Microsoft

News Center

Microsoft, financial services and others join forces to combat massive cyber-crime ring

June 05, 2013

Microsoft works with financial services industry leaders, other industry partners, and law enforcement to disrupt a global cybercrime operation responsible for over half a billion dollars (USD) in financial fraud.

REDMOND, Wash. – June 5, 2013 – In a coordinated operation, Microsoft Corp., in cooperation with leaders in the financial services industry – including the Financial Services – Information Sharing and Analysis Center (FS-ISAC), NACHA – The Electronic Payments Association, the American Bankers Association (ABA) – Agari, and other technology industry partners, as well as the Federal Bureau of Investigation, announced it has successfully disrupted more than a thousand botnets that are responsible for stealing people's online banking information and personal identities. The FBI took coordinated separate steps related to the operation. Botnets are networks of compromised computers infected by malicious software to be controlled by cybercriminals known as botherders. This cooperative action is part of a growing proactive effort by both the public and private sector to fight cybercrime, help protect people and businesses from online fraud and identity theft, and enhance cloud security for everyone.

This coordinated disruption resulted from an extensive investigation that Microsoft and its financial services and technology industry partners began in early 2012. After looking into this threat, Microsoft and its partners discovered that once a computer was infected with Citadel malware, that malware began monitoring and recording a victim's keystrokes. This tactic, known as keylogging, provides cybercriminals information to gain direct access to a victim's bank account or any other online account in order to withdraw money or steal personal identities. This means that when victims are using their computers to access their bank or online accounts, cybercriminals can use the stolen information to quietly pilfer those same accounts as well. Microsoft also found that in addition to being responsible for more than half a billion dollars (USD) in losses among people and businesses worldwide, the Citadel malware has affected upwards of five million people, with some of the highest number of infections appearing in the U.S., Europe, Hong Kong, Singapore, India, and Australia. Citadel is a global threat that is believed may have already infected victims in more than ninety countries worldwide since its inception.

"The harm done by Citadel shows the threat that botnets, malicious software, and piracy pose to individuals and businesses around the world," said Brad Smith, Microsoft general counsel and executive vice president, Legal and Corporate Affairs. "Today's coordinated action between the private sector and law enforcement demonstrates the power of combined legal and technical expertise and we're going to continue to work together to help put these cybercriminals out of business."

Last week, supported by declarations from financial services leaders and other industry partners, Microsoft filed a civil suit against the cybercriminals operating the Citadel botnets,

receiving authorization from the U.S. District Court for the Western District of North Carolina for Microsoft to simultaneously cut off communication between 1,462 Citadel botnets and the millions of infected computers under their control. On June 5, Microsoft, escorted by the U.S. Marshals, seized data and evidence from the botnets, including computer servers from two data hosting facilities in New Jersey and Pennsylvania. Microsoft also provided information about the botnets' operations to international Computer Emergency Response Teams (CERTs), so these partners could take action at their discretion on additional command and control infrastructure for the botnets located outside of the U.S.

As stated by the FBI, the FBI also provided information to foreign law enforcement counterparts so that they could also take voluntary action on botnet infrastructure located outside of the U.S. The FBI also obtained and served court-authorized search warrants domestically related to the botnets.

This operation serves as a real world example of how public-private partnerships can work effectively within the judicial system, and how 20th century legal precedent and common law principles dating back hundreds of years can be effectively applied toward 21st century cybersecurity issues.

"Today's actions represent the future of addressing the significant risks posed to our citizens, businesses, and intellectual property by cyber threats and malicious software, which are often enabled by counterfeit and unlicensed software," said FBI Executive Assistant Director Richard McFeely. "Creating successful public-private relationships—in which tools, knowledge, and intelligence are shared—is the ultimate key to success in addressing cyber threats and is among the highest priorities of the FBI. We must ensure that, as cyber policy is developed, the ability of the private sector to coordinate in real time with the FBI is encouraged so that a multi-prong attack on our cyber adversaries can be as effective as possible."

Because the operators used the malware to steal victims' online banking credentials and make fraudulent transactions, financial services industry leaders including FS-ISAC, NACHA, ABA, and Agari supported Microsoft's civil lawsuit by serving as declarants in the case. This operation is the second in which Microsoft has worked with the financial services industry to disrupt a family of botnets.

"Crimes used to happen through stickups, but today criminals use mouse clicks," said Greg Garcia, a consultant and former Department of Homeland Security cyber official serving as a spokesperson for the three major financial industry associations. "This action aims to stop the ongoing harm of these Citadel botnets against people and businesses worldwide, and you can be assured that we will continue to partner with the public and private sectors to help financial institutions protect our customers from threats like this."

Other organizations that played a part in the legal or technical aspects of this operation include Agari, A10 Networks, and Nominum. In particular, in addition to supporting Microsoft's lawsuit with a legal declaration, Agari, a partner of FS-ISAC, provided forensic data gathering based on the terabytes of email data that Agari collects from sources across the Internet to protect against email threats such as phishing. Meanwhile, A10 Networks and Nominum provided Microsoft advanced technology to support the disruptive action.

Due to the size and complexity of the threat, Microsoft and its partners do not expect to fully eliminate all of the botnets using Citadel. However, it is expected that this action will

significantly disrupt the botnets' operation, making it riskier and more expensive for the cybercriminals to continue doing business and allowing victims to free their computers from the malware. To help protect people from any remaining instances of this threat, it is critical that victims rid their computers of Citadel by using malware removal or anti-virus software as quickly as possible to help prevent additional security issues.

Immediately following the disruption, Microsoft will use the threat intelligence gathered during the seizure to work with Internet Service Providers and Computer Emergency Response Teams worldwide to quickly and efficiently notify people if their computer is infected. Microsoft will be making this information available through its Cyber Threat Intelligence Program (C-TIP), including the recently-announced cloud-based version of the program. For computer owners worried that their computers might be infected, Microsoft offers free information and malware removal tools at http://support.microsoft.com/botnets. Additionally, the FBI is providing information on its website about botnets to educate the public on how to protect themselves. Many financial services industry organizations provide resources, tips, and tools to individuals and companies on how to help protect themselves.

Like many of Microsoft's past botnet operations, this investigation once again revealed how criminals are adapting and evolving their attack methods to continue to infect people's computers with malware. In this case, Microsoft found that the cybercriminals are using fraudulently obtained product keys created by key generators for outdated Windows XP software to develop their malware and grow their business, demonstrating a continued connection between software piracy and global cybersecurity threats. This discovery showcases that in addition to exercising safe online practices like running modern, updated and legitimate software and using firewall and antivirus protection, people also need to be using modern versions of Windows software to better prevent malware, fraud, and identify theft.

More information about today's news and the coordinated action against Citadel is available at http://www.microsoft.com/en-us/news/presskits/dcu/. Legal documentation in the case can be found at http://www.botnetlegalnotice.com/citadel.

About FS-ISAC

The Financial Services Information Sharing and Analysis Center was formed in 1999 and is a non-profit, private financial sector initiative. It was designed and developed and is owned by financial institutions. Its primary function is to share timely, relevant and actionable information of physical and cyber security threat and incident information to help mitigate the risk associated with these threats. http://www.fsisac.com/

About NACHA – The Electronic Payments Association

NACHA manages the development, administration, and governance of the ACH Network, the backbone for the electronic movement of money and data. The ACH Network provides a safe, secure, and reliable network for direct account-to-account consumer, business, and government payments. Annually, it facilitates billions of Direct Deposit via ACH and Direct Payment via ACH transactions. Used by all types of financial institutions, the ACH Network is governed by the fair and equitable NACHA Operating Rules, which guide risk management and create payment certainty for all participants. As a not-for-profit association, NACHA represents more than 10,000 financial institutions via 17 regional payments associations and direct membership. Through its industry councils and forums, NACHA brings together

payments system stakeholders to foster dialogue and innovation to strengthen the ACH Network. To learn more, please visit www.nacha.org.

About ABA

The American Bankers Association represents banks of all sizes and charters and is the voice for the nation's $14 trillion banking industry and its two million employees. Learn more at aba.com.

About Agari

Agari collects terabytes of email data from sources across the Internet to create a cloud-based solution to assess, visualize, and protect against email threats to brands, such as phishing and other fraud. Today, Agari protects more than 65 percent of US consumer email traffic and processes more than 2.3 billion messages daily. The Agari Email Trust Network becomes more pervasive, intelligent, and powerful as more join Agari to protect email users, customers, brands, business models, and corporate and cyber infrastructure. Founded by the thought leaders behind Cisco's IronPort solutions, the Agari platform provides global brands with the tools needed to proactively protect brand reputation, eliminate email threats, protect customers and prevent the loss of sensitive data. Headquartered in Palo Alto, Calif., Agari is backed by Alloy Ventures, Battery Ventures, First Round Capital, and Greylock Partners. Additional information is available at www.agari.com.

About A10 Networks

A10 Networks was founded in Q4 2004 with a mission to provide innovative networking and security solutions. A10 Networks makes high-performance products that help organizations accelerate, optimize and secure their applications. A10 Networks is headquartered in Silicon Valley with offices in the United States, United Kingdom, France, The Netherlands, Germany, Spain, Brazil, Japan, China, Korea, Taiwan, Hong Kong, Singapore and Malaysia. For more information, visit: http://www.a10networks.com.

About Nominum

Nominum empowers Communication Service Providers (CSPs) to quickly and cost effectively deliver personalized services that provide a differentiated, safer customer experience, generate revenues and build brand loyalty. Nominum's N2 Platform is an open, scalable platform that leverages customer behavior data from the DNS and other network sources and monetizes the data through intelligent policy management and notification-based service offerings. The N2 Platform processes over 1.5 trillion DNS queries daily and is easily layered upon existing network infrastructure with no additional hardware. Nominum is a global organization headquartered in Redwood City, CA.

About FBI

As an intelligence-driven and a threat-focused national security organization with both intelligence and law enforcement responsibilities, the mission of the FBI is to protect and defend the United States against terrorist and foreign intelligence threats, including cyber-based attacks and high-technology crimes; to uphold and enforce the criminal laws of the United States; and to provide leadership and criminal justice services to federal, state, municipal, and international agencies and partners.

About Microsoft

Founded in 1975, Microsoft (Nasdaq “MSFT”) is the worldwide leader in software, services and solutions that help people and businesses realize their full potential.

Note to editors: For more information, news and perspectives from Microsoft, please visit the Microsoft News Center at http://www.microsoft.com/news. Web links, telephone numbers and titles were correct at time of publication, but may have changed. For additional assistance, journalists and analysts may contact Microsoft’s Rapid Response Team or other appropriate contacts listed at http://www.microsoft.com/news/contactpr.mspx.