Global Operations Lead to Arrests of Alleged Members of GandCrab/REvil and Cl0p Cartels

trendmicro.com/en_in/research/21/k/global-operations-lead-to-arrests-of-alleged-members-of-gandcrab.html

November 16, 2021

A total of 13 suspects believed to be members of two prolific cybercrime rings were arrested as a global coalition across five continents involving law enforcement and private partners, including Trend Micro, sought to crack down on big ransomware operators.

About the GandCrab/REvil arrests

According to a report by Interpol, the global operation, which was done by 19 law enforcement agencies in 17 countries, led to the apprehension of seven suspects linked as “affiliates” or partners of GandCrab/REvil. The group is a prominent ransomware network deemed responsible for more than 7,000 attacks since early 2019.

Code-named Quicksand (GoldDust), the operation was a collaboration between Interpol, Europol, law enforcement agencies, and private firms. Each contributed to the four-year-long investigations by sharing information and technical expertise.

REvil (aka Sodinokibi) and GandCrab, believed to be manned by the same individuals, peddle ransomware-as-a-service (Raas), renting out ransomware code to other cybercriminals. Set up with groups known as affiliates, the scheme includes intrusions into companies, deployment of ransomware, and demand for ransom, after which profits are shared with the rest of the coders.

A report by Europol estimates that over €200 million in ransom demands had been made collectively since 2019 by the seven suspects from all the attacks that were carried out.

The formidable global coalition enabled the following:

- Korean law enforcement's arrest of three suspects in February, April, and October
- Kuwaiti authorities' arrest of a man who allegedly carried out ransomware attacks using the GandCrab ransomware
- Romanian authorities' arrest of two individuals suspected of ransomware cyberattacks and linked to more than 5,000 infections and half a million euros in ransom payments
- The arrest of a man suspected of deploying the Kaseya ransomware attack, thought to have been done in July 2021 by the REvil group with more than 1,500 people and 1,000 businesses affected worldwide

Trend Micro's monitoring of GandCrab/REvil

Trend Micro has kept a close eye on this malware family since as early as 2018, when we reported the discovery of GandCrab v4.3, which targeted South Korean users through spam emails. The spam emails used EGG (.egg) files to deliver the GandCrab v4.3 ransomware (detected by Trend Micro as Ransom_GANDCRAB.TIAOBHO). EGG is a compressed archive file format (similar to ZIP) that is commonly used in South Korea. Evidence indicated that the attack was aimed toward South Korean users for its use of Hangul in the subject, body, and attachment file name of the spam emails.

In 2019, Trend Micro announced another noteworthy GandCrab ransomware attack, also in South Korea. Spam emails made the rounds with the subject "SHIPPED ORDER INCORRECT." The messages posed as shipping order notifications from a known courier delivery service company and were designed to dupe the recipients into opening the email attachment. As with the first attack, the email body was written in Korean and contained a RAR attachment that supposedly contained information on the parcel.

About the Cl0p arrest

Another milestone for the global public-private alliance aimed at dismantling cybercrime rings is the arrest of six suspected members of the ransomware group Cl0p, following a 30-month joint investigation into attacks against South Korean companies and US academic institutions.

The task force, acted on the request by South Korea's cybercrime investigation division, enabled the arrest of alleged gang members in Ukraine. The operation involved Interpol, Europol, and law enforcement authorities in South Korea, Ukraine, and the US in June.

Codenamed Operation Cyclone, it had global police pursuing the Cl0p malware operators in Ukraine for allegedly targeting private businesses in South Korea and the US. Interpol reports that Cl0p's attacks impeded access to their computer files and networks, and

subsequently demanded huge ransoms for restoring access.

The suspects allegedly facilitated the transfer and cash-out of assets on the ransomware group's behalf while threatening to release sensitive data to the public if demands for additional payments were declined. The six suspects are believed to be closely connected to a Russian-language cybercrime network known for naming and shaming its victims on a Tor leak site and, more notably, for amassing more than US$500 million in funds related to several ransomware attacks. Cl0p's activities target essential infrastructures and industries, such as transportation and logistics, education, manufacturing, energy, financial, aerospace, telecommunications, and healthcare.

Operation Cyclone was deployed with assistance and information given by Trend Micro and other private cybersecurity firms. The synergy in intelligence gathering enabled the Ukrainian police to search more than 20 houses, businesses, and vehicles, and seize property, computers, and cash amounting to US$185,000.

Trend Micro's monitoring of Cl0p

Trend Micro Research has written extensively about Cl0p and other ransomware actors as it helps organisations to effectively deal with ransomware attacks.

Cl0p (unstylized as Clop) first became known as a variant of the CryptoMix ransomware family. In 2020, the group behind Cl0p publicised the data of a pharmaceutical company in its maiden attempt at the double extortion scheme. Since then, the group's extortion tactics have become increasingly sophisticated and thus more destructive.

Operators hold their target organisation under duress by sending out emails to initiate negotiations. If messages are ignored, they threaten to publicise and auction off stolen data on the data leak site "Cl0p^_-Leaks". In addition, Cl0p ransomware operators employ other extortion techniques, such as going after top executives and customers to pressure companies to pay up.

Defending networks and systems from ransomware

Thwarting ransomware requires collaborative efforts from both law enforcement agencies and private companies like cybersecurity vendors. For its part, Trend Micro has been collaborating with law enforcement agencies to provide them with threat intelligence needed to aid in their investigations in order to combat ransomware and other cyberthreats.

There is no doubt that ransomware will persist as a significant security threat, one that is expected to multiply and advance in complexity. As we've seen, ransomware rapidly evolves into an even more destructive threat. To protect networks and systems from ransomware, organisations and users are advised to follow these best practices:

- Avoid downloading attachments and clicking on links in emails from unverified sources.

- Regularly patch and update operating systems, programs, and software.
- Periodically back up files by observing the 3-2-1 rule: Create at least three copies of the data, store it in two different formats, and keep at least one duplicate off-site.
- Follow security frameworks such as those set by the Center of Internet Security and the National Institute of Standards and Technology to reduce overall risk levels and exposure to threats and vulnerabilities that ransomware operators may use.

As threat actors are always waiting for the opportunity to pounce on the next victim, investing in cross-layered detection and response solutions can save organisations a lot of headache and expense. Trend Micro Vision One™ with Managed XDR is a cybersecurity platform that provides visibility into the early activities of modern ransomware attacks to help detect and block ransomware components so that attacks are thwarted even before cybercriminals are able to exfiltrate sensitive data.