Zeus, IcedID malware gangs leader pleads guilty, faces 40 years in prison

bleepingcomputer.com/news/security/zeus-icedid-malware-gangs-leader-pleads-guilty-faces-40-years-in-prison/

Sergiu Gatlan

By
Sergiu Gatlan

- February 15, 2024
- 06:05 PM
- 2

Ukrainian national Vyacheslav Igorevich Penchukov, one of the heads of the notorious JabberZeus cybercrime gang, has pleaded guilty to charges related to his leadership roles in the Zeus and IcedID malware groups.

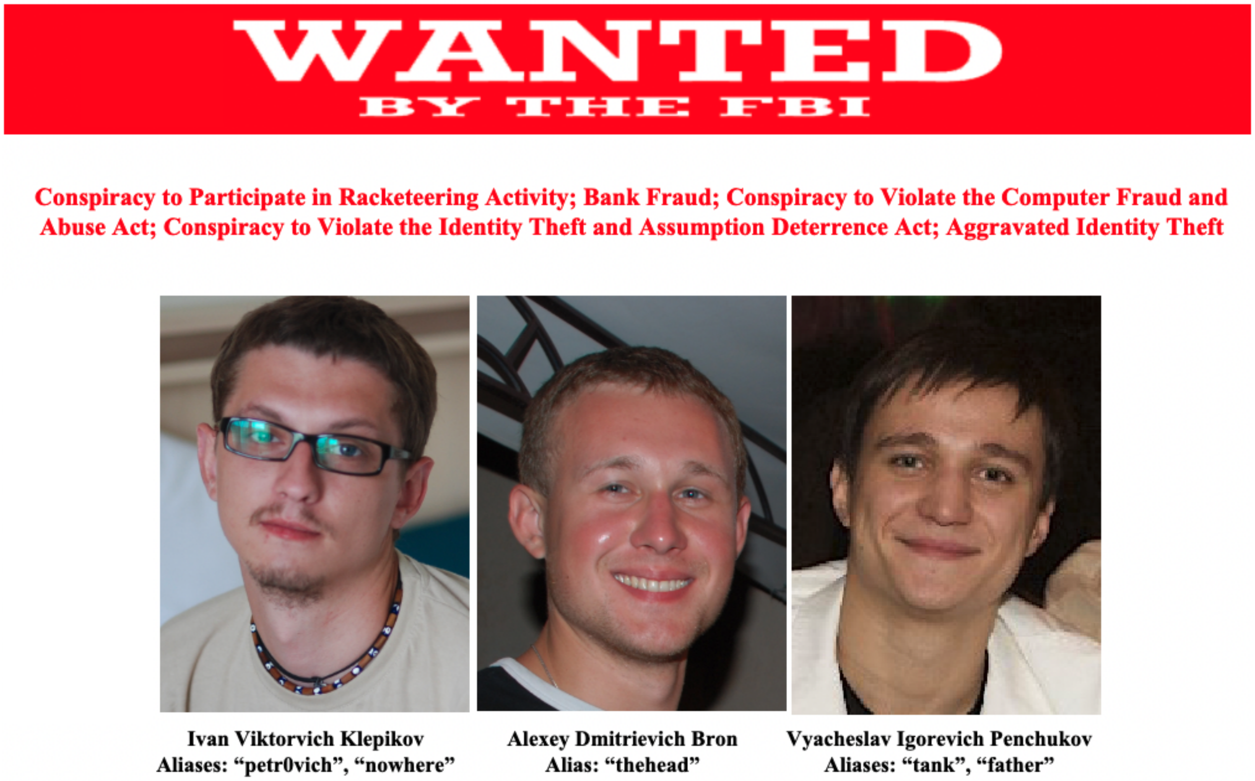
Penchukov (also known as 'tank' and 'father') was arrested in Switzerland in October 2022 while traveling to meet his wife in Geneva and extradited to the United States in 2023.

The U.S. Department of Justice first charged him in 2012 for his involvement in the Zeus malware operation and the theft of millions of dollars using personal identification numbers, bank account numbers, credentials, and other sensitive info stolen from infected devices.

Multiple sources also told BleepingComputer that Penchukov was part of the leadership of the Maze and Egregor ransomware operations. Maze was the first ransomware gang involved in double-extortion attacks where stolen data was used as leverage to pressure victims.

Maze ransomware was later rebranded to Egregor and Sekhmet to evade law enforcement. Despite this, Penchukov was among the suspects arrested in January 2021 by Ukrainian police as part of a joint international operation targeting the Egregor ransomware gang.

However, as investigative journalist Brian Krebs reported, he evaded prosecution using his political connections, including the late son of former Ukrainian President Viktor Yanukovych.



WANTED
BY THE FBI

Conspiracy to Participate in Racketeering Activity; Bank Fraud; Conspiracy to Violate the Computer Fraud and Abuse Act; Conspiracy to Violate the Identity Theft and Assumption Deterrence Act; Aggravated Identity Theft

Ivan Viktorvich Klepikov
Aliases: “petr0vich”, “nowhere”

Alexey Dmitrievich Bron
Alias: “thehead”

Vyacheslav Igorevich Penchukov
Aliases: “tank”, “father”

JABBERZEUS wanted poster (FBI)

Penchukov was also part of the leadership of the IcedID (aka Bokbot) malware operation after being added to the FBI's Cyber Most Wanted List between November 2018 and February 2021.

He and his co-conspirators used the malware to steal the victims' sensitive information, including banking account credentials, and to provide other cybercriminals with access to compromised systems to deploy additional malicious payloads like ransomware.

"Vyacheslav Igorevich Penchukov was a leader of two prolific malware groups that infected thousands of computers with malicious software. These criminal groups stole millions of dollars from their victims and even attacked a major hospital with ransomware, leaving it unable to provide critical care to patients for over two weeks," said Acting Assistant Attorney General Nicole M. Argentieri.

"Before his arrest and extradition to the United States, the defendant was a fugitive on the FBI's most wanted list for nearly a decade."

Penchukov entered a guilty plea to one charge of conspiracy related to racketeering under the Racketeer Influenced and Corrupt Organizations (RICO) Act for his leadership role in the Zeus operation and to another charge of conspiracy to commit wire fraud for his leadership role in the IcedID malware group.

Scheduled for sentencing on May 9, Penchukov faces a potential maximum penalty of 20 years imprisonment for each count.

Related Articles:

Hacker arrested for selling bank accounts of US, Canadian users

PurpleFox malware infects thousands of computers in Ukraine

Germany takes down cybercrime market with over 180,000 users

CISA warns of Microsoft Streaming bug exploited in malware attacks

New Bifrost malware for Linux mimics VMware domain for evasion