Latvian National Charged for Alleged Role in Transnational Cybercrime Organization

Press Release

Friday, June 4, 2021

For Immediate Release
Office of Public Affairs

A Latvian national was arraigned in federal court in Cleveland, Ohio, today on multiple charges stemming from her alleged role in a transnational cybercrime organization responsible for creating and deploying a computer banking trojan and ransomware suite of malware known as “Trickbot.”

Alla Witte, aka Max, 55, is charged in 19 counts of a 47-count indictment, which accuses her of participating in a criminal organization referred to as the “Trickbot Group,” which deployed the Trickbot malware. The Trickbot Group operated in Russia, Belarus, Ukraine, and Suriname, and primarily targeted victim computers belonging to businesses, entities, and individuals, including those in the Northern District of Ohio and elsewhere in the United States. Targets included hospitals, schools, public utilities, and governments. Witte, who previously resided in Paramaribo, Suriname, was arrested on Feb. 6, in Miami, Florida.

“This indictment demonstrates the broad reach of the Department of Justice’s Ransomware and Digital Extortion Task Force,” said Deputy Attorney General Lisa O. Monaco. “Trickbot infected millions of victim computers worldwide and was used to harvest banking credentials and deliver ransomware. The defendant is accused of working with others in the transnational criminal organization to develop and deploy a digital suite of malware tools used to target businesses and individuals all over the world for theft and ransom. These charges serve as a warning to would-be cybercriminals that the Department of Justice, through the Ransomware and Digital Extortion Task Force and alongside our partners, will use all the tools at our disposal to disrupt the cybercriminal ecosystem.”

“The Trickbot malware was designed to steal the personal and financial information of millions of people around the world, thereby causing extensive financial harm and inflicting significant damage to critical infrastructure within the United States and abroad,” said Acting U.S. Attorney Bridget M. Brennan of the Northern District of Ohio. “Federal law enforcement, along with assistance provided by international partners, continue to fight and disrupt ransomware and malware where feasible. We are united in our efforts to hold transnational hackers accountable for their actions.”

“Witte and her associates are accused of infecting tens of millions of computers worldwide, in an effort to steal financial information to ultimately siphon off millions of dollars through compromised computer systems,” said Special Agent in Charge Eric B. Smith of the FBI’s Cleveland Field Office. “Cyber intrusions and malware infections take significant time, expertise, and investigative effort, but the FBI will ensure these hackers are held accountable, no matter where they reside or how anonymous they think they are.”

The indictment alleges that beginning in November 2015, Witte and others stole money and confidential information from unsuspecting victims, including businesses and their financial institutions in the United States, United Kingdom, Australia, Belgium, Canada, Germany, India, Italy, Mexico, Spain, and Russia through the use of the Trickbot malware.

Witte and her co-conspirators allegedly worked together to infect victim computers with the Trickbot malware designed to capture online banking login credentials and harvest other personal information, including credit card numbers, emails, passwords, dates of birth, social security numbers and addresses. Witte and others also allegedly captured login credentials and other stolen personal information to gain access to online bank accounts, execute unauthorized electronic funds transfers and launder the money through U.S. and foreign beneficiary accounts.

According to the indictment, Witte worked as a malware developer for the Trickbot Group and wrote code related to the control, deployment, and payments of ransomware. The ransomware informed victims that their computer was encrypted, and that they would need to purchase special software through a Bitcoin address controlled by the Trickbot Group to decrypt their files. In addition, Witte allegedly provided code to the Trickbot Group that monitored and tracked authorized users of the malware and developed tools and protocols to store stolen login credentials.

Witte is charged with one count of conspiracy to commit computer fraud and aggravated identity theft; one count of conspiracy to commit wire and bank fraud affecting a financial institution; eight counts of bank fraud affecting a financial institution; eight counts of aggravated identity theft and one count of conspiracy to commit money laundering. The defendant was arraigned before U.S. Magistrate Judge William H. Baughman Jr. of the U.S. District Court for the Northern District of Ohio. If convicted, she faces a maximum penalty of five years in prison for conspiracy to commit computer fraud and aggravated identity theft; 30 years in prison for conspiracy to commit wire and bank fraud; 30 years in prison for each substantive bank fraud count; a two-year mandatory sentence for each aggravated identity theft count, which must be served

consecutively to any other sentence; and 20 years in prison for conspiracy to commit money laundering. A federal district court judge will determine any sentence after considering the U.S. Sentencing Guidelines and other statutory factors.

The FBI's Cleveland Office investigated the case.

Senior Counsel C.S. Heath of the Criminal Division's Computer Crime and Intellectual Property Section and Assistant U.S. Attorneys Daniel J. Riedl and Duncan T. Brown of the Northern District of Ohio are prosecuting the case.

This case is part of the Department of Justice's Ransomware and Digital Extortion Task Force, which was created to combat the growing number of ransomware and digital extortion attacks. As part of the Task Force, the Criminal Division, working with the U.S. Attorneys' Offices, prioritizes the disruption, investigation, and prosecution of ransomware and digital extortion activity by tracking and dismantling the development and deployment of malware, identifying the cybercriminals responsible, and holding those individuals accountable for their crimes. The department, through the Task Force, also strategically targets the ransomware criminal ecosystem as a whole and collaborates with domestic and foreign government agencies as well as private sector partners to combat this significant criminal threat.

An indictment is merely an allegation and the defendant is presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

Updated June 4, 2021

Cybercrime

Identity Theft

Press Release Number: 21-524