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 (26) Disinformation Operations

This report contains selected cyber-security information from 4th to 17th March 2023.

Synopsis

1. Russia continues to 'phish' Ukrainian government organizations. A Russian 'patriotic hacker group attacked a Ukrainian radio station. After many nuclear threats, Russia was on the receiving end of a bogus nuclear warning. Many Russians don't seem to appreciate that their actions can have consequences, from disinformation campaigns, lack of ethics or political manipulation. China is a major cyber threat. Buy Canadian?

2. Russian 'Courses of Action' for cyber forces, including allies such as 'patriotic', mercenary, and domestic criminal hackers are *assessed* as:

> **Ongoing**: Russian cyber forces, including allied forces, have launched a series of cyber ***campaigns*** against **both strategic targets and general targets** as well as vulnerable governments.
>
> **Worst Case Scenario**: President Putin decides to focus Russia's cyber attacks on one country (such as Canada) or a small group of vulnerable countries. *Assessed as UNLIKELY.*
>
> **Best Case Scenario:** Russia agrees to cease or is forced to cease offensive cyber operations. *Assessed as VERY UNLIKELY.*

Russia

3. **Cyber Attacks On Ukraine:** In February several security organizations reported that Russia was using the REMCOS Remote Access Trojan (RAT) to trap 'Ukrainian government entities' using phishing attacks.[1] The REMCOS RAT can compromise any type of Windows from Windows XP onward, placing a backdoor and granting full access to the hackers for activities such as data exfiltration and command execution using high-level privileges.[2] What is not clear is how successful the attacks were. Different organizations report different methodologies. Analysts Comments: The Russian attackers are *almost certainly* constantly changing the lures (for phishing attacks).

4. In a separate attack, Unkrainian Halychyna FM, a highly popular radio station

1 Source: CheckPoint Software. February 2023's Most Wanted Malware: Remcos Trojan Linked to Cyberespionage Operations Against Ukrainian Government

2 Source: Bleeping Computer. Old Windows 'Mock Folders' UAC bypass used to drop malware

broadcasting in Western Ukraine, was hit by a Distributed Denial of Service (DDoS) attack. A pro-Kremlin Telegram channel known as The People's Cyber Army asked its over 6000 followers to attack the Ukrainian radio station. The radio stations' web site was off-line for approximately two hours on March 2nd.[3]

5. **Disinformation Operations:** Russia is continuing its campaign of disinformation on Ukraine using TA499, a two-person group of operators, Vovan and Lexus. The objective is to fracture anti-Russian sentiment in North America and the EU. The phishing lures are emails or phone calls which masquerade as the Ukrainian Prime Minister Denys Shmyhal and his assistant. Emails can also appear to originate from official embassies with subjects such as 'Prime Minister of Ukraine Request'. *The primary purpose is to persuade the victims to take part in phone calls or video chats from which pro-Putin snippets can be elicited and published – thereby discrediting any previous anti-Putin comments."[4] TA499 have personas that not only post the material discussed in this report online but also perform reenactments on Russia state-sponsored media as well as attend conferences," says Proofpoint.*

6. CyberSecurity company 'Proofpoint', reports "*TA499 targets US and European politicians, and leading businessmen and celebrities who have spoken out against Putin's invasion. The UK Secretary of State for Defense, Ben Wallace has been targeted. Other targets have included: "The mayor of Vienna Michael Ludwig, as well as other mayors in Warsaw, Budapest, Berlin, and Madrid. Celebrities JK Rowling and Elton John have also been targeted in the past.*[5]

7. In more general terms, ... *the Kremlin has deployed new disinformation themes and tactics to weaken US support for Kyiv with help from conservative media stars and some Republicans in Congress. ... New studies from thinktanks that track disinformation have noted that alternative social media platforms such as Parler, Rumble, Gab and Odysee have increasingly been used to spread Russian falsehoods since Facebook and Twitter have imposed more curbs on Moscow's propaganda. Other pro-Russian messages focused on the economic costs of the war for the US have been echoed by Republicans in the powerful far-right House Freedom Caucus such as Marjorie Taylor Greene, Scott Perry and Paul Gosar, who to varying degrees have questioned giving Ukraine more military aid and demanded tougher oversight. Analysts who track Russia's disinformation see synergies between the Kremlin and parts of the US right that have helped spread some of the biggest falsehoods since the start of the invasion. "Russia doesn't pull even its most outlandish narratives out of thin air – it builds on existing resentments and political fissures,"*[6]

8. **Cyber Attacks on Russia:** Russian 'prime time' TV shows have asked why Russia has not used nuclear weapons against western countries such as the UK.[7] This may have been intended a 'humour' however on March 10th "Russians were urged to immediately seek shelter, take anti-radiation pills and wear gas masks. The message was shown on state TV with a black and yellow radiation symbol and a map of Russia

3 Source: ipi Media. Radio Halychyna cyber-attacked following appeal by Russian hacker group
4 Source: Security Affairs: Pre-Deepfake Campaign Targets Putin Critics
5 IBID.
6 Source: Guardian (UK). Russia disinformation looks to US far right to weaken Ukraine support
7 Source: NewsWeek. Russian State TV Keeps Threatening Nuclear Strikes—Should We Be Concerned?

slowly being covered in red."[8] It was the third time in the past month that Russian broadcasters have been targeted. Ukraine has not taken responsibility for any of the alleged cyber attacks.[9] Analysts Comment: Nor has any other group.

9. **GeoPolitical Consequences:** The Russia Ukraine conflict is growing international cyber cooperation. *During a Senate Armed Services Committee hearing Gen. Paul Nakasone, USCYBERCOM's commander and the director of the National Security Agency, told lawmakers that "success for U.S. Cyber Command will be measured by how effectively foreign adversarial actors are prevented from achieving their strategic objectives." Nakasone said that 'hunt forward' has built "tremendous confidence between nations" since it launched in 2018, including undertaking 47 different missions in 22 countries, as of Tuesday's hearing.*[10] Even before Sweden and Finland join NATO, USEUCOM's Cyber Analytics cell joined Finnish and Swedish military officials to discuss best-practices for network-based threat hunt tactics.[11] Analysts Comments: Russia's tactics were intended to 'divide and conquer'. Unfortunately for Russia their tactics are producing the opposite effect.

10. **Consequences:** The New York Post reported that "*ruthless Russian-linked hackers have posted naked photos of cancer patients on the dark web after a Pennsylvania health group refused its ransom demands. Lehigh Valley Health Network (LVHN) said that three intimate photos of patients receiving radiation oncology treatment were among items posted online by BlackCat — "a ransomware gang associated with Russia."*[12] Analysts Comment: There are some Russians who do not seem to understand that there are ethical and moral lines that, if crossed, will provoke reactions that they do not want. This incident is more likely to provoke American Health organizations into NOT paying ransoms, than getting them to co-operate.

11. There are already indications that Russian criminal hacker activity is producing unintended long-term effects. CSO (Chief Security Officer) magazine says "*attacks by identified Russian organized cybercrime groups ... have shed light on the critical need for companies to revamp security protocols, particularly within critical infrastructures such as healthcare, energy, and public services.*"[13] Analysts Comment: Many corporate and business organizations have refused to scale-up cyber defences, preferring to pay-off criminals. The recognition of the critical need for change represents a radical shift in thinking. Cyber regulators are ordering changes in how critical infrastructure is defended. The most recent action in the U.S. is from the Cybersecurity and Infrastructure Security Agency (CISP) *that ransomware vulnerability warning pilot—or RVWP—will "identify organizations with internet-accessible vulnerabilities commonly associated with known ransomware actors by using existing services, data sources, technologies and authorities, including our free Cyber Hygiene Vulnerability Scanning service.*" In effect this provides "*vulnerability and threat warning in addition to the*

8 Source: Express UK. Ukraine LIVE: Russians nuclear panic as they are ordered to rush to bomb shelters
9 Source: Independent UK. Fake 'nuclear bomb' alert on TV and radio scares Russians
10 Source: Next Gov. USCYBERCOM's Operations Have Strengthened Allies, Agency Lead Says
11 Source: EUCom. US, Swedish, Finnish militaries join forces to defend cyber domain
12 Source: New York Post. Russian hackers post nude photos of US cancer patients to dark web in sick extortion plot
13 Source: CSO Magazine. Russia-Linked Ransomware Gangs Could Spark Revamped Cybersecurity Protocols in Critical Infrastructure

requirements to report covered cyber incidents and ransomware payments" to the agency."[14] Similar regulations are going into effect in the UK and EU.

Chinese Cyber Operations

12. The UK's Internal Security organization, MI5, has been directed to form a new section to "counter Chinese hacking, espionage [in the UK]". The 'agency' will be called "National Protective Security Authority" and *is tasked to to provide businesses and universities with advice on how to deal with industrial espionage.*[15] The U.S. Director of National Intelligence, Avril Haines, told lawmakers China's Communist Party and Russia's invasion of Ukraine both present ongoing and possibly expanding threats to U.S. interests. China's political party, Haines said, is *using coordinated "whole-of-government tools to demonstrate strength" and force its regional neighbours to acquiesce to its strategic desires*.[16] The Director described China as "*our unparalleled priority*" and the PRC as "*increasingly challenging the United States economically, technologically, politically and military around the world.*"[17]

13. Analysts Comment: Many consumers don't perceive a threat from China. Unfortunately Chinese law and Internet regulations require ALL Chinese organizations to provide their government with full access to their networks and data – on demand. The other issue is that Chinese firms obey Chinese law, and tend to ignore other regulations. For example the Chinese shopping application 'SHEIN' collects user data including pricing and URL data from its customers clipboards.[18] Not ALL Chinese firms do this however it is a frequently seen pattern. Bottom Line: Doing anything with the People's Republic of China, its agents and/or its businesses has serious risks.

Canada

Christyn Cianfarani, chief executive officer of the Canadian Association of Defence and Security Industries (CADSI), told the House of Commons defence committee Canada's allies buy more Canadian cybersecurity products than Ottawa does. "*Those numbers speak to a central challenge we face in this country when it comes to cyber,*" Cianfarani said. "*Our allies see more value in Canada's cybersecurity sector than Canada does. Something is wrong with that picture.*"[19]

---

14 Source: Next Gov. CISA Launches Ransomware Warning Pilot for Critical Infrastructure
15 Source: ITPro. MI5 to establish new security agency to counter Chinese hacking, espionage
16 Source: UPI. Intelligence officials warn lawmakers about threat to U.S. posed by China, Russia
17 Source: CyberScoop. US intel: Chinese influence operations are growing more aggressive, more similar to Russia's
18 Source: Naked Security. SHEIN shopping app goes rogue, grabs price and URL data from your clipboard
19 Source: Channel Daily News. Canada's allies buy more Canadian cybersecurity products than Ottawa does, parliament told