Cyber-Intelligence Report

This cyber-intelligence product is a snapshot of selected cyber events. Collection of information is in accordance with clients' guidelines. It contains 'observations', meaning headlines and links to online information. 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, contact David Swan at DSC.Ops.Vulcan@gmail.com

CyberWarfare: (45) Govt Inaction On Cyber Proving Expensive

This report contains selected cyber-security information from 23rd November to 7th December 2023.

Synopsis

1. The European Union's Cyber Security team warns of ongoing Russian cyber attacks on the EU. Ukraine successfully cyber attacks Russian civil aviation and Russia's Crimean TV. President Zelensky of Ukraine made a TV broadcast into occupied Crimea, on Russian TV. Israel's cyber forces authorized to 'defend' against cyber attacks. China steals computer chip secrets. MOVEit! hack update.

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

> Russian cyber forces, including allied and supporting hackers, continue to launch campaigns against Ukrainian targets, **including perceived Ukrainian allies.** Targeting Includes: critical infrastructure, industrial infrastructure, political, and media organizations as well as targets of opportunity.

Russia vs Ukraine

3. The European Union's cyber emergency response team (CERT-EU) is warning that Russia's notorious hacking group, Fancy Bear, is targeting European governments with cyberattacks. CERT-EU said: "*We assess that the threat level posed to [EU institutions and agencies] by this activity is high.*" ... "*At least seven European governments have been targeted with spearphishing campaigns, which include using custom-tailored lures to target specific, high-profile targets to download malicious software or give away access to digital systems. ... The warning comes amid growing concerns that next year's European election will be targeted by hacking groups from countries with a cyberoffensive program against Europe, like Russia and China. EU voters head to the polls in June.*"[1]

4. The Russian 'patriotic hacktivist group' NoName057(16) is recruiting. "*Join our volunteer DDoSia Project to fight in the cyber war unleashed by the West against our Motherland," a representative post in the group's Telegram channel reads. Volunteers will be paid (in cryptocurrency, naturally) and will have "ranks and merit awards depending on their time of service and achievements,"*[2] The principal weapon of

[1] Source. Politico. Russian hackers pose 'high' threat level to EU, bloc's cyber team warns

[2] Source. CyberWire. NoName057(16)'s DDoSia project is looking for volunteers.

NoName is an improved Distributed Denial of Service (DDoS) script which provides more precise controls and targeting. “*The group has primarily focused on European websites. However, it has also paid attention to Canada multiple times*”[3] as well as attacks on Australia.

5. Analysts Comment: Both KillNet and NoName have previously boasted about the large size of their membership. While more members are always better, especially when launching Distributed Denial of Service (DDoS) attacks, we *assess* this as an indication of how unpopular the war has become. It is *probable* that many technically capable younger Russian men have left Russia rather than face conscription.

6. **Ukrainian Cyber Successes**. In an unusual announcement, “*Ukraine's defense intelligence directorate has claimed it carried out a successful cyber operation against Russian government’s civil aviation agency, Rosaviatsia.”*[4] The attack was described as a "*successful complex special operation in cyberspace*" that involved *“hacking and penetration of enemy information systems. ... The ministry asserts that its analysis of the documents shows the civil aviation sector of terrorist Russia is on the verge of collapse.”* The assessment is based on "*uncertified maintenance with the use of non-authentic spare parts*" and "*aviation cannibalism*".[5]

7. On the 29th of November, Russian TV channels in occupied Crimea broadcast a message from Ukraine’s President, Volodymyr Zelensky. The President appeared to have plenty of time to deliver his message:

> *“I would like to separately say to all our people in Crimea, in Sevastopol, in all the occupied regions of the south and east of our state, currently occupied regions -*
>
> *Dear Ukrainians, you all feel that the Russian presence on our land will not last forever. I know this. Ukraine will return its territory, our people.*
>
> *We will not leave anyone to the occupiers.”*[6]

Ukraine’s ‘Pravda’ magazine claims Ukrainian Intelligence was behind the broadcast.[7]

Hamas vs Israel

8. Since the start of the Hamas/Israel conflict there have been more than forty cyber attacks on Israel, some on critical infrastructure. “*Israel's National Cyber Directorate (INCD) announced last week that the government has approved emergency regulations to enhance the country's ability to defend against widespread cyberattacks.*” This means Israel’s cyber directorate, Shin Bet, has been given the

[3] Source: Australian Cybersecurity Magazine. NoName057(16) Gets Busy Recruiting an Online Hacktivist Army

[4] Source: The Record. Ukraine claims cyber operation against Russian aviation agency

[5] Source: The Register. Ukraine cyber spies claim Putin's planes are in peril as sanctions bite

[6] Source: The Sun (UK). D**K MOVE. Moment Russian TV is HACKED as Zelensky vows to drive Putin out of Crimea – while text says: ‘Vlad’s a d**khead’

[7] Source. Pravda UA. Ukrainian intelligence was behind broadcast of Zelenskyy's address in Crimea, source says

power to fight cyberattacks. “*In the event of a serious cyberattack that poses a risk to the state or essential services, either the INCD, the Shin Bet (Israel Security Agency), or the Defense Ministry - depending on the affected company type will have the authority to instruct storage service providers and digital services on how to handle the situation. These instructions will only be issued if the storage service providers and digital services fail to adequately address the cyberattack.*”[8] The emergency regulations are in effect for one month.

China Steals Chipmaking Secrets

9. According to Netherlands national news outlet NRC Handelsblad, a prolific espionage hacking group with ties to China, tracked under names including "Chimera" and "G0114," “*spent over two years looting the corporate network of NXP, the Netherlands-based chipmaker.*” The company makes chips for smartphones, smartcards, and electric vehicles. The hack lasted from late 2017 to the beginning of 2020. During that time “*the attackers accessed employee mailboxes and network drives in search of chip designs and other NXP intellectual property.*”[9] Details of the breach were kept a closely guarded secret.

10. The hack is considered a ‘big deal’. NXP is Europe’s second-biggest semiconductor company. Security firm Cycraft said “*The main objective of these attacks appeared to be stealing intelligence, specifically documents about IC chips, software development kits (SDKs), IC designs, source code, etc. ... If such documents are successfully stolen, the impact can be devastating. ... Once nested on a first computer—patient zero—the spies gradually expand their access rights, erase their tracks in between and secretly sneak to the protected parts of the network. ... They try to secrete the sensitive data they find there in encrypted archive files via cloud storage services such as Microsoft OneDrive. ... the hackers come every few weeks to see whether interesting new data can be found at NXP and whether more user accounts and parts of the network can be hacked.*”[10]

Meta (Facebook) Punishes China and Russia for ‘inauthenticity’

11. On 3rd December Meta released its Quarterly Adversarial Threat Report. The report identified three ‘clusters’ of ‘*coordinated inauthentic behavior*’, so the associated accounts and groups were deleted on both Facebook and Instagram. One Chinese group “*targeted primarily India and the Tibet region and, to a lesser extent, the United States.*” A second cluster involving 4,789 accounts “*targeted the United States and posed as Americans across different platforms to post about US politics and US-China relations.*” The third cluster was Russian. It “*targeted global English-speaking audiences. The network posted primarily in English about Russia’s invasion of Ukraine and ran fictitious “media” brands.*”[11]

[8] Source: The Jerusalem Post. Israel cyber directorate, Shin Bet given power to fight cyberattacks

[9] Source. ArsTechnica. Hackers spent 2+ years looting secrets of chipmaker NXP before being detected

[10] Source. ArsTechnica. Hackers spent 2+ years looting secrets of chipmaker NXP before being detected

[11] Source: CyberWire. 12.1.23 Meta identifies and removes Chinese and Russian accounts and groups for coordinated inauthenticity

12. Analysts Comment: Although it is good to see Meta remove information operations from its social media outlets, their rationale leaves a lot to be desired. ‘Coordinated inauthentic behavior’ does not address other types of disinformation campaigns, manipulation of social media, or illegal activities. It is *assessed* that Meta is doing enough to be left alone by governments and remain largely unregulated. Meta does not appear to be an ally of any country.

Hostile Cyber Operations

13. Hostile Cyber operations are nothing new. For example the BBC is reporting “*Russia hacking: 'FSB in years-long cyber attacks on UK', says government*”. The story released on 7th December said “*The UK is accusing Russia's Security Service, the FSB, of a sustained cyber-hacking campaign ... carrying out hundreds of highly targeted hacks against politicians, civil servants, those working for think-tanks, journalists, academics and others in public life. ... Amongst those targeted was an MP who told the BBC in February his emails had been stolen. ... Russia has repeatedly denied claims it is involved in such activities. ... The hacking group is known by a variety of names including Star Blizzard, Cold River and Seaborgium.*” The hackers are part of “*the Federal Security Service (FSB) is the successor agency to the KGB, which operated throughout the Cold War. ... the FSB - and specifically the part of it known as Centre 18 - has been targeting the UK by stealing information from those in political and public life since at least 2015.*”[12]

14. Analysts Comment: Inaction by Western governments has allowed hostile governments to develop cyber campaigns. We are learning its an expensive mistake.

MOVEit! Update

15. The MOVEit! hack continues to grow. Even conservative tracking by the KonBriefing shows the number of victim organizations and individuals continues to grow. The victim count effective 6 Dec 2023: 2592 organizations and 78.1 – 82.9 million individuals.[13] The most recent victims include: Welltok, a Healthcare SaaS provider, the Pan-American Life Insurance Company (PALIC), the Medical College of Wisconsin and nine hospitals from ‘Prime Healthcare’ of California. The Welltok breach alone added 8.5 million US patients to the victim list.[14] “*Taking IBM’s estimate, which puts the cost of an average data breach at $165 per leaked record, the impact of Cl0p attacks would add up to a staggering $13.7 billion.*”[15]

To unsubscribe from this service send an email to DSC.Ops.Vulcan@gmail.com

[12] Source: BBC News. Russia hacking: 'FSB in years-long cyber attacks on UK', says government

[13] Source: KonBriefing.

[14] Source: Bleeping Computer. Welltok data breach exposes data of 8.5 million US patients

[15] Source: cybernews. PALIC customers’ credit card data exposed via MOVEit attacks