Multiple Foreign Nationals Charged in Connection with Trickbot Malware and Conti Ransomware Conspiracies

Press Release

Thursday, September 7, 2023

For Immediate Release
Office of Public Affairs

Three indictments in three different federal jurisdictions have been unsealed charging multiple Russian cybercrime actors involved in the Trickbot malware and Conti ransomware schemes.

According to court documents and public reporting, Trickbot, which was taken down in 2022, was a suite of malware tools designed to steal money and facilitate the installation of ransomware. Hospitals, schools, and businesses were among the millions of Trickbot victims who suffered tens of millions of dollars in losses. While active, Trickbot malware, which acted as an initial intrusion vector into victim computer systems, was used to support various ransomware variants, including Conti. Conti was a ransomware variant used to attack more than 900 victims worldwide, including victims in approximately 47 states, the District of Columbia, Puerto Rico, and approximately 31 foreign countries. According to the FBI, in 2021, Conti ransomware was used to attack more critical infrastructure victims than any other ransomware variant.

“The Justice Department has taken action against individuals we allege developed and deployed a dangerous malware scheme used in cyberattacks on American school districts, local governments, and financial institutions,” said Attorney General Merrick B. Garland. “Separately, we have also taken action against individuals we allege are behind one of the most prolific ransomware variants used in cyberattacks across the United States, including attacks on local police departments and emergency medical services. These actions should serve as a warning to cybercriminals who target America’s critical infrastructure that they cannot hide from the United States Department of Justice.”

“Today’s announcement shows our ongoing commitment to bringing the most heinous cyber criminals to justice – those who have devoted themselves to inflicting harm on the American public, our hospitals, schools, and businesses,” said FBI Director Christopher Wray. “Cyber criminals know that we will use every lawful tool at our disposal to identify them, tirelessly pursue them, and disrupt their criminal activity. We, alongside our federal and international partners, will continue to impose costs through joint operations no matter where these criminals may attempt to hide.”

“The defendants charged in these three indictments across three different jurisdictions allegedly used their cyber knowledge and capabilities to victimize people and businesses around the world without regard for the damage they caused,” said Acting Assistant Attorney General Nicole M. Argentieri of the Justice Department’s Criminal Division. “These indictments should serve as a reminder that no matter a cybercriminal’s location, we will identify and pursue them by doing everything in our power to ensure they face the consequences of their actions.”

“Conti ransomware was used to exploit our financial systems and target hundreds of innocent victims,” said Special Agent in Charge William Mancino of the U.S. Secret Service’s Criminal Investigative Division. “The Secret Service will continue to work with our local, state, and federal law enforcement partners to investigate cybercriminals and bring offenders to justice.”

As detailed below, a federal grand jury in the Northern District of Ohio returned an indictment charging Maksim Galochkin, aka Bentley; Maksim Rudenskiy, aka Buza; Mikhail Mikhailovich Tsarev, aka Mango; Andrey Yuryevich Zhuykov, aka Defender; Dmitry Putilin, aka Grad and Staff; Sergey Loguntsov, aka Begemot and Zulas; Max Mikhaylov, aka Baget; Valentin Karyagin, aka Globus; and Maksim Khaliullin, aka Maxfax, Maxhax, and Kagas, all Russian nationals, with conspiring to use the Trickbot malware to steal money and personal and confidential information from unsuspecting victims, including businesses and financial institutions located in the United States and around the world, beginning in November 2015.

A federal grand jury in the Middle District of Tennessee returned an indictment charging Galochkin, Rudenskiy, Tsarev, and Zhuykov with conspiring to use Conti ransomware to attack businesses, nonprofits, and governments in the United States beginning in 2020 and continuing through June 2022.

A federal grand jury in the Southern District of California returned an indictment charging Galochkin in connection with the Conti ransomware attack on Scripps Health on May 1, 2021.

Northern District of Ohio

The indictment returned in the Northern District of Ohio charged all nine defendants for their alleged roles in developing, deploying, managing, and profiting from the malware known as Trickbot. Trickbot was a sophisticated, modular, multi-functional suite of malware tools which (a) infected victims’ computers with malware designed to capture victims’ online banking login credentials; (b) obtained and harvested other personal identification information, including credit cards, emails, passwords, dates of birth, social security numbers, and addresses; (c) infected other computers connected to the victim computer; (d) used the captured login credentials to fraudulently gain unauthorized access to victims’ online bank accounts at

financial institutions; (e) stole funds from victims' bank accounts and laundered those funds using U.S. and foreign beneficiary bank accounts provided and controlled by the defendants and co-conspirators; and (f) installed ransomware on victim computers.

"As alleged in the indictment, Trickbot infected millions of computers worldwide, including those used by hospitals, schools, and businesses," said U.S. Attorney Rebecca C. Lutzko for the Northern District of Ohio. "Today's announcement demonstrates that these dangerous cybercriminals are not anonymous, as they once believed. The indictments unsealed today show the resolve of the international community to work together to bring cybercriminals to justice. We will continue to use all resources at our disposal to stop cybercrime."

Each defendant is charged with one count of conspiracy to violate the Computer Fraud and Abuse Act, one count of wire fraud conspiracy, and one count of conspiracy to launder the proceeds of the scheme. The indictment also included an enhancement for falsely registering domains. If convicted, each defendant faces a maximum penalty of 62 years in prison.

Trickbot malware developers Alla Witte and Vladimir Dunaev were previously indicted and apprehended. Witte, a Latvian national pleaded guilty to conspiracy to commit computer fraud and was sentenced to 32 months in June 2023. Dunaev, a Russian national, currently is in custody and pending trial in Cleveland.

Middle District of Tennessee

The Middle District of Tennessee indictment charges that the individuals behind Conti ransomware, including Galochkin, Rudenskiy, Tsarev, and Zhuykov, conspired to use Conti to attack hundreds of victims. Conti's victims included hospital systems, local governments, and foreign governments. Conti conspirators allegedly extorted funds from victims in the Middle District of Tennessee and encrypted the computer systems of a local sheriff's department, a local police department, and local emergency medical services, among others. Ransom notes left on Conti victims' computer systems typically boasted "if you don't [know Conti] – just 'google it.'"

"The conspirators who developed and deployed Conti ransomware victimized businesses, governments, and non-profits around the world, including a sheriff's office and an emergency medical service in Tennessee," said U.S. Attorney Henry C. Leventis for the Middle District of Tennessee. "We will continue to use the full power of this office to ensure that hackers can no longer hide behind their computer screens and to hold them accountable."

Galochkin was a "crypter" for Conti, modifying the ransomware so that it would not be detected by anti-virus programs; Rudenskiy was a developer who supervised other Conti developers; Tsarev was a manager of other Conti conspirators; and Zhuykov was a systems administrator who managed users of Conti infrastructure, organized and paid for infrastructure and tools, and assisted in problem solving infrastructure-related issues.

Galochkin, Rudenskiy, Tsarev, and Zhuykov are each charged with one count of conspiracy to violate the Computer Fraud and Abuse Act and one count wire fraud conspiracy. If convicted, each defendant faces a maximum penalty of 25 years in prison.

Southern District of California

As alleged in the Southern District of California indictment, Galochkin caused the transmission of the Conti malware and impaired the medical examination, diagnosis, treatment, and care of one or more individuals.

Galochkin is charged with three counts of computer hacking. If convicted, he faces a maximum penalty of 20 years in prison.

“The indictment alleges a callous disregard for the medical care and the personal information of residents of the Southern District of California,” said Acting U.S. Attorney Andrew R. Haden for the Southern District of California. “This office is committed to protecting victims of cybercrime and holding perpetrators accountable.”

The FBI Cleveland Field Office is leading the investigation into Trickbot malware.

Assistant U.S. Attorneys Daniel Riedl and Duncan Brown for the Northern District of Ohio and Senior Counsel Candina Heath of the Criminal Division’s Computer Crime and Intellectual Property Section are prosecuting the Trickbot malware case.

The FBI San Diego, Memphis, and El Paso Field Offices, with U.S. Secret Service, are leading the investigation into Conti ransomware. The U.S. Attorney’s Office for the Western District of Texas provided significant assistance.

Assistant U.S. Attorney Taylor J. Phillips for the Middle District of Tennessee, Assistant U.S. Attorneys Jonathan Shapiro and Kareem Salem for the Southern District of California, and Trial Attorney Sonia V. Jimenez and Senior Counsel Ryan K.J. Dickey of the Criminal Division’s Computer Crime and Intellectual Property Section are prosecuting the Conti ransomware cases.

The Justice Department’s National Security Division provided significant assistance in the Conti ransomware and Trickbot malware investigations.

An indictment is merely an allegation. All defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

Northern District of Ohio indictment
Middle District of Tennessee indictment
Southern District of California indictment
Updated September 7, 2023

Topic

Cybercrime

Press Release Number: 23-975