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: (43) How Russia Hacked Denmark

This report contains selected cyber-security information from 10th to 23rd Nov 2023.

Synopsis

1. A Danish report on a May attack documents the potential of a Russian attack on critical infrastructure. A Russian 'worm' malware operated by a FSB hacking team has leaked out of the Russia Ukraine theatre and is spreading globally. Russia gets hacked by allies China and North Korea. Cyber attacks on Israel have been ineffective so far. Israel is progressively making counter-moves. MOVEit! hack update.

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.

Analysis

3. SektorCERT, Denmark's specialist organization for cybersecurity, released a report on a May Russian cyber attack that breached 22 companies across a number of days. On 25th April Zyxel announced that "*there was a critical vulnerability in a number of their products. The vulnerability received a score of 9.8 on a scale of 1-10, which means that the vulnerability was both relatively easy to exploit and that it could have major consequences."* Zyxel firewalls are used by many of SektorCERT's members. On 11th May the first attack was mounted against 16 Danish energy companies. The SektorCERT report noted: "*Not once did a shot miss the target. All attacks hit exactly where the vulnerabilities were. ... 11 companies were compromised immediately ... meaning the attackers gained control of the firewall at these companies and thus had access to the critical infrastructure behind it."*[1]

4. On May 22nd the second wave began. Over the next several days, "*more members were compromised and a payload named MIPSkiller was used in all cases, and ... members' firewalls were then used to participate in attacks against other targets. ... It was notable for these second-wave attacks that the attackers may have had*

1 Source: SektorCert. The attack against Danish critical infrastructure

knowledge of vulnerabilities that Zyxel had not yet disclosed,"[2] as well as new known exploits and cyber weapons.

5. Analysts Comments: Most Russian cyber attacks outside Ukraine have been Distributed Denial of Service (DDoS) attacks, conducted by Russian patriotic hacker group(s). Most of these attacks can be described as nuisance attacks. The next tier of attacks are conducted by either Government hacker teams or criminal hackers. These attacks can be information collection and/or destructive attacks. The Danish attack is a third level of capability, one previously seen only during military attacks such as the invasion of Georgia. Even those attacks were mostly suppressive instead of destructive. What the Danish attack demonstrates is:

A. Russia *highly probably* has unidentified ways of collecting information on target networks,

B. Russia *highly probably* has ways to access networks that defenders are unaware of,

C. Russia has the ability to mount destructive cyber attacks against critical infrastructure with no warning.

6. **LitterDrifter.** A Russian Federal Security Service (FSB), Gamaredon, has been using "*a USB propagating worm called LitterDrifter in attacks targeting Ukraine.* Unfortunately this 'worm' has leaked out of theatre and has been detected in: "*U.S., Vietnam, Chile, Poland, Germany, and Hong Kong ... based on VirusTotal submissions*." LitterDrifter has two main features: "*automatically spreading the malware via connected USB drives as well as communicating with the threat actor's command-and-control (C&C) servers*".[3] This means the 'worm' (the malware) makes copies of itself, in order to spread/infect other computers. What happens next to the victim's computer depends on what is downloaded from Gamaredon's command and control servers. "*Gamaredon's infrastructure remains flexible and volatile, with domains used as placeholders for the IP addresses used as C&C servers, and with IP addresses operational for roughly 28 hours, except for the active C&C, which changes several times a day."*[4]

7. Analysts Comment: This is the second known malware that has 'escaped' the Russia Ukraine theatre. The first is the improved Distributed Denial of Service script being sold by 'KillNet'. LitterDrifter is the second. Over time it can be expected to propagate globally. If the LitterDrifter virus connects to its Command and Control servers, it will download whatever instructions or malware are waiting in those servers. What does this mean? CheckPoint Software's analysts said: "*It's clear that LitterDrifter was designed to support a large-scale collection operation, ... It leverages simple, yet effective techniques to ensure it can reach the widest possible set of targets.*"[5] This malware could cause problems for a long time.

8. **Russia Hacked By Allies.** "*This week, Russian state officials and cybersecurity*

2 Source: SektorCert. The attack against Danish critical infrastructure

3 Source: The Hacker News. Russian Cyber Espionage Group Deploys LitterDrifter USB Worm in Targeted Attacks

4 Source: Security Week. Russia's LitterDrifter USB Worm Spreads Beyond Ukraine

companies, including Solar, provided some insights into what's happening in the country's cyberspace during a major information security event." Solar, a Russian cyber security company, claims the majority of state-sponsored cyberattacks against Russia originate from North Korea and China. "*The findings are a surprise given the long-standing political partnership between Russia, China, and North Korea. ... As recently as last month Russia concluded additional agreements with both China and North Korea."* The hacking targets are "*spying and data theft from Russia's telecom and government services.*" Although unexpected, "*nation-state threat actors do have an incentive ... to have a heads up when an ally is about to go rogue or maintains relations with a state that is regarded as unfriendly."*[6]

Hamas vs Israel

9. 'Pro-Palestinian' hackers have claimed a couple of successes in the last couple of weeks. A hacking group named SiegedSec "*posted that they had allegedly compromised Israir Airlines and leaked the company's internal and confidential documents online."* ... Proof if the attack included "*a screenshot that looks like a dashboard of the Israir management platform containing multiple documents. ... another threat actor codenamed Abnaa AlSaada, possibly from Yemen, claimed that they took over control of aluminum manufacturing company Profal's operations."*[7] On Nov 23rd an attack was reported against the website hosting company Signature-IT. Approximately 40 companies had their e-commerce sites disabled. "*Among Signature's clients: Keter, Osem, Strauss, as well as government bodies such as the Nature & Parks Authority and the Ministry of Health."*[8] Other information about Signature-IT clients *may* have been compromised as well.

10. An Iranian-linked APT group, Agonizing Serpens also known as Agrius, appears to have reinforced and augmented an existing campaign against Israel's Education and Tech sectors. "*... they are investing great efforts and resources to attempt to bypass endpoint detection and response (EDR) and other security measures.*" Their goals are *assessed* as: "*first, stealing sensitive information that includes PII and intellectual property" ...* and second "*is wreaking havoc and inflicting considerable damage by wiping as many endpoints as possible."*[9]

11. According to the Director of the Israeli National Cyber Directorate (INCD), Gabi Portnoy, 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. "*Their objective is to turn cyberspace into an additional front."* The lack of success of these attacks is credited to the INCD's "*proactive cyber defensive approach*" and "*as well as the mobilization of the country's cyber security ecosystem."*[10]

5 Source: The Hacker News. Russian Cyber Espionage Group Deploys LitterDrifter USB Worm in Targeted Attacks

6 Source: The Record. Russian analysts point finger at China, North Korea over cyber activity

7 Source: cybernews. Hackers claim multiple attacks on Israel and leak confidential files

8 Source: Calcalistech.com . Dozens of Israeli retailers hit by cyberattack

9 Source: Palo Alto Networks, Unit 42. Agonizing Serpens (Aka Agrius) Targeting the Israeli Higher Education and Tech Sectors

12. Two Israeli defensive cyber campaigns have been identified. Israel's NSO Group, notorious for its creation of Pegasus spyware is one of a group of companies searching for any indication of the hostages and/ their captors. "*According to the NSO-linked source, several Israeli agencies are likely using Pegasus — a "zero-click" malware that can be snuck onto a target's device without them knowing — to help track people kidnapped by Hamas, as well as people who have gone missing during Hamas' attack last month.*"[11] According to cybersecurity experts who monitor the internet, the number of internet-connected honeypots in Israel, (lures for hackers), have risen dramatically. "*Most of the honeypots are pretending to be a wide range of products/services. They're not emulating specific devices as much as they're trying to catch any malicious activity happening across Israel.*"[12] Analysts Comment: Critical infrastructure and industrial control systems appear to be defended by other other efforts.

MOVEit! Hack Update

13. According to security shop Emsisoft, 2,620 organizations and more than 77 million individuals have had their data stolen by the Cl0p ransomware group via the MOVEit! hack. One of the more recent additions to the victim list is the antivirus business Avast. According to Avast the crooks accessed some "*low-risk customer personal information.*"[13] Other "*new additions come from healthcare platform Welltok, California's Medical Eye Services, and Medicaid contractor Maximus Federal Services. ... The data-stealing attacks began around May 27, when the Clop - aka Cl0p - ransomware group began exploiting a zero-day vulnerability, later designated CVE-2023-34362, in MOVEit secure file transfer software, built by Progress Software. On May 31, the Massachusetts-based vendor alerted users to the attack campaign and released a patch to fix the flaw.*"[14] It was too late.

14. The Kon Briefing, a count by KonBriefing Research, a company specializing in 'Information security, governance, risk management and compliance', has a lower count of 2588 organizations and 77.7 - 82.5 m individuals.[15] From a strategic vantage point the differences between the counts don't matter. The number of victim organizations and individuals continues to increase. Law Enforcement and national security organizations have not managed to penetrate the Cl0p ransomware organization to either shut it down and/or stop the ransomware payments. The Cl0p ransomware group continues to hack other, new targets.

---

10 Source: nationalinterest.org . The Cyberwarfare Front of the Israel-Gaza War
11 Source: Axios. Israel's NSO unleashes controversial spyware in Gaza conflict
12 Source: TechCrunch. Thousands of new honeypots deployed across Israel to catch hackers
13 Source: The Register. MOVEit victim count latest: 2.6K+ orgs hit, 77M+ people's data stolen
14 Source: govinfosecurity. Known MOVEit Attack Victim Count Reaches 2,618 Organizations
15 Source: KonBriefing. Number of known victims of the MOVEit attack so far: