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: (42) Russia vs Ukraine / Hamas vs Israel

This report contains selected cyber-security information from 30th Oct to 9th Nov 2023.

Synopsis

1. Russia's cyber operations against Ukraine appear to be less effective – and that's the start of their issues. The IT Army of Ukraine has been busy – and successful. Iran's presence is visible in the Hamas vs Israel cyber conflict. Forty-Eight countries, including Canada, signed an agreement that governments will NOT pay ransomware.

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's Cyber Operations

3. According to Bloomberg, "*Russian cyberattacks are growing more sophisticated and have become daily occurrences aimed at disrupting vital infrastructure during wartime, Anton Demokhin, Deputy Minister of Foreign Affairs of Ukraine for Digital Development, Digital Transformation and Digitalization, said. According to Ukrainian government data seen by Bloomberg, the country recorded nearly 4,000 cyber incidents from January 2022 to September 2023, most attributed to Russia. Attacks surged threefold after Russia invaded in late February but later shifted toward espionage operations trying to obtain data on Russian spies and alleged war crimes.* "[1] The Bloomberg report not withstanding, reports of Russian cyber attacks in Ukraine are decreasing in frequency, inferring Russian cyber attacks are less effective.

4. Some Russian cyber campaigns are becoming less effective. A few Russian hacker groups (eg. KillNet) have shifted some of their targeting to Israel. Russian cyber operations outside Russia are progressively being exposed. For example Russia-based 'SWAT USA Drop Service' "*was hacked recently, exposing its internal operations, finances and organizational structure.*" The organization "*currently employs more than 1,200 people across the United States who are knowingly or unwittingly involved*

1 Source: Euromaidan Press. Bloomberg: Russia steps up cyberattacks to disrupt Ukraine's key services

in reshipping expensive consumer goods purchased with stolen credit cards."[2] This organization is exposed or doxxed but is not (yet) being persecuted. Russia Information Operations using Meta, 'X' and other social media are being discovered and their accounts shutdown.

5. The third trend we are seeing is persistent activity by Russian hackers, working inside Russia, against their own government. Security Affairs reported the arrest of two Russian hackers who were supporting Ukrainian cyber operations. The men are facing high treason charges for cyberattacks intended to disrupt Russian critical infrastructure. Russian intelligence did not reveal if the two arrests are related. One of the suspects is a student at Tomsk University while the second individual was detained in Belovo, in the Kemerovo region. He is believed to be a member of the Ukrainian cyber forces.[3]

IT Army of Ukraine

6. At the end of October hackers supporting Ukraine in the IT Army of Ukraine carried out DDoS attacks against three Russian internet providers "Miranda-media," "Krimtelekom," and "MirTelekom" affecting Crimea and occupied parts of Kherson, Zaporizhia, Donetsk, and Luhansk regions.[4] Russian internet operators confirmed that they had experienced an "*unprecedented level of DDoS attacks from Ukrainian hacker groups,*" temporarily disrupting their operations. The attack affected services such as cellular networks, phone calls, and internet connections. Most attacks were mitigated by Friday evening, 27th Oct. Some areas of Crimea experienced Internet disruptions on the following day.[5]

7. Early in November, Russia's largest bank, Sberbank, said it faced the most powerful distributed denial of Service (DDoS) attack in recent history. Sberbank's largest shareholder is the Russian government and holds approximately one third of Russian assets. "*We noticed that these are some new hackers. Their fingerprint is not known to us. That is, some new, very qualified criminals appeared on the market who began to systematically attack the largest Russian resources,*" stated the head of Sberbank. "*The bank said it managed to repel a DDoS attack that measured at 450GB/sec, which was generated by a botnet of 27,000 compromised devices.*"[6]

8. Two other pro-Ukrainian hacker groups, the 'DumpForums group' and the 'Ukrainian Cyber Alliance', "*said they defaced a website of the government-run National Payment Card System (NSPK) and reportedly gained access to the internal systems of the consumer payment network Mir ("world" in Russian).*" This is a Russian version of Visa or Mastercard. The hack was confirmed by NSPK.[7]

9. In a third hack, Rosgosstrakh, Russia's second-largest insurance company was hacked. the hackers are selling 400GB of data online for $50,000 in Bitcoin (BTC) or

2 Source: Krebs on Security. Russian Reshipping Service 'SWAT USA Drop' Exposed
3 Source: Security Affairs. Russian FSB arrested Russian hackers who supported Ukrainian cyber operations
4 Source: Security Affairs. IT Army of Ukraine disrupted internet providers in territories occupied by Russia
5 Source: The Record. Ukrainian hackers disrupt internet providers in Russia-occupied territories
6 Source: Bleeping Computer. Russian state-owned Sberbank hit by 1 million RPS DDoS attack
7 Source: The record. Pro-Ukraine group says it breached Russian card payment system

Monero (XMR) cryptocurrency. There is a single source report that personal data of Russian military intelligence agents was taken.[8]

10. Analysts Comment: We see indications of increasing capabilities/increasing skill levels in some of the hacker groups that support Ukraine. There are also indications that some groups may be co-ordinating their efforts with the Ukrainian government. For example, the DDoS attacks against Interent Service Providers (ISP) in Russian occupied Crimea occurred as Ukrainian troops crossed the Dnipro River.

Hamas vs Israel

11. As of 9th of Nov the cyber front between Hamas and Israel has generated noise in media and social media, but there have been no verified impact on critical systems or strategic damage, in either direction. According to Israel "*more than fifteen state-sponsored and Advanced Persistent Threat (APT) groups related to Iran and Hezbollah have been attempting to target critical services and infrastructure."* Also "*two pro-Russian hacktivist groups, Killnet and Anonymous Sudan, have targeted Israeli organizations since the war's outbreak.*"[9] Subsequently a number of 'hacktivists', other hackers groups such as 'AnonymousGhost' (AnonGhost) and a list of criminal hacking groups claim to have joined the pro-Palestinian side.

12. Pro-Palestinian groups have claimed successes, however these 'successes' are either unverified or substantially less than claimed. For example Pro-Palestinian hackers group 'Soldiers of Solomon' claimed: "*they damaged the production cycle of the production plant of Flour Mills Ltd ... a successful cyber attack on Ashalim Power Station located in the Negev desert and ... more than 50 servers, security cameras and a smart city management system in the Nevatim military area.*"[10] None of the claims have been verified. There are fewer groups supporting Israel. So far their hacking claims are also unverified.

13. One of the reasons for the lack of success by the pro-Palestinian side is "*the proactive cyber defensive approach adopted by the Israeli National Cyber Directorate (INCD) as well as the mobilization of the country's cyber security ecosystem.*"[11] For example, some Israeli hospitals separated their networks from the Internet in order to prevent their systems from being hacked.

International Counter Ransomware Initiative

14. Three years ago the United States created the International Counter Ransomware Initiative (CRI). This year 'top' officials from the White House worked at having all member countries, including thirteen new members, agree ***not*** to pay ransoms to cybercriminals. Among the forty-eight member countries are: the UK, Australia, Canda, the European Union, Japan, Singapore, India, and Israel.[12] According to

8 Source: Teiss. Russian insurance giant Rosgosstrakh hacked, data of Russian military intelligence agents stolen

9 Source: National Interest. The Cyberwarfare Front of the Israel-Gaza War

10 Source: Security Affairs. Pro-Palestinian hackers group 'Soldiers of Solomon' disrupted the production cycle of the biggest flour production plant in Israel

11 Source: National Interest. The Cyberwarfare Front of the Israel-Gaza War

ITWorldCanada: *"it isn't clear what the declaration means. It doesn't include a promise to forbid provincial, state, county, or municipal governments from paying to get access back to stolen or encrypted data. Nor does it include a promise to forbid businesses from paying."*

> *"CRI members affirmed the importance of strong and aligned messaging discouraging paying ransomware demands and leading by example," the group said in a statement.*[13]

15. The three themes of this years meeting were members agreeing to:

A. Help identify illicit fund flows (ransomware payments) that are funding ransomware,

B. Increase information-sharing capabilities via two dedicated platforms (Cybersecurity Intelligence hubs) that let countries rapidly exchange threat indicators, and

C. the "*First-ever joint Counter Ransomware Initiative policy statement declaring that member governments will not pay ransoms.*" Under that pact, governments, their agencies and departments won't cough up ransoms.

16. Mandiant's chief technology officer Charles Carmakal made several important observations:

A. "*governments and the private sector must work together to ensure victim organizations aren't completely left to fend for themselves when trying to get operations back online after a ransomware incident,*"

B. "*public and private sector can do more to notify victims when evidence of compromise is identified,*"

C. "*Eliminating the option for victims to pay could be difficult for those organizations that aren't as cyber mature or ready as others.*"[14]

17. Analysts Comment: Canada's Communications Security Establishment (CSE) is: limited in its work with the private sector, poor at notifying victims of compromise and has been on record as saying 'payment of ransoms is a business decision'. We have to ask: do the diplomats who signed the agreement know what the current Canadian policy is, does this represent a radical change in Canadian policy and is the government serious about this agreement.

---

12 Source: The Register. US officials close to persuading allies to not pay off ransomware crooks
13 Source: ITWorldCanada. Forty-eight governments pledge not to pay ransomware gangs
14 Source: The Register. US officials close to persuading allies to not pay off ransomware crooks