Pharos Series: Report No. 3 April 2025

Ransomware's New Masters: How States Are Hijacking Cybercrime

Aleksandar Milenkoski, Jiro Minier, Julian-Ferdinand Vögele, Max Smeets, Taylor Grossman

virtual routes

This report was developed
in partnership with:

PHAROS SERIES
Virtual Routes | www.virtual-routes.org
Design & Layout by Frank Wo | Cover by Vahram Muradyan | Edited by Katharine Khamhaengwong

Pharos Series: Report No. 3 April 2025

Ransomware's New Masters: How States Are Hijacking Cybercrime

Aleksandar Milenkoski, Jiro Minier, Julian-Ferdinand Vögele, Max Smeets, Taylor Grossman

virtual routes

About the Authors

Aleksandar Milenkoski

Aleksandar Milenkoski is a Senior Threat Researcher at SentinelLabs. With expertise in malware research and a focus on targeted attacks, he brings a blend of practical and deep insights to the forefront of cyber threat intelligence. Aleksandar has a PhD in system security and is the author of numerous reports on cyberespionage and high-impact cybercriminal operations, conference talks, and peer-reviewed research papers. From 2011 to 2014, he was a European Commission Marie Skłodowska-Curie Research Fellow. His research has won awards from SPEC, the Bavarian Foundation for Science, and the University of Würzburg.

Jiro Minier

Jiro Minier leads the Threat Intelligence Research & Analysis team at the Deutsche Cyber-Sicherheitsorganisation (DCSO), a Berlin-based cybersecurity competence center, with a personal focus on China-nexus cyberespionage and associated issues. He is actively involved in the cybersecurity and technology policy debate, including as a participant in the German Marshall Fund's Young Strategists Forum and the German Council on Foreign Relations' Action Group Zeitenwende and via prior fellowships with Virtual Routes and the Centre for International Security at the Hertie School.

Prior to joining DCSO, he was employed as a staffer to the then-Chairman of the Committee on Foreign Affairs of the House of Representatives of Japan. He holds degrees in International Relations from the London School of Economics and the University of Cambridge.

Julian-Ferdinand Vögele

Julian-Ferdinand Vögele is a threat researcher with Recorded Future's Insikt Group, specializing in malware research, threat hunting, and cyber threat intelligence. His work primarily focuses on malware analysis and the detection of malicious infrastructure. Prior to joining Recorded Future, he worked in IT security at Security Research Labs, where he was involved in security research and red team operations. Julian-Ferdinand holds a MSc in Computer Science from University College London (UCL). He is also a fellow of Virtual Routes and a scholar of the German Academic Scholarship Foundation.

Max Smeets

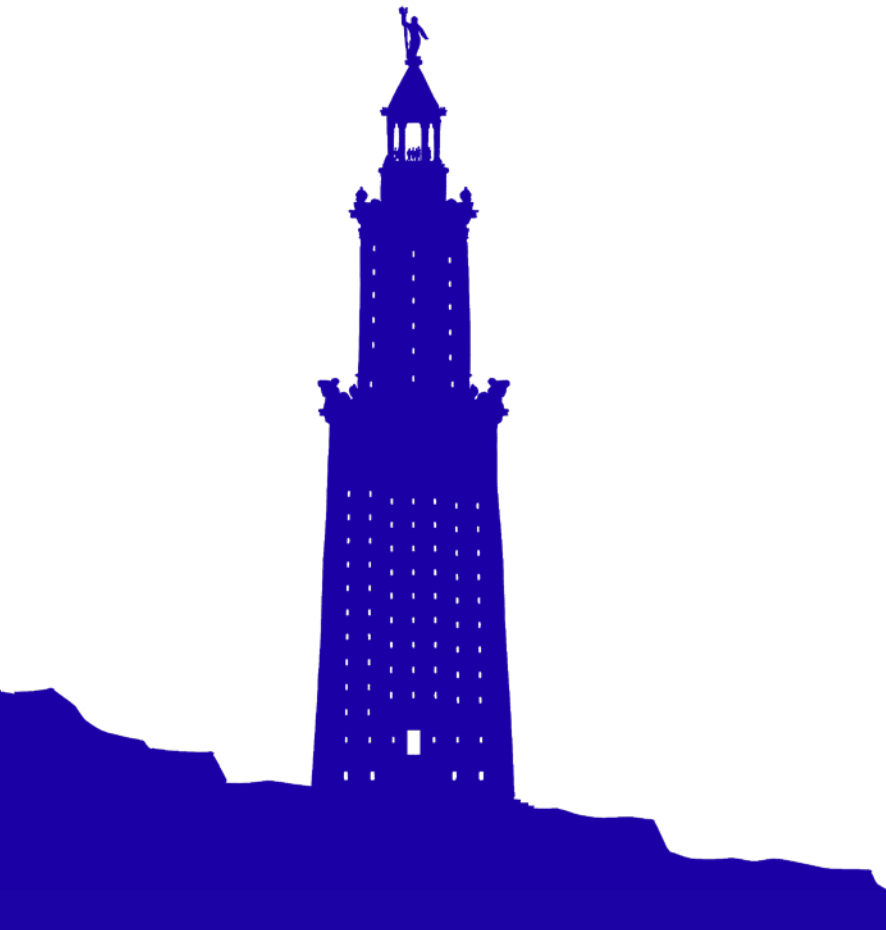
Max Smeets is the Co-Director of Virtual Routes and serves as Managing Editor of *Binding Hook*. He also holds research positions at ETH Zurich, the Royal United Services Institute (RUSI), and Stanford University's Center for International Security and Cooperation. Max is the author of *Ransom War: How Cyber Crime Became a Threat to National Security* and *No Shortcuts: Why States Struggle to Develop a Military Cyber Force*.

Max received a BA in Economics, Politics, and Statistics from University College Roosevelt, Utrecht University, and an MPhil (Brasenose College) and DPhil (St. John's College) in International Relations from the University of Oxford.

Taylor Grossman

Taylor Grossman is Director for Digital Security at the Institute for Security and Technology, where she works on the Ransomware Task Force and other ongoing projects. Previously, she was a senior researcher in the Cyberdefence Project at the Center for Security Studies at ETH Zurich. She also serves as a commissioning editor at *Binding Hook*, a Virtual Routes media organization that publishes articles on technology and security. She holds an MPhil in International Relations from the University of Oxford and a BA in Political Science from Stanford University.

Table of Contents



Executive Summary

Ransomware has evolved into one of the most pervasive cyber threats, with high-profile incidents disrupting government organizations and private companies alike. Beyond their financial impact, these attacks now pose direct risks to human safety. While ransomware has long been associated with non-state criminal actors, state-linked actors are increasingly deploying it to achieve their objectives as well.

This report provides a comparative analysis of ransomware use by groups linked to four states: Russia, China, North Korea, and Iran. We find that divergent motives and operational ecosystems contribute to varying uses of state-linked ransomware to gain strategic advantages.

Russian state-linked groups primarily leverage ransomware as an operational tool in high-tempo conflicts like Ukraine, while China often aims to enhance plausible deniability for espionage activity. Iranian actors most frequently deploy ransomware for disruption, popular perception, and reputation, particularly targeting Israeli organisations. Meanwhile, the evolution of North Korean activity reflects a focus on strategic and tactical financial gain.

Concurrently, however, we find that a degree of convergence can be observed in the state-linked use of ransomware. These convergences include the adoption of best practices from cybercriminal ransomware operations and the increasing involvement of state-linked actors within cybercriminal ransomware ecosystems, not only as beneficiaries but also as active participants.

Introduction

Ransomware has rapidly evolved into one of the most significant and pervasive cybersecurity threats in recent years. High-profile incidents demonstrate its far-reaching impact and potential for disruption. In 2023, the MOVEit data breach exploited vulnerabilities in the managed file transfer software, compromising over 2,700 organizations and exposing the personal data of approximately 93 million individuals, highlighting the systemic risks in digital supply chains.[1] Similarly, ransomware operations have targeted critical infrastructure, such as the 2021 Colonial Pipeline attack, which caused fuel shortages across the United States, and Conti group's attack on the Costa Rican government, which crippled the country's infrastructure and financial systems.[2]

> "These ransomware attacks are not merely disruptive to organisations; they increasingly pose direct threats to human lives."

For example, in June 2024, the Russian-linked Qilin ransomware gang targeted prominent hospitals in London, compromising patient care systems. Emergency departments faced significant delays, surgeries were canceled, and sensitive medical data was leaked online. Such incidents underline the growing risks ransomware poses to critical sectors where operational downtime can lead to life-threatening consequences.

While ransomware has been extensively used by criminal non-state actors, state actors are also deploying ransomware to achieve strategic objectives. This Pharos Report examines ransomware operations conducted by groups linked to four states – Russia, China, North Korea, and Iran – often referred to as the 'Big Four'. These states use ransomware not only for financial gain, but also as tools to achieve political aims.[4]

---

[1] Lawrence Abrams, 'SEC ends probe into MOVEit attacks impacting 95 million people,' Bleeping Computer, August 7, 2024, https://bleepingcomputer.com/news/security/sec-ends-probe-into-moveit-attacks-impacting-95-million-people/. Also see REvil's attack on Kaseya: Caitlin Cimpanu, '"REvil ransomware gang executes supply chain attack via malicious Kaseya update,"' *Record*, July 1, 2021, https://therecord.media/revil-ransomware-executes-supply-chain-attack-via-malicious-kaseya-update.

[2] Jen Easterly, 'The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years,' Cybersecurity and Infrastructure Agency (CISA), May 7, 2023, https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years.

[3] Victoria Cook, '"Russian criminals' behind hospitals cyber attack," *BBC*, June 5, 2024, https://www.bbc.com/news/articles/cxee7317kgmo; Sammy Gecsoyler and Dan Milmo, 'Russian crime group behind London hospitals cyber-attack, says expert,' *Guardian*, June 5, 2024, https://www.theguardian.com/technology/article/2024/jun/05/russian-group-behind-london-hospitals-cyber-attack-says-expert.

We seek to provide a comparative analysis of state-linked ransomware operations, uncovering their diverse purposes and methods. We show states deploy ransomware in distinct ways.

Russian state-linked groups, often with ties to the criminal ecosystem, deploy ransomware as an operational tool in high-intensity conflicts. A notable example is GRU Unit 74455's ransomware attacks during the 2022 invasion of Ukraine, which targeted supply routes vital to Ukraine's defense. Chinese state-linked groups tend to prioritise plausible deniability, using ransomware in cyberespionage campaigns to distract, misattribute, or erase evidence. Iranian state-linked groups typically deploy ransomware for political objectives, frequently targeting Israeli organisations, as well as those of other rivals. Finally, North Korean ransomware use instead focuses on financial gain to support its regime and operations.

The transition of states to using more ransomware instead of wipers – data destruction malware – over the past years may signify the myriad advantages of ransomware. It offers plausible deniability for some, financial gain for others, while taking less development time for most – they can simply use off-the-shelf ransomware as a service (RaaS) variants.[5]

Despite these differences, we have also identified commonalities and convergences in ransomware usage across these states. While North Korea has long used ransomware to fund itself and Chinese state hackers have incorporated it into moonlighting activities, Iranian state-linked groups have also begun exploiting unauthorized access for financial gain.

Similarly, while Iranian and Russian state-linked groups have long used ransomware for politically and militarily motivated disruption, there is now evidence that China is also using ransomware for such purposes, as evidenced by incidents such as those targeting the All India Institute of Medical Sciences (AIIMS) and the Brazilian presidency.

[4] We have seen limited analysis on the subject. For exceptions see: Google, 'Cybercrime: A Multifaceted National Security Threat,' February 2025, https://cloud.google.com/blog/topics/threat-intelligence/cybercrime-multifaceted-national-security-threat; also see Max Smeets, *Ransom War: How Cyber Crime Became a Threat to National Security*, Oxford University Press: 2025.

[5] Note that China is not part of this transition, as it does not have a public track record in conducting wiper operations.

Russia

Russia has long been recognised as a key hub for ransomware activity. Chainalysis, a blockchain analytics firm, estimates that in 2021, 74% of global ransomware revenue flowed to groups based in Russia.[6]

Criminal ransomware groups often follow tactics, techniques, and procedures which seek to avoid targeting Russian-owned systems. For example, malware is frequently designed to check the language settings of the operating system it has entered and will delete itself if it detects a keyboard set to one of the languages of Commonwealth of Independent States (CIS) countries.[7] In 2021, approximately 90% of known ransomware payments were being collected through ransomware variants that specifically avoided Russian speakers.[8] Money-laundering networks help bring cash into Russia, indirectly benefiting the sanction-strapped regime.[9]

Spotlight Case Study: GpCode and Criminals early targeting of Russian individuals

One of the earliest ransomware campaigns, GpCode (aka PGPCoder), emerged in the mid-2000s and was operated by Russian cybercriminals. GpCode was a file-encrypting Trojan spread via socially engineered emails. Notably, some variants used Russian-language lures (like fake job recruitment documents) to infect victims' computers.[10] Unlike the later ransomware gangs, which carefully avoid local targets, GpCode did not spare Russian victims. In fact, it plagued users in Russia for over a year, from 2004-2006, with Kaspersky Lab reporting an 'avalanche of emails from users in Russia' who fell prey, alongside some victims in other countries.[11]

Upon infection, GpCode encrypted dozens of file types and left ransom notes (eg readme.txt files) demanding payment (in that era, often around $100-200 in e-gold) for a decryption tool. The impact, while smaller in scale than today's multimillion-dollar incidents, was significant for individuals and businesses hit at a time when ransomware was a new phenomenon.[12]

---

[6] Joe Tidy, '74% of Ransomware Revenue Goes to Russia-Linked Hackers,' *BBC*, February 14, 2022, https://www.bbc.com/news/technology-60378009.

[7] 'Eastern Europe's Crypto Crime Landscape: Scams Dominate, Plus Significant Ransomware Activity,' Chainalysis, October 14, 2021, https://www.chainalysis.com/blog/eastern-europe-cryptocurrency-geography-report-2021-preview/; 'System Location Discovery: System Language Discovery,' Mitre | Att&ck, accessed January 5, 2025, https://attack.mitre.org/techniques/T1614/001/.

[8] Joe Uchill, 'Ransomware that avoids Russian speakers gets 90% of payments,' *SC Media*, September 2, 2021, https://www.scworld.com/analysis/ransomware-that-avoids-russian-speakers-get-90-of-ransoms.

[9] For example, see: 'NCA Disrupts Multi-Billion Dollar Russian Money Laundering Network, OFAC Sanctions Related Individuals and Entities,' Chainalysis, December 4, 2024, https://www.chainalysis.com/blog/nca-disrupts-multi-billion-dollar-russian-money-laundering-network-2024/?mkt_tok=NTAzLUZBUC0wNzQAAAGXMlfMZFDl9bImrc-p5SQK7CC9qeWWIoZcWC0z0EJEn3V16tQeAnV20TOUiM27Lsv_Pku7iqx4pZuYdohJ8mtTlu8oJOcSJ-LwxwejV8V-qum3.

Direct connections between criminal ransomware groups and the Russian government occasionally come to light. In 2019, the US Justice Department sanctioned Maksim Yakubets, the leader of Evil Corp, for providing 'direct assistance to the Russian government' and 'material assistance to the FSB', Russia's Federal Security Service.[13] Yakubets' ties to the state were reportedly strengthened through his father-in-law, Eduard Bendersky, a former member of the elite Vympel unit of the FSB.[14] Leaked internal communications of the Conti ransomware group revealed that they received specific targeting requests from the FSB. One such instance involved a proposal to target Bellingcat, the investigative organization that was probing the poisoning of Russian opposition leader Alexey Navalny.[15] These examples blur the lines between state-directed operations and independent criminal endeavors, underscoring the difficulty in distinguishing where one ends and the other begins.

While boundaries between the state and criminal ecosystem remain porous, Russian state-linked groups have deployed ransomware to achieve distinct, non-financial objectives. Public evidence suggests that ransomware has been most prominently employed by the Sandworm group, also known as APT44.[16] Sandworm is attributed to Unit 74455 of the GRU, the Russian military intelligence agency. This group has gained notoriety for destructive cyber operations targeting critical infrastructure, elections, and other strategic targets.[17] Sandworm's activities include high-profile incidents such as the deployment of BlackEnergy and Industroyer (CrashOverride) malware in attacks on Ukraine's power grid in 2015 and 2016, causing significant power outages.[18] The 'Olympic Destroyer' malware, which was used in a disruptive cyberattack during the 2018 Winter Olympics, has also been attributed to the group.[19]

Sandworm first began using pseudo-ransomware in 2017 with the deployment of NotPetya, a malware campaign that thinly disguised itself as ransomware but was, in reality, a tool of widespread digital destruction.[20]

---

[10] Denis Nazarov and Emelyanova Olga, 'Blackmailer: The Story of Gpcode,' SecureList by Kapersky, June 26, 2006, https://securelist.com/blackmailer-the-story-of-gpcode/36089/.

[11] Ibid

[12] John Leyden. 'Ransomware Author Tracked down, but Not Nicked.' *Register*, October 1, 2008. https://www.theregister.com/2008/10/01/gpcode_author_hunt/.

[13] 'Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware,' US Department of the Treasury, December 5, 2019, https://home.treasury.gov/news/press-releases/sm845.

[14] Alexander Martin, 'Eduard Benderskiy: Western authorities link Russian intelligence officer to Evil Corp cybercrime empire,' *Record*, October 1, 2024, https://therecord.media/evil-corp-cybercrime-eduard-benderskiy-russian-intelligence.

[15] Matt Burges, 'Leaked Ransomware Docs Show Conti Helping Putin from the Shadows,' *Wired*, March 18, 2022, https://www.wired.com/story/conti-ransomware-russia/

[16] APT is short for 'advanced persistent threat'

[17] Andy Greenberg, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers* (Doubleday, 2019).

[18] Dragos, 'CRASHOVERRIDE Analyzing the Threat to Electric Grid Operation,' June 13, 2017, https://www.dragos.com/wp-content/uploads/CrashOverride-01.pdf.

[19] Andy Greenberg, 'The Untold Story of the 2018 Olympics Cyberattack, the Most Deceptive Hack in History,' *Wired*, October 17, 2019, https://www.wired.com/story/untold-story-2018-olympics-destroyer-cyberattack/.

[20] Ibid.

Spotlight Case Study: Sandworm's deployment of NotPetya

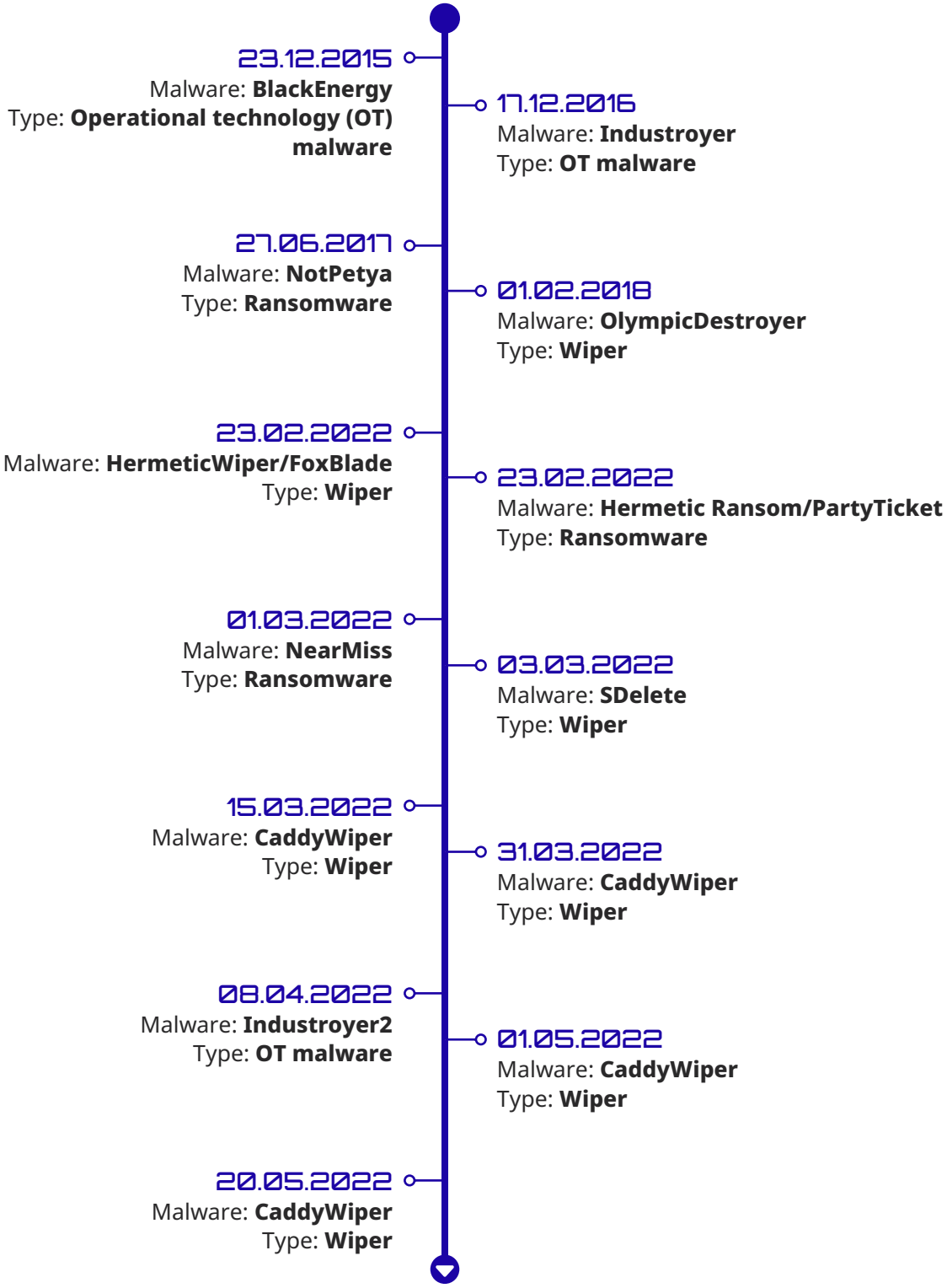
In this operation, Sandworm infiltrated the update servers of Linkos Group, a Ukrainian software provider, to insert backdoors into the systems of its clients worldwide. Once deployed, NotPetya masqueraded as ransomware, demanding payment for decryption. However, unlike its predecessor, Petya, it lacked decryption functionality altogether, rendering any ransom payments meaningless.

The malware's spread was rapid and indiscriminate, causing catastrophic damage to multinational corporations, including Maersk, Saint-Gobain, Mondelēz, Reckitt, and TNT Express. Even Russian state-owned companies, such as Rosneft, fell victim to the campaign, underscoring the collateral damage of such aggressive tactics. NotPetya exemplified how ransomware – or, in this case, its imitation – could serve as a tool for geopolitical disruption, particularly in Russia's ongoing conflict with Ukraine.

Following its full-scale invasion of Ukraine in 2022, Russia intensified its use of ransomware in targeted campaigns. For example, Sandworm deployed Prestige ransomware against transportation and logistics firms in Ukraine and Poland.[21] This attack likely aimed to disrupt supply routes essential to Ukraine's defense, demonstrating how ransomware can be weaponised for military objectives.

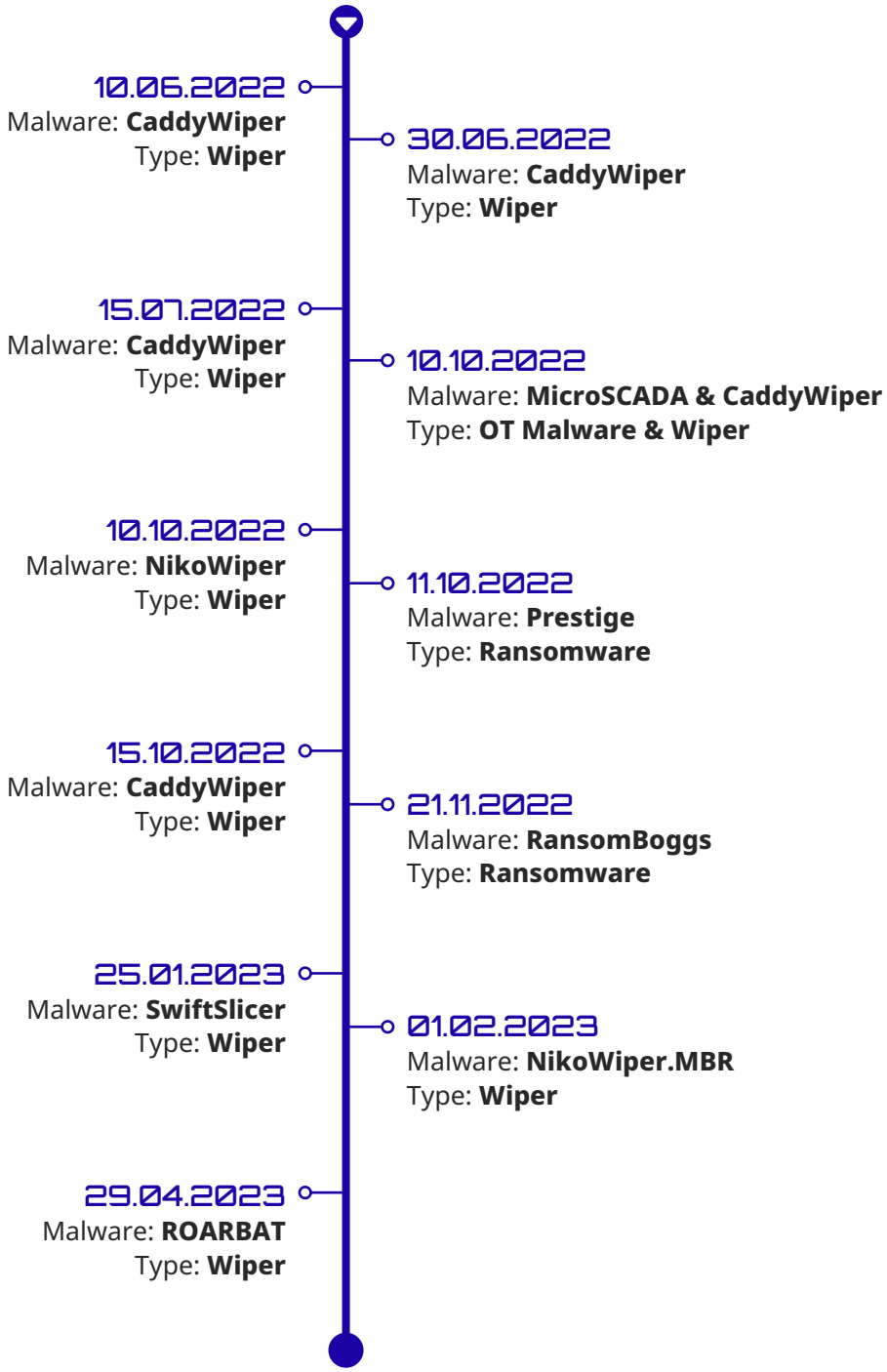
[21] Microsoft Threat Intelligence, 'New "Prestige" ransomware impacts organizations in Ukraine and Poland,' October 14, 2022, https://www.microsoft.com/en-us/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-and-poland/.

The scaling up of Sandworm's operations makes it increasingly difficult to track its full scope of activity. Below, we provide a detailed overview based on publicly available reporting.[22]



[22] For an alternative case of Russian state-linked use of (pseudo-)ransomware see WhisperGate. CISA, 'Update: Destructive Malware Targeting Organizations in Ukraine,' April 8, 2022, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-057a. Also see for an overview of Sandworm's activity following the further invasion of Ukraine: Gabby Roncone, Dan Black, John Wolfram, Tyler McLellan, Nick Simonian, Ryan Hall, Anton Prokopenkov, Dan Perez, Lexie Aytes, Alden Wahlstrom, 'APT44: Unearthing Sandworm,' *Mandiant*, April 2024, https://services.google.com/fh/files/misc/apt44-unearthing-sandworm.pdf

[23] Bilyana Lilly and Joe Cheravitch, 'The Past, Present, and Future of Russia's Cyber Strategy and Forces,' in *2020 12th International Conference on Cyber Conflict (CyCon)* (2020 12th International Conference on Cyber Conflict (CyCon), Estonia: IEEE, 2020), 129-55, https://doi.org/10.23919/CyCon49761.2020.9131723.



Cybersecurity analysts Bilyana Lilly and Joe Cheravitch observe that, 'the GRU's seemingly high tolerance for operational risk is in many ways incongruent with the traditionally furtive realm of cyber operations, which consist far more often of quiet espionage efforts than large-scale attacks.'[23] The GRU's use of ransomware fits that pattern. Sandworm has primarily deployed ransomware in Ukraine to accelerate the operational tempo of attacks amidst the war.

[23] Bilyana Lilly and Joe Cheravitch, 'The Past, Present, and Future of Russia's Cyber Strategy and Forces,' in *2020 12th International Conference on Cyber Conflict (CyCon)* (2020 12th International Conference on Cyber Conflict (CyCon), Estonia: IEEE, 2020), 129-55, https://doi.org/10.23919/CyCon49761.2020.9131723.

North Korea

In the early 2010s, North Korea's cyber activity was associated with disruptive and destructive operations, particularly those conducted by the Lazarus Group (also known as APT38, Hidden Cobra, or Labyrinth Chollima). Known for its bold campaigns, the group has carried out large-scale distributed denial-of-service (DDoS) attacks, such as the 'Ten Days of Rain' in 2011, and deployed wiper malware in incidents like the 2013 Jokra attacks on South Korean broadcasters and financial institutions and the 2014 Destover attack on Sony Pictures.[24]

This activity began to shift with the WannaCry ransomware campaign. Formally attributed by the United States government and others to North Korea, this campaign commenced in May 2017.[25] Later versions featured capability improvements, notably a ransomware payload capable of self-propagation through the abuse of the leaked EternalBlue Server Message Block (SMB) exploit.[26] Despite causing significant disruption worldwide – Europol identified over 200,000 impacted machines across 150 countries at the campaign's peak – the attackers received minimal financial gains.[27] This outcome is attributed to several factors: security researchers quickly activated a 'killswitch' embedded in the malware to stop its encryption activity;[28] the ransom demand was relatively low, at $300; the payment and decryption process was manual and ill-suited to the campaign's scale; and victims lacked trust that paying the ransom would lead to decryption.[29] Although a non-public advisory from the US Department of Homeland Security indicated that North Korea-linked wiper malware – tracked as SmashingCoconut – was observed in December 2017, subsequent North Korean cyber operations appear to have shifted toward ransomware.[30]

---

[24] Active since at least 2009, and potentially as early as 2007, the group has also conducted espionage campaigns such as Operation Troy (2009-2013) and efforts to steal South Korean military data in 2014.

[25] 'North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions,' US Department of Justice, September 6, 2018, https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and.

[26] CERT-EU, 'WannaCry Ransomware Campaign Exploiting SMB Vulnerability,' May 22, 2017, https://cert.europa.eu/static/SecurityAdvisories/2017/CERT-EU-SA2017-012.pdf.

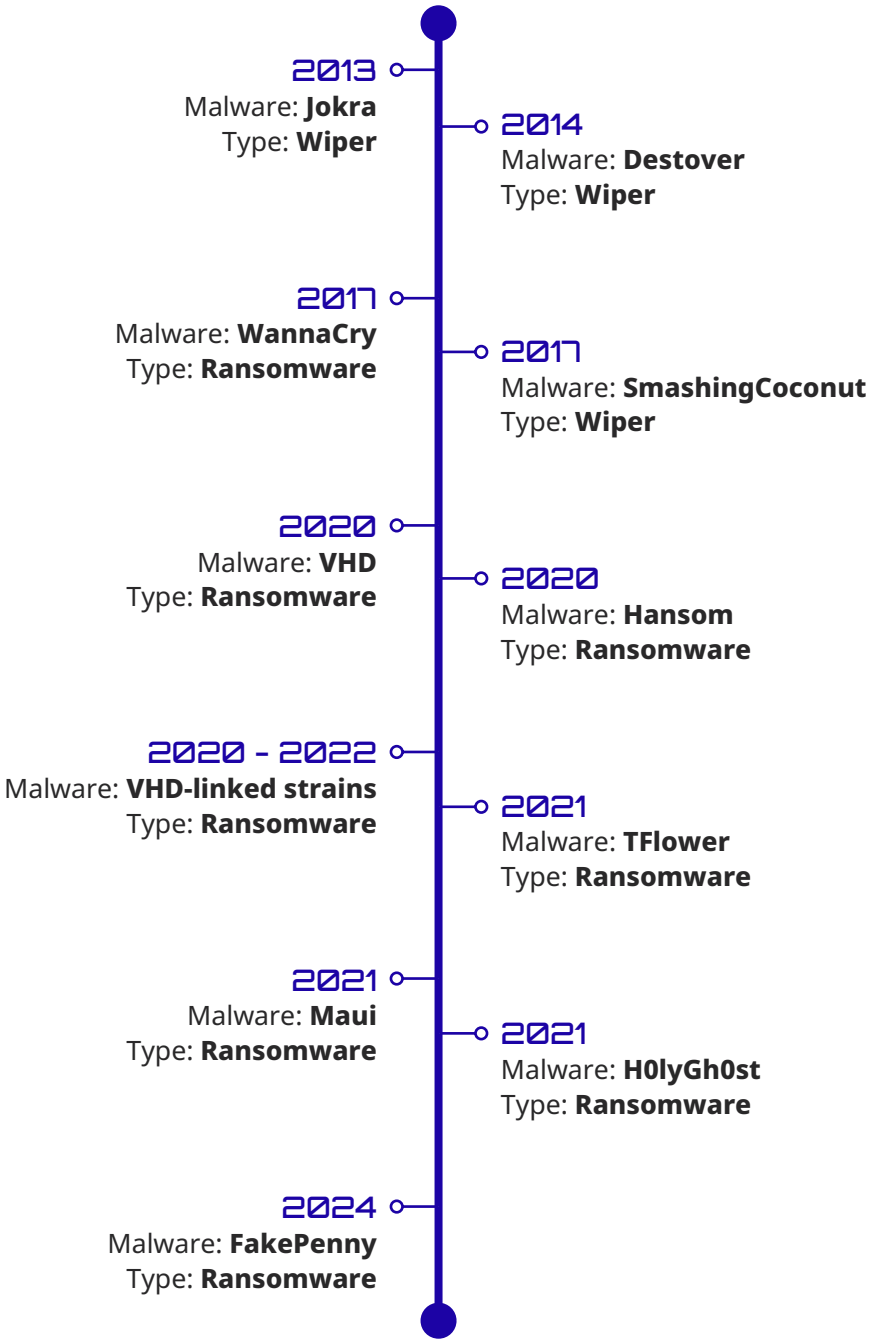
[27] Phil McCausland, Sam Petulla and Alastair Jamieson, 'Global Cyberattack Hits 150 Countries, Europol Chief Says,' *NBC News*, May 14, 2017, https://www.nbcnews.com/tech/internet/after-huge-global-cyberattack-countries-scramble-halt-spread-ransomware-n759121 ; Arjun Kharpal, 'Hackers who infected 200,000 machines have only made $50,000 worth of bitcoin,' *CNBC*, last updated May 15, 2017, https://www.cnbc.com/2017/05/15/wannacry-ransomware-hackers-have-only-made-50000-worth-of-bitcoin.html.

[28] John Miller and David Mainor (Mandiant), 'WannaCry Ransomware Campaign: Threat Details and Risk Management,' *Google Cloud Blog*, May 15, 2017, https://cloud.google.com/blog/topics/threat-intelligence/wannacry-ransomware-campaign/.

[29] Andy Greenberg, 'The WannaCry Ransomware Hackers Made Some Real Amateur Mistakes,' *Wired*, May 15, 2017, https://www.wired.com/2017/05/wannacry-ransomware-hackers-made-real-amateur-mistakes/.

[30] Elias Groll, 'North Korean Destructive Malware Is Back, Says DHS Report,' *Foreign Policy*, April 11, 2018, https://foreignpolicy.com/2018/04/11/north-korean-destructive-malware-is-back-says-dhs-report/.

An overview of North Korea-linked destructive cyber activity is provided in the overview below.



The public record of North Korean ransomware activity during the immediate post-WannaCry period is likely incomplete. However, after the WannaCry failure, North Korea-linked threat actors appeared to pause ransomware activity before tentatively resuming it around 2020, leveraging a malware framework known as Mata.[31] Around the same time, researchers observed Lazarus deploying a custom ransomware called VHD against enterprise networks.[32] Security analyses by Kaspersky concluded that VHD was not an off-the-shelf crimeware product but rather operated exclusively by Lazarus, similar to Lazarus's use of the Mata toolkit.

In a 2021 campaign, Lazarus used an updated variant of the Mata framework to distribute the TFlower ransomware strain, signaling continued ransomware experimentation. Cybersecurity firm Sygnia reported that Lazarus deployed TFlower in at least a dozen victim networks using Mata, using it to exfiltrate data for extortion, as well as encrypting data for ransom payments. Notably, TFlower ransomware first appeared in 2019 under ambiguous circumstances.[33] At the time, analysts highlighted the uncertainty surrounding its origins – raising the possibility that Lazarus might be directly operating TFlower, collaborating with its original developers, or merely impersonating the group.[34]

From mid-2021 onwards, North Korean ransomware activity surged, with North Korea-linked actor Andariel deploying ransomware variants including Maui. Microsoft also disclosed activity since June 2021 involving the H0lyGh0st ransomware variant. The threat actor responsible, Storm-0530, had clear North Korean origins and strong links with Andariel, including shared infrastructure and e-mail correspondence. Interestingly, the H0lyGh0st campaign demonstrated more advanced ransomware tradecraft than prior North Korea-linked activity, including the use of a leak site to enable double extortion via exfiltrated data.[35]

---

[31] GReAT, 'MATA: Multi-platform targeted malware framework,' Securelist, July 22, 2020, https://securelist.com/mata-multi-platform-targeted-malware-framework/97746/.

[32] Ivan Kwiatkowski, Pierre Delcher, and Félix Aime, 'Lazarus on the hunt for big game,' Securelist, July 28, 2020, https://securelist.com/lazarus-on-the-hunt-for-big-game/97757/ ; Amitai Ben Shushan et al, 'Lazarus Group's Mata Framework Leveraged To Deploy TFlower Ransomware,' Sygnia, August 1, 2021, https://www.sygnia.co/threat-reports-and-advisories/lazarus-groups-mata-framework-leveraged-to-deploy-tflower-ransomware/.

[33] GrujaRS (@GrujaRS), "New #TFlower #Ransomware does not add extensions!" X, July 30, 2019, https://x.com/GrujaRS/status/1156190042500599808.

[34] Additionally, suspected North Korea-linked ransomware campaigns from this period include 2020 cases involving the deployment of the Hansom ransomware via the Crat remote access trojan and ransomware variants such as ZZZZ and BEAF that feature code overlaps with VHD. See: Asheer Malhotra, 'CRAT wants to plunder your endpoints,' Cisco Talos, November 12, 2020, https://blog.talosintelligence.com/crat-and-plugins/ and 'The Hermit Kingdom's Ransomware play,' Trellix, May 3, 2022, https://www.trellix.com/blogs/research/the-hermit-kingdoms-ransomware-play/.

[35] Microsoft Digital Security Unit, 'North Korean threat actor targets small and midsize businesses with H0lyGh0st ransomware,' Microsoft Security (blog), July 14, 2022, https://www.microsoft.com/en-us/security/blog/2022/07/14/north-korean-threat-actor-targets-small-and-midsize-businesses-with-h0lygh0st-ransomware/.

Spotlight Case Study: Andariel

Andariel is a North Korean threat actor initially tracked as a sub-group of Lazarus and publicly attributed as a unit within the North Korean Reconnaissance General Bureau (RGB).[36] Active since at least 2015, Andariel has been observed targeting a wide range of industry verticals but is most closely associated with espionage against sensitive defence and strategic targets, with cyber operations that have included deploying ransomware.[37]

In 2021-2022, Andariel was linked to the Maui ransomware campaign that hit healthcare providers in the United States.[38] During those attacks, hospital data was encrypted for ransom, disrupting services. The US government later revealed one hospital had to divert patients due to the outage. US authorities publicly identified Andariel as behind Maui ransomware, highlighting the group's blend of financial motives with strategic targeting of critical sectors.

Mandiant now tracks Andariel as APT45, noting that the group 'engages in cybercrime to fund their operations, including the ransoming of hospitals, using their own ransomware malware dubbed Maui'.[39] At the same time, Andariel's key mandate remains intelligence collection (for example, targeting defense and government data).[40] The dual nature of its operations has led to US sanctions and indictments. In 2022, the US Treasury sanctioned Andariel as part of the North Korean state apparatus, and in 2024 an FBI indictment charged an Andariel operative for ransomware attacks on US hospitals.[41]

Furthermore, North Korean actors have leveraged a wide range of publicly available encryption tools in ransomware activity, including LockBit 2.0 and Ryuk, as well as masquerading as the REvil ransomware operation.[42]

---

[36] 'North Korean Government Hacker Charged for Involvement in Ransomware Attacks Targeting U.S. Hospitals and Health Care Providers.' United States Department of Justice. July 25, 2024. https://www.justice.gov/archives/opa/pr/north-korean-government-hacker-charged-involvement-ransomware-attacks-targeting-us-hospitals.

[37] Bill Toulas, 'Maui Ransomware Operation Linked to North Korean 'Andariel' Hackers,' *BleepingComputer*, August 9, 2022, https://www.bleepingcomputer.com/news/security/maui-ransomware-operation-linked-to-north-korean-andariel-hackers/.

[38] Ibid.

[39] Michael Barnhart, Austin Larsen, Jeff Johnson, Taylor Long, Michelle Cantos, and Adrian Hernandez (Mandiant), 'Assessed Cyber Structure and Alignments of North Korea in 2023.' *Google Cloud Blog*, October 10, 2023, https://cloud.google.com/blog/topics/threat-intelligence/north-korea-cyber-structure-alignment-2023.

[40] Cybersecurity and Infrastructure Security Agency, 'Cybersecurity Alerts & Advisories | CISA.' March 28, 2025. https://www.cisa.gov/news-events/cybersecurity-advisories.

[41] Office of Public Affairs, 'North Korean Government Hacker Charged for Involvement in Ransomware Attacks Targeting U.S. Hospitals and Health Care Providers.'

[42] Cybersecurity and Infrastructure Security Agency, '#StopRansomware: Ransomware Attacks on Critical Infrastructure Fund DPRK Malicious Cyber Activities.' February 9, 2023, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-040a.

Most recently, Microsoft has disclosed activity by novel North Korean actor Moonstone Sleet involving the deployment of the FakePenny ransomware variant since April 2024. The ransom demands made in FakePenny cases are significantly higher than in historical North Korean ransomware cases, with one demand amounting to over $6 million in Bitcoin.[43]

The primary objective of North Korean ransomware use appears to be financial gain. In the past, North Korea has relied on wiper usage as a valuable tool against adversaries. However, as North Korea increasingly uses cyber capabilities for financial gain, ransomware has become much more useful to the regime than destructive malware. Successive actions by the US Office of Foreign Assets Control over the last half decade have illustrated the strategic importance of illicit cyber-enabled financial activity for the North Korean state. A 2019 series of sanctions targeting North Korean cyber threat actors, for example, cited 'revenue streams and cyber-enabled thefts that also potentially fund North Korea's weapons of mass destruction (WMD) and ballistic missile programs.' [44] A 2023 US government assessment suggested that around half of the North Korean ballistic missile program was believed to be funded by cyber-enabled theft and extortion.[45]

However, the extent to which North Korea-linked ransomware activity is driven by strategic financial objectives remains unclear. The 2024 US Department of Justice indictment of Andariel's ransomware activity, for example, stated that the proceeds from health sector targeting had been used to fund intrusions against strategic target sets of espionage interest. The indictment specifically cited the use of ransom proceeds to pay for services such as renting virtual private servers.[46]

This suggests that at least some portion of North Korea-linked ransomware activity in recent years may have been undertaken by individual hackers as a means by which to fund their own operations, rather than feeding into national-level programs. Assessing the prevalence of financially motivated activity by diverse North Korea-linked groups in recent years, including those not assessed as having an explicit financial tasking, researchers have suggested that this may be indicative of a broader expectation on the part of the North Korean regime that these groups should self-finance their operations where possible.[47]

Analyses of historical North Korea-linked ransomware activity have emphasised their low profitability, especially when compared to other cyber-enabled revenue sources like cryptocurrency exchange breaches (which were estimated to have generated $1.3 billion for North Korea in 2024).[48] However,

---

[43] Microsoft Threat Intelligence, 'Moonstone Sleet emerges as new North Korean threat actor with new bag of tricks,' Microsoft Security (blog), May 28, 2024, https://www.microsoft.com/en-us/security/blog/2024/05/28/moonstone-sleet-emerges-as-new-north-korean-threat-actor-with-new-bag-of-tricks/.

[44] 'Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups,' US Department of the Treasury, September 13, 2019, https://home.treasury.gov/news/press-releases/sm774.

[45] Sean Lyngaas, 'Half of North Korean missile program funded by cyberattacks and crypto theft, White House says,' *CNN*, May 10, 2023, https://edition.cnn.com/2023/05/10/politics/north-korean-missile-program-cyberattacks/index.html.

[46] 'North Korean Government Hacker Charged for Involvement in Ransomware Attacks Targeting U.S. Hospitals and Health Care Providers.'

[47] Fred Plan, Van Ta, Michael Barnhart, Jeff Johnson, Dan Perez, and Joe Dobson (Mandiant), 'APT43: North Korean Group Uses Cybercrime to Fund Espionage Operations,' *Google Cloud Blog*, March 28, 2023, https://cloud.google.com/blog/topics/threat-intelligence/apt43-north-korea-cybercrime-espionage.

[48] Owen Walker, 'North Korea stole $1.3bn through crypto hacks in 2024,' *Financial Times*, December 19, 2024, https://www.ft.com/content/4ed7ce45-a653-496e-99a6-ade9c21f9908.

recent developments in North Korea-linked ransomware such as the adoption of leak sites in the H0lyGh0st campaign of 2021 and the significant increase in ransom demands by Moonstone Sleet may indicate a renewed interest in establishing ransomware as a more effective revenue stream.

Recent North Korean ransomware activity has increasingly drawn on practices and connections from the broader international cybercriminal ecosystem. In addition to adopting standard tactics like double extortion, the Andariel subgroup is suspected to have operated as an initial access broker or affiliate for the Play ransomware operation, which is believed to have links to Russia.[49] Separately, a 2024 US Department of Justice indictment revealed that North Korean IT workers involved in illicit overseas employment schemes had extorted victims using stolen data – without deploying ransomware – mirroring tactics seen in 'data-theft extortion' campaigns by groups such as Babuk.[50]

This kind of engagement with the international cybercrime ecosystem expands North Korea's operational toolkit beyond the development and deployment of custom ransomware. By integrating into pre-existing value chains and leveraging the innovations of other threat actors, North Korean groups gain access to new monetization tactics and operational models.

Over the past decade, North Korea's cyber strategy has shifted away from early destructive wiper campaigns toward the more lucrative use of ransomware. While the 2017 WannaCry outbreak remains the most high-profile example, more recent developments reveal significant evolution. North Korean actors have matured their technical capabilities – such as launching and maintaining data leak sites – and embraced international cybercriminal trends both as revenue opportunities and sources of best practices.

Looking ahead, this trajectory is likely to continue. North Korean ransomware operations are expected to keep evolving, increasingly supplementing other revenue streams such as cryptocurrency thefts, which the regime relies on for financial stability and strategic autonomy. The strong financial incentives behind these operations make it likely that North Korean threat actors will deepen their integration into global cybercriminal value chains – pursuing an adaptive approach that blends homegrown development, operational experimentation, and partnerships with cybercriminal networks.

[49] Unit 42, 'Jumpy Pisces Engages in Play Ransomware,' *Unit 42 by Palo Alto Networks* (blog), October 30, 2024, https://unit42.paloaltonetworks.com/north-korean-threat-group-play-ransomware/.

[50] Ionut Ilascu, 'Babuk quits ransomware encryption, focuses on data-theft extortion,' *BleepingComputer*, April 30, 2021, https://www.bleepingcomputer.com/news/security/babuk-quits-ransomware-encryption-focuses-on-data-theft-extortion/.

China

China has long been recognised as a dominant force in the global cyber threat landscape, particularly in cyberespionage. Its hacking ecosystem features a network of interconnected groups, including private sector entities that play a pivotal role in enabling state-linked operations.

Chinese state-linked actors have a history of suspected ransomware use, with the earliest publicly documented instance dating back to 2016.[51] The assessed objectives behind these activities primarily include financial gain and disruption. The individuals involved range from private-sector employees moonlighting as cybercriminals for extra income to well-organised teams tied to state agencies, such as the Ministry of State Security and the Ministry of Public Security.

Chinese state-linked actors also deploy ransomware in cyberespionage campaigns, serving as a tool for distraction, misattribution, or evidence removal. These tactics can be difficult to distinguish from typical criminal operations due to shared methods, such as data exfiltration followed by ransomware deployment. However, in espionage scenarios, this process is often used not for double extortion but to steal data and erase evidence once the target's intelligence value has been exploited.

The i-Soon leak offers rare insights into the private sector companies hired to support Chinese state intelligence demands, highlighting grueling work conditions and low pay.[52] For example, despite its formal prohibition in 2021, the '996' work schedule (9 am to 9 pm, six days a week) likely remains widespread in China's technology sector.[53] Such pressures may push individuals involved in state-linked operations to engage in ransomware activities for supplemental income. Notably, in 2019, Mandiant (now part of Google Cloud) reported on APT41, a suspected Chinese umbrella cluster whose cyberespionage and criminal activities included a ransomware attack on the video gaming industry for personal profit.[54] As part of its attacks, APT41 has manipulated virtual currencies, exploited in-game transaction systems, and deployed the Encryptor RaaS ransomware.

In this context, ransomware actors may hand off access to cyberespionage groups or sell it. In 2022, cybersecurity company Secureworks observed the suspected Chinese threat actor Bronze Starlight, which is known for deploying ransomware, suspending operations in an environment where another Chinese cluster, Bronze University, was also active.[55] This thus contrasts with the North Korean model, where the state typically acquires initial access, which is then used by affiliated criminal groups for ransomware operations.

---

[51] Joseph Menn, 'Exclusive: Chinese hackers behind U.S. ransomware attacks - security firms,' *Reuters*, March 15, 2016, https://www.reuters.com/article/us-china-ransomware-idUSKCN0WG2L5/.

[52] Dake Kang and Zen Soo,'Leak lifts lid on Chinese hacking company – a sordid culture fuelled by alcohol and sex,' *Independent*, March 8, 2024, https://www.independent.co.uk/asia/east-asia/i-soon-china-hacking-documents-b2509300.html.

[53] Siyuan Meng, 'China's burned-out tech workers are fighting back against long hours,' *MIT Technology Review*, November 15, 2021, https://www.technologyreview.com/2021/11/15/1039650/china-tech-workers-996-fight-back/.

[54] Nalani Fraser et al. (Mandiant), 'APT41: A Dual Espionage and Cyber Crime Operation,' *Google Cloud Blog*, August 7, 2019, https://cloud.google.com/blog/topics/threat-intelligence/apt41-dual-espionage-and-cyber-crime-operation/.

Spotlight Case Study: i-Soon

In February 2024, more than 500 files from Anxun Information Technology (i-Soon), a Chinese cybersecurity firm, were leaked to the public. The leak reveals i-Soon's role in conducting cyberespionage campaigns and supporting such activities by providing a range of services and tools to its clients, which include key Chinese government entities such as the Ministry of Public Security and the Ministry of State Security.[56]

I-Soon has been involved in cyber-espionage operations targeting a broad spectrum of high-value sectors, including government entities and private sector organizations globally. The leaked documents also indicate that i-Soon has developed tools for cyberespionage, such as the Treadstone remote control management software and hardware data exfiltration devices. Additionally, the documents disclose command-and-control infrastructure, offensive tooling, and victimology, which align with suspected Chinese cyber-espionage clusters tracked by the threat intelligence community, including APT41 and Poison Carp.[57]

The leaked documents indicate that the pricing of i-Soon's diverse range of services has varied depending on the complexity and scope of the operation, the size or relevance of the target, and the resources required. For example, access to the emails of ten targets for a year cost the Shandong Bureau of the Ministry of Public Security over $50,000, while data exfiltrated from Vietnam's Ministry of Economy earned them $55,000, with stolen data from other ministries priced lower.

Leaked chat logs reveal financial pressures within the company, with employees expressing dissatisfaction over low pay and hoping to secure positions at other firms. Such financial strains may drive individuals involved in cyberespionage to seek additional sources of income, potentially leading them to engage in cybercriminal activities, such as ransomware operations, in pursuit of personal financial gain.

In a 2025 indictment by the US Department of Justice, i-Soon was implicated in a series of cyber espionage operations, where employees conducted intrusions on their own initiative or at the request of the Chinese Ministry of Public Security or the Ministry of State Security.[58] This indictment highlights the company's role within China's broader hacker-for-hire ecosystem.

---

[55] Counter Threat Unit Research Team, 'BRONZE STARLIGHT Ransomware Operations Use HUI Loader,' Secureworks, June 23, 2022, https://www.secureworks.com/research/bronze-starlight-ransomware-operations-use-hui-loader.

[56] Dakota Cary and Aleksandar Milenkoski, 'Unmasking I-Soon | The Leak That Revealed China's Cyber Operations - *SentinelOne*,' SentinelOne, February 21, 2024, https://www.sentinelone.com/labs/unmasking-i-soon-the-leak-that-revealed-chinas-cyber-operations/.

[57] Unit42, 'Data From Chinese Security Services Company i-Soon Linked to Previous Chinese APT Campaigns,' *Unit 42 by Palo Alto Networks* (blog), February 23, 2024, https://unit42.paloaltonetworks.com/i-soon-data-leaks/.

[58] US Department of Justice, 'Justice Department Charges 12 Chinese Contract Hackers and Law Enforcement Officers in Global Computer Intrusion Campaigns,' press Release, March 5, 2025, https://www.justice.gov/opa/pr/justice-department-charges-12-chinese-contract-hackers-and-law-enforcement-officers-global.

Spotlight Case Study: Bronze Starlight

Bronze Starlight (also known as DEV-0401 or SLIME34) is a suspected China-based ransomware operator active since 2021. The group is known for frequently rebranding and rotating ransomware payloads, including LockFile, AtomSilo, NightSky, LockBit 2.0, and Pandora.[59] It is likely that the group operated as an affiliate of LockBit in 2022.[60]

Bronze Starlight has targeted organisations across sectors including government, manufacturing, technology, and financial services, with victims spanning North America, Europe, and Asia.

Bronze Starlight's primary objective is suspected to be espionage rather than financial gain, using ransomware as a means of distraction or misattribution. A 2022 report by Secureworks notes that the group's victimology, the short lifespan of its ransomware strains, and its use of malware associated with cyberespionage threat groups suggest that Bronze Starlight does not operate like conventional financially motivated cybercriminals.[61]

The group has typically targeted a small number of victims over short periods before ceasing operations, a pattern aligned with espionage-driven objectives. Additionally, Bronze Starlight has been observed using the HUI Loader malware loader and the PlugX backdoor in its campaigns, both of which are commonly associated with suspected Chinese cyberespionage actors.[62] HUI Loader variants have been observed in a series of cyberespionage operations attributed to suspected Chinese cyberespionage actors, including APT10, TA410, and Earth Tengshe.[63] Notably, the malware was used in a sustained A41APT campaign targeting Japanese companies and their international branches.[64]

Espionage and financial gain are not the sole drivers of ransomware operations by Chinese state-linked actors. China also uses ransomware as a tool of disruption, interfering in political agendas, bolstering strategic interests, or stoking regional rivalries. Prominent examples include the 2022 attacks by the suspected Chinese state-linked group ChamelGang against the All India Institute of

[59] Microsoft Threat Intelligence, 'Ransomware as a service: Understanding the cybercrime gig economy and how to protect yourself,' Microsoft Security (blog), May 9, 2022, https://www.microsoft.com/en-us/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/?msockid=2a82c0b73dd666c60d50d5bd3c7a67ee#DEV-0401.

[60] James Haughom, Júlio Dantas, and Jim Walter, 'LockBit Ransomware Side-loads Cobalt Strike Beacon with Legitimate VMware Utility,' *SentinelOne*, April 27, 2022, https://www.sentinelone.com/labs/lockbit-ransomware-side-loads-cobalt-strike-beacon-with-legitimate-vmware-utility/.

[61] Counter Threat Unit Research Team, 'BRONZE STARLIGHT Ransomware Operations Use HUI Loader.'

[62] Charles Li and Che Chang, 'To loot or Not to Loot? That Is Not a Question When State-Nexus APT Targets Online Entertainment Industry,' BlackHat Asia 2022, May 13, 2022, https://i.blackhat.com/Asia-22/Friday-Materials/AS-22-Li-To-Loot-Or-Not-To-Loot-That-Is-Not-a-Question.pdf.

[63] Aleksandar Milenkoski and Tom Hegel, 'Chinese Entanglement | DLL Hijacking in the Asian Gambling Sector,' *SentinelOne*, August 17, 2023, https://www.sentinelone.com/labs/chinese-entanglement-dll-hijacking-in-the-asian-gambling-sector/.

[64] Kaspersky GREAT, 'APT10: sophisticated multi-layered loader Ecipekac discovered in A41APT campaign,' Kaspersky, March 30, 2021, https://securelist.com/apt10-sophisticated-multi-layered-loader-ecipekac-discovered-in-a41apt-campaign/101519/.

Medical Sciences (AIIMS) and the Brazilian presidency.[65]

The AIIMS incident caused major healthcare disruptions, with Indian authorities labeling it as an 'act of cyber terrorism.'[66] This attack is likely part of a series of disruptive activities targeting Indian critical infrastructure presumed to be orchestrated by Chinese actors. These activities have occurred against the backdrop of ongoing tensions between India and China, primarily driven by border disputes that have led to physical altercations.[67]

Spotlight Case Study: All India Institute of Medical Sciences

AIIMS is one of India's leading healthcare, medical education, and research institutions, with multiple branches operating across the country. The institution has adopted digital initiatives like the eHospital platform, which provides patient services including online appointments, electronic medical records, and telemedicine.

A ransomware attack affecting the AIIMS New Delhi branch was first detected on November 23, 2022, when staff were unable to access the eHospital platform, forcing them to provide services manually. Government sources stated that five servers have been compromised, affecting almost all online services.[68] These services were restored after about a week, with remediation efforts involving the scanning of approximately 5,000 workstations and servers to determine the extent of the impact. The potential theft of patient data was a major concern, as AIIMS treats high-profile individuals including top political leaders, bureaucrats, and judges. Intelligence and anti-terror agencies, along with IT emergency teams, were involved in the investigation.

The attack against the AIIMS has led Indian government sources to suggest a possible link to China. However, Indian authorities have not publicly released technical indicators to allow for external investigation and verification of this connection. Only a few limited technical details, sourced from an Indian police report , have been shared by the media, including some email addresses and filename extensions used by the attackers.[69]

[65] Aleksandar Milenkoski and Julian-Ferdinand Vögele, 'ChamelGang & Friends | Cyberespionage Groups Attacking Critical Infrastructure with Ransomware,' *SentinelOne*, June 26, 2024, https://www.sentinelone.com/labs/chamelgang-attacking-critical-infrastructure-with-ransomware/.

[66] HT News Desk, 'AIIMS server outage being probed as 'cyber terrorism': Delhi Police,' *Hindustan Times*, November 24, 2022, https://www.hindustantimes.com/cities/delhi-news/aiims-server-outage-being-probed-as-cyber-terror-act-delhi-police-101669308187997.html.

[67] Sahil Joshi and Divyesh Singh, 'Mega Mumbai power outage may be result of cyber attack, final report awaited,' *India Today*, November 20, 2020, https://www.indiatoday.in/india/story/mumbai-power-outage-malware-attack-1742538-2020-11-20.

[68] Arvind Gunasekar, 'AIIMS Delhi Servers Were Hacked By Chinese, Damage Contained: Sources,' *NDTV*, December 14, 2022, https://www.ndtv.com/india-news/aiims-delhi-server-attack-was-by-chinese-5-physical-servers-infiltrated-by-hackers-data-retrieved-now-government-sources-3605639.

[69] Karn Pratap Singh, 'Ransomware attack: Report flags host of security lapses at AIIMS,' *Hindustan Times*, December 7, 2022, https://www.hindustantimes.com/cities/delhi-news/report-flags-host-of-security-lapses-at-aiims-101670359251255.html.

In June 2024, SentinelLABS released a report highlighting strong indicators that AIIMS was targeted in November 2022 using the CatB ransomware.[70] This ransomware, also referred to as CatB99 or Baxtoy, was first observed in late 2022.

In 2023, cybersecurity company TeamT5 linked CatB ransomware to the suspected China-based threat actor ChamelGang, also known as CamoFei.[71] TeamT5 associates CatB with ChamelGang based on shared code, malware staging mechanisms, and artifacts found in custom malware used in intrusions attributed to this actor.

ChamelGang's victimology includes organisations in critical infrastructure sectors such as healthcare, energy, and government. The group has targeted entities in multiple regions, including Russia, Taiwan, the United States, and India, indicating a strategic interest in high-value targets.

The AIIMS aligns with ChamelGang's objectives, as the institution is a critical repository of sensitive patient data, medical research, and government health records, making it a prime target for cyberespionage. Additionally, given its central role in India's healthcare system, disrupting the operations of the AIIMS further aligns with the group's goals of destabilising critical systems.

In the case of the presidency of Brazil, indicators suggest that the ransomware activity was first detected on November 1, 2022, during the presidential elections in which then-President Jair Bolsonaro was a candidate. Bolsonaro's rhetoric towards China has not always been favorable, which may have played a role in the timing of the attack.[72]

It is highly likely that the ChamelGang's CatB ransomware was used in the attack. A CatB ransom note was included in files uploaded from Brazil to a malware sharing platform on November 1, 2022, the same day Brazilian authorities first detected the malicious activity within the presidency's network. These uploaded files included relevant artifacts, such as the domain presidencia.gov.br. In addition, the same ransom note was cited by Brazilian authorities, who publicly shared technical information about the intrusion some time after the attack.

Similarly, concerns about disruption driven by geopolitical motivations were raised following a ransomware attack targeting the government of Palau.[73] The attack occurred on March 14, 2024, the

[70] Milenkoski and Vögele, 'ChamelGang & Friends | Cyberespionage Groups Attacking Critical Infrastructure with Ransomware.'

[71] Still Tsu and Zih-Cing Liao, 'Unmasking CamoFei: An In-depth Analysis of an Emerging APT Group Focused on Healthcare Sectors in East Asia,' HITCON Conference, August 18, 2023, https://hitcon.org/2023/CMT/slide/Unmasking%20CamoFei_An%20In-depth%20Analysis%20of%20an%20Emerging%20APT%20Group%20Focused%20on%20Healthcare%20Sectors%20in%20East%20Asia.pdf.

[72] Despite thriving trade, China's relationship with Brazil is weakening,' *Economist*, February 12, 2022, https://www.economist.com/the-americas/2022/02/12/despite-thriving-trade-chinas-relationship-with-brazil-is-weakening.

[73] Jonathan Graig, "An attack on the reputation of Palau': officials question who was really behind ransomware incident,' *Record*, April 4, 2024, https://therecord.media/palau-attack-who-was-behind-china-us.

same day as a ceremony commemorating the relationship between Palau and the United States, during a period of strained relations with China. The ransom notes contained invalid links for negotiation, further deepening suspicions that the motives behind the attack might not have been financial. Although the perpetrators, DragonForce ransomware, denied having any motives other than financial gain and claimed to have contacted Palauan authorities to discuss ransom terms, the government of Palau refuted their claim of contact.[74] Recent research suggests that DragonForce operated as an independent ransomware group at the time of the attack and evolved into a RaaS program in June 2024.[75] The suspicious circumstances surrounding the attack raise doubts about whether DragonForce's true motivation was financial gain or if the attack was a deliberate act of disruption.

China has consistently blamed uncovered ransomware incidents on independent cybercriminal groups, asserting that Western threat intelligence lacks concrete evidence for direct attribution. For instance, when approached about the ChamelGang ransomware activities, a spokesperson for the Chinese embassy in Washington, DC, stated 'We [...] underscore the importance of having enough evidence when identifying cyber-related incidents, rather than making groundless speculations and allegations.'[76]

Moreover, in 2024, China's Computer Virus Emergency Response Center (CVERC) released a report labeling the cyberespionage actor Volt Typhoon a ransomware group – a claim that contradicts available evidence and can be interpreted as an attempt by China to portray its cyberespionage operations as cybercriminal in nature.[77]

This report is part of a broader effort by the CVERC, which has released multiple reports asserting that the U.S. government, rather than China, is behind Volt Typhoon. Such efforts are a component of China's offensive media strategy, aimed at international audiences and directing focus toward U.S. offensive cyber operations. The strategy is likely a response to a series of public statements and reports from Western governments and private-sector cybersecurity companies regarding China's offensive behavior in cyberspace. However, reports originating from Chinese sources often lack technical detail and supporting evidence.[78]

China will likely continue publicly distancing itself from state-aligned activities, framing them as actions of independent cybercriminals to deflect international scrutiny and avoid accountability. While the cyber threat intelligence community has been able to attribute ransomware attacks to Chinese

[74] Jonathan Graig, "They're lying': Palau denies claims by ransomware gang over recent cyberattack,' *Record*, April 8, 2024, https://therecord.media/palau-denies-ransomware-gang-claims.

[75] Nikolay Kichatov, Sharmine Low, and Alexey Kashtanov, "Inside the Dragon: DragonForce Ransomware Group," Group-IB, September 25, 2024, https://www.group-ib.com/blog/dragonforce-ransomware/.

[76] A.J. Vicens, 'Chinese hackers are increasingly deploying ransomware, researchers say,' *Cyberscoop*, June 26, 2024, https://cyberscoop.com/chinese-hackers-are-increasingly-deploying-ransomware-researchers-say/.

[77] Computer Virus Emergency Response Center, 'Volt Typhoon□A Conspiratorial Swindling Campaign Targets with U.S. Congress and Taxpayers Conducted by U.S. Intelligence Community,' April 15, 2024, https://www.cverc.org.cn/head/zhaiyao/futetaifengEN.pdf.

[78] Dakota Cary, 'China's Cyber Revenge | Why the PRC Fails to Back Its Claims of Western Espionage, ' *SentinelOne*, February 12, 2024, https://www.sentinelone.com/labs/chinas-cyber-revenge-why-the-prc-fails-to-back-its-claims-of-western-espionage/; also see: Chung-Kuan Chen and Valentin Weber, 'China's Expanding Cyber Playbook: Espionage, Fear, and Influence in East Asia,' policy paper, December 2024, final_a4_policy-paper_chinas-expanding-cyber-playbook-1-1.pdf

clusters based on custom malware and infrastructure overlaps, the growing use of legitimate tools, commodity malware, and disposable infrastructure may complicate attribution and efforts to hold China accountable. Tactics such as those used by Bronze Starlight – frequent rebranding, deploying diverse ransomware families, and even operating as ransomware affiliates – add an additional layer of obscurity to the threats posed by Chinese actors, challenging the traditional distinction between cybercrime and cyberespionage.

Iran

Iran has a long history of disruptive and destructive cyber operations, both as target and perpetrator. Over the years, the country has been hit by numerous cyber incidents. These include wiper attacks on its national railway system, political billboard defacements, and the infamous Stuxnet malware – allegedly developed by US and Israeli intelligence to sabotage nuclear centrifuges. More recently, a cyberattack on a steel plant was attributed to the hacktivist group Predatory Sparrow, reportedly linked to Israel.[79]

At the same time, Iran-linked groups have carried out destructive cyber operations of their own. This began with the 2012 Shamoon wiper attack on Saudi Aramco, Saudi Arabia's national oil company. Several other major attacks followed, including Shamoon 2.0 and Stonedrill in 2016.[80]

Analyzing cyber operations linked to Iran is challenging due to the lack of public disclosure about its cyber offensive doctrine and the complexity of the ecosystem of state-linked Iranian groups.[81] While most of these groups operate under the oversight of two main intelligence and security organizations – the Islamic Revolutionary Guard Corps (IRGC) and the Ministry of Intelligence (MOIS) – this ecosystem includes a vast number of proxy groups, private contractors, universities, and recruitment facilities.

This includes the Ravin Academy, a facility to train and recruit offensive operators for the MOIS. The 2018 SamSam case highlights how the exact connections, motivations, and entities behind attacks are not always fully apparent.[82]

---

[79] Juan Andrés Guerrero-Saade, 'MeteorExpress | Mysterious Wiper Paralyzes Iranian Trains with Epic Troll,' *SentinelOne*, July 29, 2021, https://www.sentinelone.com/labs/meteorexpress-mysterious-wiper-paralyzes-iranian-trains-with-epic-troll/; James Shires, Max Smeets, and Hannah-Sophie Weber, 'Predatory Sparrow: cyber sabotage with a conscience?,' Binding Hook, December 9, 2024, https://bindinghook.com/articles-binding-edge/predatory-sparrow-cyber-sabotage-with-a-conscience/

[80] Charlie Osborne, 'Shamoon data-wiping malware believed to be the work of Iranian hackers,' ZDNET, December 19, 2018, https://www.zdnet.com/article/shamoons-data-wiping-malware-believed-to-be-the-work-of-iranian-hackers; Kaspersky, 'From Shamoon to Stonedrill: Wipers attacking Saudi organizations and beyond,' Kaspersky, March 7, 2017, https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180722/Report_Shamoon_StoneDrill_final.pdf.

[81] Maxime A. and Sekoia TDR, 'Iran Cyber Threat Overview,' *Sekoia.io Blog*, June 5, 2023, https://blog.sekoia.io/iran-cyber-threat-overview/.

[82] Charlie Cullen, 'The Men Who Never Were: Assessing Ties Between the Samsam Ransomware Campaign and the IRGC,' BSidesAtlanta 2020, March 27, 2020, https://citation.thinkst.com/talk/75445.

Spotlight Case Study: SamSam

Over a span of almost three years, the SamSam ransomware – ultimately identified as being distributed by Iranian nationals – hit more than 200 victim organisations across the US, UK, and Canada.[83]

High-profile targets included city governments, such as Atlanta, which had courts and services knocked offline for days, and major hospital networks.[84] The impact was significant: a 2016 SamSam attack forced Hollywood Presbyterian Medical Center in Los Angeles to divert patients to other hospitals when its systems were encrypted.[85]

In November 2018, the US Department of Justice unsealed an indictment charging two Iranian men – Faramarz Shahi Savandi and Mohammad Mehdi Shah Mansouri – as the authors and deployers of SamSam. The indictment described an 'Iran-based international computer hacking and extortion scheme', underscoring that the attacks were launched from Iranian soil.[86] However, the US stopped short of officially attributing SamSam to the Iranian government. Instead, the two men were indicted as cybercriminals motivated by personal gain, even as their activities aligned with Tehran's interests by sowing chaos in Western infrastructure. Notably, the US Treasury Department simultaneously sanctioned two Iran-based individuals who helped convert SamSam's bitcoin ransoms into Iranian rials.[87]

A US Treasury official stated that as Iran faces economic isolation, its 'cyber actors' exploit ransomware payments to further 'nefarious objectives' of the regime.[88]

The first documented ransomware activity attributed to Iran was Operation Quicksand, reported on in October 2020.[89] This campaign, attributed to MuddyWater – a contractor associated with the MOIS – used Thanos ransomware in destructive attacks against state-run organizations across the Middle East and North Africa.

---

[83] Office of Public Affairs. 'Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals, Municipalities, and Public Institutions, Causing Over $30 Million in Losses.' United States Department of Justice, November 28, 2018, https://www.justice.gov/archives/opa/pr/two-iranian-men-indicted-deploying-ransomware-extort-hospitals-municipalities-and-public.

[84] *Reuters*, 'U.S. Indicts Iranian Hackers Responsible for Deploying 'SamSam' Ransomware,' *Euronews*, November 28, 2018, https://www.euronews.com/2018/11/28/us-pressures-iran-with-sanctions-indictments-for-ransomware-scheme.

[85] Ibid.

[86] Office of Public Affairs, 'Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals, Municipalities, and Public Institutions, Causing Over $30 Million in Losses.'

[87] Michael Heller, SamSam Ransomware Actors Charged, Sanctioned by US Government, Search Security, Tech Target, accessed March 31, 2025, https://www.techtarget.com/searchsecurity/news/252453483/SamSam-ransomware-actors-charged-sanctioned-by-US-government.

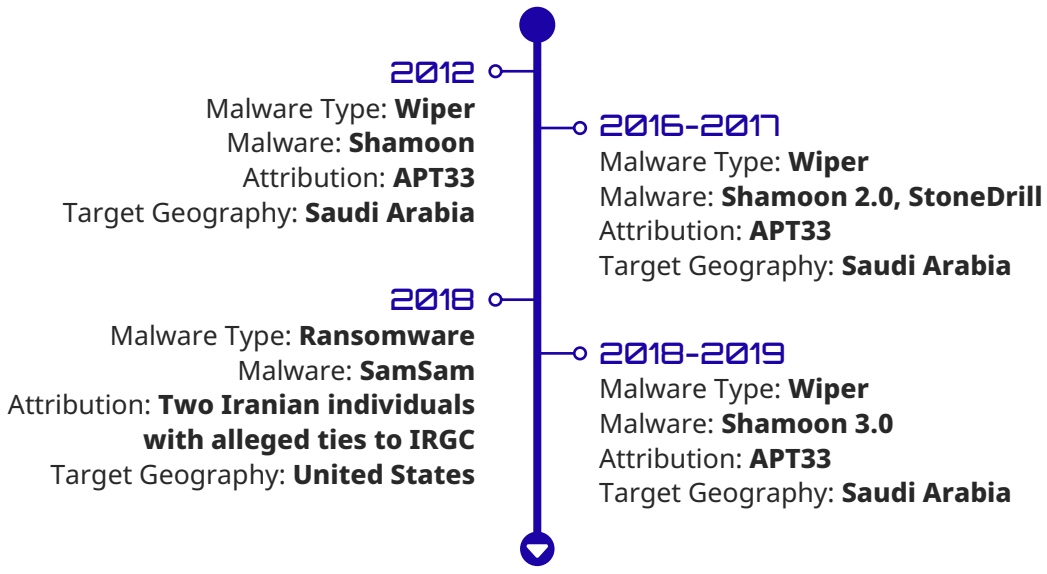
[88] Ibid.

[89] ClearSky, 'Operation Quicksand: MuddyWater's Offensive Attack Against Israeli Organizations,' October 2020, https://www.clearskysec.com/wp-content/uploads/2020/10/Operation-Quicksand.pdf

In the years after, many of the ransomware attacks conducted by Iran sought to impact Israel. A notable example is the Pay2Key campaigns in 2020, attributed to Fox Kitten. These operations aimed to incite panic in Israel through public threats and propaganda, as the group leaked stolen data instead of demanding ransom, emphasising psychological impact over financial gain. Similarly, in February 2023, a group called DarkBit targeted the Israel Institute of Technology, forcing it to shut down IT systems and postpone exams. They demanded 80 bitcoins ($1.7 million) and issued an ideologically charged note condemning Israel's actions as 'an apartheid regime' and stating that they should 'pay for occupation, war crimes against humanity, killing the people (not only Palestinians' bodies, but also Israelis' souls).'[90] Israel's National Cyber Directorate later attributed the attack to MuddyWater.[91]

State-linked Iranian groups have also used ransomware tactics in response to geopolitical events. In July 2022, the group HomeLand Justice – believed to be a collaboration between multiple Iran-linked actors – conducted an attack against the government of Albania.[92] During the operation, the group deployed a ransomware-style file encryptor alongside disk-wiping malware, disrupting websites and essential services. In addition to causing operational damage, the attack carried a clear political message: infected systems displayed an anti-Mujahedin-e-Khalq (MEK) statement criticising Albania's decision to host the Iranian dissident organization. The message, 'Why should our taxes be spent on the benefit of DURRES terrorists?' underscored the broader political motivations behind the campaign.[93]

The following timeline provides a more detailed overview of the wiper and ransomware activity.



[90] Alexander Martin, 'Israel blames state-sponsored Iranian hackers for ransomware attack on university,' *Record*, March 7, 2023, https://therecord.media/israel-technion-ransomware-attack-iran-darkbit-muddywater

[91] Israel National Cyber Directorate, 'Iranian Government-Sponsored Threat Actor MuddyWater Conducts Cyber Attack Against Israel,' Gov.il, March 9, 2023, https://www.gov.il/en/pages/_muddywater

[92] Cybersecurity and Infrastructure Security Agency, 'Iranian State Actors Conduct Cyber Operations Against the Government of Albania,' September 23, 2022, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-264a

[93] Ravie Lakshmanan, 'Iranian Hackers Likely Behind Disruptive Cyberattacks Against Albanian Government,' *Hacker News*, August 5, 2022, https://thehackernews.com/2022/08/iranian-hackers-likely-behind.html

2019
Malware Type: **Wiper**
Malware: **ZeroCleare**
Attribution: **APT34, xHunt**
Target Geography: **Arabian Peninsula**

2019
Malware Type: **Wiper**
Malware: **Dustman**
Attribution: **APT34, xHunt**
Target Geography: **Arabian Peninsula**

2020
Malware Type: **Pseudo-ransomware**
Malware: **Thanos Ransomware**
Attribution: **MuddyWater**
Target Geography: **Israel**

2020
Malware Type: **Ransomware**
Malware: **Pay2Key**
Attribution: **Fox Kitten**
Target Geography: **Israel**

2021
Malware Type: **Ransomware**
Malware: **N3tw0rm**
Attribution: **N3tw0rm**
Target Geography: **Israel**

2021
Malware Type: **Pseudo-Ransomware**
Malware: **Apostle, Deadwood**
Attribution: **Agrius**
Target Geography: **Israel**

2021
Malware Type: **Pseudo-Ransomware**
Malware: **Apostle**
Attribution: **Agrius**
Target Geography: **Israel**

2021
Malware Type: **Ransomware**
Malware: **BitLocker**
Attribution: **IRGC-affiliated group comprised of employees and associates of Najee Technology Hooshmand Fater LLC and Afkar System Yazd Company**
Target Geography: **United States**

2022
Malware Type: **Ransomware, Wiper**
Malware: **Unknown**
Attribution: **HomeLand Justice**
Target Geography: **Albania**

2022
Malware Type: **Ransomware, Wiper**
Malware: **Unknown**
Attribution: **Unknown**
Target Geography: **Albania**

2023
Malware Type: **Ransomware**
Malware: **DarkBit**
Attribution: **MuddyWater**
Target Geography: **Israel**

2023
Malware Type: **Wiper**
Malware: **Various wipers**
Attribution: **Agrius**
Target Geography: **Israel**

2023
Malware Type: **Ransomware**
Malware: **Crucio Ransomware**
Attribution: **Soldiers of Solomon**
Target Geography: **Israel**

2023
Malware Type: **Pseudo-ransomware**
Malware: **Moneybird**
Attribution: **Agrius**
Target Geography: **Israel**

2024
Malware Type: **Ransomware**
Malware: **Unknown**
Attribution: **Pioneer Kitten**
Target Geography: **United States**

State-linked Iranian groups also appear to use ransomware to cause misattribution or plausible deniability. Leaked documents reveal that the IRGC conducted a ransomware campaign known as 'Project Signal' through the contracting company Emen Net Pasargard. Initiated between July and September 2020, initially it seemed that this campaign had a financial motive, as attackers demanded Bitcoin payments and offered decryption keys upon payment. Yet, closer investigation revealed that these actions were likely designed to imitate cybercriminal activities and conceal Iranian state involvement.

There are also instances where state-linked Iranian groups have engaged in ransomware operations for financial gain. In August 2024, CISA reported that two such groups, Pioneer Kitten and Lemon Sandstorm, had targeted US organisations, including schools, government agencies, and healthcare facilities. Rather than solely pursuing political objectives, these groups monetised their access by selling domain control and administrator credentials on cybercriminal marketplaces and collaborating with ransomware affiliates such as NoEscape and ALPHV (BlackCat). Their involvement extended beyond initial access, actively supporting encryption operations and extortion efforts in exchange for a share of the ransom – operating in a manner similar to the North Korea model.[94]

The overarching motivations of geopolitical destabilisation, misdirection, and financial gain have remained relatively consistent since Iran-linked groups began pursuing their goals through cyber operations. However, three notable trends have been observed over the years:

01 First, these groups appear to have shifted away from using wipers, such as Shamoon, ZeroCleare, or Dustman, as their primary tools for disruption and destruction, instead favoring ransomware or pseudo-ransomware, likely to preserve plausible deniability.

02 Second, groups like Pioneer Kitten and Fox Kitten have increasingly engaged with the ransomware ecosystem by offering services to other affiliates, such as providing initial access through marketplaces, as reported by CISA in August 2024. This illustrates how these groups have likely recognized the value of targeting stages in the cybercriminal attack chain that align best with their capabilities, effectively adopting a 'plug-and-play' approach where feasible.

03 Finally, while difficult to quantify, Iranian state-linked groups have frequently utilised social media to publicise their ransomware activities as part of propaganda campaigns aimed at instilling fear and diverting attention.

[94] The FBI noted these actors concealed their Iran-based origins and remained vague about their nationality when interacting with ransomware affiliates.

Deepening Entanglement of State and Criminal Ransomware Activities

This report has examined how states are increasingly embedding themselves in the ransomware ecosystem, not merely as outside beneficiaries but as active participants. Through a comparative analysis of ransomware use by Russia, China, North Korea, and Iran, we have shown how divergent motives and operational ecosystems shape the ways states exploit ransomware for strategic advantage.

Russian state-linked groups use ransomware as a tactical tool in high-tempo conflicts like Ukraine, while China primarily employs it to maintain plausible deniability. Iranian actors have a strong focus on disruption and perception, often targeting Israeli organisations. North Korea, by contrast, prioritises financial gain.

Despite these differences, a broader trend has emerged: states are not building ransomware operations entirely from scratch. Instead, they are leveraging established ransomware infrastructure – relying on well-known affiliates, purchasing access, or deploying widely used strains like LockBit. In doing so, they reduce their operational overhead and complicate attribution. In some cases, such as North Korea and Iran, groups don't stop at access acquisition but play an active role in the execution of ransomware operations, from negotiation to payment, blending state objectives and personal or organisational financial gain. This includes activities such as moonlighting, redirecting funds to support other operations, and working independently under loose or shifting chains of command, as seen in the SamSam campaign. Given these dynamics, we should expect even greater entanglement between state and criminal ransomware activity in the future.

References

Abrahams, Lawrence 'SEC ends probe into MOVEit attacks impacting 95 million people,' *Bleeping Computer*, August 7, 2024, https://bleepingcomputer.com/news/security/sec-ends-probe-into-moveit-attacks-impacting-95-million-people/.

Barnhart, Michael, Austin Larsen, Jeff Johnson, Taylor Long, Michelle Cantos, and Adrian Hernandez (Mandiant). 'Assessed Cyber Structure and Alignments of North Korea in 2023.' *Google Cloud Blog*. October 10, 2023. https://cloud.google.com/blog/topics/threat-intelligence/north-korea-cyber-structure-alignment-2023.

Burgess, Matt. 'Leaked Ransomware Docs Show Conti Helping Putin From the Shadows.' *Wired*. March 18, 2022. https://www.wired.com/story/conti-ransomware-russia/.

Cary, Dakota. 'China's Cyber Revenge | Why the PRC Fails to Back Its Claims of Western Espionage.' SentinelOne. February 12, 2024. https://www.sentinelone.com/labs/chinas-cyber-revenge-why-the-prc-fails-to-back-its-claims-of-western-espionage/.

Cary, Dakota, and Aleksandar Milenkoski. 'Unmasking I-Soon | The Leak That Revealed China's Cyber Operations.' SentinelOne. February 21, 2024. https://www.sentinelone.com/labs/unmasking-i-soon-the-leak-that-revealed-chinas-cyber-operations/.

CERT-EU. 'WannaCry Ransomware Campaign SMB Vulnerability: CERT-EU Security Advisory 2017-012.' CERT-EU. May 22, 2017. https://cert.europa.eu/static/SecurityAdvisories/2017/CERT-EU-SA2017-012.pdf.

———. 'Eastern Europe's Crypto Crime Landscape: Scams Dominate, Plus Significant Ransomware Activity.' *Chainalysis* (blog). Oct 14, 2021. https://www.chainalysis.com/blog/eastern-europe-cryptocurrency-geography-report-2021-preview/.

———. 'NCA Disrupts Multi-Billion Dollar Russian Money Laundering Network.' *Chainalysis* (blog). December 4, 2024. https://www.chainalysis.com/blog/nca-disrupts-multi-billion-dollar-russian-money-laundering-network-2024/.

National Computer Virus Emergency Response Center. 'Volt Typhoon: A Conspiratorial Swindling Campaign Targets with U.S. Congress and Taxpayers Conducted by U.S. Intelligence Community.' April 15, 2024. https://www.cverc.org.cn/head/zhaiyao/futetaifengEN.pdf.

Cimpanu, Catalin. 'REvil Ransomware Gang Executes Supply Chain Attack via Malicious Kaseya Update.' *Record*. July 2, 2021. https://therecord.media/revil-ransomware-executes-supply-chain-attack-via-malicious-kaseya-update.

Cybersecurity and Infrastructure Security Agency. 'Cybersecurity Alerts & Advisories." Accessed March 28, 2025. https://www.cisa.gov/news-events/cybersecurity-advisories.

Cybersecurity and Infrastructure Security Agency. 'Iranian State Actors Conduct Cyber Operations Against the Government of Albania.' September 23, 2022. https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-264a.

Cybersecurity and Infrastructure Security Agency. 'North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector.' July 7, 2022. https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-187a.

Cybersecurity and Infrastructure Security Agency. '#StopRansomware: Ransomware Attacks on Critical Infrastructure Fund DPRK Malicious Cyber Activities.' February 9, 2023. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-040a.

Cybersecurity and Infrastructure Security Agency. 'Update: Destructive Malware Targeting Organizations in Ukraine.' April 28, 2022. https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-057a.

ClearSky. 'Operation Quicksand MuddyWater's Offensive Attack Against Israeli Organizations.' October 2020. https://www.clearskysec.com/wp-content/uploads/2020/10/Operation-Quicksand.pdf.

Cook, Victoria. "'Russian Criminals" behind London Hospitals Cyber Attack.' *BBC*. June 5, 2024. https://www.bbc.com/news/articles/cxee7317kgmo.

Counter Threat Unit Research Team. 'BRONZE STARLIGHT Ransomware Operations Use HUI Loader.' Secureworks. June 23, 2022. https://www.secureworks.com/research/bronze-starlight-ransomware-operations-use-hui-loader.

Cullen, Charlie. 'The Men Who Never Were: Assessing Ties Between the Samsam Ransomware Campaign and the IRGC.' BSidesAtlanta 2020. March 27, 2020.

'Despite Thriving Trade, China's Relationship with Brazil Is Weakening.' *Economist*. February 12, 2022. https://www.economist.com/the-americas/2022/02/12/despite-thriving-trade-chinas-relationship-with-brazil-is-weakening.

Dragos Inc. 'CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations V2.' June 13, 2017. https://www.dragos.com/wp-content/uploads/CrashOverride-01.pdf.

Easterly, Jen. 'The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years." Cybersecurity and Infrastructure Security Agency. May 7, 2023. https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years.

Fraser, Nalani, Fred Plan, Jacqueline O'Leary, Vincent Cannon, Raymond Leong, Dan Perez, and Chi-en Shen (Mandiant). 'APT41 Chinese Cyber Threat Group.' *Google Cloud Blog*. August 7, 2019. https://cloud.google.com/blog/topics/threat-intelligence/apt41-dual-espionage-and-cyber-crime-operation.

Gecsoyler, Sammy, and Dan Milmo. 'Russian Crime Group behind London Hospitals Cyber-Attack, Says Expert.' *Guardian*. June 5, 2024. https://www.theguardian.com/technology/article/2024/jun/05/russian-group-behind-london-hospitals-cyber-attack-says-expert.

Google Threat Intelligence Group. 'Cybercrime: A Multifaceted National Security Threat.' *Google Cloud Blog*. February 2025. https://cloud.google.com/blog/topics/threat-intelligence/cybercrime-multifaceted-national-security-threat

GReAT: Global Research & Analysis Team, Kaspersky. 'APT10: Sophisticated Multi-Layered Loader Ecipekac Discovered in A41APT Campaign.' SecureList by Kaspersky. March 30, 2021. https://securelist.com/apt10-sophisticated-multi-layered-loader-ecipekac-discovered-in-a41apt-campaign/101519/.

———. 'From Shamoon to Stonedrill: Wipers Attacking Saudi Organizations and Beyond.' Kaspersky Lab. 2017. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180722/Report_Shamoon_StoneDrill_final.pdf.

———. 'MATA: Multi-Platform Targeted Malware Framework.' SecureList by Kaspersky. July 22, 2020. https://securelist.com/mata-multi-platform-targeted-malware-framework/97746/.

Greenberg, Andy. 'Inside Olympic Destroyer, the Most Deceptive Hack in History.' *Wired*. October 17, 2019. https://www.wired.com/story/untold-story-2018-olympics-destroyer-cyberattack/.

———. *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. First edition. New York: Doubleday, 2019.

———. 'The Ransomware Hackers Made Some Real Amateur Mistakes.' *Wired*. May 15, 2017. https://www.wired.com/2017/05/wannacry-ransomware-hackers-made-real-amateur-mistakes/.

Greig, Jonathan. "'An Attack on the Reputation of Palau": Officials Question Who Was Really behind Ransomware Incident.' *Record*. April 4, 2024. https://therecord.media/palau-attack-who-was-behind-china-us.

———. "'They're Lying": Palau Denies Claims by Ransomware Gang over Recent Cyberattack.' *Record*. April 8, 2024. https://therecord.media/palau-denies-ransomware-gang-claims.

Guerrero-Saade, Juan Andrés. 'MeteorExpress | Mysterious Wiper Paralyzes Iranian Trains with Epic Troll.' SentinelOne. July 29, 2021. https://www.sentinelone.com/labs/meteorexpress-mysterious-wiper-paralyzes-iranian-trains-with-epic-troll/.

Gunasekar, Arvind. 'AIIMS Delhi Servers Were Hacked By Chinese, Damage Contained: Sources.' *NDTV*. December 14, 2022. https://www.ndtv.com/india-news/aiims-delhi-server-attack-was-by-chinese-5-physical-servers-infiltrated-by-hackers-data-retrieved-now-government-sources-3605639.

Haughom, James, Júlio Dantas, and Jim Walter. 'LockBit Ransomware Side-Loads Cobalt Strike Beacon with Legitimate VMware Utility.' SentinelOne. April 27, 2022. https://www.sentinelone.com/labs/lockbit-ransomware-side-loads-cobalt-strike-beacon-with-legitimate-vmware-utility/.

Heller, Michael. 'SamSam Ransomware Actors Charged, Sanctioned by US Government.' Search Security. Tech Target. Accessed March 31, 2025. https://www.techtarget.com/searchsecurity/news/252453483/SamSam-ransomware-actors-charged-sanctioned-by-US-government.

Hsu, Still, and Zih-Cing Lao. 'Unmasking CamoFei: An In-Depth Analysis of an Emerging APT Group Focused on Healthcare Sectors in East Asia.' HITCON Conference. August 18, 2023. https://hitcon.org/2023/CMT/slide/Unmasking%20CamoFei_An%20In-depth%20Analysis%20of%20an%20Emerging%20APT%20Group%20Focused%20on%20Healthcare%20Sectors%20in%20East%20Asia.pdf.

HT News Desk. 'AIIMS Server Outage Being Probed as "yber Terrorism": Delhi Police.' *Hindustan Times*. November 24, 2022. https://www.hindustantimes.com/cities/delhi-news/aiims-server-outage-being-probed-as-cyber-terror-act-delhi-police-101669308187997.html.

Ilascu, Ionut. 'Babuk Quits Ransomware Encryption, Focuses on Data-Theft Extortion.' *BleepingComputer*. April 30, 2021. https://www.bleepingcomputer.com/news/security/babuk-quits-ransomware-encryption-focuses-on-data-theft-extortion/.

Israel National Cyber Directorate. 'Iranian Government-Sponsored Threat Actor MuddyWater Conducts Cyber Attack Against Israel.' Gov.il. March 9, 2023. https://www.gov.il/en/pages/_muddywater.

Joshi, Sahil, and Divyesh Singh. 'Mega Mumbai Power Outage May Be Result of Cyber Attack, Final Report Awaited.' *India Today*. November 20, 2020. https://www.indiatoday.in/india/story/mumbai-power-outage-malware-attack-1742538-2020-11-20.

Kang, Dake, and Zen Soo. 'Leak Lifts Lid on Chinese Hacking Company – a Culture Fuelled by Alcohol and Sex.' *Independent*. March 8, 2024. https://www.independent.co.uk/asia/east-asia/i-soon-china-hacking-documents-b2509300.html.

Kharpal, Arjun. 'Hackers Who Infected 200,000 Machines Have Only Made $50,000 Worth of Bitcoin.' *CNBC*. May 15, 2017. https://www.cnbc.com/2017/05/15/wannacry-ransomware-hackers-have-only-made-50000-worth-of-bitcoin.html.

Kwiatkowski, Ivan, Pierre Delcher, and Félix Aime. 'Lazarus on the Hunt for Big Game.' SecureList by Kaspersky. July 28, 2020. https://securelist.com/lazarus-on-the-hunt-for-big-game/97757/.

Lakshmanan, Ravie. 'Iranian Hackers Likely Behind Disruptive Cyberattacks Against Albanian Government.' *Hacker News*. August 5, 2022. https://thehackernews.com/2022/08/iranian-hackers-likely-behind.html.

Leyden, John. 'Ransomware Author Tracked down, but Not Nicked.' *Register*. October 1, 2008. https://www.theregister.com/2008/10/01/gpcode_author_hunt/.

Li, Charles, and Che Chang. 'To Loot or Not to Loot? That Is Not a Question When State-Nexus APT Targets Online Entertainment Industry.' Presented at the BlackHat Asia 2022, Marina Bay Sands, Singapore. May 13, 2022. https://i.blackhat.com/Asia-22/Friday-Materials/AS-22-Li-To-Loot-Or-Not-To-Loot-That-Is-Not-a-Question.pdf.

Lilly, Bilyana, and Joe Cheravitch. 'The Past, Present, and Future of Russia's Cyber Strategy and Forces.' In *2020 12th International Conference on Cyber Conflict (CyCon)*, 129–55. Estonia: IEEE, 2020. https://doi.org/10.23919/CyCon49761.2020.9131723.

Lyngaas, Sean. 'Half of North Korean Missile Program Funded by Cyberattacks and Crypto Theft, White House Says.' *CNN*. May 10, 2023. https://www.cnn.com/2023/05/10/politics/north-korean-missile-program-cyberattacks/index.html.

Martin, Alexander. 'Eduard Benderskiy: Western Authorities Link Russian Intelligence Officer to Evil Corp Cybercrime Empire.' *Record*. October 1, 2024. https://therecord.media/evil-corp-cybercrime-eduard-benderskiy-russian-intelligence.

———. 'Israel Blames State-Sponsored Iranian Hackers for Ransomware Attack on University.' *Record*. March 7, 2023. https://therecord.media/israel-technion-ransomware-attack-iran-darkbit-muddywater.

McCausland, Phil, Sam Petulla, and Alastair Jamieson. 'Global Cyberattack Spreads to 150 Countries, 200,000 Victims: Europol.' *NBC News*. May 14, 2017. https://www.nbcnews.com/tech/internet/after-huge-global-cyberattack-countries-scramble-halt-spread-ransomware-n759121.

Meng, Siyuan. 'China's Burned-out Tech Workers Are Fighting Back against Long Hours.' *MIT Technology Review*. November 15, 2021. https://www.technologyreview.com/2021/11/15/1039650/china-tech-workers-996-fight-back/.

Menn, Joseph. 'Exclusive: Chinese Hackers behind U.S. Ransomware Attacks - Security Firms.' *Reuters*. March 15, 2016. https://www.reuters.com/article/technology/exclusive-chinese-hackers-behind-us-ransomware-attacks-security-firms-idUSKCN0WG2L4/.

Microsoft Digital Security Unit, Microsoft Threat Intelligence. 'North Korean Threat Actor Targets Small and Midsize Businesses with H0lyGh0st Ransomware.' *Microsoft Security Blog*. July 14, 2022. https://www.microsoft.com/en-us/security/blog/2022/07/14/north-korean-threat-actor-targets-small-and-midsize-businesses-with-h0lygh0st-ransomware/.

Microsoft Threat Intelligence. 'Moonstone Sleet Emerges as New North Korean Threat Actor with New Bag of Tricks.' *Microsoft Security Blog*. May 28, 2024. https://www.microsoft.com/en-us/security/blog/2024/05/28/moonstone-sleet-emerges-as-new-north-korean-threat-actor-with-new-bag-of-tricks/.

———. 'New 'Prestige' Ransomware Impacts Organizations in Ukraine and Poland.' *Microsoft Security Blog*. October 14, 2022. https://www.microsoft.com/en-us/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-and-poland/.

———. 'Ransomware as a Service: Understanding the Cybercrime Gig Economy and How to Protect Yourself.' *Microsoft Security Blog*. May 9, 2022. https://www.microsoft.com/en-us/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/.

Milenkoski, Aleksandar, and Tom Hegel. 'Chinese Entanglement | DLL Hijacking in the Asian Gambling Sector.' SentinelOne. August 17, 2023. https://www.sentinelone.com/labs/chinese-entanglement-dll-hijacking-in-the-asian-gambling-sector/.

Milenkoski, Aleksandar, and Julian-Ferdinant Vögele. 'ChamelGang & Friends | Cyberespionage Groups Attacking Critical Infrastructure with Ransomware.' *SentinelOne*. June 26, 2024. https://www.sentinelone.com/labs/chamelgang-attacking-critical-infrastructure-with-ransomware/.

Miller, John, and David Mainor (Mandiant). 'WannaCry Ransomware Campaign: Threat Details and Risk Management.' *Google Cloud Blog*. May 15, 2017. https://cloud.google.com/blog/topics/threat-intelligence/wannacry-ransomware-campaign.

Nazarov, Denis, and Emelyanova Olga. 'Blackmailer: The Story of Gpcode.' SecureList by Kaspersky. June 26, 2006. https://securelist.com/blackmailer-the-story-of-gpcode/36089/.

Office of Public Affairs. 'Justice Department Charges 12 Chinese Contract Hackers and Law Enforcement Officers in Global Computer Intrusion Campaigns.' United States Department of Justice. March 5, 2025. https://www.justice.gov/opa/pr/justice-department-charges-12-chinese-contract-hackers-and-law-enforcement-officers-global.

———. 'North Korean Government Hacker Charged for Involvement in Ransomware Attacks Targeting U.S. Hospitals and Health Care Providers.' United States Department of Justice. July 25, 2024. https://www.justice.gov/archives/opa/pr/north-korean-government-hacker-charged-involvement-ransomware-attacks-targeting-us-hospitals.

———. 'North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions.' United States Department of Justice, September 6, 2018. https://www.justice.gov/archives/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and.

———. 'Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals, Municipalities, and Public Institutions, Causing Over $30 Million in Losses.' United States Department of Justice. November 28, 2018. https://www.justice.gov/archives/opa/pr/two-iranian-men-indicted-deploying-ransomware-extort-hospitals-municipalities-and-public.

Osborne, Charlie. 'Shamoon Data-Wiping Malware Believed to Be the Work of Iranian Hackers.' *ZDNet* December 19, 2018. https://www.zdnet.com/article/shamoons-data-wiping-malware-believed-to-be-the-work-of-iranian-hackers/.

Reuters. 'U.S. Indicts Iranian Hackers Responsible for Deploying 'SamSam' Ransomware.' *Euronews*. November 28, 2018. https://www.euronews.com/2018/11/28/us-pressures-iran-with-sanctions-indictments-for-ransomware-scheme.

Roncone, Gabby, Dan Black, John Wolfram, Tyler McLellan, Nick Simonian, Ryan Hall, Anton Prokopenkov, Dan Perez, Lexie Aytes and Alden Wahlstrom. 'APT44: Unearthing Sandworm.' *Mandiant*. April 2024. https://services.google.com/fh/files/misc/apt44-unearthing-sandworm.pdf

Sekoia TDR. "'Iran Cyber Threat Overview.'" *Sekoia.io Blog.*, June 5, 2023. https://blog.sekoia.io/iran-cyber-threat-overview/.

Shires, James, Max Smeets, and Hannah-Sophie Weber. 'Predatory Sparrow: Cyber Sabotage with a Conscience?' *Binding Hook*. December 9, 2024. https://bindinghook.com/articles-binding-edge/predatory-sparrow-cyber-sabotage-with-a-conscience/.

Shusan, Amitai Ben, Noam Lifshitz, Amnon Kushnir, Martin Korman, and Boaz Wasserman. 'Lazarus Group's Mata Framework Leveraged To Deploy TFlower Ransomware./ Sygnia. August 1, 2021. https://www.sygnia.co/threat-reports-and-advisories/lazarus-groups-mata-framework-leveraged-to-deploy-tflower-ransomware/.

Singh, Karn Pratap. 'Ransomware Attack: Report Flags Host of Security Lapses at AIIMS.' *Hindustan Times*. December 7, 2022. https://www.hindustantimes.com/cities/delhi-news/report-flags-host-of-security-lapses-at-aiims-101670359251255.html.

Smeets, Max. *Ransom War: How Cyber Crime Became a Threat to National Security*. New York City: Oxford University Press, 2025.

'System Location Discovery: System Language Discovery.' Mitre Att&ck. October 15, 2021. https://attack.mitre.org/techniques/T1614/001/.

Tidy, Joe. '74% of Ransomware Revenue Goes to Russia-Linked Hackers.' *BBC*. February 14, 2022. https://www.bbc.com/news/technology-60378009.

Toulas, Bill. 'Maui Ransomware Operation Linked to North Korean "Andariel" Hackers.' *BleepingComputer*. August 9, 2022. https://www.bleepingcomputer.com/news/security/maui-ransomware-operation-linked-to-north-korean-andariel-hackers/.

Trellix. 'The Hermit Kingdom's Ransomware Play. May 3, 2022. https://www.trellix.com/blogs/research/the-hermit-kingdoms-ransomware-play/.

Uchill, Joe. 'Ransomware That Avoids Russian Speakers Gets 90% of Payments.' *SC Media*. September 2, 2021. https://www.scworld.com/analysis/ransomware-that-avoids-russian-speakers-get-90-of-ransoms.

Unit 42. 'Data From Chinese Security Services Company I-Soon Linked to Previous Chinese APT Campaigns.' *Unit 42 by Palo Alto Networks* (blog). February 23, 2024. https://unit42.paloaltonetworks.com/i-soon-data-leaks/.

———. 'Jumpy Pisces Engages in Play Ransomware.' *Unit 42 by Palo Alto Networks* (blog). October 30, 2024. https://unit42.paloaltonetworks.com/north-korean-threat-group-play-ransomware/.

US Department of the Treasury. 'Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware.' December 5, 2019. https://home.treasury.gov/news/press-releases/sm845.

———. "Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups." September 13, 2019. https://home.treasury.gov/news/press-releases/sm774.

Vicens, A. J. 'Chinese Hackers Are Increasingly Deploying Ransomware, Researchers Say.' *CyberScoop*. June 26, 2024. https://cyberscoop.com/chinese-hackers-are-increasingly-deploying-ransomware-researchers-say/.

Walker, Owen. 'North Korea Stole $1.3bn through Crypto Hacks in 2024.' *Financial Times*. December 19, 2024. https://www.ft.com/content/4ed7ce45-a653-496e-99a6-ade9c21f9908.

virtual routes

For more information, please visit: **www.virtual-routes.org**

If you have any further queries, questions, or concerns, feel free to reach out via email at:
contact@virtual-routes.org