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: (40) CyberWarfare Expands to Hamas and Israel

This report contains selected cyber-security information from 30th Sept to 12th Oct 2023.

Synopsis

1. The cyberwarfare between Russia and Ukraine was relatively quiet, with most of the reporting dedicated to hacktivists engaging between Hamas and Israel. The Red Cross published rules for Hacktivists. The saga of the MOVEit hack continues and there are a large number of Canadian victims.

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. In the UK "*it was reported that the Royal Family's website, royal.uk, was taken down for around 90 minutes, displaying an error message from around 10.20 on Sunday (1st Oct) morning.*" Hacker KillMilk, leader of the Russian hacktivist group KillNet, took credit for the attack in a Telegram post. The attack is *probably* due to the Royals support for Ukraine and in particular due to "*King Charles's condemnation of Russia's 'unprovoked aggression' ... in Paris, as he declared 'Ukraine must prevail'.*"[1] The attack was a Distributed Denial of Service attack. No breach of the website or other damage was reported.

4. On 28th Sept the Russian airline booking system 'Leonardo' was hacked by Ukraine's IT army. Mykhailo Fedorov, Ukraine's Minister of Digital Transformation was quoted: "*the Russian airline booking system Leonardo was hacked by Ukraine's IT army.*"[2] Apparently Aeroflot flights, as well as flights from Rossiya Airlines and Pobeda were disrupted. Reports differ on the effectiveness and length of the attack.

[1] Source: Daily Mail (UK). Russian hackers 'crash Royal Family website' ...

[2] Source: Yahoo News. Ukrainian IT army stopped operations at major Russian airports

Hamas vs Israel

5. Less than an hour after Hamas launched its attack on Israel (on Saturday 7th Oct) Anonymous Sudan cyber-attacked emergency warning systems, claiming to have taken down ‘alerting applications’ in Israel. They also DDoSed (Distributed Denial of Service Attack) and successfully blocked ‘The Jerusalem Post’, the largest English-language daily newspaper in Israel.[3] Other hacker groups were quick to join the Palestinian side:

A. ‘Cyber Av3ngers’ targeted the Israel Independent System Operator (Noga), a power grid organization, and the Israel Electric Corporation, the primary electrical power supplier to Israel and Palestine.[4]
B. ‘KillNet’ targeted Israeli government websites.
C. ‘Libyan Ghosts’ a hacktivist collective, focused on the digital defacement of smaller websites in Israel.
D. ‘Sylhet Gang’ attacked the Israeli patent office.[5]
E. ‘AnonGhost’ “*exploited an application programming interface (API) vulnerability in* (Israels’) *real-time rocket alert app.”*[6]

6. As many as 35 “*pro-Palestine hacking groups have commenced a series of attacks on diverse targets within Israel.” reported The Cyber Express. “These groups, while advocating for Palestinian interests, remain shrouded in mystery, their exact numbers and identities are yet to be verified.”*[7] A few pro-Israel groups have entered the conflict:

A. The cybercrime outfit ‘Arvin Club’, has also allegedly stolen data from the Iranian Islamic Azad University of Shiraz.
B. The ‘Threatsec’ hacktivist group has claimed a breach on Palestinian ISP Alfanet.[8]

Red Cross Issues Wartime Hacktivist Rules

7. The International Committee of the Red Cross (ICRC) has published a set of rules for hacktivists (civilian political activists who use hacking as their means of protest and/or activism). The ICRC describes the rate at which civilians are becoming involved in international conflicts as "*a worrying trend*". The ICRC specifically used “*the IT Army of Ukraine – the vigilante band of hacktivists that assembled early in the war using the Telegram messaging platform – as an example of civilians joining war efforts.*”[9] The ICRC also warned hackers “*their actions can endanger lives, including their own if deemed to make them a legitimate military target.*” The ICRC, responsible for overseeing and monitoring the rules of war, bases the rules on international

[3] Source: Security Week. Hackers Join In on Israel-Hamas War With Disruptive Cyberattacks
[4] Source: Security Week. Hackers Join In on Israel-Hamas War With Disruptive Cyberattacks
[5] Source: The Register. Hacktivist attacks erupt in Middle East following Hamas assault on Israel
[6] Source: Cyber News. Red Alert, Israel's rocket alert app, breached by hacktivists
[7] Source: The Cyber Express. Cyber Warfare Surges as Over 35 Hacktivist Groups Join Israel-Palestine Conflict
[8] Source: The Register. Hacktivist attacks erupt in Middle East following Hamas assault on Israel
[9] Source: The Register. Red Cross lays down hacktivism law as Ukraine war rages on

humanitarian law. The rules[10] are:

1. Do not direct cyber-attacks against civilian objects
2. Do not use malware or other tools or techniques that spread automatically and damage military objectives and civilian objects indiscriminately
3. When planning a cyber-attack against a military objective, do everything feasible to avoid or minimize the effects your operation may have on civilians
4. Do not conduct any cyber-operation against medical and humanitarian facilities
5. Do not conduct any cyber-attack against objects indispensable to the survival of the population or that can release dangerous forces
6. Do not make threats of violence to spread terror among the civilian population
7. Do not incite violations of international humanitarian law
8. Comply with these rules even if the enemy does not

8. Response to the rules varies. The IT Army of Ukraine said it will "*make best efforts to follow the rules*" *even though it may place them at a disadvantage to their adversaries.* A KillNet[11] spokesman said: "*Why should I listen to the Red Cross?*" He later said he "*agrees to the terms and rules of the Red Cross, let this be the first step from KillNet to peace*".[12] A representative of Anonymous Sudan told BBC News the new rules were "*not viable and that breaking them for the group's cause is unavoidable.*"[13]

9. The ICRC also drew up rules for countries themselves in an effort to dissuade them from tolerating hacktivist activity. Analysts Comment: The US, Russia, and China, are **NOT** part of the International Criminal Court, the institution in charge of administering international law.

The four rules[14] are:

1. If civilian hackers act under the instruction, direction or control of a State, that State is internationally legally responsible for any conduct of those individuals that is inconsistent with the State's international legal obligations, including international humanitarian law
2. States must not encourage civilians or groups to act in violation of international humanitarian law
3. States have a due diligence obligation to prevent international humanitarian law violations by civilian hackers on their territory
4. States have an obligation to prosecute war crimes and take measures necessary to suppress other IHL violations

10. Analysts Comment: It is *assessed* with *high probability* that cyber bad actors such as Russia, China, North Korea, Iran are *very unlikely* to follow the ICRC rules. Further it

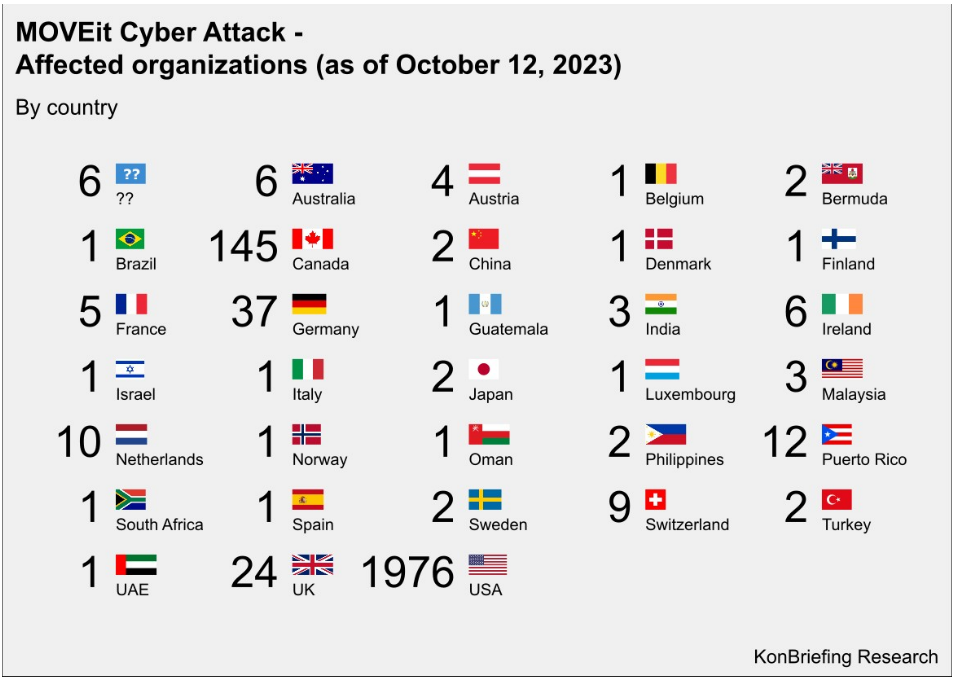
[10] Source: BBC Tech News. Rules of engagement issued to hacktivists after chaos
[11] KillNet: A Russian Patriotic Hacker group
[12] Source: BBC Tech News. Ukraine cyber-conflict: Hacking gangs vow to de-escalate
[13] Source: BBC Tech News. Rules of engagement issued to hacktivists after chaos
[14] Source: The Register. Red Cross lays down hacktivism law as Ukraine war rages on

is *assessed* with *high probability* that hacker groups operating under the sphere of influence of these countries are also *very unlikely* to follow the ICRC rules.

MOVEit

11. According to Kon Briefing as of Thursday 12th Oct, the MOVEit hack by the Cl0p ransomware group, has victimized 2274 organizations and between 62.5 and 67.4 million individuals.[15] Notable additions to the list include an American Credit Union[16] and Sony Group. Sony Interactive Entertainment has warned its American "*current and former employees and their family members about a cybersecurity breach that exposed personal information.*"[17] The estimated cost of the MOVEit breaches using IBM data is **$9,923,771,385** (USD) with the estimated earnings from the hack at **$100,000,000** (USD). The U.S. State Department is offering a $10 million dollar bounty for information on the Cl0p ransomware group.[18]

12. Analysts Comment: Very few of the Canadian organizations that have been hacked have been reported in the Canadian media. The organizations were identified by ransomware data visible to cyber security companies, such as ransom payments.



MOVEit Cyber Attack -
Affected organizations (as of October 12, 2023)

By country

6	??	6	Australia	4	Austria	1	Belgium	2	Bermuda
1	Brazil	145	Canada	2	China	1	Denmark	1	Finland
5	France	37	Germany	1	Guatemala	3	India	6	Ireland
1	Israel	1	Italy	2	Japan	1	Luxembourg	3	Malaysia
10	Netherlands	1	Norway	1	Oman	2	Philippines	12	Puerto Rico
1	South Africa	1	Spain	2	Sweden	9	Switzerland	2	Turkey
1	UAE	24	UK	1976	USA				

KonBriefing Research

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

[15] Source: Kon Briefing. MOVEit hack victim list

[16] Source: CyberNews. MOVEit saga drags on as credit union discloses 100K victims

[17] Source: Bleeping Computer. Sony confirms data breach impacting thousands in the U.S.

[18] Source: TechCrunch. MOVEit, the biggest hack of the year, by the numbers