Zombie killers: how Microsoft uses IP to fight cybercrime

A combination of IP and global law enforcement saw Microsoft successfully stop sophisticated online fraud, so why do critics reject its 'vigilante' methods?

Over the past decade, online fraud has become a lucrative illegal business through the use of botnets, zombie computers, and malware. Nearly 400m people fall victim to cybercrime each year, costing consumers upwards of $113bn dollars and the global economy $500bn.[1] Over 40m Target customers are the latest victims. The December 2013 data breach that compromised customers' personally identifiable and financial information, including credit and debit card numbers, stemmed from malware attacks on Target's point-of-sale (POS) system. The relative ease of individuals running these illegal organisations to remain anonymous, evade capture, and evolve in spite of tougher security measures taken by companies, makes such organisations and the fraud they perpetrate extremely difficult to stop. Microsoft may have a plan to bring down botnet cyber fraud, one that utilises traditional IP and computer principals in unconventional ways.

Botnet 101

Generally, the first step of perpetrating online fraud involves the infestation of users' computers with malicious software, also known as "malware". Computer users' exposure to malware can occur in many scenarios, including opening suspicious emails, visiting certain websites, interacting with malicious website advertisements, installing pirated software, or the intentional or unintentional downloading of items onto one's computer. Once installed, certain forms of malware turn a user's computer into a 'zombie', and allow cybercriminals to remotely access it for nefarious purposes. A collection of zombie computers constitutes a 'botnet'. Once part of a botnet, the zombie computer has the ability to send and receive communications, instructions, and code to and from other botnet computers, all at the request of the cybercriminal/malware-botnet creator. Once created, cybercriminals can remotely instruct zombie computers in their botnet army to send spam emails perpetuating consumer fraud schemes, generate large number of fraudulent clicks on website advertisements ("click fraud"), and redirect users to search results of the botnet operators choosing ("browser hijacking").[2]

Microsoft v John Does 1-8

On 25 November 2013, Microsoft filed a confidential, or under seal, civil case in the US District Court for the Western District of Texas in an effort to disrupt the Sirefref botnet, also known as ZeroAccess. According to Microsoft, ZeroAccess had a zombie army of over 2m infected computes and cost online advertisers over $2.7m each month based on its click fraud and browser hijacking schemes.[3] Microsoft sought eight claims of relief, including three under the Lanham Act. Microsoft alleged that ZeroAccess infringed upon, diluted, and created false designations of origin in regards to Microsoft's Bing, Internet Explorer, and Microsoft trademarks by generating counterfeit copies of the marks in connection with ZeroAccess' click fraud and browser hijacking activities.[4] Such conduct caused consumer confusion and improper association between Microsoft's marks, goods, and services and ZeroAccess' malicious conduct and actions.

Microsoft used several civil procedures to its advantage. First, it asserted its claims through a 'John Doe' lawsuit, a necessity since Microsoft lacked the true identity of the cybercriminals behind the IP addresses associated with the botnet. Second, Microsoft filed a motion for an emergency *ex parte* temporary restraining order (TRO). The *ex parte* remedy allowed Microsoft to seek immediate action and relief without informing the defendants in advance. This was extremely critical since advanced notice would have likely caused the defendants to delete or relocate their operations, destroy valuable evidence, and warn their cybercriminal associates. Third, due to the anonymity of the defendants and the fact that they likely resided in Europe, Microsoft requested alternate means to serve notice on the defendants of the complaint and preliminary injunction hearing after implementing the TRO, namely through email, online publication, and Hague Service Convention-based means. All of these procedural tactics decrease the likelihood that the defendants would come out of hiding to answer the complaint or attend the preliminary injunction hearing, thus increasing Microsoft's likelihood of getting a default judgment and permanent injunction.

In this case, the court swiftly granted the TRO, which permitted Microsoft to contact internet service providers (ISP) associated with eighteen IP addresses used by the cybercriminals to control the ZeroAccess botnet. The named ISPs were requested to identify and disable all incoming and outgoing traffic to the IP addresses, preserve content from such addresses and domains for evidentiary purposes, and transfer the control of such domains to Microsoft for monitoring. Additionally, the court granted Microsoft's service request, and scheduled the preliminary injunction hearing for 17 December, 2013.

Once the court granted the TRO, Microsoft undertook a swift coordinated effort with US ISPs and law enforcement agencies in the US (FBI) and Europe (Eurpol's European Cybercrime Centre, Germany's Bundeskriminalmt's Cyber Intelligence Unit) to block traffic to and from the fraudulent ISP addresses, monitor the cybercriminals' activities, and physically seize servers associated with the ISP addresses in Europe.[5] As expected, the botnet creators quickly sought out new ISP addresses to send out new instructions to the zombie computers to continue their criminal activities; again demonstrating the complexity and robustness of this form of cyber fraud. However, because of the collaborative partnerships Microsoft established, the new ISP addresses were quickly identified and blocked. Eleven days later after the TRO, the defendants sent out a "white flag" message to its zombie computers effectively ceasing all remaining click fraud and browser hijacking activities of the

ZeroAccess botnet.

According to its official blog, Microsoft did not expect to fully eliminate the ZeroAccess botnet when it commenced its investigation and lawsuit.[6] Therefore, it was pleased to report the successful surrender and Microsoft voluntary dismissed its civil case on 12 December 2013 to allow law enforcement agencies to continue their criminal investigations. Additionally, Microsoft provided free information and tools for computer users to rid their machines of the malware. The next few months will determine whether ZeroAccess is really down for the count or whether it or a new variant will rise again from the ashes.

A 21st Century problem

Microsoft v John Does 1-8 was not Microsoft's first foray into disrupting botnet cybercrime, but it's definitely the most successful attack thus far. Over the past three years, Microsoft has gone after some of the most infamous botnets[7]: Waledac in 2010, Kelihos and Rustock in 2011, Zeus in 2012, and Bamital, Citadel, and ZeroAccess in 2013. All have used the same novel approach – a public-private partnership between technology and financial companies and governmental enforcement agencies, civil suits brought using novel claims, and tactical civil procedure to allow Microsoft to act quickly and stealthily.

Caped crusader or profiteer?

Microsoft's botnet operations have been met with a mix of praise and criticism. Some, especially those in the security community, roundly criticise Microsoft tactics and believe the company has overstepped its boundaries. The disruptions created by the TROs and default judgments provide only a temporary fix and many of the defendants regroup, evolve, and continue using botnets to perpetuate cyber fraud. Additionally, some researchers and members of the security community claim that Microsoft disclosed privileged information on actors involved with the various botnets, information garnered through years of investigation, without permission from those who provided it.[8] Consequently, they claim that Microsoft's actions have derailed or delayed other law enforcement investigations and chilled further private-public partnership as a result. Furthermore, Microsoft's own research has been cited as sloppy, including going after defendants already incarcerated for their crimes and interfering, albeit briefly, with legitimate websites and IP addresses.[9] Overall, these critics view Microsoft's vigilante crusade as a PR ploy with short term gains and long term collateral damage.

Others applaud the company for taking a proactive, aggressive, and most importantly voluntary stance against insidious and sophisticated cybercrime. The company's legal tactics lead to swift action, unlike other investigations that tend to drag on for years. Microsoft's public-private partnerships have made its operations not only more effective, but also have been hailed as a best practice for fighting cybercrime by US government leaders, including Senator Sheldon Whitehouse, Chairman of the Senate Judiciary Subcommittee on Crime and Terrorism.[10]

Best practices for others?

Whatever your opinion of Microsoft's strategy, companies can learn valuable lessons. First, botnet-triggered cyber fraud can and does affect everyone, from the most novice individual users to the most tech-savvy Fortune 500 companies. One out of five small and medium businesses has been targeted by cybercriminals.[11] Small businesses can be especially alluring because they lack the security measures implemented by larger companies. Furthermore, if the smaller company is a subsidiary of a larger company or has a relationship that allows it access to a larger company's network, cybercriminals have an easy gateway to breach the larger company.[12] Consequently, it is vitally important for all companies to be educated on their security risks and the types and trends of cybercrime that might befall them. After a malware attack on its POS network led to a data breach and the compromise of over 2.4 m debit and credit card details, Schnuck Markets Inc, a St Louis-based grocery store chain took steps to beef up its security, including hiring a full-time director of information security.[13]

Second, proactivity matters, and could decrease the likelihood of litigation. Soon after Schnuck Market's data breach, consumers filed a class action lawsuit claiming that Schnuck had failed to adequately protect cardholder data and should have notified consumers immediately after it found out about the breach.[14] Additionally Schnuck's insurer, Liberty Mutual brought suit to seek to avoid paying losses linked to the data breach. Target is currently facing similar lawsuits by its customers. Schnuck eventually settled with its customers and insurance company, but a more proactive stance may have saved the company time, money, and a PR headache. Many companies might not have the financial or technological resources to combat cybercrime like Microsoft, but having a procedure in place in case of an attack, obtaining a cyber-insurance policy, or establishing beneficial private-public relationships can be the first steps in the right anti-zombie direction.

Footnotes

1. Jennifer Warnick, "Digital Detectives", http://tinyurl.com/m6x5zxp.
2. *Microsoft Corp v John Does 1-8 et al,* Case No.1:13-cv-01014 (WD Tex 2013) (Sparks, J) (Compl. 27,31, 33, 41) available at http://tinyurl.com/n8x4hl3.
3. Richard Domingues Boscovich, "Microsoft, Europol, FBI and industry partners disrupt notorious ZeroAccess botnet that hijacks search results," The Official Microsoft Blog (5 Dec, 2013), http://tinyurl.com/l7ohu45.
4. *Microsoft Corp v John Does 1-8* (Compl pages 20-23).
5. *Microsoft Corp v John Does 1-8* (Plaintiff's Notice of Voluntary Dismissal without Prejudice, 1-2).
6. Richard Domingues Boscovich, "ZeroAccess criminals wave white flag: The impact of partnerships on cybercrime," The Official Microsoft Blog (19 Dec, 2013) http://tinyurl.com/n8cryv6.
7. *Microsoft Corp v John Does 1-27, et al,* Case No 1:10-cv-00156 (ED Va 2010) (Anderson, J); *Microsoft Corp v Piatti, et al,* Case No 1:11-cv-1017 (ED Va 2011) (Cacheris, J); *Microsoft Corp v John Does*, 1-11, Case No 2:11-cv-00222 (W.D. Wa. 2011) (Robart, J); *Microsoft Corp et al v John Does 1-39 et al.*, Case No 12-cv-1335 (EDNY 2012) (Johnson, J); *Microsoft Corp v John Does 1-18 et al,* Case No 1:13-cv-139-LMB/TCB (ED Va 2013) (Brinkema, J).
8. "Critical analysis of Microsoft Operation B71," FOX-IT International blog (12 Apr, 2012) http://tinyurl.com/l7xw4cx.
9. id.
10. Ryan Pretzer, "Microsoft shines spotlight on public-private efforts to defeat botnets," Staysafeonlin.org (25 Jul, 2013) http://tinyurl.com/luhdcsj.
11. Warnick, *supra* note 1.
12. Parija Kavilanz, "Cybercrime's easiest prey: Small businesses," CNNMoney (23 Apr, 2013) *available at* http://tinyurl.com/laz4dmk.
13. Kavita Kumar, "Schnuck Markets names new CEO", St. Louis Post-Dispatch (9 Jan, 2014) *available at* http://tinyurl.com/lah87qj.
14. Tracy Kitten, "Schnucks' Insurer Drops Breach Lawsuit: Case Highlights Need for Cyber-Insurance," Bank Info Security (18 Oct, 2013) *available at* http://tinyurl.com/lg4ulhv.

Authors

Camille M Miller (left) is co-chair of the IP department and IP litigation practice group at Cozen O'Connor. Chanel L Lattimer is an associate in the firm's IP department.