CYBER SECURITY FOR JOURNALISTS

DIG-AWARDS 2017 - Riccione, 24 giugno 2017

Raffaele “Faffa” Angius, Giovanni “Ciaby” Civardi, Alessandro “Scinawa” Luongo, Fabio “Naif” Pietrosanti
In collaboration with GlobaLeaks, Hermes Center for Transparency and Digital Human Rights

Threat Modeling

- Chi è il tuo nemico
- Cosa vuole ottenere
- Come puoi difenderti

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 pub
- Quasi impossibile difendersi
- Intervengono solo in casi specifici e su bersagli di alto livello
- Nel 99% dei casi non sono il tuo threat model :)

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

Hacktivists

- 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

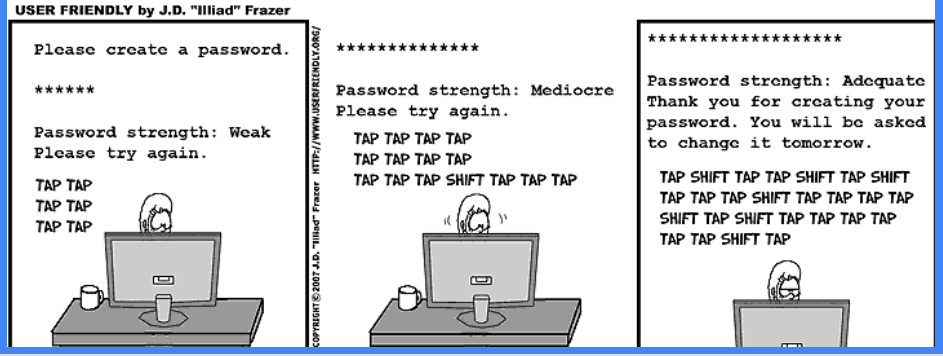
Forze dell’ordine

- 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

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.

La 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

Offline: KeyPass / KeyPassX

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

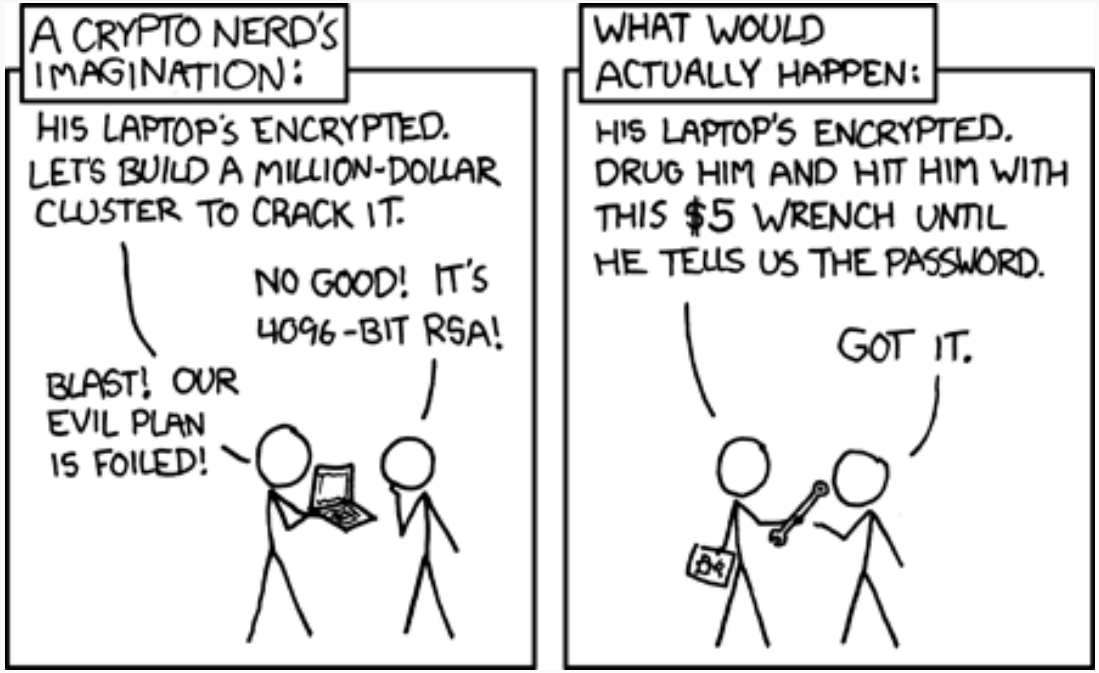
Sicurezza dei dispositivi

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

Physical Security



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

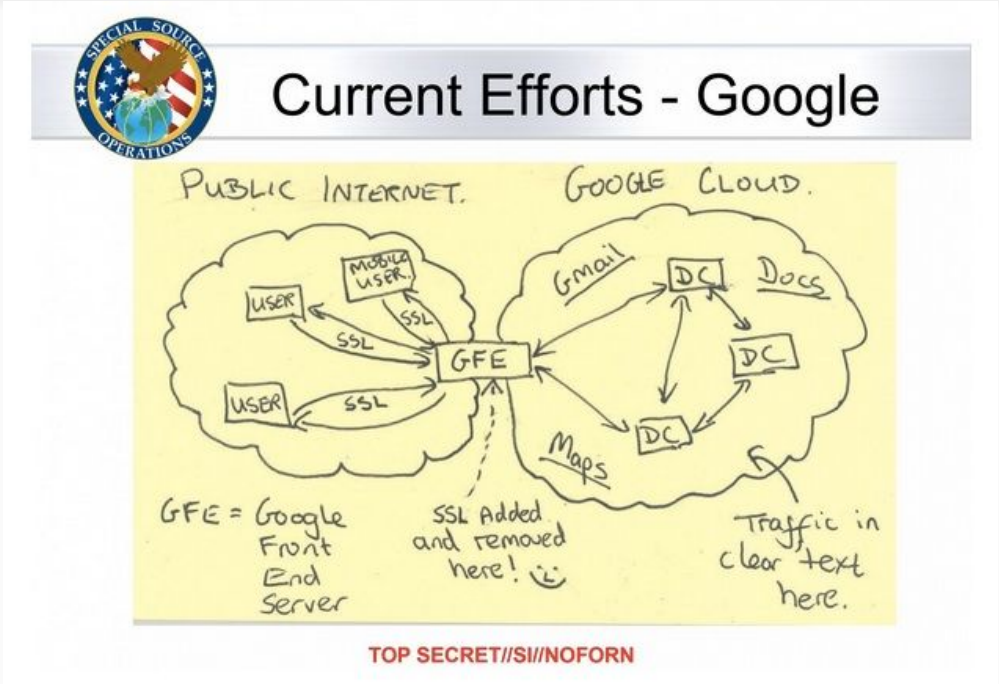
siti https://

versione sicura dei servizi

Tor

VPN

SSL Added and removed here ;)



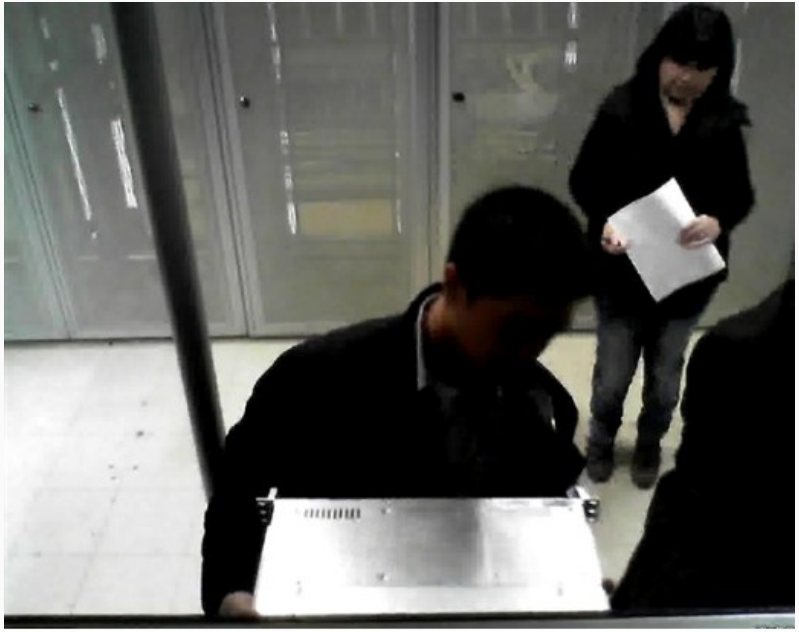
Sicurezza dei dispositivi

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

Domande? ;-)