Digital Crimes Unit rescues 100s of millions of devices

In partnership with threat intelligence and security experts across Microsoft, the Digital Crimes Unit (DCU) applies unique legal and technical solutions to identify, investigate, and disrupt malware-facilitated cybercrime and nation-state sponsored activity.

Since 2010, the DCU has collaborated with law enforcement and other partners on 19 malware disruptions, resulting in over 500 million devices rescued from cybercriminals. Traffic from victim devices that once communicated to criminal servers is safely rerouted to Microsoft's Cyber Threat Intelligence Program (CTIP). Victim devices are cleaned through antivirus programs such as Windows Defender Antivirus or intelligence is shared with Computer Emergency Response Teams (CERTs) and Internet Service Providers (ISPs) around the world to notify victims and assist with removal of the malware.

Listed below is more information related to malware disruptions in which DCU played an integral role. For threat-specific information including behavior, symptoms, and how to detect and remove the threat, search the Threat Encyclopedia on the Microsoft Security Intelligence site.

Gamarue

Disruption date: November 2017

- Also known as Andromeda
- Sold as a crime kit on the dark web with additional modules that could be added
- Steals user names and passwords, disables security protections, and blocks Windows Update
- Spreads through USB flash drives, instant messaging programs, email, and social networks
- Installs other malware types such as backdoor, downloaders, remote access, worm, spam, ransomware, and click fraud — a Gamarue infected system could be infected with dozens of additional different types malware

Microsoft blog: Microsoft teams up with law enforcement and other partners to disrupt Gamarue (Andromeda)
Europol newsroom: Andromeda botnet dismantled in international operation
Geekwire: Microsoft releases new details on Gamarue malware botnet ad its 'sprawling infrastructure'

Avalanche

Disruption date: November 2017

- Used as a delivery platform to launch and manage mass global malware attacks and money mule recruiting campaigns
- Steals user names and passwords, launches denial of service (DoS) attacks, distributes other malware families, and targeted over 40 major financial institutions
- Installs other malware types such as backdoor, downloaders, remote access, worm, spam, and click fraud

Europol newsroom: 'Avalanche' network dismantled in international cyber operation
Europol infographic: Operation Avalanche

Barium

Disruption date: November 2017

- Targets high value organizations holding sensitive data by gathering extensive information about their employees through publicly available information and social media, using that information to fashion phishing attacks

Microsoft blog: Detecting threat actors in recent German industrial attacks with Windows Defender ATP
Courthouse News: Microsoft asks judge to take down Barium hackers

Strontium

Disruption date: August 2016

- Also known as Fancy Bear or APT 28
- Leveraged Microsoft-like domains for spear phishing attacks, enabling the criminals to install a remote access kit that could be used to exfiltrate sensitive data.

Microsoft blog: Our commitment to our customers' security
ArsTechnica: Microsoft shuts down phishing sites, accuses Russia of new election meddling
Bloomberg: Microsoft embraces role as anti-hacking enforcer
Wired: How Microsoft tackles Russian hackers - and why it's never enough

Dorkbot

Disruption date: December 2015

- Steals user names and passwords, disables security protection, blocks websites related to security updates, and launches a limited denial of service (DoS) attack
- Spreads through USB flash drives, instant messaging programs, and social networks
- Installs other malware types such as backdoor, downloaders, remote access, worm, spam, and click fraud

ZDNet: Microsoft, law enforcement disrupt sprawling Dorkbot botnet
Threatpost: Microsoft, law enforcement collaborate in Dorkbot takedown

Simda

Disruption date: April 2015

- The Simda.AT variant first appeared in 2012 and caused significant damage to users through the manipulation of internet traffic and spread of other malware.
- Simda's function has ranged from a simple password stealer to a complex banking trojan

Interpol news: Interpol coordinates global operation to take down Simda botnet

Ramnit

Disruption date: February 2015

- Online banking fraud malware that impacted 3.2M unique IPs across 195 countries
- First detected as a worm, spread very quickly due to aggressive self-propagation using phishing emails and social networking sites
- Evolution to a Trojan, then to an extensive botnet, ramped up by the leaked source code of the Zeus Trojan back in 2011
- Web-injected spy module, or hook-spy module, would monitor web browsing history, inject additional fields into banking websites, and collect bank credentials

Microsoft blog: Breaking up a botnet - How Ramnit was foiled
CRN: Symantec, Microsoft support global Ramnit botnet takedown

Caphaw

Disruption date: July 2014

- The Caphaw malware family targeted banks and their customers in Europe
- It could give a malicious hacker access to and control of your PC
- Caphaw targeted several high-profile European banks to steal online banking details
- It used social engineering tactics to infect devices with information-stealing components through Facebook, YouTube, Skype, removable drives, and drive-by downloadsSimda's function has ranged from a simple password stealer to a complex banking trojan

Microsoft blog: Microsoft partners with financial services industry on fight against cybercrime

Bladabindi & Jenxcus

Disruption date: June 2014

- A pervasive family of malware that put millions of customers at risk
- The social media-savvy cybercriminals promoted their wares across the Internet, offering step-by-step instructions to completely control millions of unsuspecting victims' computers to conduct illicit crimes
- Spread through infected removable drives, such as USB flash drives, can also be downloaded by other malware

Microsoft blog: Microsoft takes on global cybercrime epidemic in tenth malware disruption
eWeek: Microsoft takes down Bladabindi and Jenxcus botnets

Game Over Zeus

Disruption date: June 2014

- The primary purpose of the malware was to hijack victims online banking sessions for monetary purposes and was also used in conjunction with ransomware

Microsoft blog: Microsoft helps FBI in GameOver Zeus botnet cleanup
FBI news: GameOver Zeus botnet disrupted: Collaborative effort among international partners
KrebsonSecurity: 'Operation Tovar' targets 'Gameover' ZeuS botnet, CryptoLocker scourge

ZeroAccess aka Sirefef

Disruption date: December 2013

- The primary purpose of this Trojan horse is to generate money through pay-per-click fraud
- A multi-component family of malware that moderates your internet experience by changing search results, generating pay-per-click advertising revenue for its controllers
- It directed users to potentially dangerous websites that could install malware, steal personal information, or fraudulently charge businesses for online advertisement clicks

Microsoft blog: Microsoft, the FBI, Europol and industry partners disrupt the notorious ZeroAccess botnet
Microsoft blog: ZeroAccess criminals wave white flag: The impact of partnerships on cybercrime
arsTechnica: Microsoft disrupts botnet that generated $2.7M per month for operators
Reuters: Microsoft leads disruption of largest infected global PC network

Citadel

Disruption date: June 2013

- Citadel has the ability to log an infected machine's key strokes stealing password and banking information
- Citadel could also perform man-in-the-middle attacks prompting infected machines users to give up personal banking information when the victim visited an otherwise legitimate website through popups and web traffic monitoring

Microsoft blog: Microsoft works with financial services industry leaders, law enforcement and others to disrupt massive financial cybercrime ring
Department of Justice news: Russian citizen who helped develop the "Citadel" malware toolkit is sentenced
Dark Reading: Microsoft, FBI trumpet Citadel botnet takedowns

Bamital

Disruption date: February 2013

- Bamital intercepts web traffic on an infected machine and redirects clicks to advertising sites which paid the criminals for the traffic.
- It is often installed via drive-by downloads.
- It redirects users to sites they were not intending to visit, taking control away from the user, leaving them vulnerable to other targeted attacks such as identity theft and additional malware infections

Microsoft blog: Microsoft and Symantec take down Bamital botnet that hijacks online searches
Microsoft blog: Bamital botnet takedown is successful; cleanup underway
KrebsonSecurity: Microsoft, Symantec hijack 'Bamital' botnet

Nitol

Disruption date: September 2012

- Trojan virus usually installed with other corrupted software downloaded from peer to peer file shares
- Nitol can use an infected computer to perform distributed denial of service attacks (DDoS) without the affected machines owner(s) knowledge.

Microsoft blog: Microsoft disrupts the emerging Nitol botnet being spread through an unsecure supply chain
Microsoft blog: Microsoft reaches settlement with defendants in Nitol case
KrebsonSecurity: Microsoft disrupts 'Nitol' botnet in piracy sweep

Zeus aka Zbot

Disruption date: March 2012

- Keylogging botnet, recording every keystroke, gaining access to usernames and passwords to steal victims' identities, withdraw money from bank accounts, and make online purchases.
- Primarily distributed through spam and drive-by downloads

Microsoft blog: Microsoft and financial services industry leaders target cybercriminal operations from Zeus botnets
Microsoft blog: Microsoft names defendants in Zeus botnets case; provides new evidence to FBI
FBI news: Cyber criminal pleads guilty to developing and distributing notorious SpyEye malware
Wired: Alleged 'SpyEye' botmaster ends up in America, handcuffs

Kelihos

Disruption date: September 2011

- Communicates with remote servers to exchange information that is used to execute various tasks, including sending spam email, capturing sensitive information or downloading and executing arbitrary files.

Microsoft blog: Microsoft neutralizes Kelihos botnet, names defendant in case
Microsoft blog: Microsoft reaches settlement with Piatti, dotFREE Group in Kelihos case
Microsoft blog: Microsoft names new defendant in Kelihos case
Microsoft blog: Update on Kelihos botnet and new related malware
CRN: Microsoft says ex-antivirus maker ran botnet

Rustock

Disruption date: March 2011

- Responsible for sending upwards of 30 billion spam emails a day
- DCU researchers observed a single Rustock-infected computer send 7,500 spam emails in just 45 minutes, for a rate of 240,000 spam mails per day.

Microsoft blog: Taking down botnets: Microsoft and the Rustock botnet
Microsoft blog: Microsoft releases new threat data on Rustock
Microsoft blog: Microsoft offers reward for information on Rustock
Microsoft blog: Rustock civil case closed: Microsoft refers criminal evidence to FBI
artsTechnica: How Operation b107 decapitated the Rustock botnet

Waledac

Disruption date: February 2010

- Collects e-mail addresses found on the computer on which it is installed and distributes spam e-mail messages.
- Ability to download and execute arbitrary files, harvest email addresses from the local machine, perform denial of service attacks, proxy network traffic and sniff passwords.

Microsoft blog: Cracking down on botnets
Microsoft blog: R.I.P. Waledac: Undoing the damage of a botnet
The Guardian: Microsoft goes to court to take down the Waledac botnet

Conficker

Disruption date: November 2008

- The worm spread through USBs and the internet. Once infected, a computer would then infect others within its common network, assisting the criminals in sending further spam/malware.

Microsoft blog: Microsoft collaborates with industry to disrupt Conficker worm