Volume 4: Edition 1

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 2024. 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

Cyber Intelligence Report: Our Cyber Forecast for 2024

This report contains selected cyber-security information from 2023 to 11th January 2024.

Synopsis

1. This is our Cyber Forecast for 2024. We cover the conflicts: Russia vs Ukraine, China vs Everybody, and Israel vs Iran. Hackers are becoming greedier while finding new targets from service companies to some less obvious organizations. No, your Bitcoin is *NOT* safe. RUSI(NS) under 'Brute Force' cyber attack.

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.

Where This Cyber Forecast Comes From

3. This Cyber Intelligence Report is how we (David Swan Consulting) see the cyber environment evolving in 2024. Clients gave us questions that we rewrote as Priority Intelligence Requirements (PIRs). We broke down those PIRs into refined questions and then went hunting for answers. Our regular reports are based on those answers/observations and our analysis. The forecasts in this report are based on our reports and the trends we have identified.

4. Our thanks to the Centre for Strategic Cyberspace and International Studies and the Royal United Services Institute (Nova Scotia) for their support. It improved our work.

CyberWarfare

5. CyberWarfare should be described as GeoPolitical conflicts in which 'cyber' is a theatre of conflict (IE. Land, Sea, Air and Space) and cyber tools (IE. malware) are conceived as a tool of war to achieve national ends. National ends can range from 'Espionage' to 'Sabotage' and include 'Information Operations'. Physical destruction is not required for 'war'. Further, cyber conflict can be primary (an attack in its own right) or a supporting attack for some event in another environment. There are three preeminent conflicts where state resources are being used to create new cyber tools

in accordance with this description. The three cyberwars are:

A. Russia vs Ukraine (and Ukraine's supporters)

B. China vs the world

C. Israel vs Iran

Each of these conflicts is creating: new malware, new tactics techniques and procedures (TTP) for using that malware, and sometimes enabling bad actors with those creations.

Russia vs Ukraine

6. **Russia:** According to the head of Ukraine's Security Service of Ukraine's (SBU), Russia's APT group Sandworm was inside Ukrainian telecoms giant Kyivstar from at least May 2023. Sandworm operates "*under the control of Unit 74455 of the Russian GRU's Main Center for Special Technologies (GtsST).*" The attack is significant because (1) The attackers had covert access to Ukraine's telecommunications for months and (2) "*threat actors wiped "almost everything", including thousands of virtual servers and PCs. The attack has "completely destroyed the core of a telecoms operator.*"[1] Analysts Comment: This attack will demonstrate to Moscow that large scale cyber attacks can be accomplished and produce significant results. More large scale destructive cyber attacks *should* be expected.

A. CERT-UA Uncovers New Malware Wave Distributing OCEANMAP, MASEPIE, STEELHOOK

B. Threat Actor 'UAC-0099' Continues to Target Ukraine

7. Russia's 'Patriotic Hackers' did not have a good year in 2023. KillMilk, leader of the KillNet hacker group, stepped down as leader. Competing group NoName 057(16) has continued operations – at a significantly reduced pace, and picked easier targets. Currently NoName 057(16) is conducting Distributed Denial of Service Attacks (DDoS) on Finland. "*The Energy Industry, Academic Institutions, Legal Services, Municipalities, and Consumer Affairs*" have all been targeted. Other "*targets included critical entities like Traficom, the National Cyber Security Centre Finland (NCSC-FI), The Railways, The Agency for Regulation and Development of Transport and Communications Infrastructure of Finland, and multiple subdomains of the Finnish Road Agency. But ... a thorough check of the websites reportedly under attack by NoName and found them operating smoothly.*"[2] Russian authorities and media have shown impatience with organizations that can not demonstrate 'impact' on victims. Unless NoName can up their game I expect they will *most probably* lose members, capability, and any government support across 2024.

NoName on Rampage! Claims DDoS Attacks on Ukrainian Government Sites

8. **Ukraine:** Ukraine's Cyber UT Army appears to have increased its operational

[1] Source: Security Affairs. Ukrainian authorities revealed that Russia-linked APT Sandworm had been inside telecom giant Kyivstar at least since May 2023

[2] Source: Cyber Express. NoName CyberAttacks Escalate, Targeting Diverse Sectors in Finland

tempo, attacking more targets using more sophisticated techniques. Russian news magazine ‘Pravda’ reported two major attacks. These are in addition to the Ukrainian attack on Russia’s aerospace industry in mid-December.

A. Ukrainian hackers report successful attack on Russian Bitrix service

B. IT Army stops operation of one of Russia's largest ERP systems

C. Ukrainian hackers breach Rosvodokanal, seize data of Russia's largest private water utility

D. Cloud Atlas' Spear-Phishing Attacks Target Russian Agro and Research Companies

9. We *assess* that the number of independent hackers actively supporting Ukraine has decreased, however many of the remaining hackers are better organized, appear to receiving training and/or access to better hacking tools. We forecast that Ukraine’s Cyber IT Army is *highly likely* to continue to refine its targets and capabilities. Given Ukraine’s operational security so far, its unlikely there will be any forewarning of their cyber attacks.

China vs Everybody

10. Although the title may seem inappropriate, President Xi of China wants the People’s republic of China to be the preeminent power of this century. China’s five year plan reflects that ambition in “*a new phase of accelerated digitized development and building a digital China.*”[3] Two of China’s recent efforts show a continuing drive to master others technology and an increasing awareness that China needs to reinforce its own cyber defences.

A. China Says State-Backed Experts Crack Apple’s 01 January:AirDrop

B. China Orders Banks, Insurers to Review Cyber and Data Security

11. Since China has not been ‘called’ on its cyber espionage and theft of intellectual property, China will continue its current activities. Unfortunately China’s cyber efforts are massive and include penetrating the critical infrastructure of many western nations.

Israel vs Iran

12. Although the conflict is officially Israel vs Hamas (Gaza), there is insufficient remaining Internet infrastructure in Gaza for a capable cyber force. It is more appropriate to identify organizations aligned with Iran, targeting Israel, operating ‘in support’ of Hamas (Gaza).

13. **Iran:** Israel’s National Cyber Directorate reports that over “*over 15 groups associated with Iran, Hezbollah, or Hamas have been engaged in cyber attacks against Israel since 7/10.*” The report also notes “*that most of these groups share intelligence, methods and tools with each other.*“[4] Some of the groups claim to have

[3] Source: Sanford University. Translation. 14th Five-Year Plan for National Informatization – Dec 2021

attacked "*Dozens of high-Profile Israeli Firms*". "*According to Cybernews, in recent weeks a massive data breach and subsequent data leaks affected 49 Israeli companies, including the Israel Innovation Authority, Toyota Israel, the Ministry of Welfare and Social security, Ikea Israel, cybersecurity and geo-intelligence company Max Security, and others.*"[5] Although the claims include 'leaked information' they have not been reflected in Israeli media reporting. Israeli media has reported some hacks as well as preventive measures by hospitals to disconnect themselves from the Internet. We *assess* Iranian cyberattacks as *generally ineffective*. Further we *assess* that it is *unlikely* that effectiveness will improve.

14. **Israel:** Before Christmas, Israel launched a series of cyber attacks against Iran. One attack shut down 70% of Iran's gas stations. More recently there has been a series of unattributed attacks against Iranian targets.

A. Troves Of Iranian Hacked Insurance Customer Data On Sale

B. Iranian Food Delivery Giant Snappfood Cyber Attack: 3TB of Data Stolen

C. Iranian crypto exchange Bit24.cash leaks user passports and IDs

15. Since Israeli cyber operations will be run by their 'National Cyber Directorate' we expect little to no information will be released about Israeli intentions or cyber operations. We *assess* that Israel will run a sophisticated cyber campaign against Iran. We *assess* it as *highly likely* that there will be a Psychological Operations (PsyOps) aspect to the campaign. By this we mean the campaign will be designed to generate Iranian displeasure with their regime.

Hacking Trends

16. Recent reporting suggests that some top tier hacker groups have expanded their target sets to include service companies (companies that service other companies). Some examples include the targeting of: Law Firms, Real Estate companies, Mortgage firms, and Insurance companies. The hackers are targeting BOTH the target firm AND their client list.

A. Law firm that handles data breaches was hit by data breach

B. Mortgage firm LoanCare warns 1.3 million people of data breach

C. Troves Of Iranian Hacked Insurance Customer Data On Sale

17. Hackers are also looking for less obvious targets, organizations that might not have increased their cyber security. Examples of these less obvious targets include: Libraries, Museums and Art Galleries, and Zoos.

A. British Library to burn through reserves to recover from cyber attack

B. Museums on alert following British Library cyber attack

[4] Source: CTech. Over 15 cyber attack groups affiliated with Iran, Hezbollah or Hamas are operating against Israel, says National Cyber Directorate

[5] Source: i-hls.com . Iranian Cybergang Attacks Dozens of High-Profile Israeli Firms

C. Museum World Hit by Cyberattack on Widely Used Software

D. Toronto Zoo hit by ransomware

18. There are no indications that despite the International Criminal Courts warning that hackers can be prosecuted under existing laws, has had any impact. Some groups have moved to a pattern called ‘Double Extortion’ and even ‘Triple Extortion’, extorting funds from both victim organizations AND their clients which can be other organizations or individuals. Top tier hacker gangs are re-constituting faster after police arrest senior leaders. Lastly, hacking groups don’t appear to have any limits. For example the Russian Ransomware group ‘Cl0p’, responsible for the MOVEit attack, continues to claim victims from the MOVEit attack[6], while seeking a more productive business model.

A. Ransomware trends, statistics and facts heading into 2024

B. BlackCat Ransomware Gang Recovers From Early December Law Enforcement Operation, Restores Websites Seized by DOJ

C. MOVEit hackers may have found simpler business model beyond ransomware

19. **Hackers will continue to target Bitcoin Exchanges**: Bitcoin promises hackers ‘untraceable financial transactions’ outside banking and tax regulations. Among the promises are Bitcoin is: permission-less, immune to seizure, censorship resistant, anonymous, etc.[7] Analysts Comment: The down side is: anything a smart person can create, another smart person can hack. Although we are unfamiliar with the technical details, we know that blockchain (a methodology for transferring bitcoin) can be (and has been) traced.

A. Canadian police now use Chainalysis to track and return stolen crypto

B. Poloniex confirms hackers identity, offers $10M white hat reward to return stolen funds

20. Analysts Comment continued: The other issue with Bitcoin is: how can you tell when you are successful? Bitcoin operates in an unregulated banking system, that is probably using unregulated accounting software and non-standard accounting practises. Worse, there are no guarantees you can get your money out of Bitcoin. Many Bitcoin exchanges and some Bitcoin currencies have been destroyed by hackers. Bitcoin exchanges are unregulated so there are no rules about ‘giving you your earnings in cash’. Large purchases made with Bitcoin are coming under increasing scrutiny as income from possible criminal activity. You can also count on some hackers targeting Bitcoin ‘wallets’ because to hackers it is easy, untraceable money.

21. Forecast: The entire Bitcoin ecosystem: Bitcoin currencies, wallets and in particular Bitcoin exchanges, will be under increasing attack from hackers.

[6] Source: Kon Briefing. Effective 20 December 2023 2611 organizations and an estimated 85.1-89.9 million individuals. MOVEit hack victim list.

[7] Reference: Bitcoin.com. The Benefits of Bitcoin

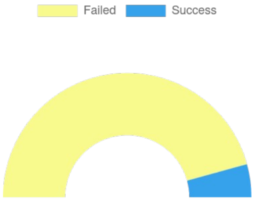
22. To sum up, 2024 will see more and worse from hackers. Top tier hackers remain largely untouched by law enforcement. Many nations lack the legislation to prosecute hackers. A relatively limited number of nations have the skill sets to protect themselves and hunt down hackers. The staggering dollar figures being paid in ransoms will continue to attract new talent to hacking groups.

RUSI(NS) under Brute Force Cyber Attack

23. DSC Staff provide technical support to RUSI(NS) (Royal United Services Institute(Nova Scotia) on an ‘as required’ basis. This week we have been receiving daily e-mail warnings of multiple ‘failed login attempts’. The warnings are a list of reports like this (below left):

Username: *Withheld*

```
IP address: 5.188.62.26
IP range: 5.188.62.*
Org: Not found
AS: AS34665 Petersburg Internet
Network ltd.
```



This image shows the number of ‘failed login attempts’ during the last 24 hours[8], thirty-five, (in yellow) vs the number of successful logins (in blue).

24. Analysts Comments: The lesson from this attack is that no organization, regardless of size, is immune from cyber attacks. Given RUSI(NS)’s composition and operations, there is no money, thus attacks for money are *highly unlikely*. This *very probably* rules out criminal hackers. There are no indications of hacktivists being interested in RUSI(NS), so an attack from them is *even less likely*. The persistence of the attacks infers a couple of possibilities: (1) an automated script may be in use to run the brute force attack and/or (2) a government (or an organization who can afford to pay for persistence) wants access to the web site.

25. The obvious inference is that this attack originates with the ‘Internet Research Agency’, a Russian company that works for the Russian government, specializing in ‘Information Operations’ using social media. A variety of other companies were also ‘spoofed’, their addresses used as the source for the attacks. Some of those companies are located in South-East Asia, more China’s normal sphere of influence than Russia’s. This raises the possibility that the attacks are Chinese in origin. Analysis of these attacks is ongoing.

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

[8] Source: The RUSI(NS) Host Provider sends an email on “User login lockout events had occurred due to too many failed login attempts or invalid username:” Analysis is based on e-mail for 10 Jan 2024. Details of Host Provider and specific attacks details withheld.