

IT-säkerhet i verkliga livet

Leif Nixon

Nyårsafton 2011

Mail från Adam i Wrocław:

Subject: Asking for some help

Date: Sat, 31 Dec 2011 14:03:37 +0100

Hi Leif,

I'm asking for help, because one of our Polish sites has been compromised. We are currently performing investigation, but it a hard time due to holiday....

Ouch

En Linux-maskin vid ett polskt superdatorcentrum utsatt för root-intrång.

Ouch

En Linux-maskin vid ett polskt superdatorcentrum utsatt för root-intrång.

Maskinen körde HP Data Protector, vars Windows-version hade ett färskt säkerhetshål (CVE-2011-0923, CVSS 10,0).

Ouch

En Linux-maskin vid ett polskt superdatorcentrum utsatt för root-intrång.

Maskinen körde HP Data Protector, vars Windows-version hade ett färskt säkerhetshål (CVE-2011-0923, CVSS 10,0).

Det visade sig att även Linux-versionen var sårbar...

Ouch

En Linux-maskin vid ett polskt superdatorcentrum utsatt för root-intrång.

Maskinen körde HP Data Protector, vars Windows-version hade ett färskt säkerhetshål (CVE-2011-0923, CVSS 10,0).

Det visade sig att även Linux-versionen var sårbar...

Inkräktaren laddade ner och kompilerade en illasinnad OpenSSH-version som loggade alla använda lösenord till `/var/run/sshd.sync`. Dessutom innehöll den en bakdörr; med det magiska lösenordet "g0t4nyr00ts" kom man alltid in som root.

Ouch

En Linux-maskin vid ett polskt superdatorcentrum utsatt för root-intrång.

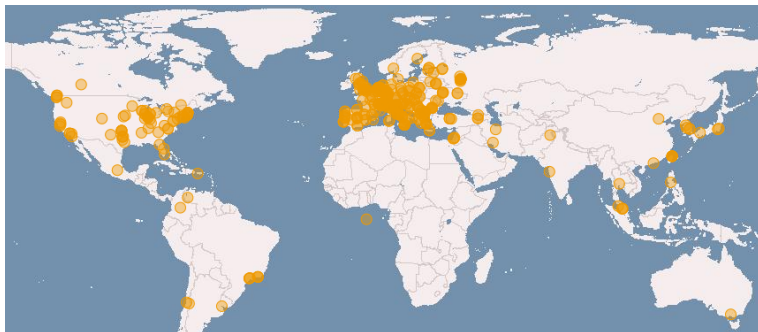
Maskinen körde HP Data Protector, vars Windows-version hade ett färskt säkerhetshål (CVE-2011-0923, CVSS 10,0).

Det visade sig att även Linux-versionen var sårbar...

Inkräktaren laddade ner och kompilerade en illasinnad OpenSSH-version som loggade alla använda lösenord till `/var/run/sshd.sync`. Dessutom innehöll den en bakdörr; med det magiska lösenordet "g0t4nyr00ts" kom man alltid in som root.

Stulna lösenord hade använts för att utföra ytterligare intrång på ett annat universitet i Polen.

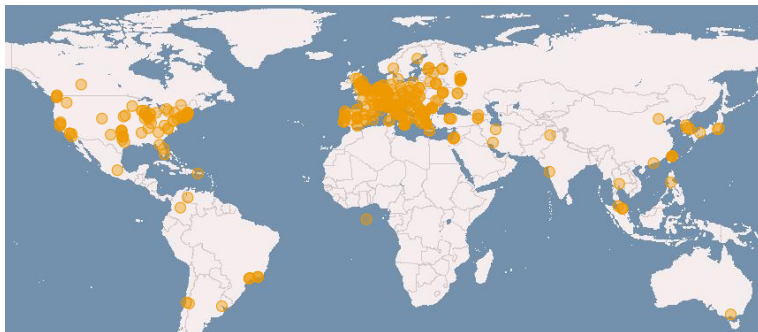
EGI – European Grid Infrastructure



- ▶ runt 300 resurscentra
- ▶ runt 60 länder

- ▶ tiotusentals kärnor
- ▶ dussintals petabyte lagring

EGI – European Grid Infrastructure



- ▶ runt 300 resurscentra
- ▶ runt 60 länder
- ▶ tiotusentals kärnor
- ▶ dussintals petabyte lagring

”En maskin för att svara på frågor”

EGI CSIRT

IRTF – Incident Response Task Force


Runt ett dussin personer runt Europa – c:a 2 FTE

Koordinerad av undertecknad

Säkerhetskontakter i varje "land", plus säkerhetskontakter på varje centrum

Plus övriga funktioner; Informationsspridning, utbildning, omvärldsbevakning, hantering av sårbarheter i egen och andras kod.

Incidenthanteringsprocess




4 SITE SPECIFICITIES

When a security incident potentially affecting grid users, services or operations is reported, the following procedures MUST be followed:

1. Immediately inform your local security team, your NIS Security Officer and the EGI CSIRT via info@egi.eu. **This step MUST be completed within 4 hours after the suspected incident has been discovered.** You are encouraged to use the templates in Appendix B.
2. Do NOT attempt to power off the host. In case no report is shortly available, whenever feasible and, if admitted by your local security procedure and if you are sufficiently familiar with the hardware, in site responsibility for this action, try to contain the incident. For instance by unplugging all connections (network, storage, etc) to the host. Please note down carefully what actions you take with a timestamp, that would be very important for later analysis as well as if the incident ends up in a legal case. **This step SHOULD be completed as soon as possible, and MUST be completed within one working day after the suspected incident has been discovered.**
3. Contain the incident, with assistance from your local security team and the EGI CSIRT.
4. If applicable, announce downtime for the affected host, in accordance with the EGI operational procedures [26], with "Security operations in progress" as the reason. **If applicable, this step MUST be completed within one working day after the suspected incident has been discovered.**
5. Perform appropriate analysis and take necessary corrective actions as per Appendix A. Logging information such as IP addresses, timestamps and identities involved etc., concerning the nature of any suspicious successful connections, must meet the national requirements specified in Appendix A. The objective is to understand the source and the extent of the incident, the affected components and services, and the possible implications for the infrastructure. **Throughout step 5, reports from the EGI CSIRT MUST be forthcoming within 4 hours.**
6. Coordinate with your local security team and the EGI CSIRT to send an incident case report within 1 month following the incident to all the sites via security-contacts@egi.eu, following format and conditions. This report should be labelled AMBER or higher, according to the Traffic Light Protocol [26].
7. Ranker the service and, if needed, update the service documentation and procedures to prevent recurrence in the future.

REG-AMBER-INFO-01-21-011 | © Member of REG-AMBER collaboration | PUBLIC | 9 / 17



5 INCIDENT COORDINATOR RESPONSIBILITIES

The EGI CSIRT appoints a security incident coordinator for each incident. This may be the Day Contact or another CSIRT member. The tasks of the incident coordinator include:

1. Evaluate the initial incident report and determine whether it appears to be part of a multiple incident. That is, whether it is related to a previously known incident (e.g. do the same attacking IP addresses appear, are the attack's tools and methodology strongly similar).
2. If this is a new, unrelated incident, assign an identifying tag of the format "[EGI-20090910]" or, if multiple incidents occur on the same date, "[EGI-20090910-01]" to the incident and announce it to all sites via info@egi.eu or info@egi.eu - use e-mail templates in Appendix B. **This step MUST be completed within 4 hours after the suspected incident is reported by the site.**
3. If the incident is part of a multi-site incident, the incident coordinator MAY choose not to announce such incident separately, but instead issue regular updates on the overall multi-site incident.
4. Whenever and as often as necessary, send updated summary reports to all sites (info@egi.eu and info@egi.eu), containing the status of the incident and possibly details needed to search locally for signs of malicious activity. Never send sensitive information without prior agreement of the originating site.
5. Whenever and as often as necessary, send updated detailed reports to the sites directly involved and affected by the incident, containing interesting findings or possible leads that could be used to resolve the incident.
6. Actively stimulate and probe the affected parties to obtain accurate information at an appropriate level of detail and in a timely manner.
7. Aim at understanding the exact cause and extent of the incident, what assets have been compromised/scrutinized etc., and how to react to the incident.
8. Help involved sites involve the incident by providing recommendations, promoting collaboration with other sites and periodically checking their status.
9. Maintain communications with any other involved parties inside and outside EGI.
10. When suspended accounts or identities no longer represent a threat, especially when the incident is resolved and compromised credentials have been replaced, inform the sites that access from these accounts or identities can be restored.

REG-AMBER-INFO-01-21-011 | © Member of REG-AMBER collaboration | PUBLIC | 10 / 17

Fokus på enkelhet, samarbete och maximal informations spridning.

Processen i praktiken

- ▶ *Security Officer on Duty* (jag) utsåg Adam till incidentkoordinator

Processen i praktiken

- ▶ *Security Officer on Duty* (jag) utsåg Adam till incidentkoordinator
- ▶ Adam skickade (inom 24 h) en heads-up till alla säkerhetskontakter plus EGI management

Processen i praktiken

- ▶ *Security Officer on Duty* (jag) utsåg Adam till incidentkoordinator
- ▶ Adam skickade (inom 24 h) en heads-up till alla säkerhetskontakter plus EGI management
- ▶ Adam arbetade tillsammans med det lokala centrumet för att utreda incidenten

Processen i praktiken

- ▶ *Security Officer on Duty* (jag) utsåg Adam till incidentkoordinator
- ▶ Adam skickade (inom 24 h) en heads-up till alla säkerhetskontakter plus EGI management
- ▶ Adam arbetade tillsammans med det lokala centrumet för att utreda incidenten
- ▶ *Security Officer on Duty* gav stöd i bakgrunden med koordination, forensik, etc

Processen i praktiken

- ▶ *Security Officer on Duty* (jag) utsåg Adam till incidentkoordinator
- ▶ Adam skickade (inom 24 h) en heads-up till alla säkerhetskontakter plus EGI management
- ▶ Adam arbetade tillsammans med det lokala centrumet för att utreda incidenten
- ▶ *Security Officer on Duty* gav stöd i bakgrunden med koordination, forensik, etc
- ▶ Adam skickade (inom 30 dagar) en detaljerad slutrapport till alla säkerhetskontakter plus EGI management

De oskrivna delarna av processen

Princip: Spåra incidenten så långt vi rimligen kan, för att:

- ▶ försvåra för inkräftaren att återvända – brända jordens taktik
- ▶ upptäcka och hjälpa andra drabbade

De oskrivna delarna av processen

Princip: Spåra incidenten så långt vi rimligen kan, för att:

- ▶ försvåra för inkräktaren att återvända – brända jordens taktik
- ▶ upptäcka och hjälpa andra drabbade

Utredningen i Polen visade att angreppet skett från ett av de stora universiteten i Sydkorea. Språkliga och organisatoriska problem.

De knappa data vi fick från Korea pekade på ytterligare offer; hosting-företag i Kanada (via sårbar Plesk) och universitet i Nederländerna (via HP Data Protector).

Bra samarbete med Nederländerna, som även gjorde polisanmälan.

De oskrivna delarna av processen

Princip: Spåra incidenten så långt vi rimligen kan, för att:

- ▶ försvåra för inkräktaren att återvända – brända jordens taktik
- ▶ upptäcka och hjälpa andra drabbade

Utredningen i Polen visade att angreppet skett från ett av de stora universiteten i Sydkorea. Språkliga och organisatoriska problem.

De knappa data vi fick från Korea pekade på ytterligare offer; hosting-företag i Kanada (via sårbar Plesk) och universitet i Nederländerna (via HP Data Protector).

Bra samarbete med Nederländerna, som även gjorde polisanmälan.

Och *där* ebbade incidenten ut.

Sidospår: hur får man folk att lyssna?

Subject: Heads up: plesk01.victim.com is root compromised
Date: Mon, 09 Jan 2012 09:45:24 +0100

I'm writing to you on behalf of the EGI CSIRT team. We are currently investigating an incident involving multiple sites in our constituency. Forensic analysis of one of the involved hosts shows that the intruders have also attacked your machine plesk01.victim.com.

My remote probing shows that this host is indeed root compromised and has had its ssh daemon replaced with a trojan version (this malware has also appeared at other involved sites).

--

Leif Nixon - Security officer

Sidospår: hur får man folk att lyssna?

Subject: Heads up: plesk01.victim.com is root compromised
Date: Mon, 09 Jan 2012 09:45:24 +0100

I'm writing to you on behalf of the EGI CSIRT team. We are currently investigating an incident involving multiple sites in our constituency. Forensic analysis of one of the involved hosts shows that the intruders have also attacked your machine plesk01.victim.com.

My remote probing shows that this host is indeed root compromised and has had its ssh daemon replaced with a trojan version (this malware has also appeared at other involved sites).

--

Leif Nixon - Security officer

Tystnad

Sidospår: hur får man folk att lyssna?

Försök två: kontakt via support-webbformulär.

Sidospår: hur får man folk att lyssna?

Försök två: kontakt via support-webbformulär.

Subject: [SUPPORT #DSJ-360864]: Support Request

Date: Fri, 13 Jan 2012 05:37:58 -0500

If this issue was emailed 4 days ago its been taken care of . Please avoid email duplicate tickets.

thank you

Best regards,

Victim Technical Support

Ticket Details

=====

Ticket ID: DSJ-360864

Priority: Normal

Status: Closed

Sidospår: hur får man folk att lyssna?

Jag: "Uhm, nej, ni har fortfarande problem."

Sidospår: hur får man folk att lyssna?

Jag: "Uhm, nej, ni har fortfarande problem."

Subject: [SUPPORT #DSJ-360864]: Support Request

Date: Fri, 13 Jan 2012 06:20:19 -0500

The issue was escalated to the appropriate department .
They are investigating the issue .

thank you

Best regards,

Victim Technical Support

Ticket Details

=====

Ticket ID: DSJ-360864

Priority: Normal

Status: Closed

Sidospår: hur får man folk att lyssna?

Subject: Re: [SUPPORT #DSJ-360864]: Support Request

Date: Tue, 17 Jan 2012 21:13:03 +0100

"Victim Support" <support@victim.com> writes:

- > The issue was escalated to the appropriate department .
- > They are investigating the issue .

It is now eight days since I reported this. Look, please just try this one thing:

```
ssh root@plesk01.victim.com
```

Enter the password "g0t4nyr00ts".

--

Leif Nixon - Security officer

14 februari 2012

Subject: security issue in tromso, and on gardar-adm
Date: Tue, 14 Feb 2012 22:11:08 +0100

We have some kind of a worm going on in our system here in tromsø and it seems that we have infected gardar-adm also.

at the moment we do not now all the machines infected.

this is how we have found the breach:

```
[root@gardar-adm ~]# ls -lad /var/log/.sshd/ssh.pid
-rw-rw-rw- root root Feb 14 12:13 /var/log/.sshd/ssh.pid
[root@gardar-adm ~]# strings /usr/sbin/sshd | grep g0
g0t4nyr00ts
```

Here we go again

Det här var uppenbart relaterat till intrången i Polen.

Incidenten återöppnades som en *multi-site incident*, och jag tog över koordinatorskapet.

Here we go again

Det här var uppenbart relaterat till intrången i Polen.

Incidenten återöppnades som en *multi-site incident*, och jag tog över koordinatorskapet.

Jag bistod Tromsø med *battlefield forensics*.

Utifrån tidsstämplar i filsystemet och systemloggar (logservern var turligt nog intakt) kunde det ursprungliga intrånget spåras till en inloggning från ett ryskt IP till ett konto tillhörande en användare i Trondheim.

Here we go again

Det här var uppenbart relaterat till intrången i Polen.

Incidenten återöppnades som en *multi-site incident*, och jag tog över koordinatorskapet.

Jag bistod Tromsø med *battlefield forensics*.

Utifrån tidsstämplar i filsystemet och systemloggar (logservern var turligt nog intakt) kunde det ursprungliga intrånget spåras till en inloggning från ett ryskt IP till ett konto tillhörande en användare i Trondheim.

Lokalt säkerhetshål (CVE-2010-3847) gav inkräktaren root, och han installerade sedan sin vanliga ssh-trojan.

Trojanen sniffade lösenord till ytterligare system i Tromsø och på Island, som också rootades.

Så långt "mina" system

Here we go again

Det här var uppenbart relaterat till intrången i Polen.

Incidenten återöppnades som en *multi-site incident*, och jag tog över koordinatorskapet.

Jag bistod Tromsø med *battlefield forensics*.

Utifrån tidsstämplar i filsystemet och systemloggar (logservern var turligt nog intakt) kunde det ursprungliga intrånget spåras till en inloggning från ett ryskt IP till ett konto tillhörande en användare i Trondheim.

Lokalt säkerhetshål (CVE-2010-3847) gav inkräktaren root, och han installerade sedan sin vanliga ssh-trojan.

Trojanen sniffade lösenord till ytterligare system i Tromsø och på Island, som också rootades.

Så långt "mina" system – **dags att bränna lite jord.**

Fiendens territorium

Med gemensamma krafter hittade jag och Trondheims säkerhetsfolk ett gäng Linux-maskiner med utbytt ssh.

Intrånget kunde spåras tillbaka till en Linux-maskin som körde HP Data Protector.

Ny twist på det hela: några av maskinerna körde en IRC-bot som kopplade upp till en C&C-server i Korea.

Fiendens territorium

Med gemensamma krafter hittade jag och Trondheims säkerhetsfolk ett gäng Linux-maskiner med utbytt ssh.

Intrånget kunde spåras tillbaka till en Linux-maskin som körde HP Data Protector.

Ny twist på det hela: några av maskinerna körde en IRC-bot som kopplade upp till en C&C-server i Korea.

Det gick alldeles utmärkt att koppla upp sig till C&C-servern och be den om en lista över anslutna bottar – en lång rad maskiner i Ostasien, USA och Europa – främst i akademien. Informationen vidarebefordrades till lämpliga kontakter (som DFN-CERT och REN-ISAC).

Dessutom fanns operatörerna inloggade på C&C-servern med sina vanliga nicks!

Rättsmaskineriet mal sakta men säkert

Norge polisanmälde sina intrång (efter visst tjat), och ärendet hamnade hos nationella polisen.

Under tiden hade ärendet i Nederländerna också eskalerats till nationell nivå, till NCSC och den nationella polisens High-Tech Crime Unit. Ett stort intrång hos KPN hade nämligen också kopplats ihop med samma härva.

Nu kopplades alla aktörer ihop.



Och så, till slut

Subject: Re: Update

Date: Thu, 15 Mar 2012 09:40:06 +0100

Expect multiple coordinated arrests within
the next two weeks.

Och så, till slut

Tillslag i Nederländerna och Australien. I slutänden rättegång mot en holländsk yngling.

OPENBAAR MINISTERIE

[Home](#) [Actueel](#) [Onderwerpen](#) [Organisatie](#) [Werken bij het OM](#)



[» Home](#) [» 17-jarige jongen verdacht van hacken KPN](#)

17-jarige jongen verdacht van hacken KPN

26 maart 2012 - Landelijk Parket

Het Team High Tech Crime van de Nationale Recherche heeft in Barendrecht een 17-jarige jongen aangehouden die wordt verdacht van het hacken van KPN op 16 januari 2012. De jongen kon vorige week dinsdag thuis worden aangehouden toen hij aan het begin van de middag online was op internet.

**AND NOW FOR
SOMETHING
COMPLETELY
DIFFERENT**



Net1:s M-90-modem

- ▶ Pratar CDMA på 450 MHz-bandet i ena änden, wifi i andra
- ▶ Bra yttäckning över hela Sverige
- ▶ Levereras färdigkonfigurerat; inte ens ett SIM-kort att stoppa i

Tidslinje

2013-07-16

Jag får mitt modem. UPnP på
WAN-sidan!?!

Universal Plug and Play

UPnP:

- ▶ Protokollsvit för hemmanätverk
- ▶ Automatisk upptäckt av mediaspelare, mediabibliotek, Internet-gateways, etc
- ▶ Stöds av de flesta hemmarouters
- ▶ Tillåter omkonfigurering av brandväggen
- ▶ Saknar normalt autentisering

UPnP på WAN-sidan!?!

Det verkar uppenbart att man inte vill exponera UPnP mot hela Internet, eller hur?

Rapid7 publicerade i januari 2013 en studie¹ av enheter på Internet med exponerad UPnP-funktionalitet.

De hittade

¹<https://community.rapid7.com/docs/DOC-2150>

UPnP på WAN-sidan!?!

Det verkar uppenbart att man inte vill exponera UPnP mot hela Internet, eller hur?

Rapid7 publicerade i januari 2013 en studie¹ av enheter på Internet med exponerad UPnP-funktionalitet.

De hittade 81 miljoner enheter som svarade på UPnP-frågor.

¹<https://community.rapid7.com/docs/DOC-2150>

Tidslinje

2013-07-16

Jag får mitt modem. UPnP på
WAN-sidan!?!

Tidslinje

2013-07-16

Jag får mitt modem.

UPnP på
WAN-sidan!?!

Portable SDK
v1.3.1!?!

CVE-2012-5958, -5959, -5960, -5961, -5962, -5963, -5964, samt -5965



Software Engineering Institute | Carnegie Mellon.

Vulnerability Notes Database

Advisory and mitigation information about software vulnerabilities



Homeland
Security

Sponsored by the DHS Office of
Cybersecurity and Communications

[DATABASE HOME](#)

[SEARCH](#)

[REPORT A VULNERABILITY](#)

[HELP](#)

Vulnerability Note **VU#922681**

Portable SDK for UPnP Devices (libupnp) contains multiple buffer overflows in SSDP

Original Release date: 29 Jan 2013 | Last revised: 05 Apr 2013

Tidslinje

2013-07-16

Jag får mitt modem.

UPnP på
WAN-sidan!?!

Portable SDK
v1.3.1!?!

Tidslinje

2013-07-16

Jag får mitt modem.

UPnP på
WAN-sidan!?!

Portable SDK
v1.3.1!?!

2013-08-07

Testversion av
firmware

UPnP på
WAN-sidan!?!

~~Portable SDK~~
~~v1.3.1!?!~~

Tidslinje

2013-07-16

Jag får mitt modem.

UPnP på
WAN-sidan!?!

Portable SDK
v1.3.1!?!

2013-08-07

Testversion av
firmware

UPnP på
WAN-sidan!?!

~~Portable SDK~~
~~v1.3.1!?!~~

2013-08-20

Testversion av
firmware

UPnP på
WAN-sidan!?!

~~Portable SDK~~
~~v1.3.1!?!~~

Tidslinje

2013-07-16

Jag får mitt modem.

UPnP på
WAN-sidan!?!

Portable SDK
v1.3.1!?!

2013-08-07

Testversion av
firmware

UPnP på
WAN-sidan!?!

~~Portable SDK~~
~~v1.3.1!?!~~

2013-08-20

Testversion av
firmware

UPnP

~~Portable SDK~~
~~v1.3.1!?!~~

Tidslinje

2013-07-16

Jag får mitt modem.

UPnP på
WAN-sidan!?!

Portable SDK
v1.3.1!?!

2013-08-07

Testversion av
firmware

UPnP på
WAN-sidan!?!

~~Portable SDK
v1.3.1!?!~~

2013-08-20

Testversion av
firmware

UPnP

~~Portable SDK
v1.3.1!?!~~

2013-09-12

Officiell
firmware

UPnP

~~Portable SDK
v1.3.1!?!~~

Det finns en viktig uppdatering för ditt modem



Viktig information till dig Leif

Vi har precis lanserat en ny mjukvara som behövs för att ditt modem skall fungera som tänkt längre fram i höst.

Det är av största vikt att du tar dig ett par minuter och uppgraderar ditt modem.

Vi utför arbeten med att göra din uppkoppling bättre och mer jämn, ett steg i det är att uppgradera ditt modem med den senaste mjukvaran, så att det fungerar så bra som möjligt.

Mjukvaran innehåller nödvändiga ändringar för att modemmet skall fungera som tänkt och ge dig som användare den bästa upplevelsen.

Videon nedan visar hur enkelt det är att installera den nya mjukvaran.

Klicka här för att läsa mer och uppdatera mjukvaran



Det här var det bra fallet

De här modemerna säkrades (förhoppningsvis) till slut.

- ▶ Operatören hade centralt ansvar för modemerna
- ▶ Operatören och tillverkaren lyssnade
- ▶ Förhoppningsvis slutar uppdaterade modem att fungera

Det här var det bra fallet

De här modemerna säkrades (förhoppningsvis) till slut.

- ▶ Operatören hade centralt ansvar för modemerna
- ▶ Operatören och tillverkaren lyssnade
- ▶ Förhoppningsvis slutar uppdaterade modem att fungera

Av 81 miljoner sårbara enheter:

- ▶ Hur många är inköpta av slutanvändaren?
- ▶ Hur många slutanvändare klarar av att uppdatera sina enheter?
- ▶ Hur stor del av enheterna har ens support längre?

Internet Census 2012

Grundläggande idé:

- ▶ Det finns ohyggligt mycket enheter som lyssnar på telnet

Internet Census 2012

Grundläggande idé:

- ▶ Det finns ohyggligt mycket enheter som lyssnar på telnet
- ▶ Ingen ändrar någonsin defaultlösenord

Internet Census 2012

Grundläggande idé:

- ▶ Det finns ohyggligt mycket enheter som lyssnar på telnet
- ▶ Ingen ändrar någonsin defaultlösenord
- ▶ Scanna Internet efter telnet-enheter, försök logga in som root:root, admin:admin, osv

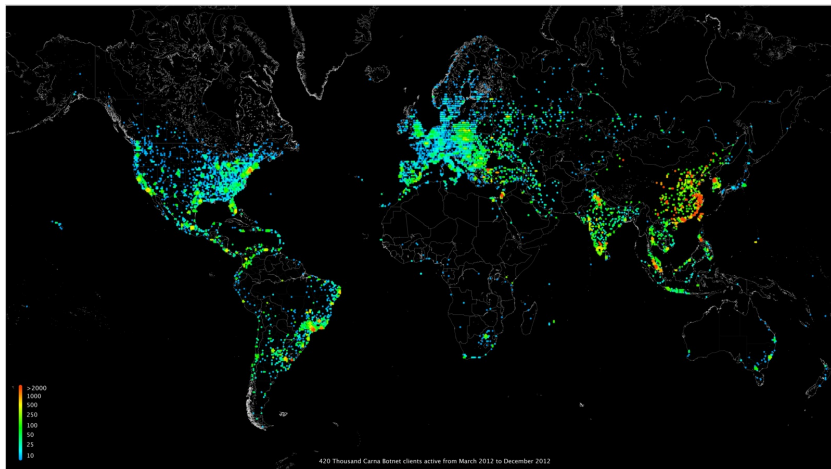
Internet Census 2012

Grundläggande idé:

- ▶ Det finns ohyggligt mycket enheter som lyssnar på telnet
- ▶ Ingen ändrar någonsin defaultlösenord
- ▶ Scanna Internet efter telnet-enheter, försök logga in som root:root, admin:admin, osv
- ▶ ...OMG!

Internet Census 2012

Den anonyma operatören byggde ett "snällt" botnet, Carna, som autonomt spridde sig till alla kompatibla telnet-enheter den hittade.



Internet Census 2012

Carna användes för att samla in diverse intressant Internet-statistik.

Internet Census 2012

...men Carna var inte först.

Internet Census 2012

...men Carna var inte först.

På en signifikant andel av enheterna fanns redan ett botnet, Aidra. Som inte är snällt.

Carna-operatören gjorde sitt bästa för att utplåna Aidra, men det gav på sin höjd tillfällig respit – just nu finns det flera varianter av Aidra som slåss med varandra.

Ytterligare angrepp



Donderdag 13 maart 2014. Het laatste nieuws het eerst op NU.nl

Vorpagina

Net binnen

Algemeen

Vermist vliegtuig

Economie

Beurs

Sport

Tech

Achterklap

Entertainment

Opmerkelijk

Wetenschap

Gezondheid

Lifestyle

Auto

NUfoto

Datablog

Tech

Gepubliceerd: 6 februari 2014 14:40

Laatste update: 7 februari 2014 08:01

Deel:   

XS4ALL-klienten slachtoffer gehackte routers

Door een hack van Fritzbox-modems die XS4ALL gebruikt, kan een klein deel van de klanten onverwacht een hoge telefoonrekening krijgen omdat de hackers stiekem naar betaalnummers bellen.



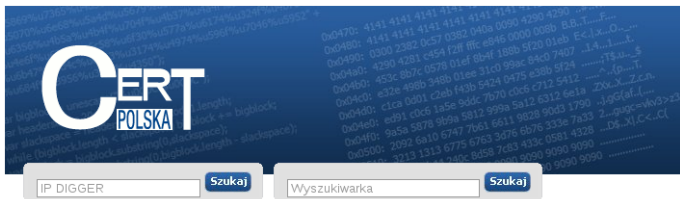
Foto: Getty Images

Dat bevestigt een woordvoerder van XS4ALL tegenover NUtech.nl na berichtgeving van [RTL Nieuws](#).

Hackers hebben toegang gekregen tot Fritzbox-routers van AVM. Daardoor kunnen ze via de Voice over IP-verbinding stiekem telefoontjes plegen naar betaalnummers. De klanten krijgen vervolgens onverwacht een hoge rekening.

Februari 2014: XS4ALL-kunders VoIP-routrar börjar ringa betalsamtal på massiv skala.

Ytterligare angrepp



[« Ogłoszenie wyników konkursu na logo CERT.pl](#)

[Warsztat "NISHA – platforma wymiany treści" »](#)

Ruch klientów banków jest przechwytywany i modyfikowany na skutek luk w routerach

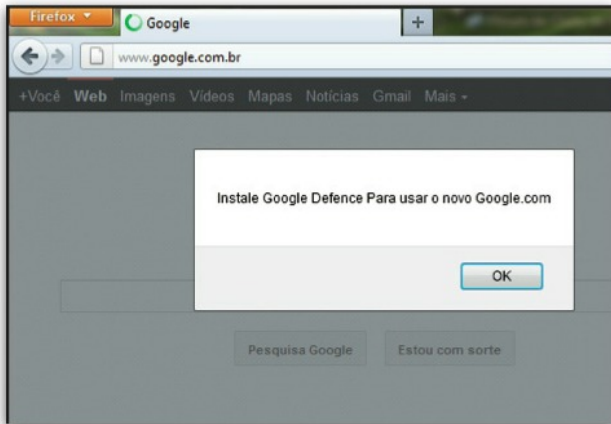


Pod koniec 2013 roku do zespołu CERT Polska dotarły potwierdzone informacje o pojawianiu się komunikatów sugerujących modyfikację stron bankowych przez złośliwe oprogramowanie na urządzeniach iPhone. Użytkownicy takich urządzeń oglądali komunikat o zmianie numeru konta bankowego, która powinna zostać potwierdzona kodem jednorazowym. Sam scenariusz był nam dobrze znany jako jedna z wersji iniekcji wykorzystywanych przez trojany bankowe. Skąd jednak taki trojan na iPhone? Ponieważ byłby to pierwszy przypadek tego typu ataku na tę platformę, w dodatku ukierunkowany na polskich klientów systemów bankowych, zwrócił on naszą szczególną uwagę. W wyniku analizy zostało ustalone wiele możliwych scenariuszy przeprowadzenia ataku,

włącznie z metodami infekcji urządzeń z systemem iOS. Niestety, z powodu braku wystarczających szczegółów dotyczących infekcji nie byliśmy w stanie jednoznacznie określić metody przeprowadzenia ataku.

Senhöstén 2013: 300000 polska hemmaroutrar hackade; DNS-inställningar ändrade för att möjliggöra kapning av bankkonton.

Ytterligare angrepp



2012: 4,5 miljoner hemmarouters i Brasilien hackade;
DNS-inställningar ändrade för att möjliggöra kapning av
bankkonton.

Vad ska vi göööööra?

Vad ska vi göööööra?

Samverkansgruppen för informationssäkerhet (SAMFI)

Följande myndigheter samverkar inom SAMFI:

- ▶ Myndigheten för samhällsskydd och beredskap (MSB)
- ▶ Post- och telestyrelsen (PTS)
- ▶ Försvarets radioanstalt (FRA)
- ▶ Säkerhetspolisen (Säpo) och Rikskriminalpolisen (RKP) i samverkan
- ▶ Försvarets materielverk (FMV)/Sveriges Certifieringsorgan för IT-säkerhet (CSEC)
- ▶ Försvarsmakten (FM)/Militära underrättelse- och säkerhetstjänsten (MUST)

Vad ska vi göööööra?

Samverkansgruppen för informationssäkerhet (SAMFI)

Följande myndigheter samverkar inom SAMFI:

- ▶ Myndigheten för samhällsskydd och beredskap (MSB)
- ▶ Post- och telestyrelsen (PTS)
- ▶ Försvarets radioanstalt (FRA)
- ▶ Säkerhetspolisen (Säpo) och Rikskriminalpolisen (RKP) i samverkan
- ▶ Försvarets materielverk (FMV)/Sveriges Certifieringsorgan för IT-säkerhet (CSEC)
- ▶ Försvarsmakten (FM)/Militära underrättelse- och säkerhetstjänsten (MUST)

Kockar. Soppa.

That's all, folks

leif.nixon@nixon-security.se