Brian Buckley

Infragard Coordinator for Northern California

www.infragard.net

Cyber-Crash and Bleed

Anatomy of a Cyber Terrorist Attack on the Nation’s Hospital Infrastructure

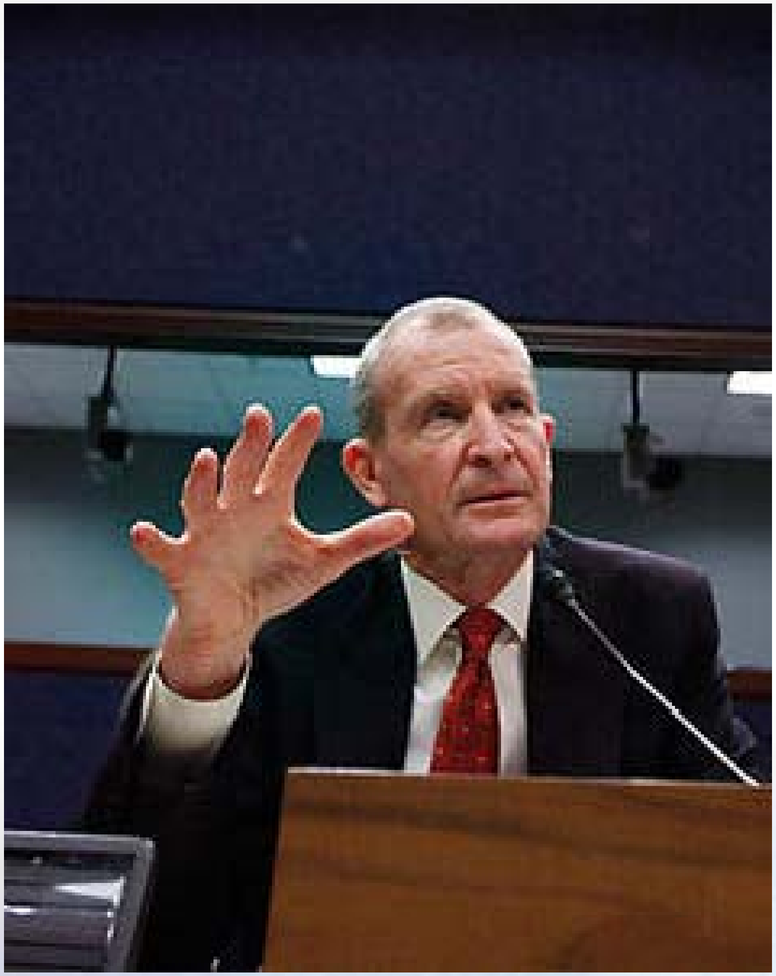
HBGary

WWW.HBGARY.COM

Evolving Risk Environment

- Hospitals are heavily reliant on information technology, everything is connected, more-so than perhaps any other industry
- Computer security has not been a high priority
- Attackers are able to get in, existing security doesn’t stop them, end of story.

Wake Up



http://www.csmonitor.com/USA/2010/0204/Google-cyber-attacks-a-wake-up-call-for-US-intel-chief-says

Google cyber attacks a 'wake-up' call

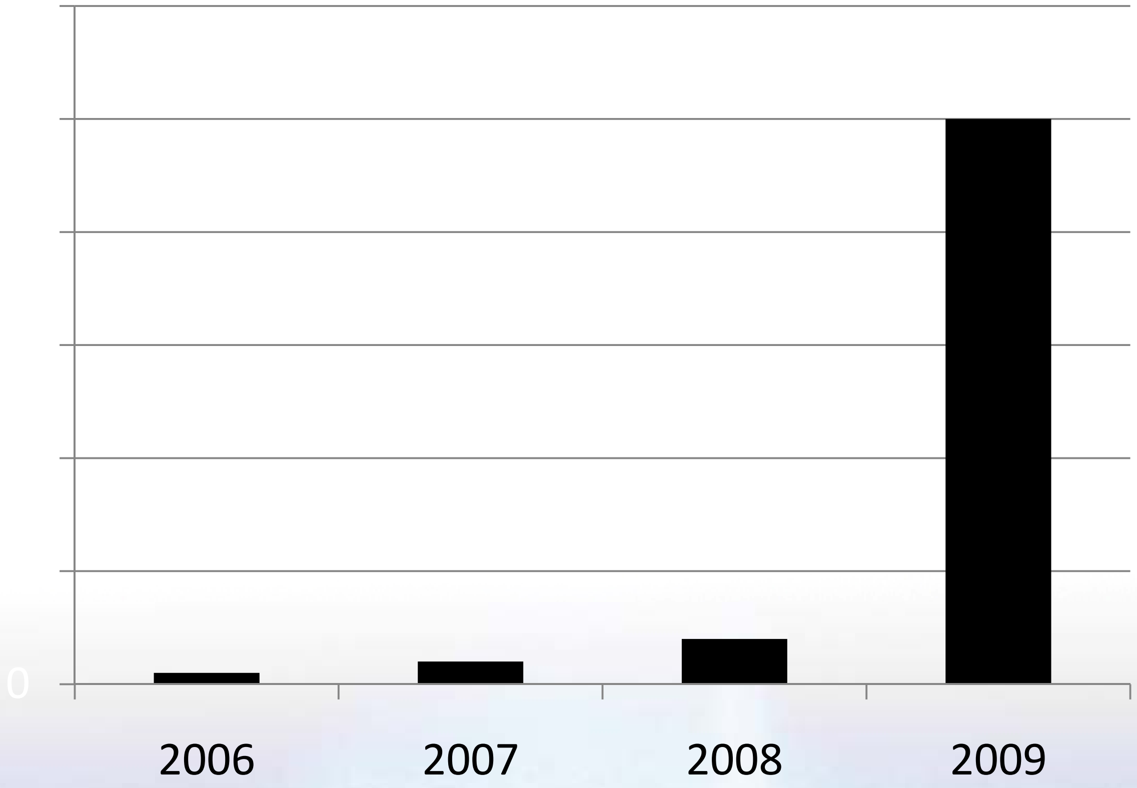
-Director of National Intelligence Dennis Blair
CNBC 2/2/10

IP is Leaving The Network Right Now

- Everybody here who manages an Enterprise with more than 10,000 nodes:

They are STEALING right now, as you watch this.

Signature based systems don’t scale



Anti-virus is rapidly losing credibility

Top 3 AV companies don’t detect 80% of new malware

Source: “**Eighty percent of new malware defeats antivirus**”, *ZDNet Australia*, July 19, 2006

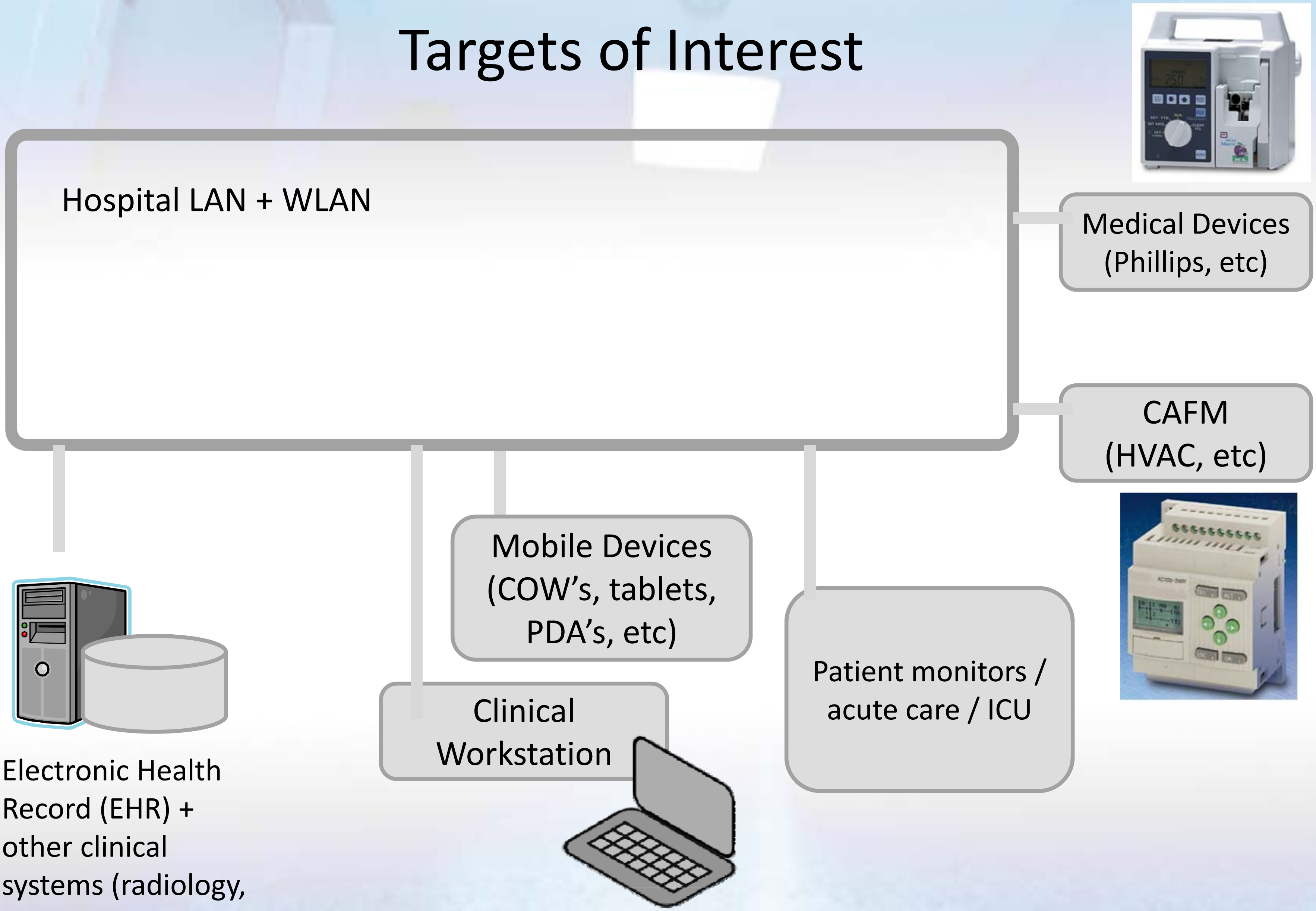
The sheer volume and complexity of computer viruses being released on the Internet today has the anti-virus industry on the defensive, experts say, underscoring the need for consumers to avoid relying on anti-virus software alone to keep their…computers safe and secure.

Source: “**Anti-Virus Firms Scrambling to Keep Up** ”, *The Washington Post, March 19, 2008*

The Target

- The terrorists intend to erode trust in technology used for managing patient care
- They intend to create a large scale event
- They intend to cause some deaths

Targets of Interest



Hospital LAN + WLAN

Medical Devices (Phillips, etc)

CAFM (HVAC, etc)

Mobile Devices (COW’s, tablets, PDA’s, etc)

Clinical Workstation

Patient monitors / acute care / ICU

Electronic Health Record (EHR) + other clinical systems (radiology, pharmacy, lab, etc)

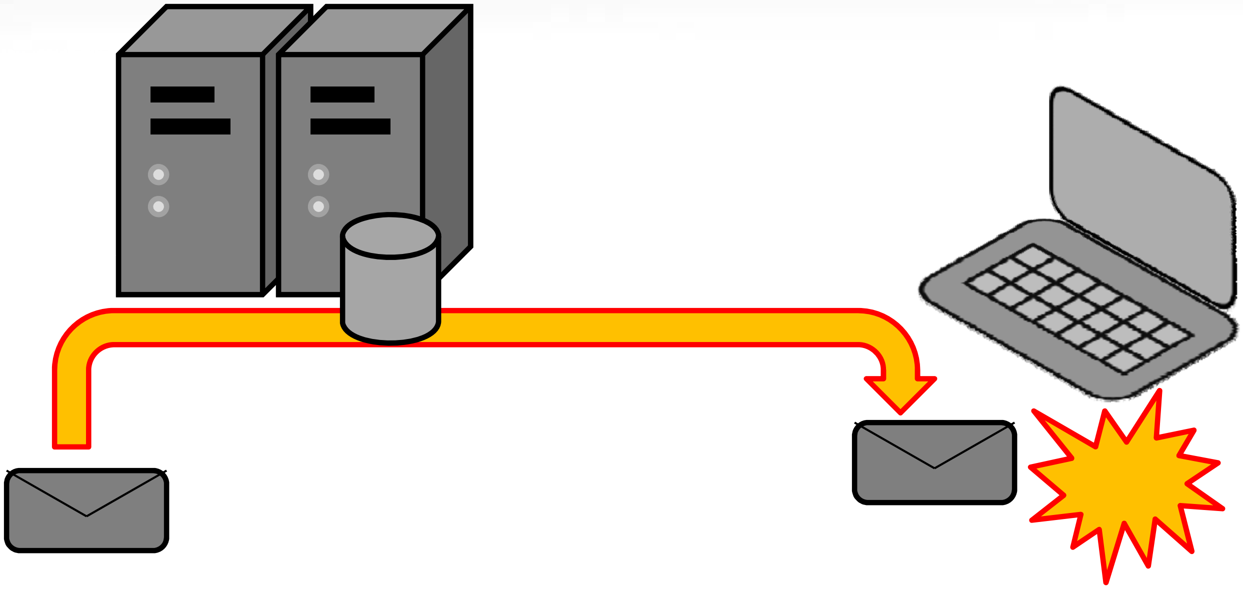
Phase-1 Recon

- Terrorists build a social map of all staff for all major hospitals
  - Focus in on Hospitals that have more than 10,000 nodes in their networks
  - These Hospitals are so reliant on technology that an attack will cause a major disruption to health care

Attack Vectors

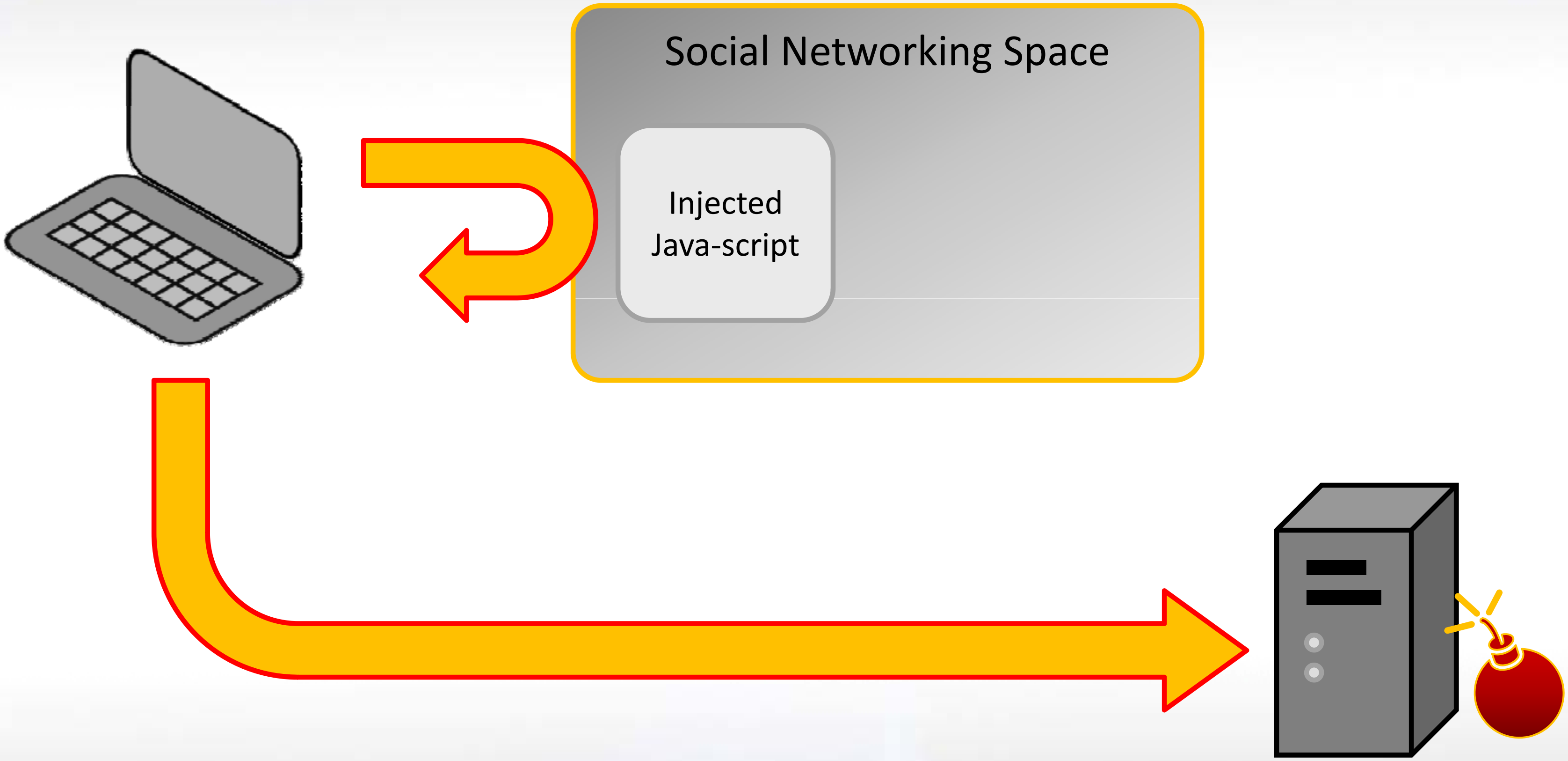
- Spear-phishing
  - Booby-trapped documents
  - Fake-Links to drive-by websites
- Trap postings on industry-focused social networks
  - Forums, Groups (clinician list-servs, AMDIS, web forums)
- SQL injections into web-based portals
  - Employee benefit portals, external labs, etc.

Boobytrapped Documents



- Single most effective *focused* attack today
- Human crafts text

Web-based attack

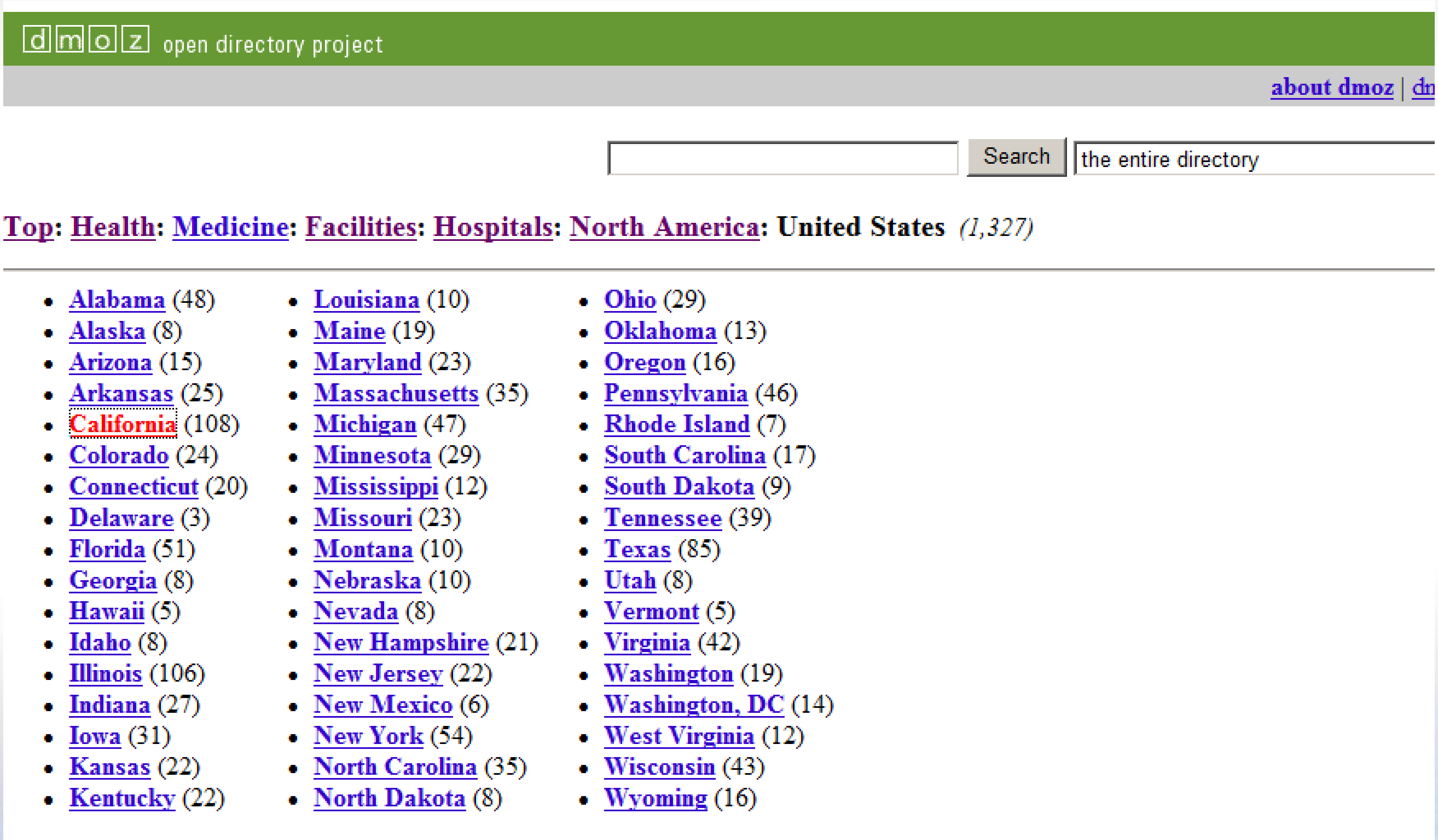


- Used heavily for large scale infections
- Social network targeting is possible

Scraping the ‘Net for emails

Attackers use search engines, industry databases, and intelligent guessing to map out the domains of all major hospitals.

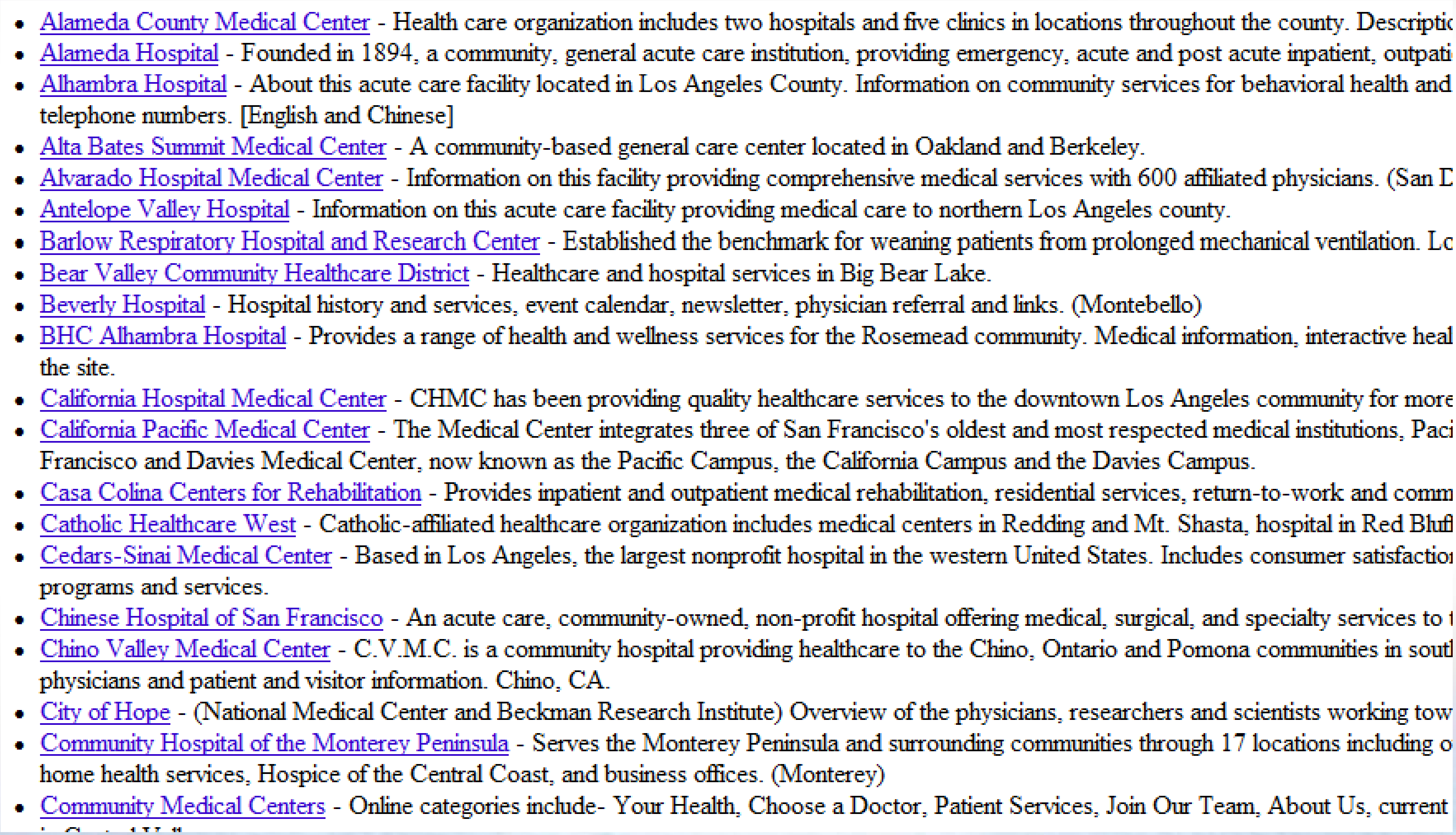
DMOZ



Top: Health: Medicine: Facilities: Hospitals: North America: United States *(1,327)*

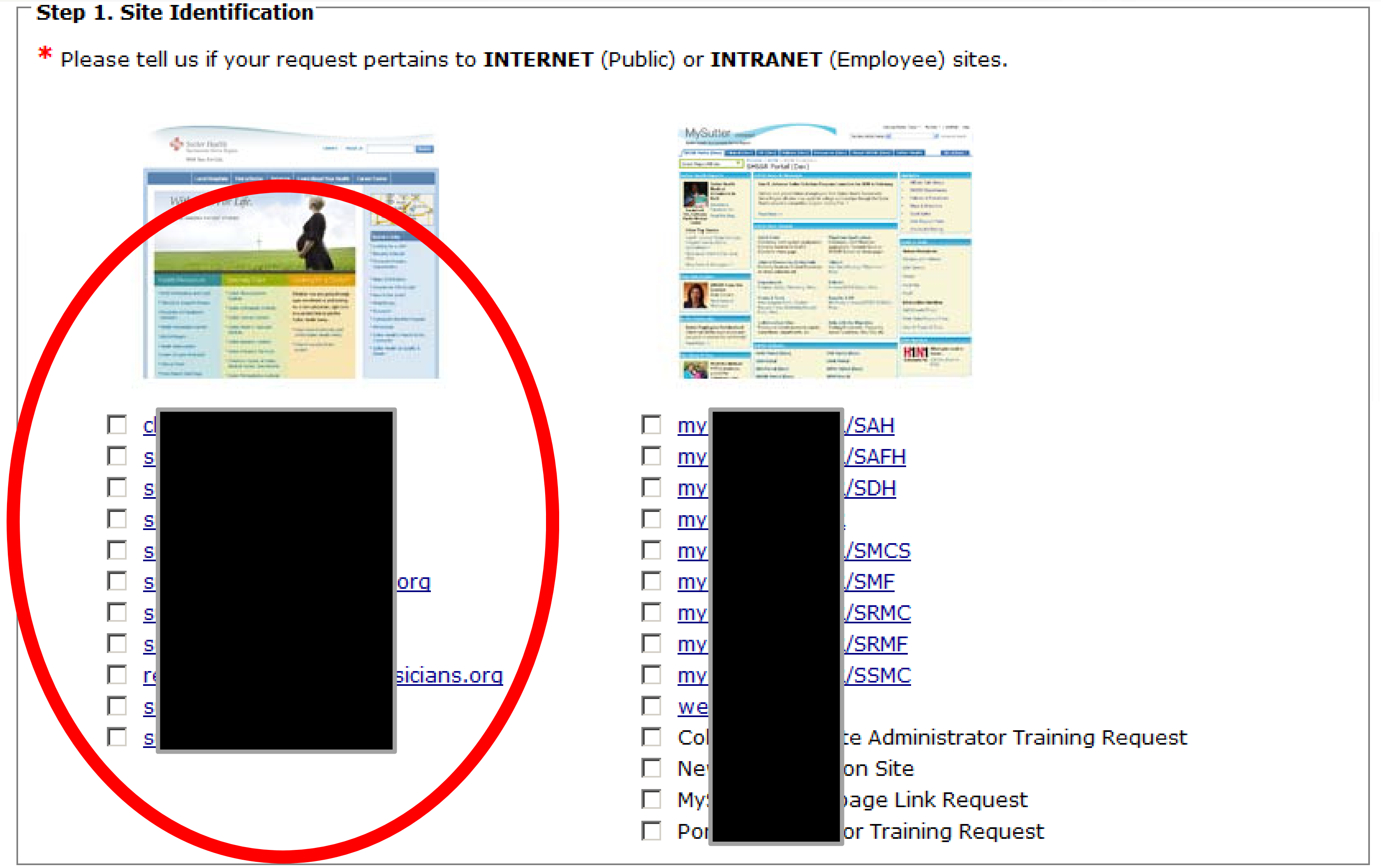
- Alabama (48)
- Alaska (8)
- Arizona (15)
- Arkansas (25)
- California (108)
- Colorado (24)
- Connecticut (20)
- Delaware (3)
- Florida (51)
- Georgia (8)
- Hawaii (5)
- Idaho (8)
- Illinois (106)
- Indiana (27)
- Iowa (31)
- Kansas (22)
- Kentucky (22)
- Louisiana (10)
- Maine (19)
- Maryland (23)
- Massachusetts (35)
- Michigan (47)
- Minnesota (29)
- Mississippi (12)
- Missouri (23)
- Montana (10)
- Nebraska (10)
- Nevada (8)
- New Hampshire (21)
- New Jersey (22)
- New Mexico (6)
- New York (54)
- North Carolina (35)
- North Dakota (8)
- Ohio (29)
- Oklahoma (13)
- Oregon (16)
- Pennsylvania (46)
- Rhode Island (7)
- South Carolina (17)
- South Dakota (9)
- Tennessee (39)
- Texas (85)
- Utah (8)
- Vermont (5)
- Virginia (42)
- Washington (19)
- Washington, DC (14)
- West Virginia (12)
- Wisconsin (43)
- Wyoming (16)

Over 1,000 in California…



- Alameda County Medical Center - Health care organization includes two hospitals and five clinics in locations throughout the county. Descriptic
- Alameda Hospital - Founded in 1894, a community, general acute care institution, providing emergency, acute and post acute inpatient, outpati
- Alhambra Hospital - About this acute care facility located in Los Angeles County. Information on community services for behavioral health and telephone numbers. [English and Chinese]
- Alta Bates Summit Medical Center - A community-based general care center located in Oakland and Berkeley.
- Alvarado Hospital Medical Center - Information on this facility providing comprehensive medical services with 600 affiliated physicians. (San D
- Antelope Valley Hospital - Information on this acute care facility providing medical care to northern Los Angeles county.
- Barlow Respiratory Hospital and Research Center - Established the benchmark for weaning patients from prolonged mechanical ventilation. Lc
- Bear Valley Community Healthcare District - Healthcare and hospital services in Big Bear Lake.
- Beverly Hospital - Hospital history and services, event calendar, newsletter, physician referral and links. (Montebello)
- BHC Alhambra Hospital - Provides a range of health and wellness services for the Rosemead community. Medical information, interactive heal the site.
- California Hospital Medical Center - CHMC has been providing quality healthcare services to the downtown Los Angeles community for more
- California Pacific Medical Center - The Medical Center integrates three of San Francisco's oldest and most respected medical institutions, Paci Francisco and Davies Medical Center, now known as the Pacific Campus, the California Campus and the Davies Campus.
- Casa Colina Centers for Rehabilitation - Provides inpatient and outpatient medical rehabilitation, residential services, return-to-work and comm
- Catholic Healthcare West - Catholic-affiliated healthcare organization includes medical centers in Redding and Mt. Shasta, hospital in Red Bluf
- Cedars-Sinai Medical Center - Based in Los Angeles, the largest nonprofit hospital in the western United States. Includes consumer satisfactio programs and services.
- Chinese Hospital of San Francisco - An acute care, community-owned, non-profit hospital offering medical, surgical, and specialty services to t
- Chino Valley Medical Center - C.V.M.C. is a community hospital providing healthcare to the Chino, Ontario and Pomona communities in soutl physicians and patient and visitor information. Chino, CA.
- City of Hope - (National Medical Center and Beckman Research Institute) Overview of the physicians, researchers and scientists working tow
- Community Hospital of the Monterey Peninsula - Serves the Monterey Peninsula and surrounding communities through 17 locations including o home health services, Hospice of the Central Coast, and business offices. (Monterey)
- Community Medical Centers - Online categories include- Your Health, Choose a Doctor, Patient Services, Join Our Team, About Us, current

[redacted] web-based portal is quite helpful



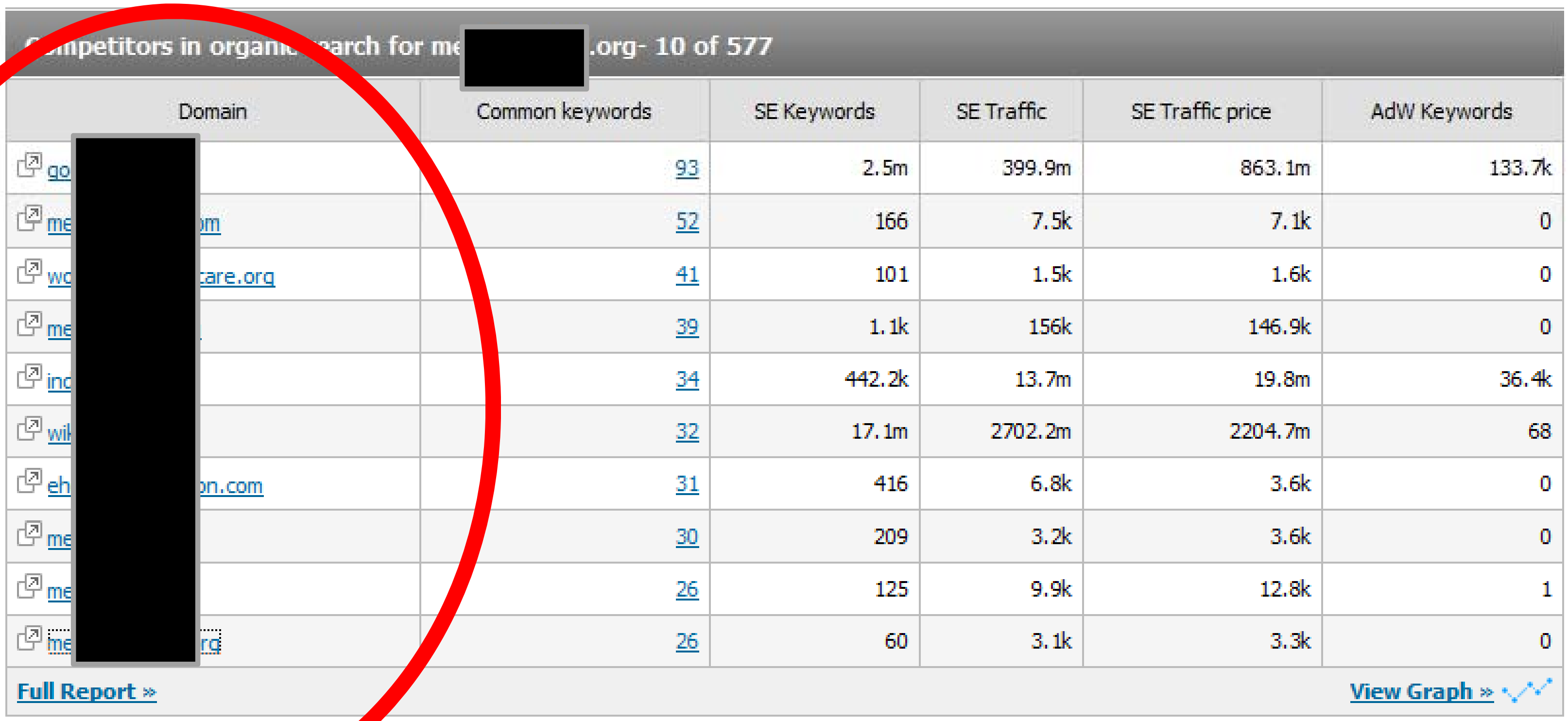
Step 1. Site Identification

* Please tell us if your request pertains to **INTERNET** (Public) or **INTRANET** (Employee) sites.

□ cl[redacted]
□ s
□ s
□ s
□ s
□ s org
□ s
□ s
□ r sicians.org
□ s
□ s

□ my[redacted]/SAH
□ my /SAFH
□ my /SDH
□ my .
□ my /SMCS
□ my /SMF
□ my /SRMC
□ my /SRMF
□ my /SSMC
□ we
□ Col te Administrator Training Request
□ Ne on Site
□ My age Link Request
□ Por or Training Request

Using SEO tracker on [redacted]



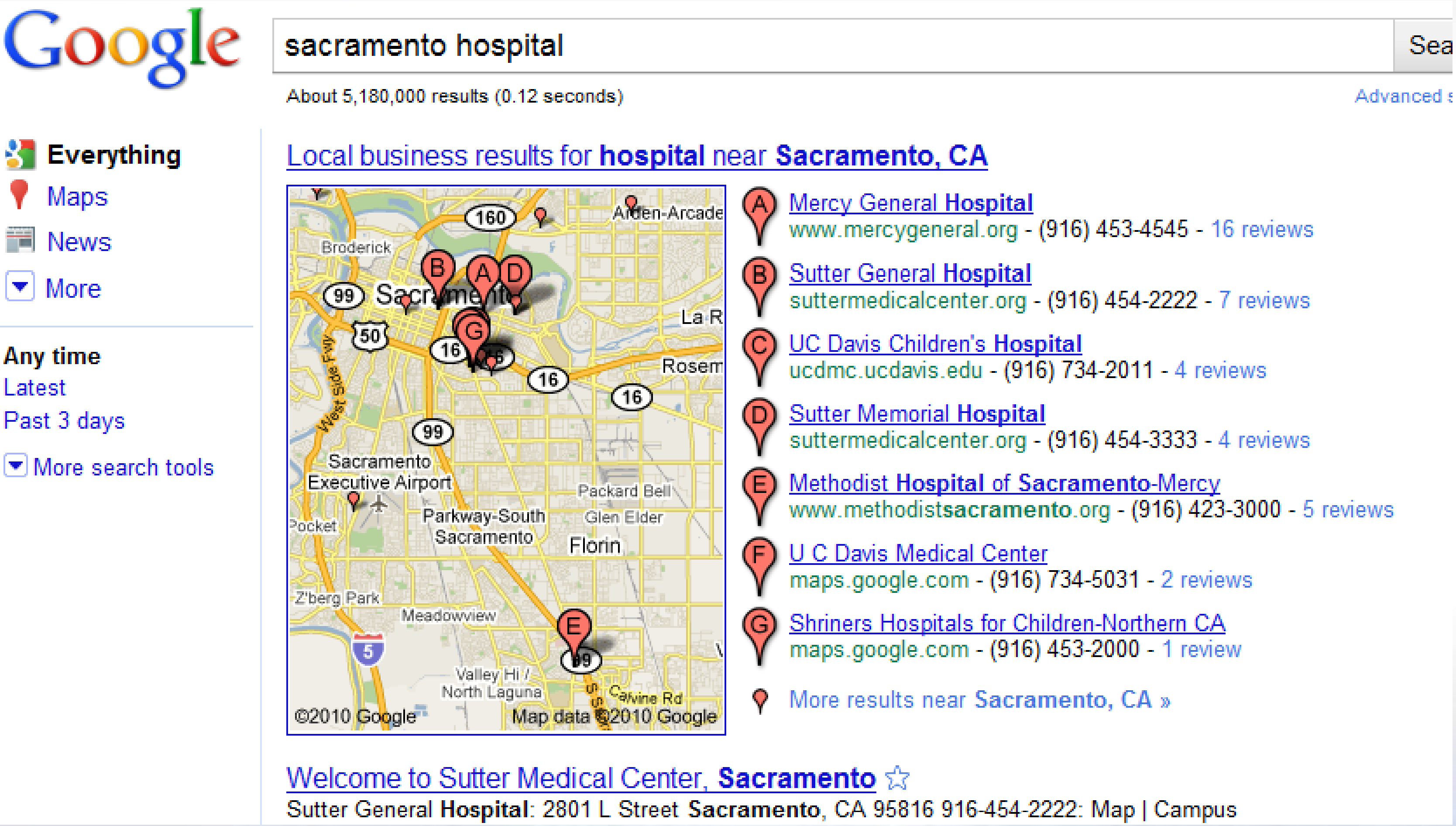
Competitors in organic search for me[redacted].org- 10 of 577

Domain	Common keywords	SE Keywords	SE Traffic	SE Traffic price	AdW Keywords
go[redacted]	93	2.5m	399.9m	863.1m	133.7k
me[redacted]om	52	166	7.5k	7.1k	0
wo[redacted]care.org	41	101	1.5k	1.6k	0
me[redacted].	39	1.1k	156k	146.9k	0
in[redacted]	34	442.2k	13.7m	19.8m	36.4k
wi[redacted]	32	17.1m	2702.2m	2204.7m	68
eh[redacted]on.com	31	416	6.8k	3.6k	0
me[redacted]	30	209	3.2k	3.6k	0
me[redacted]	26	125	9.9k	12.8k	1
me[redacted]rg	26	60	3.1k	3.3k	0

Full Report »

View Graph »

Google Maps on Sacramento



sacramento hospital

About 5,180,000 results (0.12 seconds)

Advanced s

Any time
Latest
Past 3 days
More search tools

Local business results for **hospital** near **Sacramento, CA**

A Mercy General **Hospital**
www.mercygeneral.org - (916) 453-4545 - 16 reviews

B Sutter General **Hospital**
suttermedicalcenter.org - (916) 454-2222 - 7 reviews

C UC Davis Children's **Hospital**
ucdmc.ucdavis.edu - (916) 734-2011 - 4 reviews

D Sutter Memorial **Hospital**
suttermedicalcenter.org - (916) 454-3333 - 4 reviews

E Methodist **Hospital** of **Sacramento**-Mercy
www.methodist**sacramento**.org - (916) 423-3000 - 5 reviews

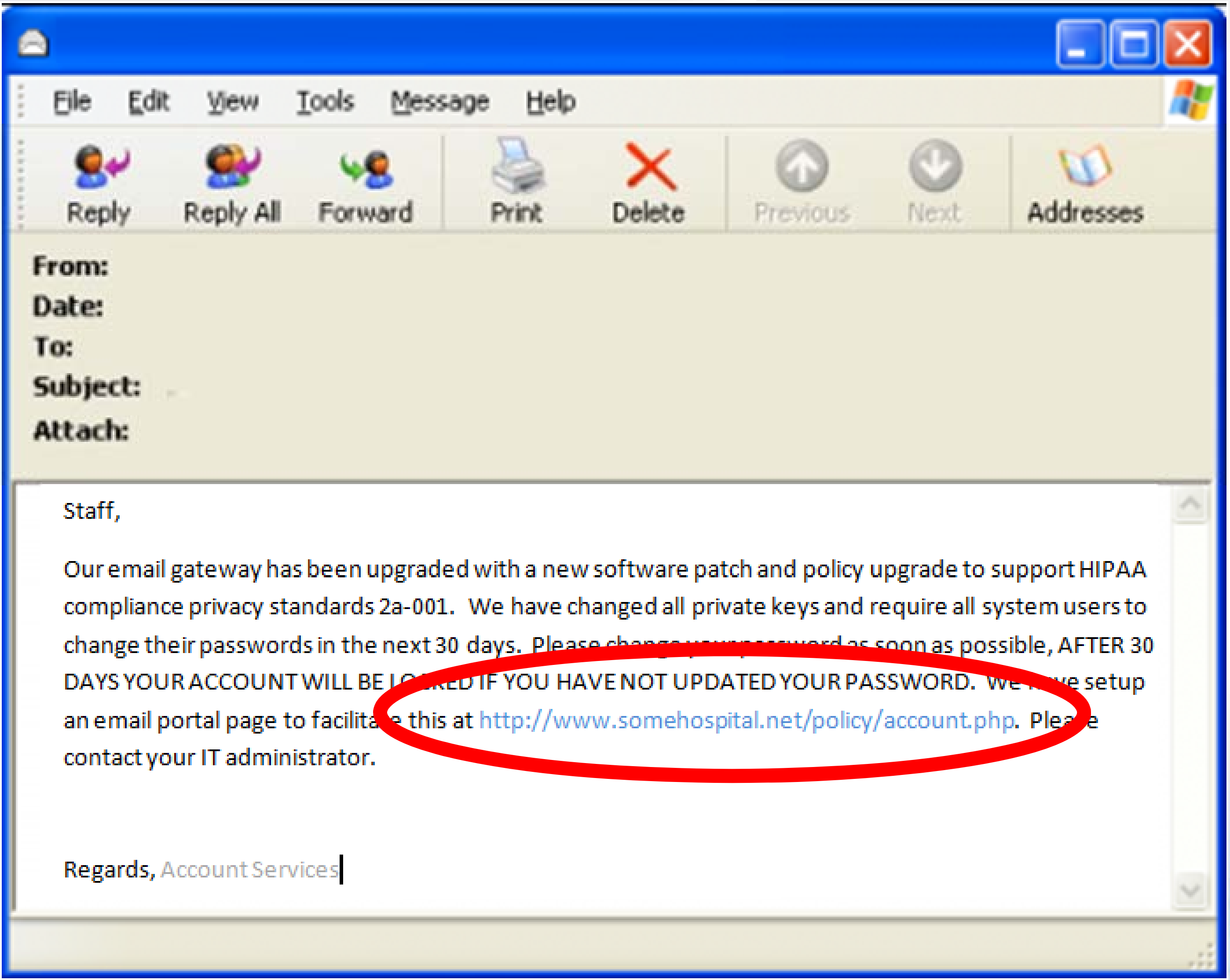
F U C Davis Medical Center
maps.google.com - (916) 734-5031 - 2 reviews

G Shriners Hospitals for Children-Northern CA
maps.google.com - (916) 453-2000 - 1 review

More results near **Sacramento, CA** »

Welcome to Sutter Medical Center, **Sacramento** ☆
Sutter General **Hospital**: 2801 L Street **Sacramento**, CA 95816 916-454-2222: Map | Campus

you *know* they will click it



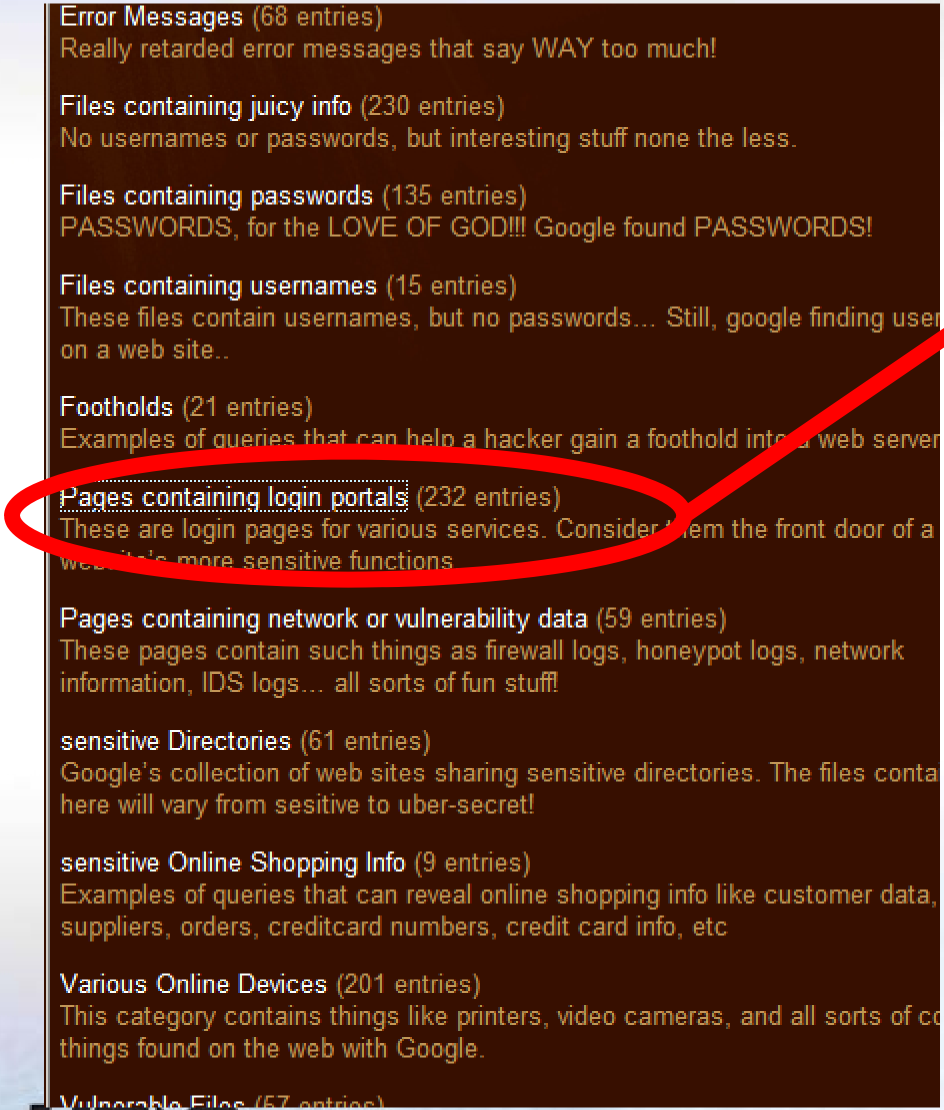
From:
Date:
To:
Subject:
Attach:

Staff,

Our email gateway has been upgraded with a new software patch and policy upgrade to support HIPAA compliance privacy standards 2a-001. We have changed all private keys and require all system users to change their passwords in the next 30 days. Please change your password as soon as possible, AFTER 30 DAYS YOUR ACCOUNT WILL BE LOCKED IF YOU HAVE NOT UPDATED YOUR PASSWORD. We have setup an email portal page to facilitate this at http://www.somehospital.net/policy/account.php. Please contact your IT administrator.

Regards, Account Services

Google Web Portal Search



Error Messages (68 entries)
Really retarded error messages that say WAY too much!

Files containing juicy info (230 entries)
No usernames or passwords, but interesting stuff none the less.

Files containing passwords (135 entries)
PASSWORDS, for the LOVE OF GOD!!! Google found PASSWORDS!

Files containing usernames (15 entries)
These files contain usernames, but no passwords... Still, google finding user on a web site..

Footholds (21 entries)
Examples of queries that can help a hacker gain a foothold into a web server

Pages containing login portals (232 entries)
These are login pages for various services. Consider them the front door of a web site's more sensitive functions.

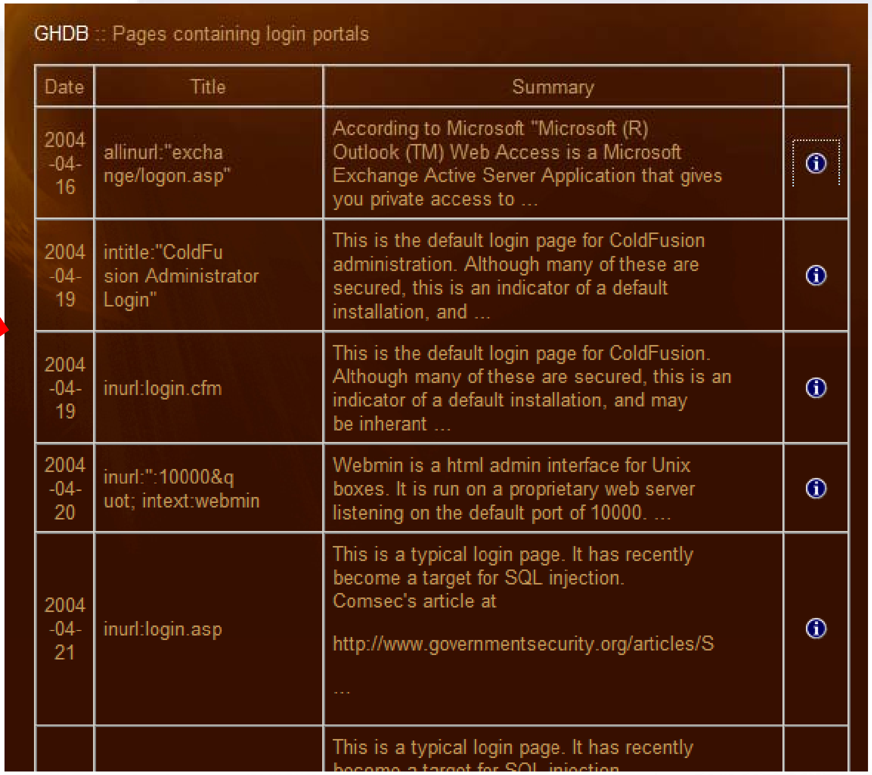
Pages containing network or vulnerability data (59 entries)
These pages contain such things as firewall logs, honeypot logs, network information, IDS logs... all sorts of fun stuff!

sensitive Directories (61 entries)
Google's collection of web sites sharing sensitive directories. The files conta here will vary from sesitive to uber-secret!

sensitive Online Shopping Info (9 entries)
Examples of queries that can reveal online shopping info like customer data, suppliers, orders, creditcard numbers, credit card info, etc

Various Online Devices (201 entries)
This category contains things like printers, video cameras, and all sorts of co things found on the web with Google.

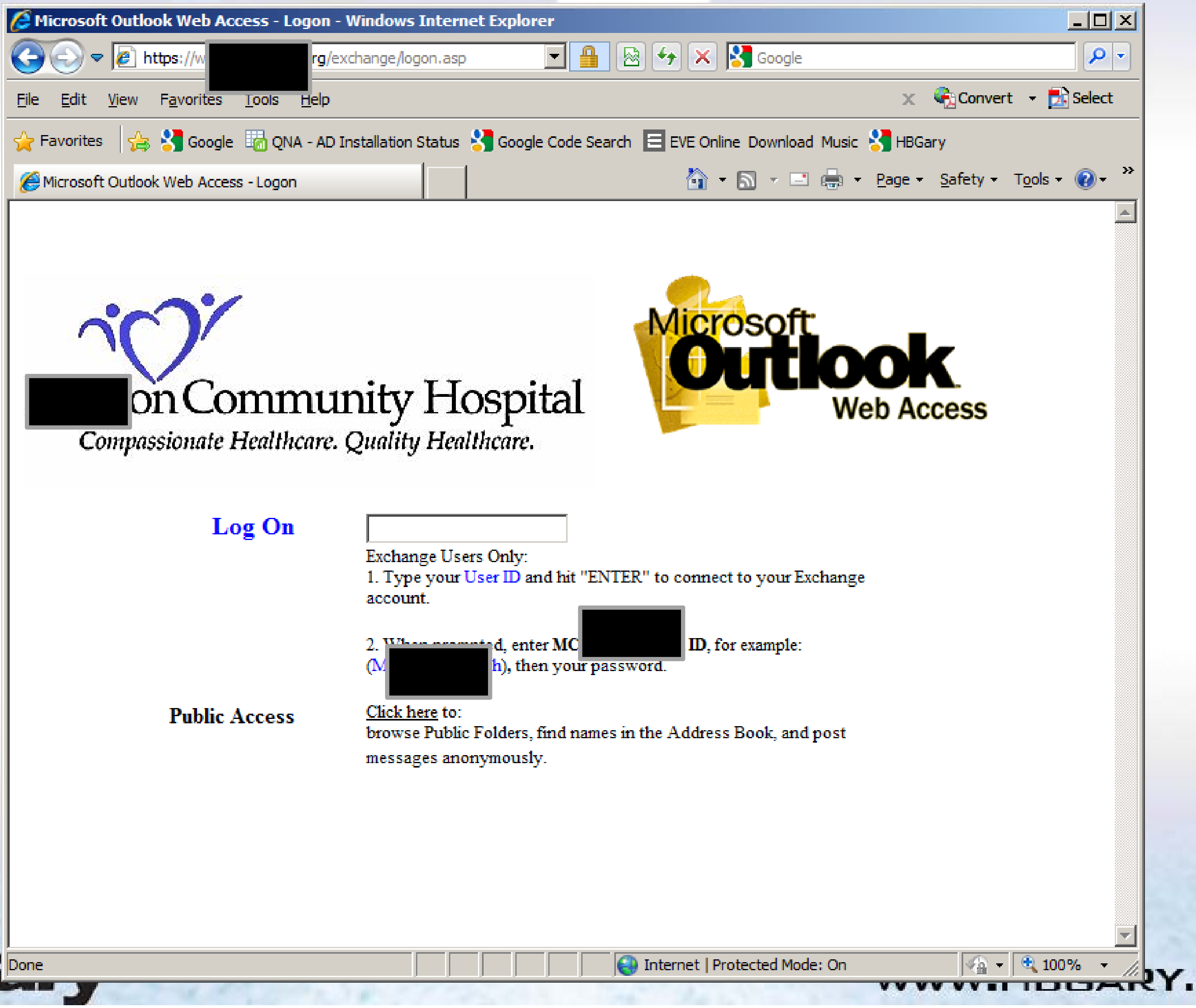
Vulnerable Files (57 entries)



GHDB :: Pages containing login portals

Date	Title	Summary	
2004-04-16	allinurl:"exchange/logon.asp"	According to Microsoft "Microsoft (R) Outlook (TM) Web Access is a Microsoft Exchange Active Server Application that gives you private access to ...	ⓘ
2004-04-19	intitle:"ColdFusion Administrator Login"	This is the default login page for ColdFusion administration. Although many of these are secured, this is an indicator of a default installation, and ...	ⓘ
2004-04-19	inurl:login.cfm	This is the default login page for ColdFusion. Although many of these are secured, this is an indicator of a default installation, and may be inherant ...	ⓘ
2004-04-20	inurl:":10000&quot; intext:webmin	Webmin is a html admin interface for Unix boxes. It is run on a proprietary web server listening on the default port of 10000. ...	ⓘ
2004-04-21	inurl:login.asp	This is a typical login page. It has recently become a target for SQL injection. Comsec's article at http://www.governmentsecurity.org/articles/S ...	ⓘ
		This is a typical login page. It has recently become a target for SQL injection	

My First Hit on allinurl:"exchange/logon.asp" – I haven't even started yet…


Microsoft Outlook Web Access - Logon - Windows Internet Explorer
https://w[redacted]rg/exchange/logon.asp
Google
File Edit View Favorites Tools Help
Convert Select
Favorites Google QNA - AD Installation Status Google Code Search EVE Online Download Music HBGary
Microsoft Outlook Web Access - Logon
Page Safety Tools
[redacted]on Community Hospital
Compassionate Healthcare. Quality Healthcare.
Microsoft Outlook Web Access
Done
Internet | Protected Mode: On
100%

Log On

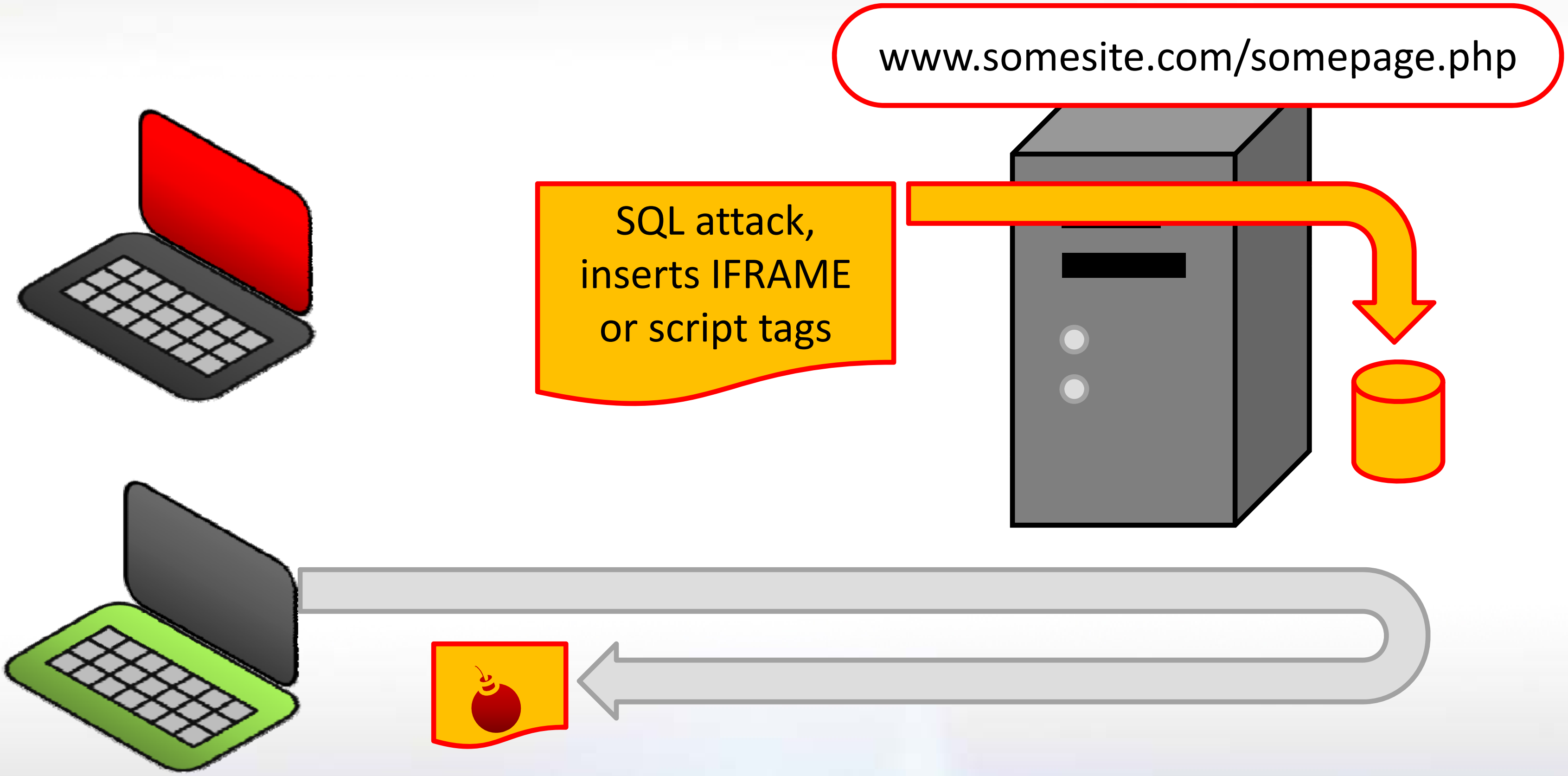
Exchange Users Only:
1. Type your User ID and hit "ENTER" to connect to your Exchange account.

2. W[redacted]d, enter MC[redacted] ID, for example:
(M[redacted]h), then your password.

Public Access

Click here to:
browse Public Folders, find names in the Address Book, and post messages anonymously.

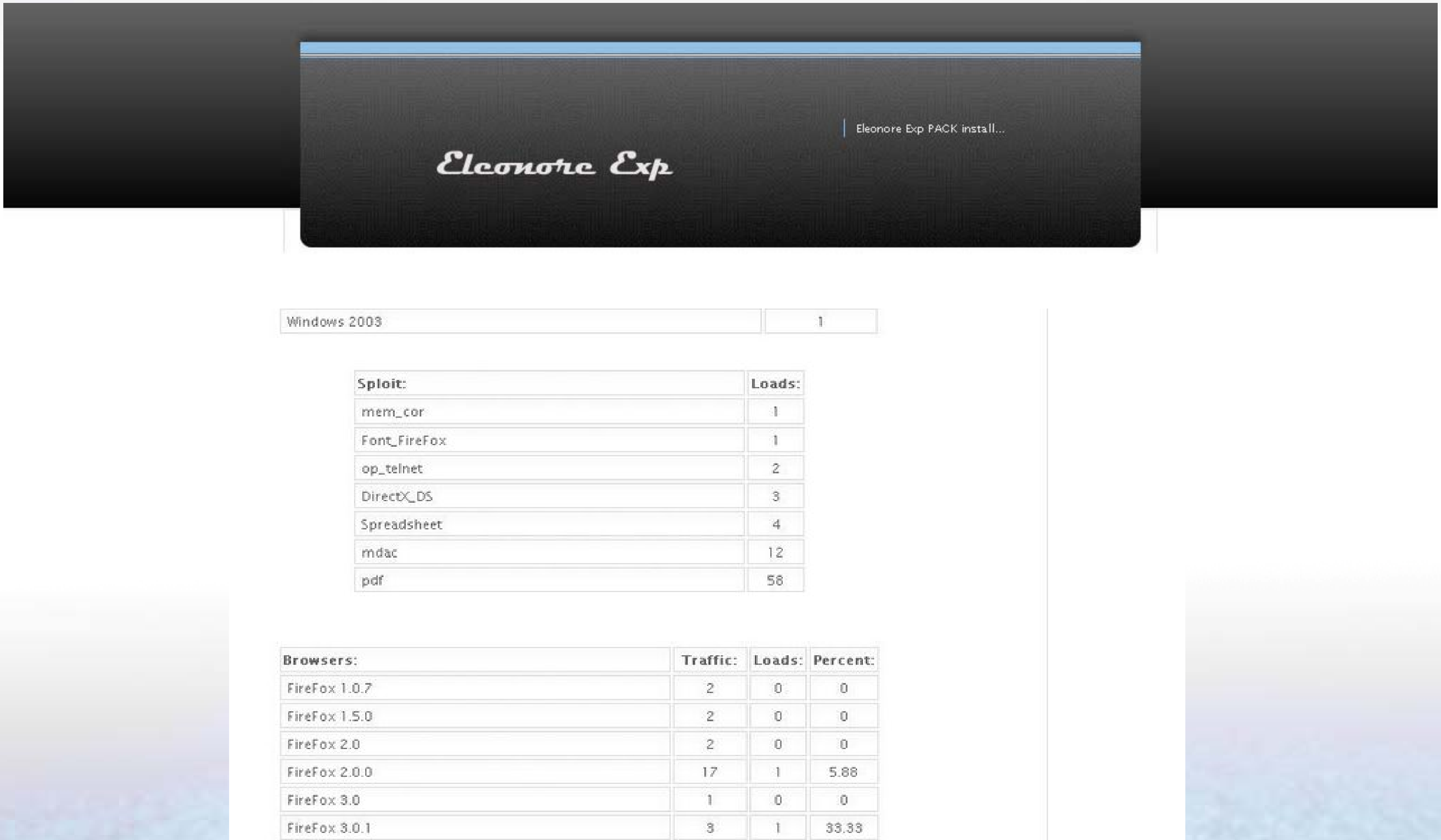
SQL Injection


www.somesite.com/somepage.php
SQL attack, inserts IFRAME or script tags

Cyber Weapons Market

- Terrorist’s don’t need to have expert hackers, they can just buy exploits for money
  - Fully weaponized and ready to use
  - Mostly developed out of the Eastern Bloc

Eleonore (exploit pack)



Eleonore Exp

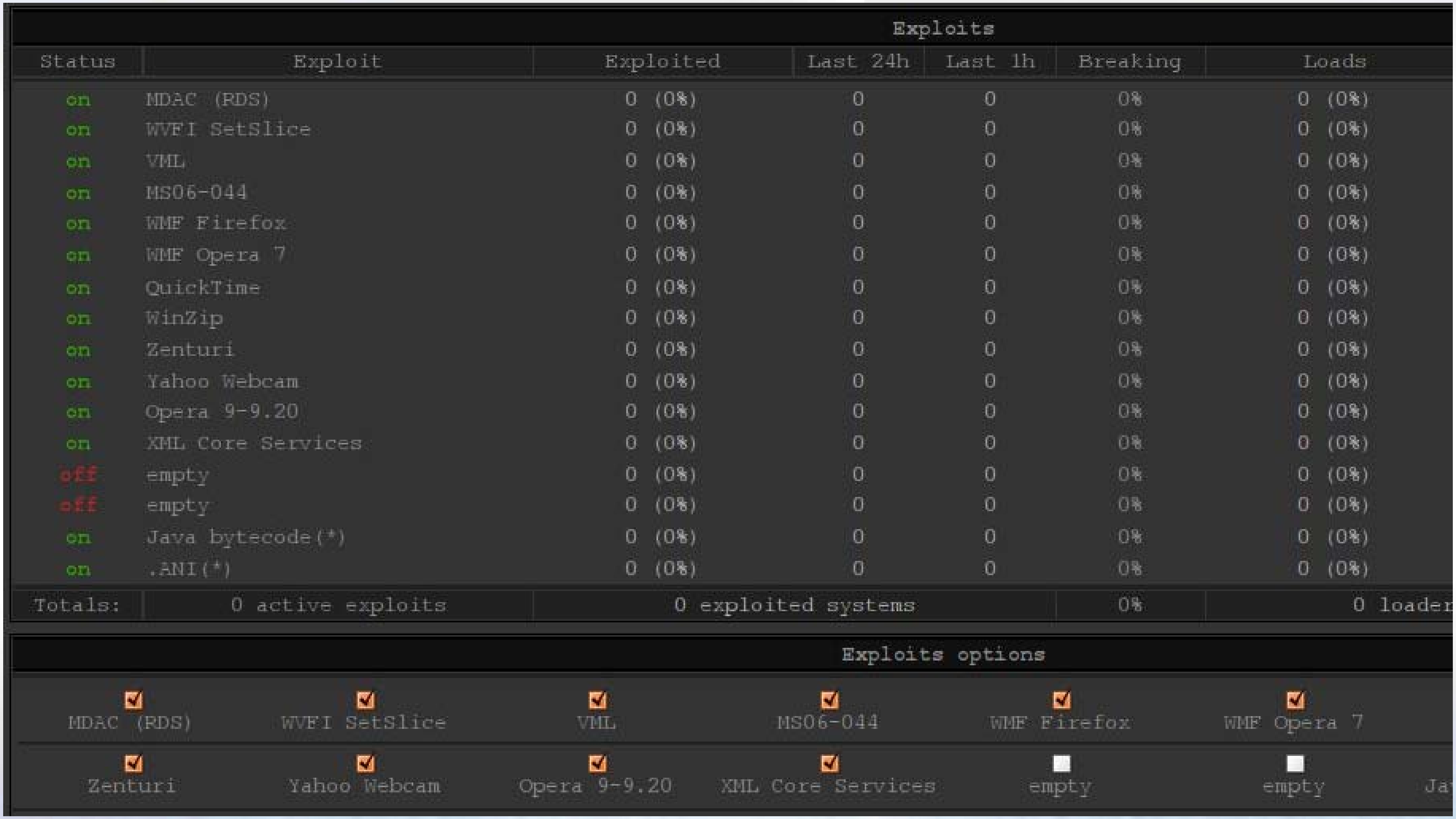
Eleonore Exp PACK install...

Windows 2003	1

Sploit:	Loads:
mem_cor	1
Font_FireFox	1
op_telnet	2
DirectX_DS	3
Spreadsheet	4
mdac	12
pdf	58

Browsers:	Traffic:	Loads:	Percent:
FireFox 1.0.7	2	0	0
FireFox 1.5.0	2	0	0
FireFox 2.0	2	0	0
FireFox 2.0.0	17	1	5.88
FireFox 3.0	1	0	0
FireFox 3.0.1	3	1	33.33

Tornado (exploit pack)



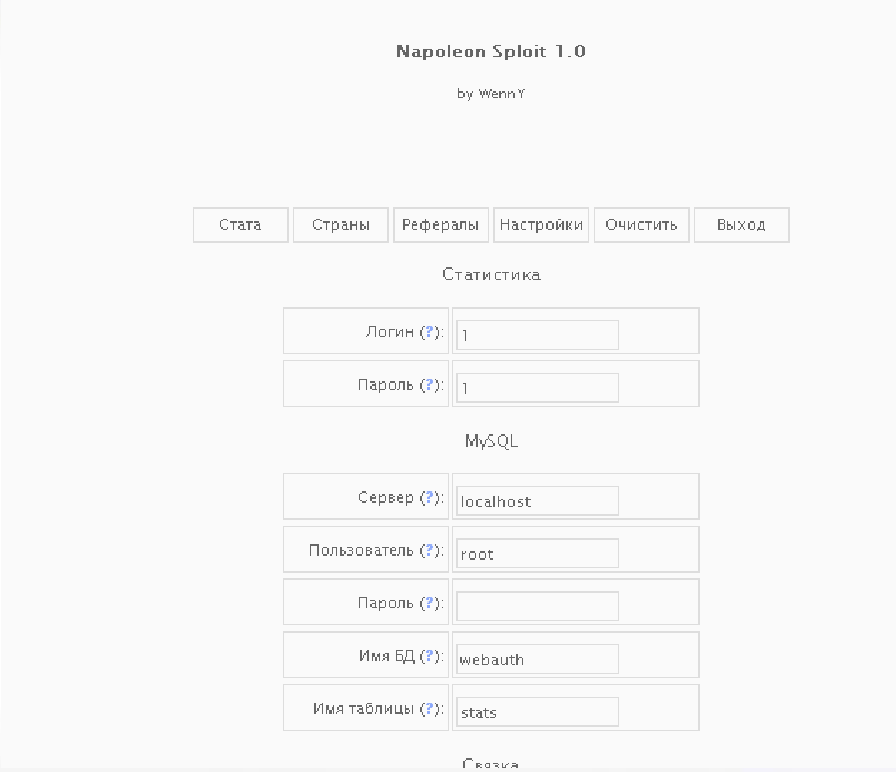
Exploits

Status	Exploit	Exploited	Last 24h	Last 1h	Breaking	Loads
on	MDAC (RDS)	0 (0%)	0	0	0%	0 (0%)
on	WVFI SetSlice	0 (0%)	0	0	0%	0 (0%)
on	VML	0 (0%)	0	0	0%	0 (0%)
on	MS06-044	0 (0%)	0	0	0%	0 (0%)
on	WMF Firefox	0 (0%)	0	0	0%	0 (0%)
on	WMF Opera 7	0 (0%)	0	0	0%	0 (0%)
on	QuickTime	0 (0%)	0	0	0%	0 (0%)
on	WinZip	0 (0%)	0	0	0%	0 (0%)
on	Zenturi	0 (0%)	0	0	0%	0 (0%)
on	Yahoo Webcam	0 (0%)	0	0	0%	0 (0%)
on	Opera 9-9.20	0 (0%)	0	0	0%	0 (0%)
on	XML Core Services	0 (0%)	0	0	0%	0 (0%)
off	empty	0 (0%)	0	0	0%	0 (0%)
off	empty	0 (0%)	0	0	0%	0 (0%)
on	Java bytecode(*)	0 (0%)	0	0	0%	0 (0%)
on	.ANI(*)	0 (0%)	0	0	0%	0 (0%)
Totals:	0 active exploits	0 exploited systems			0%	0 loader

Exploits options

☑ MDAC (RDS)	☑ WVFI SetSlice	☑ VML	☑ MS06-044	☑ WMF Firefox	☑ WMF Opera 7	
☑ Zenturi	☑ Yahoo Webcam	☑ Opera 9-9.20	☑ XML Core Services	□ empty	□ empty	Ja

Napoleon / Siberia (exploit pack)



Napoleon Sploit 1.0

by WennY

Статистика

Логин (?): 1

Пароль (?): 1

MySQL

Сервер (?): localhost

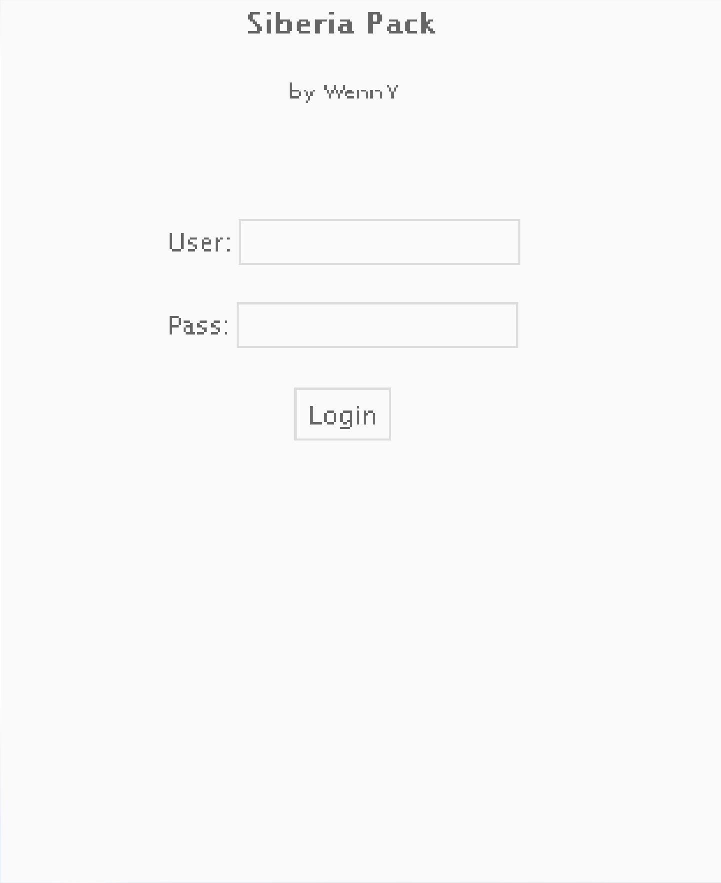
Пользователь (?): root

Пароль (?):

Имя БД (?): webauth

Имя таблицы (?): stats

Связка

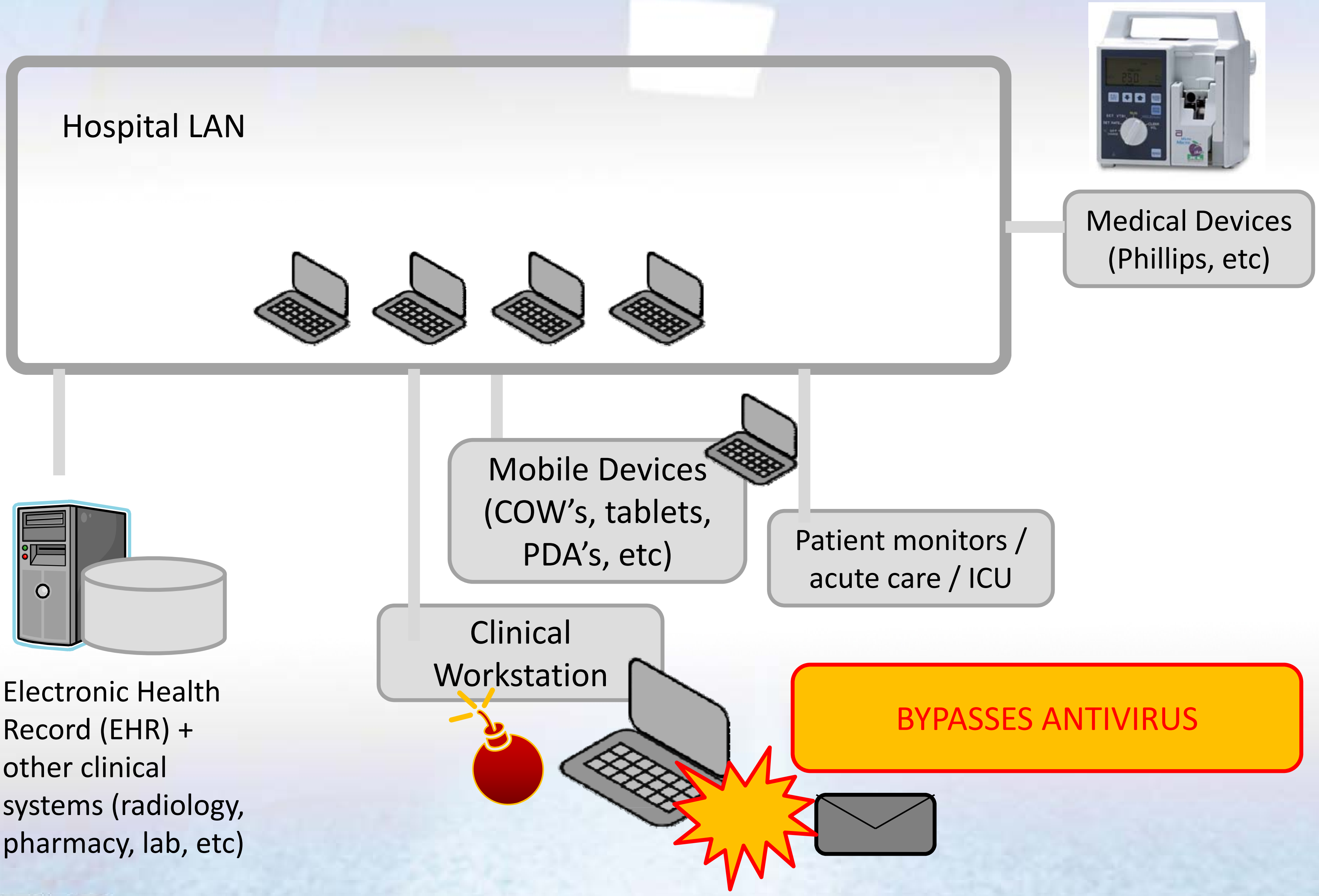


Siberia Pack

by WennY

User:

Pass:



Hospital LAN

Medical Devices (Phillips, etc)

Mobile Devices (COW's, tablets, PDA's, etc)

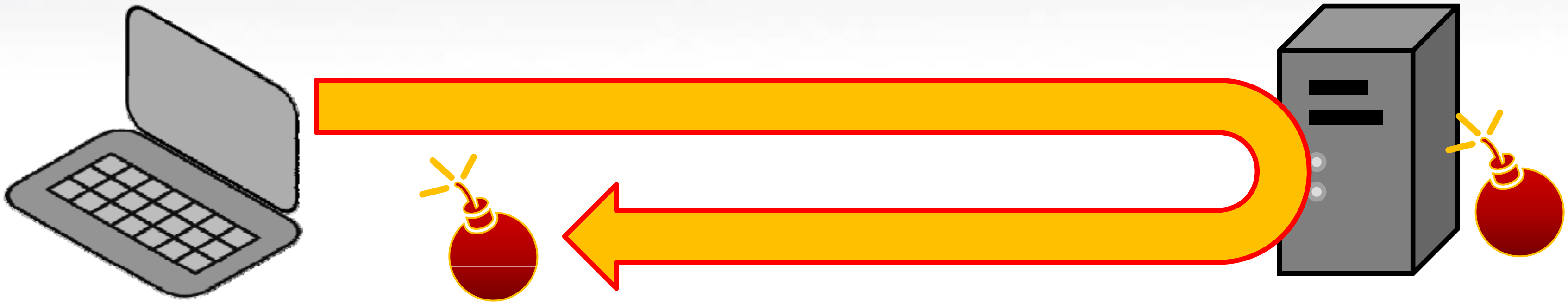
Patient monitors / acute care / ICU

Clinical Workstation

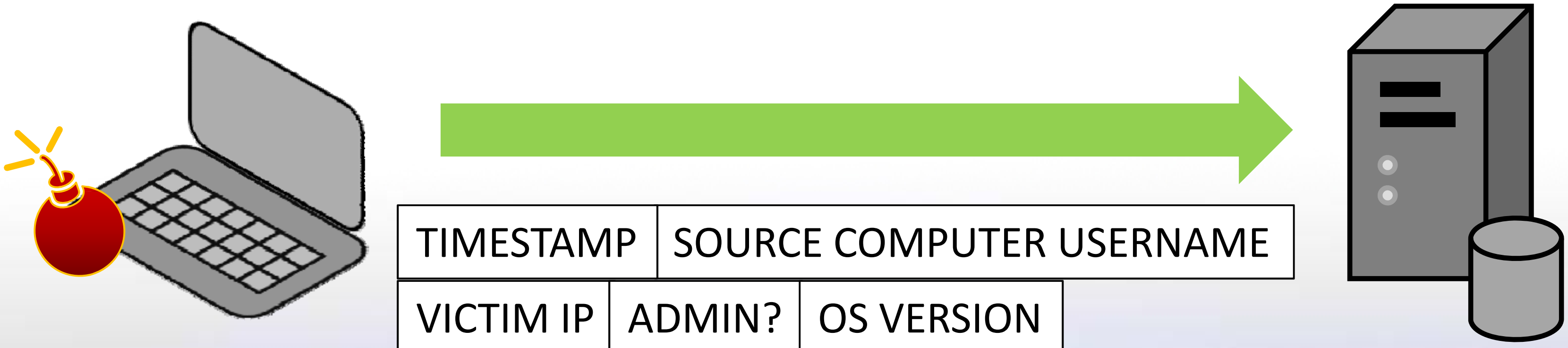
Electronic Health Record (EHR) + other clinical systems (radiology, pharmacy, lab, etc)

BYPASSES ANTIVIRUS

Command and Control



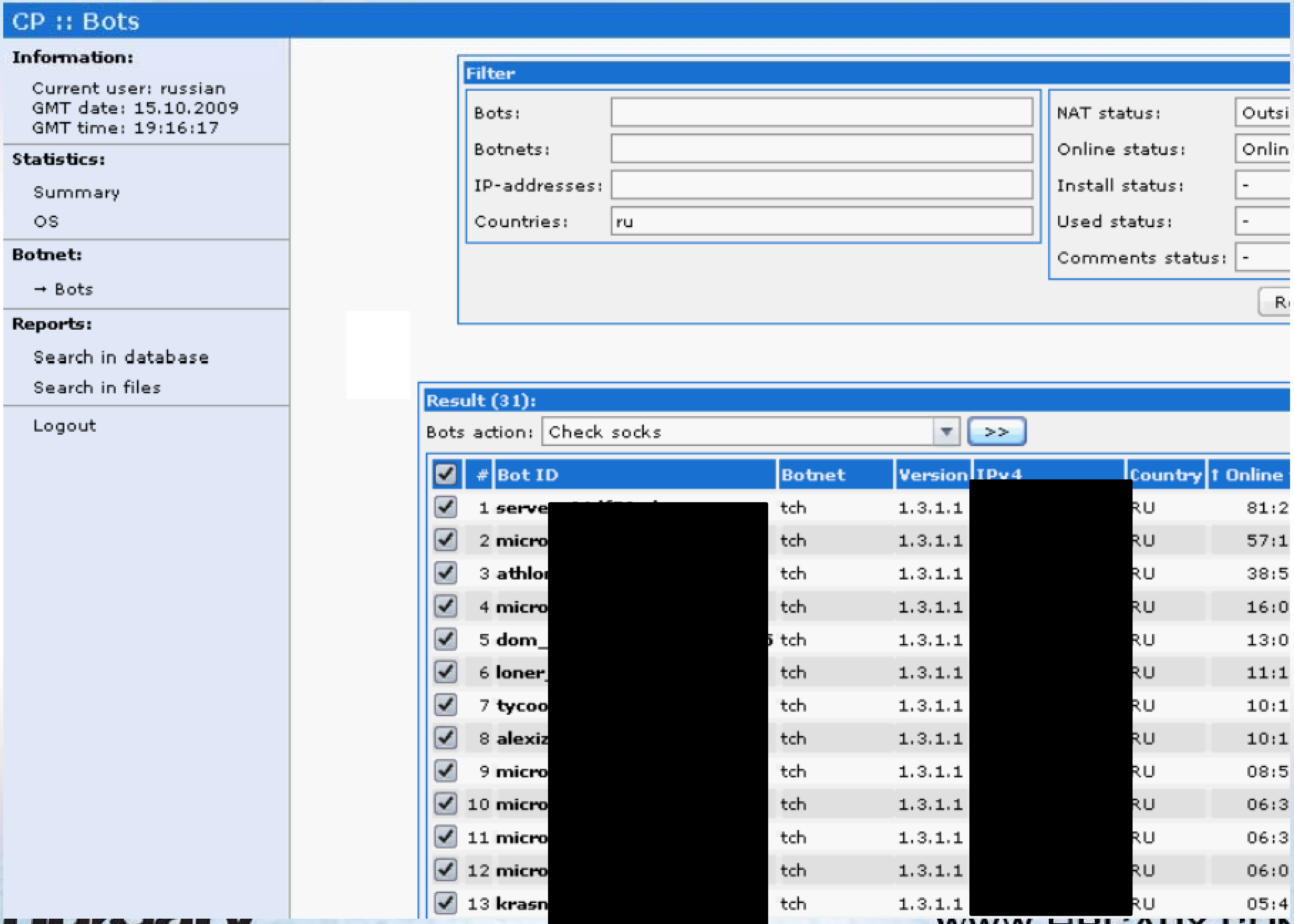
Once installed, the malware phones home…



TIMESTAMP | SOURCE COMPUTER USERNAME

VICTIM IP | ADMIN? | OS VERSION

HD SERIAL NUMBER



CP :: Bots

Information:

Current user: russian
GMT date: 15.10.2009
GMT time: 19:16:17

Statistics:

Botnet:

Reports:

Filter

Bots:
Botnets:
IP-addresses:
Countries: ru

NAT status: Outsi
Online status: Onlin
Install status: -
Used status: -
Comments status: -

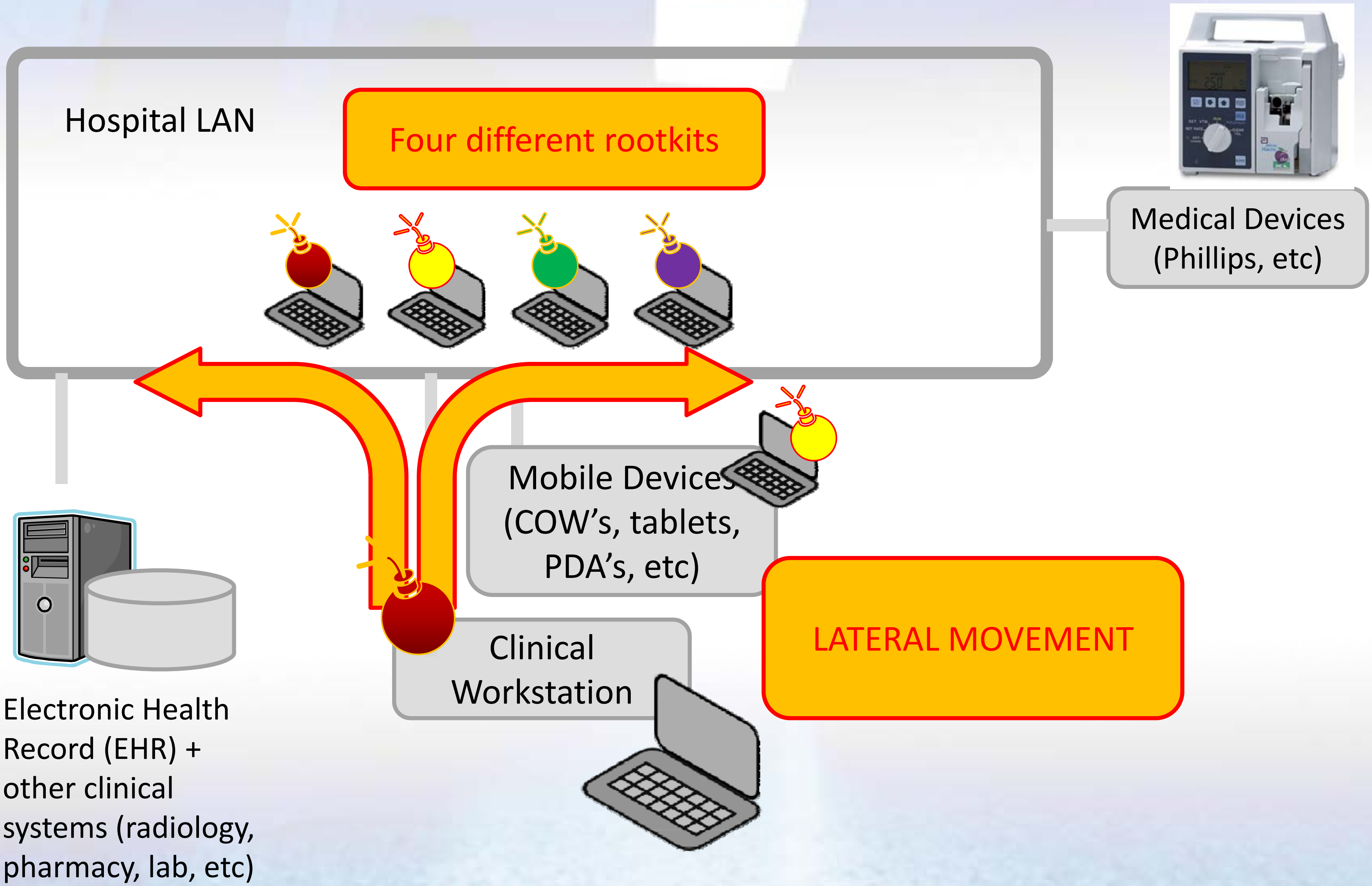
Result (31):

Bots action: Check socks ▼ >>

☑	#	Bot ID	Botnet	Version	IPv4	Country	↑ Online
☑	1	serve[redacted]	tch	1.3.1.1	[redacted]	RU	81:2
☑	2	micro[redacted]	tch	1.3.1.1	[redacted]	RU	57:1
☑	3	athlo[redacted]	tch	1.3.1.1	[redacted]	RU	38:5
☑	4	micro[redacted]	tch	1.3.1.1	[redacted]	RU	16:0
☑	5	dom_[redacted]	tch	1.3.1.1	[redacted]	RU	13:0
☑	6	loner_[redacted]	tch	1.3.1.1	[redacted]	RU	11:1
☑	7	tycoo[redacted]	tch	1.3.1.1	[redacted]	RU	10:1
☑	8	alexiz[redacted]	tch	1.3.1.1	[redacted]	RU	10:1
☑	9	micro[redacted]	tch	1.3.1.1	[redacted]	RU	08:5
☑	10	micro[redacted]	tch	1.3.1.1	[redacted]	RU	06:3
☑	11	micro[redacted]	tch	1.3.1.1	[redacted]	RU	06:3
☑	12	micro[redacted]	tch	1.3.1.1	[redacted]	RU	06:0
☑	13	krasn[redacted]	tch	1.3.1.1	[redacted]	RU	05:4

Phase-2 Access

- The terrorist group is focused on access
  - No actions are taken that would reveal the injected code
  - Long term (weeks)



Hospital LAN

Four different rootkits

Medical Devices (Phillips, etc)

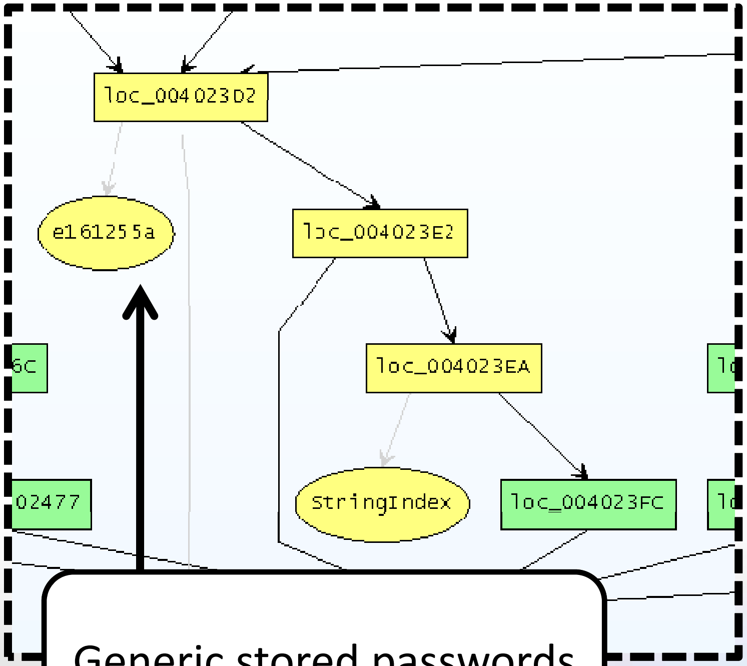
Mobile Devices (COW’s, tablets, PDA’s, etc)

Clinical Workstation

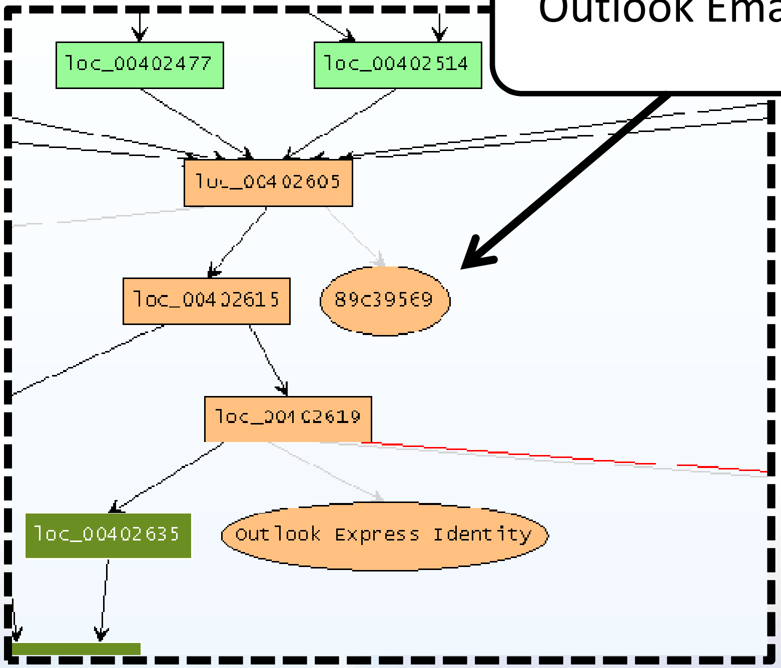
LATERAL MOVEMENT

Electronic Health Record (EHR) + other clinical systems (radiology, pharmacy, lab, etc)

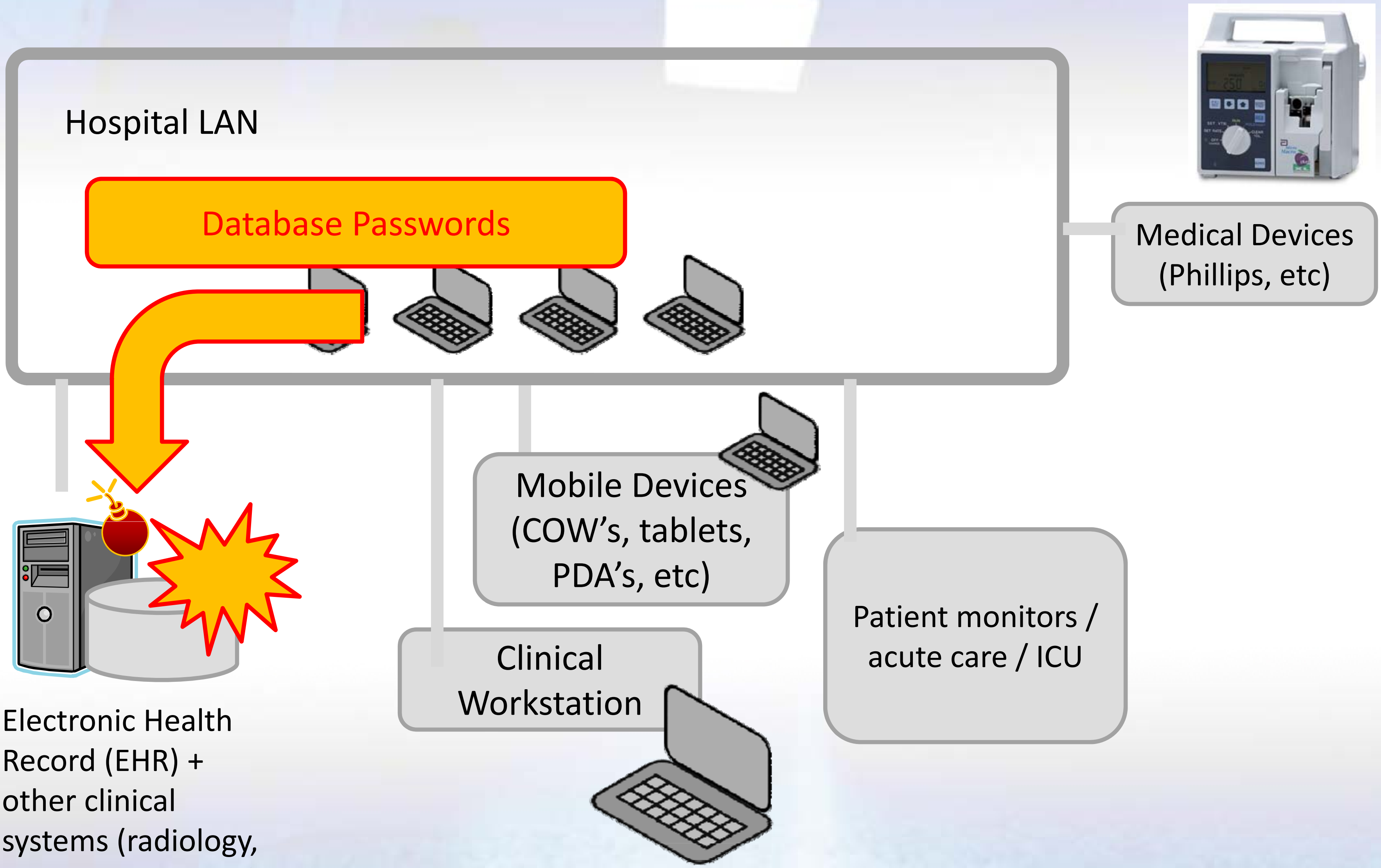
Steal Credentials



Generic stored passwords



Outlook Email Password



Hospital LAN

Database Passwords

Medical Devices (Phillips, etc)

Mobile Devices (COW's, tablets, PDA's, etc)

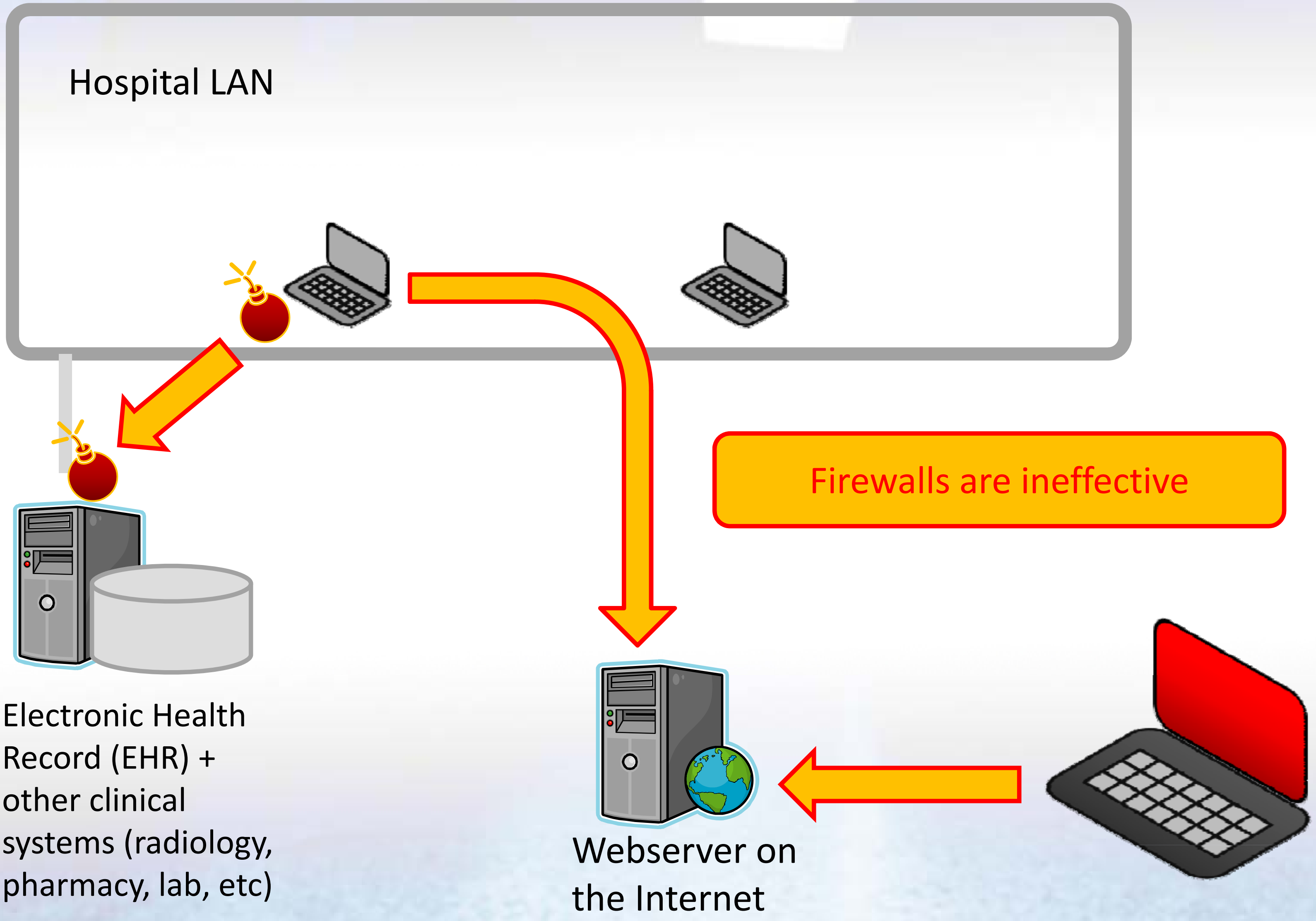
Clinical Workstation

Patient monitors / acute care / ICU

Electronic Health Record (EHR) + other clinical systems (radiology, pharmacy, lab, etc)

Day 1

- Subtle modifications to the database



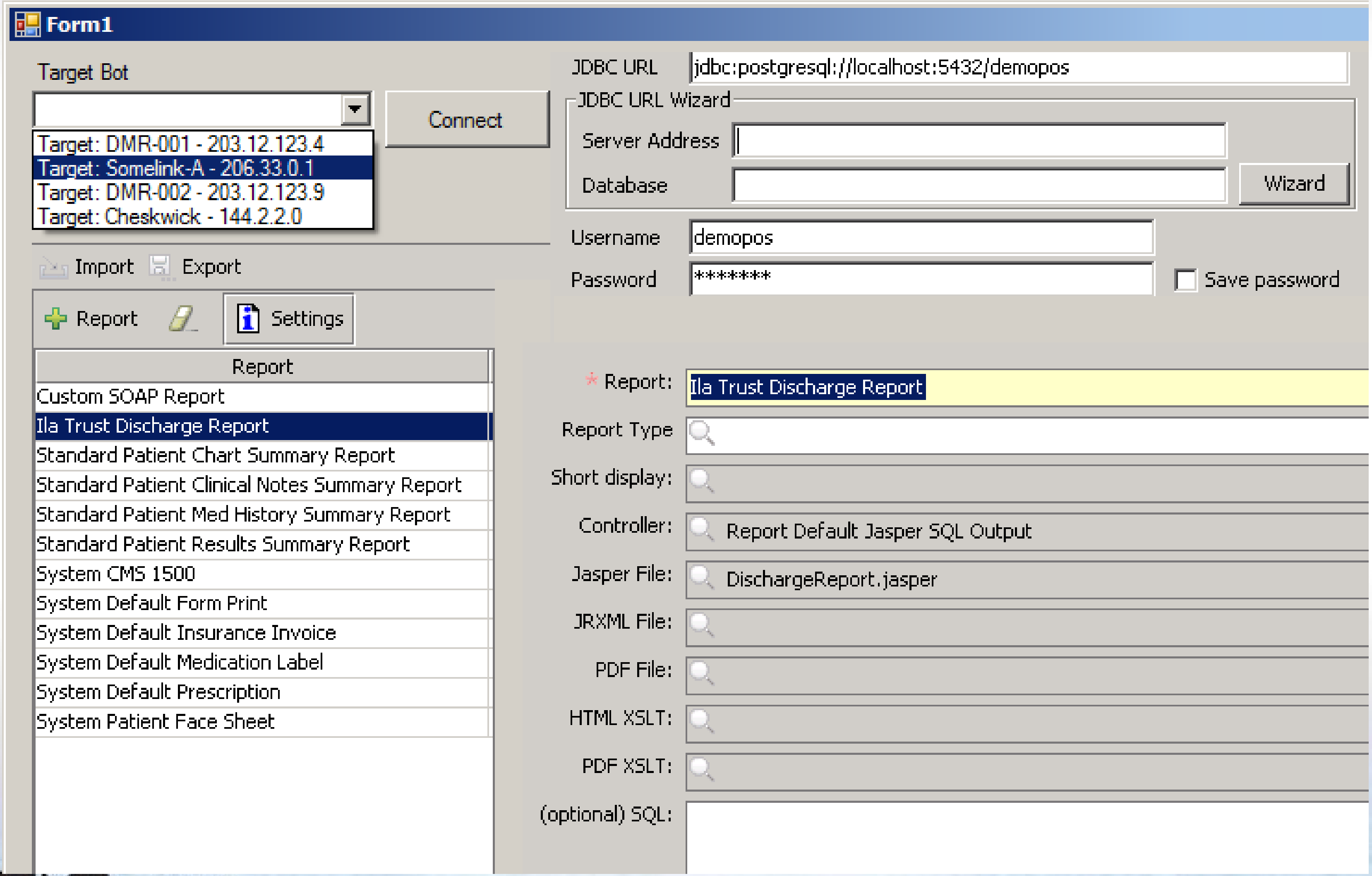
Hospital LAN

Firewalls are ineffective

Electronic Health Record (EHR) + other clinical systems (radiology, pharmacy, lab, etc)

Webserver on the Internet

Custom remote-control application



Target Bot

- Target: DMR-001 - 203.12.123.4
- Target: Somelink-A - 206.33.0.1
- Target: DMR-002 - 203.12.123.9
- Target: Cheskwick - 144.2.2.0

JDBC URL: jdbc:postgresql://localhost:5432/demopos

JDBC URL Wizard

Server Address:

Database:

Username: demopos

Password: ********

☐ Save password

Report
Custom SOAP Report
Ila Trust Discharge Report
Standard Patient Chart Summary Report
Standard Patient Clinical Notes Summary Report
Standard Patient Med History Summary Report
Standard Patient Results Summary Report
System CMS 1500
System Default Form Print
System Default Insurance Invoice
System Default Medication Label
System Default Prescription
System Patient Face Sheet

* Report: Ila Trust Discharge Report

Report Type:

Short display:

Controller: Report Default Jasper SQL Output

Jasper File: DischargeReport.jasper

JRXML File:

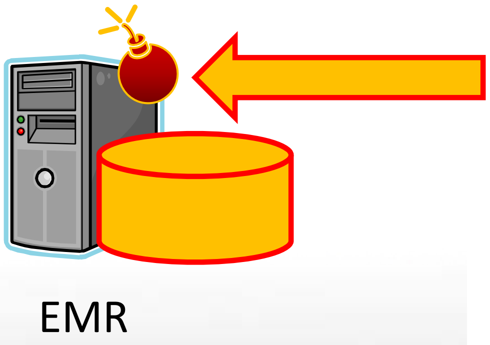
PDF File:

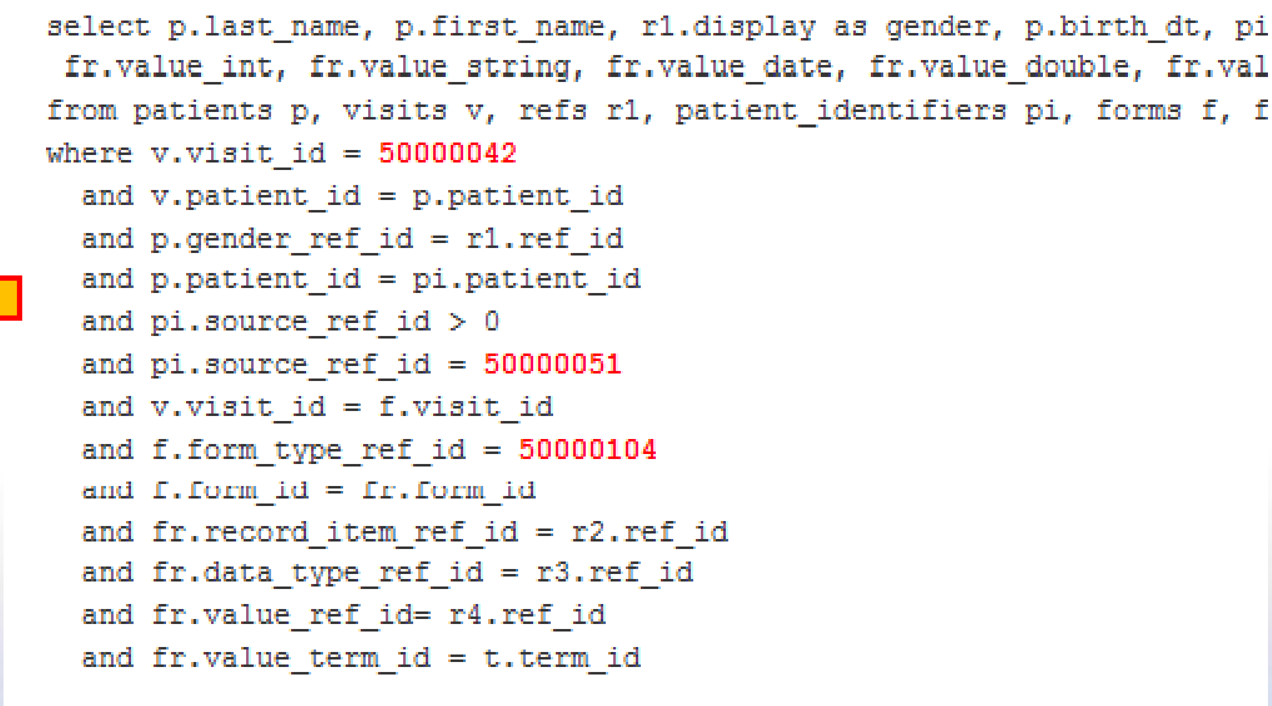
HTML XSLT:

PDF XSLT:

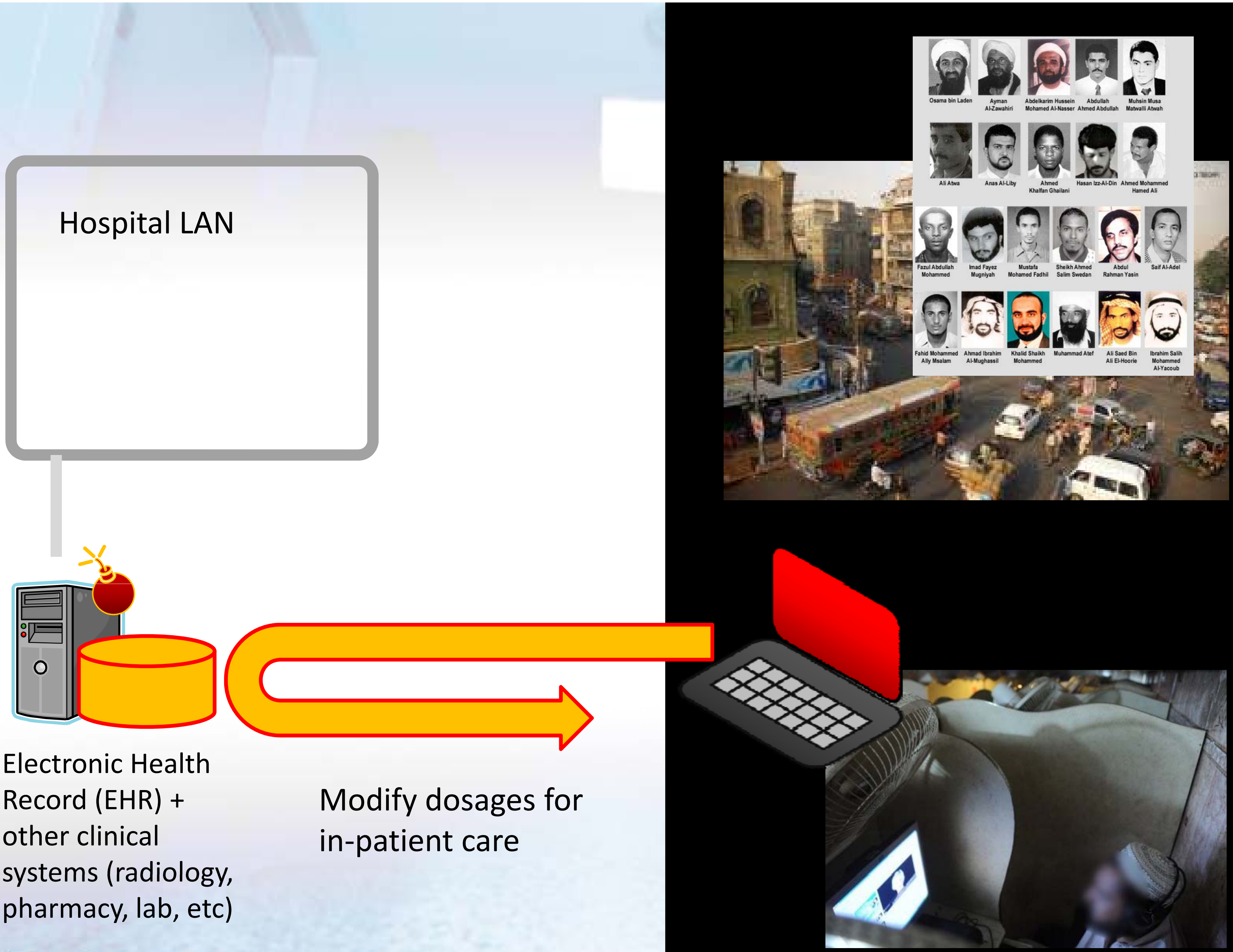
(optional) SQL:

Full SQL access





```
select p.last_name, p.first_name, r1.display as gender, p.birth_dt, pi
 fr.value_int, fr.value_string, fr.value_date, fr.value_double, fr.val
from patients p, visits v, refs r1, patient_identifiers pi, forms f, f
where v.visit_id = 50000042
  and v.patient_id = p.patient_id
  and p.gender_ref_id = r1.ref_id
  and p.patient_id = pi.patient_id
  and pi.source_ref_id > 0
  and pi.source_ref_id = 50000051
  and v.visit_id = f.visit_id
  and f.form_type_ref_id = 50000104
  and f.form_id = fr.form_id
  and fr.record_item_ref_id = r2.ref_id
  and fr.data_type_ref_id = r3.ref_id
  and fr.value_ref_id= r4.ref_id
  and fr.value_term_id = t.term_id
```



Hospital LAN

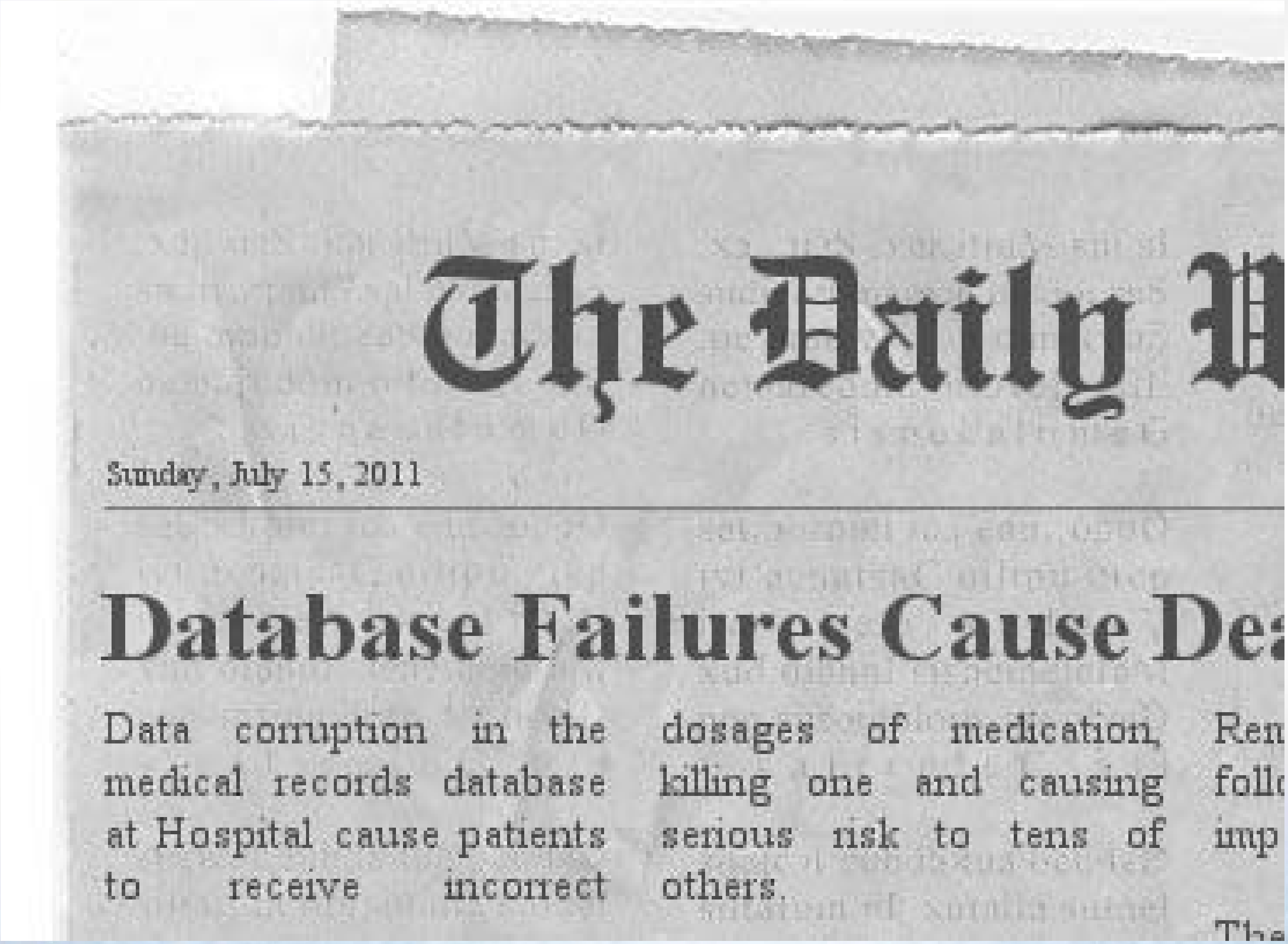
Electronic Health Record (EHR) + other clinical systems (radiology, pharmacy, lab, etc)

Modify dosages for in-patient care

Some unsavory ideas…

- False doctor orders are inserted
- Medications are changed outright
- Some medications are discontinued
- Dosages are altered
- Allergies deleted

Day 3



The Daily W

Sunday, July 15, 2011

Database Failures Cause Dea

Data corruption in the medical records database at Hospital cause patients to receive incorrect dosages of medication, killing one and causing serious risk to tens of others.

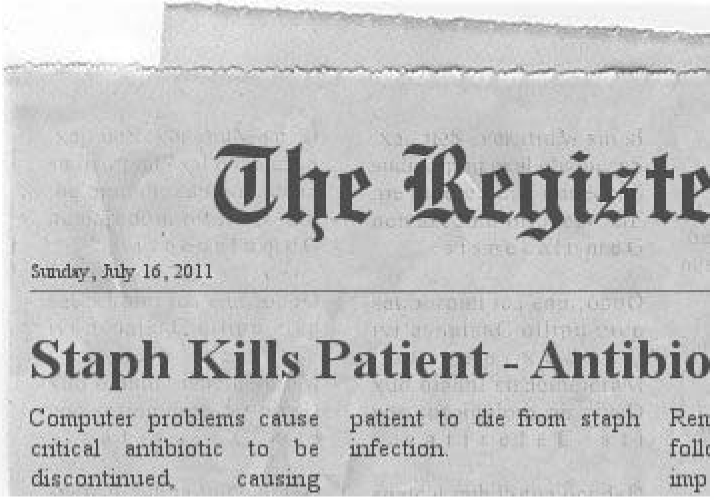
Ren
foll
imp

The

- Hospitals forced to restore database backups, losing three days or more of data
- At first, they don’t realize this was an attack
  - The database is blamed

Day 4

- After systems are restored from backup, terrorists stop using 💣
- Hospitals also start to realize this was a widespread event….



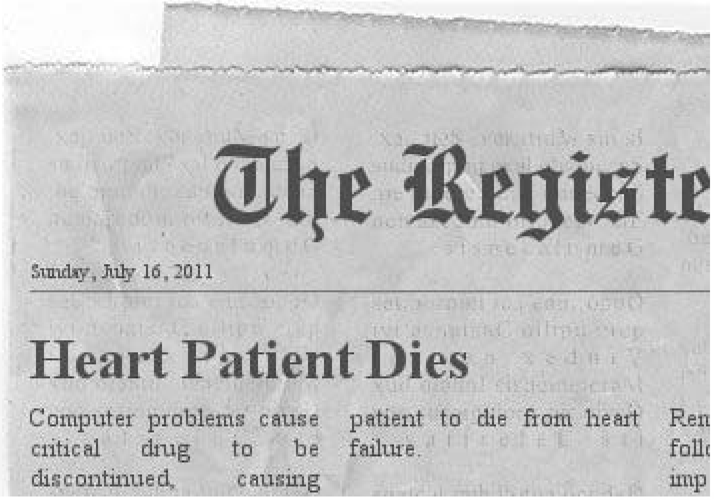
The Registe

Sunday, July 16, 2011

Staph Kills Patient - Antibio

Computer problems cause critical antibiotic to be discontinued, causing patient to die from staph infection.

Ren
foll
imp



The Registe

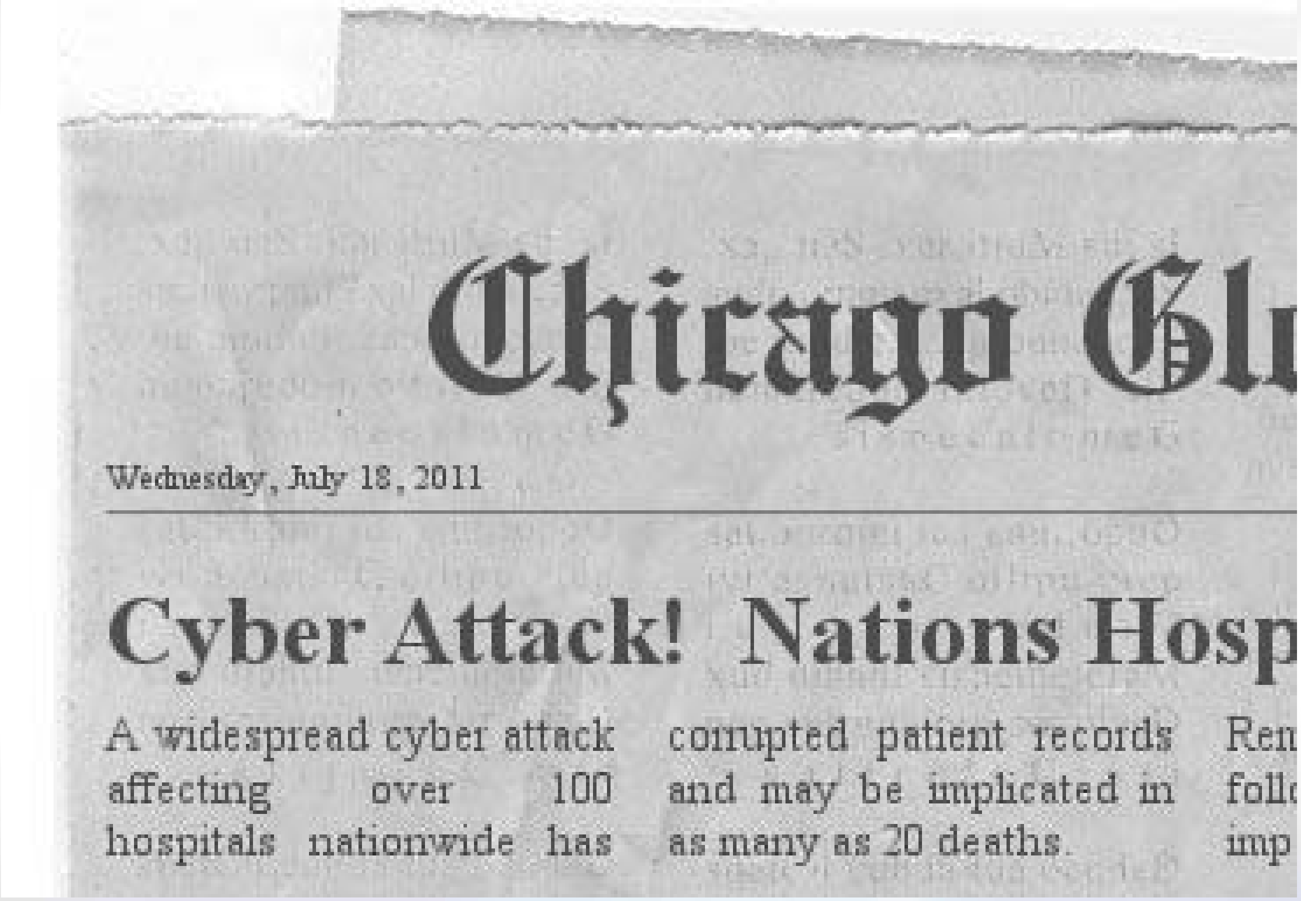
Sunday, July 16, 2011

Heart Patient Dies

Computer problems cause critical drug to be discontinued, causing patient to die from heart failure.

Ren
foll
imp

Day 5



Chicago Gl

Wednesday, July 18, 2011

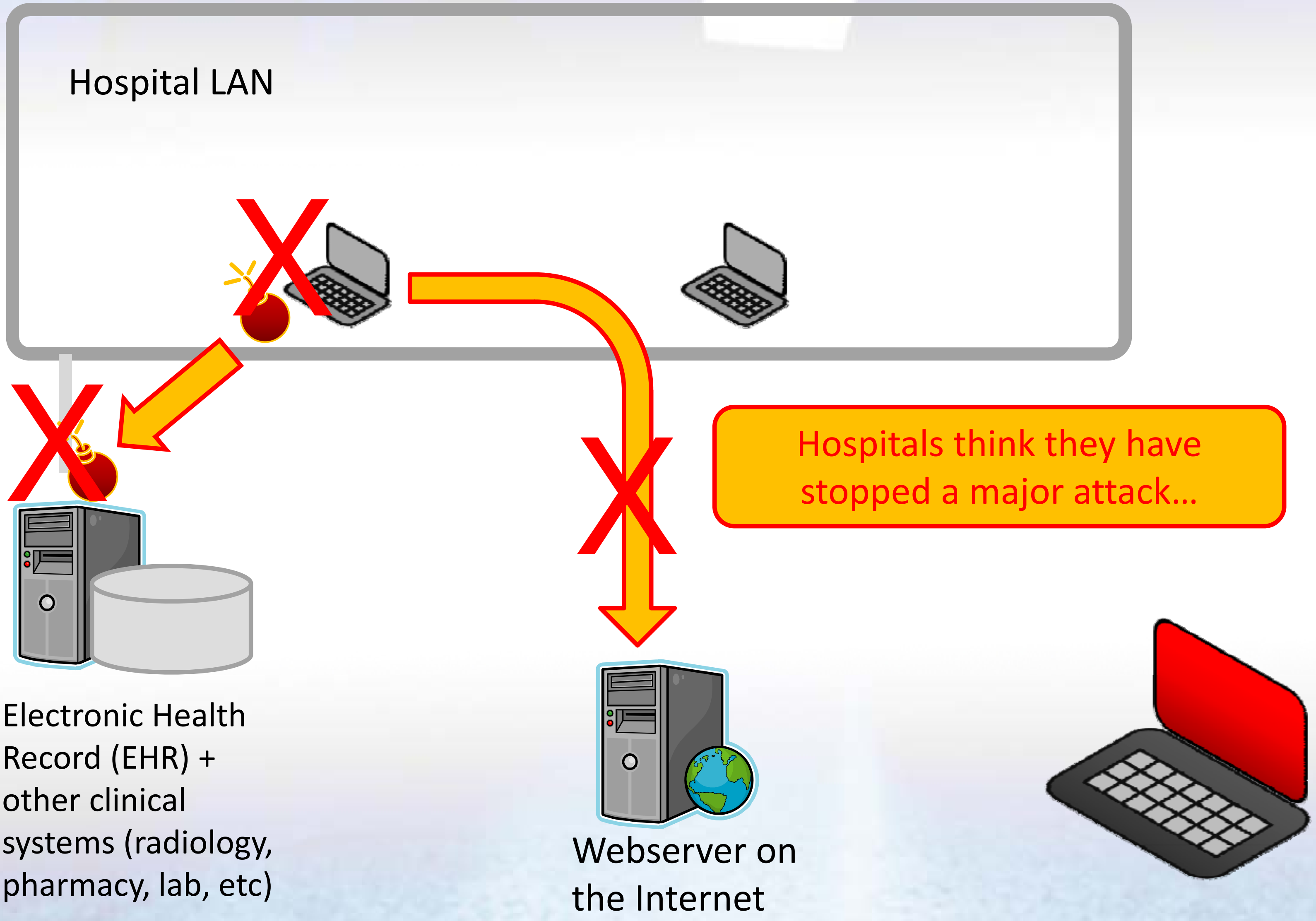
Cyber Attack! Nations Hosp

A widespread cyber attack affecting over 100 hospitals nationwide has corrupted patient records and may be implicated in as many as 20 deaths.

Ren
foll
imp

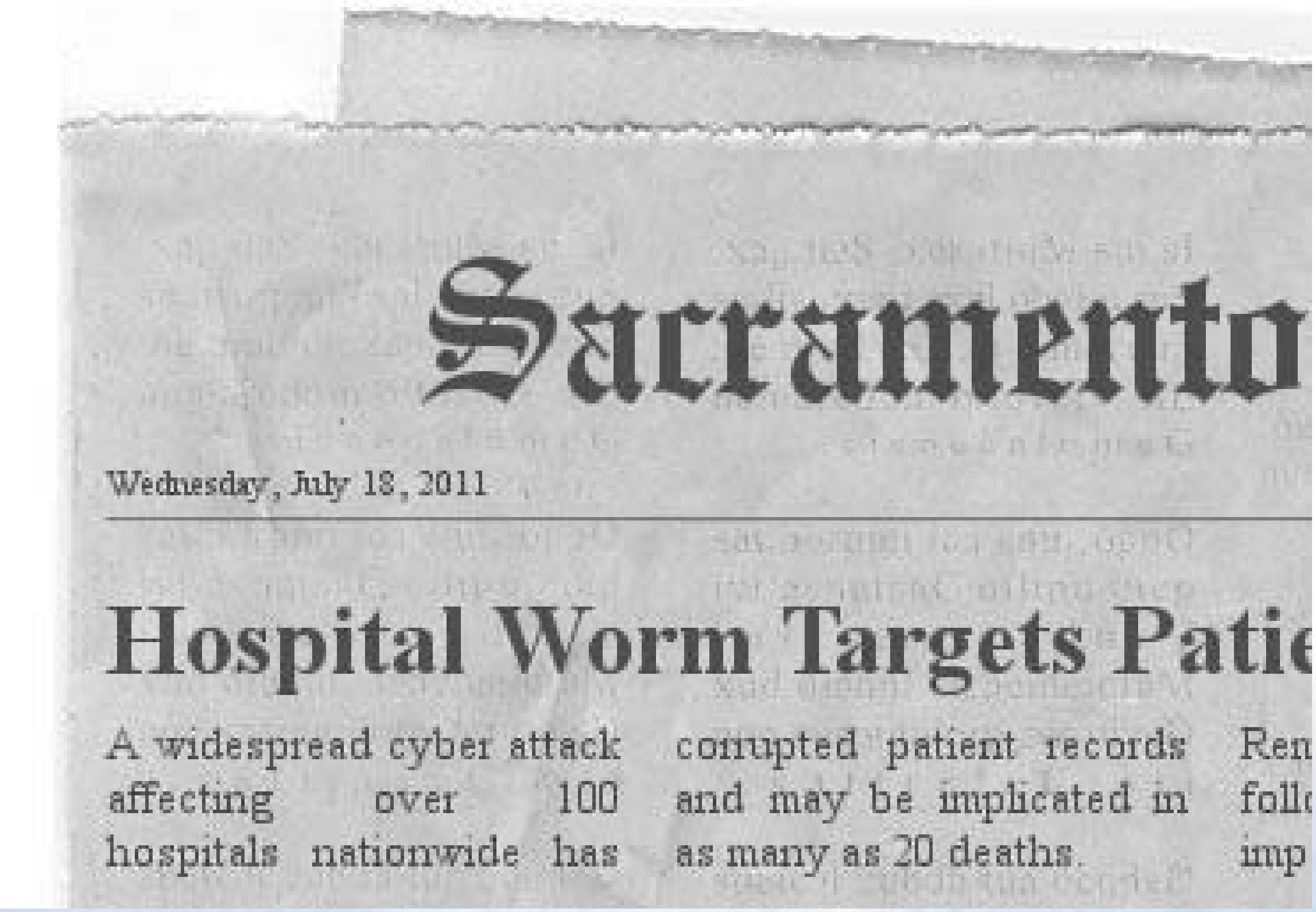
Emergency Management Plan

- Hospitals start restoring backups
- Incident Response Teams discover the command-and-control traffic & database backdoor
- Files are sent to AV vendor


Hospital LAN
Electronic Health Record (EHR) + other clinical systems (radiology, pharmacy, lab, etc)
Webserver on the Internet

Hospitals think they have stopped a major attack…

The ‘Hospital Worm’



Sacramento

Wednesday, July 18, 2011

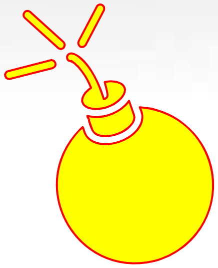
Hospital Worm Targets Patie

A widespread cyber attack affecting over 100 hospitals nationwide has corrupted patient records and may be implicated in as many as 20 deaths.

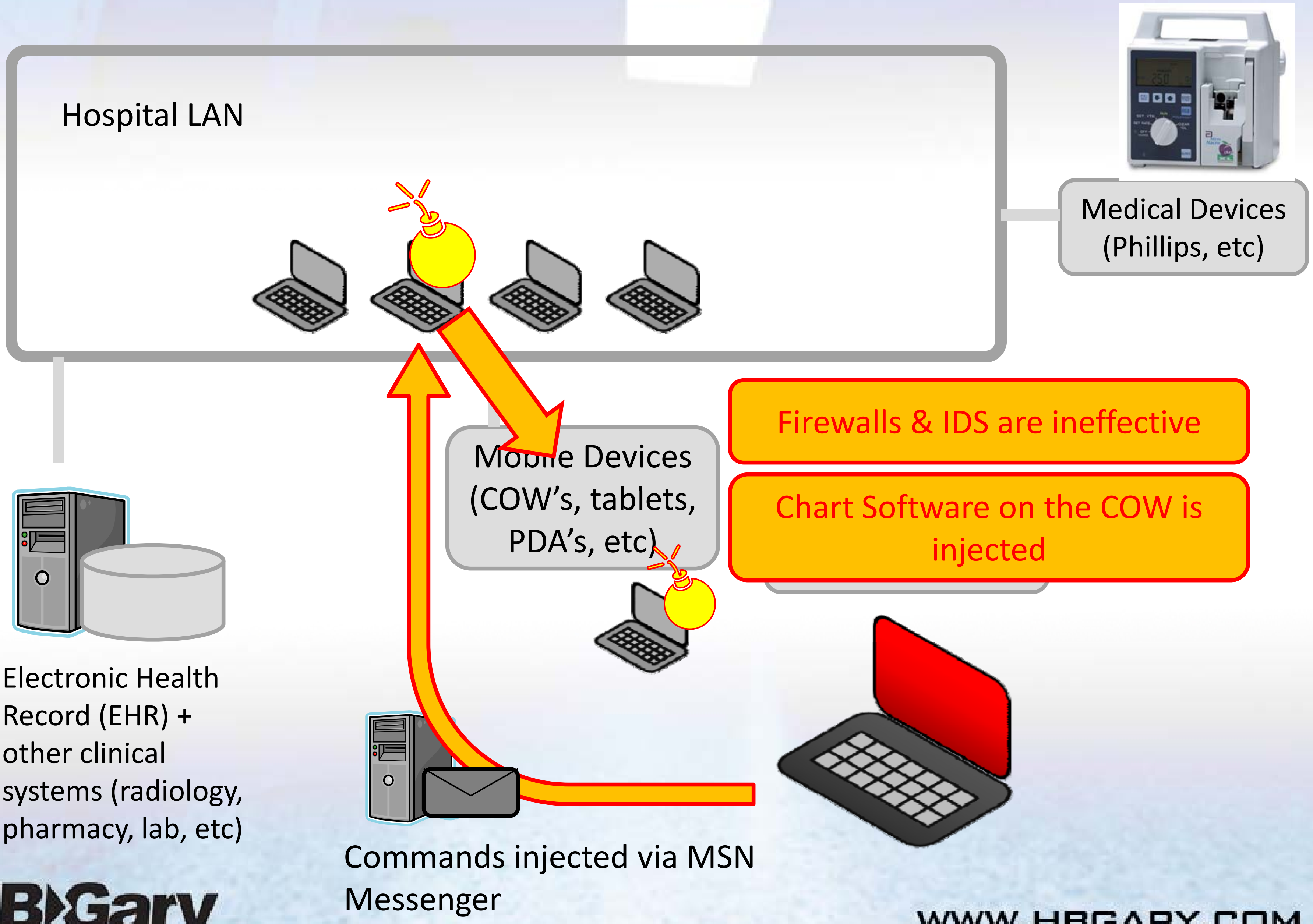
Ren
follo
imp

Meanwhile…

- Terrorists switch to secondary



- They only enable the secondary once the hospital has responded to the database corruption
  - Even if the Internet is disabled entirely, the secondary has a hard coded activation time as backup trigger



Hospital LAN

Medical Devices (Phillips, etc)

Mobile Devices (COW’s, tablets, PDA’s, etc)

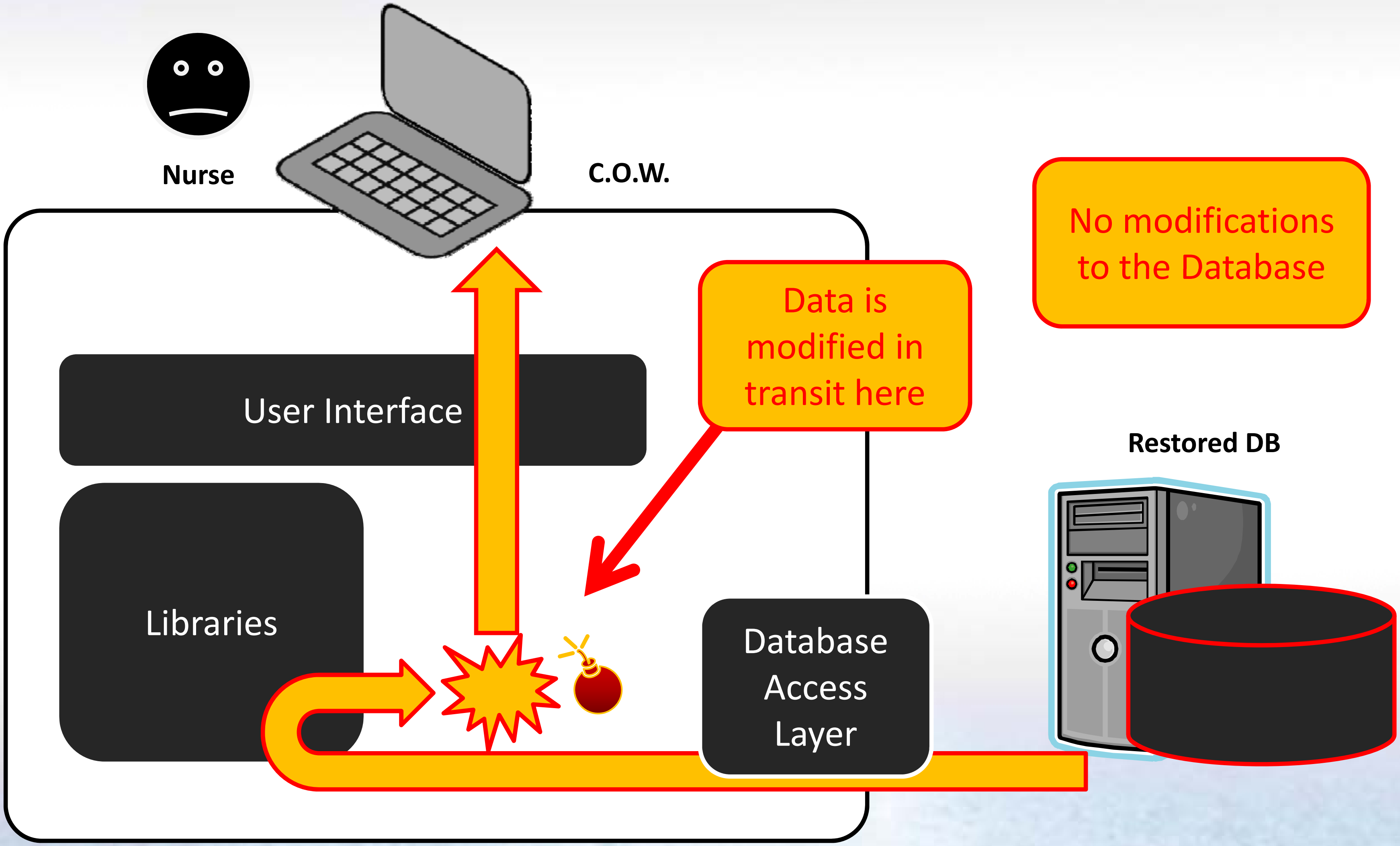
Firewalls & IDS are ineffective

Chart Software on the COW is injected

Electronic Health Record (EHR) + other clinical systems (radiology, pharmacy, lab, etc)

Commands injected via MSN Messenger

In-process Injection

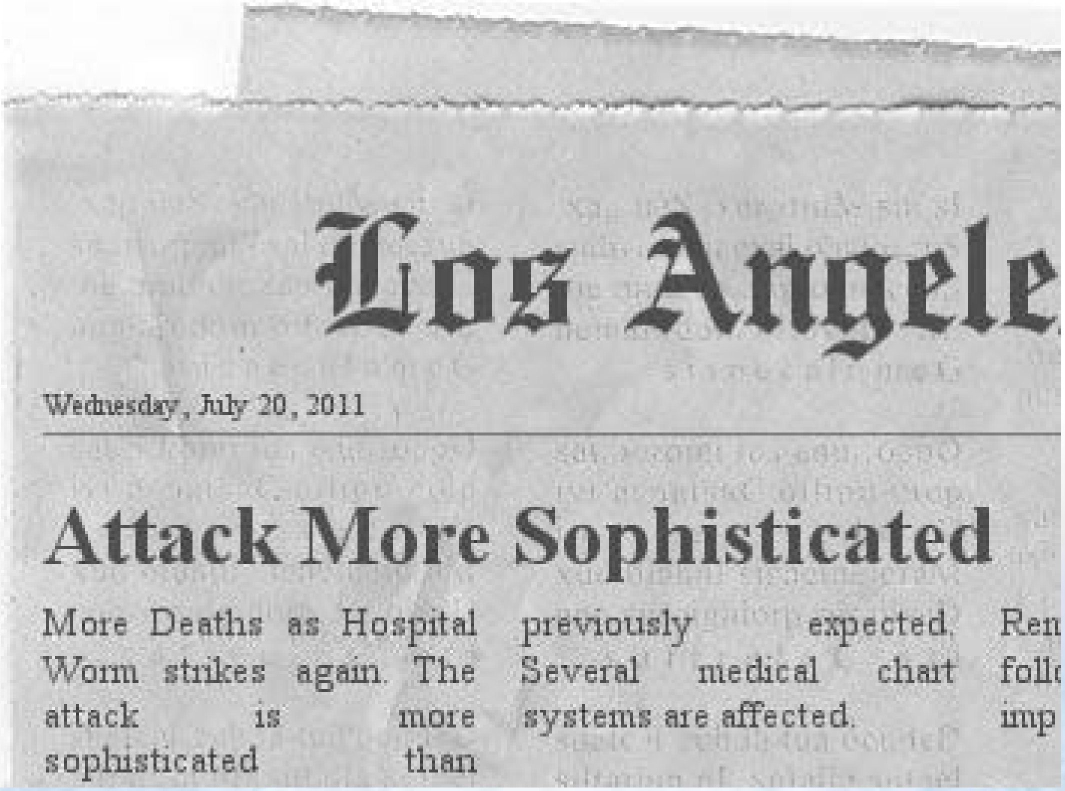


Data is modified in transit here

No modifications to the Database

Day 7

Confidence in the medical computers erodes…
Hospitals start to implement paper system…
Electronic Charts are not to be trusted….



Los Angele

Wednesday, July 20, 2011

Attack More Sophisticated

More Deaths as Hospital Worm strikes again. The attack is more sophisticated than previously expected. Several medical chart systems are affected.

Ren
foll
imp

Days 8-15 = Not Enough Staff

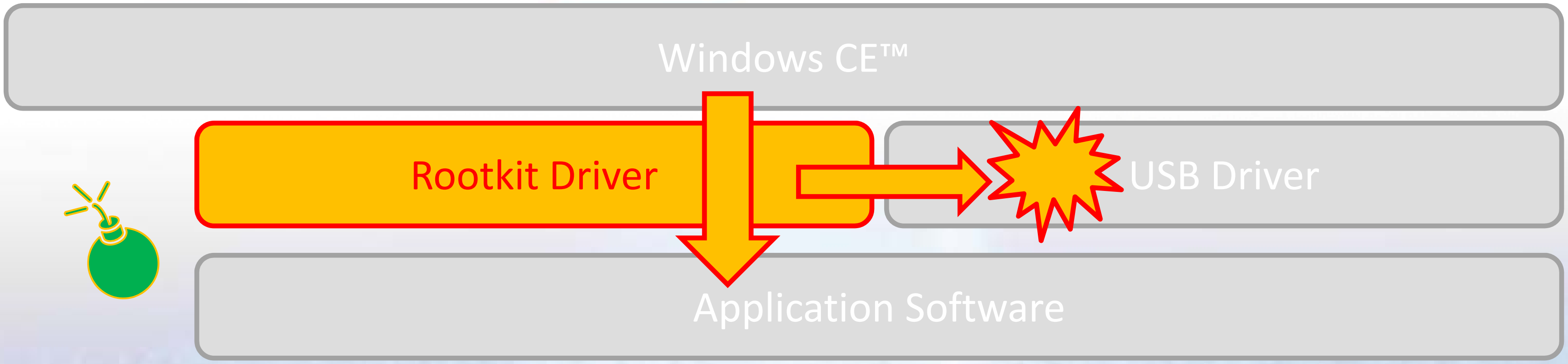
- Non essential procedures are cancelled
- Large Hospitals are completely understaffed, nurse to patient ratios are taxed when computers are shut down

Day 15

- Implant 💣 triggers automatically

- Monitors in both adult and neonatal ICU are injected to show false data – critical patients die because alarms are not working
  - Several major vendors targeted, especially those systems based on Windows embedded

ICU Monitor Injection



Windows CE™

Rootkit Driver

USB Driver

Application Software

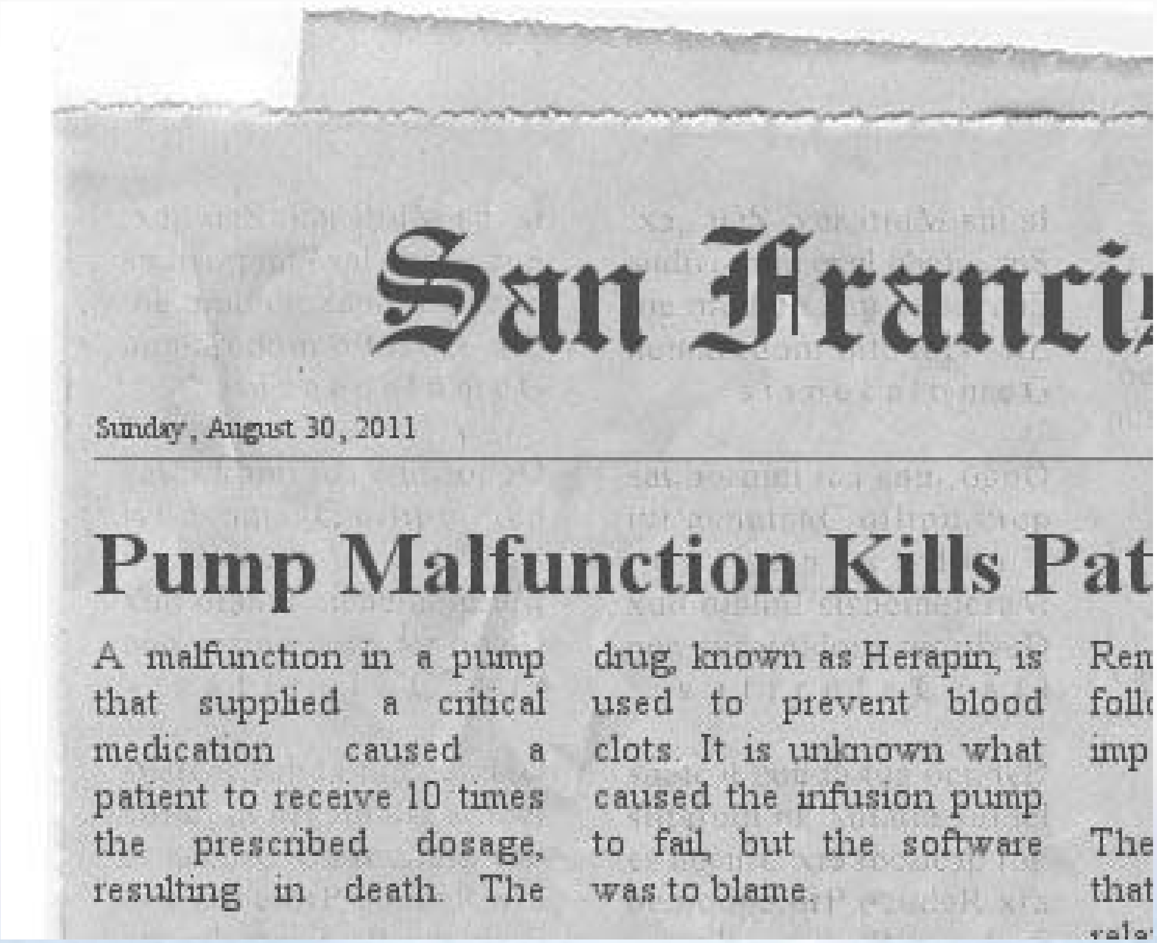
HBGary

Day 16 = Chaos

- ER services are redirected to non-affected hospitals
- The Internet is blocked causing disruption with external labs and partner services
- Family members of patients fill the hospitals, taxing the dwindling resources
- Patients are being transferred to non-affected hospitals (largely those that still use paper)

Day 20

- Implant 💣 triggers automatically
- Firmware in medical devices are altered to cause severe harm
  - Flow rates, faulty timers, incorrect dosages
  - Infusion pumps, in particular, are targeted



San Franci

Sunday, August 30, 2011

Pump Malfunction Kills Pat

A malfunction in a pump that supplied a critical medication caused a patient to receive 10 times the prescribed dosage, resulting in death. The drug, known as Herapin, is used to prevent blood clots. It is unknown what caused the infusion pump to fail, but the software was to blame.

Ren
follo
imp

The
that
rele

"No one knew when it would end. We couldn't trust or operate the medical devices. The staff could only provide basic care. The affected hospitals were more or less shut down – they were shunned as if cursed."

Will This Be You?

Notes on research

- The emergency scenario was partially modeled on Hurricane Katrina & Emergency Management Plans
- The network attacks are all modeled on real malware that can be found today
- The ICU monitor attack is based on real-world Windows CE rootkit capability
- The medical device attack is modeled on real-world JTAG hacking on ARM-processor based devices + firmware
- All newspaper clippings were fabricated for illustrative purposes, but drawn from actual historical news events regarding medical equipment failures causing deaths

Bill Fawns

CIO, Kern Medical Center

KERN
MEDICAL
CENTER

Questions

Questions can be directed to **karen@hbgary.com**