WIKIPEDIA

Cyberattacks during the Russo-Georgian War

During the **Russo-Georgian War** a series of **cyberattacks** swamped and disabled websites of numerous South Ossetian, Georgian, Russian and Azerbaijani organisations.

Contents

Attacks

On 20 July 2008, weeks before the Russian invasion of Georgia, the "zombie" computers were already on the attack against Georgia.[1][2] The website of the Georgian president Mikheil Saakashvili was targeted, resulting in overloading the site. The traffic directed at the Web site included the phrase "win+love+in+Rusia". The site then was taken down for 24 hours.[3][4]

On 5 August 2008, the websites for OSInform News Agency and OSRadio were hacked. The OSinform website at osinform.ru kept its header and logo, but its content was replaced by the content of Alania TV website. Alania TV, a Georgian government supported television station aimed at audiences in South Ossetia, denied any involvement in the hacking of the rival news agency website. Dmitry Medoyev, the South Ossetian envoy to Moscow, claimed that Georgia was attempting to cover up the deaths of 29 Georgian servicemen during the flare-up on August 1 and 2.[5]

On 5 August, Baku–Tbilisi–Ceyhan pipeline was subject to a terrorist attack near Refahiye in Turkey, responsibility for which was originally taken by Kurdistan Workers' Party (PKK) but there is circumstantial evidence that it was instead a sophisticated computer attack on line's control and safety systems that led to increased pressure and explosion.[6]

According to Jart Armin, a researcher, many Georgian Internet servers were under external control since late 7 August 2008.[7] On 8 August, the DDoS attacks peaked and the defacements began.[8]

On 9 August 2008, key sections of Georgia's Internet traffic reportedly had been rerouted through servers based in Russia and Turkey, where the traffic was either blocked or diverted. The Russian and Turkish servers were allegedly controlled by the Russian hackers. Later on the same day, the network administrators in Germany were able to temporarily reroute some Georgian Internet traffic directly to servers run by Deutsche Telekom AG. However, within hours the traffic was again diverted to Moscow-based servers.[7][9]

On 10 August 2008, RIA Novosti news agency's website was disabled for several hours by a series of attacks. Maxim Kuznetsov, head of the agency's IT department said: "The DNS-servers and the site itself have been coming under severe attack."[10]

On 10 August, Jart Armin warned that Georgian sites that were online might have been fake. "Use caution with any Web sites that appear of a Georgia official source but are without any recent news [such as those dated Saturday, Aug. 9, or Sunday, Aug. 10], as these may be fraudulent," he said.[7][9]

By 11 August 2008, the website of the Georgian president had been defaced and images comparing President Saakashvili to Adolf Hitler were posted. This was an example of cyber warfare combined with PSYOPs.[8] Georgian Parliament's site was also targeted.[8][7][11] Some Georgian commercial websites were also attacked.[9][7][11] On 11 August, Georgia accused Russia of waging cyber warfare on Georgian government websites simultaneously with a military offensive. The Foreign Ministry of Georgia said in a statement, "A cyber warfare campaign by Russia is seriously disrupting many Georgian websites, including that of the Foreign Affairs Ministry." A Kremlin spokesman denied the accusation and said, "On the contrary, a number of internet sites belonging to the Russian media and official organizations have fallen victim to concerted hacker attacks."[12] The Ministry of Foreign Affairs set up a blog on Google's Blogger service as a temporary site. The Georgian President's site was moved to US servers.[8][11] The National Bank of Georgia's Web site had been defaced at one point and 20th-century dictators' images and an image of Georgian president Saakashvili were placed.[1] The Georgian Parliament website was defaced by the "South Ossetia Hack Crew" and the content was replaced with images comparing President Saakashvili to Hitler.[11]

Estonia offered hosting for Georgian governmental website and cyberdefense advisors.[13][2] However a spokesman from Estonia's Development Centre of State Information Systems said Georgia didn't request help. "This will be decided by the government," he said.[9] It was reported that the Russians bombed Georgia's telecommunications infrastructure, including cell towers.[13]

Russian hackers also attacked the servers of the Azerbaijani Day.Az news agency. The reason was Day.Az position in covering the Russian-Georgian conflict.[14] ANS.az, one of the leading news websites in Azerbaijan, was also attacked.[15] Russian intelligence services had also disabled the information websites of Georgia during the war.[14] The Georgian news site Civil Georgia switched their operations to one of Google's Blogspot domains.[13] Despite the cyber-attacks, Georgian journalists managed to report on the war. Many media professionals and citizen journalists set up blogs to report or comment on the war.[16][17]

Barack Obama, the U.S. presidential candidate demanded Russia halt the internet attacks as well as complying with a ceasefire on the ground.[9] The President of Poland, Lech Kaczyński, said that Russia was blocking Georgian "internet portals" to supplement its military aggression. He offered his own website to Georgia to aid in the "dissemination of information".[11] Reporters Without Borders condemned the violations of online freedom of information since the outbreak of hostilities between Georgia and Russia. "The Internet has become a battleground in which information is the first victim," it said.[15]

The attacks involved Denial-of-service attacks.[1][11][15] The New York Times reported on 12 August that according to some experts, it was the first time in history a known cyberattack had coincided with a shooting war. On 12 August, the attacks continued, controlled by programs that were located in hosting centers controlled by a Russian telecommunications companies. A Russian-language site, stopgeorgia.ru, continued to operate and offer software for Denial-of-service attacks.[1]

RT reported on 12 August that during the previous 24 hours its website had been attacked. The security specialists said that the initial attacker was an IP-address registered in the Georgian capital Tbilisi.[18]

On 14 August 2008, it was reported that although a ceasefire reached, major Georgian servers were still down, hindering communication in Georgia.[17]

Analysis

The Russian government denied the allegations that it was behind the attacks, stating that it was possible that "individuals in Russia or elsewhere had taken it upon themselves to start the attacks".[1] Some sources have suggested that the Saint Petersburg-based criminal gang known as the Russian Business Network (RBN) was behind many of these cyber attacks.[7][8][9][1][19] RBN was considered to be among the world's worst spammer, child-pornography, malware, phishing and cybercrime hosting networks. It is thought that the RBN's leader and creator, known as Flyman, is the nephew of a powerful and well-connected Russian politician.[20]

Dancho Danchev, a Bulgarian Internet security analyst claimed that the Russian attacks on Georgian websites used “all the success factors for total outsourcing of the bandwidth capacity and legal responsibility to the average Internet user.”[8]

Jose Nazario, security researcher for Arbor Networks, told CNET that he was seeing evidence that Georgia was responding to the cyber attacks, attacking at least one Moscow-based newspaper site.[21]

Don Jackson, director of threat intelligence for SecureWorks, a computer security firm based in Atlanta, noted that in the run-up to the war over the weekend, computer researchers had observed as botnets were "staged" in preparation for the attack, and then activated shortly before Russian air strikes began on 9 August.[1]

Gadi Evron, the former chief of Israel's Computer Emergency Response Team, believed the attacks on Georgian internet infrastructure resembled a cyber-riot, rather than cyber-warfare. Evron admitted the attacks could be "indirect Russian (military) action," but pointed out the attackers "could have attacked more strategic targets or eliminated the (Georgian Internet) infrastructure kinetically." Shadowserver registered six different botnets involved in the attacks, each controlled by a different command server.[22]

Jonathan Zittrain, cofounder of Harvard's Berkman Center for Internet and Society, said that the Russian military definitely had the means to attack Georgia's Internet infrastructure. Bill Woodcock, the research director at Packet Clearing House, a California-based nonprofit group that tracked Internet security trends, said the attacks bore the markings of a "trained and centrally coordinated cadre of professionals." Russian hackers also brought down the Russian newspaper Skandaly.ru allegedly for expressing some pro-Georgian sentiment. "This was the first time that they ever attacked an internal and an external target as part of the same attack," Woodcock said. Gary Warner, a cybercrime expert at the University of Alabama at Birmingham, said that he found "copies of the attack script" (used against Georgia), complete with instructions for use, posted in the reader comments section at the bottom of virtually every story in the Russian media.[2] Bill Woodcock also said cyberattacks are so cheap and easy to stage, with few fingerprints, they would almost definitely stay around as a feature of modern warfare.[1]

The Economist wrote that anyone who wished to take part in the cyberattack on Georgia could do so from anywhere with an internet connection, by visiting one of pro-Russia websites and downloading the software and instructions needed to perform a distributed denial-of-service attack (DDoS) attack. One website, called StopGeorgia, provided a

utility called DoSHTTP, plus a list of targets, including Georgian government agencies and the British and American embassies in Tbilisi. Launching an attack simply required entering the address and clicking a button labelled "Start Flood". The StopGeorgia website also indicated which target sites were still active and which had collapsed. Other websites explained how to write simple programs for sending a flood of requests, or offered specially formatted webpages that could be set to reload themselves repeatedly, barraging particular Georgian websites with traffic. There was no conclusive evidence that the attacks was executed or sanctioned by the Russian government and also there was no evidence that it tried to stop them.[23]

In March 2009, Security researchers from Greylogic concluded that Russia's GRU and the FSB were likely to have played a key role in co-coordinating and organizing the attacks. The Stopgeorgia.ru forum was a front for state-sponsored attacks.[24]

John Bumgarner, member of the United States Cyber Consequences Unit (US-CCU) (http://www.usccu.us/) did a research on the cyberattacks during the Russo-Georgian War. The report concluded that the cyber-attacks against Georgia launched by Russian hackers in 2008 demonstrated the need for international cooperation for security. The report stated that the organizers of the cyber-attacks were aware of Russia's military plans, but the attackers themselves were believed to have been civilians. Bumgarner's research concluded that the first-wave of cyber-attacks launched against Georgian media sites were in line with tactics used in military operations.[25] "Most of the cyber-attack tools used in the campaign appear to have been written or customized to some degree specifically for the campaign against Georgia," the research stated. While the cyberattackers appeared to have had advance notice of the invasion and the benefit of some close cooperation from the state institutions, there were no fingerprints directly linking the attacks to the Russian government or military.[26]

See also

- 2007 cyberattacks on Estonia
- Cyxymu
- Cyberwarfare in Russia

References

1. Markoff, John (12 August 2008). "Before the Gunfire, Cyberattacks" (https://www.nytimes.com/2008/08/13/technology/13cyber.html). The New York Times.
2. Wentworth, Travis (23 August 2008). "How Russia May Have Attacked Georgia's Internet" (http://www.newsweek.com/how-russia-may-have-attacked-georgias-internet-88111). Newsweek.
3. Dancho Danchev (22 July 2008). "Georgia President's web site under DDoS attack from Russian hackers" (http://www.zdnet.com/article/georgia-presidents-web-site-under-ddos-attack-from-russian-hackers/). ZDNet.
4. "Georgia president's Web site falls under DDOS attack" (http://www.computerworld.com/article/2534930/networking/georgia-president-s-web-site-falls-under-ddos-attack.html). Computerworld. 21 July 2008.
5. "S.Ossetian News Sites Hacked" (http://www.civil.ge/eng/article.php?id=18896). Civil Georgia. 5 August 2008.
6. Jordan Robertson; Michael Riley (10 December 2014). "Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar Era" (https://www.bloomberg.com/news/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar.html). Bloomberg.com.
7. Keizer, Gregg (11 August 2008). "Cyberattacks knock out Georgia's Internet presence" (http://www.computerworld.com/s/article/9112201/Cyberattacks_knock_out_Georgia_s_Internet_presence). Computerworld.
8. Danchev, Dancho (11 August 2008). "Coordinated Russia vs Georgia cyber attack in progress" (http://www.zdnet

8. Danchev, Dancho (11 August 2008). "Coordinated Russia vs Georgia cyber attack in progress" (http://www.zdnet.com/blog/security/coordinated-russia-vs-georgia-cyber-attack-in-progress/1670). ZDNet.
9. "Georgia: Russia 'conducting cyber war' " (https://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html). The Telegraph. 11 August 2008.
10. "RIA Novosti hit by cyber-attacks as conflict with Georgia rages" (http://en.rian.ru/russia/20080810/115936419.html). RIA Novosti. 10 August 2008. Archived (https://web.archive.org/web/20080812050039/http://www.en.rian.ru/russia/20080810/115936419.html) from the original on 12 August 2008.
11. Asher Moses (12 August 2008). "Georgian websites forced offline in 'cyber war' " (http://www.smh.com.au/news/technology/georgian-websites-forced-offline/2008/08/12/1218306848654.html). The Sydney Morning Herald. Archived (https://web.archive.org/web/20080914040639/http://www.smh.com.au/news/technology/georgian-websites-forced-offline/2008/08/12/1218306848654.html) from the original on 14 September 2008.
12. "Georgia says Russian hackers block govt websites" (http://uk.reuters.com/article/2008/08/11/us-georgia-ossetia-hackers-idUKLB2050320080811). Reuters. 11 August 2008.
13. "Estonia, Google Help 'Cyberlocked' Georgia (Updated)" (https://www.wired.com/2008/08/civilge-the-geo/). 11 August 2008.
14. "Russian intelligence services undertook large scale attack against Day.Az server" (http://www.today.az/news/politics/46885.html). Today.az. 11 August 2008.
15. "Russian and Georgian websites fall victim to a war being fought online as well as in the field" (https://web.archive.org/web/20140714165753/https://en.rsf.org/georgia-russian-and-georgian-websites-fall-13-08-2008%2C28167.html). Reporters Without Borders. 13 August 2008. Archived from the original (https://en.rsf.org/georgia-russian-and-georgian-websites-fall-13-08-2008,28167.html) on 2014-07-14.
16. "Georgia: Regional Reporters" (http://globalvoicesonline.org/2008/08/24/georgia-regional-reporters/). Global Voices. 24 August 2008.
17. "Longtime Battle Lines Are Recast In Russia and Georgia's Cyberwar" (https://www.washingtonpost.com/wp-dyn/content/article/2008/08/13/AR2008081303623.html). The Washington Post. 14 August 2008.
18. "RT attacked" (https://web.archive.org/web/20080812235354/http://www.russiatoday.com/news/news/28835). RT. 12 August 2008. Archived from the original (http://www.russiatoday.com/news/news/28835) on 12 August 2008.
19. "Georgia States Computers Hit By Cyberattack" (https://www.wsj.com/articles/SB121850756472932159). The Wall Street Journal. 12 August 2008.
20. "The hunt for Russia's web crims" (http://www.theage.com.au/news/security/the-hunt-for-russias-web-crims/2007/12/12/1197135470386.html). The Age. 13 December 2007.
21. "Russia and Georgia continue attacks--online" (http://www.cnet.com/news/russia-and-georgia-continue-attacks-online/). CNET. 12 August 2008.
22. "Unlikely That Russians Hacked Georgia Though Attacks Were Political | Cyber Talk Blog by Shimon Sheves" (http://www.cybertalkblog.co.uk/unlikely-that-russians-hacked-georgia-though-attacks-were-political/). *www.cybertalkblog.co.uk*. Retrieved 2017-04-16.
23. "Marching off to cyberwar" (http://www.economist.com/science/tq/displaystory.cfm?story_id=12673385&CFID=34793589&CFTOKEN=83946352). The Economist. 4 December 2008. Archived (https://web.archive.org/web/20090506224852/http://www.economist.com/science/tq/displaystory.cfm?story_id=12673385&CFID=34793589&CFTOKEN=83946352) from the original on 6 May 2009.
24. Leyden, John (23 March 2009). "Russian spy agencies linked to Georgian cyber-attacks" (https://www.theregister.co.uk/2009/03/23/georgia_russia_cyberwar_analysis/). The Register.
25. Brian Prince (18 August 2009). "Cyber-attacks on Georgia Show Need for International Cooperation, Report States" (http://www.eweek.com/c/a/Security/Cyber-Attacks-on-Georgia-Show-Need-for-International-Cooperation-Report-States-294120/). eWeek.
26. Mark Rutherford (18 August 2009). "Report: Russian mob aided cyberattacks on Georgia" (http://news.cnet.com/8301-13639_3-10312708-42.html). CNET.

External links

- Russian Cyberwar on Georgia (http://www.mfa.gov.ge/files/556_10535_798405_Annex87_CyberAttacks.pdf)
- The Russo-Georgian War 2008: The Role of the cyber attacks in the conflict (http://www.afcea.org/committees/cyber/documents/TheRusso-GeorgianWar2008.pdf)
- Offensive Information Operations (http://www.army.gov.au/Our-future/Publications/Australian-Army-Journal/Past-editions/~/media/Files/Our%20future/LWSC%20Publications/AAJ/2010Summer/14-OffensiveInformationOpe.pdf)
- DEFINING AND DETERRING CYBER WAR (https://www.hsdl.org/?view&did=28659)