Cyberattacks during the Russo-Georgian War

From Wikipedia, the free encyclopedia

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. Russians directed the infected computers around the world to barrage Georgian Web sites, including the pages of the president, the parliament, the foreign ministry, news agencies and banks. The website of the Parliament of Georgia was replaced by images comparing Georgian president Mikheil Saakashvili to Adolf Hitler.[1] The attacks involved Denial-of-service attacks. According to some experts, it was the first time in history a known cyberattack had coincided with a shooting war.[2]

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.[3]

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.[4]

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."[5]

On 11 August 2008, 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."[6]

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.[7] Russian intelligence services had also disabled the information and governmental websites of Georgia during the war.[7]

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.[8] The Georgian news site Civil Georgia switched their operations to one of Google's Blogspot domains.[9] Estonia offered technical assistance and mirrored web pages for Georgian websites to use during the attacks.[1][9] The Georgian President's site was moved to US servers.[10]

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".[10] 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.[11] Barack Obama, the U.S. presidential candidate demanded Russia halt the internet attacks as well as complying with a ceasefire on the ground.[12]

It was reported that the Russians bombed Georgia’s telecommunications infrastructure, including cell towers.[9]

On 12 August 2008, RT reported 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.[13]

On 14 August 2008, it was reported that although a ceasefire reached, major

Georgian servers were still down, hindering communication in Georgia.[14]

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".[2] It was asserted that the Saint Petersburg-based criminal gang known as the Russian Business Network (RBN) was behind many of these cyber attacks.[4][15] 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.[16]

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.”[17]

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.[18]

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.[19]

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.[20]

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.[21]

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.[22] "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.[23]

See also

- 2007 cyberattacks on Estonia
- Cyxymu

References

1. ^ ***a b*** Wentworth, Travis (22 August 2008). "How Russia May Have Attacked Georgia's Internet" (http://www.newsweek.com/how-russia-may-have-attacked-georgias-internet-88111). Newsweek.
2. ^ ***a b*** Markoff, John (12 August 2008). "Before the Gunfire, Cyberattacks" (http://www.nytimes.com/2008/08/13/technology/13cyber.html). The New York Times.
3. ^ "S.Ossetian News Sites Hacked" (http://www.civil.ge/eng/article.php?id=18896). Civil Georgia. 5 August 2008.
4. ^ ***a b*** 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.
5. ^ "RIA Novosti hit by cyber-attacks as conflict with Georgia rages" (http://en.rian.ru/russia/20080810/115936419.html). RIA Novosti. 2008-08-10. Archived (http://web.archive.org/web/20080812050039/http://www.en.rian.ru/russia/20080810/115936419.html) from the original on 2008-08-12.