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

CyberWarfare Plus RCMP & City of Hamilton Hacked

This report contains selected cyber-security information from 23rd Feb to 7th March 2024.

Synopsis

1. Russia cyber-attacks Estonia and Sweden. Russian hackers NoName57(16) continue to develop their DDoS software. Ukraine hacks the Russian Ministry of Defense (again). Iran deploys a fake 'hostage support website' to spread malware. LockBit Ransomware group lives? In Canada the RCMP and the City of Hamilton get hacked.

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

3. **Estonia's Banking System Cyber-Attacked**. On Friday 1st March Estonia's security and software firm 'Hansab' was cyber attacked. "*Hansab manages the ATM networks for major banks such as Swedbank, Luminor, and LHV Bank.*" Information is limited however it *appears* to have been a DDoS attack. Estonia's State Information System Authority, "*swiftly took action ... ensuring that despite these challenges, commercial bank services including ATMs, card payments, and online banking continue to operate smoothly across the country.*"[1]

4. **Sweden Hit By Multiple Cyber-Attacks.** Sophiahemmet, a private hospital located in Norra Djurgården, Stockholm, was hit by a ransomware attack. The hacker group Medusa encrypted the hospitals data and demanded a ransom to delete the data they stole. The hospital has been disconnected from the regional information system and is using a combination of backups and manual system to continue its operations. This attack is seen as part of a larger pattern of cyber threats "*affecting both small municipalities like Bjuv and significant infrastructure such as Tietoevry's Swedish data center.*"[2]

1 Source: BNNBreaking. Hansab Cyber Incident Disrupts IT Systems, Estonia's Banking Operations Remain Unaffected

5. Russian hacker group, NoName057, said Tuesday 5th March it carried out targeted cyberattacks against Sweden. The group claimed to have "*taken down two government websites*" and "*also shut down the Swedish Competition Authority's website.*" Per Lovgren, spokesman for the Swedish Authority for Privacy Protection, IMY, told the Aftonbladet newspaper, "*We have been exposed to an overload attack*"[3]. (Distributed Denial of Service (DDoS) Attack)

6. Although the number of attacks executed by NoName057(16) has reduced based on a month to month comparison, the group has been observed changing tactics. Sekoia.io, a cybersecurity monitoring platform, observed significant developments in the software (Project DDoSia) shared by the group, including updates enhancing compatibility with different processor architectures and operating systems. "*The DDoSia software introduces enhanced encryption mechanisms for data transmission between users and their C2 servers*." NoName057(16) *"has also provided tailored versions of the software for users based on their geographical location, with explicit instructions for Russian users to employ a VPN."*[4] Analyst Comments: Target analysis from multiple sources suggests twenty-five percent of targeting is against Ukrainian targets[5] with most of the remaining targeting being against Western European countries including: Denmark, Finland, and Switzerland.

Ukraine

7. **Ukraine Hacks Russian Ministry of Defense**. On 4th March "*the Main Intelligence Directorate (GUR) of Ukraine's Ministry of Defense announced it had breached the Russian Ministry of Defense servers ... and exfiltrated confidential documents.*

- *confidential documents, including orders and reports circulated among over 2000 structural units of the Russian military service.*
- *software used by the Russian Ministry of Defense to encrypt and protect its data.*
- *a collection of secret service documents belonging to the Russian Ministry of War*

The stolen documents allowed intelligence analysts of Ukraine's GUR to delineate the comprehensive structure of the Russian Ministry of Defense system and its various units."[6] "*Analysis of the data obtained has also helped identify the generals, other senior officials of the Russian Defence Ministry structural units, as well as deputies, assistants and specialists − everyone who used the electronic document circulation software called Bureaucrat,*" and "*that operations in Russia's cyberspace are ongoing."*[7]

2 Source: BNNBreaking. Cyber Attack Hits Sophiahemmet Hospital, Stockholm: Ransomware and Data Theft Unfold

3 Source: AA. Russian hacker group claims cyberattack against Sweden

4 Source: Infosecurity Magazine. Hacktivist Collective NoName057 Strikes European Targets

5 Source: Cyber Security News. Project DDoSia – Russian Hackers "NoName057(16)" Planning Massive DDoS Attack

6 Source: Security Affairs. UKRAINE'S GUR HACKED THE RUSSIAN MINISTRY OF DEFENSE

Cyber-Intelligence Report

Iran

8. **Fake Website targets Hostage Supporters**. According to a report in the Jerusalem Post, Iranian hackers reportedly created a fake web site that identifies itself as part of the "*'Bring Them Home Now' movement, calling for the return of the hostages.*" What the site really does is trigger a decoy malware download disguised as an application related to the hostages. The decoy malware is called MINIBUS. "*According to Mandiant, the hacker group is identified as UNC1546, or Tortoiseshell, is heavily linked to Iran's Islamic Revolutionary Guard Corps (IRGC).*"[8] "*MINIBUS acts as a backdoor, providing ... entry to compromised devices. Cybercriminals can remotely execute commands, steal sensitive files, and introduce more malicious software.*"[9]

LockBit

9. On 19th February law enforcement in North America, Europe, and Asia seized 34 servers belonging to the LockBit ransomware group, "*took over the group's Tor-based leak sites, froze cryptocurrency accounts, and harvested technical information on the RaaS (Ransomware as a Service). Authorities also announced that they obtained 1,000 decryption keys*" and arrested two individuals. "*Shortly after, the US government announced a $10 million reward for information on LockBit leaders and a $5 million reward for information on affiliates ... Over the weekend (24 -25 February), an individual involved with the RaaS, who uses the moniker of "LockBitSupp", launched a new leak site that lists hundreds of victim organizations.*"[10] Analysts Comment: Major ransomware groups are complex. There is a small group of 'leaders' (who probably founded the group), a larger group of 'key personnel' (think department heads), a group of programmers/hackers that design the malware, often a call center, and a group who 'launders' the ransoms. Below that are the dozens of affiliates (think franchisees). Ransomware groups are VERY hard to kill off.

Canada

10. **RCMP Hacked**. On Friday 23rd February, RCMP chief security officer Paul L. Brown sent an email to staff that said "*the force is managing a "cyber event" and urged employees to stay vigilant.*" An RCMP Spokesman said "*The situation is evolving quickly but at this time, there is no impact on RCMP operations and no known threat to the safety and security of Canadians.*"[11] Bleeping Computer observed that the RCMP website was down ... and throwing an HTTP 404 (Not Found) error message. The RCMP informed the company that "*The issue with the RCMP's public website over the weekend is unrelated to the cyber event." ... Our network servers, managed by Shared Services Canada (SSC) run high volume traffic which is what happened this weekend. When the servers run slowly, some users experience an error message*

7 Source: Ukrainian Pravada. Ukraine's Defence Intelligence reports on hacking Russian Defence Ministry servers: much information obtained
8 Source: The Jerusalem Post. Iranian hackers use Israeli hostage site for cyber attacks - report
9 Source: PCrisk. How to eliminate MINIBUS malware from infected computers
10 Source: Security Week. LockBit Ransomware Gang Resurfaces With New Leak Site
11 Source: CBC. RCMP networks targeted by cyberattack

Cyber-Intelligence Report

when trying to access the website due to the overload."[12] Analysts Comment: 'high volume traffic' *could* be an indicator of a DDoS attack. No amplifying information or updates have been released.

11. **Hamilton Hacked**: On Sunday 25th February, the City of Hamilton Ontario said it "*suffered a city-wide phone and email "disruption" to municipal and public library services, which included the Bus Check Info Line and the HSRNow transit planning app.*"[13] On Monday the city changed its description to a 'cyber incident'. City manager Marnie Cluckie said "*the city initially thought it was an issue with an IT server.*" The city also said: "*Critical services such as transit, water and wastewater treatment and emergency services are operational.*"[14] On 4th March the city confirmed that the cyber incident was a ransomware attack.[15] According to the city manager: "*the City does not believe that people's personal data or information has been accessed.*"[16]

12. In a briefing 5th March, the city manager: "*wouldn't say what strain of the malware the city has been hit with, how long it will take to restore full services, or whether the city has received a demand for money. Some information has to remain confidential, she explained. Asked if the city is considering a ransom payment, Cluckie replied, "I can assure you we're going to do what's best for the city.*" According to ITWorldCanada "*Regular council meetings have been temporarily suspended.*" CHCH-TV reports that "*city council has been meeting behind closed doors to discuss the attack. Mayor Andrea Horwath told reporters that's partly because municipal staff's priority is dealing with the cyber attack, so meetings can't be staffed as needed.*"[17]

13. A week following the initial attack the following city services 'are impacted':

Phone Lines	Online Systems	Engineering Services	Cemeteries
Libraries	Public Health	Property Taxes	City Vendors
Child Care	Transit	Hamilton Water (Customer Service)	Some Recreation Services

14. Analysts Comment: Canada remains lucrative territory for hackers because Canadian political leaders at all levels refuse to talk about hackers. Instead of being forewarned, and learning a few basics to protect themselves, Canadians remain oblivious to the threat. When hacked, Canadians tend to pay ransoms, because they don't know their options. The only people who win from this approach are hackers.

---

12 Source: Bleeping Computer. RCMP investigating cyber attack as its website remains down
13 Source: ITWorldCanada. Cyber attack on Hamilton knocks out municipal phone, email
14 Source: CBC. Cyber experts 'working around the clock' to fix disruption of Hamilton services: city manager
15 Source: City of Hamilton. Cybersecurity Incident Response
16 Source: City of Hamilton. City Confirms Cyber Incident is a Ransomware Attack
17 Source: ITWorldCanada. Hamilton confirms ransomware is behind cyber attack