Pharos Series: Report No. 1 March 2025

The Ransomware Playbook and How to Disrupt It

Max Smeets

virtual routes

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

Pharos Series: Report No. 1 March 2025

The Ransomware Playbook and How to Disrupt It

Max Smeets

virtual routes

About the Author

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.

Table of Contents

Executive Summary 06

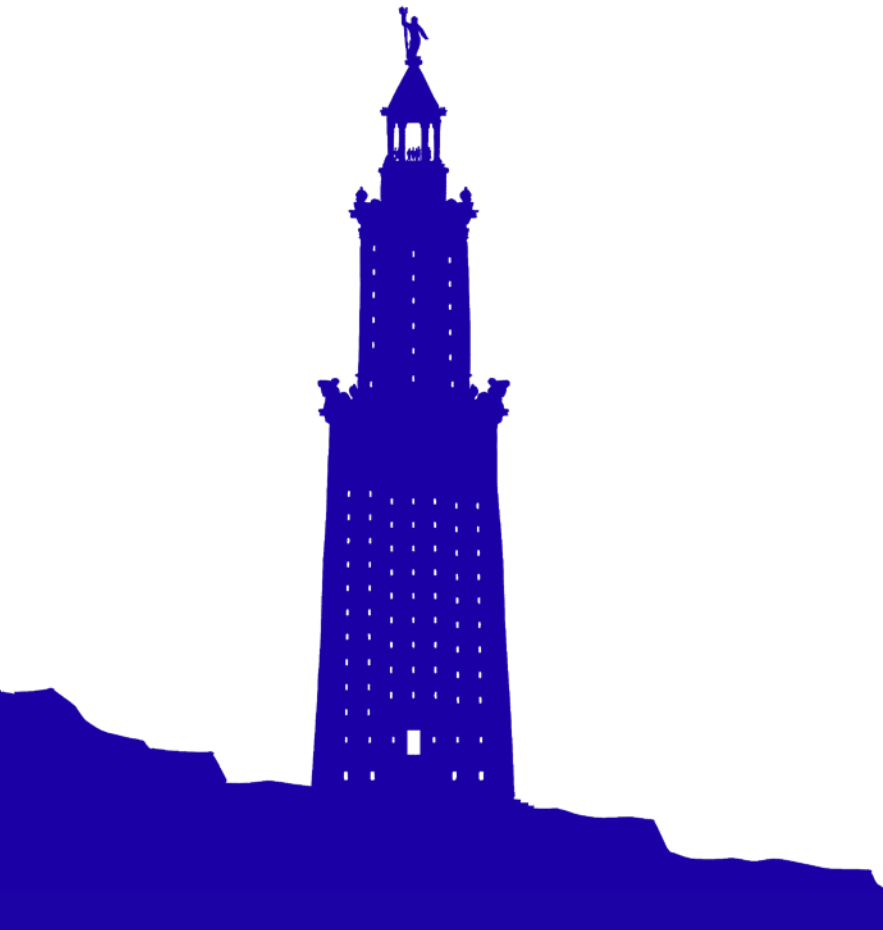
The 11 Stages of the Ransomware Playbook 07

Spotlight Case Study: Conti's Playbook in Action 09

Disrupting the Ransomware Playbook 11

The Need for International Partnerships 21

References 23



Ransomware

groups have dramatically improved their modus operandi, also informally described as their ‘playbook’, over the years.

Executive Summary

Ransomware groups have dramatically improved their modus operandi, also informally described as their 'playbook', over the years. Gone are the days when ransomware attacks were launched indiscriminately, hoping to snag any vulnerable victim that crossed their path. Ransomware groups now conduct their operations with a much higher level of calculation. A ransomware tactic known as 'big-game hunting' involves orchestrating large-scale attacks with substantial ransom demands. Ransomware payloads employ advanced encryption algorithms and techniques that make decryption without the attacker's key nearly impossible.

Once a ransomware group gains access to a potential victim, their playbook is equally well honed. Negotiation processes have become more formalised, involving dedicated communication channels, countdown timers, and threats of data exposure. The rise of cryptocurrency has enabled ransomware groups to conduct global transactions, including victim payments, with relative anonymity and greater efficiency. Furthermore, today, many ransomware groups have embraced a dual tactic of both encryption and extortion, leveraging the threat of data leaks to amplify their impact. By threatening to expose sensitive information, they create a sense of urgency and panic among victims, compelling them to comply with ransom demands. This tactic not only maximises profits but also adds to the groups' reputation as ruthless and credible threat actors.

This analysis looks at government actions that aim to counter this new ransomware playbook. It is based on two main sources: the Virtual Routes Ransomware Countermeasures Tracker and my book *Ransom War: How Cyber Crime Became a Threat to National Security*. The first part lays out the playbook of ransomware groups in 11 stages, followed by a discussion about what governments have achieved so far in disrupting ransomware groups across these stages. The last section emphasizes the need for stronger national strategies and enhanced international collaboration to combat ransomware effectively.

The **11 Stages** of the Ransomware Playbook

Ransomware operations vary in targeting, sophistication, and scale. But we can generally distinguish between 11 operational stages of the ransomware playbook.

01

RECONNAISSANCE

The initial stage of a ransomware attack is reconnaissance, where the attackers gather information about potential victims to identify vulnerabilities and entry points.

02

NETWORK COMPROMISE

The second stage, network compromise, focuses on infiltrating and establishing a foothold within the target's network. Attackers employ various tactics, such as exploiting vulnerabilities, phishing, and using initial access brokers.

03

SITUATIONAL AWARENESS AND PRIVILEGE ESCALATION

The third stage, situational awareness and privilege escalation, involves identifying exploitable vulnerabilities to gain elevated access. This step consolidates control over the target's systems and enables lateral movement within the network.

04

PERSISTENCE AND COMMAND & CONTROL (C2)

Once attackers have escalated their access, their top priority is to maintain control and avoid detection. They use tools such as backdoors, webshells, and remote access software, mimicking normal operations to remain undetected.

05

PRIVILEGE ESCALATION AND DATA IDENTIFICATION

At the next stage, attackers focus on identifying high-value data, often prioritizing administrator accounts due to their access levels to critical systems and sensitive information.

06

DATA EXFILTRATION AND RECOVERY INHIBITION

After identifying valuable data, ransomware groups proceed to the exfiltration stage. They package the data using compression and encryption to minimize detection risks during transfer, often leveraging tools designed for stealth.

07

LOCKER DEPLOYMENT AND NOTE DELIVERY

The seventh stage shifts to encrypting the victim's data and hindering recovery efforts. This pivotal action creates urgency and panic, compelling the victim to negotiate.

08

NEGOTIATION

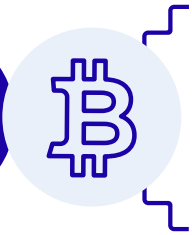
During the negotiation stage, attackers assess the victim's priorities – whether they are more concerned with decrypting data or preventing its leak. They navigate these discussions strategically to maximize profits.

09

DECRYPTION OR PUBLIC RELEASE OF DATA

The ninth stage revolves around the victim's decision to either pay the ransom or face public exposure of their data on the attacker's leak site or shaming blog.

10



PAYMENT TO OPERATIONAL TEAM AND CRYPTOCURRENCY MIXING

Next, ransomware groups focus on distributing ransom payments among members while obscuring transaction trails. Cryptocurrency, particularly Bitcoin, is preferred for its global acceptance, despite its traceability on public ledgers.

11

CASH OUT AND INVESTMENT

The final stage involves cashing out illicit earnings and reinvesting funds. Attackers convert cryptocurrency into fiat currency through over-the-counter exchanges or proxy accounts, funding operational expenses and securing the group's long-term viability.

Spotlight Case Study: **Conti's Playbook in Action**

Between 2019 and 2021, Conti emerged as the world's largest ransomware group, as measured by cryptocurrency transactions and reported incidents. At its peak, Conti accounted for nearly half of all documented ransomware activity. In 2021 alone, the group carried out over 400 successful cyberattacks targeting major corporations and organisations.[1]

For the first stage, reconnaissance, Conti relied on tools like Zoominfo to assess a target's size and revenue, which helped them estimate ransom demands. Their reconnaissance approach was opportunistic rather than deliberate, broadly scanning for vulnerabilities. After gaining access, Conti's OSINT team shifted their focus to identifying high-value systems and data within compromised networks.

To compromise a network, the second stage, Conti used phishing campaigns or worked with initial access brokers (IABs) like Exotic Lily.[2] These brokers conducted spear phishing and sometimes exploited zero-day vulnerabilities.[3] Once inside, Conti leveraged tools such as Metasploit and Cobalt Strike, targeting internet of things (IoT) devices, Active Directory systems, and other critical infrastructure to establish a strong foothold.

For the third stage, situational awareness and privilege escalation, Conti focused on identifying exploitable vulnerabilities to gain elevated access.[4] Tools like Cobalt Strike enabled lateral movement across the network, while operators mapped environments and pinpointed high-value systems and accounts. Manual techniques and automated tools ensured they maintained control over key areas of the network.

To maintain persistence and command and control, the fourth stage, Conti deployed tools like the Anchor backdoor, which used Domain Name System (DNS) protocol for covert communications, and other commercial remote access software. These tools allowed them to maintain long-term access, mimicking legitimate traffic to evade detection. Webshells and custom malware further reinforced their ability to operate stealthily.[5]

---

[1] For higher estimates see: Yaara Shriebman, 'Ransomware 2021 – The Bad, The Bad & The Ugly,' Cyberint, December 30, 2021, https://cyberint.com/blog/research/ransomware-2021-the-bad-the-bad-the-ugly/; 'Conti Ransomware Gang Shutdown, Conti Ransomware Rebranding 2022,' *CyberTalk*, May 20, 2022, https://www.cybertalk.org/2022/05/20/conti-ransomware-gang-shuts-down-rebranding-into-smaller-units/.

[2] Vlad Stolyarov, and Benoit Sevens, 'Exposing Initial Access Broker with Ties to Conti,' Google, March 17, 2022, https://blog.google/threat-analysis-group/exposing-initial-access-broker-ties-conti/.

[3] More on the vulnerability: 'Microsoft MSHTML Remote Code Execution Vulnerability: CVE-2021-40444 Security Vulnerability,' Microsoft Security Response Center, September 7, 2021, https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40444.

[4] Satnam Narang, 'ContiLeaks: Chats Reveal Over 30 Vulnerabilities Used by Conti Ransomware – How Tenable Can Help,' *Tenable Blog* (blog), March 24, 2022, https://www.tenable.com/blog/contileaks-chats-reveal-over-30-vulnerabilities-used-by-conti-ransomware-affiliates.

[5] It is also delivered through installing Trickbot. Also see: Cybereason Nocturnus, 'Dropping Anchor: From a TrickBot Infection to the Discovery of the Anchor Malware,' *Cybereason*, accessed May 6, 2024, https://www.cybereason.com/blog/research/dropping-anchor-from-a-trickbot-infection-to-the-discovery-of-the-anchor-malware; Ravie Lakshmanan, 'TrickBot Malware Gang Upgrades Its AnchorDNS Backdoor to AnchorMail,' *The Hacker News*, March 1, 2022, https://thehackernews.com/2022/03/trickbot-malware-gang-upgrades-its.html.

To identify directories with high-value data, the fifth stage, Conti operators targeted administrative accounts. Using PowerSploit to locate active directories, they manually investigated clues like group memberships and job titles, cross-referencing findings with external sources such as LinkedIn. They searched browser histories and user directories to uncover passwords, backup locations, and other sensitive information.[6]

To exfiltrate data, the sixth stage, Conti repurposed tools like Rclone and FileZilla to transfer compressed and encrypted files to cloud storage services like MEGA. Their internal forums provided detailed instructions on configuring these tools to minimise detection, ensuring stealth and efficiency during the exfiltration process.

To encrypt data and deploy ransom notes, the seventh stage, Conti used advanced encryption algorithms such as chacha20, appending the '.CONTI' extension to files. This stage, typically executed within four days of initial access, aimed to create urgency. Ransom notes included detailed instructions for payment and threats to publish stolen data on their leak site, leveraging a 'double extortion' model.[7]

To negotiate with victims, the eighth stage, Conti employed psychological tactics and bluffing to maximize payouts. Internal communications reveal tailored ransom demands based on a victim's perceived financial capacity. Third-party negotiators, such as 'The Spaniard,' facilitated payments, while Conti occasionally enlisted journalists to amplify pressure.

To push victims to pay or face exposure, the ninth stage, Conti used countdown timers and threats of public data leaks. When victims paid, Conti provided functional decryption tools to maintain their reputation and encourage compliance from future victims. If victims refused, stolen data was often published on their leak site to demonstrate consequences.

To obscure ransom payments, the tenth stage, Conti used cryptocurrency mixing services to launder funds. Bitcoin remained their primary choice for payments due to its liquidity, although Monero was occasionally used for added anonymity. Transactions through know your customer (KYC)-compliant exchanges sometimes exposed their financial activities despite efforts to avoid detection.

To cash out and reinvest, the eleventh stage, Conti used platforms like Bestchange.com to convert cryptocurrency into fiat. Proxy accounts ensured anonymity during transactions, while earnings were reinvested into operational costs such as server fees and software licenses.

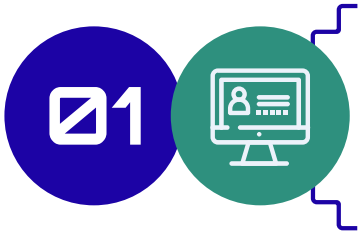
[6] For detailed discussion see: eSentire, 'Analysis of Leaked Conti Intrusion Procedures by eSentire's Threat Response Unit (TRU).' February 27, 2022, https://www.esentire.com/blog/analysis-of-leaked-conti-intrusion-procedures-by-esentires-threat-response-unit-tru

[7] Shmuel Gihon, 'To Be CONTInued? Conti Ransomware Heavy Leaks,' *Cyberint*, March 9, 2022, https://cyberint.com/blog/research/contileaks/

Disrupting the **Ransomware Playbook**

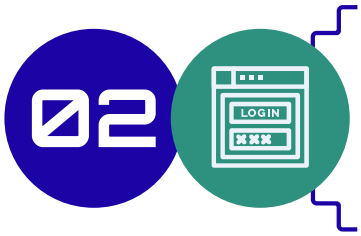
The Virtual Routes Ransomware Countermeasures Tracker has identified over 110 concrete actions taken by governments seeking to undermine the modus operandi of ransomware groups to diminish their effectiveness and profitability.

We can find examples of actions across all the stages of operations – albeit some with greater effectiveness.



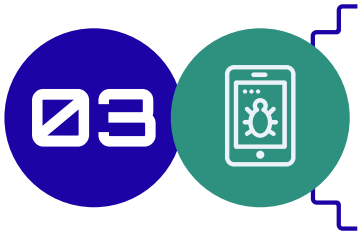
RECONNAISSANCE

- Threat intelligence sharing between private and public sectors to preemptively identify and counteract reconnaissance efforts by cybercriminals
- Proactive alerts about new ransomware campaigns



NETWORK COMPROMISE

- Cyber hygiene and awareness campaigns
- Disruption or take down initial access brokers or botnet infrastructure



SITUATIONAL AWARENESS AND PRIVILEGE ESCALATION

- Promotion of regular security audits

PERSISTENCE AND C2

- Disruption or take down of C2 infrastructure

IDENTIFICATION DIRECTORIES

- Promotion of cybersecurity frameworks that include network segmentation

06

EXFILTRATION OF DATA

- Cybersecurity frameworks that include backups

07

ENCRYPTION

- Distribution of obtained decryption tools through controlled channels

08

NEGOTIATIONS

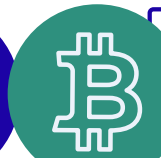
- Establishment of specialised government units that provide expert advice to (certain) ransomware victims during negotiations
- Provision of legal guidance for negotiations

09

PAYMENT OR PUBLICATION

- Takedowns or blocking access to websites that host stolen data as part of extortion schemes

10



MONEY TRANSFERS

- Introduction and enforcement of cryptocurrency exchange regulation

11

CASH OUT

- Seizure or freezing of cryptocurrency assets

To tackle the early operational elements of ransomware, governments often issue warnings to alert organizations about new ransomware campaigns. This is typically based on intelligence shared between public and private sectors. An example is StopRansomware.gov, launched in 2021 by the US government to help both public and private organisations defend against increasing ransomware attacks.[8] This whole-of-government initiative centralises ransomware resources and alerts, guiding organisations to better understand ransomware threats, mitigate risks, and respond effectively to incidents. Since its launch, agencies like the Cybersecurity and Infrastructure Security Agency (CISA) and the FBI have issued numerous alerts, advisories, and updates on various ransomware strains and groups providing important information like indicators of compromise (IoCs), Tactics, Techniques and Procedures (TTPs), and targeting activities.[9]

More proactive government measures have included the takedown of illicit online marketplaces that facilitate access brokerage. A prime example was the takedown of the Hydra market in April 2022. Operating since 2015, Hydra was the most prominent dark web marketplace in Russia and the largest globally, offering a platform for ransomware as a service (RaaS) and other cybercriminal activities.[10] The US Treasury imposed sanctions on Hydra for facilitating cyber-enabled activities that threatened the US's security, policy, economic health, or financial stability. On the same day, German federal police seized Hydra's servers in Germany and confiscated 543 Bitcoins, worth approximately $25 million at the time.[11] Similar disruptions were executed against Genesis Market in April 2023 and Breach Forum Domains in June 2023.[12]

These proactive measures also involve disrupting various botnet infrastructures, which are crucial for spreading ransomware.[13] A key botnet takedown, associated with Ryuk and later Conti, was that

---

[8] CISA: Cybersecurity and Infrastructure Security Agency, 'New StopRansomware.gov website – The U.S. Government's One-Stop Location to Stop Ransomware,' July 15, 2021, https://www.cisa.gov/news-events/alerts/2021/07/15/new-stopransomwaregov-website-us-governments-one-stop-location-stop

[9] This includes Conti, as well as BlackMatter, Play, and Scattered Spider. The effectiveness of joint alerts increases when the FBI and CISA provide detailed information on how a ransomware group infiltrates systems. For instance, their August 2022 joint alert on MedusaLocker highlighted that the group primarily exploits remote desktop protocol (RDP) vulnerabilities to penetrate victims' networks, enabling organisations to implement more targeted defenses. For other cases: Cybersecurity and Infrastructure Security Agency, 'Conti Ransomware,' March 9, 2022, https://www.cisa.gov/news-events/alerts/2021/09/22/conti-ransomware; Cybersecurity and Infrastructure Security Agency, 'BlackMatter Ransomware,' October 18, 2021, https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-291a; Cybersecurity and Infrastructure Security Agency, #StopRansomware: Play Ransomware, December 18, 2023, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-352a; Cybersecurity and Infrastructure Security Agency, 'FBI and CISA Release Advisory on Scattered Spider Group,' November 16, 2023, https://www.cisa.gov/news-events/alerts/2023/11/16/fbi-and-cisa-release-advisory-scattered-spider-group; Cybersecurity and Infrastructure Security Agency, #StopRansomware: Black Basta, May 10, 2024, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-131a; ; Cybersecurity and Infrastructure Security Agency, #StopRansomware: Daixin Team, October 26, 2022, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-294a

[10] Additionally, around $8 million ransomware proceeds from groups like Conti, REvil, and Ryuk were transferred on the market. United States Department of the Treasury, 'Treasury Sanctions Russia-Based Hydra, World's Largest Darknet Market, and Ransomware-Enabling Virtual Currency Exchange Garantex.' April 5, 2022, https://home.treasury.gov/news/press-releases/jy0701

[11] Ruth Fulterer, 'Hydra ist tot: Deutschland sperrt den grössten Darknet-Marktplatz der Welt,' April 5, 2022, https://www.nzz.ch/technologie/deutsche-ermittler-schliessen-hydra-den-groessten-darknet-marktplatz-der-welt-ld.1678073

[12] Sergiu Gatlan, 'FBI seizes BreachForums after arresting its owner Pompompurin in March,' *Bleeping Computer*, June 23, 2023, https://www.bleepingcomputer.com/news/security/fbi-seizes-breachforums-after-arresting-its-owner-pompompurin-in-march/

[13] For a general overview of botnet takedowns, see: Jason Healey, Neil Jenkins, and JD Work, 'Defenders Disrupting Adversaries: Framework, Dataset, and Case Studies of Disruptive Counter-Cyber Operations,' *12th International Conference on Cyber Conflict. 20/20 Vision: The Next Decade*, edited by T. Jančárková, L. Lindström, M. Signoretti, I. Tolga, and G. Visky, NATO CCDCOE Publications, 2020, https://ccdcoe.org/uploads/2020/05/CyCon_2020_14_Healey_Jenkins_Work.pdf

of Trickbot in October 2020.[14] Trickbot was initially released in 2016 to steal banking credentials. Over time, its capabilities expanded to collect Outlook credentials and other sensitive information from compromised machines, making it a favored tool for ransomware groups like Ryuk to deploy their payloads. By 2018, Trickbot had become a high priority cybersecurity threat for many countries, and was later recognized as a significant risk to the integrity of the 2020 US Presidential election process.[15]

The takedown itself involved both government and private sector actions. In early October 2020, Brian Krebs reported that an unknown entity was attempting to disrupt Trickbot by distributing fake configuration files to infected machines, redirecting them to a decoy control server.[16] The entity behind these efforts remained a mystery until mid-October when *The Washington Post* revealed that the US Cyber Command had orchestrated the disruptions as part of a broader strategy of 'persistent engagement' with cyber adversaries to protect the upcoming elections.[17] Concurrently, Microsoft undertook legal and technical actions against the botnet.[18]

---

[14] The other key botnet takedown related to Ryuk and Conti was Emotet in January 2022, as discussed in Chapter Two of Ransom War. Also see: United States Department of Justice, 'Emotet Botnet Disrupted in International Cyber Operation,' January 28, 2021, https://www.justice.gov/opa/pr/emotet-botnet-disrupted-international-cyber-operation; Biermann, Fedorova, Polke-Majewski, and Tanriverdi, 'Hackergruppe Conti – Don Stern und die Hackermafia,' December 11, 2022, https://www.zeit.de/digital/2022-12/conti-hackergruppe-russland-ransomsoftware-cyberangriffe

[15] Kurt Baker, 'What is Trickbot Malware?,' *CrowdStrike*, October 23, 2023, https://www.crowdstrike.com/cybersecurity-101/malware/trickbot/

[16] Brian Krebs, 'Attacks Aimed at Disrupting the Trickbot Botnet,' October 2, 2020, https://krebsonsecurity.com/2020/10/attacks-aimed-at-disrupting-the-trickbot-botnet/

[17] Ellen Nakashima, 'Cyber Command has sought to disrupt the world's largest botnet hoping to reduce its potential impact on the election,' *The Washington Post*, October 9, 2020, https://www.washingtonpost.com/national-security/cyber-command-trickbot-disrupt/2020/10/09/19587aae-0a32-11eb-a166-dc429b380d10_story.html; For the US Cyber Command vision on persistent engagement see: US Cyber Command, 'Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command,' 2018, https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf
For more on persistent engagement theory see: Michael Fischerkeller, Emily Goldman, Richard Harknett, *Cyber Persistence Theory: Redefining National Security in Cyberspace* (Oxford University Press: 2022).

[18] It has been suggested that the goal of these interventions was not to permanently dismantle Trickbot, but rather to temporarily disrupt the operators' activities, preventing them from creating chaos during the US Presidential elections. Nakashima, 'Cyber Command has sought to disrupt the world's largest botnet hoping to reduce its potential impact on the election.'; Ionut Ilascu, 'TrickBot botnet targeted in takedown operations, little impact seen,' *Bleeping Computer*, October 12, 2020, https://www.bleepingcomputer.com/news/security/trickbot-botnet-targeted-in-takedown-operations-little-impact-seen/; on Microsoft's actions see: Tom Burt, 'New action to combat ransomware ahead of U.S. elections,' October 12, 2020, https://blogs.microsoft.com/on-the-issues/2020/10/12/trickbot-ransomware-cyberthreat-us-elections/

Overview of Botnet Disruptions by Governments, Linked to Ransomware

22.09.2020

TrickBot botnet disrupted by Cyber Command

Cyber Command

US Cyber Command temporarily disrupted TrickBot, a major botnet used for ransomware deployment, to reduce threats ahead of the 2020 election.

28.01.2021

Emotet botnet disrupted by Europol and FBI

Europol, Eurojust, FBI

A global law enforcement operation, led by Europol and the FBI, dismantled the Emotet botnet, one of the most notorious malware infrastructures (Operation Ladybird).

29.08.2023

FBI and partners disrupt Qakbot botnet

Europol, Eurojust, FBI

The FBI and international partners dismantled Qakbot, a botnet used by ransomware groups, deleting it from over 700,000 devices and seizing $9 million (Operation Duck Hunt).

27.05.2024

Disruption of infrastructure

Europol

Europol led the largest-ever crackdown on botnets used in ransomware attacks, seizing 2,000 domains, taking down over 100 servers, and arresting four suspects (Operation Endgame).

In an attempt to disrupt ransomware groups' efforts to maintain persistence, establish command and control, escalate privileges, identify data for theft, and inhibit recovery – stages 4-6 of the ransomware playbook – governments have employed a mix of proactive measures and best practice promotions within organisations. One example of such proactive measures was the seizure of several Conti domains by the Irish government. Ireland's Garda National Cyber Crime Bureau (GNCCB) reported that the seizure directly prevented further ransomware incidents globally, with around 750 attempts to connect to these domains post-seizure, each potentially thwarting a ransomware deployment.

To assist organisations with decryption, governments have also at times succeeded in obtaining universal decryption keys for ransomware, which are discreetly shared with the victims.[19] For instance, in October 2022, Dutch police ingeniously tricked the DeadBolt group into handing over decryption keys without any ransom being paid.[20] DeadBolt typically targeted smaller businesses and individuals, demanding relatively modest ransoms, but the high frequency of attacks – approximately 5000 known cases within a year – made their operations lucrative.[21] A critical vulnerability in their operations was their automatic decryption key delivery system upon payment. Dutch investigators exploited a flaw where DeadBolt's system sometimes released the decryption key before the victim's payment was confirmed in the blockchain, which usually takes about 10 minutes. The Dutch police developed a script that would initiate a payment, receive the decryption key, and then automatically cancel the payment before it was confirmed in the blockchain. This process not only helped victims retrieve their data but also prevented 'hundreds of thousands of dollars' from flowing into DeadBolt's wallets before the group detected the anomaly.[22]

Other key distribution measures required more comprehensive intelligence about how the ransomware group functioned. Before taking down the Hive ransomware group in early January, the FBI infiltrated their servers for about seven months. During this time, the FBI created over 300 decryption keys and discreetly distributed them to victims, enabling them to unlock their systems without paying a ransom.[23] Additionally, the FBI supplied another 1,000 keys to individuals previously

---

[19] In 2021, the FBI issued an alert about a vulnerability in the encryption process used by Mamba ransomware. First detected in 2016, Mamba, also known as HDDCryptor, was significant for using open-source software to encrypt entire storage volumes instead of just individual files. Activity for Mamba ransomware ramped up with a new variant emerging in late 2019. Although it did not operate through an affiliate program, Mamba was considered one of the top threats at the time. For more on the FBI alert of Mamba: FBI: Federal Bureau of Investigation, 'FBI Flash: Mamba Ransomware,' StopRansomware.org, https://www.cisa.gov/stopransomware/fbi-flash-mamba-ransomware; Ionut Ilascu, 'FBI exposes weakness in Mamba ransomware, DiskCryptor,' *Bleeping Computer*, March 26, 2021, https://www.bleepingcomputer.com/news/security/fbi-exposes-weakness-in-mamba-ransomware-diskcryptor/

[20] Chainalysis, 'How the Dutch National Police Tricked Prolific Ransomware Strain Deadbolt Into Giving Up Victim Decryption Keys,' *Chainalysis*, March 1, 2023, https://www.chainalysis.com/blog/deadbolt-ransomware-strain-tricked-into-giving-up-decryption-keys/

[21] Protos, 'Dutch police recover 90% of victim decryption keys in ransomware scam,' Protos, March 1, 2023, https://protos.com/dutch-police-recover-90-of-victim-decryption-keys-in-ransomware-scam/

[22] Also see the No More Ransom portal, launched in 2016: https://www.nomoreransom.org/. EUROPOL, 'Hit by ransomware? No More Ransom now offers 136 free tools to rescue your files,' July 26, 2022, https://www.europol.europa.eu/media-press/newsroom/news/hit-ransomware-no-more-ransom-now-offers-136-free-tools-to-rescue-your-files; Chainalysis, 'How the Dutch National Police Tricked Prolific Ransomware Strain Deadbolt Into Giving Up Victim Decryption Keys,' *Chainalysis*, March 1, 2023, https://www.chainalysis.com/blog/deadbolt-ransomware-strain-tricked-into-giving-up-decryption-keys/; Note that a lot of times the decrypter is provided by a private sector company. See for example, Bitfender releases of GandCrab decryption to let victims who got infected by the ransomware recover files without paying the ransom demand: Catalin Cimpanu, 'Bitdefender releases third GandCrab ransomware free decrypter in the past year,' *ZDNET*, February 19, 2019,
https://www.zdnet.com/article/bitdefender-releases-third-gandcrab-ransomware-free-decrypter-in-the-past-year/

targeted by the group, helping them to retrieve some of their lost data. It saved victims from paying $130 million in demanded ransoms.

> When considering such measures, governments occasionally face a challenging decision with parallels in many other areas of intelligence and law enforcement: whether to disclose intelligence collected to prevent serious harm or other criminal activity, or to retain such intelligence to allow further intelligence gathering from the same source.

For ransomware, this trade-off arises most often when governments possess decryption keys or know about an encryption flaw but choose not to immediately disclose this information publicly, to prevent tipping off the ransomware group about their access. For instance, in September 2021, Ellen Nakashima and Rachel Lerman of *The Washington Post* revealed that the FBI had withheld assistance for nearly three weeks following the major ransomware attack against Kaseya.[24] This delay was due to the FBI's plans to disrupt REvil, the group responsible for the attack.

Moving to stages 8 and 9 of the ransomware playbook, governments typically advise against paying ransoms when it reaches the stage where criminals have issued a ransom demand.[25] For instance, the Swiss National Cyber Security Center (NCSC) advises 'not paying a ransom.' As they elaborate: 'once the ransom has been paid, there is no guarantee that the criminals will not publish the data anyway, or otherwise try to profit from it. Moreover, every successful ransom attempt motivates the

---

[23] US Department of Justice, Office of Public Affairs, 'U.S. Department of Justice Disrupts Hive Ransomware Variant,' January 26, 2023, https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant

[24] Kaseya asked New Zealand-based security firm Emsisoft to create a fresh decryption tool, which Kaseya released the following day. However, for some victims, the assistance came too late. Ellen Nakashima and Rachel Lerman, 'FBI held back ransomware decryption key from businesses to run operation targeting hackers,' September 21, 2021, https://www.washingtonpost.com/national-security/ransomware-fbi-revil-decryption-key/2021/09/21/4a9417d0-f15f-11eb-a452-4da5fe48582d_story.html

[25] In 2023, all 50 member nations of the International Counter Ransomware Initiative committed to a policy statement agreeing not to meet ransom demands from cyber criminals. Jessica Lyons, 'Formal ban on ransomware payments? Asking orgs nicely to not cough up ain't working,' *The Register*, January 3, 2024, https://www.theregister.com/2024/01/03/ban_ransomware_payments/; For a comparative legal analysis see: Sean O'Connell, 'To Ban Ransomware Payments or Not to Ban Ransomware Payments: The Problems Drafting Legislation in Response to Ransomware,' Journal of International Business and Law, 22(1), 2023, https://scholarlycommons.law.hofstra.edu/jibl/vol22/iss1/6

attackers to continue, finances the further development of attacks and encourages their spread.'[26]

One of the most controversial and widely discussed governmental policies regarding this stage of the playbook is the increasing call for laws that do not merely advise against, but outright prohibit ransom payments. In early 2025, the UK Home Office put forward a proposal for a payment prevention regime, requiring that ransomware victims notify the authorities and declare their intent to pay a ransom before transferring any funds to the attackers.[27] Former UK NCSC head Ciaran Martin has argued for the necessity of such a ban: 'we have to find a way of making a ransomware payments ban work'.[28] In 2023, Emisoft, a software company known for its decryption services, said that 'We believe that the only solution to the ransomware crisis – which is as bad as it has ever been – is to completely ban the payment of ransoms.'[29]

While this approach directly targets the ransomware payment model, it also presents potential adverse consequences. Implementing such a policy without exceptions is challenging, especially for critical sectors like healthcare, where decryption might be the only option to save lives.[30] This likely leads to ransomware groups targeting the very sectors where payments are still permitted, which are often the most vulnerable and critical. A variation of this argument on country-wide bans was also made in an Institute for Security and Technology report, arguing that if a ban is not introduced internationally at the same time, the ransomware groups will just shift their focus to other sectors/countries and make the situation worse for them.[31]

Regarding stages 10 and 11 of the playbook, ransomware payouts, authorities have mainly targeted cryptocurrency exchanges, which are often used for the illicit transfer of funds. An early example is the May 2013 takedown of Liberty Reserve. Based in Costa Rica, Liberty Reserve allowed users to open accounts and transfer money with minimal identification requirements – a name, date of birth, and an email address.[32] Its relative anonymity made it a favorite among criminals, facilitating

---

[26] National Cyber Security Centre, 'Ransomware – What next?,' January 5, 2022, https://www.ncsc.admin.ch/ncsc/en/home/infos-fuer/infos-unternehmen/vorfall-was-nun/ransomware.html; The Swiss Criminal Code does not categorically classify paying a ransom as a criminal offense. Yan Borboën, 'Ransomware as a business model - Legal aspects of ransom payment,' PwC, https://www.pwc.ch/en/insights/cybersecurity/ransom-payment.html#legal-aspect

[27] UK Home Office, 'Ransomware legislative proposals: reducing payments to cyber criminals and increasing incident reporting,' *Gov.uk*, February 13, 2025, https://www.gov.uk/government/consultations/ransomware-proposals-to-increase-incident-reporting-and-reduce-payments-to-criminals/ransomware-legislative-proposals-reducing-payments-to-cyber-criminals-and-increasing-incident-reporting-accessible#:~:text=The%20Home%20Office%20is%20proposing,payment%20before%20paying%20over%20any

[28] Ciaran Martin, 'Cyber ransoms are too profitable. Let's make paying illegal,' The Times, March 4, 2024, https://www.thetimes.com/article/cyber-ransoms-are-too-profitable-lets-make-paying-illegal-kc8cmhxs0; According to Laurie Mercer from HackerOne, 'Enforcing a ransomware payment ban is like banning smoking - you know it's good for society in the long run but in the short term, it is difficult to stop getting a quick fix.' Dan Raywood, 'Proposals to Ban Ransomware Payments Rumoured,' *SC Media UK*, May 22, 2024, https://insight.scmagazineuk.com/proposals-to-ban-ransomware-payments-rumoured

[29] Emisoft Malware Lab, 'The State of Ransomware in the U.S.: Report and Statistics 2023,' January 2, 2024, https://www.emsisoft.com/en/blog/44987/the-state-of-ransomware-in-the-u-s-report-and-statistics-2023/

[30] Also see: O'Connell, 'To Ban Ransomware Payments or Not to Ban Ransomware Payments: The Problems Drafting Legislation in Response to Ransomware.'

[31] Ransomware Task Force, 'Combating Ransomware A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force,' *IST: Institute for Security and Technology*, 2021, https://securityandtechnology.org/wp-content/uploads/2021/09/IST-Ransomware-Task-Force-Report.pdf

[32] BBC News, 'Liberty Reserve digital money service forced offline,' May 27, 2013, https://www.bbc.com/news/technology-22680297

the transfer of approximately $6 billion in illicit proceeds over seven years.[33] The founder, Arthur Budovsky Belanchuk, was arrested in Spain on charges of money laundering, and shortly thereafter, the Liberty Reserve website was taken offline, displaying a message that it had been seized by US authorities.[34] In 2019, the data collected from Liberty Reserve also contributed to the arrest and conviction of a member of the Reveton ransomware group.[35]

Another significant case occurred in March 2023 with the takedown of Chip Mixer. Described as a 'darknet cryptocurrency mixing service,' Chip Mixer was responsible for laundering more than $3 billion worth of cryptocurrency over about six years, sourced from activities including ransomware attacks and darknet market transactions.[36] Chip Mixer's services were popular among ransomware and other cybercriminal groups for their ability to obscure blockchain trails, making tracking by law enforcement challenging, if not impossible. On March 15, German and U.S. authorities, with support from Europol and agencies in Belgium, Switzerland, and Poland, announced the seizure of four Chip Mixer servers located in Germany, approximately $46.5 million in Bitcoin, and seven terabytes of data.[37] Additionally, Minh Quốc Nguyễn, the Vietnam-based operator of the platform, was charged with money laundering by US authorities in Philadelphia.[38]

[33] Ibid.

[34] Brian Krebs, 'Reports: Liberty Reserve Founder Arrested, Site Shuttered,' *Krebs on Security*, May 25, 2013, https://krebsonsecurity.com/2013/05/reports-liberty-reserve-founder-arrested-site-shuttered/

[35] Catalin Cimpanu, 'Reveton ransomware distributor sentenced to six years in prison in the UK,' *ZDNET*, April 9, 2019, https://www.zdnet.com/article/reveton-ransomware-distributor-sentenced-to-six-years-in-prison-in-the-uk/

[36] This included by ransomware groups like Zeppelin, SunCrypt, Mamba, Dharma, Lockbit. United States Department of Justice, 'Justice Department Investigation Leads to Takedown of Darknet Cryptocurrency Mixer that Processed Over $3 Billion of Unlawful Transactions,' March 15, 2023, https://www.justice.gov/usao-edpa/pr/justice-department-investigation-leads-takedown-darknet-cryptocurrency-mixer-processed

[37] James Reddick, "Prolific' crypto money laundering platform ChipMixer shuttered by Germany, US,' *The Record*, March 15, 2023, https://therecord.media/chipmixer-takedown-cryptocurrency-money-laundering-europol-doj; BKA: Bundes Kriminal Amt, 'BKA schaltet weltweit größten Geldwäschedienst im Darknet ab,' March 15, 2023, https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2023/Presse2023/230314_Geldwaesche_Darknet.html

[38] US Department of Justice, 'Justice Department Investigation Leads to Takedown of Darknet Cryptocurrency Mixer that Processed Over $3 Billion of Unlawful Transactions.'

List of Key Government Countermeasures Against Cryptocurrency Exchanges and Tumblers, Linked to Ransomware

24.05.2013

Liberty Reserve digital currency service taken offline, founder arrested

Liberty Reserve, a major digital currency service used for cybercrime transactions, was taken offline, and its founder was arrested in Spain for money laundering.

21.09.2021

US sanctions Suex

The US imposed its first-ever sanctions against a cryptocurrency exchange, Suex, for facilitating ransomware payments and cybercriminal transactions.

08.11.2021

Treasury sanctions Chatex crypto exchange

The US Treasury sanctioned Chatex, a crypto exchange, for processing illicit transactions, including ransomware payments.

05.04.2022

US sanctions Hydra and Garantex

The US sanctioned Hydra, the largest Russian darknet market, and Garantex, a crypto exchange, for laundering ransomware proceeds linked to Russian cybercriminals.

06.05.2022

US Treasury sanctions Blender.io

The US Treasury sanctioned Blender.io, a Bitcoin mixer used for laundering funds linked to Russian ransomware groups.

08.08.2022

US Treasury sanctions Tornado Cash

The US Treasury sanctioned Tornado Cash, a crypto mixer, barring US citizens from using it due to its role in laundering illicit cryptocurrency.

The Need for **International Partnerships**

By presenting a wide range of prominent initiatives from around the world, this analysis risks painting too rosy a picture of government countermeasures against ransomware.

> Indeed, Russia has not only failed to take meaningful action against ransomware operations based within its borders but has also maintained active ties between its government – particularly the FSB – and criminal ransomware groups.

Yet, many governments in the West and other parts of the world still need to significantly enhance their anti-ransomware measures and commitment. In other words, the list of examples here, while demonstrating many positive government countermeasures, should not obscure the fact that many governments still do not have a comprehensive national strategy to address ransomware and have taken very little action

Part of this gap is a pressing need for greater coordination of government responses – as well as with the private sector. Cyberspace transcends traditional nation-state borders, making it easy for cybercriminals to operate from one country while targeting victims in others. Recognising this, governments have stressed the importance of international cooperation from the outset as a cornerstone of major actions against ransomware. Established international law enforcement bodies like Europol and Interpol have played key roles in coordinating comprehensive actions over the years.[39] Indeed, almost all significant operations against ransomware have involved multiple agencies from various governments.

[39] Eg the Summit on Police Ransomware already in 2011, coordinated by Europol. EUROPOL, 'Europol hosts expert meeting to combat the spread of 'Police Ransomware',' May 7, 2012, https://www.europol.europa.eu/media-press/newsroom/news/europol-hosts-expert-meeting-to-combat-spread-of-police-ransomware; Or Operation GoldDust/Quicksand: INTERPOL, 'Joint global ransomware operation sees arrests and criminal network dismantled,' November 8, 2021, https://www.interpol.int/News-and-Events/News/2021/Joint-global-ransomware-operation-sees-arrests-and-criminal-network-dismantled; Sergiu Gatlan, 'REvil ransomware affiliates arrested in Romania and Kuwait,' *Bleeping Computer*, November 8, 2021, https://www.bleepingcomputer.com/news/security/revil-ransomware-affiliates-arrested-in-romania-and-kuwait/; EUROPOL, 'Five affiliates to Sodinokibi/REvil unplugged,' November 8, 2021, https://www.europol.europa.eu/media-press/newsroom/news/five-affiliates-to-sodinokibi/revil-unplugged; Operation Cronos 2024; Lockbit Takedown EUROPOL, 'Law enforcement disrupt world's biggest ransomware operation,' February 20, 2024, https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation

Beyond these institutions, there has been a rise in direct cooperation and information exchange specifically focusing on ransomware, exemplified by the establishment of the International Counter Ransomware Initiative (established in 2021) and its Counter Ransomware Task Force (established in 2023), which includes a growing number of countries. It is these efforts that need both expansion and continuation if we are to effectively combat the global ransomware threat.[40]

This report is adapted from Max Smeets' book Ransom War: How Cyber Crime Became a Threat to National Security, published by Oxford University Press and Hurst Publishers (2025).

[40] The White House, 'Joint Statement of the Ministers and Representatives from the Counter Ransomware Initiative Meeting October 2021,' October 14, 2021, https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2021/10/14/joint-statement-of-the-ministers-and-representatives-from-the-counter-ransomware-initiative-meeting-october-2021/; Australian Department of Home Affairs, 'Global task force to fight ransomware commences operations,' January 23, 2023, https://www.homeaffairs.gov.au/news-media/archive/article?itemId=1013

References

BBC News. 'Liberty Reserve Digital Money Service Forced Offline.' May 27, 2013, sec. Technology. https://www.bbc.com/news/technology-22680297.

Biermann, Kai, Maria Fedorova, Karsten Polke-Majewski, and Hakan Tanriverdi. 'Hackergruppe Conti: Don Stern und die Hackermafia.' *Die Zeit*, December 11, 2022. https://www.zeit.de/digital/2022-12/conti-hackergruppe-russland-ransomsoftware-cyberangriffe.

BKA: Bundes Kriminal Amt. 'BKA Schaltet Weltweit Größten Geldwäschedienst Im Darknet Ab,' March 15, 2023. https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2023/Presse2023/230314_Geldwaesche_Darknet.html.

Borboën, Yan. 'Ransomware as a Business Model: Legal Aspects of Ransom Payment.' *PwC* (blog). Accessed March 7, 2025. https://www.pwc.ch/en/insights/cybersecurity/ransom-payment.html.

Burt, Tom. 'New Action to Combat Ransomware Ahead of U.S. Elections.' Microsoft On the Issues, October 12, 2020. https://blogs.microsoft.com/on-the-issues/2020/10/12/trickbot-ransomware-cyberthreat-us-elections/.

Chainalysis. 'Deadbolt Ransomware Gives Up Victim Decryption Keys.' *Chainalysis* (blog), March 1, 2023. https://www.chainalysis.com/blog/deadbolt-ransomware-strain-tricked-into-giving-up-decryption-keys/.

———. 'How the Dutch National Police Tricked Prolific Ransomware Strain Deadbolt Into Giving Up Victim Decryption Keys.' *Chainalysis* (blog), March 1, 2023. https://www.chainalysis.com/blog/deadbolt-ransomware-strain-tricked-into-giving-up-decryption-keys/.

Cimpanu, Catalin. 'Bitdefender Releases Third GandCrab Ransomware Free Decrypter in the Past Year.' *ZDNET*, February 19, 2019. https://www.zdnet.com/article/bitdefender-releases-third-gandcrab-ransomware-free-decrypter-in-the-past-year/.

———. 'Reveton Ransomware Distributor Sentenced to Six Years in Prison in the UK.' *ZDNET*, April 9, 2019. https://www.zdnet.com/article/reveton-ransomware-distributor-sentenced-to-six-years-in-prison-in-the-uk/.

CISA: Cybersecurity and Infrastructure Security Agency. 'BlackMatter Ransomware | CISA,' October 18, 2021. https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-291a.

———. 'Conti Ransomware | CISA,' March 9, 2022. https://www.cisa.gov/news-events/alerts/2021/09/22/conti-ransomware.

———. 'FBI and CISA Release Advisory on Scattered Spider Group | CISA,' November 16, 2023. https://www.cisa.gov/news-events/alerts/2023/11/16/fbi-and-cisa-release-advisory-scattered-spider-group.

———. '#StopRansomware: Black Basta | CISA,' November 8, 2024. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-131a.

———. '#StopRansomware: Daixin Team | CISA,' October 26, 2022. https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-294a.

———. '#StopRansomware: Play Ransomware | CISA,' December 18, 2023. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-352a.

CISA: Cybersecurity and Infrastructure Security Agency. 'New StopRansomware.Gov Website – The U.S. Government's One-Stop Location to Stop Ransomware | CISA,' July 15, 2021. https://www.cisa.gov/news-events/alerts/2021/07/15/new-stopransomwaregov-website-us-governments-one-stop-location-stop.

Cybereason Nocturnus. 'Dropping Anchor: From a TrickBot Infection to the Discovery of the Anchor Malware.' *Cybereason*. Accessed May 6, 2024. https://www.cybereason.com/blog/research/dropping-anchor-from-a-trickbot-infection-to-the-discovery-of-the-anchor-malware.

Emsisoft Malware Lab. 'The State of Ransomware in the U.S.: Report and Statistics 2023.' Emsisoft | Cybersecurity Blog, January 2, 2024. https://www.emsisoft.com/en/blog/44987/the-state-of-ransomware-in-the-u-s-report-and-statistics-2023/.

eSentire Threat Response Unit. 'Analysis of Leaked Conti Intrusion Procedures by ESentire's Threat....' eSentire, March 18, 2022. https://www.esentire.com/blog/analysis-of-leaked-conti-intrusion-procedures-by-esentires-threat-response-unit-tru.

EUROPOL. 'Europol Hosts Expert Meeting to Combat the Spread of 'Police Ransomware." Europol, May 7, 2012. https://www.europol.europa.eu/media-press/newsroom/news/europol-hosts-expert-meeting-to-combat-spread-of-police-ransomware.

———. 'Five Affiliates to Sodinokibi/REvil Unplugged.' Europol, November 8, 2021. https://www.europol.europa.eu/media-press/newsroom/news/five-affiliates-to-sodinokibi/revil-unplugged.

———. 'Hit by Ransomware? No More Ransom Now Offers 136 Free Tools to Rescue Your Files,' July 26, 2022. https://www.europol.europa.eu/media-press/newsroom/news/hit-ransomware-no-more-ransom-now-offers-136-free-tools-to-rescue-your-files.

———. 'Law Enforcement Disrupt World's Biggest Ransomware Operation.' Europol, February 20, 2024. https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation.

Federal Bureau of Investigation. 'FBI Flash: Mamba Ransomware.' Stop Ransomware. Accessed March 7, 2025. https://www.cisa.gov/stopransomware/fbi-flash-mamba-ransomware.

Fischerkeller, Michael P., Emily O. Goldman, and Richard J. Harknett. *Cyber Persistence Theory: Redefining National Security in Cyberspace*. Bridging the Gap. New York: Oxford University Press, 2022.

Fulterer, Ruth. 'Hydra: grösster Darknet-Markt der Welt geschlossen.' *Neue Zürcher Zeitung*, April 5, 2022, sec. Technologie. https://www.nzz.ch/technologie/deutsche-ermittler-schliessen-hydra-den-groessten-darknet-marktplatz-der-welt-ld.1678073.

Gatlan, Sergiu. 'FBI Seizes BreachForums after Arresting Its Owner Pompompurin in March.' BleepingComputer, June 23, 2023. https://www.bleepingcomputer.com/news/security/fbi-seizes-breachforums-after-arresting-its-owner-pompompurin-in-march/.

———. 'REvil Ransomware Affiliates Arrested in Romania and Kuwait.' BleepingComputer, November 8, 2021. https://www.bleepingcomputer.com/news/security/revil-ransomware-affiliates-arrested-in-romania-and-kuwait/.

Gihon, Shmuel. 'To Be CONTInued? Conti Ransomware Heavy Leaks.' Cyberint, March 9, 2022. https://cyberint.com/blog/research/contileaks/.

Goodwins, Rupert. 'Rupert Goodwins' Diary.' ZDNET, October 13, 2006. https://www.zdnet.com/article/rupert-goodwins-diary-4010004362/.

Healey, Jason, Neil Jenkins, and JD Work. 'Defenders Disrupting: Framework, Dataset, and Case Studies of Disruptive Counter-Cyber.' In *20/20 Vision: The Next Decade*, edited by T. Jančárková, L. Lindström, M. Signoretti, I. Tolga, and G. Visky, 24. Tallinn, Estonia: NATO CCDCOE Publications, 2020. https://ccdcoe.org/uploads/2020/05/CyCon_2020_14_Healey_Jenkins_Work.pdf.

Ilascu, Ionut. 'FBI Exposes Weakness in Mamba Ransomware, DiskCryptor.' BleepingComputer, March 26, 2021. https://www.bleepingcomputer.com/news/security/fbi-exposes-weakness-in-mamba-ransomware-diskcryptor/.

———. ‘TrickBot Botnet Targeted in Takedown Operations, Little Impact Seen.’ BleepingComputer, October 12, 2020. https://www.bleepingcomputer.com/news/security/trickbot-botnet-targeted-in-takedown-operations-little-impact-seen/.

Krebs, Brian. ‘Attacks Aimed at Disrupting the Trickbot Botnet – Krebs on Security.’ *Krebs on Security* (blog), October 2, 2020. https://krebsonsecurity.com/2020/10/attacks-aimed-at-disrupting-the-trickbot-botnet/.

———. ‘Reports: Liberty Reserve Founder Arrested, Site Shuttered.’ *Krebs on Security* (blog), May 25, 2013. https://krebsonsecurity.com/2013/05/reports-liberty-reserve-founder-arrested-site-shuttered/.

Lakshmanan, Ravie. ‘TrickBot Malware Gang Upgrades Its AnchorDNS Backdoor to AnchorMail.’ *The Hacker News*, May 1, 2022. https://thehackernews.com/2022/03/trickbot-malware-gang-upgrades-its.html.

Lyons, Jessica. ‘Formal Ban on Ransomware Payments? Asking Orgs Nicely to Not Cough up Ain’t Working.’ *The Register*, January 3, 2024. https://www.theregister.com/2024/01/03/ban_ransomware_payments/.

Microsoft Security Response Center. ‘Microsoft MSHTML Remote Code Execution Vulnerability: CVE-2021-40444 Security Vulnerability.’ Microsoft MSRC, September 7, 2021. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40444.

Nakashima, Ellen. ‘Cyber Command Has Sought to Disrupt the World’s Largest Botnet Hoping to Reduce Its Potential Impact on the Election.’ *The Washington Post*, October 9, 2020. https://www.washingtonpost.com/national-security/cyber-command-trickbot-disrupt/2020/10/09/19587aae-0a32-11eb-a166-dc429b380d10_story.html.

Nakashima, Ellen, and Rachel Lerman. ‘FBI Held Back Ransomware Decryption Key from Businesses to Run Operation Targeting Hackers.’ *The Washington Post*, n.d. https://www.washingtonpost.com/national-security/ransomware-fbi-revil-decryption-key/2021/09/21/4a9417d0-f15f-11eb-a452-4da5fe48582d_story.html.

Narang, Satnam. ‘ContiLeaks: Chats Reveal Over 30 Vulnerabilities Used by Conti Ransomware – How Tenable Can Help.’ *Tenable* (blog), March 24, 2022. https://www.tenable.com/blog/contileaks-chats-reveal-over-30-vulnerabilities-used-by-conti-ransomware-affiliates.

NCSC: National Cyber Security Centre. ‘Ransomware - What Next?,’ November 19, 2024. https://www.ncsc.admin.ch/ncsc/en/home/infos-fuer/infos-unternehmen/vorfall-was-nun/ransomware.html.

No More Ransom. ‘Home.’ The No More Ransom Project. Accessed March 7, 2025. https://www.nomoreransom.org/.

O’Connell, Sean. ‘To Ban Ransomeware Payments or Not to Ban Ransomware Payments: The Problems Drafting Legislation in Reponse to Ransomware.’ *Journal of International Business and Law* 22, no. 1 (December 1, 2023). https://scholarlycommons.law.hofstra.edu/jibl/vol22/iss1/6.

Operation GoldDust/Quicksand: INTERPOL. ‘Joint Global Ransomware Operation Sees Arrests and Criminal Network Dismantled,’ November 8, 2021. https://www.interpol.int/News-and-Events/News/2021/Joint-global-ransomware-operation-sees-arrests-and-criminal-network-dismantled.

Protos. ‘Dutch Police Recover 90% of Victim Decryption Keys in Ransomware Scam.’ *Protos* (blog), March 1, 2023. http://protos.com/dutch-police-recover-90-of-victim-decryption-keys-in-ransomware-scam/.

Ransomware Task Force. ‘Combating Ransomware: A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force.’ *IST: Institute for Security and Technology*, 2021. https://securityandtechnology.org/wp-content/uploads/2021/09/IST-Ransomware-Task-Force-Report.pdf.

Raywood, Dan. ‘Proposals to Ban Ransomware Payments Rumoured.’ SC Media UK, May 22, 2024. https://insight.scmagazineuk.com/proposals-to-ban-ransomware-payments-rumoured.

Reddick, James. “Prolific’ Crypto Money Laundering Platform ChipMixer Shuttered by Germany, US.’ The Record, March 15, 2023. https://therecord.media/chipmixer-takedown-cryptocurrency-money-laundering-europol-doj.

Shriebman, Yaara. 'Ransomware 2021 – The Bad, The Bad & The Ugly.' Cyberint, December 30, 2021. https://cyberint.com/blog/research/ransomware-2021-the-bad-the-bad-the-ugly/.

Stolyarov, Vlad, and Benoit Sevens. 'Exposing Initial Access Broker with Ties to Conti.' *Updates from Threat Analysis Group* (blog), March 17, 2022. https://blog.google/threat-analysis-group/exposing-initial-access-broker-ties-conti/.

United Kingdom Home Office. 'Ransomware Legislative Proposals: Reducing Payments to Cyber Criminals and Increasing Incident Reporting.' GOV.UK, February 13, 2025. https://www.gov.uk/government/consultations/ransomware-proposals-to-increase-incident-reporting-and-reduce-payments-to-criminals/ransomware-legislative-proposals-reducing-payments-to-cyber-criminals-and-increasing-incident-reporting-accessible.

United States Department of Justice. 'Emotet Botnet Disrupted in International Cyber Operation,' January 28, 2021. https://www.justice.gov/archives/opa/pr/emotet-botnet-disrupted-international-cyber-operation.

United States Department of Justice, Office of Public Affairs, Office of Public Affairs. 'Justice Department Investigation Leads to Takedown of Darknet Cryptocurrency Mixer That Processed Over $3 Billion of Unlawful Transactions,' March 15, 2023. https://www.justice.gov/usao-edpa/pr/justice-department-investigation-leads-takedown-darknet-cryptocurrency-mixer-processed.

———. 'U.S. Department of Justice Disrupts Hive Ransomware Variant,' January 26, 2023. https://www.justice.gov/archives/opa/pr/us-department-justice-disrupts-hive-ransomware-variant.

United States Department of the Treasury. 'Treasury Sanctions Russia-Based Hydra, World's Largest Darknet Market, and Ransomware-Enabling Virtual Currency Exchange Garantex.' US Department of the Treasury, January 26, 2023. https://home.treasury.gov/news/press-releases/jy0701.

United States Cyber Command. 'Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command,' April 2018, 12. https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf.

White House. 'Joint Statement of the Ministers and Representatives from the Counter Ransomware Initiative Meeting October 2021.' The White House, October 14, 2021. https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2021/10/14/joint-statement-of-the-ministers-and-representatives-from-the-counter-ransomware-initiative-meeting-october-2021/.

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