WIKIPEDIA

July 2009 cyberattacks

The **July 2009 cyberattacks** were a series of coordinated cyberattacks against major government, news media, and financial websites in South Korea and the United States.[1] The attacks involved the activation of a botnet—a large number of hijacked computers—that maliciously accessed targeted websites with the intention of causing their servers to overload due to the influx of traffic, known as a DDoS attack.[1] Most of the hijacked computers were located in South Korea.[2] The estimated number of the hijacked computers varies widely; around 20,000 according to the South Korean National Intelligence Service, around 50,000 according to Symantec's Security Technology Response group,[3] and more than 166,000 according to a Vietnamese computer security researcher who analyzed the log files of the two servers the attackers controlled.[4] An investigation revealed that at least 39 websites were targets in the attacks based on files stored on compromised systems.[5][6]

The targeting and timing of the attacks—which started the same day as a North Korean short-range ballistic missile test—have led to suggestions that they may be from North Korea, although these suggestions have not been substantiated.[7][8][9] Researchers would later find links between these cyberattacks, the DarkSeoul attacks in 2013, and other attacks attributed to the Lazarus Group.[10] This attack is considered by some to be the beginning of a series of DDoS attacks carried about by Lazarus dubbed "Operation Troy."[11]

Contents

Timeline of attacks
- First wave
- Second wave
- Third wave

Effects

Perpetrators

See also

References

Timeline of attacks

First wave

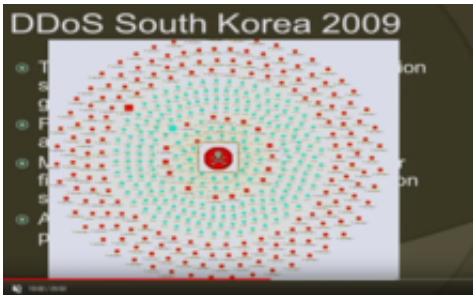
The first wave of attacks occurred on July 4, 2009 (Independence Day holiday in the United States), targeting both the United States and South Korea. Among the websites affected were those of the White House, The Pentagon, the New York Stock Exchange, the Washington Post, the NASDAQ, and Amazon.[1][12]

Second wave

The second wave of attacks occurred on July 7, 2009, affecting South Korea. Among the websites targeted were the presidential Blue House, the Ministry of Defense, the Ministry of Public Administration and Security, the National Intelligence Service and the National Assembly.[7][13][12] Security researcher Chris Kubecka presented evidence multiple European Union and United Kingdom companies unwittingly helped attack South Korea due to a W32.Dozer infections, malware used in part of the attack. Some of the companies used in the attack were partially owned by several governments, further complicating attribution.[14]

Third wave

A third wave of attacks began on July 9, 2009, targeting several websites in South Korea, including the country's National Intelligence Service as well as one of its largest banks and a major news agency.[1][15] The U.S. State Department said on July 9 that its website also came under attack.[16] State Department spokesman Ian Kelly said: "I'm just going to speak about our website, the state.gov website. There's not a high volume of attacks. But we're still concerned about it. They are continuing."[16] U.S. Department of Homeland Security spokesperson Amy Kudwa said that the department was aware of the attacks and that it had issued a notice to U.S. federal departments and agencies to take steps to mitigate attacks.[5]



Visualization of 2009 cyber warfare attacks against South Korea

Effects

Despite the fact that the attacks targeted major public and private sector websites, the South Korean Presidential office suggested that the attacks were conducted with the purpose of causing disruption, rather than stealing data.[17] However, Jose Nazario, manager of a U.S. network security firm, claimed that the attack is estimated to have produced only 23 megabits of data per second, not enough to cause major disruptions.[5] That being said, web sites reported service disruptions for days following the attack.[8]

Later, it was discovered that the malicious code responsible for causing the attack, Trojan.Dozer and its accompanying dropper W32.Dozer, was programmed to destroy data on infected computers and prevent the computers from being rebooted.[3] It is unclear if this mechanism was ever activated. Security experts said that the attack re-used code from the Mydoom worm to spread infections between computers.[3][6] Experts further shared that the malware used in the attack "used no sophisticated techniques to evade detection by anti-virus software and doesn't appear to have been written by someone experienced in coding malware."[6]

It was expected that the economic costs associated with websites being down would be large, as the disruption had prevented people from carrying out transactions, purchasing items or conducting business.[18]

Perpetrators

It is not known who is behind the attacks. Reports indicate that the type of attacks being used, commonly known as distributed denial-of-service attacks, were unsophisticated.[9][5][19] Given the prolonged nature of the attacks, they are being recognized as a more coordinated and organized series of attacks.[8]

According to the South Korean National Intelligence Service, the source of the attacks was tracked down and the government activated an emergency cyber-terror response team who blocked access to five host sites containing the malicious code and 86 websites that downloaded the code, located in 16 countries, including the United States, Guatemala, Japan and the People's Republic of China, but North Korea was not among them.[20]

The timing of the attack led some analysts to be suspicious of North Korea. The attack started on July 4, 2009, the same day as a North Korean short-range ballistic missile launch, and also occurred less than one month after the passage of UN Security Council Resolution 1874, which imposed further economic and commercial sanctions on North Korea in response to an underground nuclear test conducted earlier that year.

South Korean police analyzed a sample of the thousands of computers used by the botnet, stating that there is "various evidence" of the involvement of North Korea or "pro-North elements," but said they may not find the culprit.[21][18] Intelligence officials with the South Korean government warned lawmakers that a "North Korean military research institute had been ordered to destroy the South's communications networks."[21]

Joe Stewart, researcher at SecureWorks' Counter Threat Unit, noted that the data generated by the attacking program appeared to be based on a Korean-language browser.[5]

Various security experts have questioned the narrative that the attack originated in North Korea. One analyst thinks that the attacks likely came from the United Kingdom, while technology analyst Rob Enderle hypothesizes that "overactive students" may be to blame.[4][18] Joe Stewart of SecureWorks speculated that attention-seeking behavior drove the attack, though he notes that the breadth of the attack was "unusual."[6]

On October 30, 2009, South Korea's spy agency, the National Intelligence Service, named North Korea as the perpetrator of the attack. According to head of the NIS Won Sei-hoon, the organization found a link between the attacks and North Korea via an IP address that the North Korean Ministry of Post and Telecommunications allegedly " [was] using on rent (from China)."[22]

See also

- 2007 cyberattacks on Estonia
- Cyberterrorism
- Cyber Storm Exercise
- Moonlight Maze
- Titan Rain
- Comparison of computer viruses
- Denial-of-service attack

References

1. "New 'cyberattacks' hit S Korea" (http://news.bbc.co.uk/1/hi/world/asia-pacific/8142282.stm). BBC News. 2009-07-09. Retrieved 2009-07-09.
2. Claburn, Thomas (2009-07-10). "Cyber Attack Code Starts Killing Infected PCs" (http://www.informationweek.com/news/showArticle.jhtml?articleID=218401559). InformationWeek. Retrieved 2009-07-10.
3. Mills, Elinor (2009-07-10). "Botnet worm in DOS attacks could wipe data out on infected PCs" (http://news.cnet.com/8301-1009_3-10284281-83.html). CNET News. Retrieved 2009-07-12.
4. Williams, Martyn (2009-07-14). "UK, not North Korea, source of DDOS attacks, researcher says" (https://web.arc

4. Williams, Martyn (2009-07-14). "UK, not North Korea, source of DDOS attacks, researcher says" (https://web.archive.org/web/20110615004758/http://www.networkworld.com/news/2009/071409-uk-not-north-korea-source.html?ap1=rcb). IDG News Service. Archived from the original (http://www.networkworld.com/news/2009/071409-uk-not-north-korea-source.html?ap1=rcb) on 2011-06-15.
5. Markoff, John (2009-07-09). "Cyberattacks Jam Government and Commercial Web Sites in U.S. and South Korea" (https://www.nytimes.com/2009/07/10/technology/10cyber.html). *The New York Times*. Retrieved 2009-07-09.
6. Zetter, Kim (2009-07-08). "Lazy Hacker and Little Worm Set Off Cyberwar Frenzy" (https://www.wired.com/threatlevel/2009/07/mydoom/). Wired News. Retrieved 2009-07-09.
7. "Pyongyang blamed as cyberattack hits S Korea" (http://www.ft.com/cms/s/0/61bc6d22-6c1f-11de-9320-00144feabdc0.html). *Financial Times*. 2009-07-09. Retrieved 2009-07-09.
8. Kim, Hyung-Jin (2009-07-08). "Korean, US Web sites hit by suspected cyberattack" (https://web.archive.org/web/20090711142028/https://www.google.com/hostednews/ap/article/ALeqM5jvH8X8qojQgzc1R8X_5PceTd1nWQD99A5BQ81). Associated Press. Archived from the original (https://www.google.com/hostednews/ap/article/ALeqM5jvH8X8qojQgzc1R8X_5PceTd1nWQD99A5BQ81) on July 11, 2009. Retrieved 2009-07-09.
9. McDevitt, Caitlin (2009-07-09). "Cyberattack Aftermath" (https://web.archive.org/web/20090712051234/https://www.reuters.com/article/bigMoney/idUS292302408420090709). Reuters. Archived from the original (https://www.reuters.com/article/bigMoney/idUS292302408420090709) on July 12, 2009. Retrieved 2009-07-09.
10. Zetter, Kim (2016-02-24). "The Sony Hackers Were Causing Mayhem Years Before They Hit the Company" (https://www.wired.com/2016/02/sony-hackers-causing-mayhem-years-hit-company/). *Wired*. ISSN 1059-1028 (https://www.worldcat.org/issn/1059-1028). Retrieved 2018-12-14.
11. Martin, David (March 4, 2016). "Tracing the Lineage of DarkSeoul" (https://www.sans.org/reading-room/whitepapers/critical/tracing-lineage-darkseoul-36787). *SANS Institute*.
12. "Governments hit by cyberattack" (http://news.bbc.co.uk/1/hi/technology/8139821.stm). BBC News. 2009-07-08. Retrieved 2009-07-09.
13. "Cyber Attacks Hit Government and Commercial Websites" (https://web.archive.org/web/20090712015156/http://www.foxreno.com/news/19999665/detail.html). Foxreno.com. 2009-07-08. Archived from the original (http://www.foxreno.com/news/19999665/detail.html) on 2009-07-12. Retrieved 2009-07-09.
14. "28c3: Security Log Visualization with a Correlation Engine" (https://www.youtube.com/watch?v=j4pF9VUdphc). December 29, 2011. Retrieved November 4, 2017.
15. "Official: S. Korea web sites under renewed attack" (https://web.archive.org/web/20090715120005/https://www.google.com/hostednews/ap/article/ALeqM5jvH8X8qojQgzc1R8X_5PceTd1nWQD99ATHCO0). Associated Press. 2009-07-09. Archived from the original (https://www.google.com/hostednews/ap/article/ALeqM5jvH8X8qojQgzc1R8X_5PceTd1nWQD99ATHCO0) on July 15, 2009. Retrieved 2009-07-09.
16. "US State Department under cyberattack for fourth day" (https://www.google.com/hostednews/afp/article/ALeqM5jnGA5yrkZlqmNHmhctub8FuA9TbA). AFP. 2009-07-10.
17. "S Korea's presidential office says no damage done from hacker attacks" (http://news.xinhuanet.com/english/2009-07/08/content_11672939.htm). Xinhua. 2009-07-08. Retrieved 2009-07-09.
18. Han, Jane (2009-07-09). "Cyber Attack Hits Korea for Third Day" (https://web.archive.org/web/20090711054452/http://www.koreatimes.co.kr/www/news/biz/2009/07/123_48203.html). *Korea Times*. Archived from the original (http://www.koreatimes.co.kr/www/news/biz/2009/07/123_48203.html) on 2009-07-11. Retrieved 2009-07-09.
19. Arnoldy, Ben (2009-07-09). "Cyberattacks against US, S. Korea signal anger – not danger" (http://www.csmonitor.com/2009/0709/p06s23-woap.html). *Christian Science Monitor*.
20. Jiyeon, Lee (2009-07-11). "Cyberattack rocks South Korea" (http://www.globalpost.com/dispatch/south-korea/090710/cyberattacks). GlobalPost. Retrieved 2009-07-11.
21. Kim, Kwang-Tae (2009-07-12). "S. Korea analyzes computers used in cyberattacks" (https://web.archive.org/web/20090716043909/https://www.google.com/hostednews/ap/article/ALeqM5jO5PtkM_1FjwMZjh3LS74g26yiUQD99CRCO80). Associated Press. Archived from the original (https://www.google.com/hostednews/ap/article/ALeqM5j

O5PtkM_1FjwMZjh3LS74g26yiUQD99CRCO80) on July 16, 2009. Retrieved 2009-07-12.

22. "N. Korean ministry behind July cyberattacks: spy chief" (http://english.yonhapnews.co.kr/northkorea/2009/10/30/0401000000AEN20091030002200315.HTML). Yonhap. October 30, 2009.

Retrieved from "https://en.wikipedia.org/w/index.php?title=July_2009_cyberattacks&oldid=886565185"

This page was last edited on 7 March 2019, at 02:20 (UTC).