Le principali tipologie di malware nella PP.AA.

Conoscere i loro danni

19/01/21

Introduzione

🚫🔧 Questo **non** è un documento tecnico.

☣️🦠 Mostreremo 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
- Impadronirsi del 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

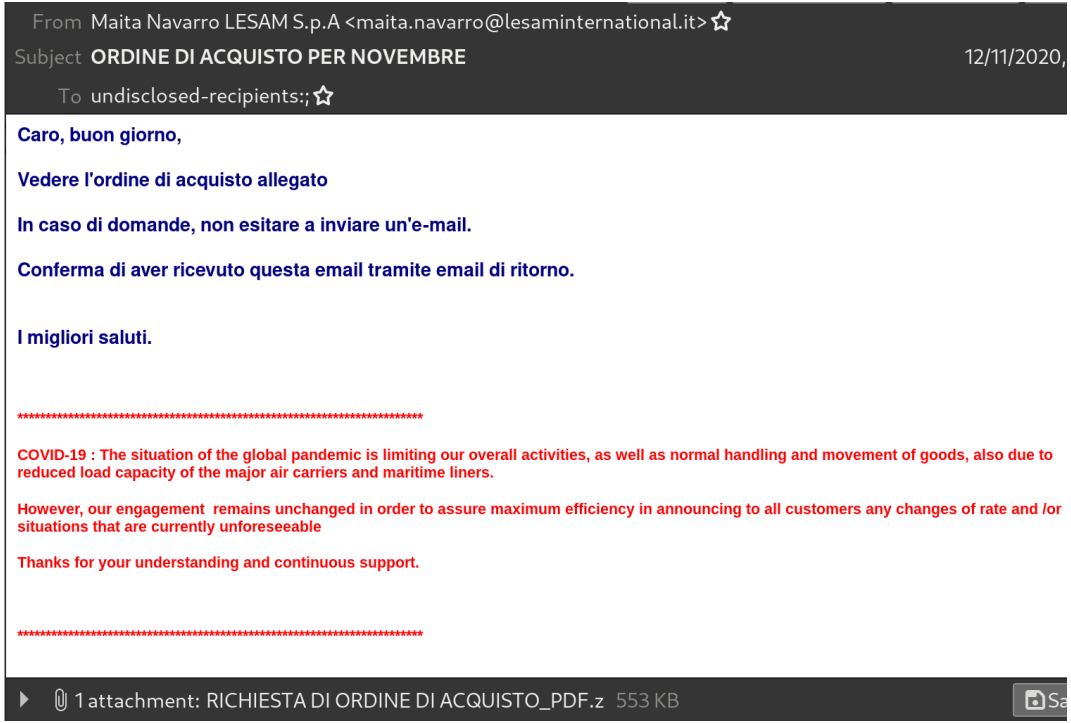
- 🧤 Ruba le password da più di 100 applicativi diversi
- 🌐 Ruba le password dei siti web (se le avete salvate nel browser)
- 🤦 Ruba i dati per fingervi voi stessi nei vostri siti web
- ⌨️ Ruba tutto quello che scrivete o copia-incollate
- 📸 Fa delle foto al vostro schermo e le ruba

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

Non è successo 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

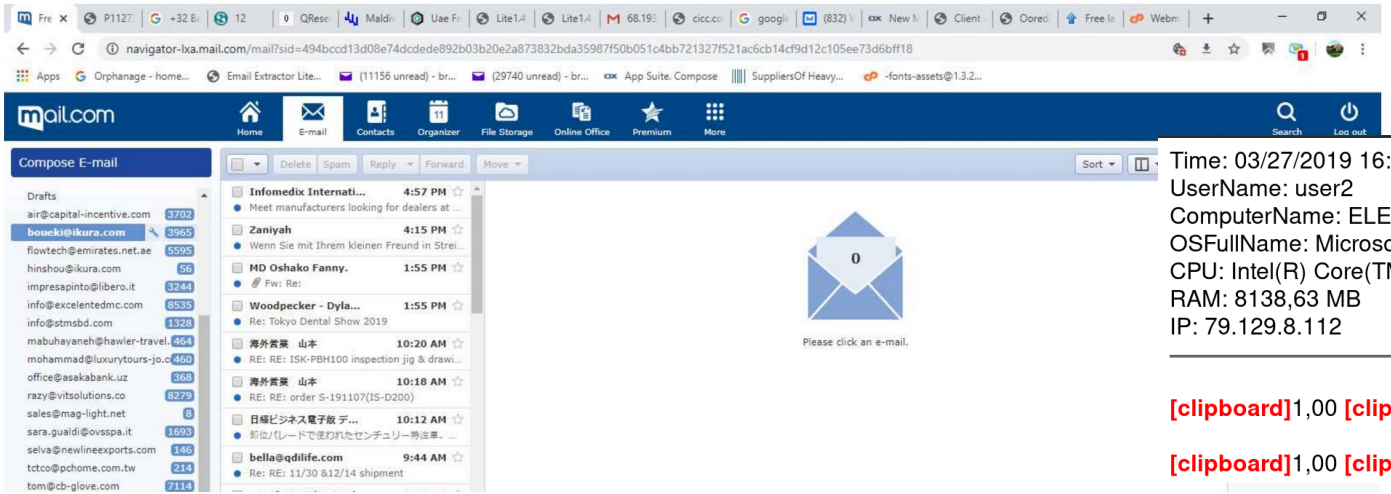
Infostealer

Demo: ASTesla

Viene rubato anche cosa scrivete ed il contenuto del vostro schermo

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

😱 Come rimediare ad un’infezione?

1 🧽🧼 Farsi **ripulire** il computer da un tecnico
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 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

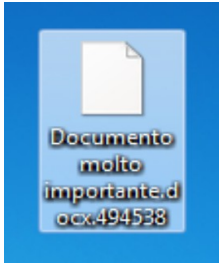
Demo: NetWalker

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 millio
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: pb36hu4spl6cyjdfhing7h3pw6dhpk32ifemawkujj4gp33ejzdq3did.onion
If the website is not available, open another one: rnfdsgm6wb6j6su5txkekw4u4y47kp2eatvu7d6xhyn5cs4lt4pdrqqd.onion

3.Put your personal code in the input form:

{code_494538:
ZqtwZ53NZSkE7aVEEci1WxvluUtNH96sEbqhjVaE1+yUozppNm
7TGPz9OMC3AR6joMKWGGzyczNUU6lIxBFh2kjlNmwBYiRw3ljs
+KQ4RUl9IoU7IMbOY8NP9qGwn5+PGStPwGfA5Yu5att5U8aQ6s
YQW9JYx+KPBUy1ly+slIow/YQRawtcF6H/+DGyWUtK7wn8OZpN
aOqqS7fhU5fCXlUsy63HwxZs/5mO5pe2OwPFQvZlzU4t8izkYo
ZVB2HAcboXsowktQwm5sgJs5vgyJCPMdnjANcIXg==}
```

Ransomware

😱 Come rimediare ad un’infezione?

1. 🧽 🧼 Farsi **ripulire** il computer da un tecnico
   I ransomware di solito non persistono una volta terminato il loro lavoro, ma perchè rischiare?
2. 🧰 Ripristinare i file da un backup se lo si ha
3. 🤞 Vedere se www.nomoreransom.org vi può aiutare
4. 💸 Pagare il riscatto **generalmente** funziona ma:
   State comunque **finanziando dei criminali** (che potrebbero **fregarvi due volte**)
   Negate sempre ed in modo assoluto di aver pagato il riscatto

Banking (trojan/malware)

🇬🇧 Banking 🇮🇹 Che riguarda operazioni di banca

Modificano il vostro computer per redirottare 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

I ❤️ 🇮🇹

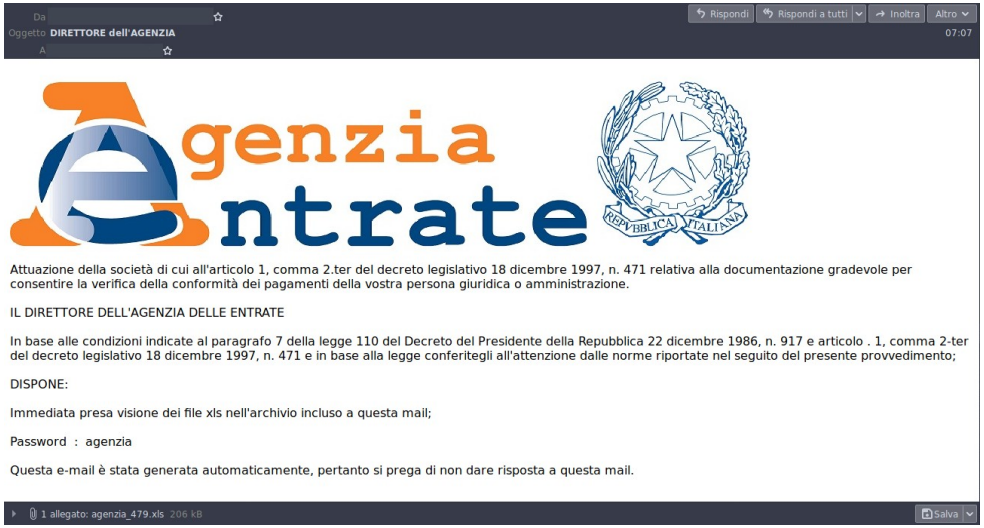
🇸🇮 Operato da criminali moldavi o russi

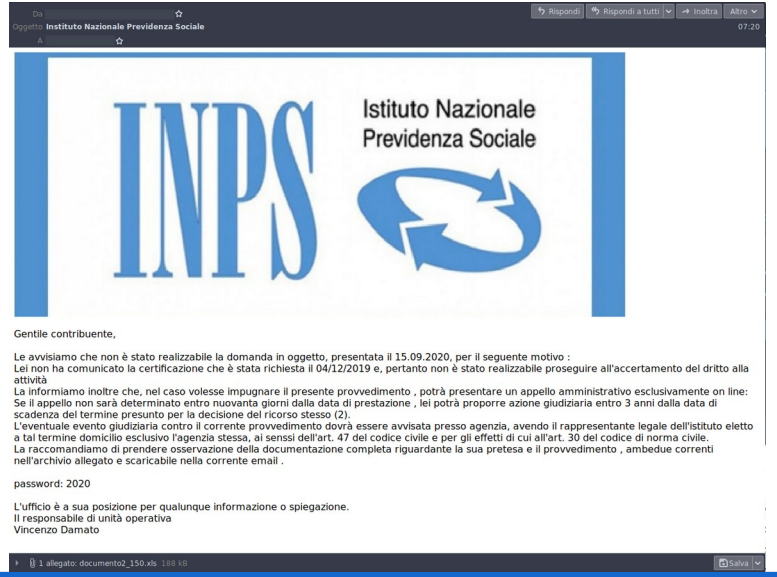
🌛🌜 Si presenta due/tre volte a settimana con una media di ~300 vittime a campagna

Banking (trojan/malware)

Esempio: Ursnif

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





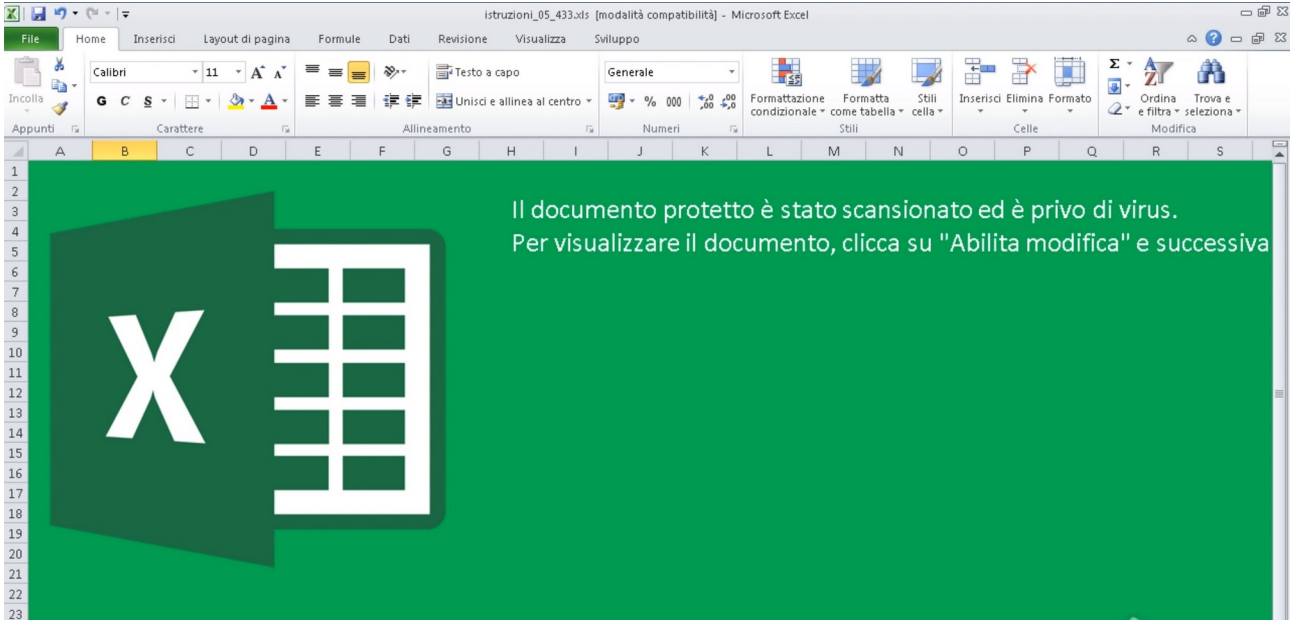
Banking (trojan/malware)

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)

😱 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

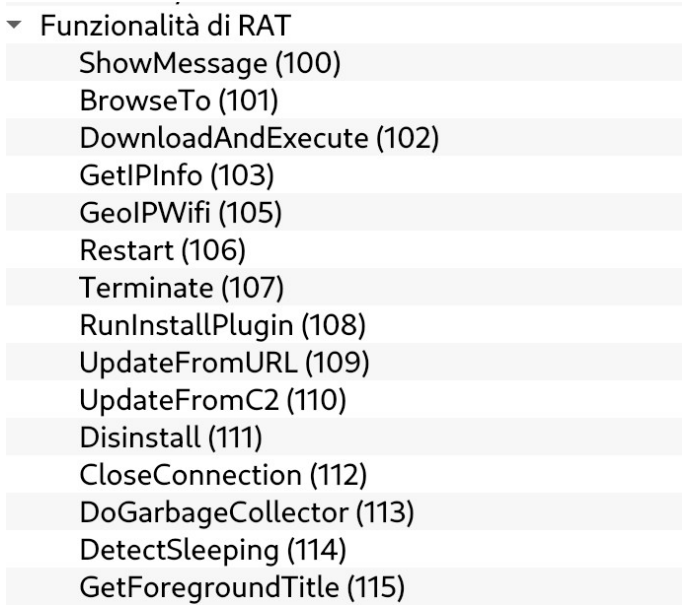
⬇️ Lo scopo principale di un RAT: scaricare programmi malevoli da eseguire

💯 Massima flessibilità per l'attaccante

💣 Sono attacchi più sofisticati e pericolosi

⌨️ Spesso spiano quello che viene scritto o è presente sullo schermo

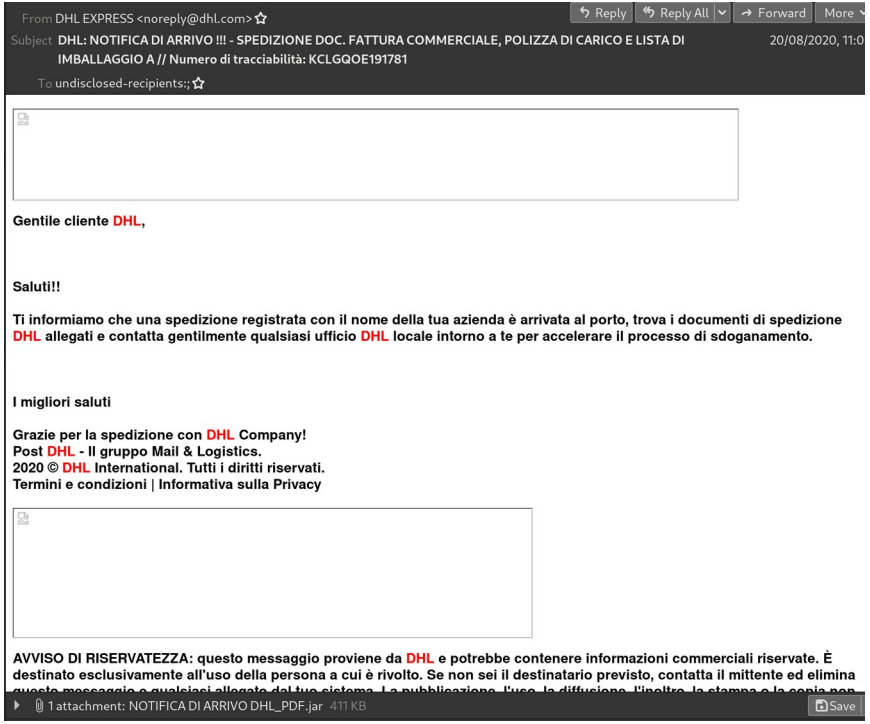
🎥 🎙️ Ci sono capitati casi (non isolati) di RAT che spiano anche da videocamera e microfono



RAT e movimenti laterali

Diffusi tramite e-mail malevole o da gruppi di criminali che setacciano internet alla ricerca di server vulnerabili

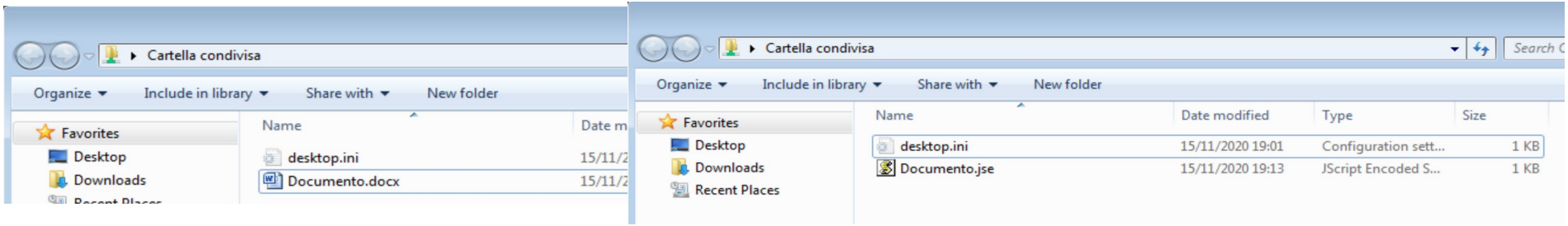
👉 Aggiornate sempre i vostri computer e i vostri server



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

😱 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

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 e CERT-AGID sono stati istituiti per supportarvi nella prevenzione e in caso di incidente