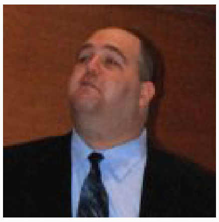
Perimeter

3/17/2009
05:18 PM



Gadi Evron
Commentary

Connect Directly

0 comments
Comment Now

Login

👍 50%

👎 50%

Share0

Authoritatively, Who Was Behind The Estonian Attacks?

In the past couple of weeks the press has been humoring a couple of rumors about who was behind the 2007 cyberattacks against Estonia [PDF]. During these attacks, Estonia's infrastructure, which relies heavily on the Internet, nearly collapsed.

In the past couple of weeks the press has been humoring a couple of rumors about who was behind the 2007 cyberattacks against Estonia [PDF]. During these attacks, Estonia's infrastructure, which relies heavily on the Internet, nearly collapsed.This is not the first time such baseless attributions were made.

I was in Estonia when the attacks occurred. I wrote the post-mortem analysis and recommendations for the Estonian CERT, and I am going to authoritatively show you why these claims are baseless. I will list these accusations and responsibility claims, and show you why they should be ridiculed.

Background In April 2007, a large-scale Internet attack was launched against Estonia in what can best be described as a politically motivated cyber-riot. Estonian society is online to an extent unimaginable in other countries; banking and voting are Internet-based, making the country reliant on the Internet. As such, any attack is a frightening proposition, the potential impact being Estonian citizens unable to buy basic groceries or gasoline.

The question of who was behind the attack has been reverberating for two years, with many fingers pointed at the Kremlin.

Here's what happened. On the eve of April 26, 2007, the online Russian-speaking population was excited: Multiple posts appeared all over the Russian blogosphere with simple instructions anyone could follow "to get back at Estonia" for moving the Russian World War II memorial of the unknown soldier from the center of the Estonian capital Tallinn to its outskirts.

Russian-speaking netizens felt empowered, and an online mob formed. The easy-to-use instructions were significant. Attacking Estonia became a fast-spreading meme or epidemic -- encouraging participation by the masses. That included hackers using advanced tools such as botnets.

While the technologies used are of little consequence to this text, they were relatively sophisticated: Botnets changed tactics, an advanced new virus was deployed, and specific network routers were targeted for attack. More important were the periodic updates in the Russian-language blogosphere directly responding to the Estonian defenders, as well as a near-simulteanous riot in the streets of Tallinn.

Whether this organization was an ad-hoc loose coupling of individuals or a planned assault, we cannot tell. We can pinpoint attackers, but not who manipulated the blogosphere -- the Heinleinian puppet masters.

The size of the attack is also of little consequence; its impact is. The Estonians, being quick to mobilize, mounted a successful defensive response, which is why they are still online in cyberspace.

Let's put all of these recent and ridiculous attributions of blame (or responsibility if you like) in order, skipping the original accusation against

Russia.

Who was blamed so far? Last week Sergei Markov, a State Duma Deputy from the pro-Kremlin Unified Russia made what I assume to be a joke: "About the cyberattack on Estonia...don't worry, that attack was carried out by my assistant. I won't tell you his name, because then he might not be able to get visas."

This was taken very seriously around the world, which was worrisome by itself. What people fail to realize is this is what Russian humor looks like. Pretty funny, too. It did get Markov some fame, though. Good for him!

This admission is especially interesting, even if I still take it as a joke, because this week Nashi (the Kremlin-backed Putin Youth movement) member Konstantin Goloskov took credit for launching attacks, mentioning it was done on the group's own initiative.

This story was also carried in an Estonian publication (Google translation here).

But, wait. Back in 2007 the same Konstantin Goloskov stated openly, that he took part in attacking Estonia, apparently as another pawn with the rest of the online mob, which did so from the comfort of their homes. Another knob in the machine:

> Konstantin Goloskov, a Nashi activist, told the Rosbalt news agency on May 2 that he personally took part in cyber-attacks on Estonian websites. But he denied that Moscow state offices were used. The hacking, he said, was done from the breakaway Moldovan region of Transdniester.

Another story shows they had taken responsibility for participating back in 2007 (translated from Estonian by Google).

My assumption here was that he changed his story, but a friend of mine, Dr. Dorothy Denning, enlightened me. He may not have. The word "launch" can have different meanings, and it's possible that what I take as "initiate" means just to "participate as well." Whether he claimed to be yet another attacker or the organizer matters little. But if we are to suspend disbelief for a moment, and say he did -- he certainly did not control them.

A theory from January 2008 was that an Estonian student masterminded it, which isn't factual to say the least, given the large amount of coordinated effort behind the attacks.

The Estonian student used a botnet (an army of compromised computers controlled by hackers) to attack computers inside Estonia. He wasn't the only Estonian to do so -- every country has extremists -- but he was caught and convicted. The headlines reviving the Estonian story with these claims were misinformed at best.

This story became a legend because of a misleading story headline stating that he was behind the attacks, all by himself. Here is Slashdot carrying the headline "DoS Attacks on Estonia Were Launched by Student." Until this day a large part of the industry is convinced a student was behind the attacks just because of the headline, because Slashdot carried it, and because the latter was followed by Bruce Schneier, who still claims that was the case to this day.

There was another student arrested for the same crime of participating in the attack, but we can skip that story as he was never blamed for "launching the attacks."

A year ago a Russian general was quoted in a Russian newspaper as saying "Russia did it." He was a war college professor, so I am unsure as to how reliable his comments were, and I took that statement in stride as well. I believe that news article was pulled shortly after, but language issues may have stopped me from finding it after it disappeared.

In Perspective Living in Israel I have seen many groups take "responsibility" for terrorist bombings at the same time, or none at all. Unless they can be somehow identified by unrelated evidence, such as forensics or intelligence, things are never clear.

What I can say is that the Estonian attacks, while simple in nature, were immense in scale. The mob that mobilized was beyond any one group's control.

While it is certainly possible that the Nashi members initiated and/or participated in these attacks, we simply can't know for sure. But that is the same as saying the tooth fairy exists just because we have no evidence that it doesn't. A common logical fallacy.

I look at this new declaration as interesting, but not much beyond that.

On a final note, you may want to check this old Russian language news story to see another, although quite different, declaration from Russian officials about the attacks, claiming the Web sites were simply not well-maintained. (Here is a Google translation from Russian.)

What We Can Say For Sure We know and have evidence to show (see PDF article linked above) that the attacks were organized; whether it was in an ad-hoc fashion of people getting together or as a planned assault, we can't tell.

We can show how Estonia was almost cyber-bombed back to the stone age.

We can't, and probably never will be able to, tell who was behind the attacks based on the technical information in our possession. Any future claim will be suspect and treated skeptically unless new, unbelievable evidence (more unbelievable than the claim) becomes available.

As you can see, theories abound. Who was actually behind the attacks is simply not that interesting. The attacks themselves were fascinating, but after two years, perhaps it is time to move on.

If I am to joke, my personal and completely unfounded conspiracy theory is that the KGB (which doesn't exist under that name anymore) was behind the attacks. I am going to stick to my unfounded opinion. What's yours?

Follow Gadi Evron on Twitter: http://twitter.com/gadievron

Gadi Evron is an independent security strategist based in Israel. Special to Dark Reading. Gadi is CEO and founder of Cymmetria, a cyber deception startup and chairman of the Israeli CERT. Previously, he was vice president of cybersecurity strategy for Kaspersky Lab and led PwC's Cyber Security Center of Excellence, located in Israel. He is widely recognized for ... View Full Bio

Comment |

Email This |

Print |

RSS

More Insights

Webcasts

DarkReading Virtual Event: Re-Thinking IT Security Strategy

Wi-Fi & Bluetooth Low Energy (BLE) are Changing the Wireless World

More Webcasts

White Papers

Darktrace Discoveries: Global Threat Case Studies 2016

You Will Be Breached

Disrupting The Attack Lifecycle

[Case Study] Scarlet Mimic Attacks

[2016 Cyberthreat] Defense Report

More White Papers

Video

Preparing For Government Data Requests ...

0 Comments

Partners In The Battle Against Cyberthreats

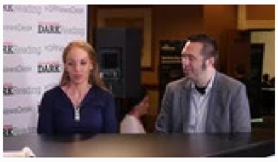
0 Comments

Cybercriminals' Superior Business Savvy ...

0 Comments

Improving Security Savvy Of Execs And ...

0 Comments



An Open-Source Security Maturity Model

0 Comments

D-FENSE! Using Research To Craft ...

3 Comments

How Windows 10 Stops Script-Based Attacks ...

0 Comments

How You Can Support InfoSec Diversity, St...

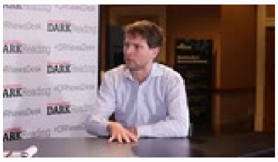
2 Comments

Rise Of Machine Learning: Advancing ...

0 Comments

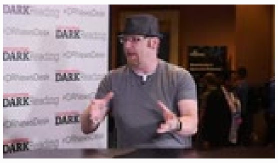
The Future Of AI-Based Cybersecurity: ...

0 Comments



Stop Blaming Users. Make Security ...

1 Comments



Making The Dark Web Less Scary

0 Comments

All Videos

Cartoon

BLOCK ALL TWEETS.
Cybersecurity in a Trump Administration
Klossner

Latest Comment: Security solution to restrict database access from hackers: No network, no database, no problem!

Cartoon Archive

Current Issue

UBM

InformationWeek Tech Digest

Five Emerging Security Threats — And What You Can Learn From Them

At Black Hat USA, researchers unveiled some nasty vulnerabilities. Is your organization ready? >>

By Ericka Chickowski

Also Inside:

Powered by DARKReading

Five Emerging Security Threats - And What You Can Learn From Them

At Black Hat USA, researchers unveiled some nasty vulnerabilities. Is your organization ready?

Download This Issue!

Back Issues | Must Reads

Flash Poll

What's missing from your incident response plan? (Pick all that apply.)

- □ Access to activity logs
- □ An up-to-date network diagram
- □ Blueprint for public disclosure
- □ Hostname-IP address maps
- □ IR fire drills before the event
- □ Plan for finding malicious files after the breach
- □ We don't have an incident response plan
- □ Other (Please explain in the comments)

Submit

All Polls

Reports

Infographics

InformationWeek DARKReading :: reports
reports.informationweek.com
October 2016

The Top Cybersecurity Risks – And How Enterprises Are Responding

Security departments are juggling threats to mobile users, cloud environments, porous endpoints, and more, creating a risk-management challenge.

Sponsored by ARCTIC WOLF

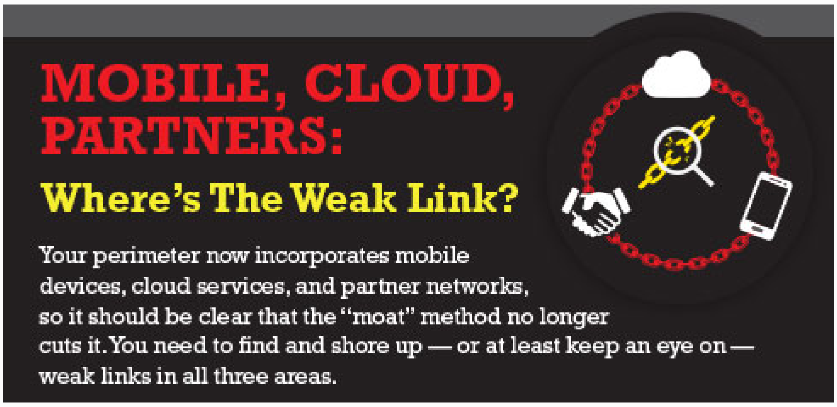
The Top Cybersecurity Risks And How Enterprises Are Responding

The information security landscape is a constantly shifting risk environment. Today's IT security department must manage both internal and external threats' ranging from malware to mobile device vulnerabilities, to cloud security and ransomware. Download the Dark Reading 2016 Strategic Security

Survey to gain insight into how security professionals view these risks, and how they are addressing them.

Download Now!

More Reports



MOBILE, CLOUD, PARTNERS:

Where's The Weak Link?

Your perimeter now incorporates mobile devices, cloud services, and partner networks, so it should be clear that the "moat" method no longer cuts it. You need to find and shore up — or at least keep an eye on — weak links in all three areas.

Mobile, Cloud, Partners: Where's The Weak Link?

Your perimeter now incorporates mobile devices, cloud services, and partner networks, so it should be clear that the "moat" method no longer cuts it.

1 comments | Read | Post a Comment

More Infographics

Slideshows

7 Reasons Consumers Don't Take Action on Cybersecurity

0 comments | Read | Post a Comment

5 Signs Your Smartphone Has Been Hacked

1

7 Scary Ransomware Families

13

More Slideshows

Twitter Feed

Bug Report

Enterprise Vulnerabilities
From DHS/US-CERT's National Vulnerability Database

CVE-2013-7445
Published: 2015-10-15
The Direct Rendering Manager (DRM) subsystem in the Linux kernel through 4.x mishandles requests for Graphics Execution Manager (GEM) objects, which allows context-dependent attackers to cause a denial of service (memory consumption) via an application that processes graphics data, as demonstrated b...

CVE-2015-4948
Published: 2015-10-15
netstat in IBM AIX 5.3, 6.1, and 7.1 and VIOS 2.2.x, when a fibre channel adapter is used, allows local users to gain privileges via unspecified vectors.

CVE-2015-5660
Published: 2015-10-15
Cross-site request forgery (CSRF) vulnerability in eXtplorer before 2.1.8 allows remote attackers to hijack the authentication of arbitrary users for requests that execute PHP code.

CVE-2015-6003
Published: 2015-10-15
Directory traversal vulnerability in QNAP QTS before 4.1.4 build 0910 and 4.2.x before 4.2.0 RC2 build 0910, when AFP is enabled, allows remote attackers to read or write to arbitrary files by leveraging access to an OS X (1) user or (2) guest account.

CVE-2015-6333
Published: 2015-10-15
Cisco Application Policy Infrastructure Controller (APIC) 1.1j allows local users to gain privileges via vectors involving addition of an SSH key, aka Bug ID

CSCuw46076.

Dark Reading Radio

Archived Dark Reading Radio

The Cyber Skills Shortage

According to industry estimates, about a million new IT security jobs will be created in the next two years – but there aren't enough skilled professionals to fill them. On top of that, there isn't necessarily a clear path to a career in security. Dark Reading Executive Editor Kelly Jackson Higgins hosts guests Carson Sweet, co-founder and CTO of CloudPassage, which published a shocking study of the security gap in top US undergrad computer science programs, and Rodney Petersen, head of NIST's new National Initiative for Cybersecurity Education.

UPCOMING!
Wednesday, November 16, 1pm EST
Bug Bounties and the Zero-Day Trade

UPCOMING!
Wednesday, December 14, 1pm EST
The Coolest Hacks of 2016

FULL SCHEDULE | ARCHIVED SHOWS

About Us
Contact Us
Customer Support
Sitemap
Reprints

Twitter
Facebook
LinkedIn
Google+
RSS

Login

X

Change Password

X

Password Reset

X