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 2023. 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: (46) Multiple Russian Cyber Attacks Blocked

This report contains selected cyber-security information from 7th to 21st Dec 2023.

Synopsis

1. Russian hackers took Ukraine's largest telecommunications provider Kyivstar offline for more than a week. Reports revealed at least four other Russian cyber attacks against other countries. Ukraine hacked Russia's tax system. An Israeli hacker group shut down 70% of Iran's gas stations.

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. **Russia Attacks Ukrainian Telecommunications**. Oleksandr Fedienko, head of the Cybersecurity Subcommittee of the Verkhovna Rada's Committee on National Security and Defense, said "*Ukraine – that is, its telecom operator, Kyivstar – suffered one of the most powerful cyberattacks in Europe, that's for sure, in the entire history of all operators, which led to a temporary halt of all services,*". The hack was described as a "*massive technical failure. Communication and internet services became unavailable for customers across Ukraine.*"[1] The UK's Ministry of Defence said: "*Effects continued for at least 48 hours, impacting the company's mobile and data services. ... Kyivstar supplies over half of Ukraine's population with mobile and home internet services. The cyber-attack reportedly left users without mobile signal or the ability to use the internet. The cyber-attack also reportedly disrupted air raid sirens, some banks, ATMs, and point-of-sale terminals. At the same time, the Ukrainian bank Monobank was targeted with a distributed denial of service (DDoS) attack, disrupting access to the bank's website.*"[2]

4. Analysts Comment: No media we have seen have reported details of the attack. There is one report that an employee account was compromised, which could have

1 Source: Ukrinform. Cyberattack on Ukraine's telecom giant Kyivstar one of largest ever recorded in Europe
2 Source: the Guardian. Russia-Ukraine war: Ukraine hit by one of the worst cyber attacks of the war, says UK

provided the attackers with an entry point. Likewise few details of the attack have been provided. The Ukrinform report did say services were restored from backups. This *infers* that the attack was a destructive attack wiping software and possibly firmware on telecommunications devices.

5. Kyivstar company president Oleksandr Komarov has announced complete stabilization and the restoration of services.[3] The restoration timeline ran as follows:

- Morning of Tuesday Dec 12th: attack commenced.
- Evening Wed Dec 13th: Kyivstar began resuming voice communication services
- Dec 14th: Mobile Internet services began working
- Evening Dec 15th: full mobile Internet services restored
- Dec 17th: Voice communication services, including in roaming, mobile data transmission, Home Internet services, virtual private network (VPN) services and began restoring access to M2M (Machine-to-Machine) services for business clients restored.
- Dec 18th: Restored access to SMS services, including international roaming, as well as M2M

6. The attackers were a group of activist hackers, or "hacktivists", called Solntsepyok. The claim was made in a Telegram messaging app post. The claim included screenshots appearing to show that the hackers had accessed Kyivstar's servers. *"Solntsepyok said it destroyed more than 10,000 computers and 4,000 servers in the attack against Kyivstar, including its cloud storage and backup systems. ... Solntsepyok has been identified as a front for a Russian hacking group dubbed "Sandworm" which has been previously linked to the GRU."*[4] Analysts Comment: Although this attack caused telecommunications outages over two weeks, strategically it was a bust. Russia did not make significant ground gains during the outage period. Company backups restored critical data. Further, Ukraine CERT now has an update on Russia's cyber tools and methodologies.

7. **Other Russian Cyber Attacks**. Multiple Russian cyber attacks against the international community were unmasked during the reporting period.

- Microsoft identified a Russian APT known as: Star Blizzard, Seaborgium, BlueCharlie, Callisto Group, and Coldriver, and identified its most recent evasion tactics. The group is known for targeting NATO member countries in fields related to politics, defense such as NGOs, think tanks, journalists, academic institutions, intergovernmental organizations etc. "*Star Blizzard has started using password-protected PDF lure documents, or links to cloud-based file sharing platforms with the protected PDFs contained*

3 Source: Interfax-Ukraine. Kyivstar plans to achieve full stabilization in provision of services by end of week - company president

4 Source: Reuters. Hackers linked to Russian spy agency claim cyberattack on Ukrainian cell network

within. The passwords to these documents typically come packaged in the same phishing email, or an email sent shortly after the first." The group has several other new tricks including: "*using a domain name service (DNS) provider as a reverse proxy* ... and *using a more randomized domain generation algorithm (DGA), to make detecting patterns in its domains more cumbersome."*[5] The group is associated with the Russian FSB and "*has has actively sought to interfere with the political process in the UK and other nations for years."*[6]

- ATP 28 also known as ITG05, BlueDelta, Fancy Bear, Forest Blizzard (formerly Strontium), FROZENLAKE, Iron Twilight, Sednit, Sofacy, and TA422 has been observed using lures based on the ongoing Israel-Hamas war. Their intention is to install a backdoor called 'HeadLace'. "*The newly discovered campaign is directed against targets based in at least 13 nations worldwide and leverages authentic documents created by academic, finance and diplomatic centers, ... ITG05's infrastructure ensures only targets from a single specific country can receive the malware, indicating the highly targeted nature of the campaign. ... Targets of the campaign include Hungary, Türkiye, Australia, Poland, Belgium, Ukraine, Germany, Azerbaijan, Saudi Arabia, Kazakhstan, Italy, Latvia, and Romania."* The targets appear to be policy creators.[7]

- Russian-speaking Malware-as-a-Service (MaaS) groups, called BatLoader and FakeBat were detected launching attacks against 23 customers of eSentire. "*They ... created Google Ads and websites that mimic legitimate software sites to lure employees to download a very stealthy and capable malware loader. ... BatLoader and FakeBat crime groups are giving low-level threat actors access to end-to-end attack campaigns that produce pools of corporate victims."*[8]

- APT29, also tracked as BlueBravo, Cloaked Ursa, Cozy Bear, Midnight Blizzard (formerly Nobelium), and The Dukes, is known for its affiliation with Russian Foreign Intelligence Service (SVR). The group has been targeting "*unpatched JetBrains TeamCity servers in widespread attacks since September 2023.*" Once the group had gained network access "*they exploited the TeamCity CVE to escalate its privileges, move laterally, deploy additional backdoors, and take other steps to ensure persistent and long-term access to the compromised network environments, ... Targets of the campaign include an energy trade association; firms that provide software for billing, medical devices, customer care, employee monitoring, financial management, marketing, sales, and video games; as well as*

5 Source: Dark Reading. Russia's 'Star Blizzard' APT Upgrades Its Stealth, Only to Be Unmasked Again
6 Source: Tech Spot. Russian cyber-spies identified in APT attacks against UK democracy
7 Source: the Hacker News. Russian APT28 Hackers Targeting 13 Nations in Ongoing Cyber Espionage Campaign
8 Source: eSentire. Two Competing, Russian-Speaking Cybercrime Groups Attack Employees from 23 Companies in the Manufacturing, Software, Legal, Retail, and Healthcare Sectors Using Malicious Google Ads

hosting companies, tools manufacturers, and small and large IT enterprises. Microsoft revealed Russia's multi-pronged assault ... to penetrate networks, exfiltrate data, and deploy destructive malware such as SharpWipe (aka WalnutWipe).”[9]

8. **Ukraine Hacks Russian Taxation Service**. “*Ukraine cyber units broke into one of the “key well-protected central servers” of the Russian tax service as well as more than 2,300 regional servers throughout Russia and occupied Crimea. ... The state-sponsored hackers also hit a Russian tech company that operates the database of Russian Federal Taxation Service (FNS). ... They wiped the databases and backups.*”[10] Ukraine believes “*According to experts, the paralysis in the work of the Federal Tax Service of the Russian Federation will last at least a month. At the same time, the full reanimation of the tax system of the aggressor state is impossible.”*[11]

Hamas vs Israel

9. A pro-Israeli group called Predatory Sparrow claimed responsibility for disrupting services at about 70 percent of Iran's gas stations. A spokesperson insisted "*A software problem with the fuel system has been confirmed in some stations across the country and experts are currently fixing the issue.*" Predatory Sparrow has been accused by Iran of “*cyberattacks on Iranian railway systems and a steel plant.”*[12] The Times of Israel believes that the group is linked to the Israeli Military Intelligence Directorate. In an off-the-record briefing “*strongly hinted that the Military Intelligence’s Unit 8200 was responsible for the 2022 cyberattack on the Iranian steel plant.”*[13] Analysts Comment: We see this as an indicator that Israel’s cyber unit the ‘8200’ is coordinating Israel’s cyber warfare.

10. An Iranian state-sponsored hacker group known as ‘OilRig’ has deployed three new downloaders to maintain persistent access to Israeli victim organizations. The campaign targets “*an organization in the healthcare sector, a manufacturing company, and a local governmental organization.*“[14] Results are unknown. Analysts Comment: It is *highly probable* that Israel will counter ‘OilRig’ with ‘the 8200’. We *forecast* escalation in cyber attacks by OilRig and the 8200.

---

9 Source: the Hacker News. Russian SVR-Linked APT29 Targets JetBrains TeamCity Servers in Ongoing Attacks
10 Source: Security Affairs. Ukrainian military intelligence service hacked the Russian Federal Taxation Service
11 Source: Interfax-Ukraine. GUR says it has hacked servers of Russian tax service
12 Source: The Register. Hacktivists boast: We shut down Iran's gas pumps today
13 Source: Times of Israel. Israel-linked group claims cyberattack that shut down 70% of Iran’s gas stations
14 Source: the Hacker News. Iranian State-Sponsored OilRig Group Deploys 3 New Malware Downloaders