Severity

High

Analysis Summary

The cybersecurity authorities of the United States, Canada, Australia, United Kingdom, and New Zealand have released a joint CSA (Cybersecurity Advisory). The advisory is against Russia's continuous cyber attacks against Ukraine in an attempt to completely invade it. This has also opened up doors for Russian cybercriminals to attack what they deem "Enemies" of Russia. Countries allying with Ukraine and sanctioning the actions by Russia are at high risk of attacks too. These attacks also include DDoS, Ransomware, and deployment of malicious software for information theft. Cyber threat actors from the following Russian government and military organizations have conducted malicious cyber operations against IT and/or OT networks:

- The Russian Federal Security Service (FSB), including FSB's Center 16 and Center 18
- Russian Foreign Intelligence Service (SVR)
- Russian General Staff Main Intelligence Directorate (GRU), 85th Main Special Service Center (GTsSS)
- GRU's Main Center for Special Technologies (GTsST)
- Russian Ministry of Defense, Central Scientific Institute of Chemistry and Mechanics (TsNIIKhM)

Some of the Threat actors to look out for are:

APT29

APT29 is linked to Russia's Foreign Intelligence Service (SVR). They have been targeting government networks in Europe and NATO member nations, research institutes, and think tanks since at least 2008. APT29 focuses on a single target, launching a payload in the first stage that investigates the area while establishing persistence. Also, the notorious Solar Wind attacks in 2020 were carried out by this group. In 2014, the APT29 group attacked commercial and government enterprises in Germany, Uzbekistan, South Korea, and the United States, including the US State Department and the White House.

They have also attacked many vaccine manufacturers in an attempt to undermine the Coronavirus pandemic response process. APT29 is also known as Nobelium, Dukes, Cozy Duke, EuroAPT, CozyBear, CozyCar, Office Monkeys, SeaDuke, Hammer Toss, Iron Hemlock, and Grizzly Steppe.

APT28

APT28 is one of Russia's longest-running APTs and its operations date back to at least 2007. The group supports Russia in their strategic operations against the U.S, countries of the former Soviet Union, Europe, and now Asia. These attacks mostly involve cyber crimes against the defense and military of targeted countries. To support Russia's national interests, APT28 compromises the targeted country's operation, steals their data, and then leaks it to their government.

Going by the aliases Fancy Bear, Pawn Storm, Tsar Team, STRONTIUM, and Sofacy Group, APT28 performs their attacks using a spoofed website and phishing emails containing malicious links.

Recently, APT 28 (allegedly) has attacked Eastern European countries using Empire and Invoke-Obfuscation. The MSHTML Remote Code Execution vulnerability, CVE-2021-40444, is being used by their threat actors.

Gamaredon

Gamaredon is a Russia-backed advanced persistent threat (APT) that has been operating since at least 2013. The main goal of this APT is to use the malicious document to gain control of the target machine. The exploit document uses the template injection technique to infect the victim's computer with further malware. When the document is opened, it connects to the hacker's server and downloads the payload file. Gamaredon's tools are simple and designed to collect sensitive information from hacked systems and propagate it further. Its information-gathering efforts are nearly comparable to those of a second-tier APT, whose primary purpose is to collect and disseminate information with their units.

Conti Ransomware

Conti ransomware was discovered in December 2019 and is delivered via TrickBot. It's been utilized against large companies and government institutions across the world, especially in North America. Conti steals important files and information from targeted networks and threatens to

disseminate it unless the ransom is paid. Conti ransomware enhances performance by utilizing “up to 32 simultaneous encryption operations,” and is very likely directly controlled by its controllers. This ransomware can target network-based resources while ignoring local files. This feature has the noticeable impact of being able to create targeted harm in an environment in a way that might hinder incident response actions.

SmokeLoader

SmokeLoader — a malicious bot application — can be used to load additional malware. SmokeLoader has been spotted in the wild since 2011, carrying a variety of payloads. This malware is mostly used to load additional malicious software, which is often obtained from a third-party source. SmokeLoader can load its modules allowing it to do several activities without the use of additional components. To date, the supplier of Smokeloader, who goes by the alias SmokeLdr, is still active in delivering this malware as a service. It is well-known for using deception and self-defense. This malware can be spread in several ways and is widely linked to criminal activity. To hide its C2 activity, this malware sends queries to popular websites like microsoft.com, bing.com, adobe.com, and others.

Impact

- Information Theft and Cyber Espionage
- System Compromise
- Exposure of Sensitive Data
- Unauthorized Access

Remediation

- Logging — Log your eCommerce environment’s network activity and web server activity.
- Passwords — Ensure that general security policies are employed including: implementing strong passwords, correct configurations, and proper administration security policies.
- Admin Access — limit access to administrative accounts and portals to only relevant personnel and make sure they are not publicly accessible.
- WAF — Web defacement must be stopped at the web application level. Therefore, set up a Web Application Firewall with rules to block suspicious and malicious requests.
- Patch — Patch and upgrade any platforms and software timely and make it into a standard security policy. Prioritize patching known exploited vulnerabilities and zero-days.
- Secure Coding — Along with network and system hardening, code hardening should be implemented within the organization so that their websites and software are secure. Use testing tools to detect any vulnerabilities in the deployed codes.
- 2FA — Enable two-factor authentication.
- Antivirus — Enable antivirus and anti-malware software and update signature definitions in a timely manner. Using a multi-layered protection is necessary to secure vulnerable assets