

# Better Safe Than Sorry

(by Gianluca Pericoli)

The talk begins with a brief theoretical introduction concerning the basis of Information Security and develops by discussing the APT (Advanced Persistent Threats) that characterise much of the news about cybersecurity impacts in the last five years. Beyond the introduction and the cases, the APT groups known so far and the different motivations are presented very quickly.

The recent case of the hospital in Padua is analysed in more detail, assessing what it has meant for the community.

After analysing the attacker point of view, we move on to the defence, explaining the main methods of analysis, prevention and relative best practices regarding cybersec with a focus on the usability of data, referring to the CIA Triad (Confidentiality, Integrity, Availability). Particular attention will then be paid to the Human Firewall part, giving the topic a practical meaning and fielding real examples. In the last part of the talk, a Cyber Threat Intelligence work carried out on the health facilities of the five largest Swiss cities will be exposed, analysing the information available in publicly accessible leaks databases.

# better safe than sorry



P.S. the first slide was a [joke](#), I promise I will try not to be boring

# # who am I



1985: I was born

1992: first computer (a blazing Commodore64)

1999: I start high school in IT specialisation

2000: I program my first video game in Turbo Pascal (Siegfried)

2001: I join the Linux group in high school, discover the world of security and have no idea about the modules I compile in the Kernel

2001: I stop playing video games and dedicate myself to programming and computer security (SpaghettiPhreakers)

2002: I write my first rootkit, which I call Nightrain (like the Gun N's Roses song)

2003: I take Nightrain as my graduation thesis but it didn't make much of a stir

2004: I start studying Computer Engineering in Padua

2005: I start working as a technician in the medical field and continue studying computer science under the department of pure and applied mathematics in Padua

2006: antiviruses start detecting Nightrain :\_(

2008: I graduate in computer science and travel around Europe as a technical manager for medical systems

2011: I decide to start programming again

2012: I start being a Penetration Tester (I never stopped studying it)

2014: I work at **Interlogica**, penetration tester, programmer, project manager

2020: I become a partner at Interlogica

2021: I become head of Interlogica's Cybersec team

2022: in between clients I like to help out with Red Team operations :D

**from here they can't  
fire me easily!!!1!**

# who am I

at 14 I wanted to be a hacker



at 37 I became a copy-editor

# # CIA Triad

The CIA Triad		
What Is the CIA?		
Confidentiality	Integrity	Availability
The information is safe from accidental or intentional disclosure.	The information is safe from accidental or intentional modification or alteration.	The information is available to authorized users when needed.
Example		
I send you a message, and no one else knows what that message is.	I send you a message, and you receive exactly what I sent you (without any modification)	I send you a message, and you are able to receive it.
What's The Purpose of the CIA?		
Data is not disclosed	Data is not tampered	Data is available
How Can You Achieve the CIA?		
e.g., Encryption	e.g., Hashing, Digital signatures	e.g., Backups, redundant systems
Opposite of CIA		
Disclosure	Alteration	Destruction

# # APT: what is it?

**Initial compromise:** performed by use of social engineering and spear phishing, over email, using zero-day viruses. Another popular infection method was planting malware on a website that the victim's employees will be likely to visit.

**Establish foothold:** plant remote administration software in victim's network, create net backdoors and tunnels allowing stealth access to its infrastructure.

Thanks Wikipedia

**Escalate privileges:** use exploits and password cracking to acquire administrator privileges over victim's computer and possibly expand it to Windows domain administrator accounts.

**Internal reconnaissance:** collect information on surrounding infrastructure, trust relationships, Windows domain structure.

**Move laterally:** expand control to other workstations, servers and infrastructure elements and perform data harvesting on them.

**Maintain presence:** ensure continued control over access channels and credentials acquired in previous steps.

**Complete mission:** exfiltrate stolen data from victim's network.



# # APT: what is it?



# #APT: why? Money / Politics





# # APT: who?

## # China

PLA Unit 61398 (also known as APT1)

PLA Unit 61486 (also known as APT2)

Buckeye (also known as APT3)

Red Apollo (also known as APT10)

Numbered Panda (also known as APT12)

DeputyDog (also known as APT17)

Codoso Team (also known as APT19)

Wocao (also known as APT20)

APT 27

PLA Unit 78020 (also known as APT30 and Naikon)

Zirconium (also known as APT31)

Periscope Group (also known as APT40)

Double Dragon (also known as APT41, Winnti Group, Barium, or Axiom)

Tropic Trooper

Hafnium

LightBasin (Also known as UNC1945)

Dragonbridge



Thanks Wikipedia



# # APT: who?

## # Iran

Elfin Team (also known as APT33)

Helix Kitten (also known as APT34)

Charming Kitten (also known as APT35)

APT39

Pioneer Kitten



Thanks Wikipedia

## # Israel

Unit 8200



## # North Korea

Kimssuky

Lazarus Group (also known as APT38)

Ricochet Chollima (also known as APT37)



# # APT: who?

# Russia

Fancy Bear (also known as APT28)

Cozy Bear (also known as APT29)

Sandworm

Berserk Bear

FIN7

Gamaredon (also known as Primitive Bear) – active since 2013, unlike most APTs, Gamaredon broadly targets all users all over the globe (in addition to also focusing on certain victims, especially Ukrainian organizations) and appears to provide services for other APTs. For example, the InvisiMole threat group has attacked select systems that Gamaredon had earlier compromised and fingerprinted.

Venomous Bear



Thanks Wikipedia

# # APT: who?

# Turkey

StrongPity (also known as APT-C-41 and PROMETHIUM)



Thanks Wikipedia

# United States  
Equation Group



# Uzbekistan

SandCat, associated with the State Security Service



# Vietnam

OceanLotus (also known as APT32)

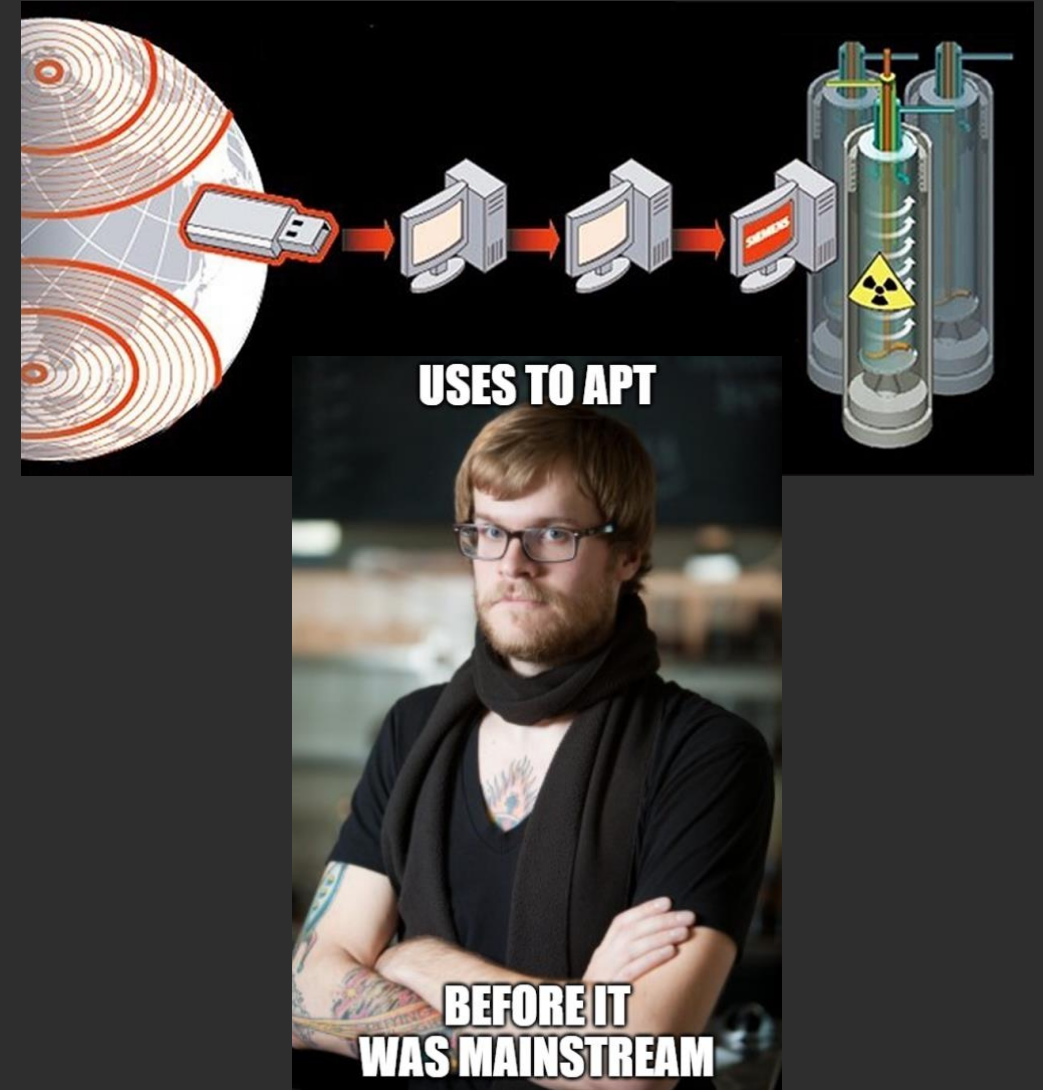


# # APT: honorable mention

The **Stuxnet** computer worm, which targeted the computer hardware of Iran's nuclear program, is one example of an APT attack. In this case, the Iranian government might consider the Stuxnet creators to be an advanced persistent threat.

Stuxnet, discovered by Sergey Ulasen, initially spread via Microsoft Windows, and targeted Siemens industrial control systems.

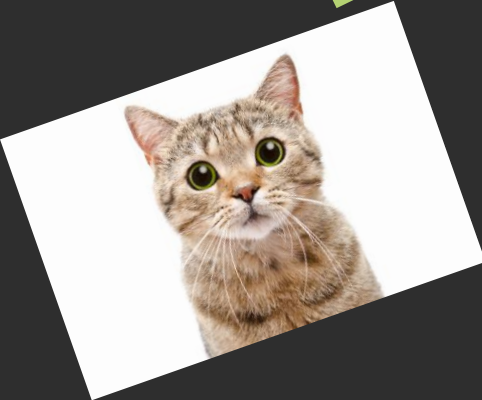
Different variants of Stuxnet targeted five Iranian organizations, with the probable target widely suspected to be uranium enrichment infrastructure in Iran;





# # APT: case study

I studied  
there!



REGIONE DEL VENETO

 **ULSS6**  
EUGANEA

Bandi di gara | Concorsi e avvisi | Albo

Cerca nel sito  

**CORONAVIRUS** COME FARE PER CON NOI UR

**Prenotazione  
vaccinazione  
Covid-19**

**Clicca qui**

- ▶ **Vaccinazioni Anticovid-19**
- ▶ Medici e Pediatri di Famiglia
- ▶ Guardia Medica
- ▶ Farmacie
- ▶ Ospedali
- ▶ Consultori Familiari e Neuropsich
- ▶ Scegli il tuo Medico o Pediatra di
- ▶ Fascicolo Sanitario Elettronico Re
- ▶ Certificazione Verde Covid 19 - GP

 **AVVISO PER GLI UTENTI**

Nella notte i nostri server sono stati oggetto di attacco hacker. Stiamo intervenendo con la massima celerità per ripristinare i servizi. Ci scusiamo per il disagio non dovuto alla nostra volontà

# # APT: case study

3 December 2021

"During the night our servers were subject to a hacker attack. We are acting as quickly as possible to restore services. We apologise for the inconvenience which was

There are **60 technicians** working to minimise the damage caused by the computer incident, Ulss operators and external collaborators who are working on all the wards (hospitals and districts) to reclaim all the machines or certify the 'clean' ones.

The buffer points and **vaccine centres** have started working again, although many wards are working with '**pen and paper**'.

There are still problems in the **emergency room, in radiology, at the cup, at the sampling points and in the analysis laboratories**, where the various teams are concentrating their interventions as a priority.

Inconveniences also in the territorial health service, starting with the general practitioners who could not enter the requests for tracing swabs into the system, as well as inconveniences in the pharmacies, where the medicines to be delivered did not appear.

Meanwhile, in the area, **there have been more than eight hundred positives in the last 24 hours in Padua and its province, but vaccinations are also resuming**, which on Thursday reached figures not seen in a long time: 9200 in total with 650 first doses. not of our making."

# # APT: case study

5 December 2021



HiveLeaks

## Unita Locale Socio

is a social and health local unit intends to qualify as a results-driven company, able, therefore, to reconcile and meet the needs of different stakeholders that are part of the organization itself.

**Website**  
[www.ulss7.it](http://www.ulss7.it)

**Revenue**  
\$800M

**Employees**  
3 000



Encrypted at

**3** December 2021

**02:39:00**



Disclosed at

**6 December 2021**

**20:27:30**

Share



# # APT: case study

11 December 2021

✓ ULSS 6 EUGANEA, AFTER HACKER ATTACK THE COMPUTER NETWORK RESTARTS! ✓

20 December 2021


Following the hacker attack on 3 December, today, Monday 20 December, a number of pick-up points in Padua are reopening for the locations of: Complesso Socio Sanitario ai Colli, Cadoneghe, Piazza Mazzini, Limena, Noventa Padovana, Rubano, Schiavonia (Monselice), Albignasego and Piove di Sacco. On Tuesday the Villatora di Saonara office reopens.

23 December 2021


The infiltration of systems had taken place some time before, as often happens in ransomware attacks. The moment when the problem 'became apparent' was only the final part of the attack.

The loot was not the ransom, but the **exfiltrated data**. In fact, even today, there is still not the slightest hint within the DLS (data leak site) of Hive Ransomware that there is a sample to prove the breach and the start of the sale;

# # APT: case study 18/01/2022


**LOCKBIT 2.0**

**LEAKED DATA**

 [CONDITIONS FOR PARTNERS AND CONTACTS](#) >


**UNTIL FILES**  
**12D 19:11:20**  
**PUBLICATION**

15 Jan, 2022 16:44:00


**aulss6.veneto.it**  
Scopri di più. martedì 21 Dicembre 2021 Variazioni orarie punti tampone dell'Ulss 6 Euganea il 25 e il 1 gennaio 2022 i punti tamponi sono chiusi.  
**ALL AVAILABLE DATA WILL BE PUBLISHED !**

[RETURN BACK](#)

NAME	DATE	SIZE
------	------	------


**LOCKBIT 2.0**

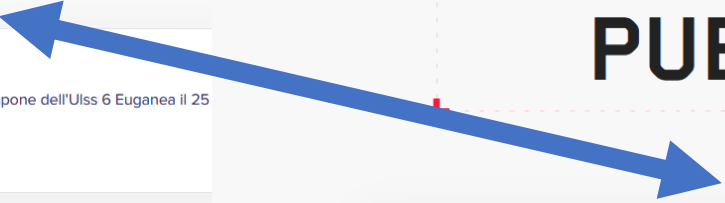
**LEAKED DATA**

 [CONDITIONS FOR PARTNERS AND CONTACTS](#) >

**UNTIL FILES**  
**3D 00:38:42**  
**PUBLICATION**

18 Jan, 2022 16:44:00

**aulss6.veneto.it**  
Scopri di più. martedì 21 Dicembre 2021 Variazioni orarie punti tampone dell'Ulss 6 Euganea il 25 dicembre e il 1 gennaio 2022 i punti tamponi sono chiusi.  
**ALL AVAILABLE DATA WILL BE PUBLISHED !**





# # APT: case study 18/01/2022

  
**Regione del Veneto**  
**AZIENDA U.L.S.S. N. 6 EUGANEA**  
**www.aulss6.veneto.it – P.E.C.: protocollo.aulss6@pecveneto.it**  
Via Enrico degli Scrovegni n. 14 – 35131 PADOVA  
Cod. Fisc. / P. IVA 00349050286  
**OSPEDALI RIUNITI PADOVA SUD**  
**U.O.C. PRONTO SOCCORSO**

**DENUNCIA ALL'AUTORITÀ GIUDIZIARIA**

aggredata a mani nude con trauma spalla destra

reporting to the judicial  
authority

A	B	C	D	E	F	G	H	I	J	K	L	M
Id	IdPaziente	IdLocalPaz			Sesso	DataNas	Descrizione	CreatedOr	ModifiedC	SpecificCh	Issuer	
1	bf98c5fa-36e1	21392814			F	19930816	NULL	2020-10-2	2020-11-1	NULL	PK	
2	1d30e5ac-36e1	0			U	18000101	NULL	2020-10-2	2020-11-1	NULL	ORGANIZER	
3	0b9458ee-631e	20675903			M	19411204	NULL	2020-10-2	2020-11-1	NULL	PK	
4	becd8c75-802e	21023463			F	19451109	NULL	2020-10-2	2020-11-1	NULL	PK	
5	dfb04ebd-9c6e	20694485			F	19681021	NULL	2020-10-2	2020-11-1	NULL	PK	
6	6d8d33ef-8bc0	0			U	19380519	NULL	2020-10-2	2020-11-1	NULL	ORGANIZER	
7	cec9a084-ba5e	0			U	19310513	NULL	2020-10-2	2020-11-1	NULL	ORGANIZER	
8	ffc8bf26-1a94	20803465			M	19610305	NULL	2020-10-2	2020-11-1	NULL	PK	
9	2b626b7c-33c1	0			U	19530321	NULL	2020-10-2	2020-11-1	NULL	ORGANIZER	
10	0f12e7a1-9ab1	0			U	19821028	NULL	2020-10-2	2020-11-1	NULL	ORGANIZER	
11	64c61c12-572e	0			U	19421208	NULL	2020-10-2	2020-11-1	NULL	ORGANIZER	
12	1cf665a3-c3f1	0			U	19300702	NULL	2020-10-2	2020-11-1	NULL	ORGANIZER	
13	f03b0abb-552c	0			U	19610429	NULL	2020-10-2	2020-11-1	NULL	ORGANIZER	
14	e9028832-d3f1	0			U	19830707	NULL	2020-10-2	2020-11-1	NULL	ORGANIZER	
15	7e2526b2-d4f1	0			U	19520121	NULL	2020-10-2	2020-11-1	NULL	ORGANIZER	
16	a20b65aa-a5f1	0			U	19800201	NULL	2020-10-2	2020-11-1	NULL	ORGANIZER	
						19780804	NULL	2020-10-2	2020-11-1	NULL	PK	
						19680208	NULL	2020-10-2	2020-11-1	NULL	ORGANIZER	
						19630401	NULL	2020-10-2	2020-11-1	NULL	PK	
						19311012	NULL	2020-10-2	2020-11-1	NULL	PK	
						19300426	NULL	2020-10-2	2020-11-1	NULL	ORGANIZER	
						19410403	NULL	2020-10-2	2020-11-1	NULL	PK	
						19300208	NULL	2020-10-2	2020-11-1	NULL	ORGANIZER	
						19530129	NULL	2020-10-2	2020-11-1	NULL	ORGANIZER	
						19750508	NULL	2020-10-2	2020-11-1	NULL	ORGANIZER	
						19541203	NULL	2020-10-2	2020-11-1	NULL	PK	
						20040514	NULL	2020-10-2	2020-11-1	NULL	ORGANIZER	
						19350605	NULL	2020-10-2	2020-11-1	NULL	ORGANIZER	
						19860316	NULL	2020-10-2	2020-11-1	NULL	ORGANIZER	
						19570802	NULL	2020-10-2	2020-11-1	NULL	ORGANIZER	

















**aulss6.veneto.it**

Scopri di più, martedì 21 Dicembre 2021 Variazioni orarie punti tampone dell'Usls 6 Euganea il 25 dicembre e il 1 gennaio 2022 i punti tamponi sono chiusi.

**ALL AVAILABLE DATA PUBLISHED !**

[RETURN BACK](#)

NAME	DATE	SIZE
 ulss17.it.c061dpssa	8 Dec, 2021	—
 ulss17.it.deskws2	8 Dec, 2021	—
 ulss17.it.emicroprint1	8 Dec, 2021	—
 ulss17.it.epsonbbu01	8 Dec, 2021	—
 ulss17.it.epsonbbu02	8 Dec, 2021	—
 ulss17.it.mcdges0	8 Dec, 2021	—
 ulss17.it.mradiows6	8 Dec, 2021	—
 ulss17.it.mtampb	8 Dec, 2021	—
 ulss17.it.na1f1057a	8 Dec, 2021	—
 ulss17.it.na1f1100f	8 Dec, 2021	—
 ulss17.it.na1f1113e	8 Dec, 2021	—
 ulss17.it.na1f1125d	8 Dec, 2021	—
 ulss17.it.na30076a	8 Dec, 2021	—
 ulss17.it.na30078a	8 Dec, 2021	—

reservations

all files

# # APT: case study 18/01/2022

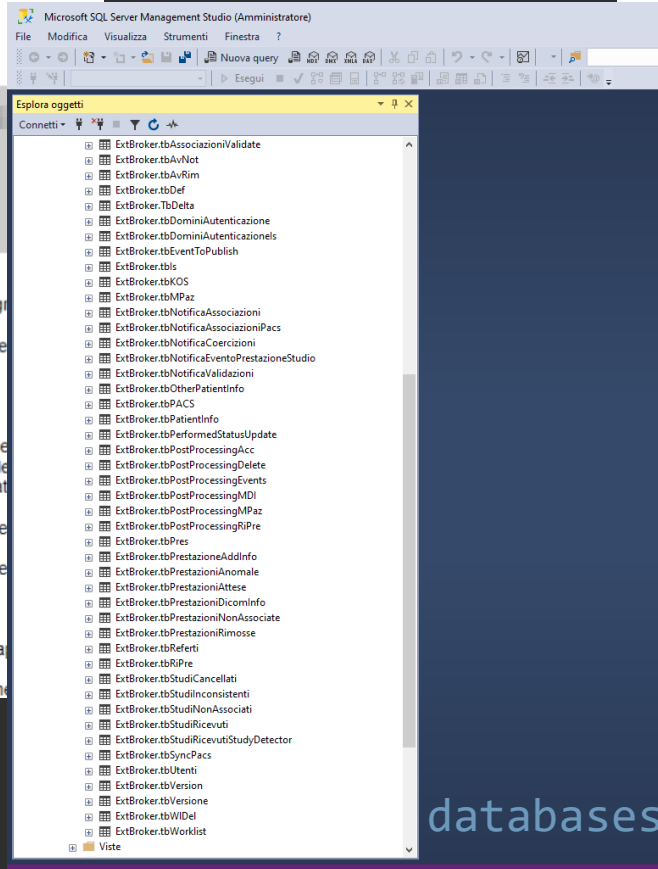
REGIONE DEL VENETO  
**ULSS6**  
Azienda ULSS 6 Euganea  
Via E. degli Scrovegni 14  
35131 Padova  
CF e P.Iva: 00349050286  
www.ulss6.veneto.it

**OSPEDALI RIUNITI PADOVA SUD**  
**U.O.C. Radiologia**  
Direttore: [REDACTED]  
Mail: radiologia.mons@ulss6.veneto.it  
Tel. Segreteria: 0429/715622 Tel. Coordinatore 0429/715668

Cognome e nome: [REDACTED] Data di nascita: [REDACTED]  
Codice fiscale: [REDACTED] Residenza: [REDACTED]  
Comune: [REDACTED] Telefono: [REDACTED]  
Provenienza: [REDACTED] N. Referto: [REDACTED]  
Data Referto: [REDACTED] Data Esame: [REDACTED]

Mezzo di Contrasto: Dotagraf 0.5 mmol/ml Quantità: 14 ml Flusso infusione: 2.5 ml/s  
RM ADDOME SUPERIORE (SENZA E CON MDC)

Esame eseguito prima e dopo somministrazione e.v. di MDC, anche con sequenze colangiografiche. Con colangio-RM, non dilatazione delle vie biliari intraepatiche. Colecisti distesa senza evidenza di vuoti di segnale riferibili a calcoli nel suo lume; essa presenta contenuto tenuemente iperintenso nelle sequenze T1w compatibile con lieve sludge biliare endoluminale. Nei limiti il calibro del coledoco. Nei limiti il calibro del dotto pancreatico principale. Nel pancreas, lungo il decorso del Wirsung, in apparente continuità con esso, in sede di processo uncinato, nel corpo e nella coda si apprezzano alcune piccole aree di iperintensità del segnale nelle sequenze a TR lungo, di tipo fluido, la maggiore di circa 10 mm, compatibili più con focali dilatazioni dei dotti secondari che con IPMN. Non aree di restrizione del segnale nelle sequenze DWI, né aree di enhancement sospette nel contesto del pancreas. Fegato nei limiti per dimensioni presenta alcune formazioni ovalari iperintense nelle sequenze lungo nel suo contesto, la maggiore di circa 8 mm nel II segmento, compatibili con cisti. Milza nei limiti per dimensioni con asse bipolare massimo di circa 10 cm. Spleno di circa 12 mm in adiacenza dell'ilo splenico. Reni in sede, entrambi presentano alcune piccole formazioni cistiche, in sede corticale e paracorticale. Non calico-pielectasie bilateralmente. Plurimi linfonodi sparsi nel ventaglio mesenteriale, i maggiori con asse corto attorno al centimetro.



20.11.2021

**DATA 31.12.2020**

DIAGNOSI TOSSE, FEBBRE BRONCOOSTRUZIONE.

ACCERTAMENTI RX TORACE, ECG, ESAMI. TROPONINA IN PLATEAU

PROGRAMMA MEGLIO DOPO TERAPIA CION STEROIDE E BRONCODILATATORE. APIRETICA.

Esito: RIC DIM

Diagnosi SINCOPE RECIDIVANTE. MONITOR.

Accertamenti IN MONITOR, VISITA CARDIOLOGICA ESAMI DA RIVEDERE DOMANI

Programma domani esami.

Esito: RIC DIM

DIAGNOSI. STATO SOPOROSO, IPORESSIA, DISIDRATAZIONE, VOMITO. T.CRANICO IN ANTICOAGULATO

ACCERTAMENTI RX TORACE, ESAMI, VISITA NEFROLOGICA, TAC CEREBRALE

FERMA OPPOSIZIONE DELLA FIGLIA ALL DIMISSIONE. LUNEDI CHIEDERE OATTIVAZIONE PER INSERIMENTO IN ODC. O TRASFERIMENTO A VILLA MARIA

DIAGNOSI STATO DI AGITAZIONE. IN EPILETTICO. CASO SOCIALE.

medical reports

databases

medical examinations



# cybersecurity challenge



This is the end of the Great Wall of China



I have no idea

What I'm doing

# # external security

monitoring



hardening



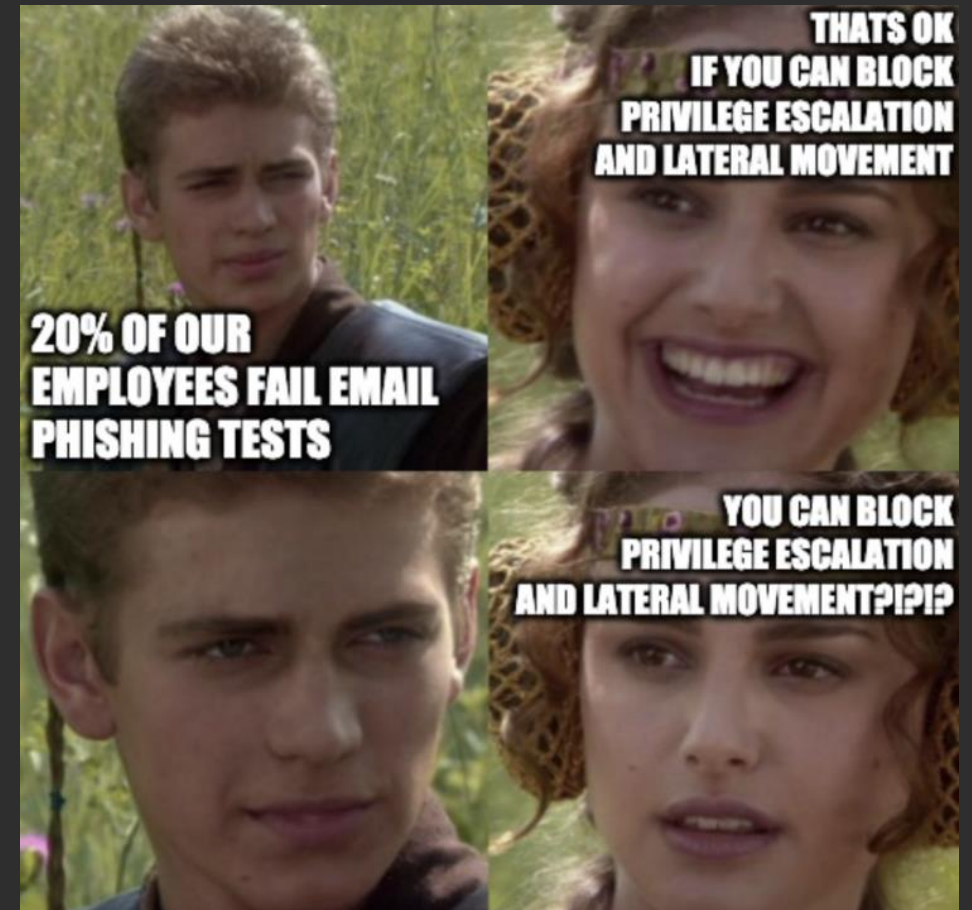
testing





# # internal security

- network segmentation
- EDR
- hardening
- monitoring
  - activities
  - accounts
  - privileges
- testing





# # availability

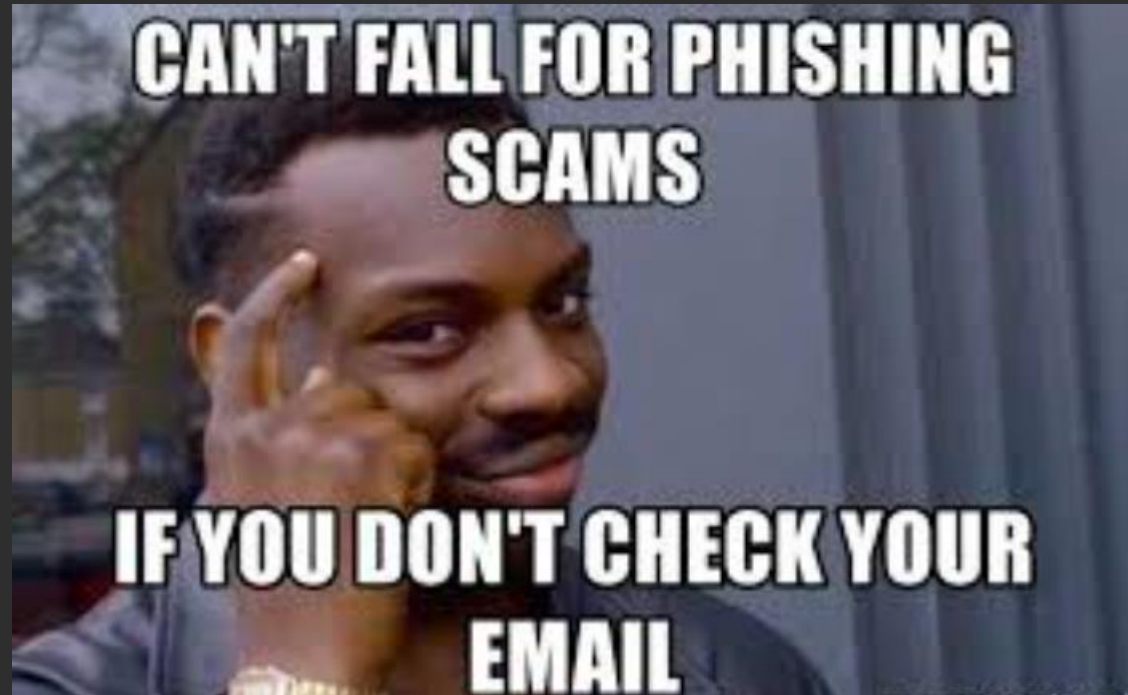
Users should use data

Availability
The information is available to authorized users when needed.
I send you a message, and you are able to receive it.



# # phishing / human firewall

- 0 trust
- avoid social engineering
- learn how to detect it
- secure passwords
- don't reuse passwords
- MFA everywhere



# # phishing: a weird story

A customer called me to test network security, they didn't call it Red Team yet.

They had done an excellent job from the Cybersec point of view, and I could not actually attack anything from the outside, plus there was no conceivable physical intrusion since there were even armed guards in the data centre.

I knew the target, I knew where the data centre was and I knew where their offices were located

# # phishing: a weird story

Time for trashing:

Information diving is the practice of recovering technical data, sometimes confidential or secret, from discarded material.



I found a copy of a packing slip for a UPS (Uninterruptible Power Supply) where the exact model and serial number of the unit was written.

Looked like a datacenter UPS



# # phishing: a weird story

I looked for authorised repairers of the UPS brand and luckily one of them had closed down the company.



Cybersquatting is the practice of registering, trafficking in, or using an Internet domain name, with a bad faith intent to profit from the goodwill of a trademark belonging to someone else.



# # phishing: a weird story

I created a website of “✧ My Shiny New Company ✧” with various information taken here and there from the web. At a certain point, thanks to the content and HTTPS, the search engines decided it could be at the top of the list.



I was really so serious

# # phishing: a weird story

after a bit of research on Linkedin I found the right person to call about UPS problems in their datacenter and so I contacted him via mail.

Good morning Mr. XXX

I am XXX and I work for "✧ My Shiny New Company ✧"

we are aware that your UPS model may have problems with the batteries and there is a risk that they will overcharge and burn out.

We will arrange for the repair completely free of charge.

# # phishing: a weird story

It's a Breach ;D



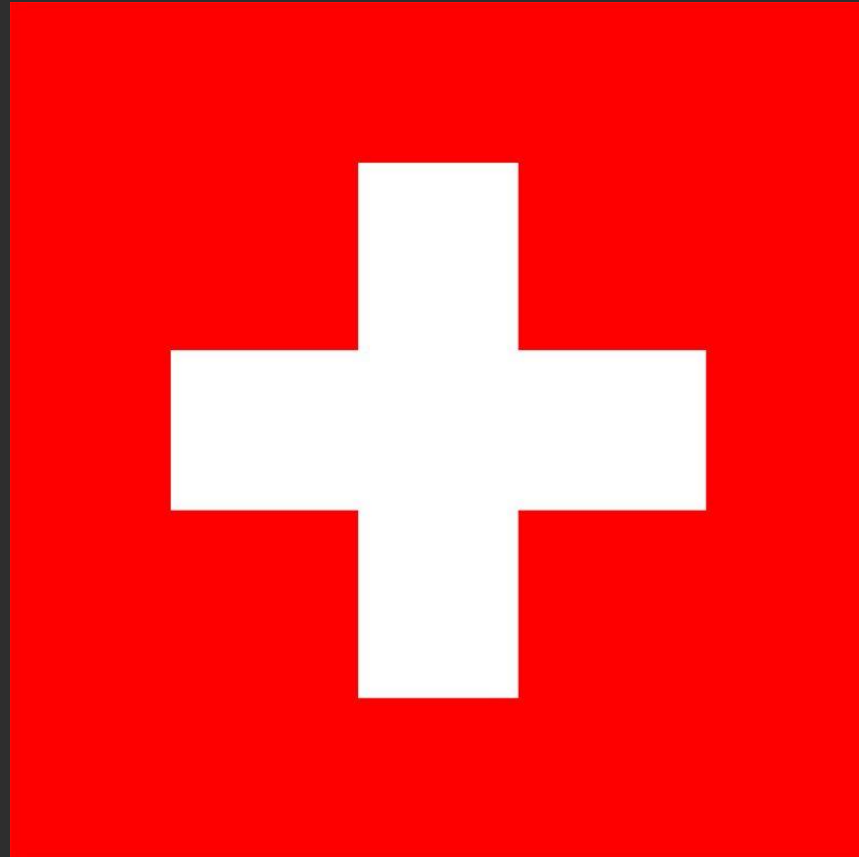


# leak time



# # leak time: who?

[https://en.wikipedia.org/wiki/List\\_of\\_hospitals\\_in\\_Switzerland](https://en.wikipedia.org/wiki/List_of_hospitals_in_Switzerland)



Thanks Wikipedia

# # leak time: exposed addresses

Città	Ospedali e cliniche	Dominio	Indirizzo IP	Range indirizzi IP	Note
Zurich	Hirslanden Clinic	<a href="http://www.hirslanden.ch">www.hirslanden.ch</a>	195.225.33.211	195.225.32.0 - 195.225.33.255	-
	Im Park Clinic	-	-	-	questa clinica è collegata alla Hirslanden Clinic, stesso dominio w
	See Spital	<a href="http://see-spital.ch">see-spital.ch</a>	217.26.51.192	217.26.51.0/24	-
	Stadtspital Triemli	<a href="http://www.stadt-zuerich.ch">www.stadt-zuerich.ch</a>	194.56.34.182	194.56.0.0 - 194.56.71.255	range del comune di zurigo
	University Hospital of Zurich	<a href="http://www.usz.ch">www.usz.ch</a>	144.200.16.203	144.200.0.0/16	AS559
	Waidspital	<a href="http://www.stadt-zuerich.ch">www.stadt-zuerich.ch</a>	194.56.34.182	194.56.0.0 - 194.56.71.255	range del comune di zurigo
Geneva	Geneva University Hospitals	<a href="http://www.hug.ch">www.hug.ch</a>	129.195.247.51	-	-
	Hirslanden Clinique La Colline	<a href="http://www.hirslanden.ch">www.hirslanden.ch</a>	195.225.33.211	195.225.32.0 - 195.225.33.255	-
Basel	Bethesda-Spital	<a href="http://www.bethesda-spital.ch">www.bethesda-spital.ch</a>	91.212.196.155	-	-
	Birshof Klinik	<a href="http://www.hirslanden.ch">www.hirslanden.ch</a>	195.225.33.211	195.225.32.0 - 195.225.33.255	-
	Bruderholzspital	<a href="http://www.ksbl.ch">www.ksbl.ch</a>	193.108.137.40	-	-
	Claraspital	<a href="http://www.claraspital.ch">www.claraspital.ch</a>	5.148.180.219	-	-
	Felix Platter-Spital	<a href="http://www.felixplatter.ch">www.felixplatter.ch</a>	18.200.205.202	-	amazon
	Merian Iselin-Spital	<a href="http://merianiselin.ch">merianiselin.ch</a>	149.126.4.74	-	-
	University Hospital of Basel	<a href="http://www.unispital-basel.ch">www.unispital-basel.ch</a>	145.250.210.164	145.250.128.0 - 145.250.255.255	-
Lausanne	University Hospital of Lausanne (CHUV)	<a href="http://www.lausanneuniversityhospital.com">www.lausanneuniversityhospital.com</a>	195.15.231.102	-	-
	Hirslanden Clinique Cecil	<a href="http://www.hirslanden.ch">www.hirslanden.ch</a>	195.225.33.211	195.225.32.0 - 195.225.33.255	-
	Hirslanden Clinique Bois-Cerf	<a href="http://www.hirslanden.ch">www.hirslanden.ch</a>	195.225.33.211	195.225.32.0 - 195.225.33.255	-
	Clinique de Montchoisi	<a href="http://www.montchoisi.ch">www.montchoisi.ch</a>	5.148.168.203	-	-
	Clinique La Source Lausanne	<a href="http://www.lasource.ch">www.lasource.ch</a>	213.193.102.212	213.193.102.192 - 213.193.102.223	-
Bern	Lindenhofspital	<a href="http://www.lindenhofgruppe.ch">www.lindenhofgruppe.ch</a>	82.199.159.116	-	82.199.159.64 - 82.199.159.127 ? fa parte di un gruppo.
	Permanence Clinic	<a href="http://www.permanence.ch">www.permanence.ch</a>	94.126.22.200	-	-
	Salem Hospital	<a href="http://hirslanden.ch">hirslanden.ch</a>	195.225.33.211	195.225.32.0/23	-
	Sonnenhof Hospitals Ltd., Klinik Sonnenhof & Klinik Engeried Bern	<a href="http://www.lindenhofgruppe.ch">www.lindenhofgruppe.ch</a>	82.199.159.116	-	82.199.159.64 - 82.199.159.127 ? fa parte di un gruppo.
	Tiefenauspital	<a href="http://www.spitaltiefenau.ch">www.spitaltiefenau.ch</a>	161.62.248.145	161.62.0.0 - 161.62.255.255	-
	University Hospital of Bern	-	-	-	-
	Zieglerspital	-	-	-	-



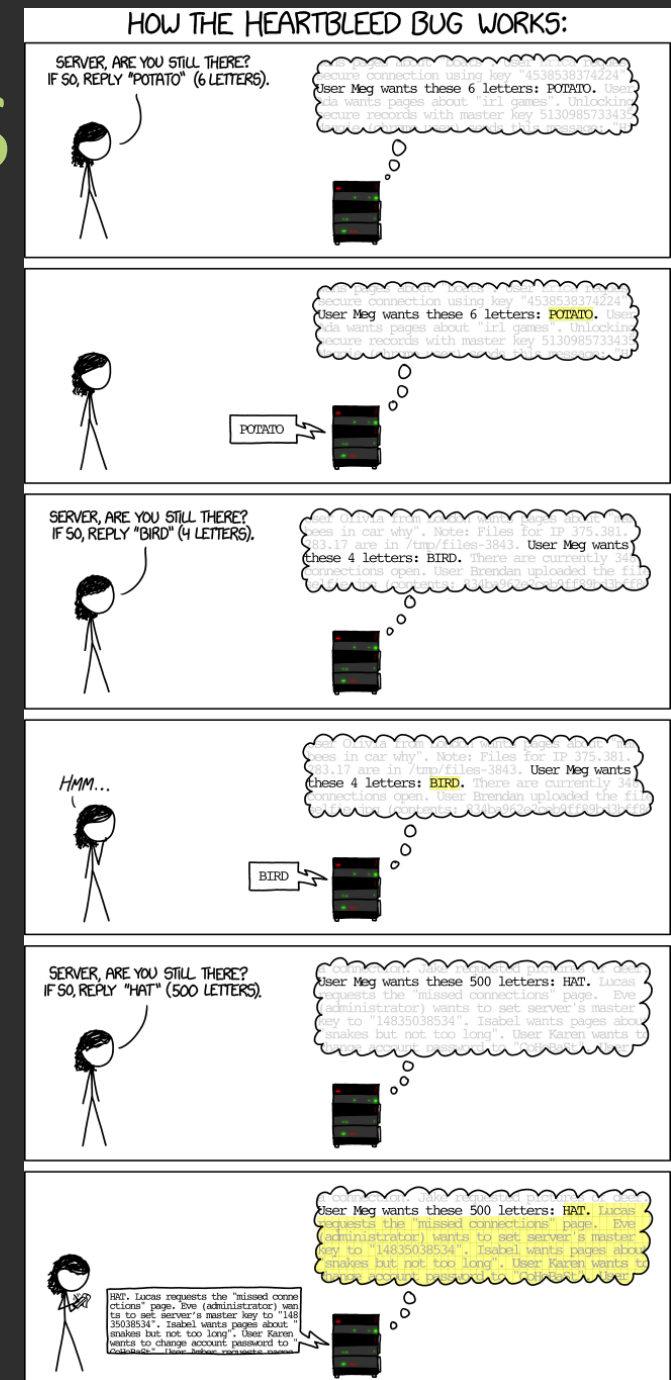
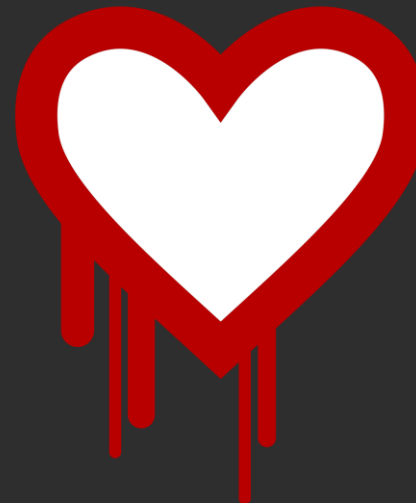
# # leak time: vulnerabilities

Exposed Services: 160

Domains/Subdomains: 637

Vulnerabilities on Domains/Subdomains:

By passive scan: 42 + 40 Heartbleed (SSL)



# # leak time: data leakage

Number of discovered leaks: 1282:

- only email address: 35
- email address and plain password: 1247

Please check: <https://haveibeenpwned.com/>

The logo for 'Have I Been Pwned?' is displayed within a blue square. It features the text 'have i been pwned?' in a white, lowercase, sans-serif font, with a semicolon and two dashes at the beginning.

‘;--have  
i been  
pwned?

# end

