GhostNet

For the fishing net, see Ghost net.

GhostNet (simplified Chinese: 幽灵网; traditional Chinese: 幽靈網; pinyin: *YōuLíngWǎng*) is the name given by researchers at the Information Warfare Monitor to a large-scale cyber spying[1][2] operation discovered in March 2009. The operation is likely associated with an advanced persistent threat, or a network actor that spies undetected.[3] Its command and control infrastructure is based mainly in the People's Republic of China and GhostNet has infiltrated high-value political, economic and media locations[4] in 103 countries. Computer systems belonging to embassies, foreign ministries and other government offices, and the Dalai Lama's Tibetan exile centers in India, London and New York City were compromised.

Discovery

GhostNet was discovered and named following a 10-month investigation by the Infowar Monitor (IWM), carried out after IWM researchers approached the Dalai Lama's representative in Geneva[5] suspecting that their computer network had been infiltrated.[6] The IWM is composed of researchers from The SecDev Group and Canadian consultancy and the Citizen Lab, Munk Centre for International Studies at the University of Toronto; the research findings were published in the *Infowar Monitor*, an affiliated publication.[7] Researchers from the University of Cambridge's Computer Laboratory, supported by the Institute for Information Infrastructure Protection,[8] also contributed to the investigation at one of the three locations in Dharamshala, where the Tibetan government-in-exile is located. The discovery of the 'GhostNet', and details of its operations, were reported by *The New York Times* on March 29, 2009.[7][9] Investigators focused initially on allegations of Chinese cyber-espionage against the Tibetan exile community, such as instances where email correspondence and other data were extracted.[10]

Compromised systems were discovered in the embassies of India, South Korea, Indonesia, Romania, Cyprus, Malta, Thailand, Taiwan, Portugal, Germany and Pakistan and the office of the Prime Minister of Laos. The foreign ministries of Iran, Bangladesh, Latvia, Indonesia, Philippines, Brunei, Barbados and Bhutan were also targeted.[1][11] No evidence was found that U.S. or UK government offices were infiltrated, although a NATO computer was monitored for half a day and the computers of the Indian embassy in Washington, D.C., were infiltrated.[4][11][12]

Since its discovery, GhostNet has attacked other government networks, for example Canadian official financial departments in early 2011, forcing them off-line. Governments commonly do not admit such attacks, which must be verified by official but anonymous

sources.[13]

Technical functionality

Emails are sent to target organizations that contain contextually relevant information. These emails contain malicious attachments, that when opened, enable a trojan horse to access the system. This Trojan connects back to a control server, usually located in China, to receive commands. The infected computer will then execute the command specified by the control server. Occasionally, the command specified by the control server will cause the infected computer to download and install a trojan known as Gh0st Rat that allows attackers to gain complete, real-time control of computers running Microsoft Windows.[4] Such a computer can be controlled or inspected by attackers, and the software even has the ability to turn on camera and audio-recording functions of infected computers, enabling attackers to perform surveillance.[7]

Origin

The researchers from the IWM stated they could not conclude that the Chinese government was responsible for the spy network.[14] However, a report from researchers at the University of Cambridge says they believe that the Chinese government is behind the intrusions they analyzed at the Office of the Dalai Lama.[15]

Researchers have also noted the possibility that GhostNet was an operation run by private citizens in China for profit or for patriotic reasons, or created by intelligence agencies from other countries such as Russia or the United States.[7] The Chinese government has stated that China "strictly forbids any cyber crime."[1][10]

The "Ghostnet Report" documents several unrelated infections at Tibetan-related organizations in addition to the Ghostnet infections. By using the email addresses provided by the IWM report, Scott J. Henderson had managed to trace one of the operators of one of the infections (non-Ghostnet) to Chengdu. He identifies the hacker as a 27-year-old man who had attended the University of Electronic Science and Technology of China, and currently connected with the Chinese hacker underground.[16]

Despite the lack of evidence to pinpoint the Chinese government as responsible for intrusions against Tibetan-related targets, researchers at Cambridge have found actions taken by Chinese government officials that corresponded with the information obtained via computer intrusions. One such incident involved a diplomat who was pressured by Beijing after receiving an email invitation to a visit with the Dalai Lama from his representatives.[15]

Another incident involved a Tibetan woman who was interrogated by Chinese intelligence officers and was shown transcripts of her online conversations.[14][17] However, there are other possible explanations for this event. Drelwa uses QQ and other instant messengers to

communicate with Chinese Internet users. In 2008, IWM found that TOM-Skype, the Chinese version of Skype, was logging and storing text messages exchanged between users. It is possible that the Chinese authorities acquired the chat transcripts through these means.[18]

IWM researchers have also found that when detected, GhostNet is consistently controlled from IP addresses located on the island of Hainan, China, and have pointed out that Hainan is home to the Lingshui signals intelligence facility and the Third Technical Department of the People's Liberation Army.[4] Furthermore, one of GhostNet's four control servers has been revealed to be a government server.[19]

See also

References

1. ^ **a** **b** **c**
2. **^** *Glaister, Dan (March 30, 2009). "China Accused of Global Cyberspying". The Guardian Weekly. Vol. 180, no. 16. London. p. 5. Retrieved April 7, 2009.*
3. **^** *Sean Bodmer; Dr. Max Kilger; Gregory Carpenter; Jade Jones (2012). Reverse Deception: Organized Cyber Threat Counter-Exploitation. McGraw-Hill Osborne Media. ISBN 978-0071772495.*
4. ^ **a** **b** **c** **d** *Harvey, Mike (March 29, 2009). "Chinese hackers 'using ghost network to control embassy computers'". The Times. London. Retrieved March 29, 2009.*
5. **^** *"Tracking GhostNet: Investigating a Cyber Espionage Network".*
6. **^**
7. ^ **a** **b** **c** **d** *Markoff, John (March 28, 2009). "Vast Spy System Loots Computers in 103 Countries". New York Times. Retrieved March 29, 2009.*
8. **^** *Shishir Nagaraja, Ross Anderson (March 2009). "The snooping dragon: social-malware surveillance of the Tibetan movement" (PDF). University of Cambridge. p. 2. Retrieved March 31, 2009.*
9. **^**
10. ^ **a** **b** China-based spies target Thailand. Bangkok Post, March 30, 2009. Retrieved on March 30, 2009.
11. ^ **a** **b** *"Canadians find vast computer spy network: report". Reuters. March 28, 2009. Retrieved March 29, 2009.*
12. **^** *"Spying operation by China infiltrated computers: Report". The Hindu. March 29, 2009. Archived from the original on April 1, 2009. Retrieved March 29, 2009.*
13. **^** *"Foreign hackers attack Canadian government". CBC News. February 17, 2011. Retrieved February 17, 2011.*
14. ^ **a** **b** Tracking GhostNet: Investigating a Cyber Espionage Network. Munk Centre for International Studies. March 29, 2009

15. ^ *a b* *Nagaraja, Shishir; Anderson, Ross (March 2009). "The snooping dragon: social-malware surveillance of the Tibetan movement" (PDF). Computer Laboratory, University of Cambridge.*
16. ^ *Henderson, Scott (April 2, 2009). "Hunting the GhostNet Hacker". The Dark Visitor. Archived from the original on April 6, 2009. Retrieved April 2, 2009.*
17. ^ U of T team tracks China-based cyber spies Toronto Star March 29, 2009 Archived March 31, 2009, at the Wayback Machine
18. ^ BREACHING TRUST: An analysis of surveillance and security practices on China's TOM-Skype platform
19. ^ Meet the Canadians who busted Ghostnet *The Globe and Mail* March 29, 2009

External links

- The SecDev Group
- Citizen Lab at the University of Toronto
- Tracking GhostNet: Investigating a Cyber Espionage Network (Infowar Monitor Report (SecDev and Citize Lab), March 29, 2009)
- F-Secure Mirror of the report PDF
- Information Warfare Monitor - Tracking Cyberpower (University of Toronto, Canada/Munk Centre)
- Twitter: InfowarMonitor
- *Kelly, Cathal (March 31, 2009). "Cyberspies' code a click away - Simple Google search quickly finds link to software for Ghost Rat program used to target governments". Toronto Star (Canada). Toronto, Ontario, Canada. Retrieved April 4, 2009.*
- *Lee, Peter (April 8, 2009). "Cyber-skirmish at the top of the world". Asia Times Online. Archived from the original on April 10, 2009. Retrieved April 9, 2009.* `{{cite web}}` : CS1 maint: unfit URL (link)
- Bodmer, Kilger, Carpenter, & Jones (2012). Reverse Deception: Organized Cyber Threat Counter-Exploitation. New York: McGraw-Hill Osborne Media. ISBN 0071772499, ISBN 978-0071772495

Hacking in the 2000s

Timeline

Incidents	**2004** • Titan Rain (2003–2006) • Operation Firewall **2007** • Cyberattacks on Estonia • Operation: Bot Roast **2008** • Project Chanology • Cyberattacks on Georgia • Sarah Palin email hack • US Military Cyberattack **2009** • Operation Troy • WebcamGate (2008–2010)
Groups	• Anonymous associated events • Avalanche • GNAA • GhostNet • PLA Unit 61398 • RBN • ShadowCrew • World of Hell
Individuals	• Jeanson James Ancheta • BadB • camZero • Coolio • Cyxymu • diabl0 • Albert Gonzalez • Jaschan • Samy Kamkar • Kirtaner • Dmitry Sklyarov • Stakkato
Vulnerabilities discovered	• Shatter attack (2002) • sslstrip (2009)
Malware	

2000	• ILOVEYOU • Pikachu
2001	• Anna Kournikova • Code Red • Nimda • Klez
2002	Simile
2003	• SQL Slammer • Welchia • Sobig • Gruel • Blaster
2004	• Bagle • NetSky • Sasser • Mydoom
2005	• PGPCoder • Samy
2006	• Rostock • ZLOB • Stration
2007	• Storm • ZeuS
2008	• Asprox • Patched • Agent.btz • Mariposa
2009	• Conficker • Koobface • Waledac