Estonia under cyber attack

Compiled by Beatrix Toth (Hun-CERT)

1. The fact (start time, end time, type of attack)

Estonian government websites and others have been the victims of denial-of-service (DDoS)[1] attacks since 27. April 2007 till 11 Maj 2007. Additionally some Estonian websites were defaced, replacing the pages with Russian propaganda or bogus apologies. The attacks are gradually intensifying. The number on May 9th—the day when Russia and its allies commemorate Hitler's defeat in Europe—was the biggest.

2. Technical details

2.1 DDos

On the basis of the data collecting ATLAS2 Jose Nazario made a technical analysis3: they have seen 128 unique DDoS attacks on Estonian websites during the above mentioned two weeks. Of these, 115 were ICMP floods4, 4 were TCP SYN floods5, and 9 were generic traffic floods. Attacks were not distributed uniformly, with some sites seeing more attacks than others:

Attacks	Destination	Address or owner
35	“195.80.105.107/32″	pol.ee
7	“195.80.106.72/32″	www.riigikogu.ee
36	“195.80.109.158/32″	www.riik.ee, www.peaminister.ee, www.valitsus.ee
2	“195.80.124.53/32″	m53.envir.ee
2	“213.184.49.171/32″	www.sm.ee
6	“213.184.49.194/32″	www.agri.ee
4	“213.184.50.6/32″	
35	“213.184.50.69/32″	www.fin.ee (Ministry of Finance)

[1] A **denial of service (DoS)** attack is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have. In a **distributed denial-of-service (DDoS)**, large numbers of compromised systems (sometimes called a botnet) attack a single target.

2 ATLAS is a globally distributed network that Arbor claims can see 80 percent of the world's Internet traffic. http://atlas.arbor.net/

[3] http://asert.arbornetworks.com/2007/05/estonian-ddos-attacks-a-summary-to-date/

[4] **ICMP flood**, also known as Ping flood or Smurf attack, is type of Denial of Service attack that sends large amounts of (or just over-sized) ICMP packets to a machine in order to attempt to crash the TCP/IP stack on the machine and cause it to stop responding to TCP/IP requests.

[5] A **SYN flood** is a form of denial-of-service attack in which an attacker sends a succession of SYN requests to a target's system. There are two methods, but both involve the server not receiving the ACK.

a) The attacker sends several packets but does not send the "ACK" back to the server. The connections are hence half-opened and consuming server resources.

b) By spoofing the source IP address in the SYN, the server sends the SYN-ACK to the falsified IP address, and never receives the ACK.

Attacks	Destination	Address or owner
1	“62.65.192.24/32″	

The attacks themselves haven’t been steady, at least from the perspective given by ATLAS. If we look at how many attacks occurred on every day, we can see that they peaked a week or so ago, but they haven’t necessarily stopped.

Attacks	Date
21	2007-05-03
17	2007-05-04
31	2007-05-08
58	2007-05-09
1	2007-05-11

As for how long the attacks have lasted, quite a number of them last under an hour. However, when you think about how many attacks have occurred for some of the targets, this translates into a very long-lived attack. The longest attacks themselves were over 10 and a half hours long sustained, dealing a truly crushing blow to the endpoints.

Attacks	Date
17	less than 1 minute
78	1 min - 1 hour
16	1 hour - 5 hours
8	5 hours to 9 hours
7	10 hours or more

Finally, this is a decent sized botnet6 behind the attack, with aggregate bandwidth at our points of measurement maxing out at nearly 100 Mbps.

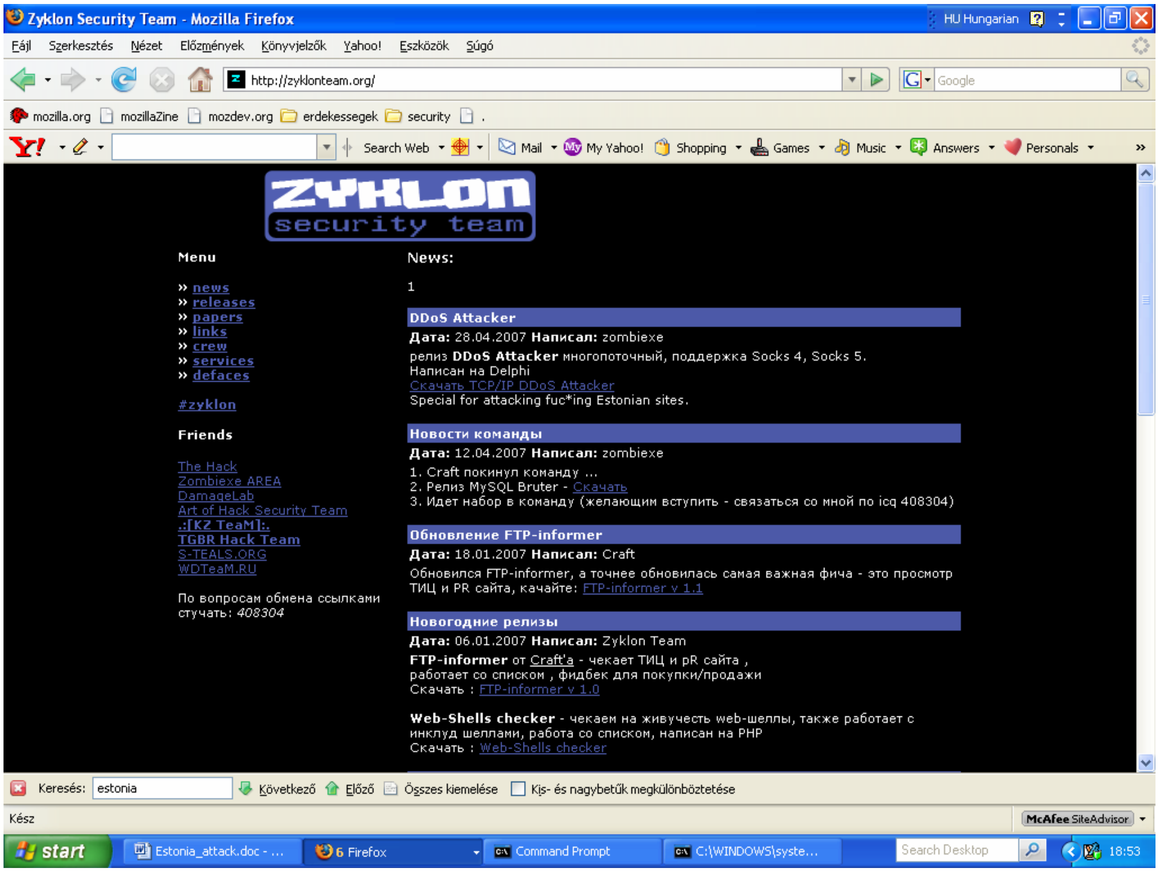
Attacks	Bandwidth measured
42	Less than 10 Mbps
52	10 Mbps - 30 Mbps
22	30 Mbps - 70 Mbps
12	70 Mbps - 95 Mbps

Largest attacks measured by ATLAS: 10 attacks measured at 90 Mbps, lasting upwards of 10 hours.

---

[6] **Botnet** used to refer to a collection of compromised computers (called zombie computers) running programs, usually referred to as worms, Trojan horses, or backdoors, under a common command and control infrastructure.

Here's an example of a Russian hacker site, offering Denial-of-Service tools crafted for this particular attack (http://zyklonteam.org/):


Zyklon Security Team - Mozilla Firefox
HU Hungarian
Fájl Szerkesztés Nézet Előzmények Könyvjelzők Yahoo! Eszközök Súgó
http://zyklonteam.org/
Google
mozilla.org mozillaZine mozdev.org erdekessegek security
Y! Search Web Mail My Yahoo! Shopping Games Music Answers Personals
ZYKLON security team
Keresés: estonia Következő Előző Összes kiemelése Kis- és nagybetűk megkülönböztetése
Kész
McAfee SiteAdvisor
start Estonia_attack.doc - ... 6 Firefox Command Prompt C:\WINDOWS\syste... Search Desktop 18:53

Menu

» news
» releases
» papers
» links
» crew
» services
» defaces

#zyklon

Friends

The Hack
Zombiexe AREA
DamageLab
Art of Hack Security Team
.:[KZ TeaM]:.
TGBR Hack Team
S-TEALS.ORG
WDTeaM.RU

По вопросам обмена ссылками стучать: *408304*

News:

1

DDoS Attacker

Дата: 28.04.2007 **Написал:** zombiexe

релиз **DDoS Attacker** многопоточный, поддержка Socks 4, Socks 5.
Написан на Delphi
Скачать TCP/IP DDoS Attacker
Special for attacking fuc*ing Estonian sites.

Новости команды

Дата: 12.04.2007 **Написал:** zombiexe

1. Craft покинул команду ...
2. Релиз MySQL Bruter - Скачать
3. Идет набор в команду (желающим вступить - связаться со мной по icq 408304)

Обновление FTP-informer

Дата: 18.01.2007 **Написал:** Craft

Обновился FTP-informer, а точнее обновилась самая важная фича - это просмотр ТИЦ и PR сайта, качайте: FTP-informer v 1.1

Новогодние релизы

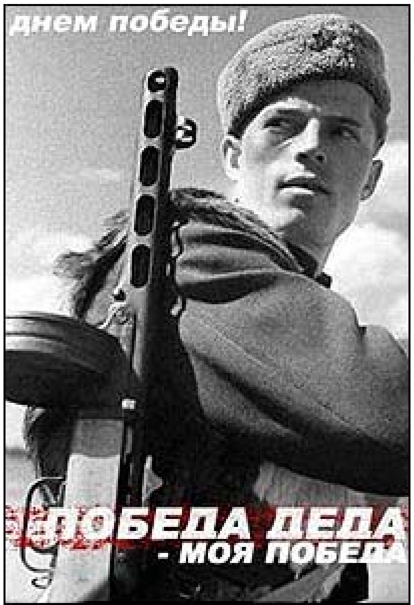
Дата: 06.01.2007 **Написал:** Zyklon Team

FTP-informer от Craft'a - чекает ТИЦ и pR сайта ,
работает со списком , фидбек для покупки/продажи
Скачать : FTP-informer v 1.0

Web-Shells checker - чекаем на живучесть web-шеллы, также работает с инклуд шеллами, работа со списком, написан на PHP
Скачать : Web-Shells checker

2.2 Defaced websites

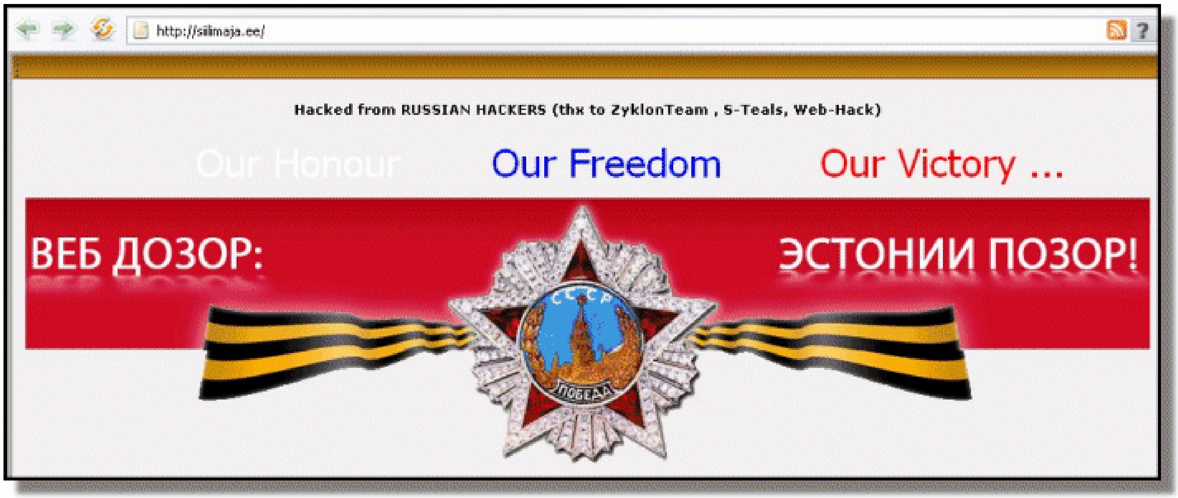
More www sites were defaced. The first WWW target to be hit was apparently that of the Foreign Minister Urmas Paet's free market liberal Reform Party, the home page of which was given a makeover by the intruding crackers. The pages were nevertheless restored in short order.



Among the targets have been all the Estonian ministries, with the exception of Culture and Agriculture.

Some Estonian website was defaced to show a Soviet soldier.

The front page of the website of a Tallinn housing company, Siilimaja, after treatment by Russian crackers (http://siilimaja.ee)[7]:



Hacked from RUSSIAN HACKERS (thx to ZyklonTeam , S-Teals, Web-Hack)

Our Honour Our Freedom Our Victory ...

ВЕБ ДОЗОР: ЭСТОНИИ ПОЗОР!

3. The trigger cause of attack

A Soviet war monument was removed from the centre of the capital, Tallinn, to a military cemetery. The move sparked rioting and looting by several thousand protesters from Estonia's large population of ethnic Russians, who tend to see the statue as a cherished memorial to wartime sacrifice. Estonians mostly see it rather as a symbol of a hated foreign occupation.[8]

They say the attack is originating in Russia, which is angry over Estonia's recent relocation of a Soviet war memorial. Russian officials deny any government involvement.

4. Countermeasures

4.1 Official countermeasures

Estonia blocked all .ru domains, but a botnet attack was launched. When bots were turned loose on Estonia, roughly 1 million unwitting computers worldwide were employed. Officials said they traced bots to countries as dissimilar as the

[7] http://www.hs.fi/english/article/Virtual+harassment+but+for+real+/1135227099868
[8] Citation from: http://www.economist.com/world/europe/displaystory.cfm?story_id=9163598

United States, China, Vietnam, Egypt and Peru, the Post says.[9] Estonia asked help from Terena, Nato etc.

Terena[10] Community News[11]

„TF-CSIRT[12] to Estonia's Rescue

A prolonged and large-scale denial of service attack on Estonia's websites continues to be fended off thanks to the support of Computer Security Incident Response Teams (CSIRTs) based in various countries. The attacks have been perpetrated as part of wider civil unrest after Estonia relocated a statue of a Soviet Russian soldier at the end of April.

The CSIRTs have been helping to defend Estonia's public and government websites since Thursday, 3 May, when Hillar Aarelaid of the Estonian incident response team CERT-EE joined the delegates at the TERENA Task Force meeting TF-CSIRT in Prague.

Mr Aarelaid made an impassioned plea to the gathered security experts after explaining that the attacks were crippling his country's Internet activities. ***In response, the Task Force chairman, Gorazd Božič of ARNES (Slovenia), sent out a request for assistance to TI Accredited Teams and FIRST Teams, and within 24 hours the situation was immensely improved.***

However, during a telephone conversation with TERENA staff on Thursday this week, Mr Aarelaid said that since Tuesday May 8th the attacks had escalated again, with a wider range of websites and services now coming under increasing fire.

"If you have lost government sites, newspaper sites, bank sites and so on, it's quite awful," he said.

Sounding remarkably cheerful despite the situation, Mr Aarelaid expressed enthusiastic thanks to TERENA and to his CSIRT colleagues around the world. "They''re all still helping," he explained. "I really appreciate every single team that has been working with us". "

Estonia appealed to NATO and European Union to help defend against cyber attack

Estonia has urged its allies in the European Union and NATO to take firm action against a new mode of warfare that has been unleashed on the Baltic state in a bitter row with Russia over a Soviet war memorial: cyber-attacks.

[9] http://government.zdnet.com/?p=3161

[10] Trans-European Research and Education Networking Association

[11] http://www.terena.org/news/fullstory.php?news_id=2103

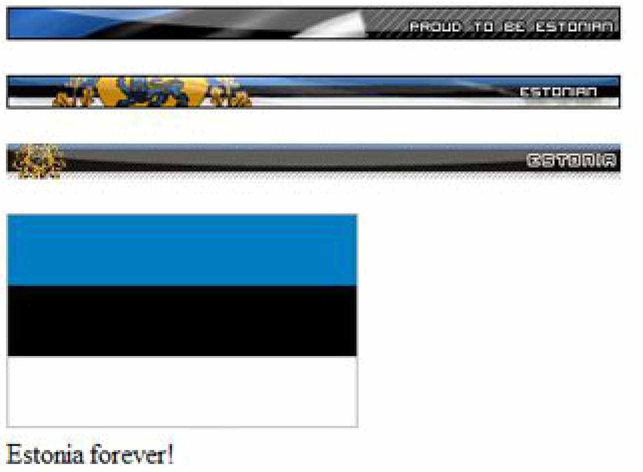
[12] Task Force of Computer Security Incident Response Teams

"Taking into account what has been going on in Estonian cyber-space, both the EU and NATO clearly need to take a much stronger approach and cooperate closely to develop practical ways of combatting cyber-attacks," Estonian Defence Minister Jaak Aaviksoo told AFP Tuesday.[13]

Two of NATO's top specialists in internet warfare, plus an American colleague, have hurried to Tallinn to observe the onslaught. But international law is of little help, complains Rein Lang, Estonia's justice minister.[14]

4.2 Non-official actions:

In reply Estonian hackers also defaced Russian websites[15] (i.e. http://www.web-dozor.ru, http://www.1-net.ru) with labels :”Proud to be Estonian!” and “Estonia forever!”.



[13] http://www.smh.com.au/news/Technology/Estonia-urges-firm-EU-NATO-response-to-new-form-of-warfarecyberattacks/2007/05/16/1178995207414.html
[14] http://www.economist.com/world/europe/displaystory.cfm?story_id=9163598
[15] http://clipmarks.com/clipmark/D6D732A0-6849-47B8-99D5-B31917174CF8/