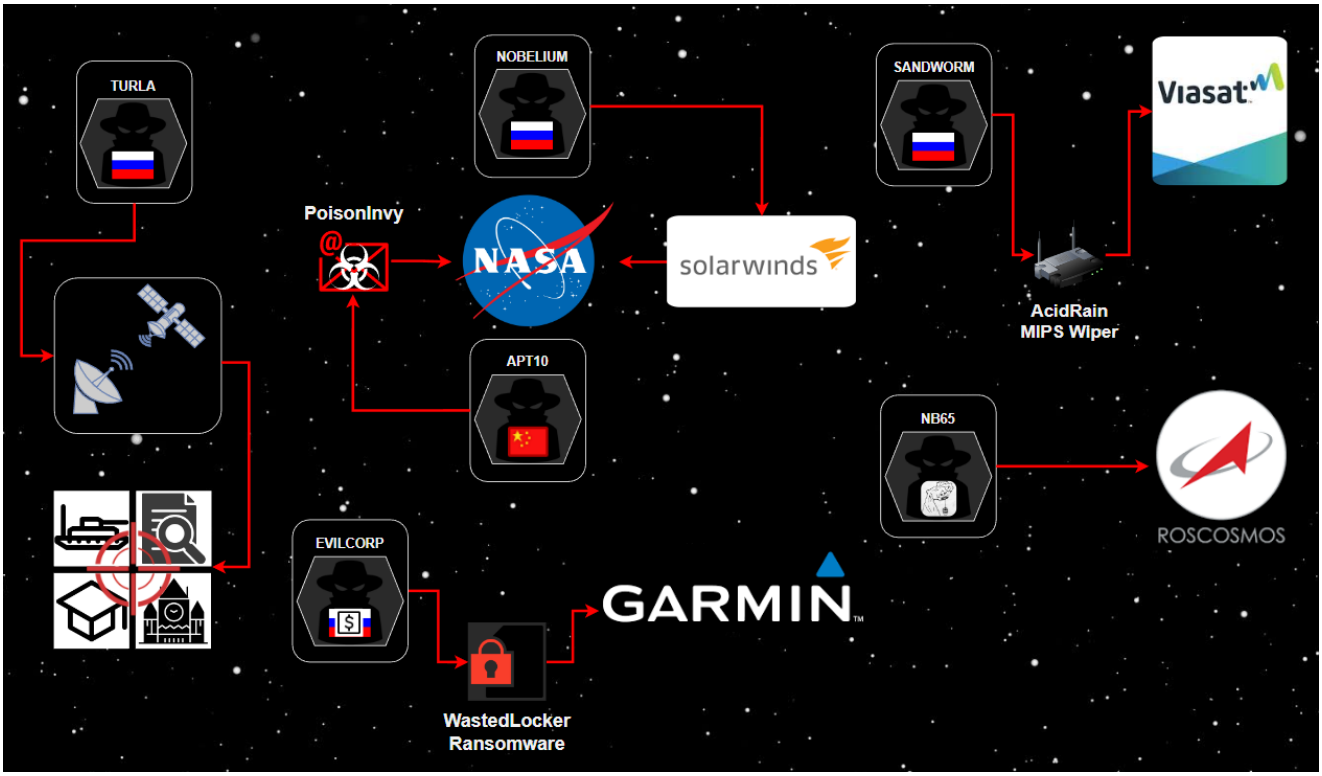
Space Invaders: Cyber Threats That Are Out Of This World

blog.bushidotoken.net/2022/07/space-invaders-cyber-threats-that-are.html

BushidoToken



Background

Destructive cyberattacks and digital espionage campaigns targeting international space programs is a growing and concerning trend. Some of the most significant cyberattacks over the last five years have been turning points in the state of cybersecurity of international space programs and organizations with satellite infrastructure in space.

Space exploration and the significance of having satellite infrastructure in space is a key driver of scientific research and technological innovation. However, despite receiving billions of dollars in funding, the digital infrastructure and information systems supporting space programs have been impacted by significant cyberattacks from nation-state threat actors and financially motivated cybercriminal groups. This blog aims to use open source intelligence (OSINT) research to compile and highlight significant cybersecurity incidents impacting the space industry that defenders should consider when securing these types of environments.

There have been a number of positive and landmark headlines recently, such as the successful launches by SpaceX, BlueOrigin, and Boeing, SpaceX providing critical communications infrastructure to Ukraine via Starlink, and the creation of the Space Force and Space ISAC. Space is also rarely able to escape geopolitical tensions and, as such, the Russian mission announced it was pulling out of the International Space Station (ISS), which has had its share of cybersecurity issues in the past.

In 2008, prior to when the ISS switched to Linux from Windows XP, Russian cosmonauts reportedly introduced an infected USB device to the computers aboard the space station. The Windows XP-based laptops used by the astronauts on the ISS were infected with a virus called W32.Gammima.AG, a malicious password-swiping computer virus. Not many technical details about the event and the impact it had on the station's computers were reported publicly. National Aeronautics and Space Administration (NASA) officials at the time described the virus as a "nuisance." Adding that it is "not a frequent occurrence, but this isn't the first time."

Digital Espionage in Space: Satellites and NASA

Satellite Turla

Satellite communications (SATCOM) can provide both TV broadcasting and access to the internet to remote locations. This type of satellite-based internet access, however, is known as downstream-only connection. In September 2015, Kaspersky Labs disclosed that a Russia-based advanced persistent threat (APT) group called Turla (aka Snake or VenomousBear) exploited weaknesses in these downstream-only satellite internet connections. Turla would monitor downstream connections, identify active IP addresses, select one to appear as the originating source IP during intrusions, and hijack it by hiding malicious code within packets sent to and from the satellite. Systems compromised by Turla would also then exfiltrate data to IP addresses of regular satellite-based internet users. Turla used this special technique to target systems of governments, embassies, military entities, educational institutions, research organizations, and pharmaceutical firms across the Middle East and Africa. Turla's operations have been tied to the Russian Federal Security Service (FSB) by Estonian intelligence services. In February 2022, German investigative reporters disclosed the identities of two Turla developers and their ties to the Russian FSB.

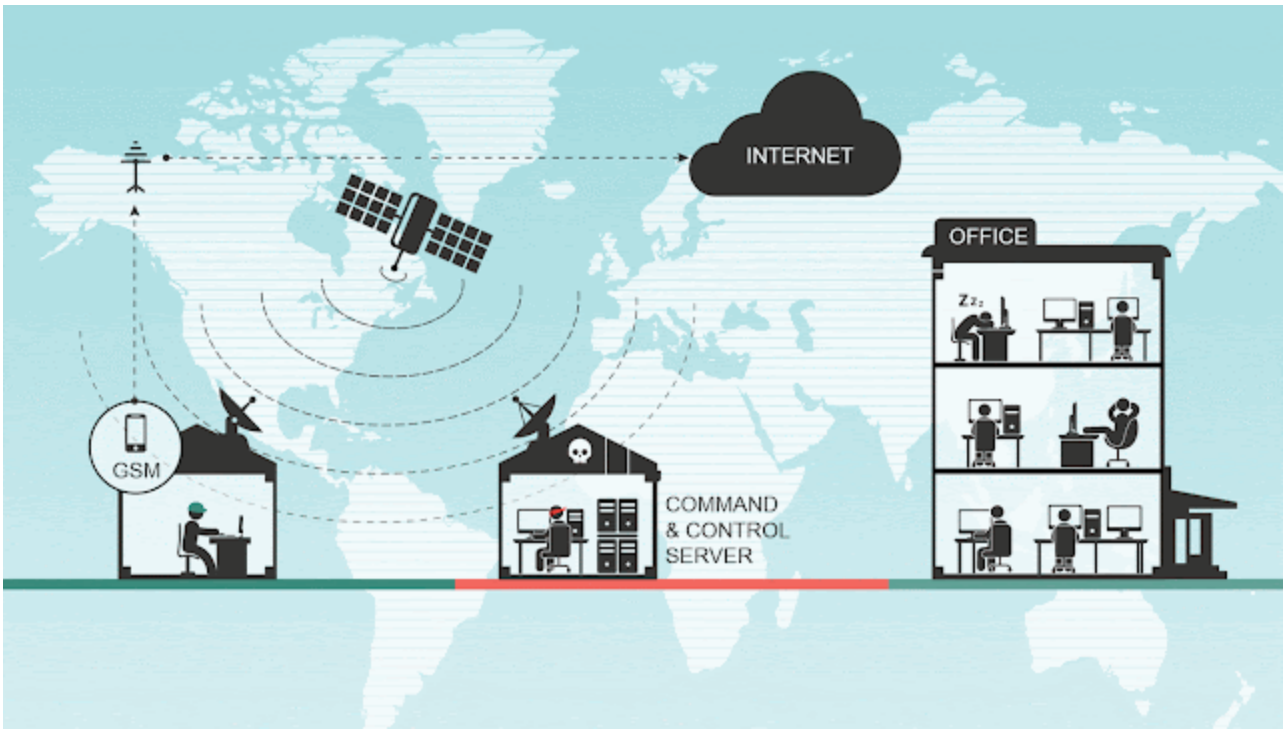


Figure 1: Satellite Turla hijacking attack explanation (Source: Kaspersky)

NASA & Chinese Technology Theft

In December 2018, the US Department of Justice charged two Chinese nationals part of APT10 (aka menuPass, StonePanda or POTASSIUM) that conducted a 12-year, Chinese Ministry of State Security (MSS) global hacking spree that stole data from dozens of US companies and government agencies in a sophisticated technology theft campaign. Two of the victims who had hundreds of gigabytes of sensitive data and information stolen included the NASA Goddard Space Center and the NASA Jet Propulsion Laboratory. The APT10 operators were able to use spear-phishing attachments) to deploy the PoisonIvy malware onto the victim's computers. The emails used malicious document attachments and sender addresses of legitimate but compromised accounts. Once installed, PoisonIvy records user keystrokes to steal credentials and could collect relevant files and other information from infected systems. Collected files were then added to encrypted archives and exfiltrated to remote servers owned by APT10.

Figure 2: APT10 members on Cyber Most Wanted list (Source: FBI)

NASA & The SolarWinds Supply Chain Attack

NASA was also more recently a victim of sophisticated Russian cyber-espionage campaigns. In December 2020, the SolarWinds supply chain attack linked to the Nobelium APT group (aka APT29, CozyBear, or DarkHalo) was disclosed. It involved a malicious software update for SolarWinds Orion platform that was downloaded by over 18,000 SolarWinds customers. Nobelium had managed to compromise the SolarWinds software build environment and used a custom implant called SUNSPOT to load the SUNBURST backdoor into the Orion software update. The intrusion reportedly began in September 2019 and had a first attempt in October 2019 when test code was added and pushed to SolarWinds customers. To make it harder to detect, SUNBURST's code was signed using stolen certificates from the Orion platform and it same naming conventions as Orion's code so SolarWinds developers would mistake it for their own. Once installed, SUNBURST would sleep for 12-14 days before it contacted the group's C&C domain via DNS. SUNBURST's traffic also used the Orion Improvement Program (OIP) protocol to blend in with legitimate SolarWinds activity. Nobelium would then use SUNBURST to deploy additional malware, such as TEARDROP, RAINDROP, and several others. According to the US National Security Agency (NSA) statement, around 100 nongovernment entities received follow-up activity, which included several US federal government agencies and NASA. In January 2021, the US Office of the Director of National Intelligence (ODNI) formally stated that the attack was orchestrated by the Russian Foreign Intelligence Service (SVR).

Analysis: So What?

- Although space exploration and research involves a lot of collaboration between international space agencies, these intelligence agencies operate outside of and ignore these agreements.

- These types of digital espionage campaigns are orchestrated by threat actors operating on behalf of nation-state intelligence agencies. To be able to utilize these techniques, it requires vast resources, technically skilled researchers, and disciplined operators.
- Turla, APT10, and Nobelium are the very definition of advanced persistent threats. These groups operate constantly and stop and nothing to execute intelligence gathering campaigns and intellectual property theft.
- These types of campaigns are essentially the cyber version of traditional spying that will always happen between nation-state rivals. It is difficult to call these types of intrusions "attacks" because there were no destructive components. However, the information collected in these cyber-espionage campaigns may support future destructive offensive operations.

Destructive Cyberattacks affecting Space

".garminwasted"

Cyberattacks degrading the performance of IT systems and networks are more likely to originate from cybercriminal threat groups than nation-state APTs. In late July 2020, Garmin, a major manufacturer of navigation equipment - used by NASA's Ingenuity Mars Helicopter - and smart devices was the victim of a WastedLocker ransomware. Garmin's cloud services, including device syncing and geopositioning instruments used by pilots, were disabled as a result. In its official statement, Garmin confirmed that it was the victim of the cyberattack that interrupted online services and encrypted some internal systems. Garmin reported that there was no evidence anyone gained unauthorized access to user data during the incident. An anonymous Garmin employee familiar with the incident told *BleepingComputer* that the ransom demand was $10 million. After a four-day global service outage, Garmin suddenly announced that they were starting to restore services after paying the ransom to the cybercriminals to receive a decryptor. Notably, WastedLocker has been attributed to EvilCorp via its similarities to DoppelPaymer and BitPaymer, other ransomware families developed by the eCrime threat group. In December 2019, EvilCorp was placed on the US OFAC sanctions list for causing $100 million in financial damages. Therefore, paying the ransom to EvilCorp could lead to heft fines from the US government.

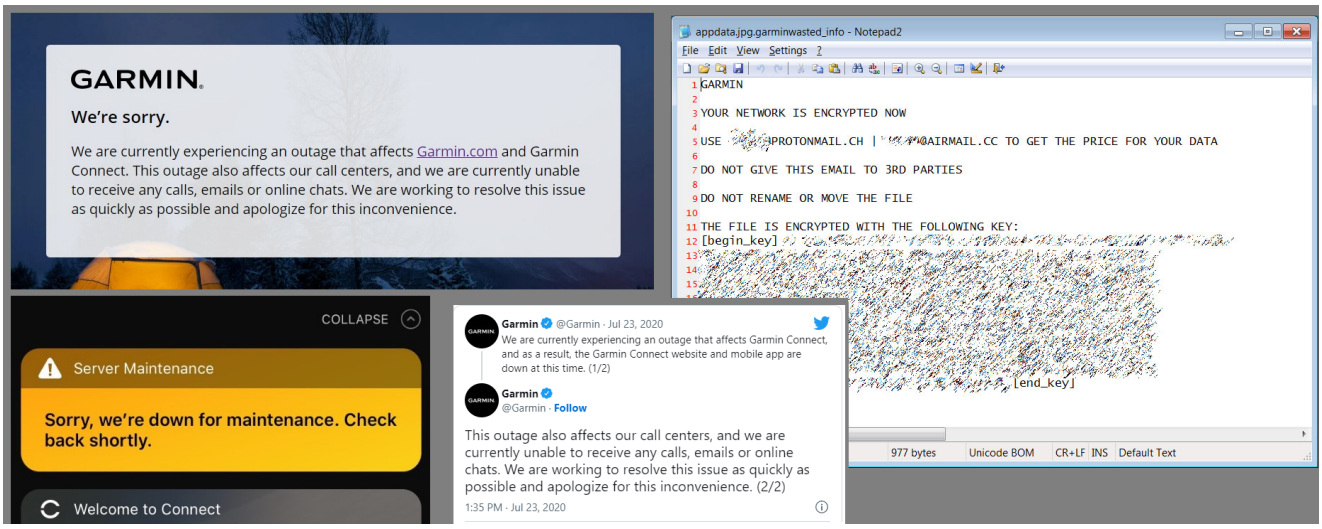


Figure 3: Garmin outage notices and WastedLocker ransom note (Source: BleepingComputer)

World's First SATCOM Attack

One of the most destructive cyberattacks in space was against Europe's SATCOM networks on the night of Russian invasion of Ukraine. The US and EU stated that on 24 February 2022, Russia launched cyberattacks against commercial satellite communications networks known as KA-SAT, belonging to Viasat. The cyberattack was aimed to disrupt the Ukrainian command and control operations, and resulted in significant spillover impacts into other European countries, including Germany, Greece, Poland, Italy, and Hungary. Broadband services took over one month to recover from the incident. According to Viasat, tens of thousands of SATCOM modems were destroyed as a result and had to be replaced. The adversaries were reportedly able to gain access via exploiting a "misconfigured VPN" and moved laterally to the management segment of the KA-SAT network. From there, the attackers executed commands to flash the memory of the modems, rendering them unusable. Interestingly, researchers from cybersecurity vendor SentinelOne uncovered a wiper malware called AcidRain designed for MIPS firmware used by the SATCOM modems that was potentially used in the KA-SAT attack. SentinelOne researchers assess with medium confidence that AcidRain was developed by the same malware authors as VPNFilter, which was officially attributed to the Russian Main Intelligence Directorate (GRU), more specifically GTsST Unit 74455, most well-known as the Sandworm Team.

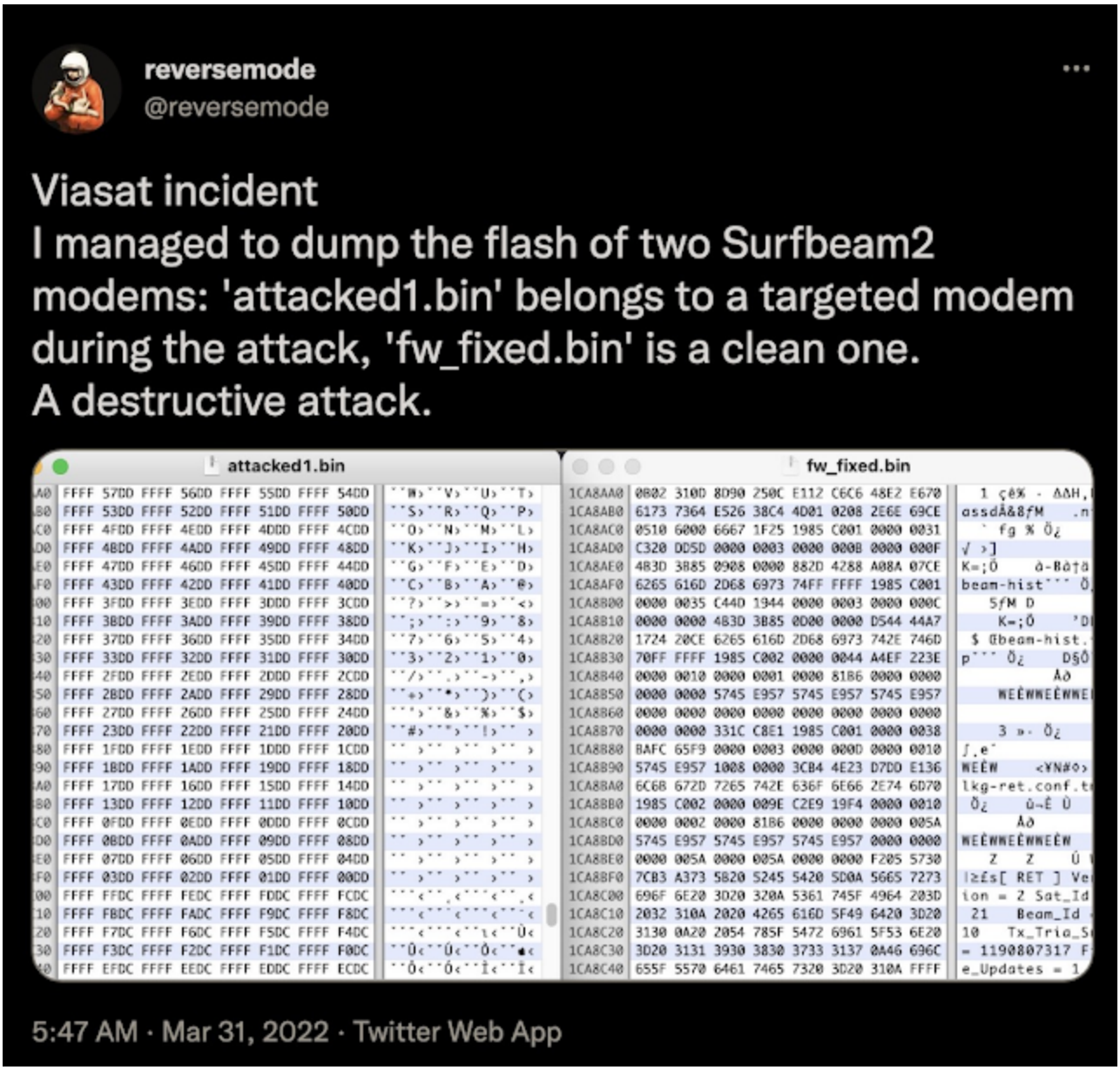


Figure 4: Side-by-side analysis of attacked KA-SAT modems (Source: reversemode)

Russian Space Agencies Attacked By Hacktivists

State-sponsored APT groups and organized cybercriminals are not the only perpetrators of destructive cyberattacks against the space industry. In March 2022, a pro-Ukraine hacktivist group known as Network Battalion 65 (aka NB65) shared via Twitter that it had launched an attack on Roscosmos, Russia's space agency. Dmitry Rogozin, director general of Roscosmos, later Tweeted that NB65's claims were "not true" and called them "scammers and petty swindlers." However, the screenshots shared by NB65 allegedly belong to Russian satellite imaging software and vehicle monitoring systems. The incident at Roscosmos was ultimately denied by officials and unconfirmed by NB65. Also in March, a Twitter account allegedly tied to the Anonymous collective shared that another hacktivist group known as v0g3lSec defaced a website belonging to Russia's Space Research Institute (IKI) and leaked files that allegedly belong to the Russian space agency Roscosmos. One of the stolen documents discusses the location of potential landing sites for lunar spacecraft on the

Moon's South Pole. This matches with what Russian authorities have already announced their South Pole sites, which potentially increases the likelihood that these documents were successfully stolen.

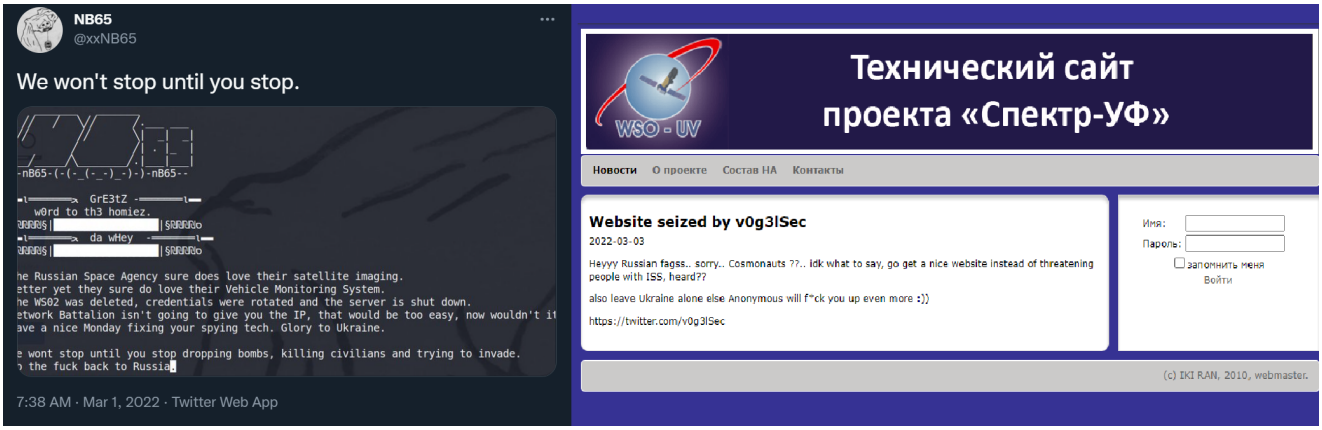


Figure 5: NB65 and v0g3lSec attacked Russian Space Agencies (Source: Vice)

Analysis: So What?

- Although uncommon, purely destructive cyberattacks are often the most feared. The loss of data and access to systems can cause millions of dollars of damage to an organization and set back operations for months or years. The most destructive attacks often include data encrypting ransomware or data destroying wipers.
- Russia has been one of the main sources of destructive cyberattacks globally. Leading up to and during the invasion of Ukraine, Russian APT groups have deployed several data wiping malware variants against Ukrainian government entities and Ukrainian critical infrastructure organizations.
- Offensive cyber operations perpetrated by the Sandworm Team are some of the most dangerous in the world. It is one of the few APT groups that has successfully launched multiple cyberattacks that had destructive kinetic affects, mostly against Ukraine.

Courses of Action

Cybersecurity experts have often warned that Russian offensive cyber operations treat Ukraine like a sandbox, in that new attack types are often tested and proven in the region first. Therefore, it can be deemed vital for cyber threat intelligence analysts to monitor the threat landscape in Ukraine to capture the tactics, techniques, and procedures (TTPs) leveraged by Russian APTs before they are deployed elsewhere globally.

The adversaries targeting space organizations and satellite networks are some of the most advanced in the wild. This includes highly well-resourced intelligence agencies operating on behalf of Russia and China, as well as agencies from hostile states such as Iran and North Korea. It is therefore important to recruit and cultivate skilled cybersecurity practitioners to compete with the adversaries and direct investment into technologies to prevent sophisticated attacks.

A lot of the focus has been on nation-state and cybercriminal threat groups, but more focus should be on hacktivists groups that can also cause significant reputational damage to any organization. Unlike nation-states that usually try to covertly gain and maintain access or cybercriminals who look to monetise their access, hacktivists seek to embarrass an organization by defacing websites, shutting down websites by DDoS attacks, or hack-and-leak operations to spread unsavoury information publicly. State-backed threat actors have also adopted hacktivists tactics due to the ability to generate headlines with the aim of embarrassing their geopolitical opposition.

The threat model for the space industry is very different for many other verticals. The attack surface involves a lot of advanced technology, such as SATCOM networks, that modern vendors are not suited to protect and requires custom solutions. One main example of this is that endpoint security for Internet-of-Things (IoT) devices is not currently anywhere near the level that modern workstations have available. This makes this an area that is woefully underprepared for nation-state advanced persistent threat groups that are going undetected and waiting for the time to strike.

Lessons from the Conti Leaks

Overview of Russian GRU and SVR Cyberespionage Campaigns 1H 2022

How Do You Run A Cybercrime Gang?