TechXplore

Cybercops derail malware botnet, FBI makes ransomware arrest

January 27 2021, by Mike Corder and Frank Bajak

In this file photo dated Wednesday, Oct. 10, 2018, the Europol headquarters building in The Hague, Netherlands. European Europol and North American cyber cops have joined forces Wednesday Jan. 27, 2021, to disrupt what may be the world's largest network for seeding malware infections, striking a major blow against criminal gangs that have been using it for years to install ransomware in extortion schemes, steal data and engage in financial theft.(AP Photo/Peter Dejong, FILE)

European and North American cyber cops have joined forces to disrupt what may be the world's largest network for seeding malware infections, striking a major blow against criminal gangs that have been using it for years to install ransomware in extortion schemes, steal data and engage in financial theft.

Separately, the FBI announced the arrest Wednesday of a Canadian as part of a bid to disrupt a ransomware gang it said had targeted the health care sector and included the seizure of nearly half a million dollars in cryptocurrency.

European Union police and the judicial agencies Europol and Eurojust said Wednesday that investigators took control of the infrastructure behind the botnet known as Emotet. A botnet is a network of hijacked computers, and this one has effectively served as a primary door-opener for cybercriminals since 2014.

"This is a really big deal. Emotet was one of the largest, if not the largest, botnets delivering a wide variety of malware. Their botnet consisted of hundreds of thousands compromised hosts which were used to send more than 10 million spam and phishing emails a week," said Allan Liska, an analyst with Recorded Future.

The Emotet model of recent years was "a game changer for ransomware gangs who otherwise rely on other access methods," said Jake Williams, president of Rendition Infosec, another cybersecurity firm.

Emotet has allowed ransomware gangs to outsource initial access, and focus their efforts instead on a cybercrime variety that has crippled Western government, healthcare and educational networks by scrambling their data and only providing a decoding software key after they have paid up. Those who don't risk having data exfiltrated by the hackers exposed publicly.

Williams said via text message that although someone will eventually fill the gap "there's no question that this will hurt (ransomware gangs) and help defenders in the short/mid term."

Authorities in the Netherlands, Germany, the United States, the U.K., France, Lithuania, Canada and Ukraine took part in the international operation coordinated by the two Hague-based agencies.

Dutch prosecutors said the malware, run out of eastern Europe by a Russian-speaking organization, was first discovered in 2014 and "evolved into the go-to solution for cybercriminals over the years," responsible for hundreds of millions of dollars in losses beginning with financial theft through a banking trojan. They said two of the main servers for the infrastructure were based in the Netherlands and a third in another undisclosed country.

The Emotet botnet was effectively used to manage infections of victims and provide a distributed bulwark against takedown attempts by authorities. In the disruption by law enforcement, its command-and-control infrastructure was routed to servers controlled by law enforcement, cutting off criminal tenants of Emotet from quarry they have infected.

Europol said law enforcement agencies' approach was "unique and new."

In Washington, D.C., later Wednesday, the FBI announced the attempt to disrupt against NetWalker, a relatively new ransomware gang accused of amassing tens of millions of dollars. Ransomware expert Brett Callow at the cybersecurity firm Emsisoft said its victims include Michigan State University, the Champaign-Urbana Public Health District in Illinois, the College of Nurses of Ontario and the Medical School of the University of California at San Francisco, which paid a $1.1 million ransom.

An FBI spokesman said Sebastien Vachon-Desjardins of Gatineau, Quebec, was arrested in the scheme and the agency said in a statement that cryptocurrency worth $454,000 in ransomware income was seized. Earlier this week, authorities in Bulgaria took down a dark web site that NetWalker used to communicate with its victims, it said.

Callow said it was too early to say how big of an impact the arrest would have on NetWalker, whose members are Russian speakers. He said he was not aware of the group using Emotet for distribution.

The Emotet and NetWalker operations build on one by Microsoft late last year against a different botnet known as Trickbot—which was pushed out using Emotet and used in ransomware attacks. The U.S. National Security Agency was also reported to have tried to take down Trickbot.

Costin Raiu, research director at the cybersecurity firm Kaspersky, said the Emotet takedown "should impact other cybercriminal groups' ability to maintain and grow their botnets. It remains to be seen if they will be able to stage a comeback, be it either as Emotet, or perhaps merge with another group and continue from there."

Emotet's "door-opening" malicious software was automatically delivered to computers in infected email attachments containing Word documents. "A variety of different lures were used to trick unsuspecting users into opening these malicious attachments," Dutch prosecutors said in a statement. Emotet email campaigns have been disguised as invoices, shipping notices and COVID-19 information.

Cryptocurrency has been a great enabler of cybercrime and has led law enforcement to step up efforts to track online transactions of dirty money. In 2017, police shut down the world's leading "darknet" marketplace—then Dutch police quietly seized a second bazaar to amass intelligence on illicit drug merchants and buyers.

Citation: Cybercops derail malware botnet, FBI makes ransomware arrest (2021, January 27) retrieved 26 April 2024 from https://techxplore.com/news/2021-01-cyber-cops-nations-team-disrupt.html