

Weekly Intelligence Brief

A Chanticleer Intelligence Brief Project



ShinyHunters Targets FBI Employment Website

Atticus Brandenburg
Analyst
Cyber Desk

On SEP 22, the cybercriminal group ShinyHunters claimed responsibility for an attack against the U.S. Federal Bureau of Investigation's (FBI) official employment website, FBIJobs.gov. The group reportedly exploited a vulnerability in Oracle PeopleSoft, a human resources management platform, to steal between two and three terabytes of sensitive data, including Social Security numbers, home addresses, job assignments, and family information belonging to FBI employees and applicants. ShinyHunters claimed the attack was in retaliation for an FBI advisory accusing the group of cyber extortion, harassment, and swatting.

Authorities subsequently arrested three suspected members. On SEP 15, Dutch authorities arrested 24-year-old Pepijn van der Stap, known by the alias "Umbreon," in Amsterdam. On SEP 29, Jordanian authorities detained Saif al-Din Khader, known by the alias "Rey," who reportedly is cooperating with investigators. On OCT 9, the FBI arrested Canadian cybersecurity expert Edward Dubrovsky in Pennsylvania. Dubrovsky previously helped companies respond to cyberattacks and authored *Cyber Extortion Strategic Response*, published the month before his arrest. Federal authorities reportedly consider him a primary co-conspirator in the FBI breach. Dubrovsky was charged with

conspiracy to commit extortion. The details of the charges against him remain under seal in Texas. He is expected to be transported there to face these charges.

These attacks and arrests highlight the growing threat posed by transnational cybercriminals that exploit software vulnerabilities in order to obtain sensitive information. We assess with high confidence that groups such as ShinyHunters will continue to pose a significant cybersecurity risk to governments. Their cross-border operations complicate law enforcement efforts to identify, investigate, and prosecute suspected members, thus increasing challenges for international cooperation and cybersecurity defenses.

Mysterious Death at Russian Anti-Plague Lab Raises Questions

Cody Hitchcock
Senior Analyst
Global Threats Desk

On 2 OCT, Darya Shipilova, a 28-year-old laboratory technician at the Irkutsk Anti-Plague Research Institute of Siberia, died after hospitalization due to a severe pneumonia of unknown cause. The institute was created to monitor and control plague across Siberia and Russia's Far East, where the bacterium exists in wildlife. The institute was also allegedly used as a facility to weaponize plague and other viruses during the Soviet era.

Initial reports suggested that Shipilova may have been exposed to the virus after breaking a test vial containing

plague bacteria, although this remains unconfirmed. Russian authorities continue to deny the incident, while reports state Shipilova and her contacts tested negative for plague.

It is important to note plague is not a virus; it is caused by the bacterium *Yersinia pestis*, which is found in small mammals and fleas. The pneumonic form affects the lungs and spreads person to person through particulates like saliva. Common antibiotics may be effective with an early diagnosis; however, it can be fatal without quick treatment.

Russian media reported that 197 people who may have come in contact with Shipilova were identified. Of those,

189 were hospitalized for medical observation. President Trump spoke with reporters on Monday 5 OCT regarding the case and stated that the U.S. is willing to help Russia and will monitor the case closely. Although the cause remains unresolved, no linked spread has been identified. We can access with high confidence that it is likely countries will continue to closely follow developments in the case.



AI-Assisted Cyberattacks Target South Korean Banks

Robert Samano
Analyst
Cyber Desk

On 6 OCT, South Korean authorities expanded an investigation into cyberattacks targeting at least nine banks since late September. Investigators suspect that a China-based cyber attacker used artificial intelligence (AI) tools, including the Chinese-developed ARTEX AI agent, to assist in the intrusions. Cybersecurity firm CrowdStrike reportedly connected the activity to the suspected attacker. The breaches exposed customer information, although no major financial theft has been reported.

The attacks raised concerns about security weaknesses within South

Korea's financial sector, prompting South Korean President Lee Jae Myung to order a broader investigation. ARTEX was originally developed as an open-source tool to identify security vulnerabilities, but reports suggest it was repurposed for offensive cyber operations. Its developer subsequently removed the tool from public access. The identity of the attacker remains unconfirmed, and available reporting does not establish whether the attacker belonged to a Chinese advanced persistent threat (APT) group. The incidents demonstrate how AI tools could help attackers identify potential weaknesses and thus target financial institutions more efficiently.

We assess with moderate confidence that AI-assisted cyberattacks against

financial institutions will increase as these tools become more accessible. We also assess that similar methods could threaten U.S. banks and critical infrastructure. Additionally, we assess with moderate confidence that financial institutions will increase investment in AI-assisted threat detection and monitoring. These developments highlight the growing importance of cybersecurity defenses as attackers adopt more advanced technologies.



Weekly Intelligence Brief

Editor-in-Chief
Connor Ellinghaus

Associate Editors
Malena Santa Ana
Olivia Connell
Anna Howard

For access to past issues and other Chanticleer Intelligence Brief projects, visit our website, cibrief.org/publications/wib

