Kelihos botnet

The **Kelihos botnet**, also known as **Hlux**, is a botnet mainly involved in spamming and the theft of bitcoins.[1]

History

The Kelihos botnet was first discovered around December 2010.[2] Researchers originally suspected having found a new version of either the Storm or Waledac botnet, due to similarities in the modus operandi and source code of the bot,[3][4] but analysis of the botnet showed it was instead a new, 45,000-infected-computer-strong, botnet that was capable of sending an estimated 4 billion spam messages a day.[5][6] In September 2011[7] Microsoft took down the botnet in an operation codenamed "Operation b79".[5][8] At the same time, Microsoft filed civil charges against Dominique Alexander Piatti, dotFREE Group SRO and 22 John Doe defendants for suspected involvement in the botnet for issuing 3,700 subdomains that were used by the botnet.[8][9] These charges were later dropped when Microsoft determined that the named defendants did not intentionally aid the botnet controllers.[10][11]

In January 2012 a new version of the botnet was discovered, one sometimes referred to as Kelihos.b or Version 2,[1][6][7] consisting of an estimated 110,000 infected computers.[1][12] During this same month Microsoft pressed charges against Russian citizen Andrey Sabelnikov, a former IT security professional, for being the alleged creator of the Kelihos Botnet sourcecode.[11][13][14] The second version of the botnet itself was shut down by it in March 2012 by several privately owned firms by sinkholing it – a technique which gave the companies control over the botnet while cutting off the original controllers.[2][15]

Following the shutdown of the second version of the botnet, a new version surfaced as early as 2 April, though there is some disagreement between research groups whether the botnet is simply the remnants of the disabled Version 2 botnet, or a new version altogether.[16][17] This version of the botnet currently consists of an estimated 70,000 infected computers. The Kelihos.c version mostly infects computers through Facebook by sending users of the website malicious download links. Once clicked, a Trojan horse named Fifesoc is downloaded, which turns the computer into a zombie, which is part of the botnet.[18]

On 24 November 2015 a Kelihos botnet event occurred causing widespread false positives of blacklisted IPs:

> ″November 24, 2015 Widespread false positives
>
> Earlier today, a very large scale Kelihos botnet event occurred - by large scale, many email installations will be seeing in excess of 20% kelihos spam, and some will see their inbound email volume jump by a volume of as much as 500%. This isn't an unusual thing normally, the CBL/XBL has been successfully dealing with large scale Kelihos spam spikes like this, often daily, for years.
>
> The email was allegedly from the US Federal Reserve, saying something about restrictions in "U.S. Federal Wire and ACH online payments." Not only was the notice itself fraudulent, the attached Excel spreadsheet (.xls) contained macro instructions (a downloader) to download a Windows executable virus, most likely Dyreza or Dridex malware.
>
> The detection rules initially deployed by the CBL unfortunately were insufficiently detailed, and listed a number of IP addresses in error.″[19]

An affidavit unsealed on 5 February 2018, showed Apple's unexpected role in bringing the Russian spam king to justice. Peter Levashov allegedly ran the Kelihos botnet under the alias "Severa", renting out access to spammers and other cybercriminals. But despite Levashov's significant efforts at anonymity, court records show that federal agents had been surveilling his iCloud account since 20 May 2016, funneling back crucial information that may have led to his arrest. The standing federal iCloud warrant would have given authorities a running tab of IP addresses used to log in to the account, which could easily have tipped them off to his vacation in Barcelona, Spain, and was arrested at the request of US law enforcement and extradited to the United States for prosecution.[20]

Structure, operations and spread

The Kelihos botnet is a so-called peer-to-peer botnet, where individual botnet nodes are capable of acting as command-and-control servers for the entire botnet. In traditional non-peer-to-peer botnets, all the nodes receive their instructions and "work" from a limited set of servers – if these servers are removed or taken down, the botnet will no longer receive instructions and will therefore effectively shut down.[21] Peer-to-peer botnets seek to mitigate that risk by allowing every peer to send instructions to the entire botnet, thus making it more difficult to shut down.[2]

The first version of the botnet was mainly involved in denial-of-service attacks and email spam, while version two of the botnet added the ability to steal Bitcoin wallets, as well as a program used to mine bitcoins itself.[2][22] Its spam capacity allows the botnet to spread itself by sending malware links to users in order to infect them with a Trojan horse, though later versions mostly propagate over social network sites, in particular through Facebook.[16][23] A more comprehensive list of the Kelihos spam can be found in the following research paper.[24]

UNITED STATES DISTRICT COURT

U.S. v. Levashov Search Warrant (Unsealed)

Arrest and extradition

On 2 February 2018, the United States Department of Justice announced that a Russian national has been extradited from Spain and will be arraigned in Connecticut on charges stemming from his alleged operation of the Kelihos botnet. Peter Yuryevich Levashov, 37, also known as Pyotr Levashov,[25] Petr Levashov, Peter Severa, Petr Severa and Sergey Astakhov, of St. Petersburg, was detained on 7 April 2017 in Barcelona, when he was arrested by Spanish authorities based upon a criminal complaint and arrest warrant issued in the United States District of Connecticut.[26] On 3 February 2018, he pleaded not guilty to the charges of wire and email fraud, hacking, identity theft and conspiracy after appearing before a federal judge in the U.S. state of Connecticut. He remains in detention.[25] In September 2018, Levashov pleaded guilty.[27]

See also

References

1. ^ **a** **b** **c** *Mills, Elinor (28 March 2012). "110,000 PC-strong Kelihos botnet sidelined". CNET. Retrieved 28 April 2012.*
2. ^ **a** **b** **c** **d** *Ortloff, Stefan (28 March 2012). "FAQ: Disabling the new Hlux/Kelihos Botnet". Securelist.com. Retrieved 19 May 2020.*
3. **^** *Adair, Steven (30 December 2010). "New Fast Flux Botnet for the Holidays: Could it be Storm Worm 3.0/Waledac 2.0?". Shadowserver. Retrieved 28 April 2012.*
4. **^** *Donohue, Brian (29 March 2012). "Kelihos Returns: Same Botnet or New Version?". Threatpost. Archived from the original on 4 April 2012. Retrieved 28 April 2012.*
5. ^ **a** **b** *Mills, Elinor (27 September 2011). "Microsoft halts another botnet: Kelihos". CNet. Retrieved 28 April 2012.*

6. ^ a b Kirk, Jeremy (1 February 2012). "Kelihos botnet, once crippled, now gaining strength". Network World. Archived from the original on 5 September 2012. Retrieved 28 April 2012.
7. ^ a b Constantin, Lucian (28 March 2012). "Security Firms Disable the Second Kelihos Botnet". PCWorld. Retrieved 28 April 2012.
8. ^ a b Boscovich, Richard (27 September 2011). "Microsoft Neutralizes Kelihos Botnet, Names Defendant in Case". Microsoft TechNet. Retrieved 28 April 2012.
9. ^ Microsoft (26 September 2011). "Operation b79 (Kelihos) and Additional MSRT September Release". Microsoft Technet. Retrieved 28 April 2012.
10. ^ Latif, Lawrence (27 October 2011). "Microsoft drops Kelihos botnet allegations against ISP owner". The Inquirer. Archived from the original on 30 October 2011. Retrieved 28 April 2012. {{cite web}} : CS1 maint: unfit URL (link)
11. ^ a b Gonsalves, Antone (24 January 2012). "Microsoft Says Ex-Antivirus Maker Ran Botnet". CRN Magazine. Retrieved 28 April 2012.
12. ^ Warren, Tom (29 March 2012). "Second Kelihos botnet downed, 116,000 machines freed". The Verge. Retrieved 28 April 2012.
13. ^ Brewster, Tom (24 January 2012). "Microsoft suspects ex-antivirus worker of Kelihos botnet creation". IT PRO. Retrieved 28 April 2012.
14. ^ Keizer, Gregg (24 January 2012). "Accused Kelihos botnet maker worked for two security firms | ITworld". ITworld. Retrieved 28 April 2012.
15. ^ Donohue, Brian (28 March 2012). "Kaspersky Knocks Down Kelihos Botnet Again, But Expects Return". ThreatPost. Archived from the original on 12 April 2012. Retrieved 28 April 2012.
16. ^ a b Raywood, Dan (2 April 2012). "CrowdStrike researchers deny that Kelihos has spawned a new version – SC Magazine UK". SC Magazine. Retrieved 29 April 2012.
17. ^ Leyden, John (29 March 2012). "Kelihos zombies erupt from mass graves after botnet massacre". The Register. Retrieved 28 April 2012.
18. ^ SPAMfighter News (13 April 2012). "Kelihos Botnet Re-emerges, This Time Attacking Social Networks". SPAMfighter. Retrieved 28 April 2012.
19. ^ http://www.abuseat.org
20. ^ "Feds tracked down Russian spam kingpin with help from his iCloud account". The Verge. Retrieved 6 February 2018.
21. ^ Grizzard, Julian; David Dagon; Vikram Sharma; Chris Nunnery; Brent ByungHoon Kang (3 April 2007). "Peer-to-Peer Botnets: Overview and Case Study". The Johns Hopkins University Applied Physics Laboratory. Retrieved 28 April 2012.
22. ^ SPAMfighter (5 April 2012). "Security Companies Take Down Kelihos Botnet of Version 2". SPAMfighter. Retrieved 28 April 2012.
23. ^ Jorgenson, Petra (6 April 2012). "Kelihos Botnet Could Resurge via Facebook Worm". Midsize Insider. Retrieved 29 April 2012.
24. ^ Arora, Arsh; Gannon, Max; Warner, Gary (15 May 2017). "Kelihos Botnet: A Never-Ending Saga". Annual ADFSL Conference on Digital Forensics, Security and Law.
25. ^ a b

26. ^ *"Alleged Operator of Kelihos Botnet Extradited From Spain". www.justice.gov. 2 February 2018. Retrieved 3 February 2018.*
27. ^ *Farivar, Cyrus (13 September 2018). "Russian man pleads guilty, admits he ran notorious Kelihos botnet". ArsTechnica. Retrieved 2 April 2019.*

Botnets

- Akbot
- Asprox
- Bagle
- BASHLITE
- Bredolab
- Cutwail
- Conficker
- Donbot
- Festi
- Grum
- Gumblar
- Kelihos
- Koobface
- Kraken
- Lethic
- Mariposa
- Mega-D
- Mirai
- Metulji
- Nitol
- Rustock
- Sality
- Slenfbot
- Srizbi
- Storm
- TDL-4
- Torpig
- Virut
- Vulcanbot
- Waledac
- ZeroAccess
- Zeus

Notable botnets

- Browser security
- Computer virus
- Computer worm
- Malbot
- Internet security
- Malware
- Man-in-the-browser
- Network security
- Operation: Bot Roast
- Trojan horse

Main articles