# Core DoppelPaymer ransomware gang members targeted in Europol operation

bleepingcomputer.com/news/security/core-doppelpaymer-ransomware-gang-members-targeted-in-europol-operation/

Bill Toulas

By
Bill Toulas

- March 6, 2023
- 09:00 AM
- 0

Europol has announced that law enforcement in Germany and Ukraine targeted two individuals believed to be core members of the DoppelPaymer ransomware group.

The operation consisted in raiding multiple locations in the two countries on February and was the result of a coordinated effort that also involved Europol, the FBI and the Dutch Police.

## Two suspects detained

"German officers raided the house of a German national, who is believed to have played a major role in the DoppelPaymer ransomware group," Europol informs in a press release published today.

The agency notes that "despite the current extremely difficult security situation that Ukraine" due to the Russian invasion, police officers in the country "interrogated a Ukrainian national who is also believed to be a member of the core DoppelPaymer group."

German officers raided one location - the house of the German national believed to have had a "major role in the DoppelPaymer ransomware group." In Ukraine, the police searched two locations - in Kiev and Kharkiv.

Electronic equipment has been seized and investigators and IT experts are examining it for forensic evidence.

Three experts from Europol have also been deployed to Germany to cross-check operational information with information from Europol's databases and to help with analysis, crypto tracing, and forensic work.

"The analysis of this data and other related cases is expected to trigger further investigative activities," Europol says. This work may reveal other members of the ransomware group as well as affiliates that deployed the malware and ransomed victims across the world.

Both the investigation and the legal procedures are ongoing at the moment.

## Three more DoppelPaymer suspects wanted

German authorities believe that the DoppelPaymer ransomware operation involved five core members that maintained the attack infrastructure, the data leak sites, handled negotiations, and deployed the malware on breached networks.

Arrest warrants have been issued for another three suspects that law enforcement are currently looking for worldwide:

- Igor Garshin/Garschin - believed to be responsible for reconnaissance, breaching, and deploying the DoppelPaymer locker on victim networks
- Igor Olegovich Turashev - believed to have had a major part in attacks against German companies, acting as the admin of the infrastructure and malware used for intrusions
- Irina Zemlianikina - responsible for the initial stage of the attack, sending out malicious emails; she was also handling the data leak sites, the chat system, and publishing the data stolen from the victims

According to the German police, the five suspects are the "masterminds" of the DoppelPaymer ransomware gang and are connected to Russia.

## DoppelPaymer ransomware

The DoppelPaymer ransomware operation emerged in 2019 targeting critical infrastructure organizations and large companies.

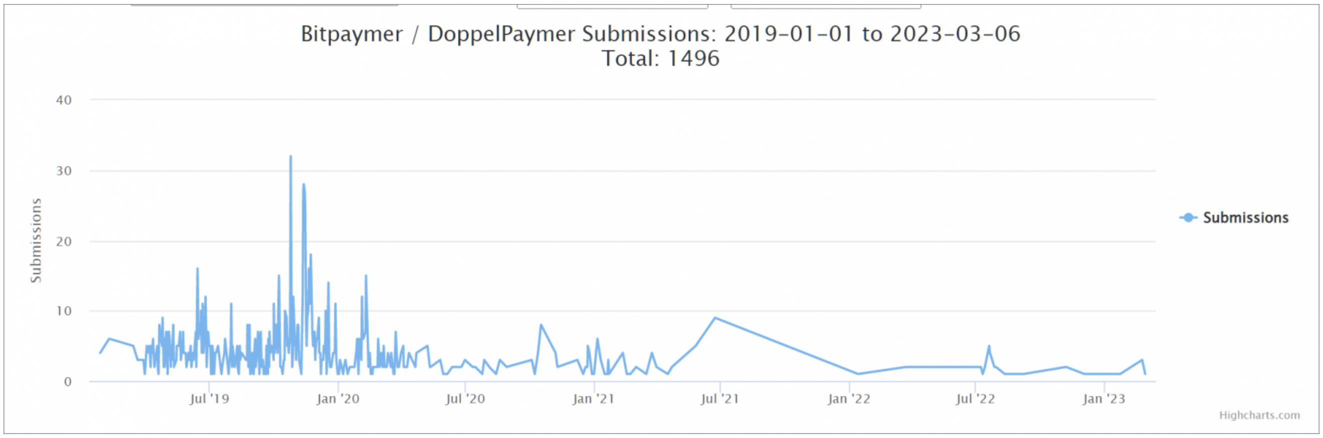
In 2020, the threat actor started to steal data from the victim networks and adopted the double extortion method by threatening to publish the stolen files on a leak site on the Tor network.

Europol estimates that between May 2019 and March 2021, victims based in the United States alone paid DoppelPaymer at least $42.4 million. The German authorities have also confirmed 37 cases where companies were targeted by the ransomware gang.

The DoppelPaymer malware is based on the BitPaymer ransomware. The file-encrypting threat was delivered through Dridex malware, which was pushed by the infamous Emotet botnet.

The infection vector was spear-phishing emails containing documents with malicious VBS or JavaScript code. The threat actor also used a legitimate tool, Process Hacker, to terminate security-related products running on the victim systems.

Although the operation rebranded as "Grief" (Pay or Grief) in July 2021 in an attempt to escape law enforcement, attacks became more sparse.



**DoppelPaymer attack rate drops**
source: ID-Ransomware

Among DoppelPaymer's high-profile victims are Kia Motors America, the Delaware County in Pennsylvania (paid a $500,000 ransom), laptop maker Compal, the Newcastle University (files leaked), electronics giant Foxconn, and the Dutch Research Council (NWO).

To force victims into paying the ransom, the operators of the DoppelPaymer ransomware threatened to wipe the decryption keys if victims contracted professional negotiators to obtain a better price for recovering the locked data.

However, the attack frequency decreased to the point that the gang no longer maintains the leak site.

**UPDATE [March 6, 11:10 AM EST]**: Article updated with new information about three more suspects sought by law enforcement for their major role in the DoppelPaymer ransomware operation.

## Related Articles:

Australian police arrest four BEC actors who stole $1.7 million

RAT developer arrested for infecting 10,000 PCs with malware

ChipMixer platform seized for laundering ransomware payments, drug sales

The Week in Ransomware - March 10th 2023 - Police Take Action

Dutch Police arrest three ransomware actors extorting €2.5 million

Bill Toulas

Bill Toulas is a technology writer and infosec news reporter with over a decade of experience working on various online publications. An open source advocate and Linux enthusiast, is currently finding pleasure in following hacks, malware campaigns, and data breach incidents, as well as by exploring the intricate ways through which tech is swiftly transforming our lives.