2007 cyberattacks on Estonia

From Wikipedia, the free encyclopedia

Cyberattacks on Estonia are a series of cyber attacks that began 27 April 2007 and swamped websites of Estonian organizations, including Estonian parliament, banks, ministries, newspapers and broadcasters, amid the country's disagreement with Russia about the relocation of the Bronze Soldier of Tallinn, an elaborate Soviet-era grave marker, as well as war graves in Tallinn.[1][2] Most of the attacks that had any influence on the general public were distributed denial of service type attacks ranging from single individuals using various methods like ping floods to expensive rentals of botnets usually used for spam distribution. Spamming of bigger news portals commentaries and defacements including that of the Estonian Reform Party website also occurred.[3]

Some observers reckoned that the onslaught on Estonia was of a sophistication not seen before. The case is studied intensively by many countries and military planners as, at the time it occurred, it may have been the second-largest instance of state-sponsored cyberwarfare, following Titan Rain.[4]

Estonian Foreign Minister Urmas Paet accused the Kremlin of direct involvement in the cyberattacks.[5] On 6 September 2007 Estonia's defense minister admitted he had no evidence linking cyber attacks to Russian authorities. "Of course, at the moment, I cannot state for certain that the cyber attacks were managed by the Kremlin, or other Russian government agencies," Jaak Aaviksoo said in interview on Estonian's Kanal 2 TV channel. Aaviksoo compared the cyber attacks with the blockade of Estonia's Embassy in Moscow. "Again, it is not possible to say without doubt that orders (for the blockade) came from the Kremlin, or that, indeed, a wish was expressed for such a thing there," said Aaviksoo. Russia called accusations of its involvement "unfounded," and neither NATO nor European Commission experts were able to find any proof of official Russian government participation.[6]

As of January 2008, one ethnic-Russian Estonian national has been charged and convicted.[7]

During a panel discussion on cyber warfare, Sergei Markov of the Russian State Duma has stated his unnamed aide was responsible in orchestrating the cyber attacks. Markov alleged the aide acted on his own while residing in an unrecognised republic of the former Soviet Union, possibly Transnistria.[8] On 10 March 2009 Konstantin Goloskokov, a "commissar" of the Kremlin-backed youth group Nashi, has claimed responsibility for the attack.[9] Experts are critical of these varying claims of responsibility.[10]

Contents

Legalities

On 2 May 2007, a criminal investigation was opened into the attacks under a section of the Estonian Penal Code criminalising *computer sabotage* and *interference with the working of a computer network*, felonies punishable by imprisonment of up to three years. As a number of attackers turned out to be within the jurisdiction of the Russian Federation, on 10 May 2007, Estonian Public Prosecutor's Office made a formal investigation assistance request to the Russian Federation's Supreme Procurature under a Mutual Legal Assistance Treaty (MLAT) existing between Estonia and Russia. A Russian State Duma delegation visiting Estonia in early May in regards the situation surrounding the Bronze Soldier of Tallinn had promised that Russia would aid such investigation in every way available.[11] On 28 June, Russian Supreme Procurature refused assistance,[11] claiming that the proposed investigative processes are not covered by the applicable MLAT.[12] Piret Seeman, the Estonian Public Prosecutor's Office's PR officer, criticized this decision, pointing out that all the requested processes are actually enumerated in the MLAT.[12]

On 24 January 2008, Dmitri Galushkevich, a student living in Tallinn, was found guilty of participating in the attacks. He was fined 17,500 kroons (approximately US$1,640) for attacking the website of the Estonian Reform Party.[3][13]

As of 13 December 2008, Russian authorities have been consistently denying Estonian law enforcement any investigative cooperation, thus effectively eliminating chances that those of the perpetrators that fall within Russian jurisdiction will be brought to trial.[14]

Opinions of experts

Critical systems whose network addresses would not be generally known were targeted, including those serving telephony and financial transaction processing.[15] Although not all of the computer crackers behind the cyberwarfare have been unveiled, some experts believed that such efforts exceed the skills of individual activists or even organised crime as they require a co-operation of a state and a large telecom company.[4]

A well known Russian hacker Sp0Raw believes that the most efficient online attacks on Estonia could not have been carried out without the blessing of the Russian authorities and that the hackers apparently acted under "recommendations" from parties in higher positions.[16] [17] At the same time he called claims of Estonians regarding direct involvement of Russian government in the attacks[18] "empty words, not supported by technical data".[17]

Mike Witt, deputy director of the United States Computer Emergency Readiness Team (CERT) believes that the attacks were DDoS attacks. The attackers used botnets – global networks of compromised computers, often owned by careless individuals. "The size of the cyber attack, while it was certainly significant to the Estonian government, from a technical standpoint is not something we would consider significant in scale," Witt said.[19]

Professor James Hendler, former chief scientist at The Pentagon's Defense Advanced Research Projects Agency (DARPA) characterised the attacks as "more like a cyber riot than a military attack."[19]

"We don't have directly visible info about sources so we can't confirm or deny that the attacks are coming from the Russian government," Jose Nazario, software and security engineer at Arbor Networks, told *internetnews.com*.[20] Arbor Networks operated *ATLAS* threat analysis network, which, the company claimed, could "see" 80% of Internet traffic. Nazario suspected that different groups operating separate distributed botnets were involved in the attack.

Experts interviewed by IT security resource SearchSecurity.com "say it's very unlikely this was a case of one government launching a coordinated cyberattack against another": Johannes Ullrich, chief research officer of the Bethesda said "Attributing a distributed denial-of-service attack like this to a government is hard." "It may as well be a group of bot herders showing 'patriotism,' kind of like what we had with Web defacements during the US-China spy-plane crisis [in 2001]." Hillar Aarelaid, manager of Estonia's Computer Emergency Response Team "expressed skepticism that the attacks were from the Russian government, noting that Estonians were also divided on whether it was right to remove the statue".[21]

Clarke and Knake report that upon the Estonian authorities informing Russian officials they had traced systems controlling the attack to Russia, there was some indication in response that incensed patriotic Russians might have acted on their own.[15] Regardless of conjectures over official involvement, the decision of Russian authorities not to pursue individuals responsible—a treaty obligation—together with expert opinion that Russian security services could readily track down the culprits should they so desire, leads Russia observers to conclude the attacks served Russian interests.[15]

Claiming responsibility for the attacks

A Commissar of the Nashi pro-Kremlin youth movement in Moldova and Transnistria, Konstantin Goloskokov (Goloskov in some sources[22]), admitted organizing cyberattacks against Estonian government sites.[16] Goloskokov stressed, however, that he was not carrying out an order from Nashi's leadership and said that a lot of his fellow Nashi members criticized his response as being too harsh.[17]

Like most countries, Estonia does not recognise Transnistria, a secessionist region of Moldova. As an unrecognised nation, Transnistria does not belong to Interpol.[23] Accordingly, no Mutual Legal Assistance Treaty applies. If residents of Transnistria were responsible, the investigation may be severely hampered, and even if the investigation succeeds finding likely suspects, the legal recourse of Estonian authorities may be limited to issuing all-EU arrest warrants for these suspects. Such an act would be largely symbolic.

Head of Russian Military Forecasting Center, Colonel Anatoly Tsyganok confirmed Russia's ability to conduct such an attack when he stated: "*These attacks have been quite successful, and today the alliance had nothing to oppose Russia's virtual attacks*", additionally noting that these attacks did not violate any international agreement.[24]

Influence on international military doctrines

The attacks triggered a number of military organizations around the world to reconsider the importance of network security to modern military doctrine. On 14 June 2007, defence ministers of NATO members held a meeting in Brussels, issuing a joint communiqué promising immediate action. First public results were estimated to arrive by autumn 2007.[25]

On 25 June 2007, Estonian president Toomas Hendrik Ilves met with US President, George W. Bush.[26] Among the topics discussed were the attacks on Estonian infrastructure. [27] NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) operates out of Tallinn, Estonia, since August 2008[28]

The events have been reflected in a NATO Department of Public Diplomacy short movie *War in Cyberspace*.[29]