Ransomware gang Conti published data of 850 companies | Group-IB

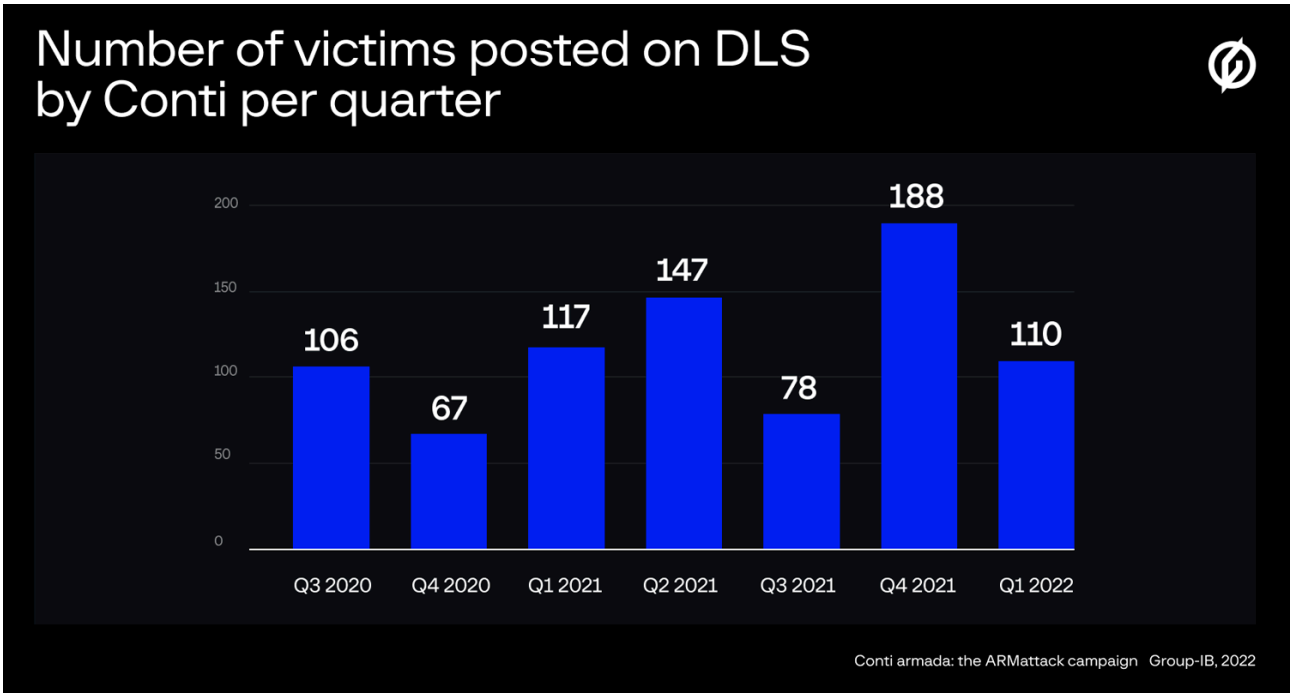
Archived: 2026-05-01 02:36:05 UTC

Group-IB, one of the global leaders in cybersecurity and headquartered in Singapore, has today presented its findings about ARMattack, one of the shortest yet most successful campaigns by the Russian-speaking ransomware gang Conti. In slightly more than a month, the notorious ransomware collective compromised more than 40 companies worldwide. The fastest attack took only three days according to Group-IB's report "CONTI ARMADA: ARMATTACK CAMPAIGN". In two years, the ransomware operators attacked more than 850 victims including corporations, government agencies, and even a whole country. The research dives deep into the history and major milestones of one of the most aggressive and organized ransomware operations.

Double hit

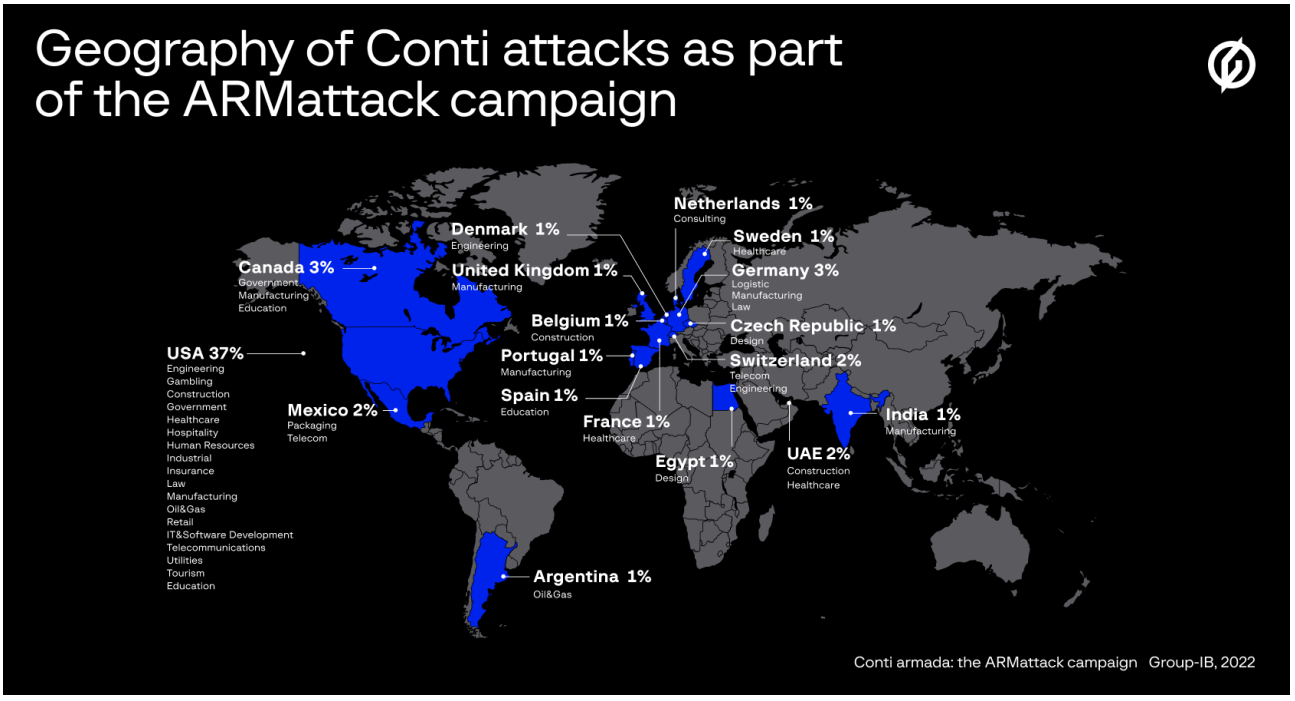
Conti is considered one of the most successful ransomware groups. The gang's existence first came to light in February 2020, when malicious files with the extension ".conti" appeared on the radar of Group-IB researchers. However, the initial test versions of the malware date back to November 2019.

Since 2020, Conti has been dominating the ransomware scene alongside Maze and Egregor in terms of the number of companies whose data has been encrypted. In 2020, Conti published data belonging to 173 victims on their dedicated leak site (DLS). By the end of 2021, Conti came out on top as one of the largest and most aggressive groups, having published data belonging to 530 companies on its DLS. In just four months in 2022, the group posted information belonging to 156 companies, making for a total of 859 DLS victims in two years, including 46 in April 2022. The actual number of victims is believed to be significantly higher.



On a roll

Conti and their affiliates attack often and quickly. Group-IB experts analyzed one of the group's lightning-fast and most productive campaigns, codenamed "ARMattack". The campaign lasted only about a month (from November 17 to December 20, 2021), but it turned out to be extremely effective. The attackers compromised more than 40 organizations worldwide. Most attacks were carried out in the US (37%), but the campaign also surged through Europe, with victims in Germany (3%), Switzerland (2%), the Netherlands, Spain, France, the Czech Republic, Sweden, and Denmark (1% each). The group also attacked organizations in the UAE (2%) and India (1%).



Historically, the top five industries most frequently targeted by Conti are manufacturing (14%), real estate (11.1%), logistics (8.2%), professional services (7.1%), and trade (5.5%). After gaining access to a company's infrastructure, the threat actors exfiltrate specific documents (most often to determine what organization they are dealing with) and look for files containing passwords (both plaintext and encrypted). Lastly, after acquiring all the necessary privileges and gaining access to all the devices they are interested in, the hackers deploy ransomware to all the devices and run it.

According to the Group-IB Threat Intelligence team, the gang's fastest attack was carried out in exactly three days, from initial access to data encryption. Group-IB for the first time analyzed Conti's "working hours". Most likely, the group members are located in different time zones; however, the schedule shows their high efficiency: on average, Conti "works" 14 hours a day without holidays (except for "New Year holidays") and weekends. The group starts working closer to noon (GMT+3) and its activity declines only after 9:00 PM.

The geography of Conti's attacks is vast but does not include Russia. The group clearly adheres to the unspoken rule among Russian-speaking cybercriminals: do not attack Russian companies. Most attacks occur in the United States (58.4%), followed by Canada (7%), the United Kingdom (6.6%), Germany (5.8%), France (3.9%), and Italy (3.1%).

Another reason behind not targeting Russian companies is that key Conti members refer to themselves as “patriots”. This fact was the cause of an “internal conflict” in the group in February 2022, which resulted in some of Conti’s valuable information being leaked online. The published data included private chat logs, the servers they use, a list of victims, and details of Bitcoin wallets, which stored over 65,000 BTC in total. The leaked chats revealed that the group had faced serious financial difficulties and that their boss had gone off the radar. Yet its members were fully prepared to restart the project after 2 to 3 months.

Despite the “stab in the back” and increased attention from law enforcement, Conti’s appetites continued to increase. They attacked not only large companies, but entire countries as well. Conti’s “cyber war” against Costa Rica in April 2022 led to a state of emergency being declared.

Incentive program

Conti has worked closely with other ransomware operators such as Ryuk, Netwalker, LockBit, and Maze. They even tested Maze’s ransomware, reverse-engineered it, and thereby significantly improved their own. An analysis of the ARMattack campaign revealed that the group’s arsenal included not only previously described Windows tools, but also Linux ransomware: Conti and Hive.

That said, the group tends to create unique tools without reusing code snippets. This way, when compared, the code for their tools will not help identify common patterns. Before the chat logs were leaked, cybersecurity researchers could only assume that some RaaS (Ransomware-as-a-service) affiliate programs were in fact Conti divisions. At the same time, the interaction was extensive. Sometimes Conti used network access from other initial access brokers, other times the gang shared their own access for a modest 20% of the revenue.

Just like a legitimate IT business, Conti has its own HR, R&D, and OSINT departments. There are team leads, regular salary payments, and an incentive program.

One of Conti’s distinctive features is using new vulnerabilities, which helps the group gain initial access. For instance, Conti was seen exploiting the recent CVE-2021-44228, CVE-2021-45046 and CVE-2021-45105 vulnerabilities in the log4j module. Less than a week later, Conti exploited these vulnerabilities to attack vCenter servers. The leaked chat logs also showed that the group monitors fresh vulnerabilities carefully. One of the tasks from Conti’s CEO to the technical team was to monitor Windows updates and analyze changes made with new patches — which once again highlights the need to install updates as soon as possible. In addition, the Conti crew includes specialists with experience in discovering zero-days.

Conti’s increased activity and the data leak suggest that ransomware is no longer a game between average malware developers, but an illicit RaaS industry that gives jobs to hundreds of cybercriminals worldwide with various specializations. In this industry, Conti is a notorious player that has in fact created an “IT company” whose goal is to extort large sums. It is difficult to predict what will happen to Conti in the future: whether it will continue working after a large-scale rebranding or be divided into smaller sub-projects. It is clear, however, that the group will continue its operations, either on its own or with the help of its “subsidiary” projects.

Ivan Pisarev

Head of Dynamic Malware Analysis Team at Group-IB's Threat Intelligence department

As always, Group-IB's analytical report entitled "CONTI ARMADA: THE ARMATTACK CAMPAIGN" provides companies and technical specialists with indicators of compromise and information about Conti's techniques, tactics and tools mapped to the MITRE ATT&CK® matrix.

About Group-IB

Established in 2003, Group-IB is a leading creator of predictive cybersecurity technologies to investigate, prevent, and fight digital crime globally. Headquartered in Singapore, and with Digital Crime Resistance Centers in the Americas, Europe, Middle East and Africa, Central Asia, and the Asia-Pacific, Group-IB delivers predictive, intelligence-driven defense by analysing and neutralizing regional and country-specific cyber threats via its Unified Risk Platform, offering unparalleled defense through its industry-leading Cyber Fraud Intelligence Platform, Cloud Security Posture Management, Threat Intelligence, Fraud Protection, Digital Risk Protection, Managed Extended Detection and Response (XDR), Business Email Protection, and External Attack Surface Management solutions, catering to government, retail, healthcare, gaming, financial sectors, and beyond. Group-IB collaborates with international law enforcement agencies like INTERPOL, Europol, and AFRIPOL to fortify cybersecurity worldwide, and has been awarded by advisory agencies including Datos Insights, Gartner, Forrester, Frost & Sullivan, and KuppingerCole.

For more information, visit us at www.group-ib.com or connect with us on LinkedIn, X, Facebook, and Instagram.

Discover our podcasts to hear from leading voices on Masked Actors and Fraud Intel, where top cybersecurity experts share real-world experiences, emerging trends, and practical insights to help you stay one step ahead in the fight against cyber crime.

Source: https://www.group-ib.com/media/conti-armada-report/