Cyber Center of Excellence

Unclassified Threat Read Book
16-31 January 2023

Prepared by: Threat Management Office
CCoE
Fort Gordon, GA 30905

POC: Threat Management Office, jeffrey.t.hardimon.civ@army.mil or
kevin.m.bird.civ@army.mil 706-849-9263/9266

Table of Content

Cyber

1. **Phishing attacks are getting scarily sophisticated. Here's what to watch out for (ZDNet, 31 JAN, Danny Palmer)**

   Phishing campaigns use fake social media profiles, in-depth research, and more to trick unsuspecting victims into clicking malicious links.

   Hackers are going to great lengths, including mimicking real people and creating and updating fake social media profiles, to trick victims into clicking phishing links and handing over usernames and passwords.

2. **Cyber warfare will only increase after end of Ukraine-Russia war, expert warns (The Jerusalem Post, 31 JAN, Yohah Jeremy Bob)**

   Nadav Zafrir spoke about what the world can expect to see in the future in terms of cyber warfare and threats at the Tel Aviv Cybertech Conference on Tuesday.

   If there is a resolution to the Russia-Ukraine war in 2023, countries worldwide can expect to see cyber warfare become worse, not better, former IDF intelligence Unit 8200 chief and Team8 Co-Founder and CEO Nadav Zafrir said on Tuesday.

   "Cyber as part of the toolkit will become the main tool and we will see more threats, not less," he explained at the Cybertech conference in Tel Aviv.

   The former IDF cyber intelligence chief also said sarcastically that the world is "almost celebrating a year of war in Ukraine. A year ago, no one would believe we would have a global war in Ukraine that looks like World War."

3. **Dark Covenant 2.0: Cybercrime, the Russian State, and the War in Ukraine (Recorded Future, 31 JAN, Insikt Group)**

   Editor's Note: This is an excerpt of a full report. To read the entire analysis with endnotes, click here to download the report as a PDF.

   This report examines the unspoken connections between the Russian Federation, cybercriminals, and self-described hacktivists in Russia and Eastern Europe in the context of the Russian war in Ukraine. It is a direct continuation of the findings presented in our 2021 report "Dark Covenant: Connections Between the Russian State and Criminal Actors". This report will be of interest to threat researchers, as well as law enforcement, government, and defense organizations.

4. **These Russian and Iranian hackers are fooling vital industries (Tech RADAR, 26 JAN, Lewis Maddison)**

   The UK's National Cyber Security Centre (NCSC) has issued a warning over the continual cyberattacks perpetrated by Russian and Iranian hacker groups.

   Its report says SEABORGIUM (AKA: Callisto Group/TA446/COLDRIVER/TAG-53) and TA453 (AKA: APT42/Charming Kitten/Yellow Garuda/ITG18) are using spear-phishing techniques to target institutions and individuals with the aim of gathering intel.

5. **Russia and Iran are stepping up cyber spying on politicians and activists, warns GCHQ (The Telegraph, 26 JAN, Gareth Corfield)**

   State-sponsored hackers have been targeting prominent Britons in 'espionage campaign'

   Russian and Iranian hacker gangs are stepping up an espionage campaign targeting British politicians, officials and activists, GCHQ has warned.

   State-sponsored hackers from both nations have been targeting prominent Britons in an "espionage campaign" to steal sensitive information about British foreign policy, GCHQ's the National Cyber Security Centre warned on Thursday.

6. **Chinese Group Targeting Vulnerable Cloud Providers, Apps (GOV Info Security, Prajeet Nair, 21 JAN)**

   Cybersecurity researchers say a Chinese for-profit threat group tracked as 8220 Gang is targeting cloud providers and poorly secured applications with a custom-built crypto miner and IRC bot.

7. **Cybersecurity in 2023: Russian escalation, Chinese espionage, Iranian "hacktivism" (Help Net Security, 18 JAN, Mike McLellan)**

   In 2022, state-sponsored cyber activity has been drawn into sharp focus, ransomware continued to dominate as the primary threat facing organizations, and there have been several highly publicized incidents. Beyond the headlines, there have been some interesting shifts in both tools and tactics of cyber adversaries.

8. **British and Ukrainian cyber officials meet in London for threat intelligence talks (The Record, 18 JAN, Alexander Martin)**

   Senior cybersecurity officials from the United Kingdom and Ukraine met for several hours on Wednesday to discuss threat intelligence relating to Russian cyberattacks.

   The bilateral talks between National Cyber Security Centre (NCSC) staff and a delegation from Ukraine's State Service of Special Communications and Information Protection (SSSCIP) and its Computer Emergency Response Team (CERT-UA) covered the latest developments in the conflict, although the substance of the meetings was not disclosed.

Electronic Warfare

1. **Russian state defense conglomerate skirts sanctions to buy electronic warfare equipment in the West to use in Ukraine (Meduza, 27 JAN)**

   Russian investigative outlet Important Stories reports that Rostec, a Russian state-owned defense conglomerate, has been buying electronic warfare components from the U.S., which it then uses against the Ukrainian Army.

Information Advantage

1. **[How Russia is molding the minds of schoolkids to support its brutal invasion of Ukraine] (Insider, 29 JAN, Elise Morton)**

   Russia is targeting schoolkids with propaganda meant to underpin its invasion of Ukraine, preparing children as young as 7 to be ready to die for their country.

   The campaign takes the form of compulsory patriotic lessons, rolled out by the Kremlin in late 2022.

   Officials uploaded a slew of approved lesson plans and talking points to a government website, which Insider reviewed and translated.

   Although clearly a response to the invasion of Ukraine, the materials avoid naming the conflict and instead take a more subtle route.

2. **[Ukraine War: Russia's Military 'Spreading Misinformation' About Its Attacks, UK Says] (Huffington Post, 27 JAN, Kate Nicholson)**

   Russia could be “deliberately spreading misinformation” to suggest its efforts in the Ukraine war are “sustaining momentum”, UK intelligence has said.

   Moscow struggled to make any real gains over the autumn, especially as Kyiv’s successful counteroffensive saw troops reclaim vast areas of Ukrainian land from Russia in the east.

   Russia did manage to seize Soledar recently, a small town in the Donbas region, after a period of intense and bloody battle.

   The Ukrainian government only confirmed it this week though, while Russian forces had been claiming victory over the area for some time.

   Now the UK’s Ministry of Defence has suggested that the Kremlin has been “deliberately” putting out misleading details about other parts of the war, too.

3. **[Google: Influence Operator Dragonbridge Floods Social Media in Sprawling Cyber Campaign] (DARKReading, 27 JAN, Nathan Eddy)**

   Google has mounted a massive takedown, but Dragonbridge's extensive capabilities for generating and distributing vast amounts of largely spammy content calls into question the motivation behind the group.

   Google's Threat Analysis Group (TAG) spent 2022 working to disrupt the online presence of pro-Chinese influence operation (IO) Dragonbridge (aka Spamoflage Dragon) in 2022, wiping out more than 50,000 instances of activity across Twitter, YouTube, Blogger, and other channels.

4. **[Russian Disinformation Keeps Ukraine and Allies Guessing] (Globely News, 21 JAN, Stefan Wolff)**

   Russian disinformation seeks to convince its public that the war is winnable and distract Ukraine and its Western allies.

   During a recent visit to St Petersburg, Russian President Vladimir Putin reiterated his confidence in his country’s victory over Ukraine. Visiting a defense contractor, he also

took the opportunity to reassure workers that his so-called “special military operation” was in defense of ethnic Russians and Russian speakers in Ukraine against a “neo-Nazi regime” in Kyiv. In other words, Russia is acting in the tradition of the “great patriotic war” that saved Europe from Nazi Germany.

5. **How China funds foreign influence campaigns (Medium, 12 JAN, Digital Forensic Research Lab)**

CCP financial statements reveal details of influence operations, from news programming to documentaries to feature films

A review of financial records for Chinese Communist Party (CCP) organizations with foreign influence capabilities reveals that funding for propaganda activities in China is largely project based, with most of the financing comes from public funds. CCP organizations release public financial reports that can be analyzed to understand China’s priorities when it comes to information operations. The DFRLab dissected the financials of two Chinese media organizations and two municipal-level CCP departments to reveal insights into the funding of foreign influence campaigns. Our examination included the financial records for Xinhua News Agency, China Media Group (CMG), the Beijing United Front Work Department (UFWD), and the Beijing Propaganda Department.

Signal

1. **Satellite billed as the 'future GPS' begins key tests (Space News, 27 JAN, Sandra Erwin)**

   L3Harris announced Jan. 26 it delivered the Navigation Technology Satellite-3 (NTS-3) to the U.S. Air Force and the spacecraft is now undergoing final tests in preparation for a planned launch in late 2023.

   NTS-3 is an experiment funded by the Air Force Research Laboratory that will broadcast positioning, navigation and timing (PNT) signals from geostationary Earth orbit. The goal is to demonstrate next-generation PNT technologies for the U.S. military and provide an alternative to GPS.

   The satellite is now going through a series of tests at Kirtland Air Force Base, New Mexico, and will soon head to the Air Force's Benefield Anechoic Facility at Edwards Air Force Base, California, for radio frequency testing.

2. **Over 19,000 End-of-life Cisco VPN Routers Open for RCE Attacks (Cybersecurity News, 23 DEC, Erik Keith)**

   Censys recently reported that there are 19,500 end-of-life Cisco VPN routers being used by individuals and small businesses on the internet that may be at risk of being targeted by a new attack.

   Using a combination of the two vulnerabilities mentioned below, threat actors have been able to evade authentication processes and execute arbitrary commands on Cisco Small Business routers based on the underlying operating system:-

   - CVE-2023-20025
   - CVE-2023-2002

Items of Interest

1. **Russia-Ukraine Situation Report, (U.S. Army Asian Studies Detachment)**

   These reports are a compilation of articles from Russia, Ukraine, and other nations regarding the current tensions between Russia and Ukraine. Topics covered in this report include the following:

   - Foreign Observations and Reactions
   - Social Media Highlights
   - Russian Eastern Military District Movements
   - Other Topics

   Russia-Ukraine Situation Report, 31 January 2023
   Russia-Ukraine Situation Report, 30 January 2023
   Russia-Ukraine Situation Report, 27 January 2023
   Russia-Ukraine Situation Report, 26 January 2023
   Russia-Ukraine Situation Report, 25 January 2023
   Russia-Ukraine Situation Report, 24 January 2023
   Russia-Ukraine Situation Report, 23 January 2023
   Russia-Ukraine Situation Report, 20 January 2023
   Russia-Ukraine Situation Report, 19 January 2023
   Russia-Ukraine Situation Report, 18 January 2023
   Russia-Ukraine Situation Report, 17 January 2023

2. **Doctor Paid $60,000 in Bitcoin to Hire Dark Web Hitmen (Cybersecurity News, 31 JAN, Balaji N)**

   A former neonatologist received an 8-year prison sentence and was mandated to pay over $25,000 in compensation, along with a $100,000 fine.

3. **Facing Drone Strikes, Iran Warns Any U.S. Military Action Means War (Newsweek, 30 JAN, Tom O'Connor)'**

   In the wake of a drone strike against at least one defense factory in the central city of Isfahan, Iranian officials told Newsweek that any military option pursued by the United States against the Islamic Republic would result in all-out conflict with regionwide ramifications.

   While the U.S. military has denied any role in the attack that took place late Saturday, local time, unnamed U.S. officials cited in major outlets such as The Wall Street Journal and The New York Times have placed the blame on Israel, a U.S. ally and Iran's top foe, which has neither accepted nor denied involvement. No other entity has come forward with claims of responsibility.

4. **Ukrainian troops are calling the US military in the middle of shootouts with Russia for help fixing their artillery (Insider, 30 JAN, Jake Epstein)**

   As Ukrainian troops push their Western artillery to the limits, and sometimes past them, while fighting off Russian forces, the US military is helping to repair broken down pieces over the phone and through video chats.

5. **Entire US "no fly list" leaked online after being left on an unsecured server (Tech RADAR, 23 JAN, Craig Hale)**

   The entire of the US "No Fly List" has been exposed online by a Swiss hacker who reportedly found three sensitive files stored on an unsecure cloud storage server.

   One of the files contains the information of more than 1.5 million entries into the list, which covers individuals who have been barred from travelling to or from the US.

   The data was found out of boredom, according to a blog post(opens in new tab) written by the hacker, known online as maia arson crimew, which saw her searching Shodan for exposed Jenkins servers.

6. **PayPal Data Breach – Thousands of Users Accounts Compromised (Cybersecurity News, 20 JAN, Guru)**

   The unauthorized parties used login credentials to access PayPal user accounts, according to a PayPal notification of a security incident.

   Between December 6 and December 8, 2022, hackers gained unauthorized access to the accounts of thousands of individuals. A total of 34,942 accounts were reportedly accessed by threat actors employing a ‘credential stuffing attack’.

7. **The West Has Banned the Sale of Components for Weapons Production to Russia. But Russia Is Still Buying Them (Important Stories, 15 DEC, Maria Zholobova, Stephen Grey, Maurice Tamman)**

   During the course of Russia’s war on Ukraine, Western companies have supplied Russia with components to produce Orlan drones that help kill Ukrainians. An investigation by IStories, Reuters and the Royal United Services Institute.

   Throughout Russia’s war on Ukraine, going on almost a year, the company manufacturing Russian drones has been receiving components from Western companies. The Orlan-10, a modern Russian drone, is powered by foreign microelectronics. Its manufacturer, the “Special Technology Center,” is under sanctions, so it can’t purchase components itself. But IStories, Reuters and the Royal United Services Institute (RUSI) have uncovered that intermediaries in the U.S., China and Russia are helping the country get around the restrictions.