Emotet Botnet Disrupted in International Cyber Operation

justice.gov/opa/pr/emotet-botnet-disrupted-international-cyber-operation

January 28, 2021

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

Thursday, January 28, 2021

Emotet Malware Infected More than 1.6 Million Victim Computers and Caused Hundreds of Millions of Dollars in Damage Worldwide

The Justice Department today announced its participation in a multinational operation involving actions in the United States, Canada, France, Germany, the Netherlands, and the United Kingdom to disrupt and take down the infrastructure of the malware and botnet known as Emotet. Additionally, officials in Lithuania, Sweden, and Ukraine assisted in this major cyber investigative action.

“The Emotet malware and botnet infected hundreds of thousands of computers throughout the United States, including our critical infrastructure, and caused millions of dollars in damage to victims worldwide,” said Acting Deputy Attorney General John Carlin. “Cyber criminals will not escape justice regardless of where they operate. Working with public and private partners around the world we will relentlessly pursue them while using the full arsenal of tools at our disposal to disrupt their threats and prosecute those responsible.”

According to an unsealed search warrant affidavit, Emotet is a family of malware that targets critical industries worldwide, including banking, e-commerce, healthcare, academia, government, and technology. Emotet malware primarily infects victim computers through

spam email messages containing malicious attachments or hyperlinks. Emails were designed to appear to come from a legitimate source or someone in the recipient's contact list. Once it has infected a victim computer, Emotet can deliver additional malware to the infected computer, such as ransomware or malware that steals financial credentials. Ransomware, in particular, has increased in scope and severity in the past year, harming businesses, healthcare providers, and government agencies even as the country has struggled to respond to the pandemic.

"The coordinated disruption of Emotet was a great success for the FBI and our international partners," said FBI Director Christopher Wray. "The FBI utilized sophisticated techniques, our unique legal authorities, and most importantly, our worldwide partnerships to significantly disrupt the malware. The operation is an example of how much we can achieve when we work with our international law enforcement partners to combat the cyber threat. The FBI remains committed, now more than ever, to imposing risk and consequences on cyber criminals to put an end to this type of criminal activity."

The computers infected with Emotet malware are part of a botnet (i.e., a network of compromised computers), meaning the perpetrators can remotely control all the infected computers in a coordinated manner. The owners and operators of the victim computers are typically unaware of the infection.

"Cybercrime transcends physical and political boundaries and costs U.S. citizens and businesses billions each year," said U.S. Attorney Matt Martin of the Middle District of North Carolina. "That was certainly true with Emotet. Now, more than ever, international collaboration is an imperative as we employ a technically and legally sophisticated approach to thwart cybercriminals in whatever corner of the globe they are found. This investigation will be a paradigm for effective international law enforcement cooperation directed at global cybercrime, and we applaud the FBI and the international law enforcement partners who contributed to the effort to take down this global threat."

According to the affidavit, in 2017, for example, the computer network of a school district in the Middle District of North Carolina was infected with the Emotet malware. The Emotet infection caused damage to the school's computers, including but not limited to the school's network, which was disabled for approximately two weeks. In addition, the infection caused more than $1.4 million in losses, including but not limited to the cost of virus mitigation services and replacement computers. From 2017 to the present, there have been numerous other victims throughout North Carolina and the United States, to include computer networks of local, state, tribal, and federal governmental units, corporations, and networks related to critical infrastructure.

"The Emotet malware quickly elevated to one of the top cyber threats in the world," said Special Agent in Charge Robert R. Wells of the FBI Charlotte Field Office. "The strong relationships with international law enforcement partners were critical to the success of this

FBI investigation which began with a small North Carolina school system that did the right thing and quickly contacted their local FBI office for help."

According to the U.S. Cybersecurity & Infrastructure Security Agency (CISA), Emotet infections have cost local, state, tribal, and territorial governments up to $1 million per incident to remediate. More information about the malware, including technical information for organizations about how to mitigate its effects, is available from CISA here: https://us-cert.cisa.gov/ncas/alerts/TA18-201A.

According to the affidavit, foreign law enforcement agents, working in coordination with the FBI, gained lawful access to Emotet servers located overseas and identified the Internet Protocol addresses of approximately 1.6 million computers worldwide that appear to have been infected with Emotet malware between April 1, 2020, and Jan. 17, 2021. Of those, over 45,000 infected computers appear to have been located in the United States.

Foreign law enforcement, working in collaboration with the FBI, replaced Emotet malware on servers located in their jurisdiction with a file created by law enforcement, according to the affidavit. This was done with the intent that computers in the United States and elsewhere that were infected by the Emotet malware would download the law enforcement file during an already-programmed Emotet update. The law enforcement file prevents the administrators of the Emotet botnet from further communicating with infected computers. The law enforcement file does not remediate other malware that was already installed on the infected computer through Emotet; instead, it is designed to prevent additional malware from being installed on the infected computer by untethering the victim computer from the botnet.

The scope of this law enforcement action was limited to the information installed on infected computers by the Emotet operators and did not extend to the information of the owners and users of the computers.

According to the affidavit, in coordination with foreign law enforcement officials, FBI personnel also gained lawful access to an Emotet distribution server located overseas and identified several servers worldwide that were used to distribute the Emotet malware. These servers were typically compromised web servers belonging to what appear to be unknowing third parties. The perpetrators uploaded the Emotet malware to the servers through unauthorized software applications. Victims who clicked on spam email messages containing malicious attachments or hyperlinks would then download the initial Emotet malware file from a distribution server.

In addition, according to the affidavit, FBI personnel notified more than 20 U.S.-based hosting providers that they hosted more than 45 IP addresses that had been compromised by the perpetrators associated with the Emotet malware and botnet. FBI Legal Attachés further notified authorities in more than 50 countries that hosting providers in their respective jurisdictions hosted hundreds of IP addresses that were compromised by Emotet.

The U.S. Attorney's Office for the Middle District of North Carolina, the FBI Charlotte Division, and the Criminal Division's Computer Crime and Intellectual Property Section (CCIPS) conducted the operation in close cooperation with Europol and Eurojust who were an integral part of coordination and messaging, and investigators and prosecutors from several jurisdictions, including the Royal Canadian Mounted Police, France's National Police and Judicial Court of Paris, Germany's Federal Criminal Police and General Public Prosecutor's Office Frankfurt/Main, Lithuanian Criminal Police Bureau, Netherlands National Police and National Public Prosecution Office, Swedish Police Authority, National Police of Ukraine and Office of the Prosecutor General of Ukraine, and the United Kingdom's National Crime Agency and Crown Prosecution Service. The Justice Department's Office of International Affairs and the U.S. Department of the Treasury Financial Crimes Enforcement Network (FinCEN) also provided significant assistance. CCIPS Senior Counsel Ryan K.J. Dickey and Assistant U.S. Attorneys Eric Iverson and Anand Ramaswamy of the Middle District of North Carolina led the U.S. efforts.

More information about the operation is available by clicking: Eurojust/Europol. In addition, the Dutch National Police have created the following website to check whether your email address has been compromised by the administrators of Emotet: https://www.politie.nl/emocheck.

In September 2020, FBI Director Christopher Wray announced the FBI's new strategy for countering cyber threats. The strategy focuses on imposing risk and consequences on cyber adversaries through the FBI's unique authorities, world-class capabilities, and enduring partnerships. Victims are encouraged to report the incident online with the Internet Crime Complaint Center (IC3) www.ic3.gov. For more information on ransomware prevention, visit: https://www.ic3.gov/Home/Ransomware.

Documents and Resources Related to the Disruption of the Emotet Malware and Botnet