

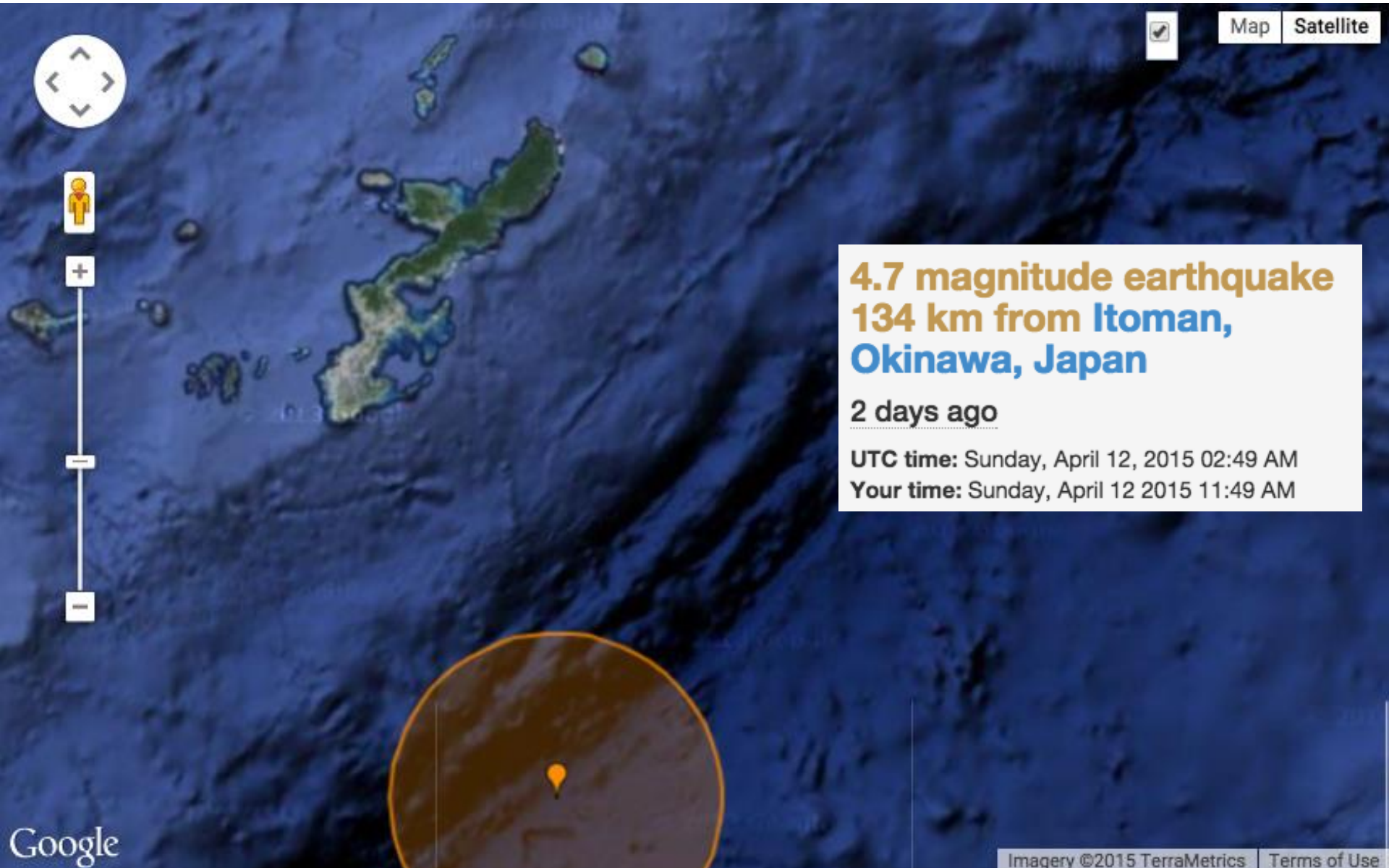
Computer Security in 2015: Where are we? What to expect? How does it affect science / HEP?

Sebastian Lopienski

CERN Deputy Computer Security Officer

CHEP 2015

Congratulations!



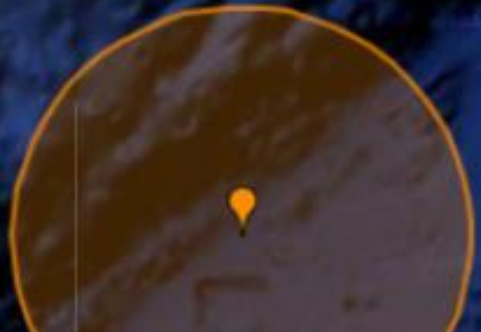
Map | Satellite



4.7 magnitude earthquake
134 km from Itoman,
Okinawa, Japan

2 days ago

UTC time: Sunday, April 12, 2015 02:49 AM
Your time: Sunday, April 12, 2015 11:49 AM



Delete any YouTube video

1. Send this:

```
POST live_events_edit_status_ajax?action_delete_event=1
Host: www.youtube.com
```

```
event_id: ANY_VIDEO_ID
session_token: YOUR_TOKEN
```

2. Receive this:

```
{
  "success": 1
}
```

3. Report to Google and get \$5'000 bounty

<http://kamil.hism.ru/posts/about-vrg-and-delete-any-youtube-video-issue.html>

Blunders happen to everyone

... but better to be ready to react fast

Security on the Internet?

https

Apple's "goto fail" SSL bug (late 2012 – Feb 2014)

```
if ((err = SSLHashSHA1.update(&hashCtx, &clientRandom)) != 0)
    goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)
    goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
    goto fail;
if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
    goto fail;

err = sslRawVerify(ctx,
                  ctx->peerPubKey,
                  dataToSign,
                  dataToSignLen,
                  signature,
                  signatureLen);

if(err) {
    sslErrorLog("SSLDecodeSignedServerKeyExchange: sslRawVerify "
               "returned %d\n", (int)err);
    goto fail;
}

fail:
SSLFreeBuffer(&signedHashes);
SSLFreeBuffer(&hashCtx);
return err;
```



`goto fail;`
`goto fail;`

Heartbleed bug (OpenSSL)





SERVER, ARE YOU STILL THERE?
IF SO, REPLY "HAT" (500 LETTERS).



a connection. Jake requested pictures of deer.
User Meg wants these 500 letters: HAT. Lucas
requests the "missed connections" page. Eve
(administrator) wants to set server's master
key to "14835038534". Isabel wants pages about
snakes but not too long". User Karen wants to
change account password to "CoHeBaSt". User



HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about "snakes but not too long". User Karen wants to change account password to "CoHeBaSt". User Isabel requests pages

a connection. Jake requested pictures of deer.
User Meg wants these 500 letters: HAT. Lucas
requests the "missed connections" page. Eve
(administrator) wants to set server's master
key to "14835038534". Isabel wants pages about
snakes but not too long". User Karen wants to
change account password to "CoHeBaSt". User



Software and protocols
we all rely on
are vulnerable

```
goto fail;  
goto fail;
```

A simple mistake...
but honest or intentional?

Software and protocols
we all rely on
are sometimes *made* or *kept* vulnerable

Code from 2004, running as *root*

```
foreach my $f (<$_[0]/*.out>) {  
    [..]  
    my $nf="$f.cut";           # files are in /tmp  
    system "  
        head -100 $f > $nf;  
        echo \"----CUT----\" >> $nf;  
        tail -100 $f >> $nf";
```

Two **root privilege escalation** vulnerabilities:

- **\$f** tainted (name of user-created file, can include shell commands)
- **\$nf** controlled by user (can be a symbolic link to system files)

Code from 2004, still running as *root*

Reported by a user:

*“I was in a usual boring meeting
and just did ps aux in lxplus :)”*

We often rely on very old code
... but who knew secure coding
back in 2004?



Source: Dick Thomas Johnson/flickr (CC BY)

DRAM *rowhammer* bug => kernel exploit

Access repeatedly a row of DRAM memory

```
code1a:  
    mov (X), %eax    // Read from address X  
    mov (Y), %ebx    // Read from address Y  
    clflush (X)      // Flush cache for address X  
    clflush (Y)      // Flush cache for address Y  
    jmp code1a
```

This can cause bit flips in neighboring rows

Proof-of-concepts: **privilege escalation exploits**

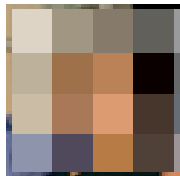
- e.g. modifying page table entries (PTEs)
- goal: gain write access to its own page table
- result: **gain read-write access to all of physical memory**

Attack techniques are highly sophisticated
... and they only get better

Prepare for your day and stay in touch.

See More

Job Changes

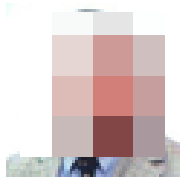


████████████████████ has a new job.

Now Senior Software Engineer at ██████████

 [Say congrats](#)

Work Anniversaries



██████████ is having a work anniversary.

1 year this April at ██████████

 [Say congrats](#)

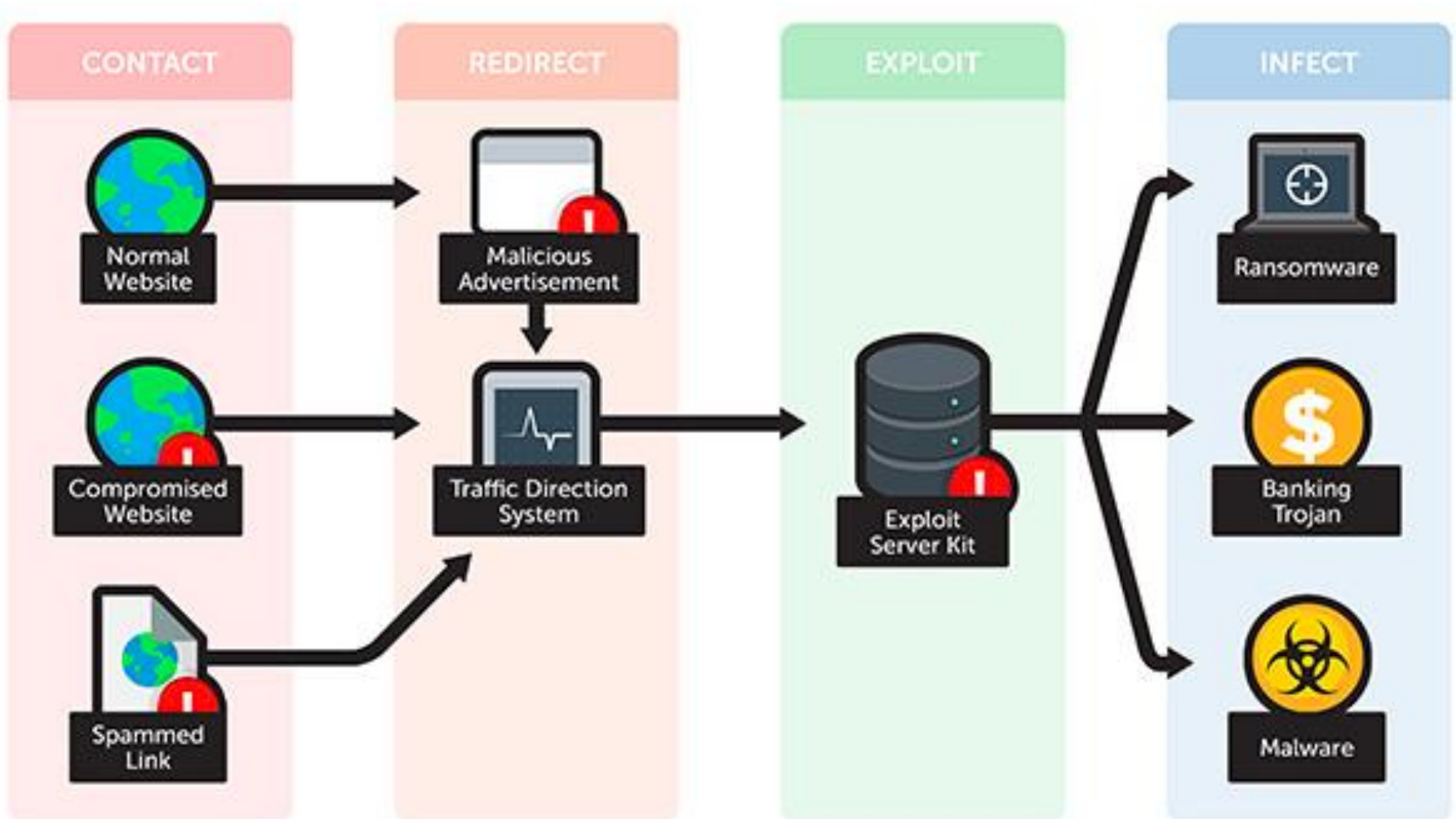


████████████████████ is having a work anniversary.

4 years this April at CERN.

 [Say congrats](#)

Exploit kit infection chain



Source: Trend Micro

Attacking is so much easier
than defending

... and cheaper, too

Your personal files are encrypted by CTB-Locker.



Your personal files are encrypted by CTB-Locker.

Your documents, photos, databases and other Important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

You only have 96 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them.

Press 'View' to view the list of files that have been encrypted.

Press 'Next' for the next page.



WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION.

View

95:58:56

Next >>

Opportunistic attacks

Criminals are just after the money,
so they usually chose the “easy targets”

PLEASE DO NOT LOG ONTO
YOUR PC EQUIPMENT OR
COMPANY WIFI UNTIL
FURTHER NOTICE



For update information contact OMD on ext. 1419



Sony Pictures Entertainment breach

Hacked By #GOP

Warning :

We've already warned you, and this is just a beginning.

We continue till our request be met.

We've obtained all your internal data including your secrets and top secrets.

If you don't obey us, we'll release data shown below to the world.

Determine what will you do till November the **24th, 11:00 PM(GMT)**.

Data Link :

<https://www.sonypicturesstockfootage.com/SPEDData.zip>

<http://dmiplaewh36.spe.sony.com/SPEDData.zip>

<http://www.ntcnt.ru/SPEDData.zip>

<http://www.thammasatpress.com/SPEDData.zip>

<http://moodle.universidadebematech.com.br/SPEDData.zip>

Targeted attacks

Much harder to protect against,
much more devastating



... but who is really behind this attack?

8 months

“Average time between intrusion and detection”




Two types of organisations:

those that know they've been hacked
and those that don't know




Source: Bruce Williams/flickr (CC BY-SA)

“We are currently experiencing *the largest DDoS attack in github.com's history* [...] *we believe the intent of this attack is to convince us to remove a specific class of content.*” Mar 27

 **GitHub Status** @githubstatus · Mar 29
The DDoS attack has evolved and we are working to mitigate

← ↻ 173 ★ 67 ...

 **GitHub Status** @githubstatus · Mar 30
After 113 hours of sustained DDoS attacks our defenses are holding. We will keep our status at yellow until the threat has subsided.

← ↻ 575 ★ 382 ...



Target: BBC and NYTimes on Github

This page has been translated from Chinese... to English Show original

This repository Search Explore Gist Blog Help SebastianLopienski

greatfire / Wiki Watch 713 Star 4,506 Fork

bbc

greatfire edited this page 20 hours ago · 1 Revision

BBC

RSS Free web version over the wall

Pages 13

The Dalai Lama's visit to Japan, "the right to pass human happiness"

The Dalai Lama's visit to Japan since 1967, the beginning of the interval and sometimes as long as 10 years, almost a year after the 1998 visit to Japan, also twice a year in some years, excluding Japan, he visits in turn, has made a special visit to Japan has been at least 19 times .

March 18, 2015: the current page image being DDOS attack. Please read the contents of the mirror or on the Github download the free Android browser over the wall to read.

Free to browse Android app

Automatic over the wall to access blocked sites.

Man-on-the-side attack



1. A web site you visit loads <http://hm.baidu.com/h.js>
(Baidu analytics)
2. Your browser requests this JavaScript file from Baidu,
but gets a response from elsewhere (!)

```
192.168.70.160 61.135.185.140 0x0002 64 <- SYN (client)
61.135.185.140 192.168.70.160 0x0012 42 <- SYN+ACK (server)
192.168.70.160 61.135.185.140 0x0010 64 <- ACK (client)
192.168.70.160 61.135.185.140 0x0018 64 <- HTTP GET (client)
61.135.185.140 192.168.70.160 0x0018 227 <- Injected packet 1 (injector)
192.168.70.160 61.135.185.140 0x0010 64
61.135.185.140 192.168.70.160 0x0018 228 <- Injected packet 2 (injector)
61.135.185.140 192.168.70.160 0x0019 229 <- Injected packet 3 (injector)
192.168.70.160 61.135.185.140 0x0010 64
192.168.70.160 61.135.185.140 0x0011 64
```

From <http://netres.ec/?b=153DB4E>

1. The injected, malicious script hammers two github projects

```
url_array = ["https://github.com/greatfire", "https://github.com/cn-nytimes"];
```

Github didn't give in... this time.

“Superhuman” espionage malware

Equation group victims map

- Finance
- Diplomatic / Embassies
- Energy / Infrastructure
- Military
- Telecommunications
- Islamic Scholars
- Other / Unknown
- Government
- Research institution
- University
- Aerospace
- Medical
- Media

High infection rate

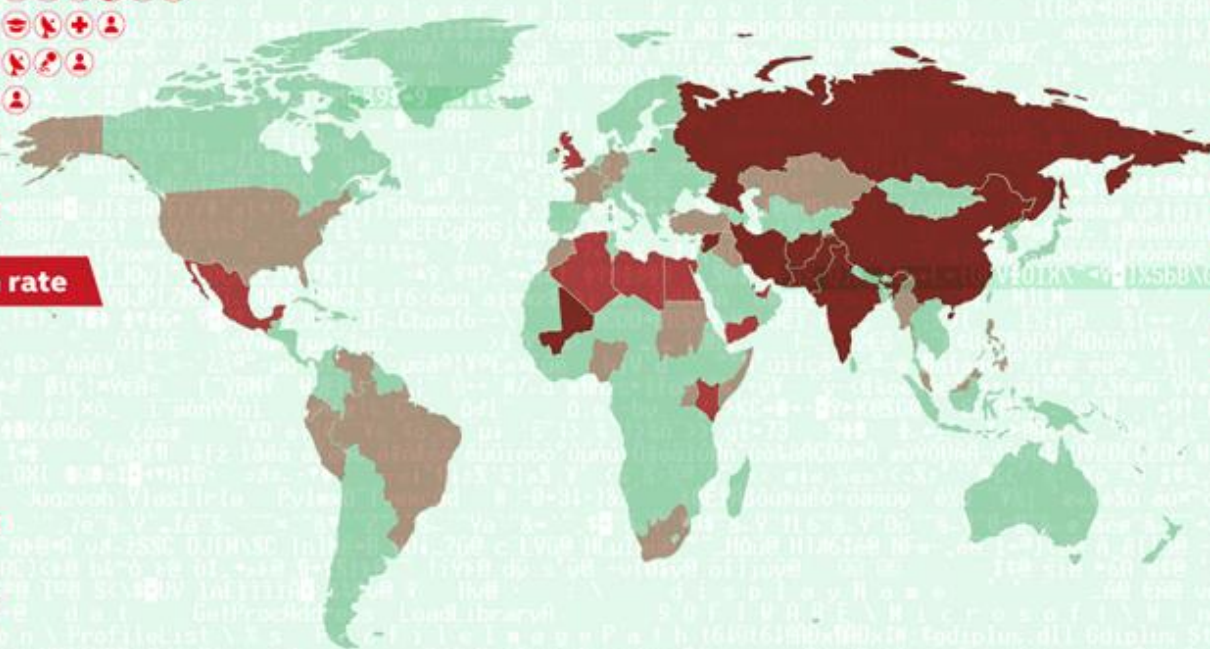
- Iran
- Russian Federation
- Pakistan
- Afghanistan
- India
- China
- Syria
- Mali

Medium-level infection rate

- Lebanon
- Yemen
- United Arab Emirates
- Algeria
- Kenya
- United Kingdom
- Libya
- Mexico
- Qatar
- Egypt

Low infection rate

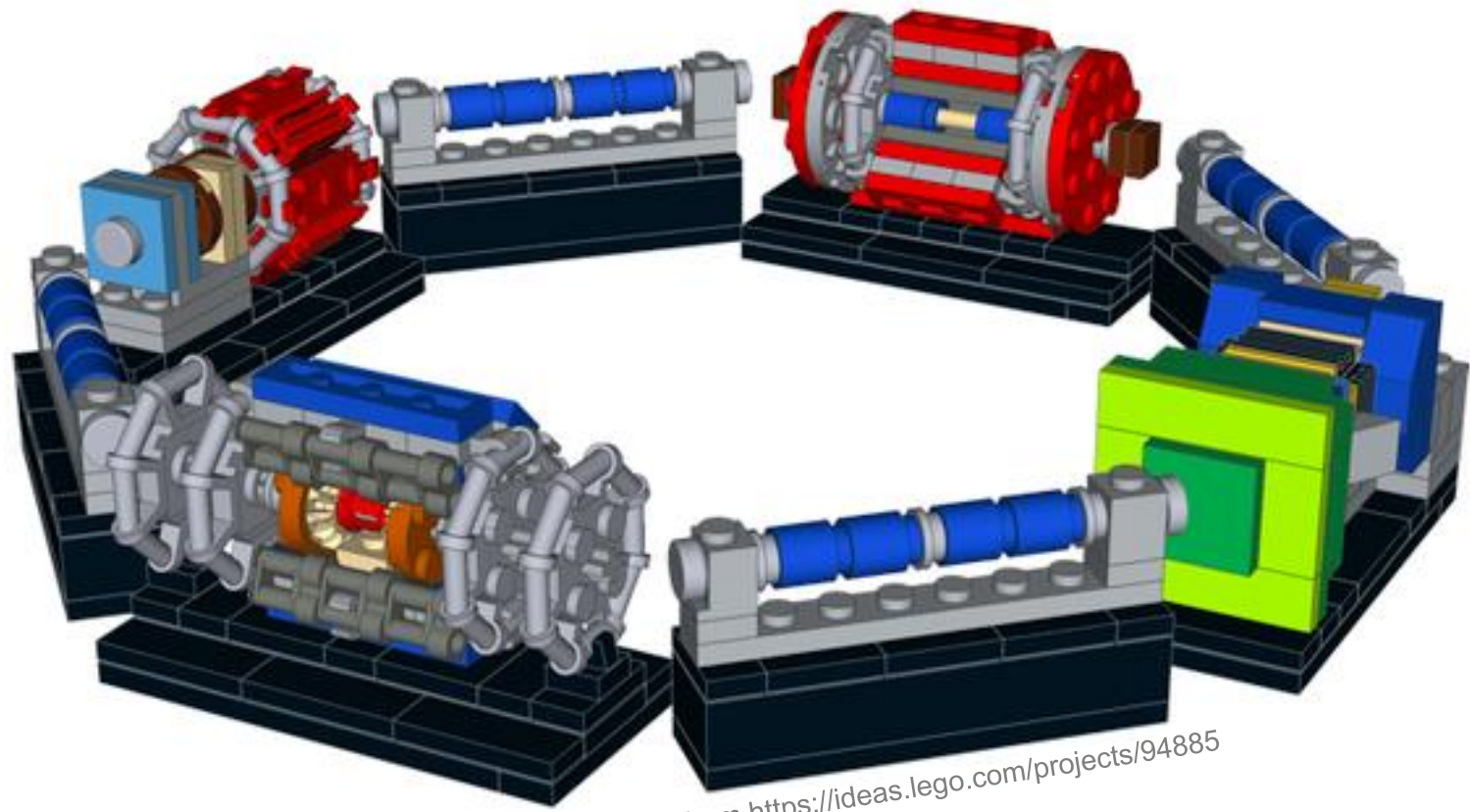
- Turkey
- Somalia
- Myanmar
- Germany
- South Africa
- Nigeria
- United States
- Venezuela
- Sudan
- Palestinian
- Morocco
- Malaysia
- Kazakhstan
- Iraq
- Brazil
- Uganda
- Switzerland
- Singapore
- Philippines
- Peru
- France
- Ecuador
- Belgium
- Bahrain



What else is out there,
that we don't know about yet?

Is it possible to repel
government-sponsored attacks?

What to do when
criminals or hacktivists of tomorrow
use the same attacks techniques
as governments of today?



How is HEP affected?



Resources, assets

Motivations



criminals

**motivation:
profit**



hacktivists

**motivation:
ideology,
revenge**



governments

**motivation:
control,
politics**

*“ OK, so can someone make money
from hacking HEP? ”*

Bitcoin mining by a rouge sysadmin

Inspired (issue 18, Feb 2015)

http://www.egi.eu/news-and-media/newsletters/Inspired_Issue_18/cryptocoin.html

*“[..] substantial amounts of mining jobs were submitted over the 2013 Christmas holidays before being discovered in early January. **The user had attempted to masquerade the mining activities as legitimate production jobs and also tried to hide his traces by planting false evidence of external attacks on the job submission machine. He failed and was caught.**”*

Computing power == money

*“ We just do fundamental research
– how can this motivate an attacker? ”*

CERN, “a fun real-world example”



Lab Mouse Security
@InfoSecMouse

+ Follow

Hacking CERN
Particles and Profit
[blog.securitymouse.com](http://blog.securitymouse.com/2014/07/hacking-cern-exploiting-python-lz4-for.html)
with @DonAndre



RETWEETS 33
FAVORITES 12

1:56 PM - 7 Jul 2014

Hacking CERN - Exploiting python-lz4 for Particles and Profit

TL;DR

Editor's Note: The TL;DR of this long technical report can be summarized as

- LZ4 was always critically vulnerable whether in Kernel or User-land
- Exploitation is easy regardless of the attack used (16MB or 2+MB)
- PoCs are written for python2.7 on 32bit ARM/x86 (scroll to the end)
- Updating is critical for all consumers of LZ4, not just python-lz4

Additional Note: The author of LZ4 claims that the PoC presented in the blog below was written against some ghostly alternative version of LZ4. For further proof of exploitation, the sample payload generated by the script at the end of this blog post will also crash python-lz4 (versions prior to r119) directly. The CERN software was simply used as a fun real-world example because their package depends on python-lz4. To test, call the Python bindings directly with:

<http://blog.securitymouse.com/2014/07/hacking-cern-exploiting-python-lz4-for.html>

LHC start-up? Death threats

#CultOfSiduri #OpDamageControl [edit] @cern 1 of 5

Send email to update those at CERN who may be in danger:

[redacted] @cern.ch

[redacted] @cern.ch

[redacted] @cern.ch

[redacted] @cern.ch

April 3rd 2015. Re: Death threats posted on dark net regarding upcoming CERN high energy experiment

Dear Dr. [redacted],

I regret to inform you that your life may be in danger for higher energy particle collision experiments.

Due to warnings by prominent theoretical physicists, some anonymous theoretical physicists with the same dire predictions, some anonymous individuals have become convinced that the only way to save our universe from destruction is to kill these 7 men, of which, unfortunately, you may be one.

SIDURI retweeted

JimRothschild @LordJimRoth · Apr 3

@mrtbenigno @AnonOpAcc

Yeah, #CERN are risking our Universe to play God. Even if the risk is small they shouldn't do it! >0% = TOO RISKY!!!

← ↻ 1 ★ 1 ... [View conversation](#)

*“ But black hole fears aside,
why would someone
specifically target HEP? ”*

CERN Internet Exchange Point



[Home](#)

[About](#) ▾

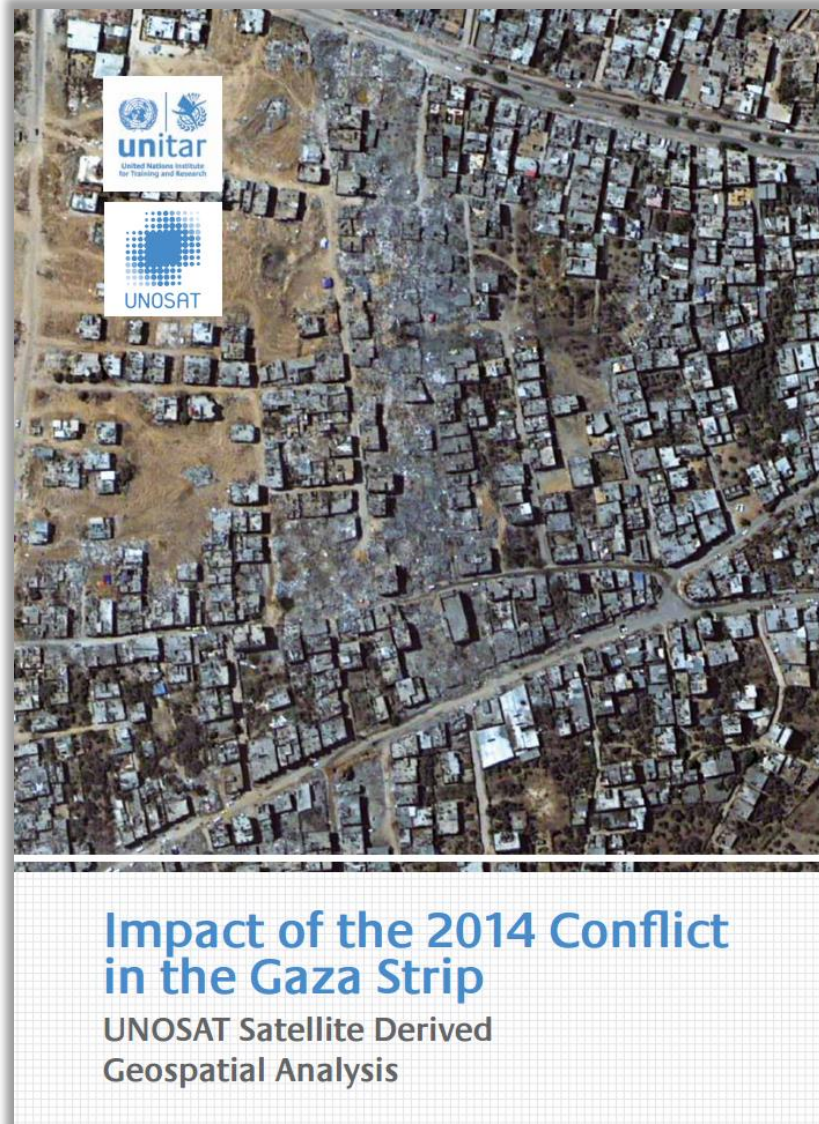
[Join](#) ▾

[Members](#) ▾

Welcome to the CERN Internet eXchange Point

The CERN Internet eXchange Point (CIXP) is a carrier-neutral exchange point based at CERN in Geneva, Switzerland.

Our partners are telecom operators and ISPs in Switzerland and France, as well as national and international research network operators. The service is provided jointly by CERN and Equinix's data-centres in Geneva and Zurich.



The URL?

https://unosat.web.cern.ch/unosat/unitar/publications/UNOSAT_GAZA_REPORT_OCT2014_WEB.pdf



The URL?

<https://zenodo.org>

Scope

All fields of science. All types of research or copyright, or breach confidentiality or n subjects.

Eligible depositors

Anyone may register as user of Zenodo. All users are allowed to deposit content for which they possess the appropriate rights.

Safe

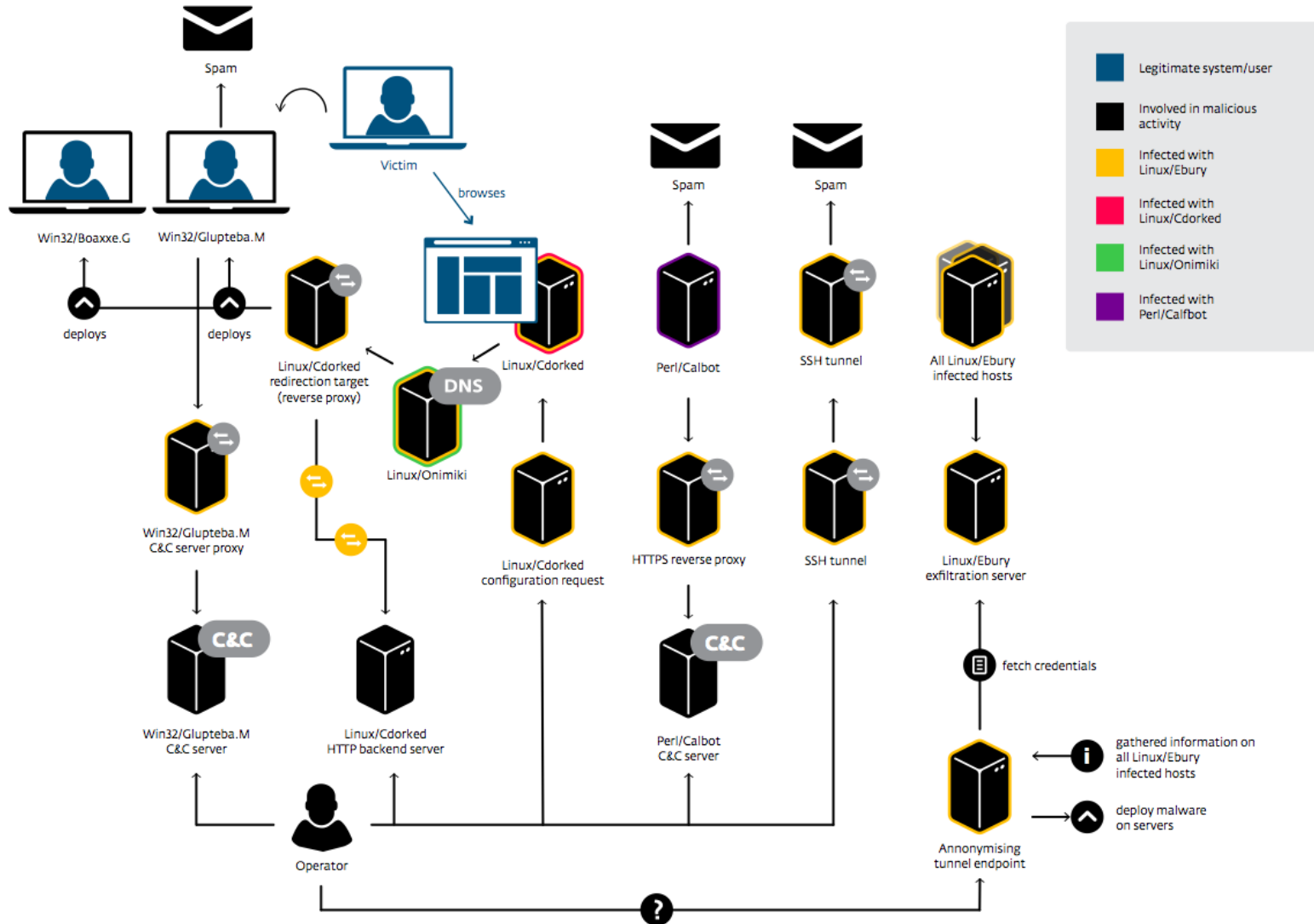
– more than just a drop box!

Your research output is stored safely for the future in same cloud infrastructure as research data from CERN's [Large Hadron Collider](#) using a CERN's battle-tested repository software [INVENIO](#) used by some of the world's largest repositories such as [INSPIRE HEP](#) and [CERN Document Server](#).

From <https://zenodo.org/policies>

We never do “just HEP”

Windigo operation



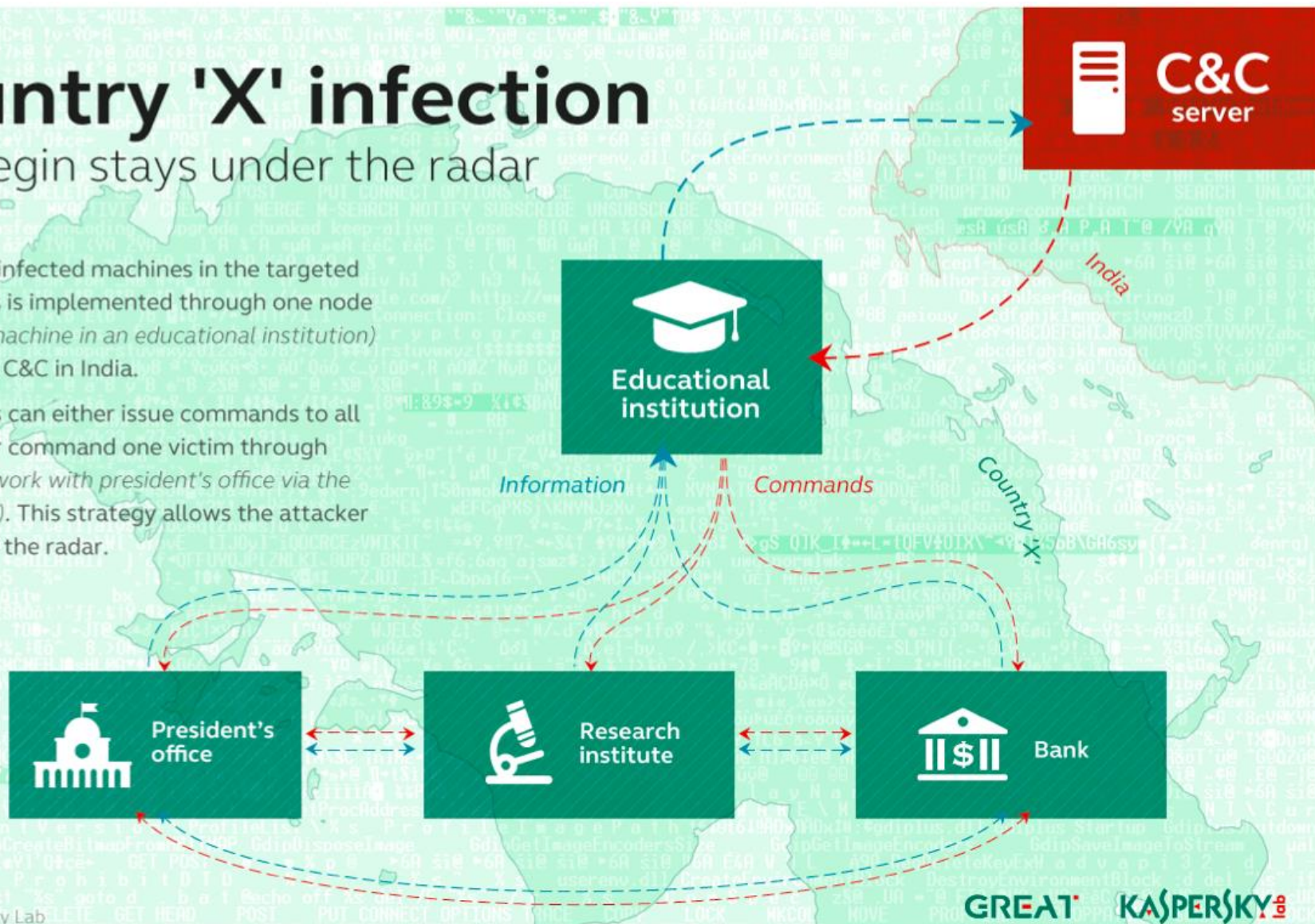
Educational/research labs as relays

Country 'X' infection

how Regin stays under the radar

Control over infected machines in the targeted organizations is implemented through one node (an infected machine in an educational institution) connected to C&C in India.

The attackers can either issue commands to all the victims or command one victim through another (eg. work with president's office via the bank network). This strategy allows the attacker to stay under the radar.



Watering hole attacks



We may be *not* the primary target

... but we may still be attacked

Security - it's just as with earthquakes

Risks are there, whether we like it or not

Addressing them means investing in protection and preparation

Including security early is the only option

We need awareness and education on all levels

Additionally, our systems *and* outside threats constantly evolve



