NSA targets the privacy-conscious

von J. Appelbaum, A. Gibson, J. Goetz, V. Kabisch, L. Kampf, L. Ryge

The investigation discloses the following:

- Two servers in Germany - in Berlin and Nuremberg - are under surveillance by the NSA.

- Merely searching the web for the privacy-enhancing software tools outlined in the XKeyscore rules causes the NSA to mark and track the IP address of the person doing the search. Not only are German privacy software users tracked, but the source code shows that privacy software users worldwide are tracked by the NSA.

- Among the NSA's targets is the Tor network funded primarily by the US government to aid democracy advocates in authoritarian states.

- The XKeyscore rules reveal that the NSA tracks all connections to a server that hosts part of an anonymous email service at the MIT Computer Science and Artificial Intelligence Laboratory (CSAIL) in Cambridge, Massachusetts. It also records details about visits to a popular internet journal for Linux operating system users called "the Linux Journal - the Original Magazine of the Linux Community", and calls it an "extremist forum".

DOWNLOADS

XKeyscore rules

Read/download the XKeyscore rules here | download
Infosec & counter-surveillance
writing what powerful people don't want written means you have something to hide
My First Cavity Search

Helping your child understand why he may pose a threat to National Security

Ages 6 and up
THE MIDDLE EAST

SECY GATES MEETING WITH ISRAEL'S MINISTER OF DEFENSE EHUD BARAK
Snowden seeks asylum in Russia but must end leaks

WHISTLEBLOWER Edward Snowden has applied for asylum in Russia and 14 other countries, reports suggested yesterday. His representative, Briton Sarah Harrison, is said to have handed his application to the foreign ministry in Russia, where the former National Security Agency contractor has been holed up since June 23.

Russian president Vladimir Putin yesterday said he was willing to consider Mr Snowden’s request, adding: ‘If he wants to remain here, there is one condition – he should stop his work aimed at inflicting damage on our American partners.’

Meanwhile, French president Francois Hollande has called on the US to come clean about claims it has spied on EU diplomats. ‘We cannot accept this kind of behaviour from partners and allies,’ he said, adding talks on a free trade deal should be put on hold until president Barack Obama ‘guarantees’ the practice was stopped.

‘I guarantee you that, in European capitals, there are people who are interested in, if not what I had for breakfast, at least what my talking points might be should I end up meeting with their leaders. That’s how intelligence services operate,’ he said.

Snowden praises Ecuador for defying ‘threats’ of US

SPYING whistleblower Edward Snowden has written to the president of Ecuador praising his country’s ‘bravery’ in considering his request for political asylum, it was revealed last night.

The fugitive, thought to be hiding in Russia, said the country had stood up to the US when other nations were afraid of the global superpower’s ‘threats’.

He accuses the government of a ‘grave violation’ of human rights and of ‘unwar-

by HAYDEN SMITH

anted spying against innocent people’. ‘The government of the United States has built the world’s largest system of surveillance,’ says the letter, leaked by government sources in Ecuador’s capital Quito.

‘This global system affects every human life touched by technology; recording, analysing, and passing secret judgment over each member of the public.’ Mr Snowden, who is said to have applied for asylum in Russia, Ecuador and 13 other countries, hints he is fearing for his life in the letter.

‘No matter how many more days my life contains, I remain dedicated to the fight for justice in this unequal world,’ he says.

Russian president Vladimir Putin said he would consider giving Mr Snowden asylum if he stops revealing secrets. ‘If he wants to remain here, he should stop his work aimed at damaging our American partners.’
Mein Vater sagt, Sie können in meinen Computer gucken

Das ist nicht dein Vater
Have you been using:

e-mail
video or voice chat
videos
photos
stored data
VoIP calls
file transfers
video conferencing

...from any of...

Microsoft / Hotmail, since Sep 11, 2007
Google, since Jan 14, 2009
Yahoo, since Mar 12, 2008
Facebook, since June 3, 2009
PalTalk, since Dec 7, 2009
YouTube, since Sep 24, 2010
Skype, since Feb 6, 2011
AOL, since Mar 31, 2011
Apple, since Oct 2012

than you are in the NSA database
Isn't it great? We have to pay nothing for the barn.

Yeah! And even the food is free.

Facebook and You

If you're not paying for it, you're not the customer. You're the product being sold.
Spooks at the US National Security Agency (NSA) can't believe we're all paying for the equipment it's using to spy on us, describing Steve Jobs as Big Brother and iPhone buyers as "zombies".

That assertion comes from NSA documents leaked to Germany's Spiegel Online.

The self-promoting presentation, purportedly an internal NSA report from 2010 titled "Exploring Current Trends, Targets and Techniques", includes a number of slides presenting snapshots of grinning iPhone-brandishing customers as analogous to the "zombies" brainwashed by Big Brother – in a reference to George Orwell's Nineteen Eighty-Four.
Revealed: how Microsoft handed the NSA access to encrypted messages

- Secret files show scale of Silicon Valley co-operation on Prism
- Outlook.com encryption unlocked even before official launch
- Skype worked to enable Prism collection of video calls
- Company says it is legally compelled to comply

Glenn Greenwald, Ewen MacAskill, Laura Poitras, Spencer Ackerman and Dominic Rushe
The Guardian, Thursday 11 July 2013 18.53 BST
Jump to comments (1971)
NSA Strategic Partnerships

Alliances with over 80 Major Global Corporations
Supporting both Missions

- Telecommunications & Network Service Providers
- Network Infrastructure
- Hardware Platforms
  Desktops/Servers
- Operating Systems
- Applications Software
- Security Hardware & Software
- System Integrators

EDS
AT&T
Qwest
H-P
Motorola
Cisco
Qualcomm
IBM
Oracle
Intel
Microsoft
Verizon
Tailored Access Operations

- TAO
- SSG
- TAO / R&T

Overall Classification: TOP SECRET//COMINT//REL to USA,FVEY
COTTONMOUTH-I

ANT Product Data

(TS//SI//REL) COTTONMOUTH-I (CM-I) is a Universal Serial Bus (USB) hardware implant which will provide a wireless bridge into a target network as well as the ability to load exploit software onto target PCs.

(TS//SI//REL) CM-I will provide air-gap bridging, software persistence capability, "in-field" re-programmability, and covert communications with a host software implant over the USB. The RF link will enable command and data infiltration and exfiltration. CM-I will also communicate with Data Network Technologies (DNT) software (STRAITBIZARRE) through a covert channel implemented on the USB, using this communication channel to pass commands and data between hardware and software implants. CM-I will be a GENIE-compliant implant based on CHIMNEYPOOL.

(TS//SI//REL) CM-I conceals digital components (TRINITY), USB 1.1 FS hub, switches, and HOWLERMONKEY (HM) RF Transceiver within the USB Series-A cable connector. MOCCASIN is the version permanently connected to a USB keyboard. Another version can be made with an unmodified USB connector at the other end. CM-I has the ability to communicate to other CM devices over the RF link using an over-the-air protocol called SPECULATION.
TIN FOIL
FREE YOUR MIND
Government policy today

- EU & Euro nations have known about Echelon since 2000
- Euro nations have known about effective counter-measures since at least July 2001
- Despite formal repeated requests from parliaments none of these measures have been implemented
- Government is, at best, completely incompetent, at worst your enemy
Now what?
KEEP CALM AND FIGHT BACK
I always sign someone else’s name.

Before hitting ‘send,’ I will myself invisible.

I don’t move my lips while typing.

Personal Encryption Tips
NSA budget: $78 billion
(about $0.10 per westerner per day)

Increase the cost of monitoring you from $0.10 per day to $100,000+ per day
Infosec policies

- **C**onfidentiality, who can access the data?
- **I**ntegrity, is the data unaltered?
- **A**vailability, is the data available?

- Do the rules apply to everyone the same way?
'security'

confidentiality, integrity & availability

behaviour

technology
hardware

BIOS

hardware

operating system
(Windows, MacOSX, Linux)

middleware
(database, crypto)

applications
(email, browser, office)

interface
(screen, keyboard, mouse)
We hold these truths to be self-evident, that all Users are created equal, that they are endowed by Hackers with certain unalienable Rights, that among these are Life, Liberty and the pursuit of Culture.
That to secure these rights, Software is distributed among Users, deriving its powers from their consent.
That whenever any Form of Software becomes destructive of these ends, it is the right of the Users to alter or to abolish it, and to institute new Software, laying its foundation on such Principles and organizing its Powers in such form, as to them shall seem most likely to effect their Safety and Happiness.
What is sourcecode?

- programming language versus machine language

```c
int main () {
    printf ("Hello World!\n");
}
```

Hello World!

compiler
Ubuntu is a fast, secure and easy-to-use operating system used by millions of people around the world.

Get Ubuntu

11.04 is here!

It works with your favourite apps:

http://www.ubuntu.com/download
use different browsers!
How Tor Works: 2

Step 2: Alice’s Tor client picks a random path to the destination server. Green links are encrypted, red links are in the clear.
I changed all my passwords to "incorrect".

So whenever I forget, it will tell me "Your password is incorrect."
WHICH CHARACTERS ARE REQUIRED IN MY PASSWORD?

Hint: it depends on password length!

- **8-11**: requires mixed case letters, numbers, and symbols
- **12-15**: requires mixed case letters and numbers
- **16-19**: requires mixed case letters
- **20+**: any characters you like!
Bob

Hello Alice!

Encrypt

6EB69570 08E03CE4

Alice's public key

Alice

Decrypt

Hello Alice!

Decrypt

Alice's private key
-----BEGIN PGP MESSAGE-----
Charset: windows-1252
Version: GnuPG v1.4.11 (GNU/Linux)
Comment: Using GnuPG with Mozilla - http://enigmail.mozdev.org/

hQEMA6fb6wuWWmMeAQf+PRn9+qteYbdTwFou/hmL4SRLEOTCw4CM7hxddMlv1j7u
rJVlKp9Cd8UrNpcPnGLS0w6/0eJA7rI0r8hWMVJxEFAHu/JMYV0kAFdWhzjuuIY/jP
OIEj+wxpHF9M8VT0drA0Vir60gEW5Q2pGxg8nag9phhGsQljZm7SxywtHJmkP20px
59HGUn9unSYF0sR0qeWfLYkqdT0/ZmITXr4K8GBRmsZxMqebiwNzhFGrxzQG32SB
ZTKvPGrfxv0MtQJAqUYWKqwWGf17pDNAhXKF18IssJbLswIc9zxSeohjHph8nPmI
2TNjxkJr5VAQAks4AvfE6350pQsBuWQH4GQaLZYUEdG0G6SoX59QZsBAQANlq
HjNwB706kR0CzGRVEC29UF05P6+Ib0w+wATbru/Zr6zNzSfYTltpZm7fP/v7wXgO
sCQ02UUtWXy3oLSIQRxLqwwYotX0jDoDS5Mc5Cxp6sSkT3UxFGCWylgmxv7I2fW
ZRJa4is+UEFZd0G8sg/MffqmPtXnIIB/aqu0yYn3pYhvmFxgDGwjXIXz7vYCEmR
ADwTPUb3rLyLNpYztdr5+vcw1lj0Bx7uQhFhtDcF+NRIB8Vs1ICKxirB6Bs1xcB
BJHHuQ1qBymfzYNbPjHKKBySM3lzR8rppJ5DoKoitZD8rYLan9ewcAjFJDCFaHTrd
DtEyMNvzGpknVKMtjIf8zRcg3NOmWJtTXVparoDDsmDXIGt6hpI17dq3Ao/2gZpKxq
MksXmmEV+87P7AlILYvpujCFaw1co4U05G+UwE3zeuyytLMkkXYOlTslsOCh+jbV

-----END PGP MESSAGE-----
This document explains the need for secure communication beyond the status quo in the world somehow and...

OpenPGP Security Info

Decrypted message
Good signature from Arjen Kamphuis <arjen@gendo.ch>
Key ID: 0x118A0EC2 / Signed on: 09/08/2013 10:21 PM
Key fingerprint: 55FB B3B7 949D ABF5 F31B BA1D 237D 4C50 118A 0EC2
What is protected?

- Protects the content & integrity of your communications
- Protects your (IP) location and (sometimes) identity
- Protects the content of your communications
Welcome to Tails

Administration password

Enter an administration password in case you need to perform administration tasks. Otherwise it will be disabled for better security.

Password: **************
Verify Password: **************

Windows Camouflage

This option makes Tails look more like Microsoft Windows XP. This may be useful in public places in order to avoid attracting suspicion.

- [ ] Activate Microsoft Windows XP Camouflage

Login