EuRepoC

ADVANCED PERSISTENT THREAT profile

Conti/Wizard Spider

Associated APT designations

- **Conti** (VMware)
- **Wizard Spider** (CrowdStrike)
- **ITG23** (IBM X-Force)
- **G0102** (MITRE ATT&CK)

Sources: [1] [2] [3]

Country of origin

Time period of activity

2019-2022

Wizard Spider has been active since 2016; Conti ransomware was first spotted in December 2019. The group shut down its infrastructure after the US State Department offered a reward of $10 million for information facilitating the identification or localisation of group members in May 2022. It has likely reorganised since then as different groups, possibly including BlackByte, BlackBasta, and Karakurt.

Sources: [2] [4] [8] [9]

Political affiliations

Prior to the war in Ukraine, the group has been "widely regarded as a semi-autonomous asset of the Russian intelligence services" by IT experts because its activity aligned with Russian security interests. Conti publicly pledged their allegiance to the Russian government after the invasion of Ukraine in Spring 2022, but revoked it after serious backlash. However, leaked documents from February 2022 indicate that some members of the group had informal ties to the Russian Federal Security Service (FSB). Sources: [4] [5] [6]

Agency type

State-tolerated cyber criminals, **with patriotic sentiments**. An IBM Security X-Force report from July 2022 noted that the group's targeting had evolved following Russia's invasion to include Ukrainian entities. Sources: [2] [6] [10]

By Kerstin Zettl-Schabath , Lena Rottinger and Camille Borrett

November 2022

Most frequent targets:

 **Australia**
 **Bahamas**
 **Canada**
 **Costa Rica**
 **France**
 **Germany**
 **India**
 **Ireland**
 **Italy**
 Japan
 **Mexico**
 **New Zealand**
 **Spain**
 **Switzerland**
 **Taiwan**
 **United Kingdom**
 **Ukraine** (since 2022)
 **USA**

According to the group's data leak site, ransomware operations targeted nearly 800 organisations across 40 countries. The majority of victims are active in the manufacturing, legal and professional services, construction and engineering, and retail sectors. As the cybersecurity firm Mandiant observed, the large share of North American targets (60%) may indicate a targeting pattern focused on North America. Sources: [7] [10] [12]

Group composition/organisational structure

The Russia-based cyber-crime group ran a ransomware-as-a-service business model, employing multiple affiliates who oversee the penetration of their victims' networks and file encryption. Usually, Russian-speaking affiliates were recruited from forums based on their experience, reputation, and activity level. Some affiliates paid Conti a commission ranging between 10-30% of their received ransom payments; others appeared to be part of a payroll system. The group regularly cooperated with other ransomware gangs such as Maze, LockBit 2.0, and Ragnar Locker. In August 2021, a former Conti affiliate "m1Geelka" leaked sensitive information about the group's organisation, training, and leadership. A few team members' online identities had been previously disclosed, including its leader/project frontman ("reshaev" aka "cybergangster"), Conti admin ("Tokyo"), an assistant, and a recruiter ("IT-Work").

The group publicly pledged allegiance to the Russian government after the invasion of Ukraine, causing a stir both within the group (among Ukrainian members and Russians supporting Ukraine), as well as other threat actors (mostly other cyber criminals) that considered involvement in political issues a business risk. Following this controversy, one of the Conti group members decided to leak private Conti chat logs and other internal information. Moreover, this pledge of allegiance led states to associate Conti with the Russian state, tying the group to the severe sanctions regime imposed in response to the aggressions against Ukraine. Any victim making a ransom payment involving a designated individual or entity, including sanctioned financial institutions to process a transaction, risked violating the sanctions framework. In the US, a single violation of sanction provisions can result in fines of up to $1 million and a 20-year prison sentence. Although the group sought to walk back the significance of its pledge, the announcement caused irreparable damage to its business and reputation. On 19 May 2022, core infrastructure components to upload victim data and run payment negotiations were switched off. Security researchers at AdvIntel have observed a surge of activity across a number of former Conti affiliates, suggesting a decentralisation away from Conti's strong vertical hierarchy as the group's core actors restructure their operations. BlackByte, BlackBasta, and Karakurt are some of the suspected subsidiaries central in this reorganisation. Sources: [4] [11] [17] [19] [23] [24]

Impact type(s)

Direct

- **Financial impact** (Conti has attacked more than 1000 victims and received over $150 million up to January 2021; Average Conti Ransom Payment: $480.333 [May 2022])
- **Business impact** (the average length of a Conti ransomware attack is 15 days)

Indirect

- **Reputational impact** (e.g., for the newly elected government of Costa Rica during/after the attack wave starting in April 2022)

Sources: [11] [13]

Incident type(s)

- **Ransomware**
- **Data Theft & Doxing**

Sources: [2] [11]

Threat Level Index

7/24 moderate level threat

Index scoring scale

Score	Label
≤6	Low
>6 - ≤12	Moderate
>12 - ≤18	High
>18 – 24	Very high

The Threat Level Index is derived from the EuRepoC dataset 1.0. It is a composite indicator covering five dimensions: the **sectorial** and **geographical scope** of the APT's attacks, the **intensity** of the attacks, the **frequency** of attacks and the **use of zero-days**. Please note that only attacks that have been publicly attributed to the APT group during its period of activity and which meet the specific EuRepoC criteria for inclusion are considered. The scores account for the practice of other APT groups analysed by EuRepoC, as thresholds used for determining low/high scores are based on the range of scores obtained across multiple APT groups. For more detailed information on the methodology underpinning the Threat Level Index see here.

Breakdown of the scores for the Conti/Wizard Spider:

Sub-indicator	Score	Explanation
Intensity of attacks	2 /5	This sub-indicator represents the average "Weighted Cyber Intensity" score from the EuRepoC codebook for all attacks attributed to the APT for its period of activity. It assesses the type of attacks, their potential physical effects, and their socio-political severity – see here for more information.
Sectorial scope of attacks	2 /8	This sub-indicator calculates average number of targeted sectors per attack attributed to the APT groups over its period of activity. If the majority of the targeted sectors are critical to the functioning of the targeted societies (i.e. political systems and critical infrastructure) a multiplier is applied. On average, attacks attributed to Conti/Wizard Spider within the EuRepoC database, targeted one type of sector. However, as 100% of the attacks were against political systems and/or critical infrastructure, the score was multiplied by 2.
Geographical scope of attacks	1 /4	This sub-indicator considers the average number of targeted countries per attack attributed to the APT group. Whole regions or continents affected during one attack are weighted higher. In the case of Conti/Wizard Spider, on average, the attacks attributed to the group within the EuRepoC database targeted only one country at a time.
Frequency of attacks	2 /4	This sub-indicator is calculated by dividing the total number of attacks attributed to the APT group within the EuRepoC database by the number of years of activity of the APT group. The obtained scores are then converted to a four-level scale. On average, Conti/Wizard Spider was held responsible for less than 1 attack per year of activity (0.67).
Exploitation of Zero days	0 /3	This indicator calculates the percentage of attacks attributed to the APT that make use of one or multiple zero days. The obtained score is then converted to a three-level scale. None of the attacks attributed to the Equation Group exploited zero-days.

→ Overall, Conti/Wizard Spider obtains a moderate threat score compared to other APT groups. The attacks analysed within the EuRepoC framework, on average, did not target many countries nor sectors in one go. In addition, none of the attacks attributed to the group exploited zero-days.

TECHNICAL CHARACTERISTICS / PECULIARITIES / SOPHISTICATION

The group runs a ransom-as-a-service (RaaS) business model and provides a digital management panel for their affiliates (other threat actors/criminals). Operating as semi-automatic recovery service, the group uses automatic network scans to identify valuable targets by spreading through compromised networks and encrypting every device and account it can find. In general, Conti uses many freely-available technologies, often developed for legitimate uses (e.g., Cobalt Strike, AnyDesk, Atera, or Tor), which the group abuses for criminal purposes. Like other ransomware threat actors, the group employs a double extortion tactic, which threatens the release of confidential data stolen by the group while exploring a victim's network if the first ransom demand to decrypt targeted systems is not met. The group is highly sophisticated, as reflected in the monetising practices of Conti's business operations, such as its money laundering techniques.

Basic attack pattern

Conti changed and updated its attack pattern on an almost daily basis, using exploits for recently-discovered software flaws and taking advantage of delayed patch deployments to target still-vulnerable networks. Within these variations in the execution, a basic attack pattern has emerged:

(1) **Target selection** (observed techniques: phishing, mass vulnerability scanning, high-end malware distribution software, credential stuffing, fake websites, impersonating)

(2) **Deployment and execution** (installation of backdoors, identification of mission-critical systems, such as domain controllers or backup servers, exfiltration of data)

(3) **Encrypting the victim's data** (using randomly-generated keys)

(4) **Sending demand and initiating negotiation** (sending a ransom note, providing communication for negotiations)

Zero-Day exploits

Conti commonly employed known vulnerabilities. But in late 2020, the group used a purchased zero-day exploit in Internet Explorer 11.

Malware used (non-exhaustive)

Conti v3.0	Trickbot	Emotet
BazarLoader	ColbaltStrike	Ryuk
ICEDID		

Sources [11] [14] [15] [16]

Select tactics and techniques leveraged by the group based on the MITRE ATT&CK Framework

MITRE Initial Access

External Remote Services
Phishing
Spearphishing attachment
Spearphishing link
Valid Accounts

MITRE Persistence

Boot or logon autostart execution
Create or modify system process
Scheduled task/job
Valid Accounts

MITRE Defense Evasion

File and directory permissions modification
Impair Defenses
Indicator removal
Masquerading
Modify Registry
Obfuscated files or information
Process injection
Subvert trust controls
Valid Accounts

MITRE Exfiltration

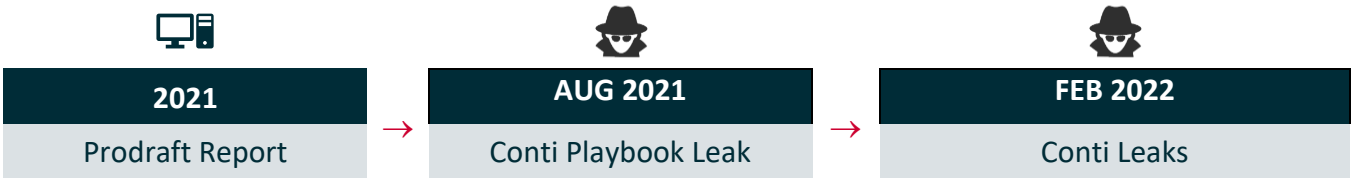
Exfiltration over alternative protocol
Exfiltration over C2 channel

MITRE Impact

Data encrypted for impact
Service Stop

ATTRIBUTION

Attribution milestones



Sources: [11] [17] [18]

Attribution controversies

Wizard Spider/Conti/Ryuk: CrowdStrike attributes operations with Conti and Ryuk malware to the same high-profile and sophisticated eCrime group, Wizard Spider. Other experts regard Conti and Ryuk as two separate threat actors that share very similar ransomware samples and bitcoin wallets, indicating a connection between the two groups. Conti's ransomware seems to be a continuation of the Ryuk ransomware. One top-level Conti operative (senior manager) apparently had contact with and access to several members of Ryuk. It is a clear example of the frequent ambiguity in distinguishing threat actors and malware samples, especially as criminal groups reorganise to avoid law enforcement.

Conti and UNC1756: The threat actor behind the deployment of Conti ransomware against the government of Costa Rica in April referred to itself as UNC1756 when it announced the operation. UNC – short for uncategorised – is a nod to the designation used by Mandiant for clusters of intrusion activity that cannot yet be linked to an identified group. Updates regarding the attack signed by UNC1756 and published via Conti's dark web PR page raised questions as to whether Conti's leadership was highlighting the work of an affiliate or whether UNC1756 was a stunt deliberately made to distract law enforcement and security researchers with a fake identity.

Conti and Maze: Researchers at Intel 471 found copied features from Maze malware in Conti's codes. Conti top-level developers were reportedly in close contact with Maze developers while the Conti malware was still in development itself.

Sources: [2] [5] [11] [19] [20]

Attribution-/detection sensitivity

Conti is known for its resilience and quick adoption of new techniques and tactics. The group adjusted its attack patterns almost daily, which is likely not a response to specific attributions but rather a preventive strategy to avoid detection. Furthermore, the group used various obfuscation techniques and weekly code changes to disrupt malware analysis systems. Sources: [2] [11]

LEGAL AND POLITICAL ACTIONS TAKEN AGAINST THE GROUP

Political/Legal/Law enforcement actions

On 6 May 2022, the US State Department announced a $10 million reward for information on Conti ransomware co-conspirators under its Rewards for Justice program, first introduced as a counterterrorism initiative. Sources: [13] [21] [22]

Indicted individuals / sanctioned (associated) entities

No individuals indicted (as of November 2022)

Landmark incidents

Irish healthcare shutdown 2021:
Ireland's Health Service Executive was hit by a major Conti ransomware attack, disrupting some health care services.

Conti's ransomware attack on Costa Rica 2022:
Conti breached several governmental institutions and agencies during a presidential transition, demanding a $10 million ransom. The new president, Rodrigo Chaves, subsequently declared a national state of emergency. The group ultimately disclosed 97% of the data it had stolen from Costa Rican entities.

Sources: [4] [5] [25]

SOURCES

[1] Baskin (2020), *TAU Threat Discovery: Conti Ransomware*, VMware Security Blog. Available at: https://blogs.vmware.com/security/2020/07/tau-threat-discovery-conti-ransomware.html [Last accessed: 29.11.2022]

[2] The CrowdStrike Intel Team (2020), *WIZARD SPIDER Update: Resilient, Reactive and Resolute*, Crowdstrike Blog. Available at: https://www.crowdstrike.com/blog/wizard-spider-adversary-update/ [Last accessed: 29.11.2022]

[3] Villadsen and Hammond (2021), *Trickbot Rising – Gang Doubles Down on Infection Efforts to Amass Network Footholds*, Security Intelligence. Available at: https://securityintelligence.com/posts/trickbot-gang-doubles-down-enterprise-infection/ [Last accessed: 29.11.2022]

[4] Bogusalvskiy and Kremez (2022), *DisCONTInued: The End of Conti's Brand Marks New Chapter For Cybercrime Landscape*, AdvIntel. Available at: https://www.advintel.io/post/discontinued-the-end-of-conti-s-brand-marks-new-chapter-for-cybercrime-landscape [Last accessed: 29.11.2022]

[5] Ferrett (2022), *Conti Attack on Costa Rica: Who is UNC1756?*, Searchlight Security. Available at: https://www.slcyber.io/blog/conti-attack-on-costa-rica-who-is-unc1756 [Last accessed: 29.11.2022]

[6] Burgess (2022), *Leaked Ransomware Docs Show Conti Helping Putin From The Shadows*, Wired. Available at: https://www.wired.co.uk/article/conti-ransomware-russia [Last accessed: 29.11.2022]

[7] Mandiant (2022), *Keeping up with CONTI*, Mandiant. Available at: https://www.mandiant.com/resources/conti-ransomware [Last accessed: 29.11.2022]

[8] Naeem (2022), *CONTI*, MITRE ATT&CK. Available at: https://attack.mitre.org/software/S0575/ [Last accessed: 29.11.2022]

[9] Cyble Team (2021), *Conti Ransomware Resurfaces, Targeting Government & Large Organizations*, Cyble Blog. Available at: https://blog.cyble.com/2021/01/21/conti-ransomware-resurfaces-targeting-government-large-organizations/ [Last accessed: 29.11.2022]

[10] Villadsen et al. (2022), *Unprecedented Shift: The Trickbot Group is Systemically Attacking Ukraine*, SecurityIntelligence. Available at: https://securityintelligence.com/posts/trickbot-group-systematically-attacking-ukraine/ [Last accessed: 29.11.2022]

[11] PTI Team (2021), *Conti Ransomware Group In-Depth Analysis*, Prodaft: Proactive Defense Against Future Threats. Available at: https://www.prodaft.com/m/reports/Conti_TLPWHITE_v1.6_WVcSEtc.pdf [Last accessed: 29.11.2022]

[12] Unit 42 Team (2022), *Conti-Ransomware*, Unit 42. Available at: https://unit42.paloaltonetworks.com/atoms/conti-ransomware/ [Last accessed: 29.11.2022]

[13] Gatlan (2022), *US Offers $15 Million Reward for Info on Conti Ransomware Gang*, BleepingComputer. Available at: https://www.bleepingcomputer.com/news/security/us-offers-15-million-reward-for-info-on-conti-ransomware-gang/ [Last accessed: 29.11.2022]

[14] CISA, FBI, and NSA (2022), *Joint Cybersecurity Advisory: Conti Ransomware*, CISA. Available at: https://www.cisa.gov/uscert/sites/default/files/publications/AA21-265A-Conti_Ransomware_TLP_WHITE.pdf [Last accessed: 29.11.2022]

[15] Comeau (2022), *The Conti Ransomware Leaks: Six Takeaways*, Tech Decisions. Available at: https://mytechdecisions.com/network-security/conti-ransomware-leaks/ [Last accessed: 29.11.2022]

[16] Millington and Gayda (2020), *Wizard Spider*, MITRE ATT&CK. Available at: https://attack.mitre.org/groups/G0102/ [Last accessed: 29.11.2022]

[17] Abrams (2021), *Angry Conti Ransomware Affiliate Leaks Gang's Attack Playbook*, BleepingComputer. Available at: https://www.bleepingcomputer.com/news/security/angry-conti-ransomware-affiliate-leaks-gangs-attack-playbook/ [Last accessed: 29.11.2022]

[18] Fokker and Tologonov (2022), *Conti Leaks: Examining the Panama Papers of Ransomware*, Trellix. Available at: https://www.trellix.com/en-us/about/newsroom/stories/research/conti-leaks-examining-the-panama-papers-of-ransomware.html [Last accessed: 29.11.2022]

[19] Intel 471 Team (2022), *Cybercrime Loves Company: Conti cooperated with other ransomware gangs*, Intel 471. Available at: https://intel471.com/blog/conti-ransomware-cooperation-maze-lockbit-ragnar-locker [Last accessed: 29.11.2022]

[20] Hanel and Stone-Gross (2019), *WIZARD SPIDER Adds New Features to Ryuk for Targeting Hosts on LAN*, Crowdstrike Blog. Available at: https://www.crowdstrike.com/blog/wizard-spider-adds-new-feature-to-ryuk-ransomware/ [Last accessed: 29.11.2022]

[21] Price (2022), *Reward Offers for Information to Bring Conti Ransomware Variant Co-Conspirators to Justice*, United States Department of State. Available at: https://www.state.gov/reward-offers-for-information-to-bring-conti-ransomware-variant-co-conspirators-to-justice/ [Last accessed: 29.11.2022]

[22] Rewards for Justice (2022), *Conti*, US State Department. Available at: https://rewardsforjustice.net/rewards/conti/ [Last accessed: 29.11.2022]

[23] Sulkin and Schaetzel (2022), *Ransomware Response Complicated by Growing Number of Sanctions in Wake of Russian Invasion of Ukraine*, Benesch: Data Meets World. Available at: https://www.datameetsworld.com/blog/ransomware-response-complicated-by-growing-number-of-sanctions-in-wake-of-russian-invasion-of-ukraine [Last accessed: 29.11.2022]

[24] Office of Foreign Assets Control (2021), *Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments*, Department of the Treasury. Available at: https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf [Last accessed: 29.11.2022]

[25] Sharma (2022), *Costa Rica Declares National Emergency After Conti Ransomware Attacks*, BleepingComputer. Available at: https://www.bleepingcomputer.com/news/security/costa-rica-declares-national-emergency-after-conti-ransomware-attacks/ [Last accessed: 29.11.2022]

Calculations for the Threat Level Index Indicator are based on version 1.0 of the EuRepoC Database downloadable here: https://strapi.eurepoc.eu/uploads/Eu_Repo_C_Global_Database_1_0_22d4a4aee7.xlsx

Last updated: 30.11.2022