Numbered Panda

By Contributors to Wikimedia projects

Published: 2017-04-15 · Archived: 2026-04-06 03:26:44 UTC

From Wikipedia, the free encyclopedia

Numbered Panda	
Country	People's Republic of China
Branch	People's Liberation Army
Type	Cyber force Advanced persistent threat
Role	Cyber warfare Electronic warfare
Engagements	• Operation Double Tap • Operation Clandestine Fox

Numbered Panda (also known as **IXESHE**, **DynCalc**, **DNSCALC**, and **APT12**) is a cyber espionage group believed to be linked with the Chinese military.[1] The group typically targets organizations in East Asia.[1] These organizations include, but are not limited to, media outlets, high-tech companies, and governments.[2] Numbered Panda is believed to have been operating since 2009.[3] However, the group is also credited with a 2012 data breach at the New York Times.[4] One of the group's typical techniques is to send PDF files loaded with malware via spear phishing campaigns.[5] The decoy documents are typically written in traditional Chinese, which is widely used in Taiwan, and the targets are largely associated with Taiwanese interests.[3] Numbered Panda appears to be actively seeking out cybersecurity research relating to the malware they use. After an Arbor Networks report on the group, FireEye noticed a change in the group's techniques to avoid future detection.[1]

Discovery and security reports

[edit]

Trend Micro first reported on Numbered Panda in a 2012 white paper.[5] Researchers discovered that the group launched spear phishing campaigns, using the Ixeshe malware, primarily against East Asian nations since approximately 2009.[5] CrowdStrike further discussed the group in the 2013 blog post *Whois Numbered Panda*.[2] This post followed the 2012 attack on the New York Times and its subsequent 2013 reporting on the attack.[4] In

June 2014, Arbor Networks released a report detailing Numbered Panda's use of Etumbot to target Taiwan and Japan.[3] In September 2014, FireEye released a report highlighting the group's evolution.[1] FireEye linked the release of Arbor Network's report to Numbered Panda's change in tactics.[1]

East Asian Nations (2009-2011)

[edit]

Trend Micro reported on a campaign against East Asian governments, electronics manufacturers, and a telecommunications company.[5] Numbered Panda engaged in spear phishing email campaigns with malicious attachments.[5] Often, the malicious email attachments would be PDF files that exploited CVE-2009-4324, CVE-2009-09274, CVE-2011-06095, or CVE-CVE-2011-0611 vulnerabilities in Adobe Acrobat, Adobe Reader, and Flash Player.[5] The attackers also used an exploit that affected Microsoft Excel - CVE-2009-3129.[5] The Ixeshe malware used in this campaign allowed Numbered Panda to list all services, processes, and drives; terminate processes and services; download and upload files; start processes and services; get victims' user names; get a machine's name and domain name; download and execute arbitrary files; cause a system to pause or sleep for a specified number of minutes; spawn a remote shell; and list all current files and directories.[5] After installation, Ixeshe would start communicating with command-and-control servers; oftentimes three servers were hard-coded for redundancy.[5] Numbered Panda often used compromised servers to create these command-and-control servers to increase control of a victim's network infrastructure.[5] Using this technique, the group is believed to have amassed sixty servers by 2012.[5] A majority of the command-and-control servers used from this campaign were located in Taiwan and the United States.[5] Base64 was used for communication between the compromised computer and the server.[5] Trend Micro found that, once decoded, the communication was a standardized structure that detailed the computer's name, local IP address, proxy server IP and port, and the malware ID.[5] Researchers at CrowdStrike found that blogs and WordPress sites were frequently used in the command-and-control infrastructure to make the network traffic look more legitimate.[2]

Japan and Taiwan (2011-2014)

[edit]

An Arbor Security report found that Numbered Panda began a campaign against Japan and Taiwan using the Etumbot malware in 2011.[3] Similar to the previously observed campaign, the attackers would use decoy files, such as PDF, Excel spreadsheets, or Word documents, as email attachments to gain access to victims' computers.[3] Most of the documents observed were written in Traditional Chinese and usually pertained to Taiwanese government interests; several of the files related to upcoming conferences in Taiwan.[3] Once the malicious file was downloaded and extracted by the victim, Etumbot uses a right-to-left override exploit to trick the victim to download the malware installer.[3] According to Arbor Security, the "technique is a simple way for malware writers to disguise the names of malicious files. A hidden Unicode character in the filename will reverse the order of the characters that follow it, so that a .scr binary file appears to be a .xls document, for example."[3] Once the malware is installed, it sends a request to a command-and-control server with a RC4 key to encrypt subsequent communication.[3] As was with the Ixeshe malware, Numbered Panda used Base64 encoded characters to

communicate from compromised computers to the command-and-control servers.[3] Etumbot is able to determine if the target computer is using a proxy and will bypass the proxy settings to directly establish a connection.[3] After communication is established, the malware will send an encrypted message from the infected computer to the server with the NetBIOS name of the victim's system, user name, IP address, and if the system is using a proxy.[3]

After the May 2014 Arbor Security report detailed Etumbot, FireEye discovered that Numbered Panda changed parts of the malware.[1] FireEye noticed that the protocols and strings previously used were changed in June 2014.[1] The researchers at FireEye believe this change was to help the malware evade further detection.[1] FireEye named this new version of Etumbot HighTide.[1] Numbered Panda continued to target Taiwan with spear phishing email campaigns with malicious attachments.[1] Attached Microsoft Word documents exploited the CVE-2012-0158 vulnerability to help propagate HighTide.[1] FireEye found that compromised Taiwanese government employee email accounts were used in some of the spear phishing.[1] HighTide differs from Etumbot in that its HTTP GET request changed the User Agent, the format and structure of the HTTP Uniform Resource Identifier, the executable file location, and the image base address.[1]

New York Times (2012)

[edit]

Numbered Panda is believed to be responsible for the computer network breach at the New York Times in late 2012.[6][4] The attack occurred after the New York Times published a story about how the relatives of Wen Jiabao, the sixth Premier of the State Council of the People's Republic of China, "accumulated a fortune worth several billion dollars through business dealings."[4] The computers used to launch the attack are believed to be the same university computers used by the Chinese military to attack United States military contractors.[4] Numbered Panda used updated versions of the malware packages Aumlib and Ixeshe.[6] The updated Aumlib allowed Numbered Panda to encode the body of a POST request to gather a victim's BIOS, external IP, and operating system.[6] A new version of Ixeshe altered the previous version's network traffic pattern in an effort to evade existing network traffic signatures designed to detect Ixeshe related infections.[6]

1. ^ Jump up to: *a b c d e f g h i j k l m* *Moran, Ned; Oppenheim, Mike (3 September 2014). "Darwin's Favorite APT Group". Threat Research Blog. FireEye. Archived from the original on 18 July 2017. Retrieved 15 April 2017.*
2. ^ Jump up to: *a b c* *Meyers, Adam (29 March 2013). "Whois Numbered Panda". CrowdStrike. Archived from the original on 16 March 2016. Retrieved 15 April 2017.*
3. ^ Jump up to: *a b c d e f g h i j k l* *"Illuminating the Etumbot APT Backdoor" (PDF). Arbor Networks. June 2014.*
4. ^ Jump up to: *a b c d e* *Perlroth, Nicole (2013-01-30). "Chinese Hackers Infiltrate New York Times Computers". The New York Times. ISSN 0362-4331. Archived from the original on 2017-04-30. Retrieved 2017-04-24.*

5. ^ Jump up to: ***a*** ***b*** ***c*** ***d*** ***e*** ***f*** ***g*** ***h*** ***i*** ***j*** ***k*** ***l*** ***m*** ***n*** *Sancho, David; Torre, Jessa dela; Bakuei, Matsukawa; Villeneuve, Nart; McArdle, Robert (2012). "IXESHE: An APT Campaign" (PDF). Trend Micro. Archived (PDF) from the original on 2018-03-07. Retrieved 2017-04-15.*
6. ^ Jump up to: ***a*** ***b*** ***c*** ***d*** *"Survival of the Fittest: New York Times Attackers Evolve Quickly « Threat Research Blog". FireEye. Archived from the original on 2018-05-21. Retrieved 2017-04-24.*
