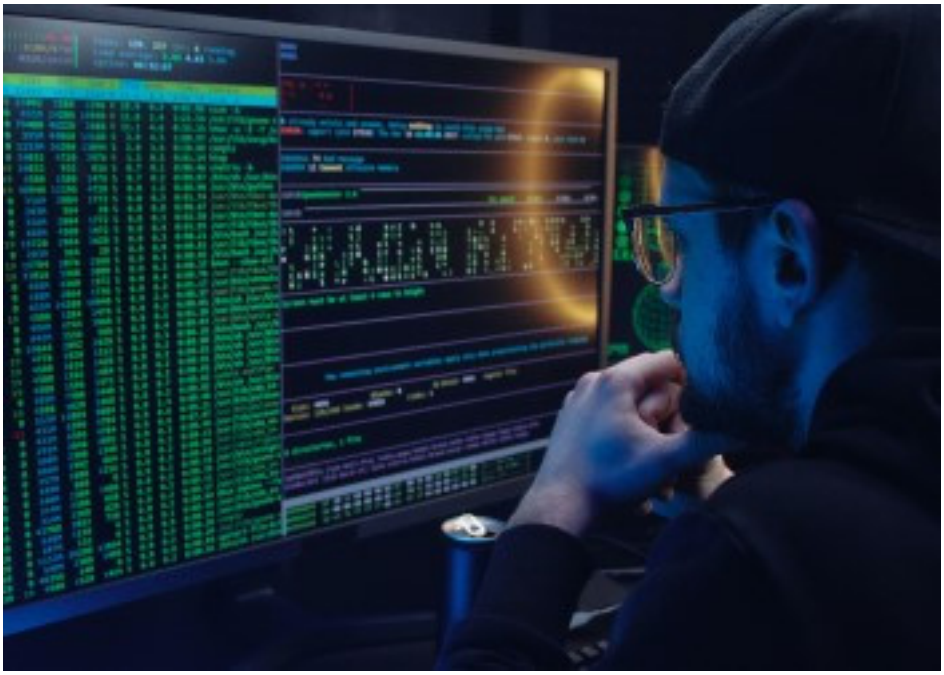
Five ransomware gangs and their tactics (part two)

Learn which ransomware gangs pose the most threat in 2022 and uncover the tactics they employ

---

Adam Jeffs
07/01/2022



Ransomware continues in an upwards trend and attacks have increased by 13% in 2022 compared with the previous year, according to Verizon's 2022 Data Breach Investigations Report.

With this in mind, it is clear that malicious threat actors are prolific and pose a significant threat to any organization that cannot boast solid cyber security.

Following on from CS Hub's article *five active ransomware gangs and their tactics (part one)*, we look into five more of the top ransomware gangs that pose a threat to organizational cyber security.

BlackMatter

BlackMatter is a ransomware-as-a-service (RaaS) tool first identified in July 2021. The Cybersecurity and Infrastructure Security Agency (CISA) has noted that BlackMatter may be a possible rebrand of DarkSide, an RaaS outfit active from September 2020 through May 2021.

It is believed that BlackMatter is responsible for an data breach involving NEW Cooperative, an Iowa-based farmer's cooperative, which was subjected to a ransomware attack in September 2021. Those responsible for the attack claimed to have stolen 1,000 GB of data including the source code for the soilmap.com project, financial information, network information, R&D results, sensitive employee information and legal and executive information and demanded a $5.9mn ransom for its return.

The RaaS uses embedded admin or user credentials that have been compromised to enumerate running processes and services. BlackMatter then uses these credentials in the lightweight directory access protocol (LDAP) and server message block (SMB) protocol to discover all hosts in the active directory.

Ryuk

First identified in 2017, Ryuk is a form of ransomware and a common payload for banking Trojans. Ryuk has been one of the most active and successful ransomware organizations in recent years, with the US Federal Bureau of Investigation (FBI) estimating that victims paid over $61mn to recover files encrypted by Ryuk as of November 2020. Research by SonicWall revealed that it was one of the top three most prolific perpetrators in 2021.

Initial versions of Ryuk were not able to automatically move laterally through a network, however a newer version was detected in January 2021 that displayed “worm-like capabilities” that can spread copies of itself between devices without the need for human interaction or to attach itself to a specific software program.

CLOP

CLOP is a ransomware variant associated with the FIN11 threat actor group that applies the popular double extortion ransomware tactic, in which threat actors will exfiltrate stolen data so that they can threaten its release or sale if the ransom is not paid.

Initially going into circulation in February 2019, the ransomware has been implicated in attacks on the healthcare and public health sector after discovering weaknesses in the Accellion File Transfer Appliance product and began targeting its users. As well as employing the double extortion tactic, CLOP actors also combine ‘spray and pray’ tactics with more targeted approaches, suggesting there is operator discretion in who is targeted.

DopplePaymer

DopplePaymer ransomware has been used to encrypt data from victims within critical industries worldwide such as healthcare, emergency services and education since August 2019, disrupting public access to these services, according to the FBI cyber division.

These actors employ the double extortion tactic and demand six or seven figure sums to be paid in Bitcoin. DopplePaymer actors have also been known to contact victims via phone calls to pressure them into paying the ransom.

A DopplePaymer attack in September 2020 that targeted a hospital in Germany left emergency services unable to communicate with the hospital, resulting in patients being rerouted to other facilities, some more than 20 miles away. After being contacted by German authorities, DopplePaymer provided a digital decryption key upon learning that patient’s lives were in danger.

REvil

REvil is a ransomware first discovered by Cisco in April 2019 and the threat actors involved offer REvil as an RaaS as well as maintaining an active leak

site and engaging in distributed-denial-of-service (DDoS) and phishing attacks, among other malicious activities.

The US Department of Health and Human Services notes that the operators of the ransomware are known as ‘Gold Southfield’ and ‘Pinchy Spider’ and have stated that they do not target Commonwealth of Independent States or Syria.

REvil, also known as Sodinokibi, is believed to have begun as Gandcrab, an earlier ransomware identified in January 2018. They are believed to be connected as in 2019, threat actors deployed both REvil and Gandcrab in the same attack, with SecureWorks even suggesting that REvil was directly developed from a version of Gandcrab