

Le principali tipologie di malware nella PP.AA.

- conoscerne i danni

11/06/2021

Introduzione

-  Questo **non** è un documento tecnico.
-  Mostriamo solo le più **comuni conseguenze** di un'infezione, niente codice o dettagli tecnici.
-  Per sapere cosa aspettarsi.

Principio base dei malware



Fare più soldi possibile



con il minore impegno possibile



Si basano più sull'**inganno** che su prodezze tecniche
(minor impegno)



Chiunque può cascarci



Sono truffe

Principio base dei malware



Fare più soldi possibile



con il minore impegno possibile



Vogliono tutto ciò che porta **denaro**

-  Le vostre password
-  L'accesso al vostro conto corrente
-  Ricattarvi
-  Rivendere l'accesso al vostro computer

Infostealer



Information stealer



Ladri di informazioni

- Interessati a nomi utenti e password di qualsiasi applicazione (posta, banca, server interni, siti web usati)

- **Demo: ASTesla**



Per i tecnici:

<https://cert-agid.gov.it/news/astesla-analisi-di-un-nuovo-malware-parente-di-agenttesla/>

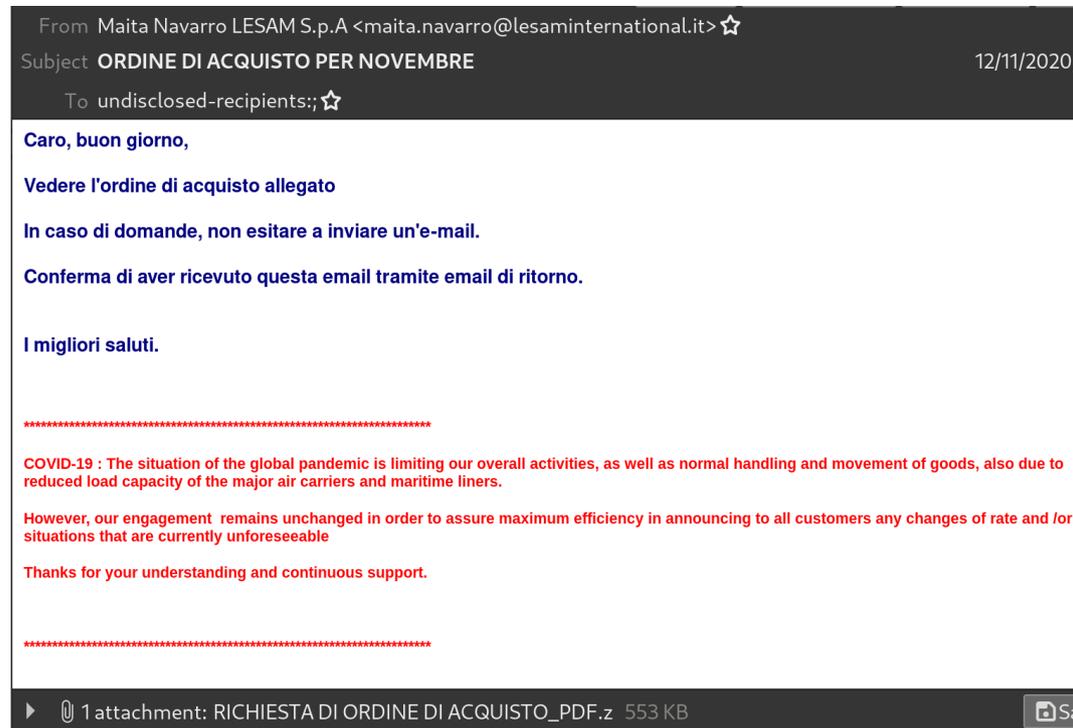
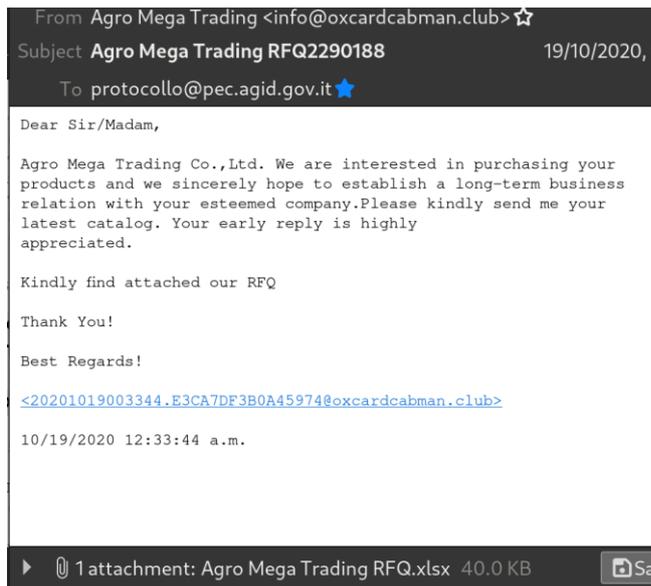
Infostealer

- **Demo: ASTesla**
- 🧤 Ruba le password da più di 100 applicativi diversi
- 🌐 Ruba le password dei siti web (se le avete salvate nel browser)
- 👤 Ruba i dati per fingervi voi stessi nei vostri siti web
- 🌨️ Ruba tutto quello che scrivete o copia-incollate
- 📷 Fa delle foto al vostro schermo e le ruba
- I dati rubati sono inviati per ✉️ e-mail o messi su un server o in una 🗨️ chat

Infostealer

- **Demo: ASTesla**

Tutto inizia da un'e-mail con un allegato



Infostealer

- **Demo: ASTesla**

Le e-mail vogliono farvi aprire l'allegato che sembra innocente (truffa), tipo un documento Office

👉 Che succede se ci clicchiamo?

Infostealer

- **Demo: ASTesla**

...niente!

Tutto avviene silenziosamente e in automatico

Ma in realtà... le vostre password vengono rubate

Se dopo aver aperto un documento Office vedete che **non** c'è contenuto significativo... **insospettitevi.**

Chiedete ai vostri esperti di sicurezza di analizzarlo.

Time: 10.19.2020 12:54:28
User Name: Aquila
Computer Name: STATIA29
OSFullName: Microsoft Windows 7 Home Premium
CPU: Intel(R) Core(TM)2 Quad CPU Q9300 @ 2.50GHz
RAM: 3991,25 MB

URL:smtp://mail2.edituraaquila93.ro
Username:office@roland-toys.eu
Password:👤👤👤👤
Application:Thunderbird

URL:smtp://mail2.edituraaquila93.ro
Username:orsolya.lengyel@edituraaquila93.ro
Password:👤👤👤👤
Application:Thunderbird

URL:mailbox://pop3.microware.hu
Username:office@roland-toys.eu
Password:👤👤👤👤
Application:Thunderbird

URL:http://www.farmerama.hu
Username:delfinsors
Password:👤👤👤👤
Application:Firefox

Infostealer

Spesso sono accoppiati ad un **keylogger** che ruba cosa scrivete, cosa copia-incollate ed il contenuto del vostro schermo (**screen grabber**).

Time: 11/11/2019 17:49:20
UserName: PROBOOK
ComputerName: HP
OSFullName: Microsoft Windows 10 Pro
CPU: Intel(R) Core(TM) i5-4210U CPU @ 1.70GHz
RAM: 3993.11 MB

—PROBOOK/HP Screen Capture_2019_11_11_17_49_21.jpeg—

Time: 03/27/2019 16:21:20
UserName: user2
ComputerName: ELENA
OSFullName: Microsoft Windows 8 Pro
CPU: Intel(R) Core(TM) i5-3330 CPU @ 3.00GHz
RAM: 8138,63 MB
IP: 79.129.8.112

[clipboard]1,00 [clipboard]
[clipboard]1,00 [clipboard]

Infostealer



I password manager aiutano contro i keylogger?

Sì ma con alcuni accorgimenti (al netto dei dettagli tecnici):

-  Il password manager deve essere un processo privilegiato (la vostra utenza non deve essere in grado di leggere i suoi file o la sua memoria). Impedisce l'interazione con i malware.
-  Il password manager deve usare un desktop sicuro (leggete la lista delle feature).
-  L'inserimento della password deve avvenire tramite **Drag'n'Drop** o tramite un **plugin** (per i browser sono tipicamente disponibili entrambi i modi).
 -  No copia-incolla! No autotype/inject. **Forti dubbi** sul metodo usato da KeePass...



🕶️ Come proteggersi?



Salvate le password nei password manager **non** nei browser.

1 Usate con password manager con un plugin per il vostro browser (comodo e sicuro)

2



Configurate l'invio di codici sul cellulare (2FA).

3



Dato che usate un password manager, cambiate le password regolarmente.
(è però noioso da fare)

Infostealer



Come rimediare ad un'infezione?



Farsi **ripulire** il computer da un tecnico

1

La formattazione completa è il metodo più sicuro ma anche più oneroso



Prima di formattare, **copiatevi le password che non ricordate più!**

2



Le password sono ormai state rubate, il danno è fatto

Vanno cambiate tutte, iniziate da quelle importanti (banca, lavoro, posta)



Cambiate le password dopo aver ripulito il computer oppure usate un altro computer, altrimenti verranno rubate di nuovo

Ransomware

-  Ransom malware  Malware del riscatto
- Mettono i vostri file in una cassaforte (in gergo: li cifrano) e vi chiedono soldi per darvi la chiave
- **Demo: NetWalker**



Per i tecnici:

<https://cert-agid.gov.it/news/netwalker-il-ransomware-che-ha-beffato-lintera-community/>

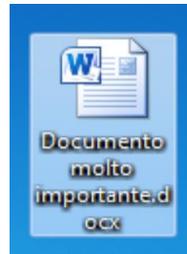
Ransomware

-  Hanno avuto forte diffusione via e-mail intorno al 2018-19, al momento stiamo osservando un calo nel panorama italiano.
-  Oggi principalmente diffusi a **seguito di intrusioni** nella rete dell'amministrazione.
-  Tuttavia il rischio di contrarli via e-mail è **sempre presente**.
- **Demo: NetWalker**

Ransomware

- **Demo: NetWalker**

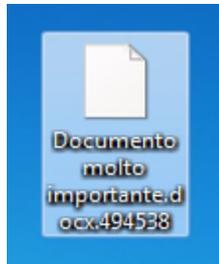
Prima del
ransomware
il documento è integro



Ransomware

- **Demo: NetWalker**

Dopo l'esecuzione del Ransomware il documento non è più apribile e viene lasciata una nota di riscatto



```
494538-Readme.txt - Notepad
File Edit Format View Help
Hi!
Your files are encrypted.
All encrypted files for this computer has extension: .494538

--
If for some reason you read this text before the encryption ended,
this can be understood by the fact that the computer slows down,
and your heart rate has increased due to the ability to turn it off,
then we recommend that you move away from the computer and accept that you have been compromised.
Rebooting/shutdown will cause you to lose files without the possibility of recovery.

--
Our encryption algorithms are very strong and your files are very well protected,
the only way to get your files back is to cooperate with us and get the decrypter program.

Do not try to recover your files without a decrypter program, you may damage them and then they will be impossible to recover.

For us this is just business and to prove to you our seriousness, we will decrypt you one file for free.
Just open our website, upload the encrypted file and get the decrypted file for free.

Additionally, you must know that your sensitive data has been stolen by our analyst experts and if you choose to no cooperate with
to huge penalties with lawsuits and government if we both don't find an agreement. We have seen it before; cases with multi milli,
not to mention the company reputation and losing clients trust and the medias calling non-stop for answers. Come chat with us and
fast we both can find an agreement without getting this incident public.

--
Steps to get access on our website:
1. Download and install tor-browser: https://torproject.org/
2. Open our website: pb36hu4spl6cyjdfhing7h3pw6dhpk32ifemawkujj4gp33ejzdg3did.onion
If the website is not available, open another one: rnfds6m6b6j6su5txkek4u4y47kp2eatvu7d6xhyn5cs41t4pdrqqd.onion
3. Put your personal code in the input form:
{code_494538:
ZqtWz53NZsKE7aVEEci1wxv1uUTNH96sEbghjVaE1+yUozppNm
7TGPz90MC3AR6j0KkWGZyCZNUU6lIXBFh2k3lNmWBYlRw3ljs
+KQ4RU19tOu7IMbOY8NP9qGwn5+PGstPwGfA5Yu5att5U8aq6s
YQw9JYx+kPBuY1ly+s1Iow/YQRawtCF6H/+DgyWUTK7wn80ZpN
a0qQs7fhu5fCX1Usy63HwxZs/5moSpe20wPFQvZ1Zu4t8izkYo
ZVB2HacboxsowktQwm5SgJ55vgYJCPMdnjANCIXg==}
```

Ransomware

- 🤔 Come mi accorgo di un attacco ransomware?

I vostri file **non si aprono più**, hanno un'estensione/**icona strana** e c'è un file di testo con una **nota di riscatto in inglese**.

- 🙅 Posso recuperare i miei file?

No. Tranne nel rarissimo caso in cui i criminali siano degli incompetenti.

- 😞 Neanche con il cloud di machine learning a curve q-bit?

... NO!

Ransomware

-  Gli attacchi ransomware oggi presentano anche altre minacce, un tipico attacco consiste in:

- 1 Compromissione di una macchina vulnerabile.
- 2 Spostamento all'interno della rete per individuare i dati più interessanti.
- 3 **Furto** e cifratura dei dati. Eliminazione dei backup.



Se i vostri file sono stati cifrati, probabilmente sono stati **anche rubati** e la rete **compromessa**.

Se il ransomware vi è arrivato per posta, allora solo cifratura, niente furto o compromissione.

Ransomware



Come proteggersi?

- 1  Ordinate ai sysadmin di fare backup **multipli** e **regolarmente**.
I backup vanno salvati in macchine **isolate** dalla rete (se non per il tempo di backup e comunque che **non diano la possibilità di sovrascrivere** o **leggere** i backup esistenti).

Ransomware

• 🤖 Come rimediare ad un'infezione?

1 🚩 Identificare se il ransomware è **fine a sè stesso** o parte di un **attacco più grande**.

Per i tecnici: come si fa?

Ci sono più computer infetti?

Nella nota come si firmano i criminali?

Su Google si trova come agiscono?

Si evince niente dai log dei server esposti?

Il registro eventi di Windows contiene righe di login anomale?

Il malware è arrivato per e-mail?

2 🧀 🍷 Far sistemare le macchine **vulnerabili** e far **ripulire** i computer della rete dai tecnici.

I ransomware di solito non persistono una volta terminato il loro lavoro, ma i criminali possono aver installato altri malware.

Ransomware

- 🤖 Come rimediare ad un'infezione?
 - 3 🗝️ Ripristinare i file da un backup se lo si ha.
 - 4 👉 Se non avete un backup, forse www.nomoreransom.org vi può aiutare.
 - 5 📁 Pagare il riscatto **generalmente** funziona ma:
State comunque **finanziando dei criminali** (che potrebbero **fregarvi due volte**)
Non fate commenti riguardo l'aver pagato o meno un riscatto.

Banking (trojan/malware)

-  Banking  Che riguarda operazioni di banca
- Modificano il vostro computer per redirigere i movimenti di denaro che fate tramite il sito della vostra banca
- **Esempio: Ursnif**



Per i tecnici:

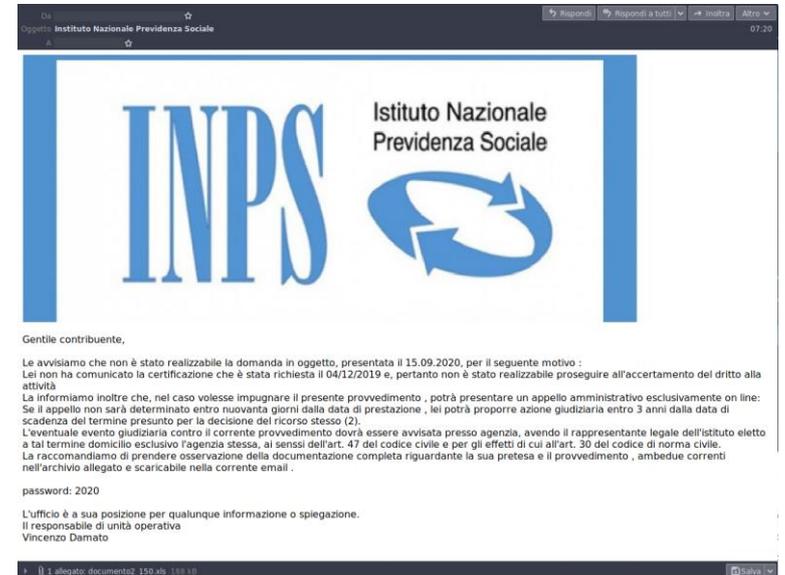
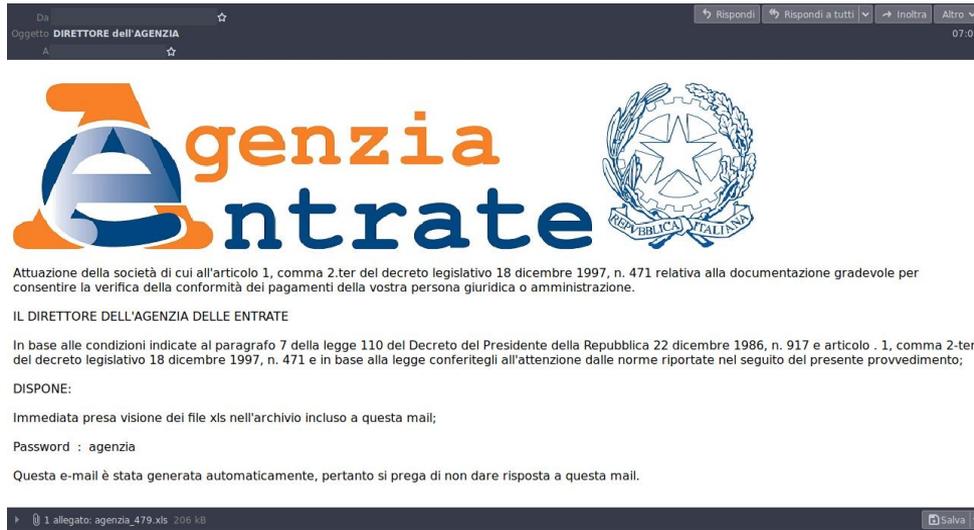
<https://cert-agid.gov.it/tag/yau/>

Banking (trojan/malware)

- **Esempio:** Ursnif
- Uno dei malware più diffusi in Italia, pensato appositamente contro di noi 
-  Operato da criminali moldavi o russi
-   Si presenta due/tre volte a settimana con una media di ~300 vittime a campagna

Banking (trojan/malware)

- **Esempio: Ursnif**
- Malware di lunga data, specializzato nei temi che meglio funzionano in Italia (Agenzia delle entrate, INPS, e simili)



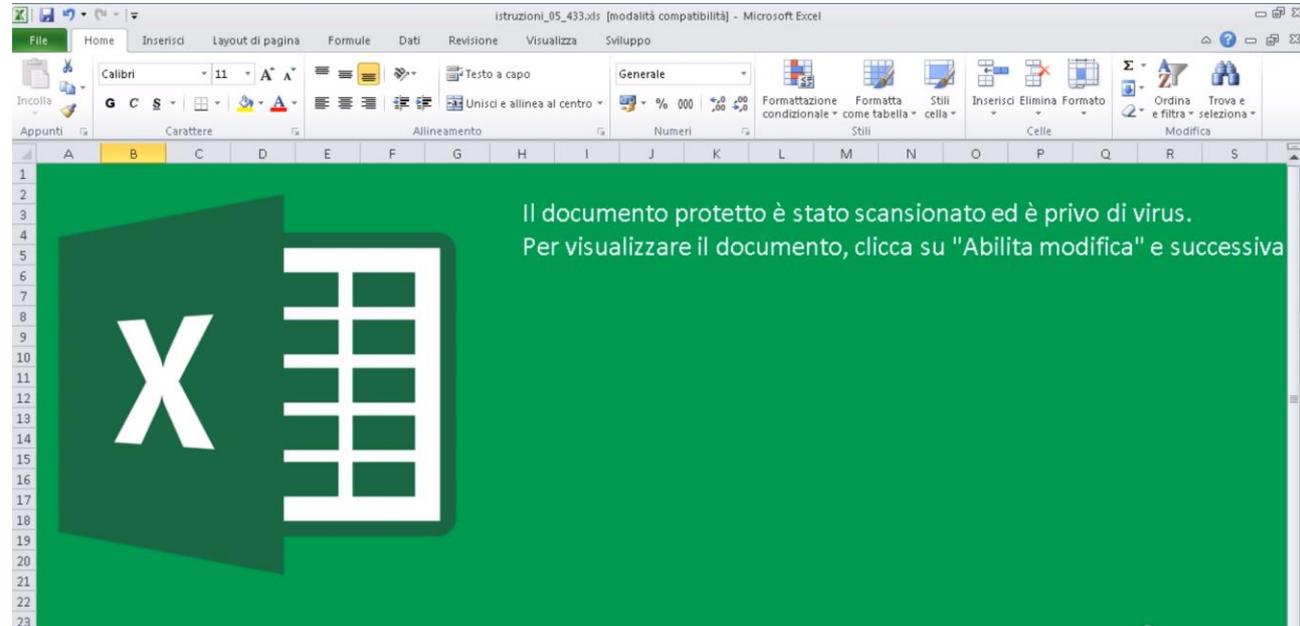
Banking (trojan/malware)

- **Esempio: Ursnif**

- Si presenta (principalmente) come document Excel.

- Chiedete al vostro tecnico di disabilitare le macro di Office da ogni installazione.

- **Mai cliccare sui pulsanti “abilita” nelle barre arancioni di Office.**



Banking (trojan/malware)

- **!?** Che effetti ha un banking trojan?

- 1  Simili al furto di carta di credito.
Trovate addebiti anomali (acquisti, bonifici).
- 2  Vi arrivano messaggi dalla vostra banca riguardo a movimenti di denaro.
- 3  I destinatari e gli importi dei bonifici effettuati indicati negli SMS della vostra banca non corrispondono a quanto effettuato da voi.

NB. Le banche non risarciscono se il furto è colpa dell'interessato
(come accade nel caso di malware/phishing)

Banking (trojan/malware)

- 🧐 Come proteggersi?



Quando muovete del denaro sopra una certa soglia la vostra banca dovrebbe mandarvi un SMS con:

Un codice di autorizzazione

Il destinatario

L'importo

Data e ora



Controllate tutti i dettagli prima di autorizzare il pagamento, anche se sembra inutile! il malware può nascondere il vero importo e il vero destinatario nel vostro computer ma non nell'SMS!

Banking (trojan/malware)



- 🤖 Come rimediare ad un'infezione?
 - 1 🧼 🧴 Farsi **ripulire** il computer da un tecnico
La formattazione completa è la soluzione più sicura ma anche più onerosa.
 - 2 🏦 Cambiare la password usata nel sito della banca
Per sicurezza cambiate **tutte** le password dei servizi critici.
 - 3 💳 Controllate il vostro conto corrente (se lo avete usato dal computer infetto)
Chiamate la banca in caso di problemi o sospetti.

⚠️ Non usate il computer finchè non è stato ripulito!

RAT e movimenti laterali

-  RAT – Remote Administration Trojan
 Trojan per l'amministrazione da remoto
- Permettono ad **altri** di controllare il vostro computer
Dà modo ai criminali di decidere cosa avete di valore
Usati anche per infettare altri computer della rete (movimenti laterali)
- **Esempi:** Qarallax, jRAT, Trickbot, Nanocore



Per i tecnici:

<https://cert-agid.gov.it/news/analisi-del-malware-qarallax-rat-rilevata-la-deadline/>

RAT e movimenti laterali

-  Lo scopo principale di un RAT: scaricare programmi malevoli da eseguire

 Massima flessibilità per l'attaccante

 Sono attacchi più sofisticati e pericolosi

 Spesso spiano quello che viene scritto o è presente

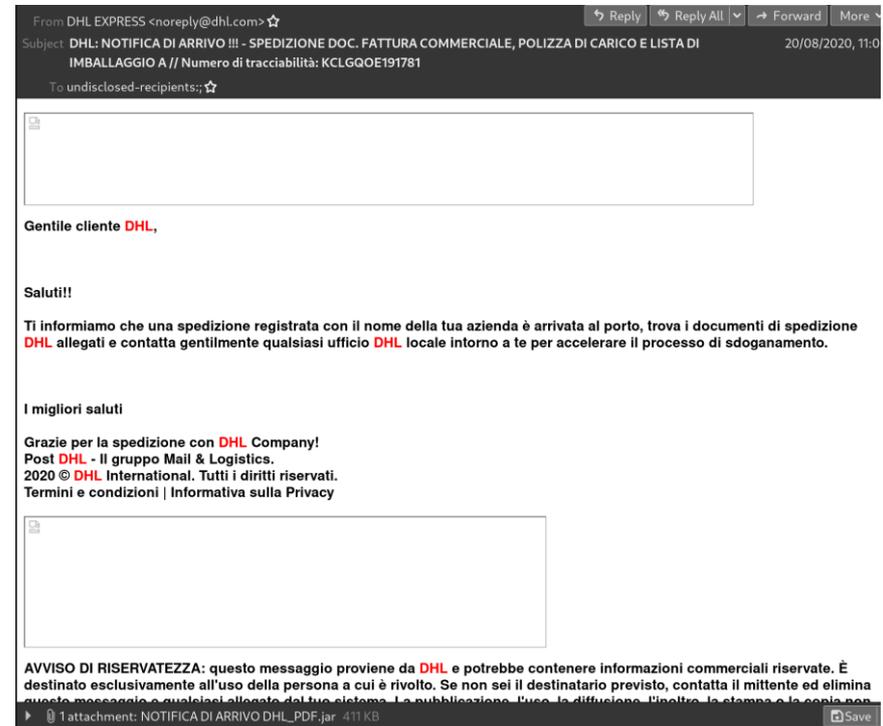
sullo schermo

  Ci sono capitati casi (non isolati) di RAT che spiano anche da videocamera e microfono

- ▼ Funzionalità di RAT
 - ShowMessage (100)
 - BrowseTo (101)
 - DownloadAndExecute (102)
 - GetIPInfo (103)
 - GeoIPWifi (105)
 - Restart (106)
 - Terminate (107)
 - RunInstallPlugin (108)
 - UpdateFromURL (109)
 - UpdateFromC2 (110)
 - Disinstall (111)
 - CloseConnection (112)
 - DoGarbageCollector (113)
 - DetectSleeping (114)
 - GetForegroundTitle (115)

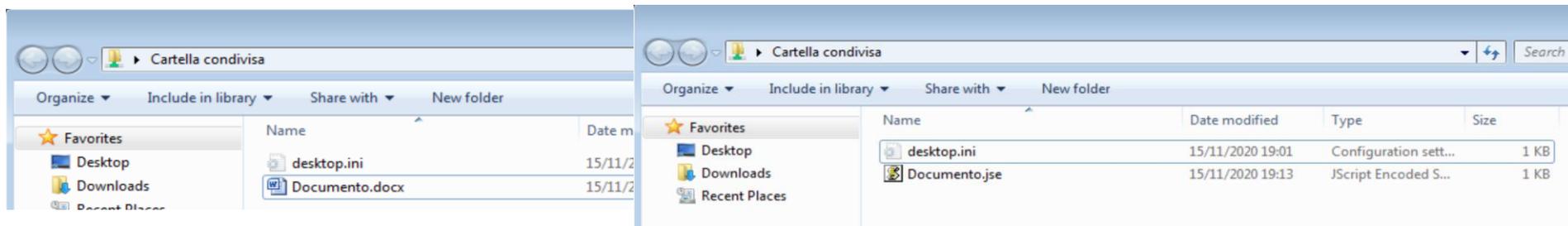
RAT e movimenti laterali

- Diffusi tramite e-mail malevole o da gruppi di criminali che setacciano internet alla ricerca di server vulnerabili
-  Aggiornate sempre i vostri computer e i vostri server



RAT e movimenti laterali

- Tendono a diffondersi su altri computer (movimenti laterali) tramite trucchetti come la **sostituzione dei file nelle cartelle condivise** con altri file malevoli.
- I più sofisticati provano le password più comuni o sfruttano vulnerabilità note in programmi non aggiornati.



RAT e movimenti laterali

- **!?** Che effetti ha un RAT?

Un RAT è solitamente individuato a **posteriori**, dopo che altri malware sono stati installati o altri attacchi sono stati compiuti.

Difficile elencarne gli effetti, i principali:

Spionaggio

Installazione reiterata di malware

RAT e movimenti laterali

- 😎 Come proteggersi?

- ★ Tenere computer, server e AntiVirus aggiornati.

- 🔦 Utilizzare software per rilevare comportamenti anomali nella rete (IDS).

RAT e movimenti laterali

- 🤯 Come rimediare ad un'infezione?
 - 1 🔌 Scollegare il computer infetto dalla rete
 - 2 🎲 I RAT possono avere qualsiasi conseguenza (sono onerosi da ripulire)
 - 3 🧽 🧑🔧 Farsi **ripulire** il computer da un tecnico
Nel dubbio, formattare
 - 4 🔍 🧑🔧 Far **controllare** e **ripulire** ogni computer della rete

Android

-  Android è perfettamente in grado di **isolare le app, impedendo comportamenti malevoli**; ma la filosofia di Google è di lasciare l'**ultima parola all'utente**.
- Questo apre la strada ad app **ingannevoli** che possono acquisire permessi molto pericolosi. In particolare tutti i malware moderni per Android ingannano l'utente per installare un **servizio di accessibilità** malevolo.
- **Nota:** su iOS non circolano malware per una serie di scelte meno liberali di Apple. Tuttavia sia iOS che Android possono essere soggetti ad exploit/0-day, iOS ne è particolarmente prono (ma questi vettori di attacchi sono troppo sofisticati per essere usati da criminali comuni).



Per i tecnici:

<https://cert-agid.gov.it/whatisit/selinux-ed-i-meccanismi-di-isolamento-delle-app-in-android/>

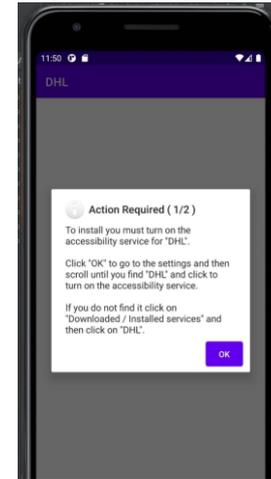
Android

- **Demo: FluBot**
- Vi arriva un SMS che sembra provenire dal corriere e contenente un link. Vi viene fatta scaricare ed installare un'app che successivamente chiede di installare un servizio di accessibilità.



Per i tecnici:

<https://cert-agid.gov.it/news/campagna-flubot-veicolata-anche-in-italia-via-sms-prende-di-mira-i-dispositivi-android/>

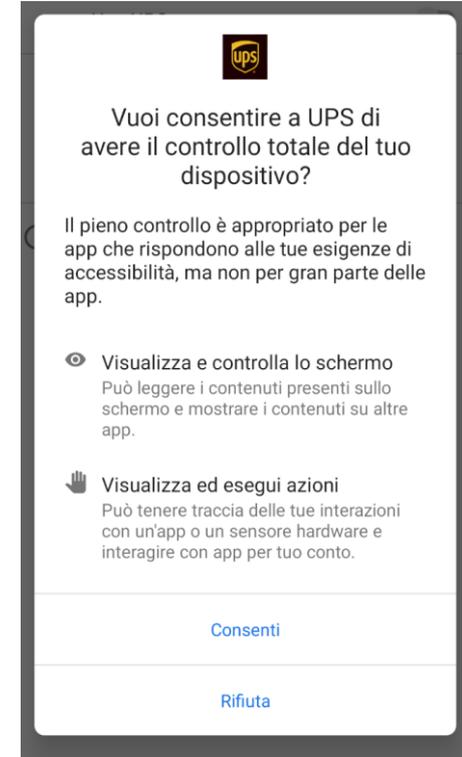


Android

- **Demo:** FluBot
- Se installate il servizio di accessibilità il malware:
- *Ruba la vostra rubrica e SMS*
Cerca di ingannarvi mostrando false pagine di login a tema
Vi presenta una falsa pagina in cui inserire carta di credito
Invia SMS per diffondersi
Altro
-  **Obiettivo:** Carta di credito, password e SMS per 2FA
- Se non installate il servizio di accessibilità, l'app è innocua.
Un servizio di accessibilità legge il contenuto dello schermo e simula il tocco.



E' come dare il cellulare in mano ad un'altra persona!



Android

- **!?** Che effetti hanno questi tipi di malware?
 - Solitamente sfruttano il fatto di poter leggere gli SMS per accedere ai vostri account rubando dati e, soprattutto, soldi (quando colpiscono gli home banking).
Le 2FA non proteggono in questi casi!
- 🤖 Come riconosco che il dispositivo è infetto?
 - Ci sono icone duplicate di app (una vera ed una finta).
Quando provate ad aprire l'app finta questa si chiude subito e/o mostra un messaggio di errore generico.
Se provate a disinstallarla, la finestra si chiude con un errore generico (impedendo la disinstallazione).
A volte si aprono e chiudono delle finestre in modo automatico.

Android

- 🕶️ Come proteggersi?
 - **Mai, mai, mai, mai, mai, mai installare un servizio di accessibilità.**
Non importa quanto urgente sembra la necessità.
(A meno che non vi serva realmente, es: non udenti, e solo da Google Play)
- 😱 Come ripulire un dispositivo infetto?
 - **E' necessario e sufficiente disinstallare l'app**, ma potrebbe non essere banale. Un qualsiasi tecnico/sviluppatore può però farlo (es: adb):
Notare:
 - Non serve il factory reset
 - Non è un'operazione complessa o lunga (es: qualche minuto al massimo)
 - I tipici tecnici dei negozi non sanno probabilmente farlo

Alcuni consigli

-  Fate sempre dei **backup** dei vostri dati
-  **Disabilitate le macro** di Office e non usate versioni più **vecchie di Office 2016**
-  **Aggiornate** gli antivirus **ogni giorno** (se lo fanno da soli, controllateli)
-  Prima di aprire un allegato sospetto, se possibile, **aspettate** 24/36 ore
(per dare tempo ai produttori di antivirus di rilevare le ultime minacce)
-  **Aggiornate** i vostri sistemi (**tutti!**) ogni giorno
-  Siate sospetti e ricordatevi che CSIRT Italiano e CERT-AGID sono stati istituiti per supportarvi nella prevenzione e in caso di incidente