IT Security

Gioele Schirripa
GDG Reggio Calabria Manager

Francesco Fresta
Associate Consultant @ TIBCO Software Inc.

Chi sono

DTU Technical University of Denmark & DTU Skylab - where it begins

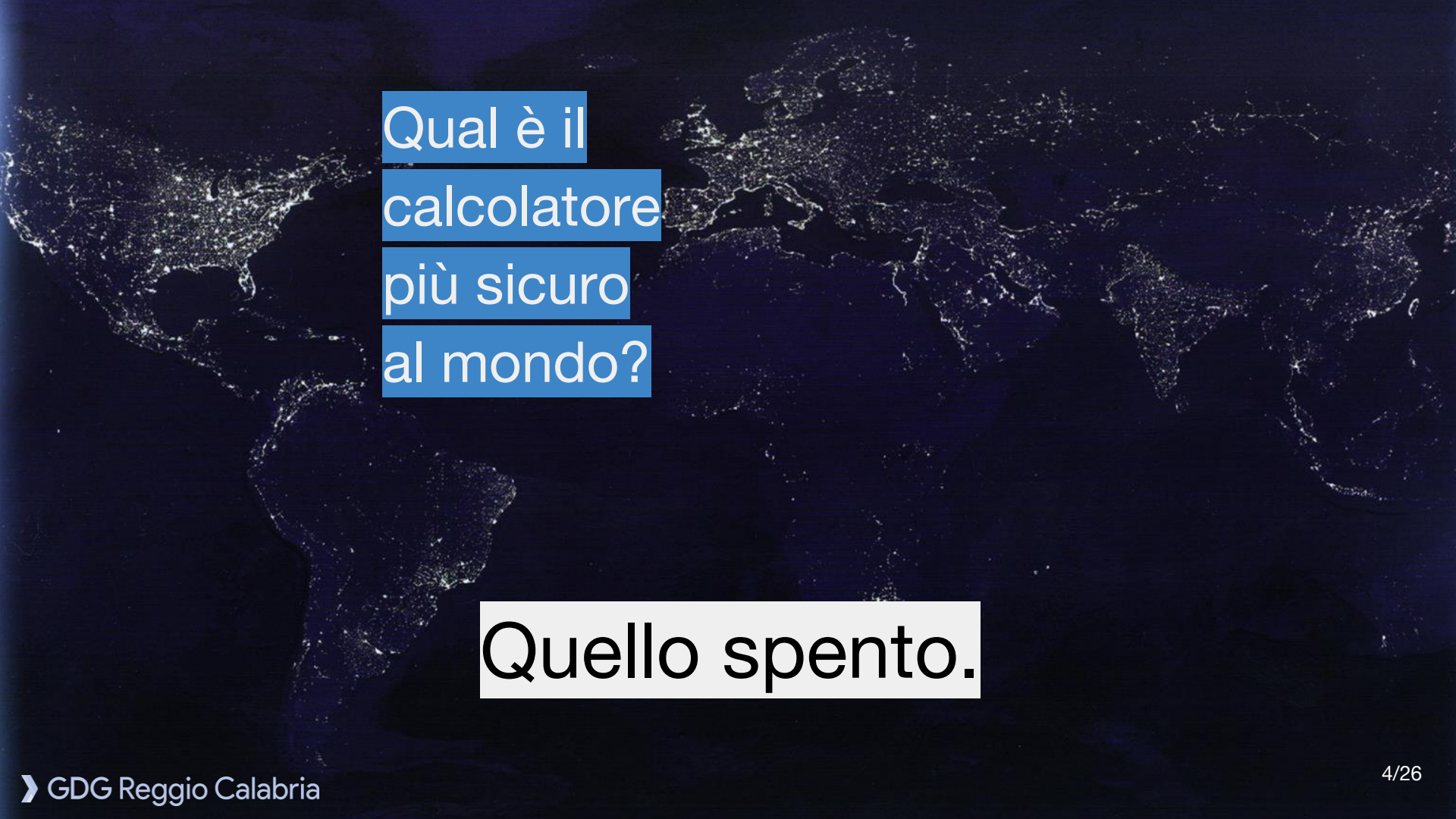
The University Of Sheffield.

GDG

TIBCO™

Obiettivi

Analisi degli attacchi più comuni.
Tecniche di difesa e best practices.


Qual è il
calcolatore
più sicuro
al mondo?
Quello spento.

Che cos’è la sicurezza informatica?

È una parte fondamentale dell’Informatica che si occupa di analizzare le minacce e le vulnerabilità nei dispositivi informatici al fine di proteggerli da eventuali attacchi.

Sicurezza informatica - Perché?

Privacy

Protezione

Crescente uso della Rete

Attacchi informatici

Accesso fisico

Attacco nel quale il criminale ha accesso ai locali, eventualmente anche agli stessi terminali.

- Interruzione di corrente
- Vandalismo
- Apertura del case e furto del disco rigido

Phishing

Truffa su Internet attraverso la quale, un malintenzionato, fingendosi un soggetto affidabile, cerca di convincere l’utente a fornire dati sensibili.

Virus informatico

È un programma che infetta i file e il sistema operativo della vittima.

Questo tipo di attacco è rivolto ai calcolatori in generale*

Malware Spyware Worm Adware Rootkit Keylogger ...

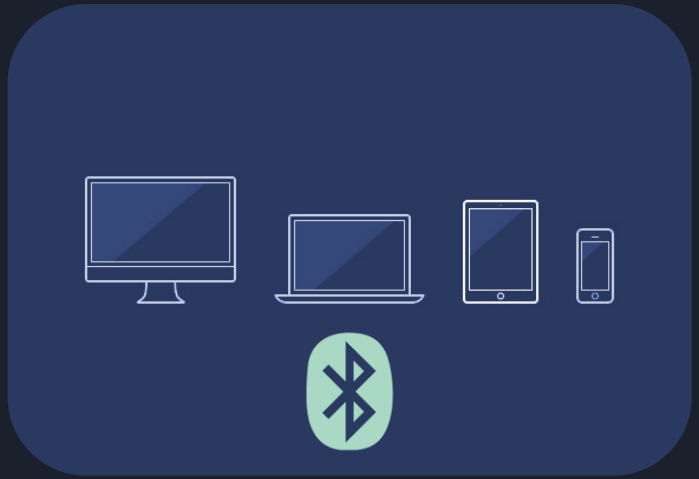
Ransomware

"Tengono in ostaggio" i dati e i file dell'utente finché non paga una somma di denaro per sbloccarli.

Tipologia di attacco - Nocivo

Bluesnarfing

È una tecnica impiegata per accedere senza autorizzazione ad informazioni memorizzate in qualsiasi dispositivo dotato di connessione Bluetooth.



Altri attacchi

Swatting	Ingegneria sociale	Defacing
Mailbombing	Calcolo parassita	SQL Injection
Backdoor	Catena di Sant'Antonio	Arbitrary code execution
Shoulder surfing	Jamming	Rogue access point

Strumenti per la difesa

Strumenti base

Buonsenso

Antivirus & Antispyware

Password complesse

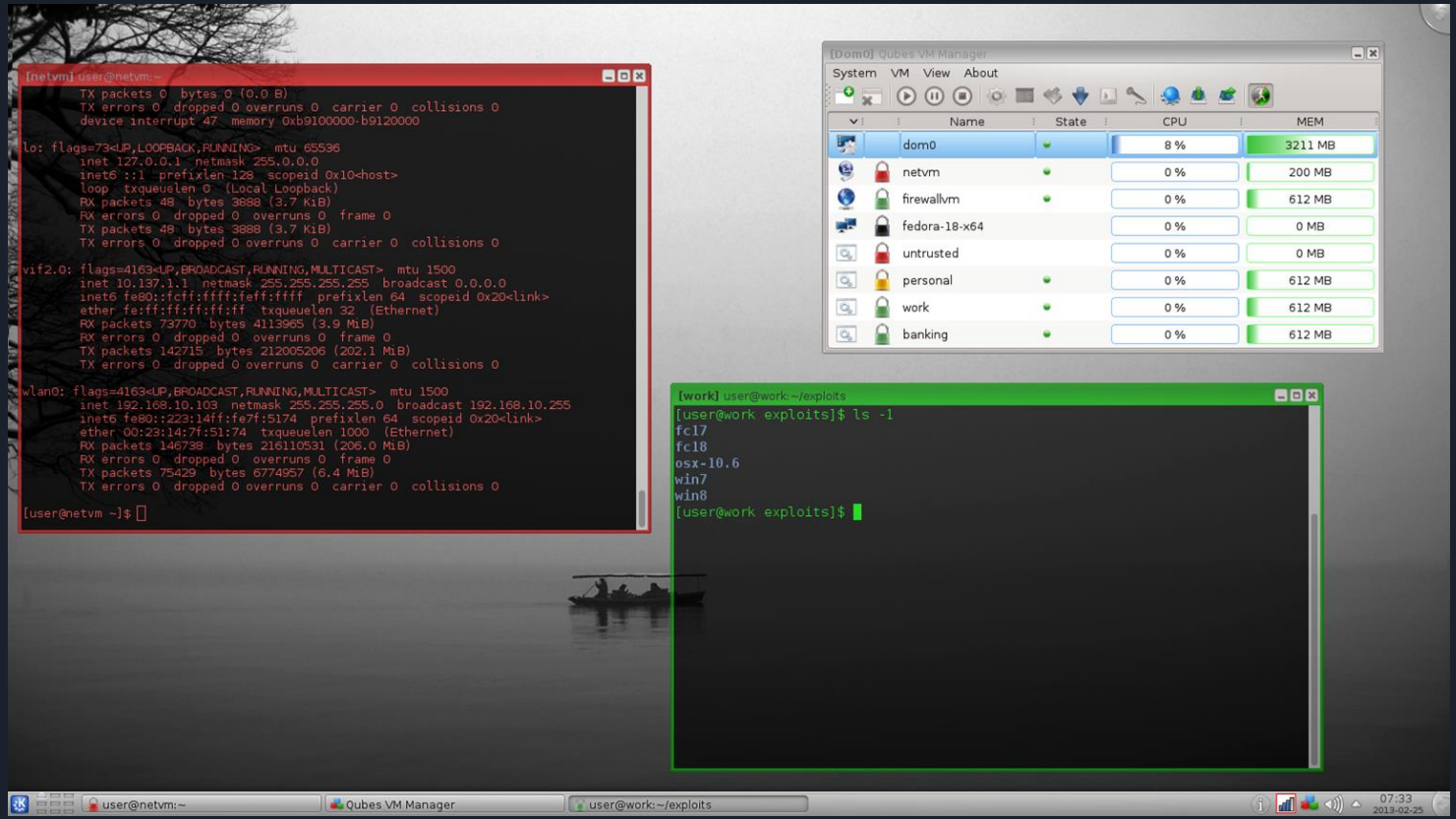
S.O e software originali e aggiornati

AdBlock & HTTPS Everywhere

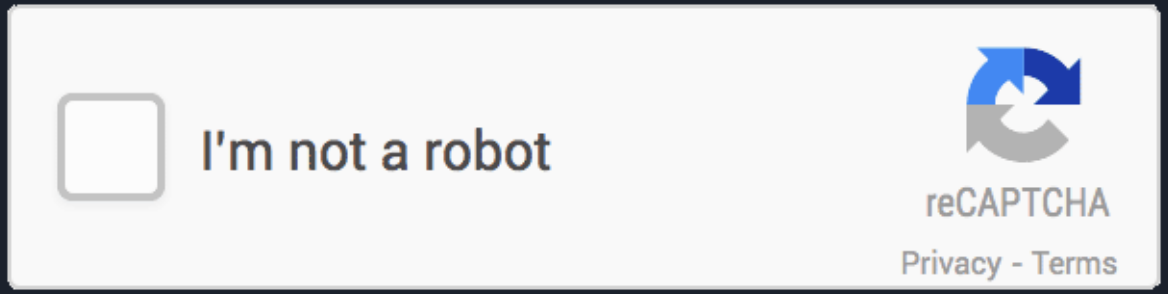
Consente di filtrare contenuti indesiderati e impedire che vengano mostrati alcuni elementi ingannevoli della pagina Web.

Permette di forzare l’uso del protocollo HTTPS nei siti che lo supportano.

Qubes OS


[netvm] user@netvm:~
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
device interrupt 47 memory 0xb9100000-b9120000
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 0 (Local Loopback)
RX packets 48 bytes 3888 (3.7 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 48 bytes 3888 (3.7 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
vif2.0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.137.1.1 netmask 255.255.255.255 broadcast 0.0.0.0
inet6 fe80::fcff:ffff:feff:ffff prefixlen 64 scopeid 0x20<link>
ether fe:ff:ff:ff:ff:ff txqueuelen 32 (Ethernet)
RX packets 73770 bytes 4113965 (3.9 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 142715 bytes 212005206 (202.1 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.10.103 netmask 255.255.255.0 broadcast 192.168.10.255
inet6 fe80::223:14ff:fe7f:5174 prefixlen 64 scopeid 0x20<link>
ether 00:23:14:7f:51:74 txqueuelen 1000 (Ethernet)
RX packets 146738 bytes 216110531 (206.0 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 75429 bytes 6774957 (6.4 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
[user@netvm ~]$
[Dom0] Qubes VM Manager
System VM View About
Name State CPU MEM
dom0 8 % 3211 MB
netvm 0 % 200 MB
firewallvm 0 % 612 MB
fedora-18-x64 0 % 0 MB
untrusted 0 % 0 MB
personal 0 % 612 MB
work 0 % 612 MB
banking 0 % 612 MB
[work] user@work:~/exploits
[user@work exploits]$ ls -1
fc17
fc18
osx-10.6
win7
win8
[user@work exploits]$
user@netvm:~
Qubes VM Manager
user@work:~/exploits
07:33
2013-02-25

CAPTCHA



BleachBit

BleachBit è un software libero e gratuito, scritto in Python, per la pulizia del disco, la tutela della privacy e l'ottimizzazione del proprio S.O.

Per approfondire

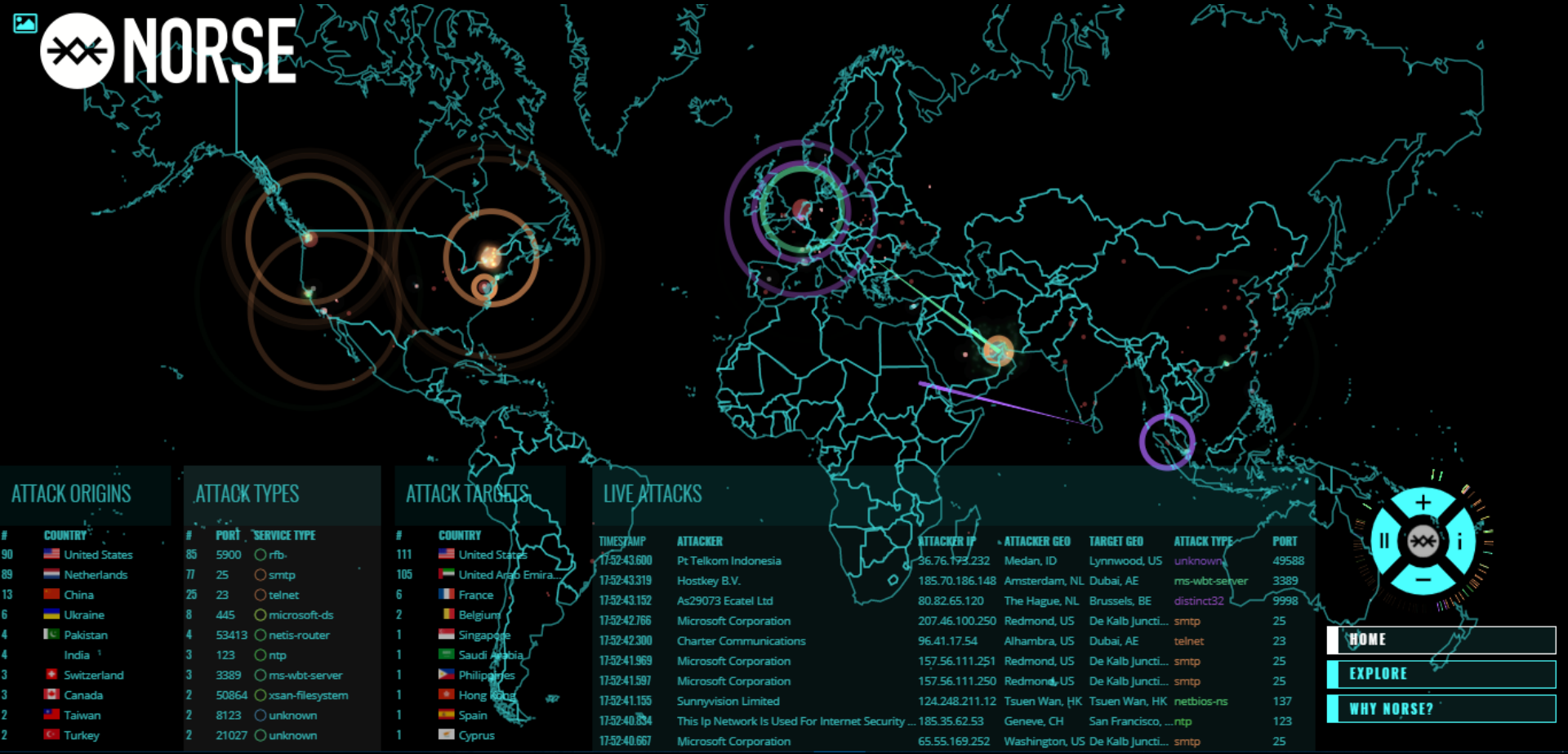
The Onion Router (TOR)

Virtual Private Network (VPN)

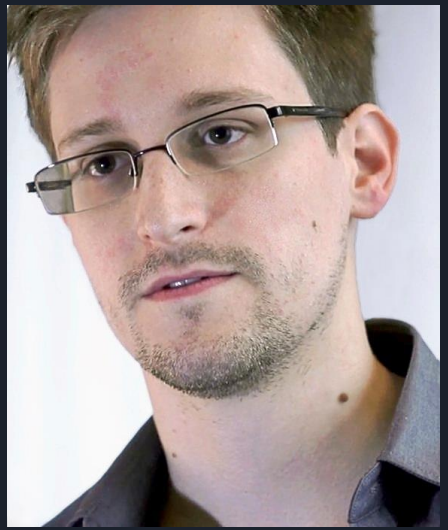
Bitcoin

Pretty Good Privacy (PGP)

Kali Linux, Tails OS, …


NORSE
ATTACK ORIGINS
COUNTRY
90 United States
89 Netherlands
13 China
6 Ukraine
4 Pakistan
4 India
3 Switzerland
3 Canada
2 Taiwan
2 Turkey
ATTACK TYPES
PORT SERVICE TYPE
85 5900 rfb
77 25 smtp
25 23 telnet
8 445 microsoft-ds
4 53413 netis-router
3 123 ntp
3 3389 ms-wbt-server
2 50864 xsan-filesystem
2 8123 unknown
2 21027 unknown
ATTACK TARGETS
COUNTRY
111 United States
105 United Arab Emira...
6 France
2 Belgium
1 Singapore
1 Saudi Arabia
1 Philippines
1 Hong Kong
1 Spain
1 Cyprus
LIVE ATTACKS
TIMESTAMP ATTACKER ATTACKER IP ATTACKER GEO TARGET GEO ATTACK TYPE PORT
17:52:43.600 Pt Telkom Indonesia 36.76.173.232 Medan, ID Lynnwood, US unknown 49588
17:52:43.319 Hostkey B.V. 185.70.186.148 Amsterdam, NL Dubai, AE ms-wbt-server 3389
17:52:43.152 As29073 Ecatel Ltd 80.82.65.120 The Hague, NL Brussels, BE distinct32 9998
17:52:42.766 Microsoft Corporation 207.46.100.250 Redmond, US De Kalb Juncti... smtp 25
17:52:42.300 Charter Communications 96.41.17.54 Alhambra, US Dubai, AE telnet 23
17:52:41.969 Microsoft Corporation 157.56.111.251 Redmond, US De Kalb Juncti... smtp 25
17:52:41.597 Microsoft Corporation 157.56.111.250 Redmond, US De Kalb Juncti... smtp 25
17:52:41.155 Sunnyvision Limited 124.248.211.12 Tsuen Wan, HK Tsuen Wan, HK netbios-ns 137
17:52:40.834 This Ip Network Is Used For Internet Security ... 185.35.62.53 Geneve, CH San Francisco, ... ntp 123
17:52:40.667 Microsoft Corporation 65.55.169.252 Washington, US De Kalb Juncti... smtp 25
HOME
EXPLORE
WHY NORSE?

Inoltre...



“Io, alla mia scrivania, sono di certo autorizzato ad intercettare chiunque, da uno come lei a un giudice federale e persino al Presidente, se intendessi entrare nella sua posta elettronica personale.”

Domande?

Per saperne di più...

“Il mondo nella Rete, quali i diritti quali i vincoli”, Stefano Rodotà, iLibra, 2014

it.wikipedia.org/wiki/Categoria:Tecniche_di_attacco_informatico

https://blog.kaspersky.it

Grazie per l’attenzione

Per qualsiasi informazione puoi contattarci ai seguenti indirizzi

https://www.facebook.com/GDGReggioCalabria/

https://www.meetup.com/GDG-Reggio-Calabria/

IT Security

Gioele Schirripa
GDG Reggio Calabria Manager

Francesco Fresta
Associate Consultant @ TIBCO Software Inc.