



IT Security

Gioele Schirripa

Project Management Consultant

Francesco Fresta

Associate Consultant @ TIBCO Software Inc.



Chi sono






Obiettivi

Analisi degli attacchi

Tecniche di difesa

Best practices



Qual è il
dispositivo
più sicuro
al mondo?

Quello spento.



IT Security

Si basa su tre concetti importanti

Disponibilità dei dati

Integrità dei dati

Riservatezza informatica





IT Security - Perché?

Privacy

Protezione

Crescente uso della Rete



Attacchi informatici



Accesso fisico

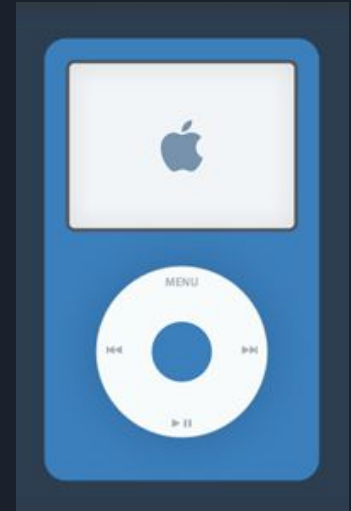
Attacco nel quale il criminale ha materialmente accesso ai locali

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

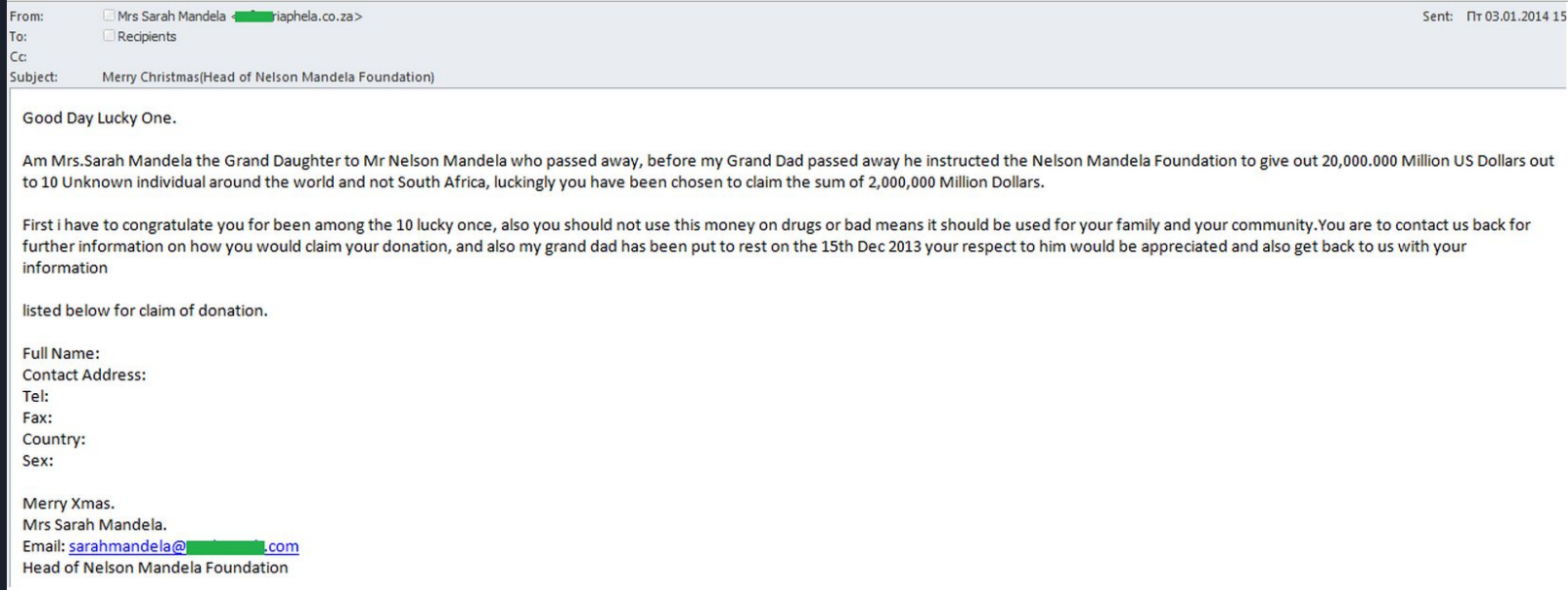


Pod slurping

Usare un dispositivo portatile, es. un iPod, per scaricare enormi quantità di dati, collegandolo direttamente al sistema che li contiene.



Phishing



https://www.ted.com/talks/james_veitch_this_is_what_happens_when_you_reply_to_spam_email

Swatting



▶ ▶ 🔊 0:42 / 6:12

⌂ ⚙️ 📺 🖥️ 🗑️

Jordan(Kootra) of The Creatures gets SWATTED on stream

Prossimi video

RIPRODUZIONE AUTOMATICA 🔴

11/34

Malware

Esecuzione di **malicious software** così da disturbare le operazioni svolte dai sistemi.

Questo tipo di attacco è rivolto a vari dispositivi*



Dialer Worm Adware Backdoor Rootkit Keylogger ...

Ransomware

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



SQL Injection

Questa tecnica prevede l'iniezione di codice SQL, al solo scopo di accedere, manomettere o distruggere una base di dati.





SQL Injection

Solitamente per attuare l'attacco l'utente inserisce del codice SQL nei campi `<input>` della pagina Web.

Il comando SQL verrà eseguito sulla base di dati a nostra insaputa.

```
$txtUserId = $_GET["UserId"];  
$txtSql = "SELECT * FROM Users WHERE UserId = ".$txtUserId;
```



SQL Injection

Se non è previsto un sistema di controllo dei caratteri inseriti, può digitare qualcosa come

1001 OR 1=1

La query corrispondente sarà

```
SELECT * FROM Users WHERE UserId = 1001 OR 1=1;
```

La query è valida, poiché OR 1=1 è sempre TRUE.

Altri attacchi

Cross-site scripting

Ingegneria sociale

Mailbombing

Calcolo parassita

Catena di Sant'Antonio

Bufala

Bufala

Jamming



Shoulder surfing



Catena di Sant'Antonio



Germania. Angela Merkel annuncia il rimpatrio degli italiani che preferiscono il vino alla birra

Oggi











Mi hanno chiesto di diffonderlo dal policlinico per il reparto pediatria... Mi aiuti a diffonderlo? C'è bisogno di sangue A RH negativo x una bambina che sta molto male.. aiutate a diffonderlo. La referente è [redacted] - tel. [redacted] [0857172](tel:0857172) Mandalo ai tuoi contatti WhatsApp per favore. grazie

11:04

Come (non) difendersi

10 RISKIEST EMPLOYEE BEHAVIORS



1  Using personal devices to connect to the organization's network.	2  Sharing passwords with others within the organization.	3  Using the same username and password for websites and online accounts.	4  Using USB devices that have not been encrypted to store confidential data.	5  Failing to delete unnecessary, but confidential data from devices.
6  Not using privacy screens when working remotely on confidential data.	7  Accessing the internet via unsecured networks while working.	8  Failing to notify after losing USB or other devices with confidential data.	9  Leaving devices unattended when away from the work-place.	10  Carrying unnecessary confidential data on devices when traveling.

Strumenti per la difesa



Strumenti base

Calma e circospezione

Impostare password complesse

Installare un software di protezione

Software originale e aggiornato





Calma e circospezione

Essere prudenti e diffidenti nei confronti di tutto ciò che vediamo ci permette di evitare gran parte dei pericoli.



Generare password sicure

0. Scegliere un nome

1. Trasformare alcuni caratteri

2. Aggiungere in testa e in coda dei caratteri
Le password sono come le mutande: le cambi spesso

3. Alla fine inserire una lettera legata al servizio da proteggere
Le prestiti agli altri non le far vedere alle persone in giro (si spera).



francesco -> Fr@ncesc0 -> PFr@ncesc0W -> PFr@ncesc0W_E

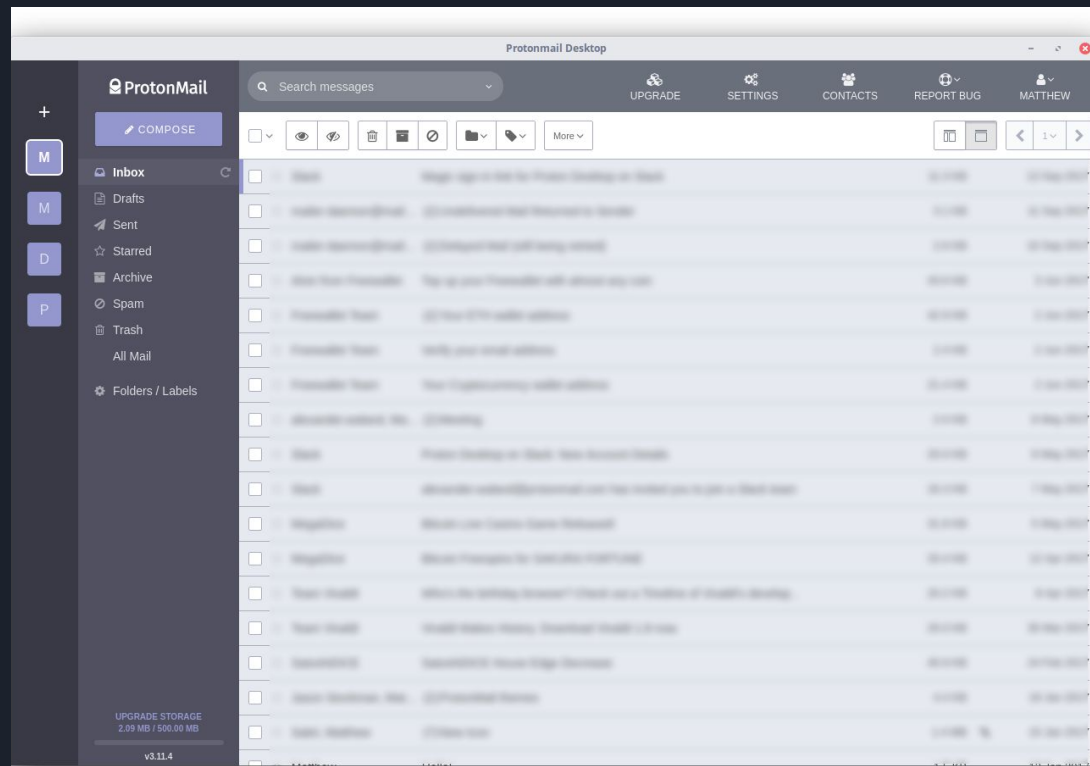
AdBlock & HTTPS Everywhere

Consente di filtrare contenuti indesiderati e impedire che vengano mostrati alcuni elementi ingannevoli della pagina web. Permette di bloccare la pubblicità, anche su YouTube.

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



ProtonMail



"The only email system NSA can't access" [Forbes]



Le domande di sicurezza

Quando si crea un nuovo account, rispondere alle domande di sicurezza per il ripristino delle password dimenticate con parole senza senso.

Qual è la città dove è nata tua madre?

Milano

Qubes OS

The screenshot displays the Qubes OS desktop environment. At the top left, there is a blue and green geometric logo. The desktop background features a serene image of a small boat on a calm body of water. Three windows are open:

- Terminal Window (top left):** Displays network statistics for the 'netvm' user. The output shows details for the loopback interface 'lo' and the Ethernet interface 'vif2.0', including flags, IP addresses, netmasks, broadcast addresses, and packet statistics (RX/TX packets, bytes, errors, dropped, overruns, carrier, collisions).
- Qubes VM Manager (top right):** A window titled '[Dom0] Qubes VM Manager' showing a table of virtual machines. The table has columns for Name, State, CPU, and MEM.
- Terminal Window (bottom right):** Displays the file listing for the '/exploits' directory, showing files named 'fc17', 'fc18', 'osx-10.6', 'win7', and 'win8'.

The taskbar at the bottom shows the current user as 'user@netvm:~' and the active window as 'user@work: ~/exploits'. The system clock in the bottom right corner indicates the time as 07:33 on 2019-02-25.

Name	State	CPU	MEM
dom0	Running	8 %	3211 MB
netvm	Running	0 %	200 MB
firewallvm	Running	0 %	612 MB
fedora-18-x64	Running	0 %	0 MB
untrusted	Running	0 %	0 MB
personal	Running	0 %	612 MB
work	Running	0 %	612 MB
banking	Running	0 %	612 MB

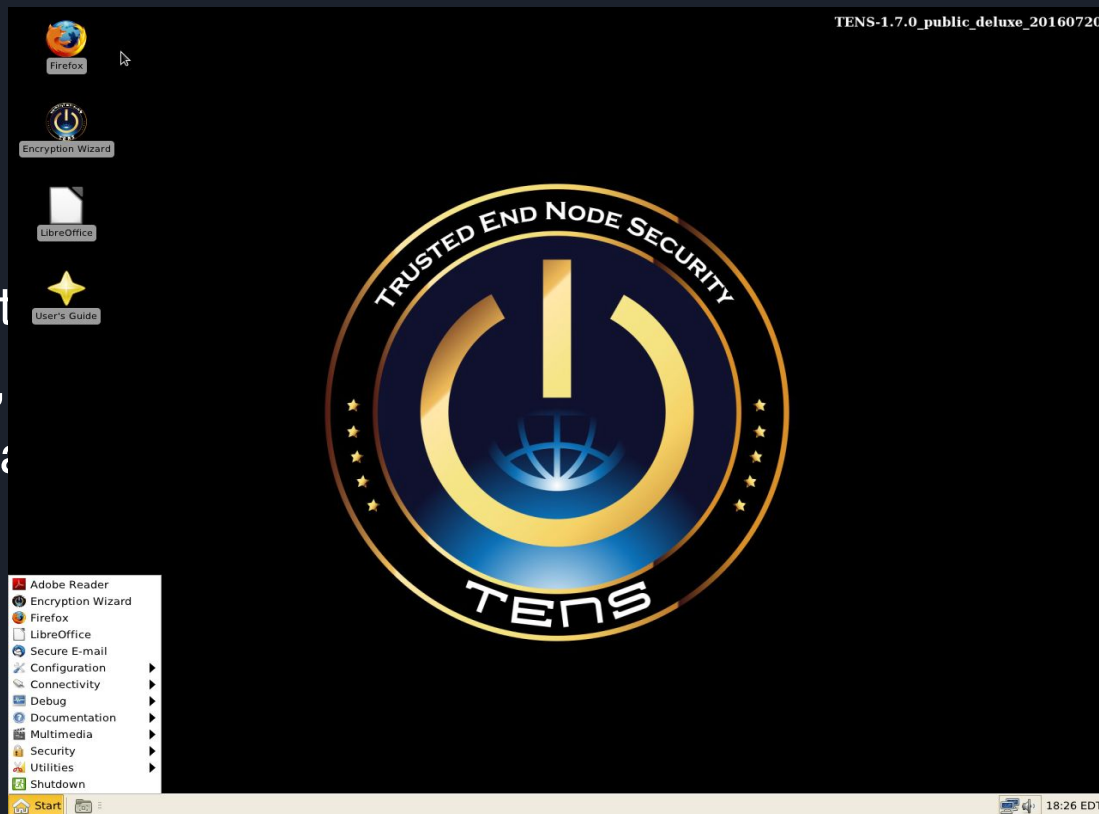
```
[user@netvm ~]$
```

```
[work] user@work:~/exploits
[user@work exploits]$ ls -l
fc17
fc18
osx-10.6
win7
win8
[user@work exploits]$
```

Security by compartmentalization

Trusted End Node Security (TENS)

Project
mode,
applic



live
i



Backup

“Il backup è quella cosa che andava fatta prima.”

Per approfondire





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.” [Edward Snowden]



Domande?





Per saperne di più...

<https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/>

[it.wikipedia.org/wiki/Categoria:Tecniche di attacco informatico](https://it.wikipedia.org/wiki/Categoria:Tecniche_di_attacco_informatico)

<https://blog.kaspersky.it>

Grazie per l'attenzione





IT Security

Gioele Schirripa
Project Management Consultant

Francesco Fresta
Associate Consultant @ TIBCO Software Inc.