U.S. Leads Multi-National Action Against “Gameover Zeus” Botnet and “Cryptolocker” Ransomware, Charges Botnet Administrator

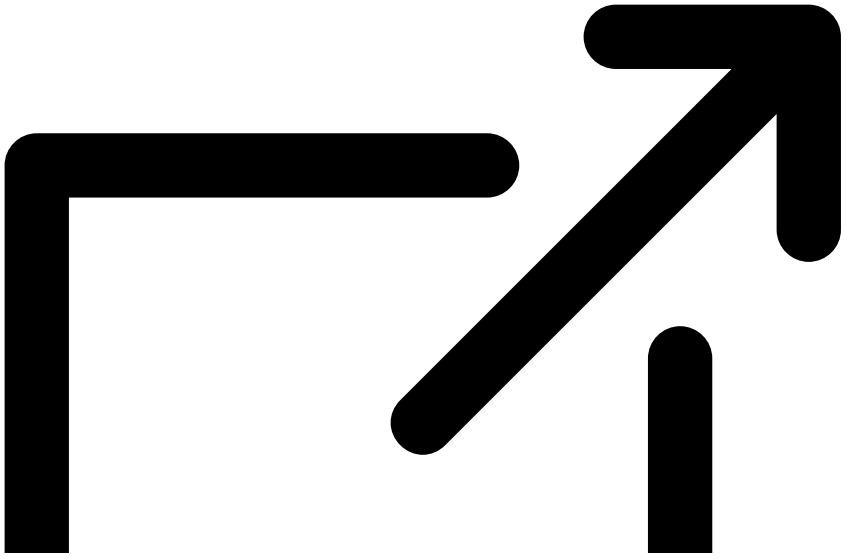
Published: 2014-06-02 · Archived: 2026-04-05 21:56:02 UTC

The Justice Department today announced a multi-national effort to disrupt the Gameover Zeus Botnet – a global network of infected victim computers used by cyber criminals to steal millions of dollars from businesses and consumers – and unsealed criminal charges in Pittsburgh, Pennsylvania, and Omaha, Nebraska, against an administrator of the botnet. In a separate action, U.S. and foreign law enforcement officials worked together to seize computer servers central to the malicious software or “malware” known as Cryptolocker, a form of “ransomware” that encrypts the files on victims’ computers until they pay a ransom.

Deputy Attorney General James M. Cole, Assistant Attorney General Leslie R. Caldwell of the Justice Department’s Criminal Division, FBI Executive Assistant Director Robert Anderson Jr., U.S. Attorney David J. Hickton of the Western District of Pennsylvania, U.S. Attorney Deborah R. Gilg of the District of Nebraska, and Department of Homeland Security’s (DHS) Deputy Under Secretary Dr. Phyllis Schneck made the announcement.

Victims of Gameover Zeus may use the following website created by DHS’s Computer Emergency Readiness Team (US-CERT) for assistance in removing the malware:

https://www.us-cert.gov/gameoverzeus



.

“This operation disrupted a global botnet that had stolen millions from businesses and consumers as well as a complex ransomware scheme that secretly encrypted hard drives and then demanded payments for giving users access to their own files and data,” said Deputy Attorney General Cole. “We succeeded in disabling Gameover Zeus and Cryptolocker only because we blended innovative legal and technical tactics with traditional law enforcement tools and developed strong working relationships with private industry experts and law enforcement counterparts in more than 10 countries around the world.”“These schemes were highly sophisticated and immensely lucrative, and the cyber criminals did not make them easy to reach or disrupt,” said Assistant Attorney General Caldwell. “But under the leadership of the Justice Department, U.S. law enforcement, foreign partners in more than 10 different countries and numerous private sector partners joined together to disrupt both these schemes. Through these court-authorized operations, we have started to repair the damage the cyber criminals have caused over the past few years, we are helping victims regain control of their own computers, and we are protecting future potential victims from attack.”

“Gameover Zeus is the most sophisticated botnet the FBI and our allies have ever attempted to disrupt,” said FBI Executive Assistant Director Anderson. “The efforts announced today are a direct result of the effective relationships we have with our partners in the private sector, international law enforcement, and within the U.S. government.”

“The borderless, insidious nature of computer hacking and cybertheft requires us to be bold and imaginative,” said U.S. Attorney Hickton. “We take this action on behalf of hundreds of thousands of computer users who were unwittingly infected and victimized.”

“The sophisticated computer malware targeting of U.S. victims by a global criminal enterprise demonstrates the grave threat of cybercrime to our citizens,” said U.S. Attorney Gilg. “We are grateful for the outstanding collaboration of our international and U.S. law enforcement partners in this successful investigation.”

“The FBI has demonstrated great leadership in continuing to help combat cyber crime, and our international and private sector partners have made enormous contributions as well,” said Deputy Under Secretary Schneck. “This collective effort reflects our ‘whole-of-government’ approach to cybersecurity. DHS is proud to support our partners in helping to identify compromised computers, sharing that information rapidly, and developing useful information and mitigation strategies to help the owners of hacked systems.”

Gameover Zeus Administrator Charged

A federal grand jury in Pittsburgh unsealed a 14-count indictment against Evgeniy Mikhailovich Bogachev, 30, of Anapa, Russian Federation, charging him with conspiracy, computer hacking, wire fraud, bank fraud and money laundering in connection with his alleged role as an administrator of the Gameover Zeus botnet. Bogachev was also charged by criminal complaint in Omaha with conspiracy to commit bank fraud related to his alleged involvement in the operation of a prior variant of Zeus malware known as “Jabber Zeus.”

In a separate civil injunction application filed by the United States in federal court in Pittsburgh, Bogachev is identified as a leader of a tightly knit gang of cyber criminals based in Russia and Ukraine that is responsible for the development and operation of both the Gameover Zeus and Cryptolocker schemes. An investigation led in Washington, D.C., identified the Gameover Zeus network as a common distribution mechanism for Cryptolocker. Unsolicited emails containing an infected file purporting to be a voicemail or shipping confirmation are also

widely used to distribute Cryptolocker. When opened, those attachments infect victims' computers. Bogachev is alleged in the civil filing to be an administrator of both Gameover Zeus and Cryptolocker. The injunction filing further alleges that Bogachev is linked to the well-known online nicknames "Slavik" and "Pollingsoon," among others. The criminal complaint filed in Omaha alleges that Bogachev also used "Lucky12345," a well-known online moniker previously the subject of criminal charges in September 2012 that were unsealed in Omaha on April 11, 2014.

*Disruption of Gameover Zeus Botnet*Gameover Zeus, also known as "Peer-to-Peer Zeus," is an extremely sophisticated type of malware designed to steal banking and other credentials from the computers it infects. Unknown to their rightful owners, the infected computers also secretly become part of a global network of compromised computers known as a "botnet," a powerful online tool that cyber criminals can use for numerous criminal purposes besides stealing confidential information from the infected machines themselves. Gameover Zeus, which first emerged around September 2011, is the latest version of Zeus malware that began appearing at least as early as 2007. Gameover Zeus's decentralized, peer-to-peer structure differentiates it from earlier Zeus variants. Security researchers estimate that between 500,000 and 1 million computers worldwide are infected with Gameover Zeus, and that approximately 25 percent of the infected computers are located in the United States. The principal purpose of the botnet is to capture banking credentials from infected computers. Those credentials are then used to initiate or re-direct wire transfers to accounts overseas that are controlled by cyber criminals. The FBI estimates that Gameover Zeus is responsible for more than $100 million in losses.

The Gameover Zeus botnet operates silently on victim computers by directing those computers to reach out to receive commands from other computers in the botnet and to funnel stolen banking credentials back to the criminals who control the botnet. For this reason, in addition to the criminal charges announced today, the United States obtained civil and criminal court orders in federal court in Pittsburgh authorizing measures to redirect the automated requests by victim computers for additional instructions away from the criminal operators to substitute servers established pursuant to court order. The order authorizes the FBI to obtain the Internet Protocol addresses of the victim computers reaching out to the substitute servers and to provide that information to US-CERT to distribute to other countries' CERTS and private industry to assist victims in removing the Gameover Zeus malware from their computers. At no point during the operation did the FBI or law enforcement access the content of any of the victims' computers or electronic communications.

Besides the United States, law enforcement from the Australian Federal Police; the National Police of the Netherlands National High Tech Crime Unit; European Cybercrime Centre (EC3); Germany's Bundeskriminalamt; France's Police Judiciare; Italy's Polizia Postale e delle Comunicazioni; Japan's National Police Agency; Luxembourg's Police Grand Ducale; New Zealand Police; the Royal Canadian Mounted Police; Ukraine's Ministry of Internal Affairs – Division for Combating Cyber Crime; and the United Kingdom's National Crime Agency participated in the operation. The Defense Criminal Investigative Service of the U.S. Department of Defense also participated in the investigation.

Invaluable technical assistance was provided by Dell SecureWorks and CrowdStrike. Numerous other companies also provided assistance, including facilitating efforts by victims to remediate the damage to their computers inflicted by Gameover Zeus. These companies include Microsoft Corporation, Abuse.ch, Afilias, F-Secure, Level 3 Communications, McAfee, Neustar, Shadowserver, Anubis Networks, Symantec, Heimdal Security, Sophos and Trend Micro.

The DHS National Cybersecurity and Communications Integration Center (NCCIC), which houses the US-CERT, plays a key role in triaging and collaboratively responding to the threat by providing technical assistance to information system operators, disseminating timely mitigation strategies to known victims, and sharing actionable information to the broader community to help prevent further infections.*Disruption of Cryptolocker*In addition to the disruption operation against Gameover Zeus, the Justice Department led a separate multi-national action to disrupt the malware known as Cryptolocker (sometimes written as "CryptoLocker"), which began appearing about September 2013 and is also a highly sophisticated malware that uses cryptographic key pairs to encrypt the computer files of its victims. Victims are forced to pay hundreds of dollars and often as much as $700 or more to receive the key necessary to unlock their files. If the victim does not pay the ransom, it is impossible to recover their files.

Security researchers estimate that, as of April 2014, Cryptolocker had infected more than 234,000 computers, with approximately half of those in the United States. One estimate indicates that more than $27 million in ransom payments were made in just the first two months since Cryptolocker emerged.

The law enforcement actions against Cryptolocker are the result of an ongoing criminal investigation by the FBI's Washington Field Office, in coordination with law enforcement counterparts from Canada, Germany, Luxembourg, the Netherlands, United Kingdom and Ukraine.

Companies such as Dell SecureWorks and Deloitte Cyber Risk Services also assisted in the operation against Cryptolocker, as did Carnegie Mellon University and the Georgia Institute of Technology (Georgia Tech). The joint effort aided the FBI in identifying and seizing computer servers acting as command and control hubs for the Cryptolocker malware.

The FBI's Omaha and Pittsburgh Field Offices led both malware disruptions and conducted the investigation of Bogachev. The prosecution in Pittsburgh is being handled by Assistant U.S. Attorney Shardul Desai of the Western District of Pennsylvania, and the prosecution in Omaha by Trial Attorney William A. Hall of the Criminal Division's Computer Crime and Intellectual Property Section (CCIPS) and Assistant U.S. Attorney Steven Russell of the District of Nebraska. The civil action to disrupt the Gameover Zeus botnet and Cryptolocker malware is led by Trial Attorneys Ethan Arenson and David Aaron of CCIPS and Assistant U.S. Attorney Michael A. Comber of the Western District of Pennsylvania.

The Criminal Division's Office of International Affairs provided significant assistance throughout the criminal and civil investigations.

The details contained in the indictment, criminal complaint and related pleadings are merely accusations, and the defendant is presumed innocent unless and until proven guilty.Anyone claiming an interest in any of the property seized or actions enjoined pursuant to the court orders described in this release is advised to visit the following website for notice of the full contents of the orders: http://www.justice.gov/opa/gameover-zeus.html .
