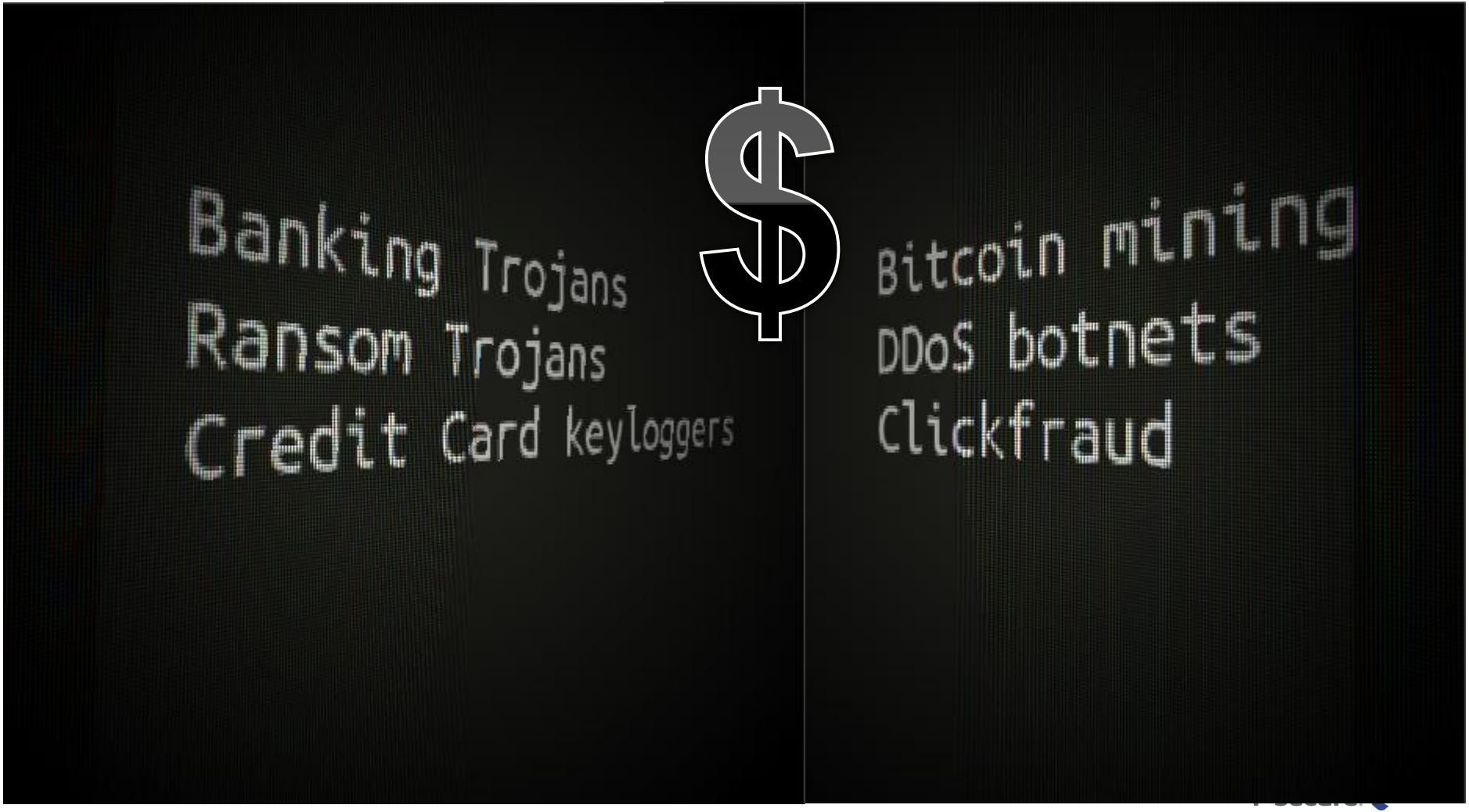

The Online Arms Race
Mikko Hypponen
Twitter: @mikko
F-Secure.

Internet changes everything

F-Secure.


Mihai ghiata


Т993ТН

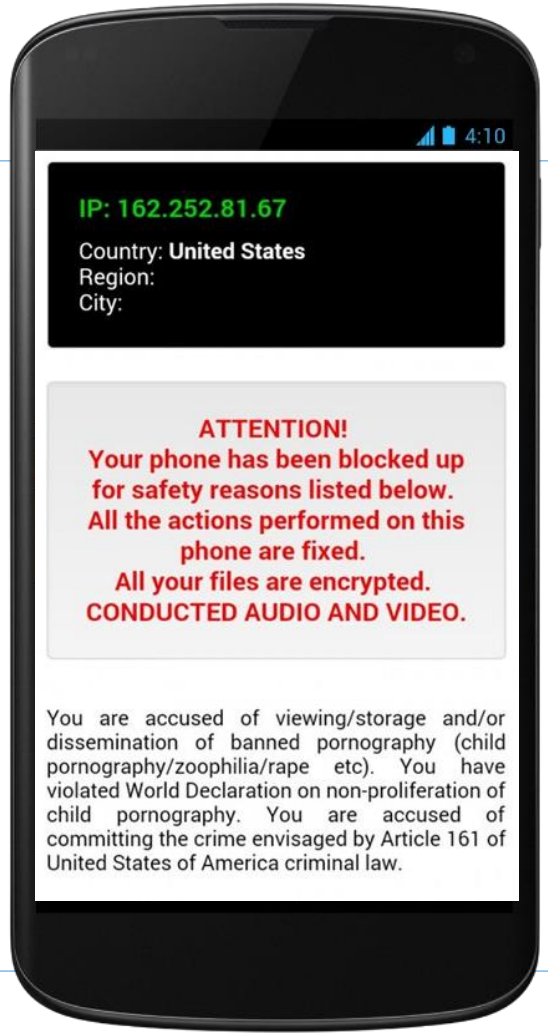

Banking Trojans
Ransom Trojans
Credit Card keyloggers
$
Bitcoin mining
DDoS botnets
Clickfraud

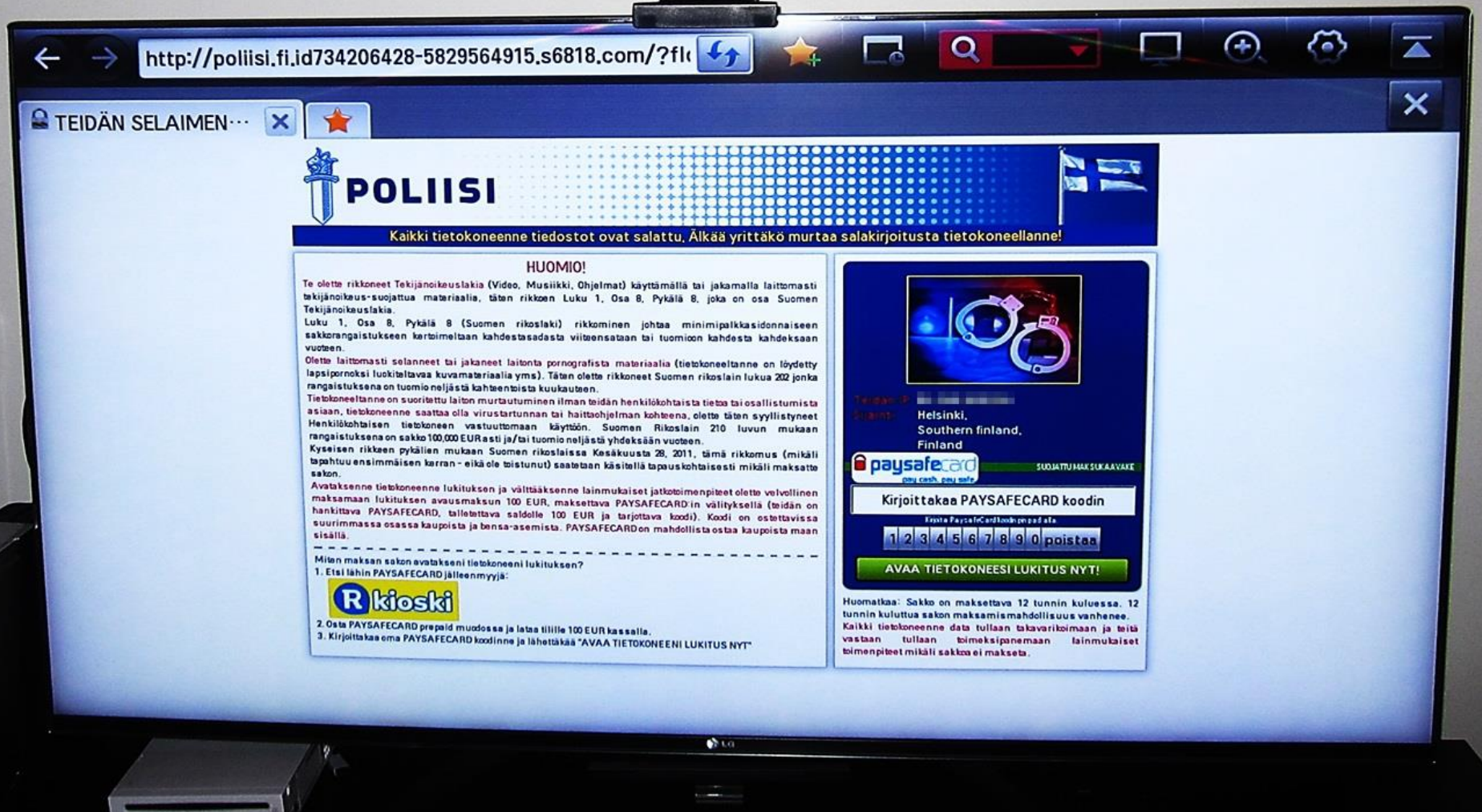

CryptoLocker
Your personal files are encrypted!
Your important files encryption produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.
Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the private key.
The single copy of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will destroy the key after a time specified in this window. After that, nobody and never will be able to restore files...
To obtain the private key for this computer, which will automatically decrypt files, you need to pay 300 USD / 300 EUR / similar amount in another currency.
Click «Next» to select the method of payment and the currency.
Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.
Private key will be destroyed on
9/13/2013
5:27 AM
Time left
71 : 19 : 53
Next >>

F-Secure


Task Manager
IMPORTANT! PLEASE READ!
Unfortunately the files on this computer (ie. documents, photos, videos) have been encrypted using an extremely secure and unbreakable algorithm. This means that the files are now useless unless they are decrypted using a key.
The good news is that your files are not lost forever! This tool is able to rescue the files on your computer for you!
BY PURCHASING A LICENSE FROM US, WE ARE ABLE TO RESCUE YOUR FILES 100% GUARANTEED FOR A VERY LOW EARLY BIRD PRICE OF ONLY $300 USD!* In 5 days however, the price of this service will increase to $600 USD, and after 10 days to $1000 USD.
Payment is accepted in Bitcoin only. You can purchse Bitcoin very easily in your area by bank transfer, Western Union, or even cash.
Visit www.localbitcoins.com to find a seller in your area. You can also google Bitcoin Exchanges to find other methods for buying Bitcoin.
Please check the current price of Bitcoin and ensure you are sending the correct amount before making your payment! Visit www.bitcoinaverage.com for the current Bitcoin price.
After making your payment, please wait up to 24 hours for us to make your key available. Usually done in much less time however.
IMPORTANT: Once the key is available and you click "Decrypt Files", please wait and let the decryption process complete before closing this tool. This process can take from 15 minutes to 2+ hours depending on how many files need to be decrypted. You will get a notification that the decryption process is complete, at which time you can click "Exit". Removing this tool from your computer without first decrypting your files will cause your files to be lost forever.
bitcoin ACCEPTED HERE
SEND BITCOIN PAYMENT TO THIS ADDRESS:
DECRYPT FILES
EXIT
*Please note that early bird qualification is determined from the date that this tool was first run as recorded on our servers.

F-Secure.


4:10
IP: 162.252.81.67
Country: United States
Region:
City:
ATTENTION!
Your phone has been blocked up for safety reasons listed below.
All the actions performed on this phone are fixed.
All your files are encrypted.
CONDUCTED AUDIO AND VIDEO.
You are accused of viewing/storage and/or dissemination of banned pornography (child pornography/zoophilia/rape etc). You have violated World Declaration on non-proliferation of child pornography. You are accused of committing the crime envisaged by Article 161 of United States of America criminal law.


http://poliisi.fi.id734206428-5829564915.s6818.com/?fl
TEIDÄN SELAIMEN···
POLIISI
Kaikki tietokoneenne tiedostot ovat salattu. Älkää yrittäkö murtaa salakirjoitusta tietokoneellanne!
HUOMIO!
Te olette rikkoneet Tekijänoikeuslakia (Video, Musiikki, Ohjelmat) käyttämällä tai jakamalla laittomasti tekijänoikeus-suojattua materiaalia, täten rikkoen Luku 1, Osa 8, Pykälä 8, joka on osa Suomen Tekijänoikeuslakia.
Luku 1, Osa 8, Pykälä 8 (Suomen rikoslaki) rikkominen johtaa minimipalkkasidonnaiseen sakkorangaistukseen kertoimeltaan kahdestasadasta viiteensataan tai tuomioon kahdesta kahdeksaan vuoteen.
Olette laittomasti selanneet tai jakaneet laitonta pornografista materiaalia (tietokoneeltanne on löydetty lapsipornoksi luokiteltavaa kuvamateriaalia yms). Täten olette rikkoneet Suomen rikoslain lukua 202 jonka rangaistuksena on tuomio neljästä kahteentoista kuukautteen.
Tietokoneeltanne on suoritettu laiton murtautuminen ilman teidän henkilökohtaista tietoa tai osallistumista asiaan, tietokoneenne saattaa olla virustartunnan tai haittaohjelman kohteena, olette täten syyllistyneet Henkilökohtaisen tietokoneen vastuuttomaan käyttöön. Suomen Rikoslain 210 luvun mukaan rangaistuksena on sakko 100,000 EUR asti ja/tai tuomio neljästä yhdeksään vuoteen.
Kyseisen rikkeen pykälien mukaan Suomen rikoslaissa Kesäkuusta 28, 2011, tämä rikkomus (mikäli tapahtuu ensimmäisen kerran - eikä ole toistunut) saatetaan käsitellä tapauskohtaisesti mikäli maksatte sakon.
Avataksenne tietokoneenne lukituksen ja välttääksenne lainmukaiset jatkotoimenpiteet olette velvollinen maksamaan lukituksen avausmaksun 100 EUR, maksettava PAYSAFECARD:in välityksellä (teidän on hankittava PAYSAFECARD, talletettava saldolle 100 EUR ja tarjottava koodi). Koodi on ostettavissa suurimmassa osassa kaupoista ja bensa-asemista. PAYSAFECARDon mahdollista ostaa kaupoista maan sisällä.
Miten maksan sakon avatakseni tietokoneeni lukituksen?
1. Etsi lähin PAYSAFECARD jälleenmyyjä:
R kioski
2. Osta PAYSAFECARD prepaid muodossa ja lataa tilille 100 EUR kassalla.
3. Kirjoittakaa oma PAYSAFECARD koodinne ja lähettäkää "AVAA TIETOKONEENI LUKITUS NYT"
Helsinki,
Southern finland,
Finland
paysafecard
SUOJATTU MAKSUKAAVAKE
Kirjoittakaa PAYSAFECARD koodin
1 2 3 4 5 6 7 8 9 0 poistaa
AVAA TIETOKONEESI LUKITUS NYT!
Huomatkaa: Sakko on maksettava 12 tunnin kuluessa. 12 tunnin kuluttua sakon maksamismahdollisuus vanhenee. Kaikki tietokoneenne data tullaan takavarikoimaan ja teitä vastaan tullaan toimeksipanemaan lainmukaiset toimenpiteet mikäli sakkoa ei makseta.

POS trojans


GO
R
C
Pay
Sub Total
Deposit
Tax
Discount
Grand Total
15.00
HP L5006tm


godzilla (192.168.1.13, 192.168.65.1, 192.168.91.1)
Recycle Bin
LCEConfig
QuickTime Player
VLC media player
µTorrent
ron-gulas-computer (rongula)
192.168.1.16
Terminal File Edit Scrollback Font Window Help
Fri 10:19 AM
RealPlayer
vlc-0.9.9a.dmg
Karate Videos
lce_client-3.4.0-osx.tar.gz
*disk1`
04
lce_client-3.4.0-RC2-osx
ServeToMe
ServeToMe-v3.6.6.dmg
ServeToMe
plugins
Microsoft Windows
ron-gulas-compute...
10:21 AM
Recycle Bin
Picasa 3
SoftIPT
WebEx One-Click

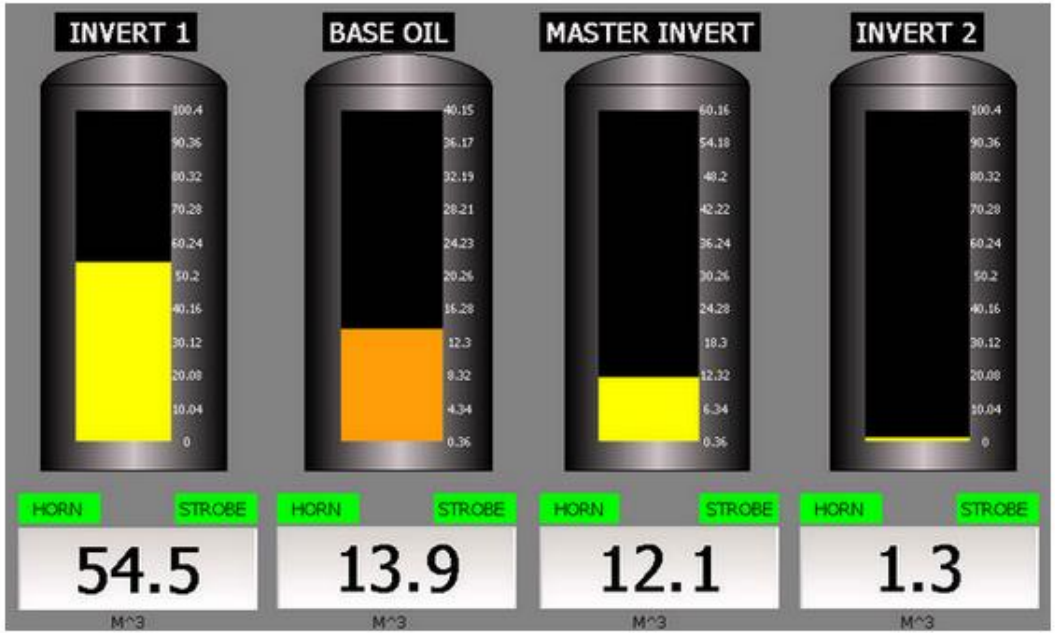

Dan Tentler
@Viss
Following
Phil, I think you're gonna have a bad time.
Reply
Retweet
Favorite
Share
More
Audio
Video
Lights
Phil's Office
Home
Irrigation
Alarm
Phil's Office Lights
68°
ROOM TEMP 74°
Eliz
Phil
Wash Wall
Entry
Stairs
Bath
OFF
Off

Dan Tentler
@Viss

Follow

an oil field?

Reply Retweet Favorited More

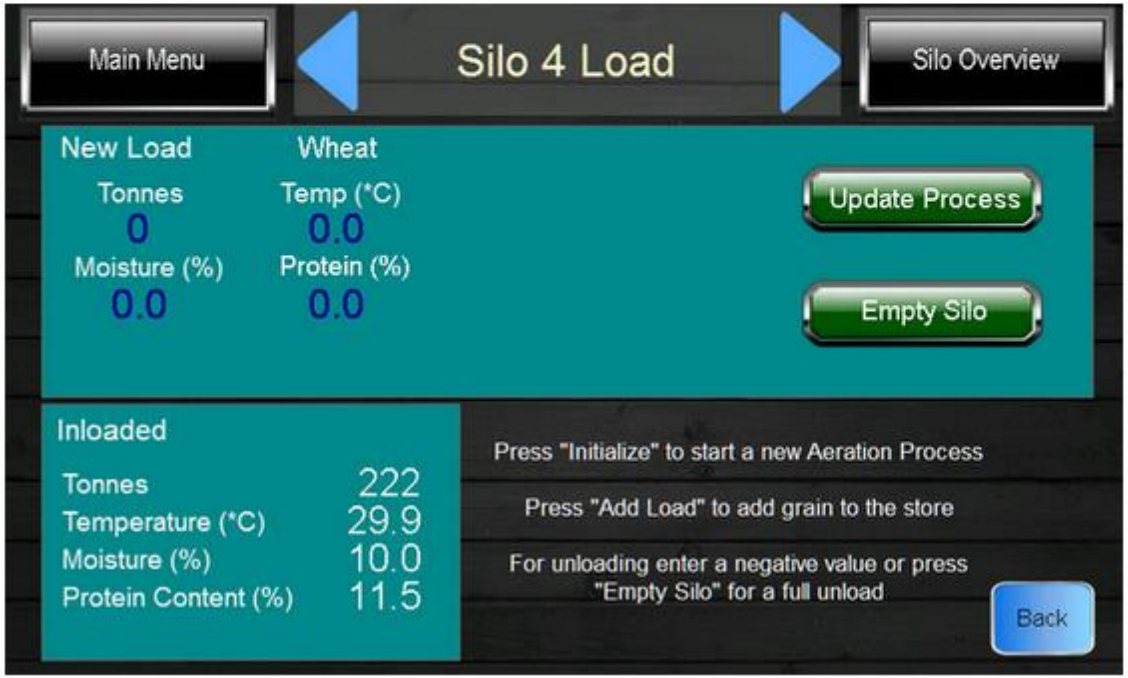


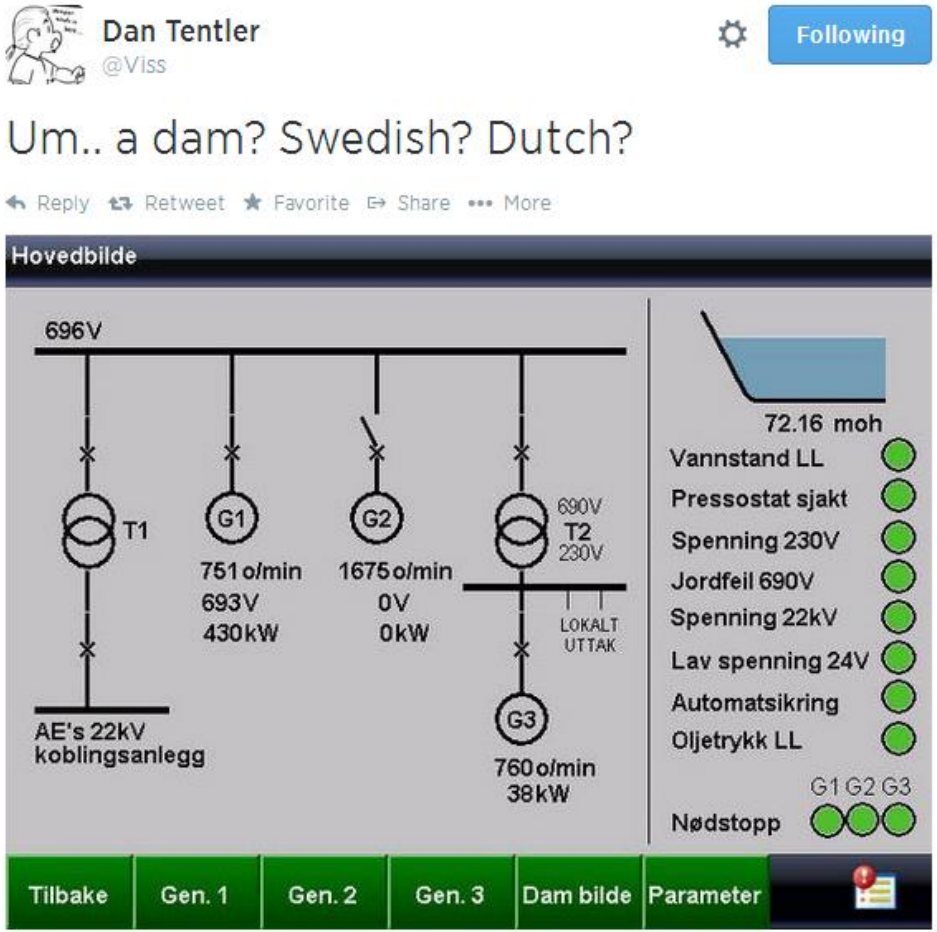
Dan Tentler
@Viss

Follow

a wheat silo!

Reply Retweet Favorite More



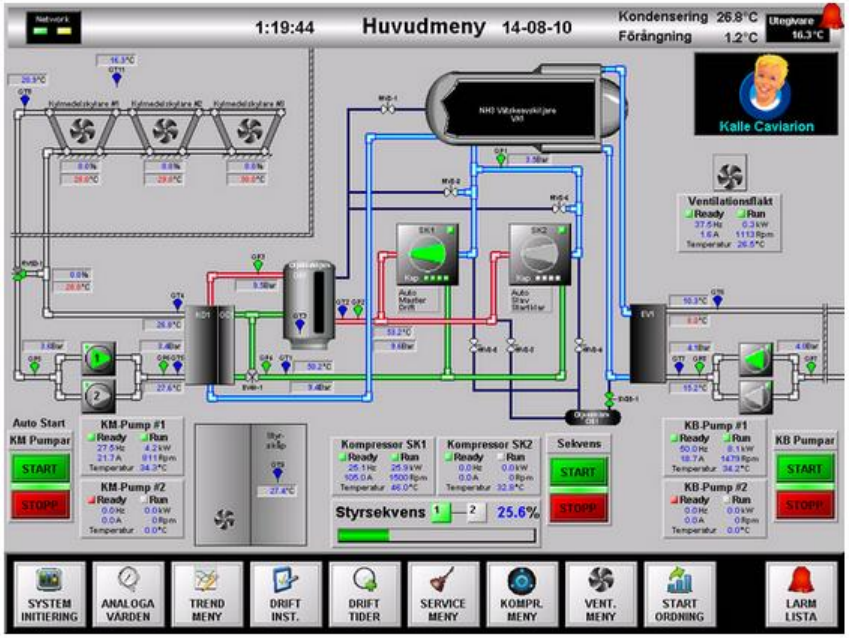

Dan Tentler
@Viss
Following
Um.. a dam? Swedish? Dutch?
Reply
Retweet
Favorite
Share
More
Hovedbilde
696V
T1
G1
751 o/min
693V
430kW
G2
1675 o/min
0V
0kW
690V
T2
230V
LOKALT
UTTAK
G3
760 o/min
38kW
AE's 22kV
koblingsanlegg
72.16 moh
Vannstand LL
Pressostat sjakt
Spenning 230V
Jordfeil 690V
Spenning 22kV
Lav spenning 24V
Automatsikring
Oljetrykk LL
G1 G2 G3
Nødstopp
Tilbake
Gen. 1
Gen. 2
Gen. 3
Dam bilde
Parameter

Dan Tentler
@Viss

Follow

hahaha the little face in the upper right makes this. FRIENDLIEST SCADA ON THE NET!

Reply Retweet Favorited More



Dan Tentler
@Viss

Follow

NO! Is this a radio station?! :D nowai.

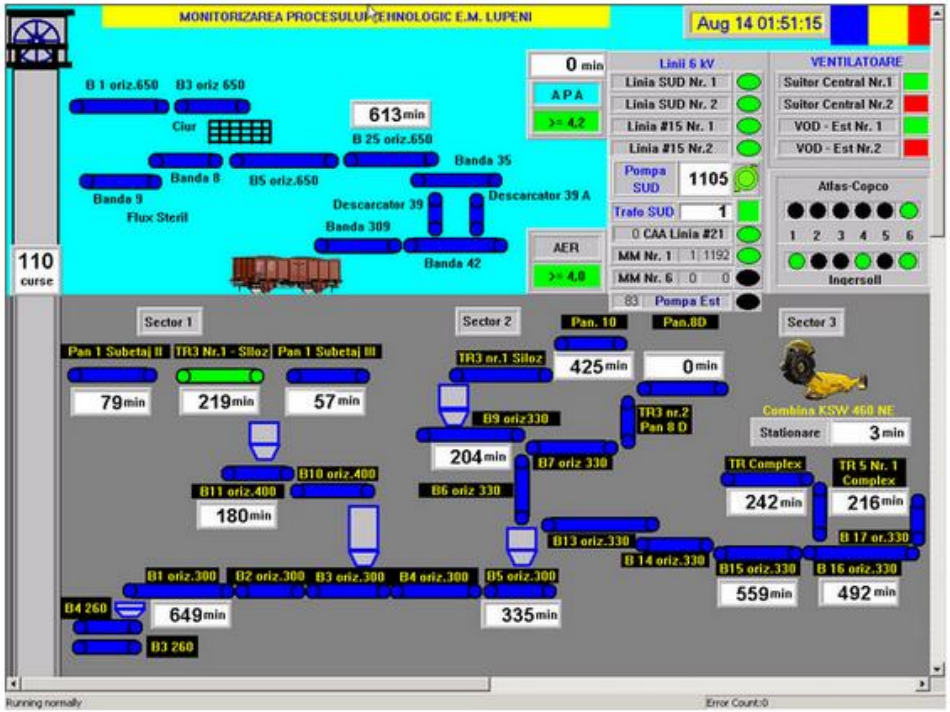
Reply Retweet Favorited More

Dan Tentler
@Viss

Follow

I want to say this is a train control system, but I'm not sure. Italian maybe?

Reply Retweet Favorite ••• More

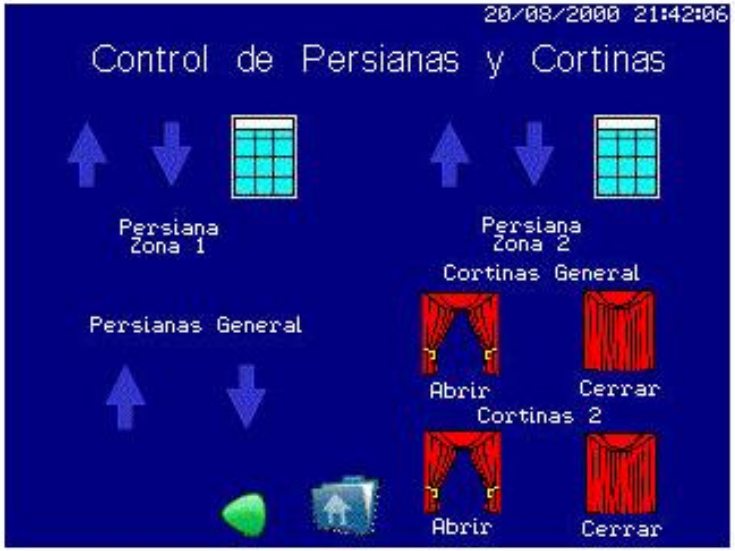


Dan Tentler
@Viss

Following

Curtains. There are FUCKING CURTAINS on the internet.

Reply Retweet Favorite ••• More

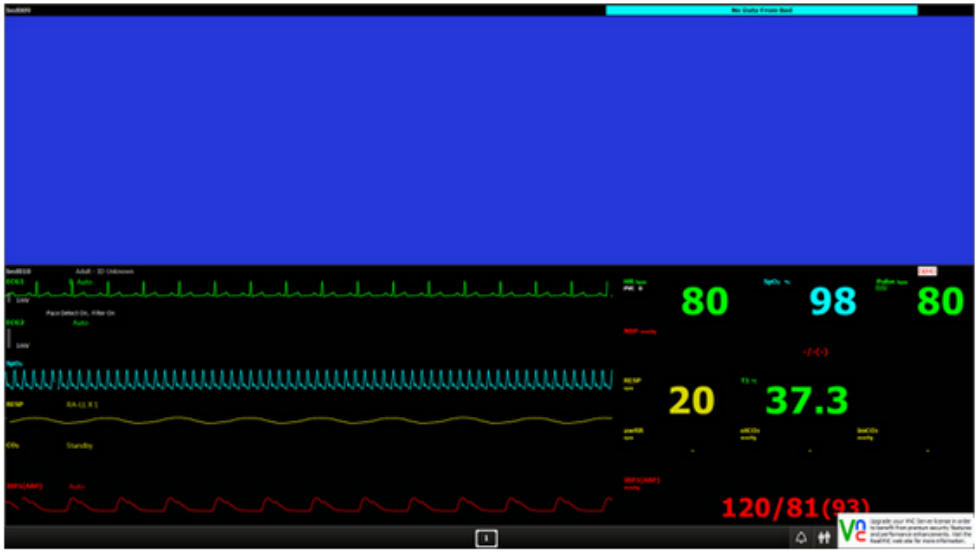


Dan Tentler
@Viss

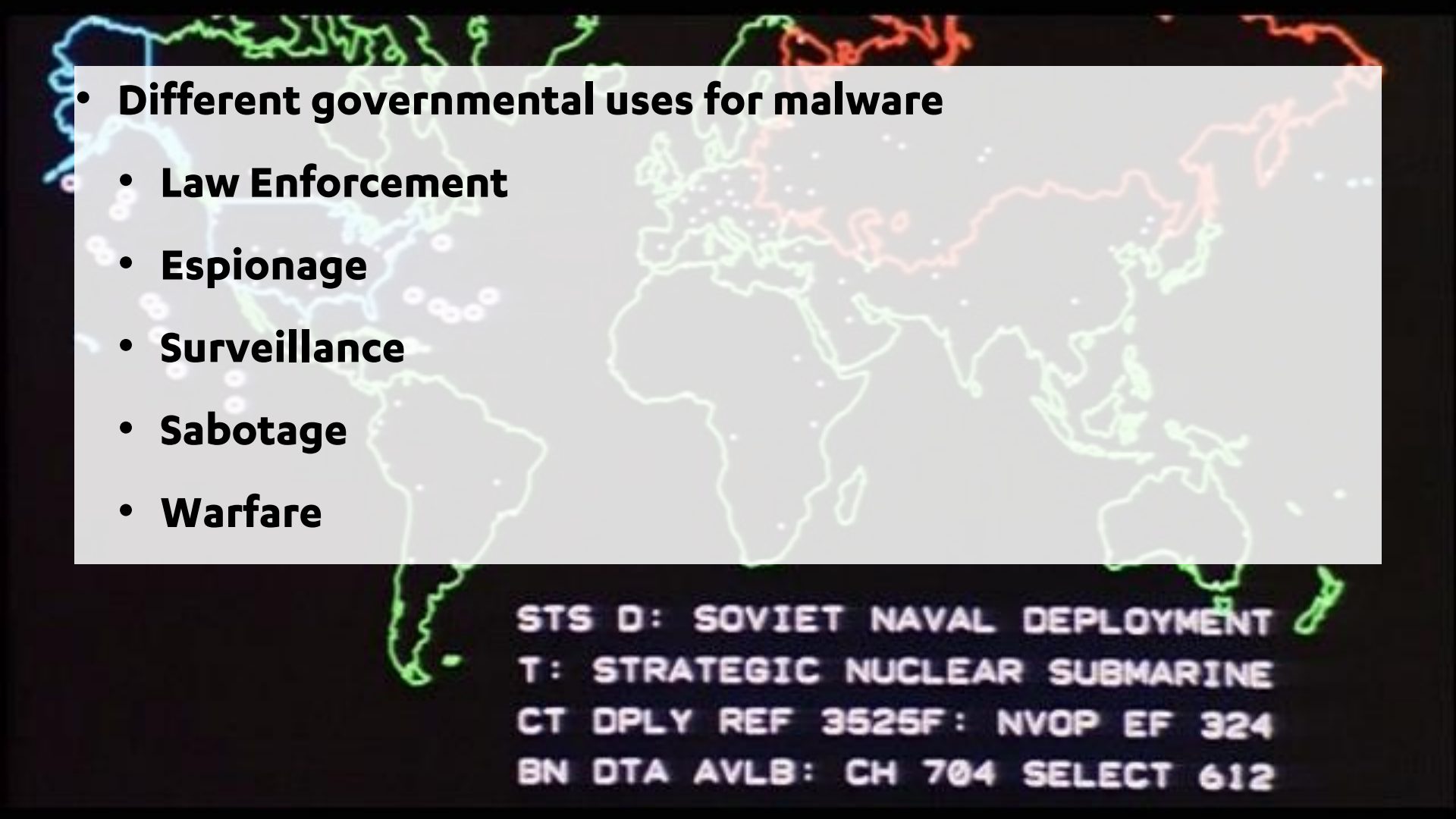
Following

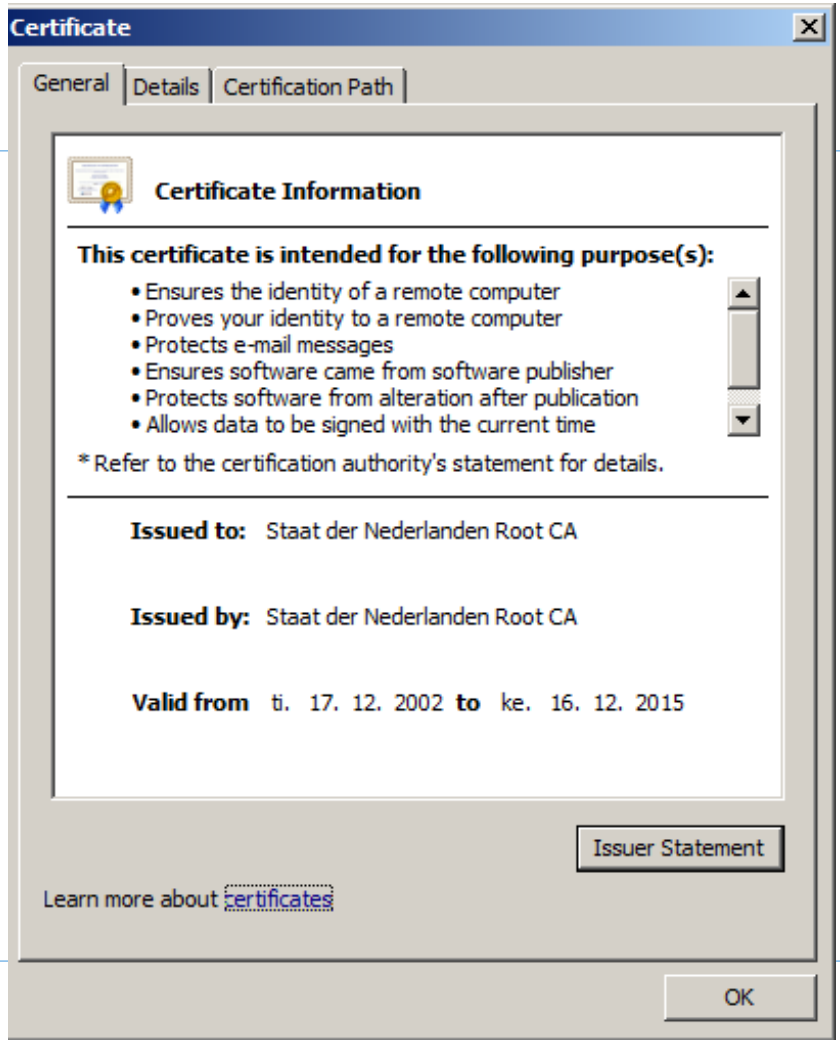
Dear medical infosec device researchers: hold onto your butts! a hospital bed with what appears to be a live patient

Reply Retweeted Favorite Share More

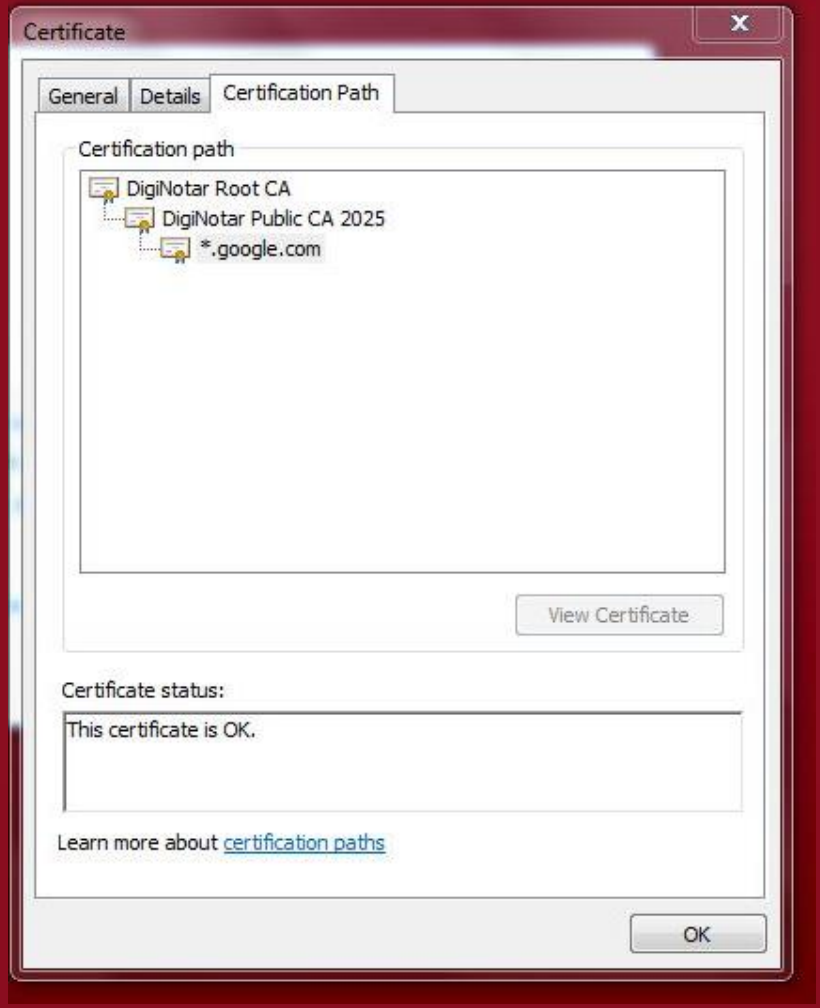


- Different governmental uses for malware
  - Law Enforcement
  - Espionage
  - Surveillance
  - Sabotage
  - Warfare



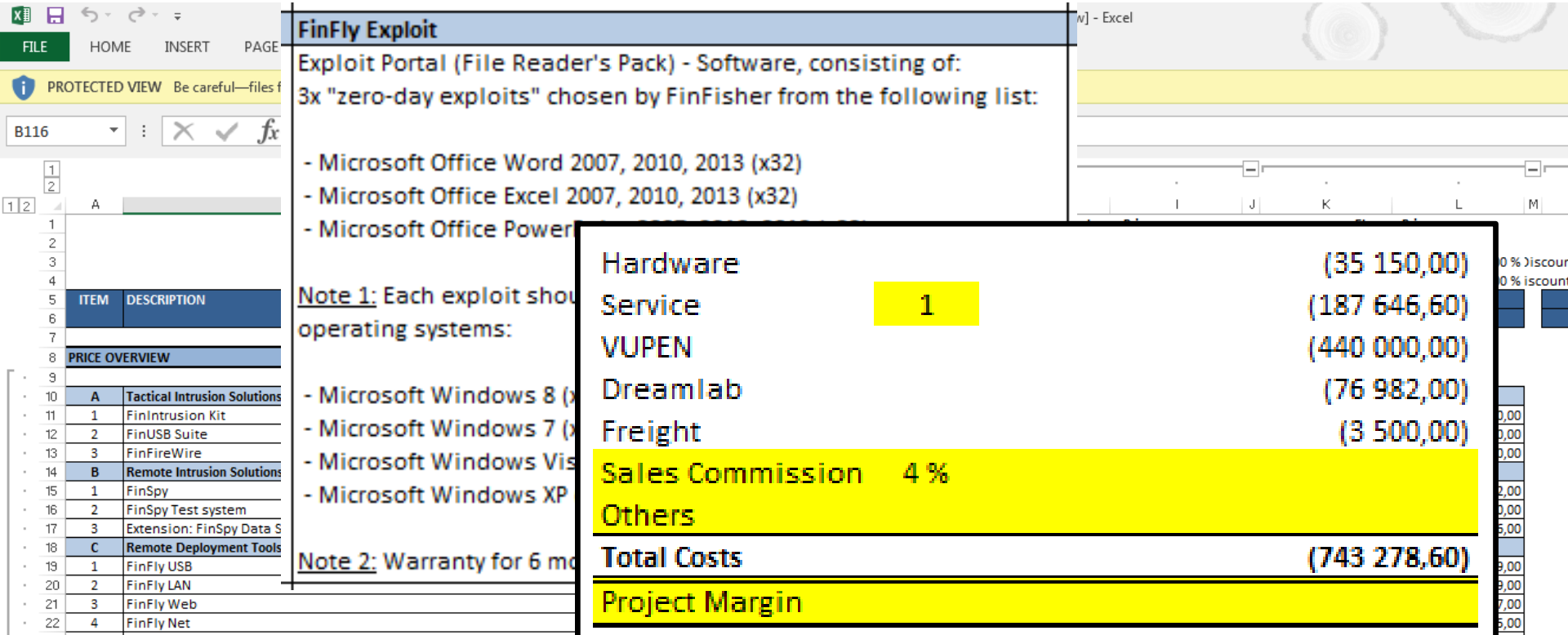

Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Ensures the identity of a remote computer
• Proves your identity to a remote computer
• Protects e-mail messages
• Ensures software came from software publisher
• Protects software from alteration after publication
• Allows data to be signed with the current time
* Refer to the certification authority's statement for details.
Issued to: Staat der Nederlanden Root CA
Issued by: Staat der Nederlanden Root CA
Valid from ti. 17. 12. 2002 to ke. 16. 12. 2015
Issuer Statement
Learn more about certificates
OK

*.google.com
*.mozilla.org
*.skype.com
*.torproject.org
login.live.com
login.yahoo.com
twitter.com
www.facebook.com
www.update.microsoft.com


Certificate
General
Details
Certification Path
Certification path
DigiNotar Root CA
DigiNotar Public CA 2025
*.google.com
View Certificate
Certificate status:
This certificate is OK.
Learn more about certification paths
OK

FinFisher (Gamma) + RCS (Hacking Team)

@GammaGroupPR



FinFly Exploit

Exploit Portal (File Reader's Pack) - Software, consisting of:
3x "zero-day exploits" chosen by FinFisher from the following list:

- Microsoft Office Word 2007, 2010, 2013 (x32)
- Microsoft Office Excel 2007, 2010, 2013 (x32)
- Microsoft Office Power

Note 1: Each exploit shou
operating systems:

- Microsoft Windows 8 (x
- Microsoft Windows 7 (x
- Microsoft Windows Vis
- Microsoft Windows XP

Note 2: Warranty for 6 mo

Hardware		(35 150,00)
Service	1	(187 646,60)
VUPEN		(440 000,00)
Dreamlab		(76 982,00)
Freight		(3 500,00)
Sales Commission	4 %	
Others		
Total Costs		**(743 278,60)**
Project Margin		

mjm

Martin J. Muench is the founder and Managing Director of Gamma International GmbH where he is heading the FinFisher product portfolio. In his past he was one of the core members behind the well-known Linux distribution BackTrack which is used world-wide by security professionals.

FinFly

Usage Example 2: Intelligence Agency

The customer deployed **FinFly ISP within the main Internet Service Provider** of their country. It was **combined with FinFly Web** to remotely **infect Targets that visited government offensive websites** by covertly injecting the FinFly Web code into the targeted websites.

2 SUPPORTED PLATFORMS

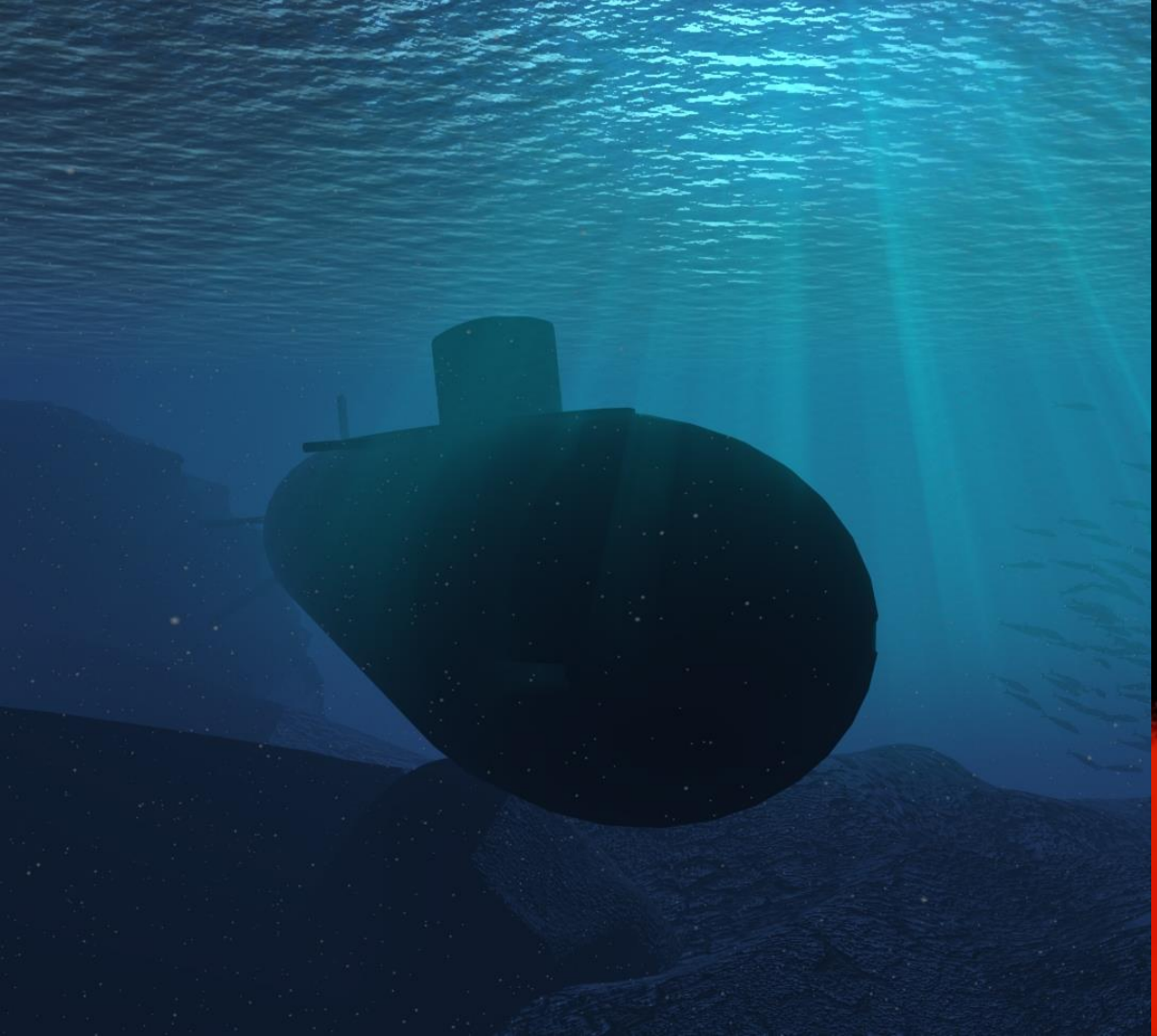
Platform	Supported Version	Latest Version on the Market
Android	2.x.x, 3.x.x, 4.0.x, 4.1.x, 4.2.x, 4.4.x	4.4.x
Blackberry	5.x, 6.x, 7.x	10.1
iOS Untethered Jailbreak required	4.3.x, 5.x, 6.x, 7.0.x	7.1
Symbian	Symbian ^3, Anna, Belle, S60 v5.x v3.x	Symbian ^3 Anna, Belle
Windows Mobile	6.1, 6.5	6.5
Windows Phone	Not Supported Yet	8

UAE, Bahrain, Saudi Arabia, Syria…

- Finfisher (Gamma)
- RCS (Hacking Team)
- DarkComet
- BlackShades
- Xtreme RAT
- Spynet
- Appin Security Group

Image Source: When Governments Hack Opponents: A Look at Actors and Technology, Citizen Lab + ICSI


27%
下午8:23
CODE4HK
+852 9678 8249
在線上
封鎖
新增
2014年9月16日
Check out this Android app designed by CODE4HK for the coordination of OCCUPYCENTRAL!
http://is.gd/bh4adz
下午8:16



THE HUNT IS ON.

SEAN CONNERY

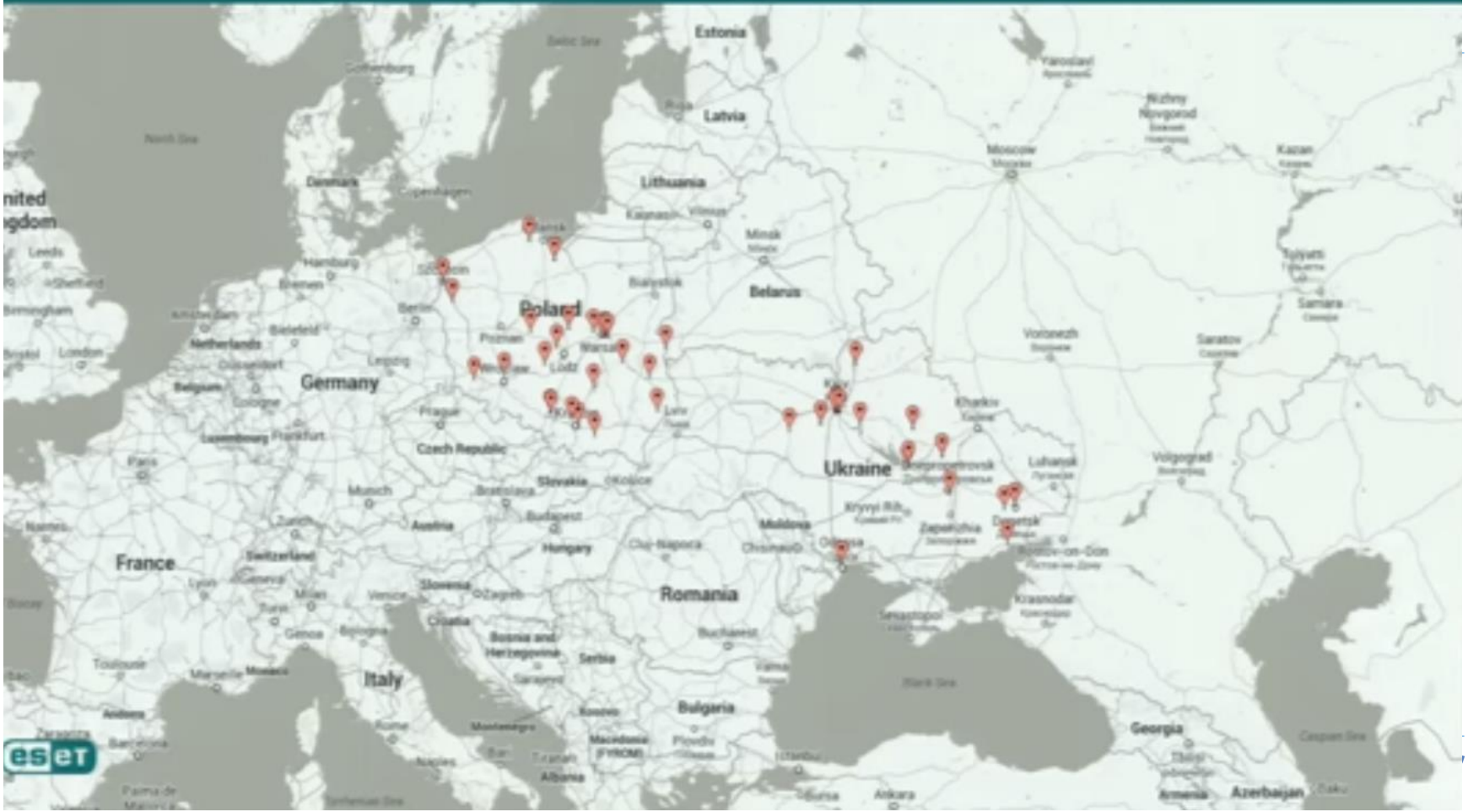
THE HUNT FOR RED OCTOBER

ALEC BALDWIN

CosmicDuke

F-Secure.

Targets in 2014 Campaigns



Masking "file.scr"

file.scr
Screen saver
917 KB

fdp.4102-hcraM-tropeR-ytiruceS-senilepiP-saG-eniarkU.scr

rcs.Ukraine-Gas-Pipelines-Security-Report-March-2014.pdf

F-Secure.

DIGITAL JUDO


The Online Arms Race
Mikko Hypponen
Twitter: @mikko
F-Secure.