Justice Department Announces Court-Authorized Disruption of Snake Malware Network Controlled by Russia's Federal Security Service

Press Release

Tuesday, May 9, 2023

For Immediate Release
Office of Public Affairs

Through Operation MEDUSA, the FBI, and the U.S. Attorney's Office for the Eastern District of New York Neutralized the FSB's Premier Cyberespionage Malware Implant in Coordination with Multiple Foreign Governments

The Justice Department today announced the completion of a court-authorized operation, code-named MEDUSA, to disrupt a global peer-to-peer network of computers compromised by sophisticated malware, called "Snake", that the U.S. Government attributes to a unit within Center 16 of the Federal Security Service of the Russian Federation (FSB). For nearly 20 years, this unit, referred to in court documents as "Turla," has used versions of the Snake malware to steal sensitive documents from hundreds of computer systems in at least 50 countries, which have belonged to North Atlantic Treaty Organization (NATO) member governments, journalists, and other targets of interest to the Russian Federation. After stealing these documents, Turla exfiltrated them through a covert network of unwitting Snake-compromised computers in the United States and around the world.

Operation MEDUSA disabled Turla's Snake malware on compromised computers through the use of an FBI-created tool named PERSEUS, which issued commands that caused the Snake malware to overwrite its own vital components. Within the United States, the operation was executed by the FBI pursuant to a search warrant issued by U.S. Magistrate Judge Cheryl L. Pollak for the Eastern District of New York, which

authorized remote access to the compromised computers. This morning, the court unsealed redacted versions of the affidavit submitted in support of the application for the search warrant, and of the search warrant issued by the court. For victims outside the United States, the FBI is engaging with local authorities to provide both notice of Snake infections within those authorities' countries and remediation guidance.

"The Justice Department, together with our international partners, has dismantled a global network of malware-infected computers that the Russian government has used for nearly two decades to conduct cyber-espionage, including against our NATO allies," said Attorney General Merrick B. Garland. "We will continue to strengthen our collective defenses against the Russian regime's destabilizing efforts to undermine the security of the United States and our allies."

"Through a high-tech operation that turned Russian malware against itself, U.S. law enforcement has neutralized one of Russia's most sophisticated cyber-espionage tools, used for two decades to advance Russia's authoritarian objectives," said Deputy Attorney General Lisa O. Monaco. "By combining this action with the release of the information victims need to protect themselves, the Justice Department continues to put victims at the center of our cybercrime work and take the fight to malicious cyber actors."

"For 20 years, the FSB has relied on the Snake malware to conduct cyberespionage against the United States and our allies – that ends today," said Assistant Attorney General Matthew G. Olsen of the Justice Department's National Security Division. "The Justice Department will use every weapon in our arsenal to combat Russia's malicious cyber activity, including neutralizing malware through high-tech operations, making innovative use of legal authorities, and working with international allies and private sector partners to amplify our collective impact."

"Russia used sophisticated malware to steal sensitive information from our allies, laundering it through a network of infected computers in the United States in a cynical attempt to conceal their crimes. Meeting the challenge of cyberespionage requires creativity and a willingness to use all lawful means to protect our nation and our allies," said U.S. Attorney Breon Peace for the Eastern District of New York. "The court-authorized remote search and remediation announced today demonstrates my office and our partners' commitment to using all of the tools at our disposal to protect the American people."

"Today's announcement demonstrates the FBI's willingness and ability to pair our authorities and technical capabilities with those of our global partners to disrupt malicious cyber actors," said Assistant Director Bryan Vorndran of the FBI's Cyber Division. "When it comes to combating Russia's attempts to target the United States and our allies using complex cyber tools, we will not waver in our work to dismantle those efforts. When it comes to any nation state engaged in cyber intrusions which put our national security at risk, the FBI will leverage all tools available to impose cost on those actors and to protect the American people."

As detailed in court documents, the U.S. Government has been investigating Snake and Snake-related malware tools for nearly 20 years. The U.S. government has monitored FSB officers assigned to Turla conducting daily operations using Snake from a known FSB facility in Ryazan, Russia.

Although Snake has been the subject to several cybersecurity industry reports throughout its existence, Turla has applied numerous upgrades and revisions, and selectively deployed it, all to ensure that Snake remains Turla's most sophisticated long-term cyberespionage malware implant. Unless disrupted, the Snake implant persists on a compromised computer's system indefinitely, typically undetected by the machine's owner or authorized users. The FBI has observed Snake persist on particular computers despite a victim's efforts to remediate the compromise.

Snake provides its Turla operators the ability to remotely deploy selected malware tools to extend Snake's functionality to identify and steal sensitive information and documents stored on a particular machine. Most importantly, the worldwide collection of Snake-compromised computers acts as a covert peer-to-peer network, which utilizes customized communication protocols designed to hamper detection, monitoring, and collection efforts by Western and other signals intelligence services.

Turla uses the Snake network to route data exfiltrated from target systems through numerous relay nodes scattered around the world back to Turla operators in Russia. For example, the FBI, its partners in the U.S. Intelligence Community, together with allied foreign governments, have monitored the FSB's use of the Snake network to exfiltrate data from sensitive computer systems, including those operated by NATO member governments, by routing the transmission of these stolen data through unwitting Snake-compromised computers in the United States.

As described in court documents, through analysis of the Snake malware and the Snake network, the FBI developed the capability to decrypt and decode Snake communications. With information gleaned from monitoring the Snake network and analyzing Snake malware, the FBI developed a tool named PERSEUS which establishes communication sessions with the Snake malware implant on a particular computer, and issues commands that causes the Snake implant to disable itself without affecting the host computer or legitimate applications on the computer.

Today, to empower network defenders worldwide, the FBI, the National Security Agency, the Cybersecurity and Infrastructure Security Agency, the U.S. Cyber Command Cyber National Mission Force, and six other intelligence and cybersecurity agencies from each of the Five Eyes member nations issued a joint cybersecurity advisory (the Joint Advisory) with detailed technical information about the Snake malware that will allow cybersecurity professionals to detect and remediate Snake malware infections on their networks. The FBI and U.S. Department of State are also providing additional information to local authorities in countries where computers that have been targeted by the Snake malware have been located.

Although Operation MEDUSA disabled the Snake malware on compromised computers, victims should take additional steps to protect themselves from further harm. The operation to disable Snake did not patch any vulnerabilities or search for or remove any additional malware or hacking tools that hacking groups may have placed on victim. The Department of Justice strongly encourages network defenders to review the Joint Advisory for further guidance on detection and patching. Moreover, as noted in court documents, Turla

frequently deploys a “keylogger” with Snake that Turla can use to steal account authentication credentials, such as usernames and passwords, from legitimate users. Victims should be aware that Turla could use these stolen credentials to fraudulently re-access compromised computers and other accounts.

The FBI has provided notice of the court-authorized operation to all owners or operators of the computers remotely accessed pursuant to the search warrant.

Assistant U.S. Attorney Ian C. Richardson for the Eastern District of New York is prosecuting the case, with valuable assistance provided by the National Security Division’s Counterintelligence and Export Control Section.

The efforts to disrupt the Snake malware network were led by the FBI New York Field Office, FBI’s Cyber Division, the U.S. Attorney’s Office for the Eastern District of New York, and the National Security Division’s Counterintelligence and Export Control Section. The Criminal Division’s Computer Crime and Intellectual Property Section provided valuable assistance. Those efforts would not have been successful without the partnership of numerous private-sector entities, including those victims who allowed the FBI to monitor Snake communications on their systems.

Updated May 9, 2023

Attachment
23-MJ-0428 Affidavit [PDF, 383 KB]
Topics

Countering Nation-State Threats

National Security

Cybercrime

Press Release Number: 23-530