



DECEMBER 2021

RANSOMWARE WEAPONIZED

Nation States, Cryptocurrencies, and Great Power Competition

Authored By:

Drew Spaniel, Lead Researcher, ICIT

Contributors:

Parham Eftekhari, Chairman, ICIT and Senior Vice President and Executive Director, the Cybersecurity Collaborative

Stan Mierzwa, ICIT Fellow & Director and Adjunct Professor, Center for Cybersecurity, Kean University

Laura Whitt-Winyard, ICIT Fellow & Global CISO, DLL

Joyce Hunter, Executive Director, ICIT & Former Deputy CIO for Policy & Planning, USDA

ICIT Research Publication

Ransomware Weaponized

Nation States, Cryptocurrencies, and Great Power Competition

December 2021

Copyright 2021 Institute for Critical Infrastructure Technology. Except for (1) brief quotations used in media coverage of this publication, (2) links to the www.icitech.org website, and (3) certain other noncommercial uses permitted as fair use under the United States copyright law, no part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher. For permission requests, contact the Institute for Critical Infrastructure Technology.

Executive Summary

Nation state-sponsored threat actors develop, disseminate, and deploy ransomware in conjunction with lower sophistication threat actors as a means to disrupt critical infrastructures and covertly influence global great power competitions. While the profits from ransomware attacks appeal to lower-tier attackers and draw them into the threat landscape, nation-state APTs instead benefit from the disruption and chaos that results from both targeted and widespread attacks on the critical infrastructures of their geopolitical rivals. This publication will discuss:

- How and why nation-state sponsored advanced persistent (APT) threat actors support and leverage lower sophistication threat actors in ransomware campaigns.
- The role of disruptionware in great power competition
- Key nation-state threat actors in disruptionware campaigns
- A "whole-of-nation" stakeholder response to combating ransomware

Contents

Executive Summary.....	0
Introduction	4
Nation States Weaponize the Cyber Threat Landscape	4
Why Ransomware Appeals to Sophisticated Adversaries	4
The Role of Disruptionware in Great Power Competition.....	7
Reputational Harm.....	7
Economic Impact	7
Geopolitical Impact.....	7
Key Nation State Threat Actors in Global Disruptionware Campaigns.....	8
Russia	8
Iran.....	10
China	11
North Korea	12
A “Whole of Nation” Approach to Combat Ransomware	13
Board and Executive Level Preparedness for Ransomware	13
US Executive and Agency Response.....	14
Disrupt Ransomware Infrastructure and Actors:	14
Bolster Resilience to Withstand Ransomware Attacks:	15
Address the Abuse of Virtual Currency to Launder Ransom Payments:	15
Bolster International Cooperation to Disrupt the Ransomware Ecosystem and Address Safe Harbors for Ransomware Criminals:	16
International Response	17
Conclusion	17

Introduction

The disruptions resultant of the COVID-19 pandemic evoked a wave of cybercriminals intent on capitalizing on the vulnerabilities exposed in networks, systems, and people's personal and professional lives. Amidst the tumult, nation-states such as Russia and China have seized upon the opportunity to leverage cybercriminal threat actors as components in broader multi-layer attacks and geopolitical soft power struggles. Nation-states may conduct ransomware attacks to subsidize more resource-intensive cyberattack campaigns, disrupt critical supply chains, or sow discord in the populations and institutions of their geopolitical rivals. This publication will discuss:

- How and why nation-state sponsored advanced persistent (APT) threat actors support and leverage lower sophistication threat actors in ransomware campaigns.
- The role of disruptionware in great power competition
- Key nation-state threat actors in disruptionware campaigns
- A "whole-of-nation" stakeholder response to combating ransomware

Nation-States Weaponize the Cyber Threat Landscape

Nation-state adversaries weaponize lower sophistication attackers as obfuscation, disruption, and additional (often unknowing) accomplices in multi-stage attack campaigns that are predicated on expanded ubiquity and pervasiveness of ransomware variants. The COVID-19 pandemic disrupted organizations' network traffic and workflow, creating opportunities for adversaries. Not only did adversaries capitalize on the chaos and tumult of the COVID-19 pandemic by exploiting the nascent points of network ingress and egress that arose from the rapid migration to distributed workforces, but they also may have increased targeted attacks against third party entities in attempts to laterally compromise critical systems. Between 2020-2021, the FBI measured a 300% increase in reported cybercrimes, including ransomware [1]. For that period, Skybox found that there was a 106% increase in new ransomware, and RiskIQ estimates that six organizations were victimized by ransomware per minute [2] [3].

While cybercrime, in general, is on the rise, this publication will focus on the potential for ransomware to disrupt operations, stress supply chains, extort resources, and fund nation-state-sanctioned operations of advanced persistent threat actors and cyber mercenaries. But just how profitable is ransomware? Does it cause impacts sufficient to garner the attention and resources of more sophisticated adversaries? Is it profitable enough to fund the great power competitions between nation-states?

Why Ransomware Appeals to Sophisticated Adversaries

Ransomware is profitable to low-tier attackers, and with ransomware-as-a-service and "plug-and-play" variants, it is becoming increasingly easier to deploy. While the funds extorted from a ransom may be insignificant to a nation-state APT, ransomware is an efficient vector for enticing low-tier attackers into

the threat landscape, which the APT can leverage as "components" in larger-scale attacks intent on disruption or espionage. Further, in the event that the nation-state deputizes low-tier attackers as cyber-mercenaries, cryptocurrencies provide an anonymous, international, digital currency for solicitation. The benefits of payment via cryptocurrencies are:

1. Nation-states can initiate many attacks just by releasing a variant of ransomware without the need to pay individual attackers.
2. The nation-state threat and the lower tier attacker are kept pseudo-anonymous during the attack
3. The ransomware variant can be loaded with malicious backdoors or malicious bootloaders that can facilitate simultaneous or later APT compromises
4. A culture of allowing small attackers to launch disruptionware attacks unimpeded by law enforcement both "churns" the waters of the threat landscape and iteratively depletes the resources of and inflicts harm on the victim.

Ransomware depends on cryptocurrencies, and the amount extorted can be used as a metric of the overall proliferation of ransomware across all variants. For simplicity, let's begin by examining just Bitcoin, the most popular and most requested cryptocurrency for ransomware extortions. The U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN) has identified roughly \$5.2 billion worth of outgoing Bitcoin transactions likely tied to the top 10 most reported ransomware variants. According to the FinCEN report, "According to data generated from ransomware-related SARs, the mean average total monthly suspicious amount of ransomware transactions was \$66.4 million, and the median average was \$45 million." The total value of ransomware-related SARs from the first six months of 2021, \$590 million, already exceeds the \$416 million reported for the entire year of 2020. The 635 SARs filed until June 2021 have also exploded compared to the 487 SARs reported last year. From SARs filed until June 2021, FinCEN also identified 68 active ransomware variants (most reported were REvil/Sodinokibi, Conti, DarkSide, Avaddon, and Phobos), as well as the top 10 ransomware with most victims and highest demanded ransoms [4].

Of the ten ransomware variants examined, each exceeded \$3 million in total extorted revenue, while "Variant 5" solicited \$3.6 billion. It is worth noting that the collective Bitcoin extorted likely accounts for the efforts of hundreds or thousands of cyber criminals leveraging each variant; however, a resourced adversary such as a nation-state advanced persistent threat (APT), accustomed to developing and deploying sophisticated malware may be enticed by the quick and easy profits of ransomware enough to release a proprietary variant. FinCEN's data also does not reflect the profits the ransomware developer gained by selling the malware to the various cybercriminals who later deployed it en masse. Further complicating the query are discrepancies in victim and attacker behaviors. Many victims are reluctant to report ransomware incidents, and attackers tend to demand significantly larger ransoms from enterprise companies than small-medium businesses (SMBs). Given the rise of cyber insurance and "professional negotiators," a valid assumption may be that in some cases, large, impactful ransomware attacks may be less likely to be reported than smaller-scale attacks.

In short, while we cannot definitively state the profitability of a ransomware to a sophisticated adversary separate from other categories of adversaries, we can assume certain factors. Ransomware is essentially weaponized encryption, and consequentially, it requires fewer resources to develop than multi-stage sophisticated malware. Due to its infamy in the media and its ease of access, ransomware may be more marketable as an "As-a-Service" or "Click-and-Deploy" malware on cybercrime markets and forums. Perhaps even more importantly, in many instances, ransomware can be designed as a passive deployment. In other words, while sophisticated malware requires intense resource dedication for network reconnaissance, data exfiltration, and sustained obfuscation, ransomware can be automated to spread to vulnerable networks, and its operations of encryption and decryption can be automated and integrated with the victim complicity of payment. Worse, a sophisticated adversary can deploy ransomware, pair it with the simultaneous deployment of a multi-stage toolkit (remote access trojan, data exfiltration, etc.), and then sell a version of the ransomware to lower-tier attackers as a means of obfuscation.

The other side of the equation that needs to be considered is whether ransomware proves effective against victims in proportion to the amount allocated for cyber defenses. According to McAfee, the average U.S. organization dedicates about 3-5% of its total revenue to I.T. costs, and about 10% of the I.T. budget is allocated to cybersecurity. The table below depicts the average cybersecurity budgets of U.S. organizations and the average impacts of a cyber incident.

Even with significant investment in cybersecurity, the average company can expect only to mitigate 95-97% of the potential impact per dollar spent. Sophisticated or nation-state adversaries may enter the ransomware market as either distributors or participants to inflict socio-economic and geopolitical harms on an organization or the governments that depend on that infrastructure. Consider:

- Solarwinds was compromised at some in 2020 by an APT, and the company reported losses of \$25 million to its investors.
- Amazon was targeted with a DDOS attack earlier this year, and it succeeded. The one-hour outage resulted in an estimated total loss of \$75 million.
- In May of 2021, Brazilian meatpacking company JBS was the victim of a ransomware attack. The ransom alone was \$4.4 million, and the loss of revenue might have been even greater.
- On May 6, the Colonial Pipeline was hacked, and the ransom paid by the company was reported as \$5 million.

While not all the attacks mentioned were ransomware, the common trend is that all were critical infrastructure or in the critical infrastructure supply chain. The attacks listed above can be categorized as disruptionware incidents. As detailed in previous ICIT whitepapers, disruptionware is malware designed, in part or whole, to inflict an outage of a mission-critical service, product, or supply. For a nation-state or sophisticated threat actor, soliciting a ransom can help fund multi-level malware attacks or sustained campaigns, but the potential disruption to mission-critical operations and supply chains of an adversary may prove far more valuable.

The Role of Disruptionware in Great Power Competition

"Great Power Competition" is a recently resurgent term in conversations of U.S. defense policy, making repeated appearances in the [2017 National Security Strategy](#), [2018 National Defense Strategy](#), and the [2018 National Military Strategy](#). The original term was coined in 1944 by William T.R. Fox and set the tone for the Cold War by defining the "spheres of influence" controlled by the United States, Great Britain, and the Soviet Union. For the purposes of cybersecurity and the use of Great Power Competition in the digital age, the term more broadly describes how nation-states can influence or exert leverage against their adversaries through economic impacts, disruptions to critical infrastructures and supply chains, and other "soft power operations" that may not be directly attributable to the adversarial nation.

Arguably, the first demonstration of a "Great Power Competition" cyberattack may have been the 2014-2015 OPM breach that resulted in the exfiltration of nearly 80 million SF-86 forms and impacted 21.5 million U.S. government employees and their families. The theft of the records took nearly a year of infiltration and exfiltration attributed to the Chinese nation-state APT dubbed Deep Panda. Security analysts, including ICIT, worried that the records could be leveraged to disrupt or influence U.S. intelligence efforts for decades to come. However, in the subsequent years, malware-as-a-service has become more accessible to average cybercriminals, and the potential impacts of disruptionware attacks have become greater. While sustained APT campaigns are still valuable for espionage and reconnaissance, more immediate disruptions or socio-economic impacts can be achieved by lower-tier attacks such as ransomware. Some potential vectors of the Great Power Competition are detailed below.

Reputational Harm

In addition to being less resource-intensive, the attacks are also less likely to invoke an international incident as the campaign is more likely to be attributed to a cybercriminal. Public disclosure of a ransomware incident inflicts reputational harm on the victim. Even if the victim quietly pays the ransom, the attacker could "leak" the attack to the public to capture the media cycle or achieve an impact. For example, a Russian-sanctioned attacker might target U.S. agencies with repeated ransomware attacks as a means of causing global embarrassment or undermining the effectiveness of diplomacy efforts in a region.

Economic Impact

Sustained cyberattacks against an organization stress their defenses and drains resources. Though the cost of paying a ransom can often be significant, for many organizations, the cost of downtime and system recovery is often greater. While ICIT maintains that paying a ransom is rarely the "right" decision, we acknowledge that not all victims have the luxury of choice. Ransomware works because attackers are also aware of the economic dilemma. Ransoms vary from victim to victim because they are strategically priced using first-degree price discrimination; the victim is asked to pay what the attacker assumes they can afford but not more than it would cost not to pay the ransom.

Geopolitical Impact

An additional example of a socio-economic impact of ransomware is an attack on a critical supply chain that disrupts global markets or norms. Consider that as of November 2021, there is a global shortage of

silicon chips necessary for manufacturing across numerous critical infrastructures. The majority of chips are manufactured in Taiwan, and as a result of these proprietary processes, Taiwan is protected from some Chinese influence by the "Silicon Shield." However, if Chinese APTs conducted targeted and sustained disruptionware attacks on Taiwanese chip manufacturers, whose resources are already stressed by the insurmountable demand for chips, then China may be able to shift global silicon chip markets away from Taiwan towards Chinese alternatives. Afterward, Taiwan's "Silicon Shield" may be weakened by a decrease in global support, and as a result, China may be more inclined or better positioned to exert "hard influence" on Taiwan without condemnation from geopolitical partners.

Key Nation State Threat Actors in Global Disruptionware Campaigns

Attributing ransomware attacks or, generally, any cybercrime to nation-state advanced persistent threat actors is challenging because the model of attack is built upon leveraging lower-tier cybercriminals as a mechanism for obfuscation. Some nations, such as Russia, cultivate a culture of inaction against international cybercrime and occasionally piggyback off of cybercriminal infrastructure to deliver more sophisticated malware or exfiltrate data; meanwhile, others such as China, occasionally deputize or coopt cybercriminal gangs in more targeted attacks. Below, this report details some high-level indicators of nation-state threat actors' adoption or facilitation of ransomware.

Russia

For instance, in their extensive August 2021 study of the links between the Russian Federal Security Service (FSB) and Foreign Intelligence Service (SVR), and ransomware gangs that compromised U.S. government-affiliated organizations between October and December 2020, Analyst1 researcher Jon DiMaggio summarized, "We have smoke, the smell of gunpowder, and a bullet casing, but we do not have the gun to link the activity to the Kremlin [5]."

According to Analyst1's report, "[Nation-State Ransomware](#)," cybercriminals used a Ryuk ransomware variant called "Sidoh" launched between June 2019 and January 2020 to collect sensitive information. The variant, capable of targeting financial institutions, operating in the Windows background, collecting keystrokes, and searching documents for sensitive keywords. Evidence presented in the report suggests that the Russian intelligence agencies used ransomware gangs' cybercrime infrastructure to monitor victims, share information with other directorates, and launch multi-stage attacks. For example, in October 2020, the cybercriminal collective dubbed EvilCorp executed a ransomware attack on a victim only for the SilverFish gang to compromise the same victim two months later. The subsequent attack used the same infrastructure, hacking tools, malicious scripts, and domain fronting to conceal the gang's activity. The report found that the ransomware gangs deployed the "Sidoh" malware variant that searches for keywords like "weapons" and "top secret" to identify sensitive documents and exfiltrate them to the command-and-control servers run by the ransomware gangs. Despite its value to both the cybercriminal and Russian intelligence, evidence suggests that this was a low-resource and low sophistication attack because Sidoh was not tailored for cyber-espionage in the same way an APT

malware might be. Instead, DiMaggio suggests that someone obtained Ryuk source code and did a "terrible job of repurposing it as espionage malware [5]."

Using online forum activity analysis, researchers found that most members of the ransomware gangs resided in Eastern Europe, mostly Russia, Ukraine, and Moldova. Some individuals include Evgeniy Bogachev, who allegedly developed the Zeus banking trojan and worked with other cybercrime gangs like RockPhish and Avalanche before forming his cybercrime gang, "The Business Club." Ukraine says that Bogachev works under "supervision of a special unit of the FSB." Allegedly living in Anapa, Russia, Bogachev was allegedly known using online monikers like "Slavik," "Lucky 12345", "Monstr," among others. A 2009 criminal complaint filed in United States District Court in Nebraska mentioned Bogachev while the FBI tracked him as "John Doe #1." Other suspected ransomware gang members allegedly working with Russian intelligence agencies include Maksim Yakubets, tracked by the FBI as John Doe #2 and using the online handle "aqua." Yakubets, Igor Turashev, and other cybercriminals who worked with Bogachev formed another gang known as EvilCorp that uses Bugat malware built from the Zeus source code. The group was responsible for high-profile attacks like the Garmin ransomware attack, demanding a \$10 million ransom. The group also faced U.S. sanctions before adopting other names like Wasted Locker and Babuk. The U.S. Treasury also designated Yakubets as an agent of the Russian FSB. While Ukrainian officials have arrested several members of the Russia-affiliated ransomware gangs, those inside Russia are untouchable. Historically, despite indictments in the United States, "Russia had no interest" in cooperating with the U.S. to apprehend the ransomware cyber criminals [5].

Although the FSB, specific Russian APTs, or Vladimir Putin cannot be definitively linked to the rise in ransomware attacks against critical infrastructure in countries opposed to Russian interests, their inaction to cooperatively combat the global ransomware epidemic speaks louder than any single linkage. Russia has strategically positioned itself as a safe haven for cybercriminals so long as they do not target Russian infrastructure [6]. In short, Russia has fostered a mutually symbiotic relationship with ransomware gangs and cybercriminals.

The value of Kremlin protection isn't lost on the cybercriminals. In early 2021, on a Russian-language dark web forum, fellow cybercriminals criticized a ransomware purveyor known only as "Bugatti," whose gang had been caught in a rare U.S.-Europol sting. The assembled posters accused him of inviting the crackdown with technical sloppiness and by recruiting non-Russian affiliates who might be snitches or undercover cops. One long-active forum member opined that Bugatti had allowed Western authorities to seize ransomware servers that could have been sheltered in Russia instead. They lamented, "Mother Russia will help. Love your country, and nothing will happen to you [7]."

According to the Recorded Future in their report, "[Dark Covenant: Connections Between the Russian State and Criminal Actors](#)," Russian Intelligence may not directly tell the groups what to do or who to target, but it is aware of their activities and asserts influence. The Russian intelligence agencies both recruit talent from the groups and can set some limits on their activities. As an example, National Cyber Director Chris Inglis points to the REvil ransomware gang that launched attacks over summer 2021, decreased its activity, and then recently returned to the dark web and reactivated a portal victims use to make payments. He asserts that when a pattern of attacks has fallen off, "it's a fair bet" that the criminal networks are looking for signals from the Russian government about how they can restart their attacks.

Recorded Future has also published interviews with Russian hackers that admit their involvement in the BlackMatter ransomware attacks against the United States [9].

Even when Russia does not intentionally direct ransomware gangs or offer them protection, its vast offensive cyber-espionage apparatus still contributes to the growing plague of cybercrime. In October 2021, Mieke Eoyang, Deputy Assistant Defense Secretary for Cyber Policy, expressed concern that the individual members of sophisticated Russian advanced persistent threat groups (APTs) may leave government service and launch ransomware attacks or simply conduct cybercrime as a secondary income source. Eoyang points out that just how much control the Russian government has over these actors "is an open question [8]." In some instances, these types of attacks make it harder for the United States and its allies to respond because behavior characteristic of a sophisticated APT may only be attributed to an individual, and it is geopolitically nebulous whether their actions merit international conflict. In summation, Russia has cultivated a mist of plausible deniability that shields it from stronger international responses to its alleged facilitation or involvement in ransomware campaigns.

Iran

FBI and CISA have observed this Iranian government-sponsored [advanced persistent threat] group exploit Fortinet vulnerabilities since at least March 2021 and a Microsoft Exchange ProxyShell vulnerability since at least October 2021 to gain initial access to systems in advance of follow-on operations, which include deploying ransomware," reads an advisory the agencies jointly issued Wednesday.

Iran's cyber activity has previously been more closely tied to regional power plays and its geopolitical objectives. Officials expected espionage operations and were bracing for a retaliatory attack after the Trump administration pulled out of a nuclear agreement brokered by President Barack Obama and assassinated a top Iranian general, for example. But last September, the FBI, and CISA warned that Iran would likely start using their capabilities to improve its financial situation through ransomware operations.

The new joint advisory is also coming as the Biden administration implements a strategy of global cross-agency collaboration to combat ransomware. "The Iranian government-sponsored APT actors are actively targeting a broad range of victims across multiple U.S. critical infrastructure sectors, including the Transportation Sector and the Healthcare and Public Health Sector, as well as Australian organizations," the advisory reads. "FBI, CISA, [the Australian Cyber Security Centre] and [the United Kingdom's National Cyber Security Centre] assess the actors are focused on exploiting known vulnerabilities rather than targeting specific sectors. The Fortinet and Microsoft Exchange vulnerabilities flagged in the advisory are all listed in a catalog of hundreds of known vulnerabilities being actively exploited. The joint advisory also details specific indicators of compromise for organizations to check their systems against. Victims may see new accounts created—including those that mimic real ones—especially in domain controllers, servers, workstations, and active directories, for example. The threat actor may also have manipulated a Task Scheduler used for synchronizing time zones and managing Google Chrome and Microsoft Outlook updates and placed resources like WinRAR and FileZilla in strange locations to facilitate their data exfiltration.

Microsoft has detailed the activities of six Iranian hacker groups that are behind waves of ransomware attacks that have arrived every six to eight weeks since September 2020. Microsoft said Iranian hacking groups are using ransomware to either collect funds or disrupt their targets and are "patient and persistent" while engaging with their targets – although they will use aggressive brute-force attacks. The most consistent of the six Iranian threat groups is one Microsoft tracks as Phosphorus (others call it APT35). Microsoft has been playing cat and mouse with the group for the past two years. While initially known for cyber espionage, Microsoft details the group's strategies for deploying ransomware on targeted networks, often using Microsoft's Windows disk-encryption tool BitLocker to encrypt victim files.

Other cybersecurity firms last year detected a rise in ransomware from Iranian state-backed hackers using known Microsoft Exchange vulnerabilities to install persistent web shells on email servers and Thanos ransomware.

According to Microsoft, Phosphorus was also targeting unpatched on-premise Exchange servers and Fortinet's FortiOS SSL VPN in order to deploy ransomware. In the second half of 2021, the group started scanning for the four Exchange flaws known as ProxyShell that were initially exploited as zero-days by Beijing-backed hackers. Microsoft released patches for CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065 in April. ProxyLogon was one of several exploits that made up ProxyShell.

An account by security specialist DFIR Report notes Phosphorus used BitLocker on servers and DiskCryptor on P.C.s. Their activity stood out because it didn't rely on ransomware-as-a-service offerings that are popular among cybercriminals and didn't create custom encryptors. "After compromising the initial server (through vulnerable VPN or Exchange Server), the actors moved laterally to a different system on the victim network to gain access to higher-value resources," the Microsoft Threat Intelligence Center (MSTIC) notes in a blog post. "From there, they deployed a script to encrypt the drives on multiple systems. Victims were instructed to reach out to a specific Telegram page to pay for the decryption key." The group also tries to steal credentials by sending "interview requests" to targeted individuals through emails that contain tracking links to confirm whether the user has opened the file. Once a response is received from the target user, the attackers send a link to a list of interview questions and then a link to a fake Google Meeting, which would steal login details. Other groups mentioned in Microsoft's report included an emerging Iranian hacking group that recently targeted Israel and U.S. organizations in the Persian Gulf with password-spraying attacks. Microsoft highlights that the adoption of ransomware aided the Iranian hackers' efforts in espionage, disruption and destruction, and to support physical operations. Their arsenal of attacks included ransomware, disk wipers, mobile malware, phishing, password-spray attacks, mass exploitation of vulnerabilities, and supply chain attacks.

China

While it may seem unlikely that a well-resourced nation like China would launch cybercrime attacks, some reports indicate that the PLA units tasked with China's offensive cyber capabilities are actually only allocated 70% of their operating budget and are responsible for providing the remainder through data exfiltration, malware-as-a-service, and cybercrime operations. Chinese threat actors may launch disruptionware attacks for economic gain, to inflict reputational harm, or to distract from other multi-

layer attacks. For instance, code belonging to Chinese APT27 was recently associated with a ransomware deployment, and it is feasible that the backdoor embedded in the code may have been intended to deploy a more sophisticated malware [4] simultaneously.

Researchers have discovered that the Chinese espionage group APT27 has moved into more financially-motivated cybercrimes, using ransomware to encrypt core servers at major gaming companies worldwide. In a blog released by Profero and Security Joes, researchers said the team first started following APT27 closely in early 2020 when they responded to the ransomware incident. During that investigation, they found malware identified by TrendMicro back in July 2019, which was linked to a campaign by APT27 and Winnti, known as DRBControl. Both groups are linked to China.

The Profero/Security Joes' report on the ransomware incidents found extremely strong links to APT27 in terms of code similarities and tactics, techniques, and procedures. They said what stood out in this incident was the encryption of core servers using BitLocker, a drive encryption tool built into Windows. The approach was unusual, given threat actors typically drop the ransomware to the machines as opposed to using local tools. What solidified their belief that APT27 had moved into financially-motivated cybercrime was a report in April 2020 by Positive Technologies that found APT27 had also dropped the Polar ransomware on systems.

Austin Merritt, a cyber threat intelligence analyst at Digital Shadows, said the significant use of tooling that has historically been linked to Chinese threat actors suggests it's realistically possible that APT27 or Winnti could have been responsible for the ransomware actions outlined by the Profero/Security Joes report. Merritt added that other nation-state affiliated APTs such as TA505 (Russia) and Lazarus Group (North Korea) had used ransomware in the past. "As many ransomware variants are deployed using commodity malware variants, such as TrickBot and Emotet, it's often hard to pinpoint attribution to one specific APT," Merritt said. "Given the prominence of ransomware across the threat landscape, it's likely that financially-motivated nation-state threat actors will use ransomware in future attacks."

Although a cyberespionage group engaging in a financially-motivated campaign is unusual, this attack would not be the first time APT27 deploys ransomware on victim systems. Researchers at Positive Technologies attributed a Polar ransomware attack from April 2020 to APT27, based on the use of malware normally used by this group.

North Korea

North Korea is often referred to as a "hail-mary" threat actor in that they lack the resources that China and Russia have to launch sustained campaigns. North Korean threat actors may launch ransomware attacks to revenge a political slight or to solicit ransoms necessary to provide funds to the nation-state.

In October 2021, Kaspersky researchers saw The North Korean state APT use a new variant of the BlindingCan RAT to breach a Latvian I.T. vendor and then a South Korean think tank. Lazarus – a North Korean advanced persistent threat (APT) group – is working on launching cyberespionage-focused attacks on supply chains with its multi-platform MATA framework. The MATA malware framework can target three operating systems: Windows, Linux, and macOS. MATA has historically been used to steal

customer databases and to spread ransomware in various industries, but in June, Kaspersky researchers tracked Lazarus using MATA for cyber-espionage.

Researchers have also seen Lazarus building supply-chain attack capabilities with an updated DeathNote (aka Operation Dream Job) malware cluster that consists of a slightly updated variant of the North Korean remote-access trojan (RAT) known as BlindingCan.

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) sent out an alert about BlindingCan in August 2020, warning that Hidden Cobra – another name for Lazarus that's used by the U.S., in general, to refer to malicious cyber activity by the North Korean government – was using BlindingCan to siphon intelligence out of military and energy outfits. The researchers have also discovered campaigns targeting a South Korean think tank – with an infection chain that included legitimate South Korean security software that was carrying a malicious payload – and a Latvian I.T. asset-monitoring tool vendor.

A "Whole of Nation" Approach to Combat Ransomware

Stan Mierzwa, ICIT Fellow, and Director and Adjunct Professor, Center for Cybersecurity, Kean University, proffers that a multi-faceted, multi-stakeholder response is necessary to respond to the rise in ransomware as an attack vector. He continues, "When executive leaders and decision-makers may look at their organizational operations from a distance and high level, everything may appear to be fine and working smoothly. However, one area that should not be gleaned from a distance is the reality that ransomware may likely, at some point, come smashing in. Leadership levels, starting at the key stakeholders, such as stock owners, to the board of directors, and executive management, need to become more intimate with the ransomware reality and step-by-step reaction plans. With proper transparent discussions, the responsibility of making critical action decisions will benefit these executive teams, and more importantly, the constituents they serve."

Board and Executive Level Preparedness for Ransomware

Proactive preparedness that includes what exact logic pattern or flowchart to consider in the event of a serious incident can be helpful to an organization in minimizing unexpected malicious surprises. Mr. Mierzwa adds, "The FBI has stated for some time that they do not advocate to pay a ransom, in large part because there is no guarantee that an organization will regain access to their data and systems (Federal Bureau of Investigation, 2019). In the event of cyber-attacks that involve the extortion of funds in order to resume proper operations for businesses, it will no doubt involve decisions from the tippy top, including board and executive-level staff. In these situations, the role of ethical considerations for key stakeholders will need to ensure as a best practice and help guide decision making. Although the FBI states to avoid paying a ransom, they also state that businesses faced with the inability to function may result in executives providing considerations to their key stakeholders, including shareholders, employees, customers, and the general public (Federal Bureau of Investigation, 2019). This can essentially translate to paying the ransom, as was the case in the Colonial Pipeline ransomware episode from the summer of 2021."

As a minimal step, all board of directors should strongly consider including the topic of what to do in the event of a ransomware attack on their organization in their routine meetings. Including a transparent and real discussion on the framework, they will follow if critical systems are unavailable. This sort of

tabletop exercise will ensure that all board members are educated on the topic and help to decide on the length of time that an outage can last before having to resort to less savory decisions. The scenario planning will provide an opportunity also to detail how long restoring systems would take and even to review the effectiveness of backup and restore operations in the said organization. In the case of government policymakers, such tabletop exercises can also aid in specific industry policies to be maintained and followed, such as the critical infrastructure of energy supply.

In many businesses, agencies, and organizations, the use of cybersecurity awareness training is provided as an ultimate goal of forming habits of repeatable actions and behaviors pertaining to proper cyber hygiene (Pearlson et al., 2021). This type of cybersecurity training is meant for all employees. The creation of repeatable actions or habits for executive leaders can have the same effect with dealing with ransomware or the next big vulnerability that may attack an organization. By including the board and executive leaders in proactive training, tabletops, or other like exercises, to precisely outline approaches to critical decisions in a transparent fashion can aid an organization when things go awry.

U.S. Executive and Agency Response

The Biden Administration's counter-ransomware efforts are organized along four lines of effort:

- Disrupt Ransomware Infrastructure and Actors
- Bolster Resilience to Withstand Ransomware Attacks
- Address the Abuse of Virtual Currency to Launder Ransom Payments
- Bolster International Cooperation to Disrupt the Ransomware Ecosystem and Address Safe Harbors for Ransomware Criminals

Disrupt Ransomware Infrastructure and Actors:

The Administration is bringing the full weight of U.S. government capabilities to disrupt ransomware actors, facilitators, networks, and financial infrastructure. The Department of Justice established a Task Force to enhance coordination and alignment of law enforcement and prosecutorial initiatives combating ransomware. Law enforcement agencies, working through the National Cyber Investigative Joint Task Force (NCIJTF) and with the support of the interagency, are surging investigations, asset recovery, and other efforts to hold ransomware criminals accountable.

The Department of the Treasury levied its first-ever sanctions against a virtual currency exchange. The exchange, SUEX, was responsible for facilitating ransomware payments to ransomware criminals associated with at least eight ransomware variants. Treasury will continue to disrupt and hold accountable these ransomware actors and their money-laundering networks to reduce the incentive for cybercriminals to continue to conduct these attacks. The Department of the Treasury published updated sanctions advisory encouraging and emphasizing the importance of reporting ransomware incidents and payments to U.S. Government authorities.

U.S. Cyber Command and National Security Agency are dedicating people, technology, and expertise to generate insights and options against ransomware actors. Their technical expertise and insights enable and support whole-of-government efforts, including actions against criminals, their infrastructure, and

their ability to profit from their crimes. The Department of State's Rewards for Justice (RFJ) Office has offered a \$10 million reward for information leading to the identification or location of any person who, while acting at the direction or under the control of a foreign government, engages in, or aids or abets, certain malicious cyber activities against U.S. critical infrastructure, to include ransomware activities.

[Bolster Resilience to Withstand Ransomware Attacks:](#)

The Administration has called on the private sector to step up its investment and focus on cyber defenses to meet the threat. The Administration has also outlined the expected cybersecurity thresholds for critical infrastructure and introduced cybersecurity requirements for critical transportation infrastructure.

The President launched an Industrial Control System Cybersecurity (ICS) Initiative in April – a voluntary, collaborative effort between the federal government and the critical infrastructure community. The ICS Initiative has led to over 150 electricity utilities representing almost 90 million residential customers to deploy or commit to deploying control system cybersecurity technologies, bolstering the security and resilience of these facilities. The ICS Initiative has been expanded to natural gas pipelines and will shortly be expanded to the water sector.

Deputy National Security Advisor for Cyber and Emerging Technology, Anne Neuberger, sent an open letter to CEOs in June communicating best practices to defend against and prepare for ransomware incidents, including backing up data, implementing multi-factor authentication, and testing incident response plans.

In July, the U.S. Department of Homeland Security (DHS) and the U.S. Department of Justice (DOJ) established the StopRansomware.gov website to help private, and public organizations access resources to mitigate their ransomware risk. The Transportation Security Administration (TSA) at the Department of Homeland Security issued two Security Directives requiring critical pipeline owners and operators to bolster their cyber defenses, enabling DHS to identify better, protect against, and respond to threats to critical companies in the pipeline sector.

In August, President Biden met with the private sector and education leaders to discuss the whole-of-nation effort needed to address cybersecurity threats – and leaders announced ambitious initiatives to bolster the Nation's cybersecurity. The National Institute of Standards and Technology (NIST), within the Department of Commerce, is working with industry to improve current and emerging standards, practices, and technical approaches to address ransomware. Their efforts include the development of the Cybersecurity Framework Profile for Ransomware Risk Management, which builds off the NIST Cybersecurity Framework to provide organizations a guide to prevent, respond to, and recover from ransomware events. Treasury and the Department of Homeland Security's CISA are engaging the cyber insurance sector to explore incentives to enhance implementation of cyber hygiene and improve visibility of ransomware activity.

[Address the Abuse of Virtual Currency to Launder Ransom Payments:](#)

Virtual currency is subject to the same Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) controls that are applied to fiat currency, and those controls and laws must be enforced. The Biden Administration is leveraging existing capabilities and acquiring innovative

capabilities to trace and interdict ransomware proceeds. The United States remains at the forefront of applying anti-money laundering/countering the financing of terrorism (AML/CFT) requirements on virtual currency businesses and activities. We continue to hold U.S. virtual currency exchanges accountable to our regulatory requirements, and we have shared indicators and typologies of virtual currency misuse with the virtual currency and broader financial sector through venues like the Financial Crimes Enforcement Network (FinCEN) Exchange program.

Treasury is leading efforts to drive implementation of international standards on financial transparency related to virtual assets at the Financial Action Task Force and to build bilateral partnerships designed to strengthen AML/CFT controls for virtual currency exchanges overseas. Uneven implementation of international AML/CFT virtual currency standards creates vulnerabilities ransomware actors exploit and inhibits the U.S. Government's ability to disrupt ransomware-associated money laundering. Led by the Federal Bureau of Investigation, the Administration is building an Illicit Virtual Asset Notification (IVAN) information sharing partnership and supporting platform to improve the timeliness of detection and disruption of ransomware and other illicit virtual currency payment flows.

[Bolster International Cooperation to Disrupt the Ransomware Ecosystem and Address Safe Harbors for Ransomware Criminals:](#)

Responsible states do not permit criminals to operate with impunity from within their borders. We are working with international partners to disrupt ransomware networks and improve partner capacity for detecting and responding to such activity within their own borders, including imposing consequences and holding accountable those states that allow criminals to operate from within their jurisdictions.

The Administration is working closely with international partners to address the shared threat of ransomware and galvanize global political will to counter ransomware activities – as reflected in the recent G7 and North Atlantic Treaty Organization (NATO) joint statements and Financial Action Task Force (FATF) efforts, among others. The Administration continues to advocate for expanded membership in and implementation of the Budapest Convention and its principles.

Departments and Agencies continue to engage with States to improve their capacity for addressing ransomware threats, including through capacity building that promotes cybersecurity best practices and combats cybercrime, such as training on network defense and resilience, cyber hygiene, virtual currency analysis, and other training and technical assistance to foreign law enforcement partners to combat criminal misuse of information technologies.

The United States remains committed to eliminating safe harbors for ransomware criminals through a more direct diplomatic approach. President Biden has directly engaged President Putin and established the White House and Kremlin Experts Group to discuss and address ransomware activity directly. The Experts Group continues to meet to address the ransomware threat and to press Russia to act against criminal ransomware activities emanating from its territory. The President has made clear the United States will act to protect our people and critical infrastructure.

International Response

The threat of ransomware and its potential impacts on the geopolitical and socio-economic landscapes are likely going to continue to increase. As the technological barrier decreases and the profitability increases, more threat actors ranging from script kiddies to nation-state advanced persistent threat actors are going to leverage ransomware to garner quick profits, strategically disrupt supply chains, and shifting geopolitical norms. However, the rising threat is not entirely unopposed. Ransomware depends on anonymous cryptocurrency exchanges. Mitigating the abuse of virtual assets on a global scale would impact the business model and the main instrument used by the ransomware cybercrime groups to collect ransoms from their victims and launder the funds obtained in attacks targeting organizations around the world. In October 2021, senior officials from 31 countries and the European Union said that their governments would take action to disrupt the cryptocurrency payment channels used by ransomware gangs to finance their operations. It was issued by ministers and representatives from Australia, Brazil, Bulgaria, Canada, the Czech Republic, the Dominican Republic, Estonia, European Union, France, Germany, India, Ireland, Israel, Italy, Japan, Kenya, Lithuania, Mexico, the Netherlands, New Zealand, Nigeria, Poland, Republic of Korea, Romania, Singapore, South Africa, Sweden, Switzerland, Ukraine, United Arab Emirates, the United Kingdom, and the United States. The joint statement was issued following the virtual Counter-Ransomware Initiative meetings facilitated this week by the White House National Security Council in response to ongoing attacks that revealed significant vulnerabilities across the critical worldwide infrastructure.

Conclusion

Nation state-sponsored threat actors develop, disseminate, and deploy ransomware in conjunction with lower sophistication threat actors as a means to disrupt critical infrastructures and covertly influence global great power competitions. While the profits from ransomware attacks appeal to lower-tier attackers and draw them into the threat landscape, nation-state APTs instead benefit from the disruption and chaos that results from both targeted and widespread attacks on the critical infrastructures of their geopolitical rivals. A multi-stakeholder approach that unites agencies, the private sector, and geopolitical partners is necessary to protect national security and combat the rise of disruptionware.

Sources

- [1]"Internet Crime Report", *ic3.gov*, 2021. [Online]. Available:
https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf. [Accessed: 28- Dec- 2021].
- [2] "Vulnerability and Threat Trends Report 2021", Skybox Security, 2021. [Online]. Available:
<https://www.skyboxsecurity.com/trends-report/>. [Accessed: 10- Aug- 2021].
- [3]"RiskIQ's 2021 Evil Internet Minute | RiskIQ", *RiskIQ*, 2021. [Online]. Available:
<https://www.riskiq.com/resources/infographic/evil-internet-minute-2021/>. [Accessed: 28- Dec- 2021].
- [4]"Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021", *Fincen.gov*, 2021. [Online]. Available:
https://www.fincen.gov/sites/default/files/shared/Financial%20Trend%20Analysis_Ransomware%20508%20FINAL.pdf. [Accessed: 28- Dec- 2021].
- [5]J. DiMaggio, "Nation State Ransomware", *Analyst1.com*, 2021. [Online]. Available:
https://analyst1.com/file-assets/Nationstate_ransomware_with_consecutive_endnotes.pdf. [Accessed: 28- Dec- 2021].
- [6]E. TUCKER and A. SUDERMAN, "Ransomware persist even as high-profile attacks have slowed | A.P. News," *AP NEWS*, 2021. [Online]. Available: <https://apnews.com/article/ransomware-attacks-us-russia-biden-putin-fce2ebd29cdffc43737a4243a1f04321>. [Accessed: 28- Dec- 2021].
- [7]"Dark Covenant: Connections Between the Russian State and Criminal Actors | Recorded Future", *Recorded Future*, 2021. [Online]. Available: <https://www.recordedfuture.com/russian-state-connections-criminal-actors/>. [Accessed: 28- Dec- 2021].
- [8]M. Matishak, "Pentagon official:'Open question' if Putin's government can stop hackers," *The Record by Recorded Future*, 2021. [Online]. Available: <https://therecord.media/pentagon-officialopen-question-if-putins-government-can-stop-hackers/>. [Accessed: 28- Dec- 2021].