22-12-2020 – Analisi variante trojan Emotet

future. perfect. simple.

Sommario

Introduzione

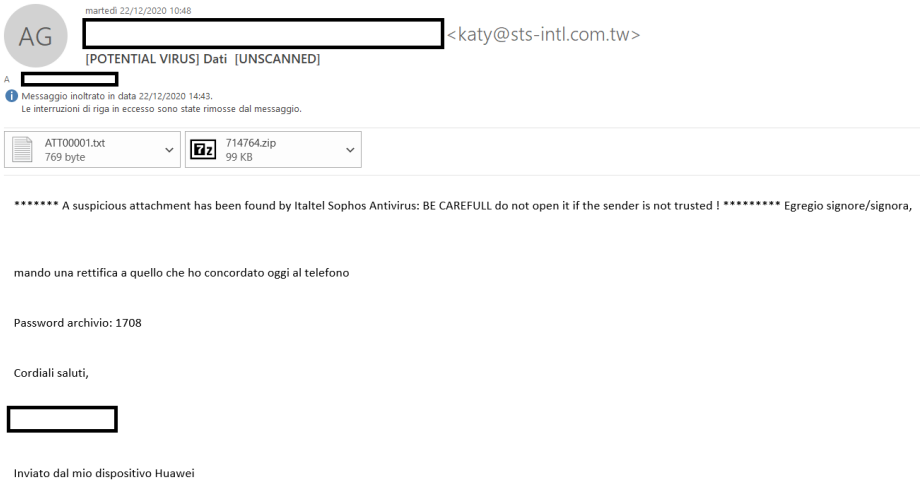
È stata identificata una nuova variante del malware Emotet che viene veicolata tramite campagna mail spam, impersonando la mail aziendale.

Emotet è uno dei trojan più pericolosi mai creati. Da quando è stato creato, sono state implementate diverse varianti per eludere i sistemi di sicurezza. Si rivolge principalmente alle vittime aziendali, ma anche gli utenti privati vengono infettati in campagne di posta elettronica di spam di massa.

Oggi, 22/12/2020 ore 23:43, su 63 vendor differenti di antivirus, questa variante del malware è stata identificata da 20 vendor.

Vettore d'attacco

La campagna massiva di mail spam è stata riscontrata per la prima volta, il giorno 21/12/2020 dalle ore 20.50 e la mail si presenta come da immagine seguente:

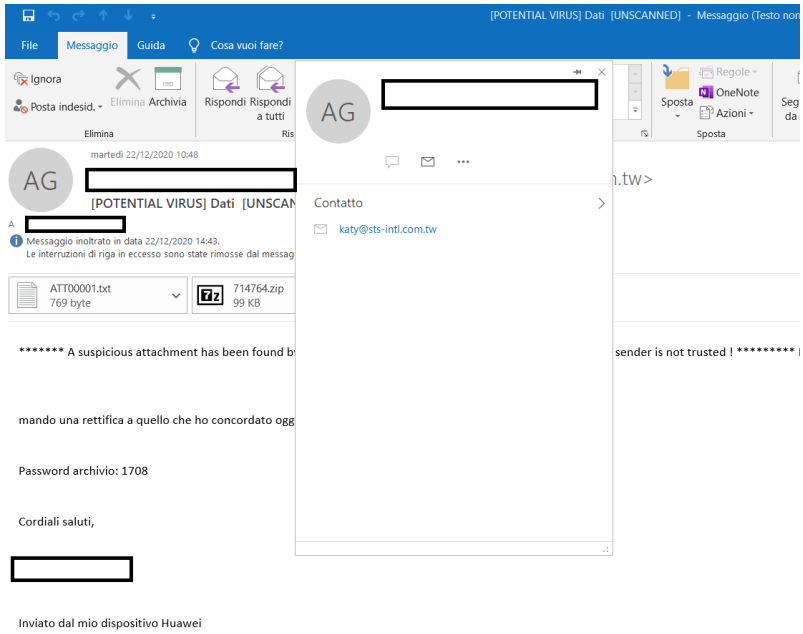


Analizzando le proprietà della mail, l'IP dei server da cui parte la campagna di mail spam sono:

- 137.59.125.145
- 59.120.55.108
- 128.199.73.58

Le mail sembrano essere inviate da un dominio aziendale ma viene utilizzata una tecnica di "email spoofing attack" che nasconde il reale mittente della mail.

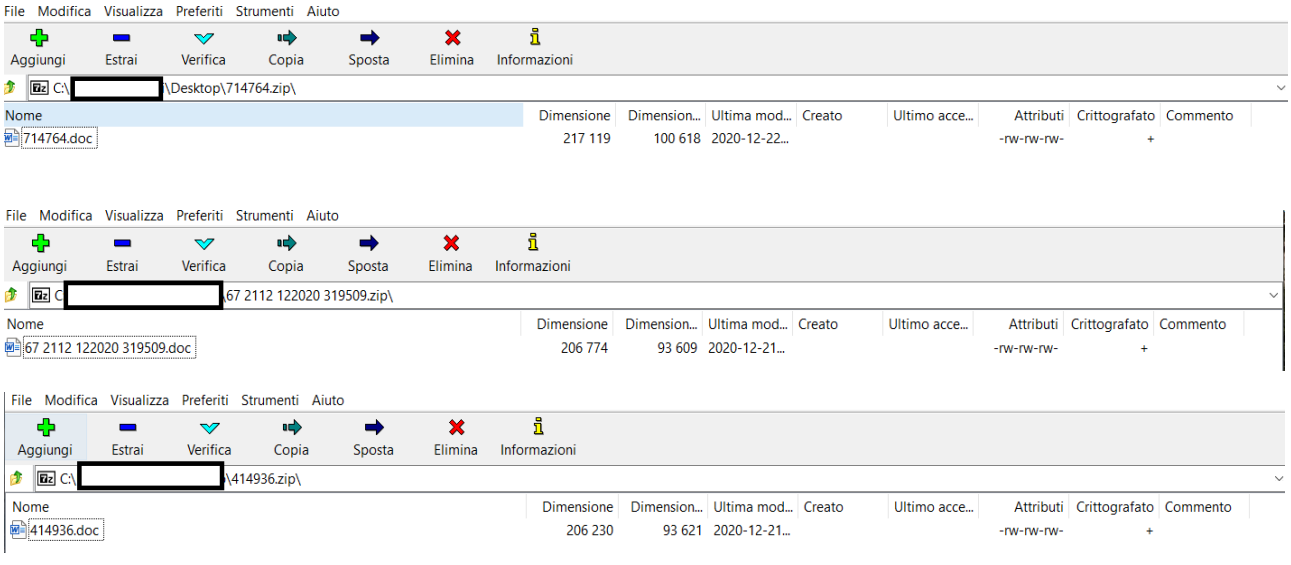
Per verificare il reale mittente della mail, fare doppio click l'indirizzo mail del mittente.



In allegato è presente un file ".zip", denominato da una sequenza causale di numeri e protetto da password (presente nella mail).
Al suo interno è presente un file word con estensione ".doc", denominato con lo stesso nome del file in allegato.

Attualmente sono stati identificati 3 documenti differenti:

- 714764.doc
- 67 2112 122020 319509.doc
- 414936.doc



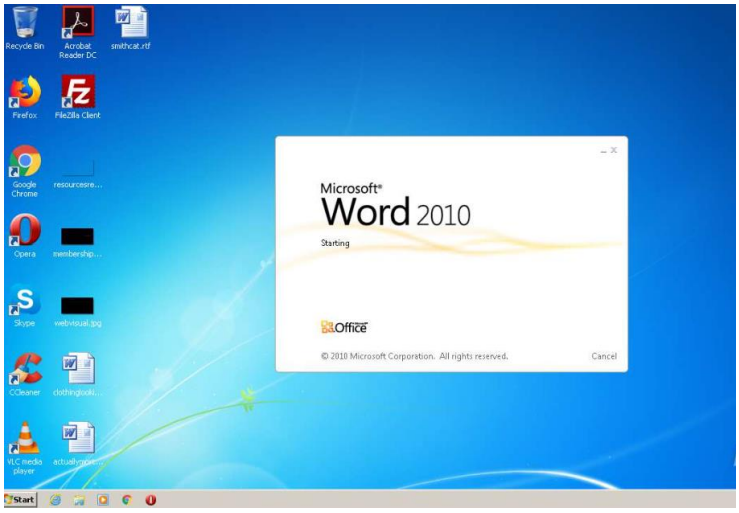
Nella sezione successiva sarà analizzata l'infezione del documento "*714764.doc*".

Infezione

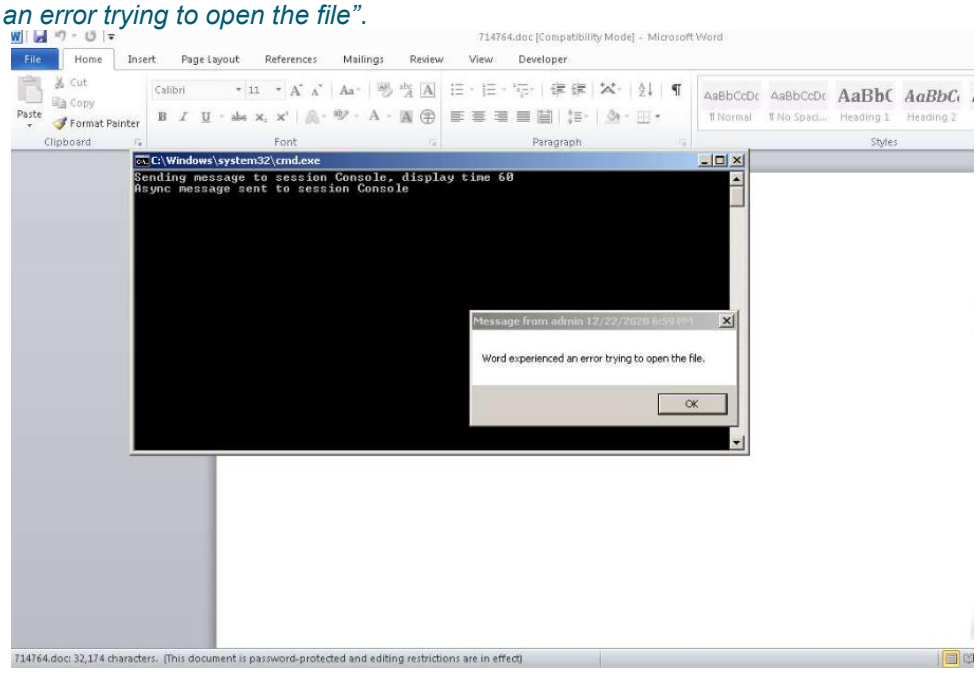
Il test è stato effettuato utilizzando il seguente SO:

- Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
- Microsoft Office 2010

STEP 1:
Facendo doppio click sul documento "*714764.doc*", come si può vedere dall'immagine seguente, il documento viene aperto, senza mostrare alcun comportamento anomalo.



STEP 2:
In modo automatico viene mostrato il prompt dei comandi di Window, con il seguente pop-up d'errore *"Word experienced an error trying to open the file"*.



STEP 3:
Il prompt dei comandi di Windows si chiude in senza alcun'interazione con l'utente. Il pop-up d'errore risulta ancora presente ed infine viene caricata la semplice pagina di word contente un printscreen di Office365.

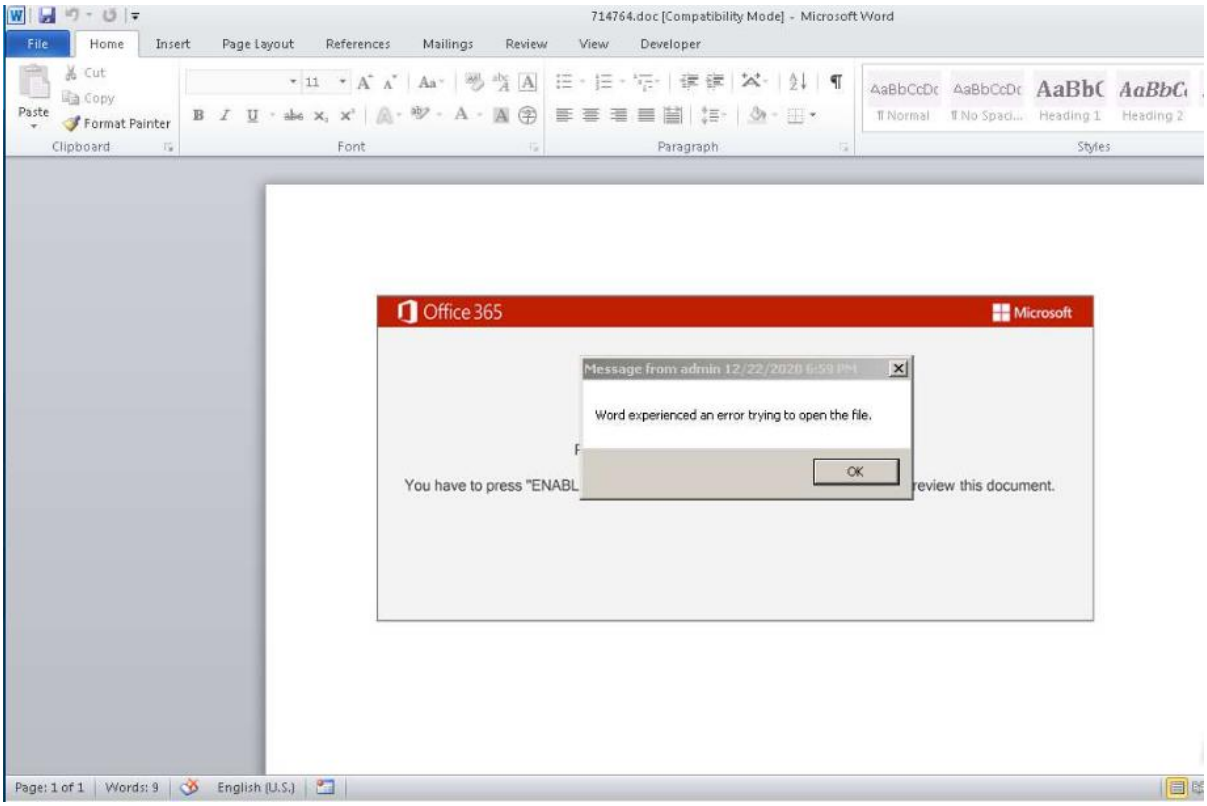
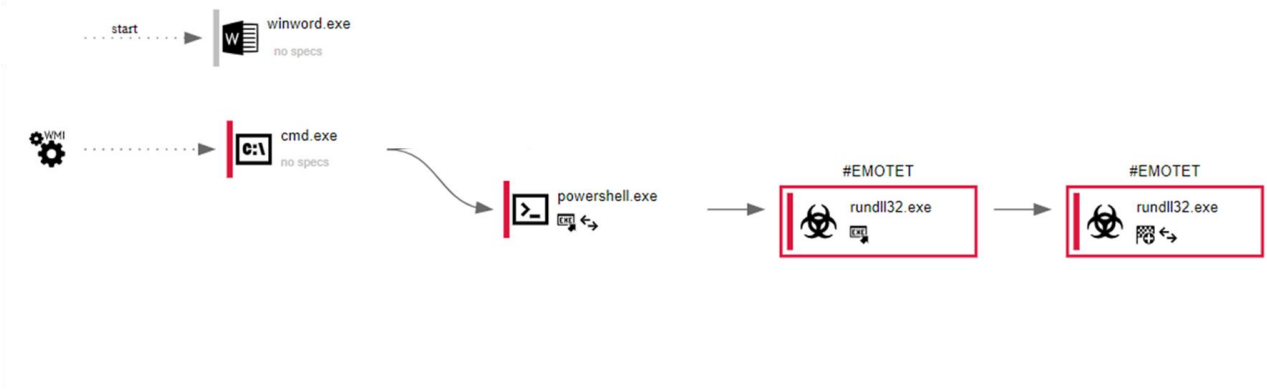


Grafico dell'infezione



Dettaglio dei processi

Di seguito sono descritti in cascata tutti i processi:

1. WINWORD.EXE

Comando eseguito: “C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /n "C:\Users\admin\AppData\Local\Temp\714764.doc"

Comportamento riscontrato:

- Creates files in the user directory
- Reads Microsoft Office registry keys

2. CMD.EXE

Invocata la powershell

Comportamento sospetto riscontrato:

- Executes PowerShell scripts
- Executed via WMI

2.1 POWERSHELL.EXE

Download della libreria “*Lyeta6ud.dll*” dal seguente URL “http://localaffordableroofer.com/ralphs-receipt-f2uhf/qTT5DC/”

Comportamento sospetto riscontrato:

- Uses RUNDLL32.EXE to load library
- Executable content was dropped or overwritten
- Creates files in the user directory

2.2 RUNDLL32.EXE

Comando eseguito: “C:\Windows\system32\rundll32.exe" C:\Users\admin\O_wgqv7\C0316em\Lyeta6ud.dll"

Comportamento sospetto riscontrato:

- Drops a file with a compile date too recent
- Executable content was dropped or overwritten
- Uses RUNDLL32.EXE to load library
- Application launched itself

Comportamento pericoloso riscontrato:

- Loads dropped or rewritten executable
- Drops executable file immediately after starts
- EMOTET was detected

2.3 RUNDLL32.EXE

Comando eseguito: “C:\Windows\system32\rundll32.exe "C:\Users\admin\AppData\Local\Aode\bhfn.uvx",RunDLL"

Connessione al seguente URL http://184.66.18.83/3njedqcfmdmg6du9/

Comportamento pericoloso riscontrato:

- Changes the autorun value in the registry
- EMOTET was detected
- Connects to CnC server

Network Activity

HTTP REQUEST

Process	Method	HTTP Code	IP	URL
powershell.exe	GET	404	35.200.206.198:80	http://zenithcampus.com/l/yQ/
powershell.exe	GET	200	107.180.12.39:80	http://localaffordableroofer.com/ralphs-receipt-f2uhf/qTT5DC/
rundll32.exe	POST	200	184.66.18.83:80	http://184.66.18.83/3njedqcfmdmg6du9/

DNS REQUESTS

Domain	IP
zenithcampus.com	35.200.206.198
localaffordableroofer.com	107.180.12.39

Indici di compromissione (IOC)

Main object- "714764.doc"
sha256 27c0c98a27584653b04d03c79bbef358ba437033a9fb2fbf641b2a89b3eca495
sha1 4b92067d0224acaea57b01973a6d6dcdbf78c75c
md5 aa3c0a3844dd5cd7b6a0935aafe86951

Dropped executable file
sha256 C:\Users\admin\O_wgqv7\C0316em\Lyeta6ud.dll
d5d11ac65cc867cedd264ae2486bbced69a65041765f640575e899e8f743e629

DNS requests
domain zenithcampus.com
domain localaffordableroofer.com

Connections
IP 35.200.206.198
IP 107.180.12.39
IP 184.66.18.83

HTTP/HTTPS requests

URL http://zenithcampus.com/l/yQ/
URL http://localaffordableroofer.com/ralphs-receipt-f2uhf/qTT5DC/
URL http://184.66.18.83/3njedqcfmdmg6du9/

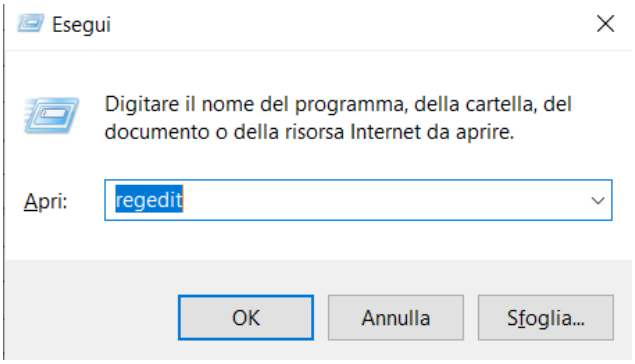
Ulteriori IOC

MD5	ba22ac5de84bcfb11a951094307d59ac 0e276401e21ba606361f506e3a2061df
SHA1	d75ab948a347edcd934756a1bc802e781de938e7 d7d0607ce2789cf7a190ba3a416cd8c05daa5f2f
SHA256	c99e251a3f0bb358f66d98f7528c7adda9acd8f95d53a13283951f06f1e0c0fd b1287acbc0882e8b3b65d4c9136928bbab731df5c41fbe0c6e34123dd8d29a59
URL	http://hbprivileged.com/cgi-bin/kcggF/ http://azraktours.com/wp-content/NWF9jC/ http://paulscomputing.com/CraigsMagicSquare/H/ http://biglaughs.org/smallpotatoes/rRwRzc/ http://azraktours.com/wp-content/NWF9jC/
IP	181.136.190.86 118.38.110.192 181.136.190.86

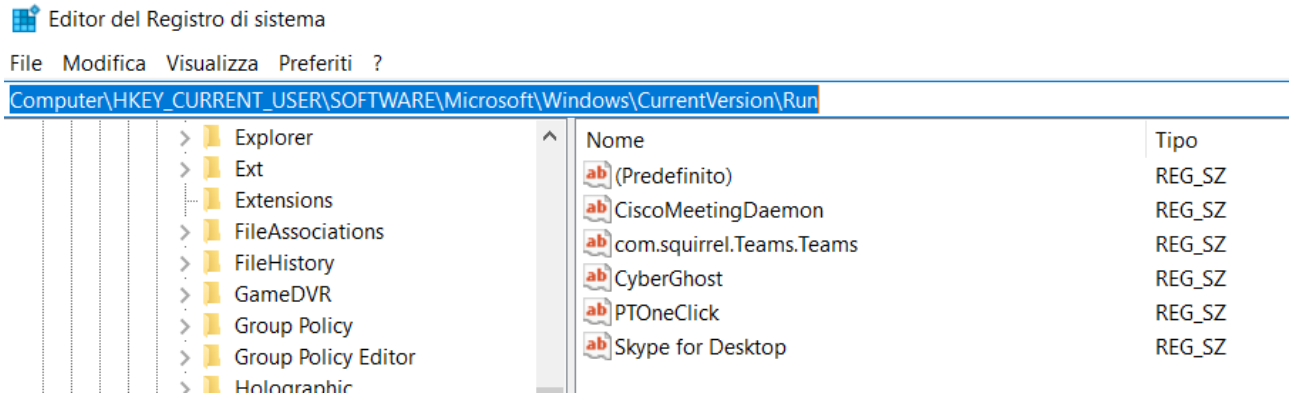
Come riconoscere l'infezione

Per riconosce la presenza di questa variante di emotet, eseguire un controllo del file di registro di Windows.

Cliccare su Win + R e digitare "regedit".



Recarsi al seguente path "HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run".



Controllare di non aver un registro con i seguenti valori:

- **name:** bhfn.uvx
- **operation:** write
- **typeValue:** REG_SZ
- **value:** C:\Windows\system32\rundll32.exe "C:\Users\admin\AppData\Local\Aode\bhfn.uvx",RunDLL

In caso affermativo, oppure se notate che il nome non è come quello menzionato precedentemente ma l'estensione del nome file termina con "**.uvx**", contatta il responsabile tecnico della tua organizzazione.

Cosa fare se si ha il sospetto di aver ricevuto un attacco di questo tipo

- Verificare che l'Antivirus riconosca le firme del malware. Allego link a virustotal dove è possibile verificare la lista degli antivirus che lo riconoscono (https://www.virustotal.com/gui/file/27c0c98a27584653b04d03c79bbef358ba437033a9fb2fbf641b2a89b3eca495/detection).

- Nei capitoli precedenti abbiamo dato indicazioni su IOC .

- Exprivia è a disposizione con il suo Global Reponse Team (Red Team) per supportarvi nella remediation ed analisi forense. In caso di necessità, contattate urgentemente :

- Antonio.pontrelli@exprivia.com
- Antonio.dechirico@exprivia.com

Come proteggersi

Il miglior modo per proteggersi da attacchi di questo tipo è ridurre il rischio con azioni preventive che richiedono un approccio progettuale

- *usare e mantenere aggiornato il proprio antivirus*: l'antivirus riconosce e protegge il computer contro la maggior parte dei virus in circolazione. Non è però in grado di proteggerci dai nuovi virus, è perciò fondamentale mantenerlo costantemente aggiornato

- *dotarsi di un sistema di Endpoint Detection and Response(EDR):* raggruppa gli strumenti avanzati che hanno il compito di rilevare minacce su endpoint ed eseguire attività di indagine e risposta. Il sistema EDR è in grado di:
  - Ricerca e indagare sui dati degli incidenti
  - Triage degli avvisi o convalida di attività sospette
  - Rilevamento di attività sospette
  - Caccia alle minacce o esplorazione dei dati
  - Bloccare le attività dannose

- *dotarsi di un sistema che svolga l'attività di Security Operation Center (SOC)*: unità costituita da un insieme di persone, processi e tecnologie che monitorano reti, sistemi, dispositivi e applicazioni. Con l'utilizzo di sistemi intelligenti di monitoraggio e di rilevamento degli attacchi, un SOC analizza un flusso continuo di dati generati da ogni azione e interazione informatica. La scopo principale di un SOC è rilevare e fornire la giusta priorità agli incidenti che potrebbero avere un impatto negativo sui sistemi.

Exprivia è a disposizione per supportarvi nella progettazione e gestione di sistemi per proteggere gli endpoint e riconoscere in tempo un attacco.

Allego qui di seguito riferimenti ad alcuni paper ed articoli interessanti.

- https://www.securenews.it/cybercrime-domenico-raguseo-direttore-cybersecurity-di-exprivia-attacchi-informatici-in-crescita-durante-la-pandemia-ecco-su-cosa-investire-per-essere-meno-vulnerabili/
- https://www.cybersecurity360.it/nuove-minacce/cyber-security-i-crimini-aumentano-in-linea-con-la-curva-epidemica-i-consigli-per-difendersi/
- https://www.exprivia.it/it/cybersecurity-ottimizzare-gli-investimenti-per-ridurre-il-rischio-complessivo/6151/retail-40-quando-la-vendita-e-online-la-sicurezza-informatica-diventa-una-priorita.php
- https://www.exprivia.it/it/cybersecurity-ottimizzare-gli-investimenti-per-ridurre-il-rischio-complessivo/6277/threat-calculator-proteggersi-al-meglio.php

Per coinvolgerci in attività di questo tipo, coinvolgere il vostro riferimento commerciale in Exprivia.