police Department of the National Police of Ukraine announced the seizure and take-down of a "massive" Russian bot farm that conducted "*disinformation and psychological operations.*" The scale of the operation is remarkable. After conducting 21 searches, police discovered:

- More than 100 people acting as 'operators',
- computer equipment and mobile phones,
- more than 250 GSM gateways, and
- 150,000 SIM cards of various mobile (cell phone) companies.[13]

8. Bot farm operators were located in Vinnytsia, Zaporizhzhia, and Lviv. The police alert said: "*The Cyber Police established that the attackers used special equipment and software to register thousands of bot accounts in various social networks and*

9 Source: Sofia News Agency. Russian Hackers Blocked the Website of the Bulgarian Parliament because of the APCs for Ukraine

10 Source: CyberSecurity Connect. Anonymous Sudan hits PayPal with DDoS attack

11 Source: Stuff.co.nz . National Cyber Security Centre said it was aware of attacks which it said affected a range of New Zealand websites overnight.

12 Source: The Mirror. UK airports 'targeted by coordinated Russia cyber attack groups'

13 Source: Security Affairs. Ukraine's cyber police dismantled a massive bot farm spreading propaganda

subsequently launch advertisements." Ukraine has "*busted multiple bot farms behind more than one million fake social media accounts since the invasion began in February 2022.*"[14]

9. Ukrainian hackers continue to try and affect 'ordinary Russians'. "*Customers of the Russian medical laboratory Helix have been unable to receive their test results for several days due to a "serious" cyberattack that crippled the company's systems over the weekend.*"[15] The attack was a ransomware type attack that the lab countered.

Future of the Internet

10. An article in 'Scientific American' reported Russia tried to disconnect from the Internet (again) causing 'outages'. Russia wants full control over what its citizens see and do.[16] Chinese president Xi Jinping has directed his officials to build a Beijing-supervised "security barrier" around its internet. He wants to make the 'Great Firewall of China' better. To him it is 'imperative' to operate the Internet 'according to the law.'[17] Many governments are sympathetic to that point of view. Countries such as Iran also want full control. Other countries demand 'moderation' and 'accountability' from the mega-corporations who control massive portions of the Internet. Given current hacking campaigns such as MOVEit!, Russian – Ukraine cyberwarfare, ongoing Chinese cyber espionage and hacking, it seems highly likely that the drivers for change are in place.

What Do We Do With 'Veteran' Hackers

11. 'Friends of Europe', a Brussels -based, not-for-profit think tank for European Union policy analysis and debate, is warning about the impact of 'war-experienced hackers' in the post-war environment. To quote from their web site: "*The Ukrainians have mobilised a staggering 400,000 national and foreign hackers, while the Russians have relied on a hefty track record of offensive cyberwarfare capacities and connections with criminal cybergangs. ... While the attacks include a lot of petty pirate activities, such as bringing down official websites, the unprecedented attacks on critical civilian infrastructures should not be overshadowed. Paralysing heating systems in the midst of winter, breaking power grids, destroying telecoms infrastructures and crippling railways and stock exchanges are now part of conventional warfare.*" Analysts Comment: We agree with their theme: "*If you want peace, prepare for cyberwar.*"[18] Governments and legislators need to address 'criminal hacking' as something more than white-collar crime or an inconvenience.

---

14 Source: The Register. Ukraine busts bot farm spreading Russian infowar propaganda and fraud
15 Source: The Record. Russian medical lab suspends some services after ransomware attack
16 Source: Scientific American. Russia Is Trying to Leave the Internet and Build Its Own
17 Source: The Register. Beijing wants to make the Great Firewall of China even greater
18 Source: Friends of Europe: If you want peace, prepare for... cyberwar