

Raffaele “Faffa” Angius
(@faffa42)

Giovanni “Ciaby” Civardi
(@ciaby)

Alessandro “Scinawa” Luongo
(@scinawa - <https://luongo.pro>)



Cybersecurity for Journalists

1 Giugno 2018

Hermes Center for Transparency and Digital Human Rights

Che differenza c'è tra un sito 'https://' e uno 'http://'?

- Il primo è dotato di maggiore definizione
- Nel primo le informazioni inserite sono criptate
- Il primo è alla sua versione più aggiornata
- Il sito non è accessibile a certi dispositivi
- Non so

Quale dei seguenti è un esempio di “phishing”?

- E-mail che sembra provenire da un mittente noto, ma che contiene un link malevolo
- Pagina web fittizia per indurre l’utente a inserire le proprie credenziali
- Sms che contiene un link e annuncia la vittoria di un premio fittizio
- Tutte le precedenti
- Non so

Quale delle seguenti è una password sicura?

- Boat123
- WTh!5Z
- into*48
- 123456
- Non so

Disattivare il Gps del proprio dispositivo ne previene il tracciamento della posizione?

- Si
- No
- Non so

Una rete Wi-Fi pubblica (aeroporto o bar) che ha la password è da considerarsi sicura?

- Sì, è sicura
- No, non è sicura
- Non so

Che differenza c'è tra un sito 'https://' e uno 'http://'?

- Nel primo le informazioni inserite sono criptate

Criptare le informazioni inserite in un sito web rende più l'intercettazione delle informazioni trasmesse più difficile. A febbraio 2017 circa metà del traffico internet era criptato

Correctly: 75% - Incorrectly: 8% - Not Sure: 17%

Quale dei seguenti è un esempio di “phishing”?

- Tutte le precedenti

Gli attacchi di tipo ‘phishing’ cercano di indurre l’utente a cliccare su un link o file malevolo, impersonando una fonte fidata

Correctly: 73% - Incorrectly: 7% - Not Sure: 20%

Quale delle seguenti è una password sicura?

- WTh!5Z

Questa password contiene gli elementi basilari di una password sicura. Combina lettere maiuscole e minuscole, numeri e simboli.

Correctly: 48% - Incorrectly: 9% - Not Sure: 43%

Disattivare il Gps del proprio dispositivo ne previene il tracciamento della posizione?

- No

Oltre al Gps, gli smartphone si geolocalizzano attraverso la rete telefonica o il Wi-Fi

Correctly: 10% - Incorrectly: 71% - Not Sure: 18%

Una rete Wi-Fi pubblica (aeroporto o bar) che ha la password è da considerarsi sicura?

- No, non è sicura

Anche se una rete Wi-Fi pubblica chiede una password altri utenti potrebbero potenzialmente intercettare i dati trasmessi

Correctly: 16% - Incorrectly: 10% - Not Sure: 73%

Definizioni

Threat

In computer security, a threat is a potential event that could undermine your efforts to defend your data. Threats can be intentional (conceived by attackers), or they could be accidental (you might leave your computer turned on and unguarded).

Asset

In threat modeling, any piece of data or a device that needs to be protected.

Threat Modeling

- Chi è il tuo nemico?
- Cosa vuole ottenere?
- Come può attaccarti?
- Come puoi difenderti?
- Quali sono le probabilità di essere attaccati?
- Quali sono le conseguenze?

Nation State Actors



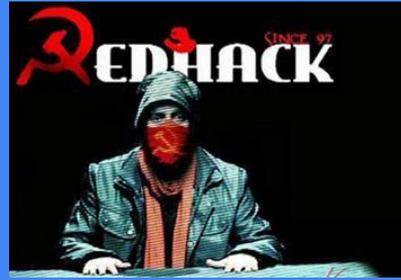
- Altissimo livello tecnico
- Operano al di fuori del contesto legale
- Seguono gli interessi della nazione di cui fanno parte
- Possono usare 0-day (attacchi/exploit non conosciuti al pubblico)
- Quasi impossibile difendersi
- Intervengono solo in casi specifici e su bersagli di alto livello
- Nel 99% dei casi non sono il tuo threat model :)
- Esempi: Ahmed Mansoor, Stuxnet



Individual Actors

- Livello tecnico variabile
- Se scoperti, vengono processati dal sistema legale (non sempre)
- Agiscono per interessi personali o “just for fun”
- Raramente usano 0-day
- Ci si può difendere
- Possono operare sia su grandi gruppi (campagne di phishing) che su specifici individui
- Rientrano nel nostro threat model
- Esempio: Occhionero

Hacktivisti



- Livello tecnico variabile
- Se scoperti, vengono processati dal sistema legale (quasi sempre)
- Agiscono per una causa sociale/politica che vogliono appoggiare
- Raramente usano 0-day
- Ci si può difendere
- Possono operare sia su grandi gruppi (campagne di phishing) che su specifici individui
- Rientrano nel nostro threat model

Crimine organizzato

- Livello tecnico variabile
- Raramente vengono processati
- Agiscono per interesse economico
- Raramente usano 0-day
- Ci si può difendere
- Possono operare sia su grandi gruppi (campagne di phishing) che su specifici individui
- Rientrano nel nostro threat model
- Esempi: ?

Forze dell'ordine

- Livello tecnico variabile
- Hanno la legge dalla loro parte, anche quando commettono atti illegali
- Agiscono per interesse legale
- Raramente usano 0-day
- Ci si può difendere
- Di solito lavorano su specifici individui
- Rientrano nel nostro threat model
- Esempi: Indagini (metadati, sequestro di dispositivi, captatori)

Sicurezza dei dati

- Fisica / locale (il tuo pc/tablet/smartphone)
- Remota (email sul server, cloud storage, IM)
- In transito (intercettazioni, analisi del traffico, MITM)



Password

La password spesso è il

primo (e anche l'unico) strumento di controllo degli accessi

Gli esseri umani fanno molta fatica a ricordare tante password diverse, specialmente se si seguono le regole imposte da molti provider/servizi (maiuscole, minuscole, numeri, caratteri speciali).

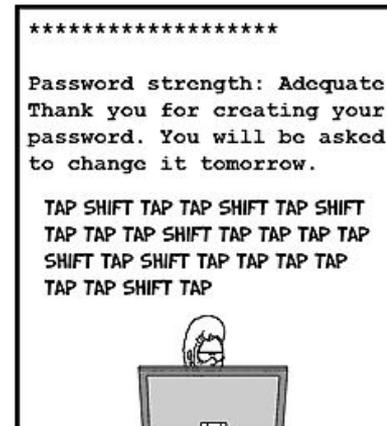
Questo genera due conseguenze:

1. Password molto brevi e/o facili da indovinare.
2. La stessa password utilizzata su più servizi.

USER FRIENDLY by J.D. "Illiad" Frazer



COPYRIGHT © 2007 J.D. "Illiad" Frazer [HTTP://WWW.USERFRIENDLY.ORG/](http://www.USERFRIENDLY.ORG/)



Le 25 password più comuni

- 123456
- 123456789
- qwerty
- 12345678
- 111111
- 1234567890
- 1234567
- password
- 123123
- 987654321
- qwertyuiop
- mynoob
- 123321
- 666666
- 18atcskd2w
- 7777777
- 1q2w3e4r
- 654321
- 555555
- 3rjs1la7qe
- google
- 1q2w3e4r5t
- 123qwe
- zxcvbnm
- 1q2w3e

Password manager

Un password manager permette di doversi ricordare una sola password, riducendo il rischio di riuso e/o l'uso di password facili da indovinare.

Online: Lastpass

LastPass . . . |

Offline: KeePass / KeePassX



2FA (Two Factor Authentication)

Ci si può autenticare in 3 maniere:

1. Quello che sai (password/segreto)
2. Quello che sei (biometrico)
3. Quello che hai (smartcard/dongle)

Ognuno di questi sistemi ha vantaggi e svantaggi.

La 2FA con SMS/chiamate non può più considerarsi sicura in caso di attacchi mirati.

Sicurezza dei dispositivi

La sicurezza di un dispositivo (pc/tablet/smartphone) dipende principalmente da

DATI IN USO

patch di sicurezza

ridurre la superficie di attacco

software libero o commerciale con licenza

≈ firewall e antivirus

Sicurezza dei dispositivi

La sicurezza di un dispositivo (pc/tablet/smartphone) dipende principalmente da

DATI A RIPOSO

- full disk encryption (anche di dispositivi esterni)
- password manager
- cellulari cifrati
- computer spenti nei momenti critici

A CRYPTO NERD'S
IMAGINATION:

HIS LAPTOP'S ENCRYPTED.
LET'S BUILD A MILLION-DOLLAR
CLUSTER TO CRACK IT.

NO GOOD! IT'S
4096-BIT RSA!

BLAST! OUR
EVIL PLAN
IS FOILED!



WHAT WOULD
ACTUALLY HAPPEN:

HIS LAPTOP'S ENCRYPTED.
DRUG HIM AND HIT HIM WITH
THIS \$5 WRENCH UNTIL
HE TELLS US THE PASSWORD.

GOT IT.



Sicurezza dei dispositivi

La sicurezza di un dispositivo (pc/tablet/smartphone) dipende principalmente da

DATI IN TRANSITO

tutto ciò che esce senza essere cifrato è da considerarsi di dominio pubblico

siti <https://>

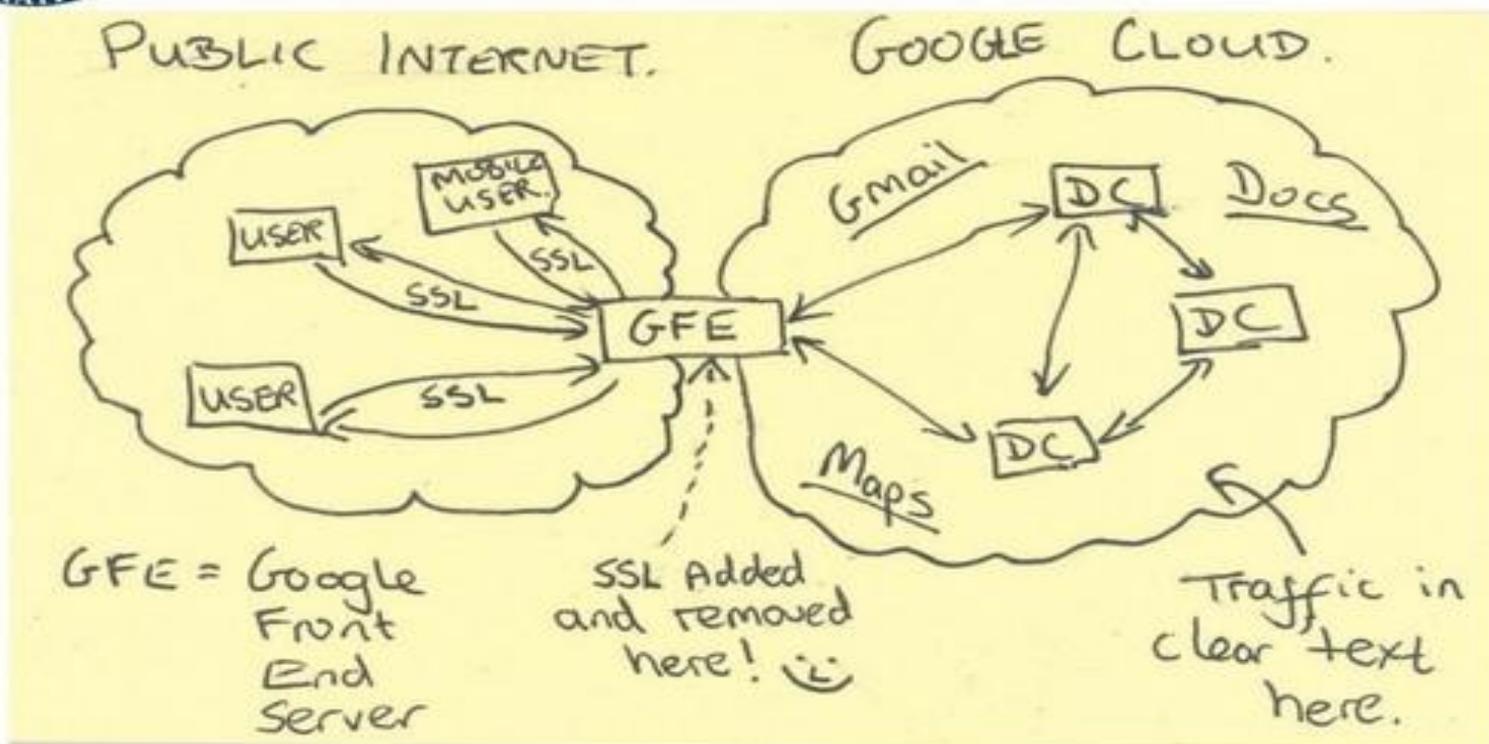
versione sicura dei servizi

Tor

VPN



Current Efforts - Google



Sicurezza dei dispositivi

La sicurezza di un dispositivo (pc/tablet/smartphone) dipende principalmente da

DATI SU SERVER

giurisdizione

sicurezza (informatica e legale)

EULA (end user license agreement)

Datacenter Security



Presumed FBI agents reinstall the server seized from MayFirst/PeopleLink. The bureau won't say why it took it or why it returned it in such an unusual manner. (Click pic for swf video)

Compartimentalizzazione

Usare lo stesso dispositivo per ambiti diversi della tua vita (per es. personale/ufficio/finanziario/intrattenimento) non è una buona idea.

Usare dispositivi diversi permette di mantenere una separazione fisica e logica.

In caso di compromissione di uno dispositivo, non si compromettono tutti i nostri dati degli altri ambiti.

Strumenti consigliati

Instant messaging: Signal - Wire

Email: autistici.org - riseup.net - protonmail.com - tutanota.com

Navigazione anonima: Tor Browser - TAILS

Full Disk Encryption: Bitlocker (Win), FileVault (Mac), dm-crypt (Linux)

Password Manager: KeePass/KeePassX (locale), LastPass (online)

File Encryption: VeraCrypt

Sincronizzazione di file: OwnCloud, SyncThing

Estensioni del browser: uBlock Origin, HTTPS Everywhere, SaferChrome

Altre risorse

<https://www.securitywithoutborders.org/>

<https://ssd.eff.org/>

Domande? ; -)

 @faffa42

 @scinawa - <https://luongo.pro>

 @ciaby

AGI > Innovazione

Benigni spiega come la crittografia quantistica ci salverà dagli hacker

Una chiave passata di mano tra la Cina e l'Austria mostra che rendersi invulnerabili agli attacchi è possibile. Basta agire per primi

di **RAFFAELE ANGIUS**

06 ottobre 2017, 20:20



Archives du 7eme Art / Photo12

Roberto Benigni e Nicoletta Braschi in una scena del film 'La vita è bella'