PhotoMiner - FTP e SMB ancora a rischio

Author : Sergio Caruso

Date : 5 Marzo 2019

Durante una ricerca su Shodan, mi sono imbattuto in alcuni file eseguibili con estensione *.exe e *.scr, presenti in delle directory FTP senza autenticazione (o con account Guest).

I file erano presenti non solo nella root, ma anche in tutte le sottocartelle contenenti immagini e video.

Analizzandoli su Virustotal e su altre sandbox, ho notato subito che erano conosciuti già da diverso tempo.

Ho voluto vederci chiaro anche perché, da un'analisi più approfondita, ho notato che erano presenti su altri FTP pubblici con la stessa persistenza e metodologia.

Da una veloce ricerca su Google con gli MD5, sono risalito a un articolo di un paio di anni fa, dove era presente un'analisi su un nuovo malware adibito a minare criptovaluta infettando NAS e server FTP denominato "***PhotoMiner***[1]".

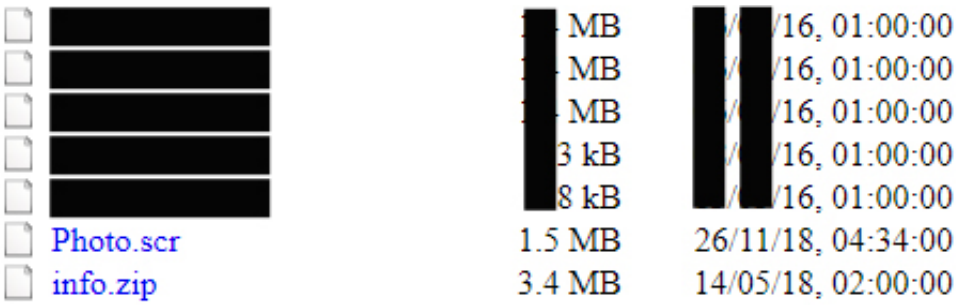


Fig.1 – ***Esempio di directory FTP compromessa dal malware.***

I file analizzati sono:

- **Photo.scr**

https://www.virustotal.com/#/file/807126cbae47c03c99590d081b82d5761e0b9c57a92736fc8516cf41bc564a7d/detection

https://www.hybrid-analysis.com/sample/807126cbae47c03c99590d081b82d5761e0b9c57a92736fc8516cf41bc564a7d?environmentId=120

https://www.joesandbox.com/analysis/94216/0/html

- **IMG001.scr**

https://www.virustotal.com/#/file/d9901b16a93aad709947524379d572a7a7bf8e2741e27a1112c95977d4a6ea8c/detection

https://www.joesandbox.com/index.php/analysis/50558/0/html

- **Info.zip** (IMG001.exe \ information.vbe)

- IMG001.exe

https://www.virustotal.com/#/file/52389828c44846fa863a6b308fad05315c13176e94c989511c2629fef0847d51/detection

- Information.vbe

https://www.virustotal.com/#/file/30daba44a4a25ff5750508613f897057a55337458f19b562e2ed1172c77e626b/detection

Fig.2 – ***File contenuti nell'archivio denominato Info.zip\info2.zip (a seconda della variante).***

A questo punto la situazione è stata molto più chiara, dato che ho potuto intuire che il meccanismo di propagazione dei malware sfrutta proprio l'assenza di autenticazione su NAS e server FTP, permettendo al worm di propagarsi e replicarsi senza ostacoli.

La situazione al febbraio 2019 appare abbastanza complessa dato che, negli ultimi 3 anni, la botnet ha continuato a estendersi.

Effettuando una rapida ricerca con Shodan, possiamo vedere che i server FTP senza autenticazione sono circa 304.000; affinando la ricerca, in Italia, ne abbiamo circa 5.000.

Query per i servizi FTP:

"230 user logged in"

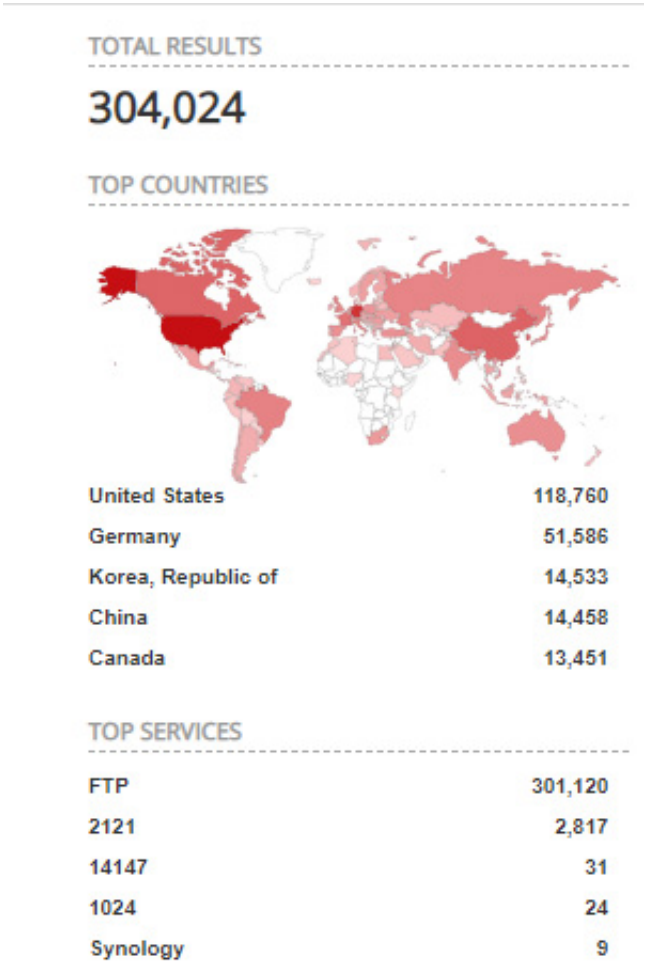


Fig.3 – *Servizi FTP senza autenticazione nel mondo*

Servizi FTP in Italia
"230 user logged in" country:"IT"

TOTAL RESULTS

4,975

TOP COUNTRIES

Italy	4,975

TOP CITIES

Rome	271
Milan	231
Naples	124
Florence	64
Ravenna	40

TOP SERVICES

FTP	4,779
2121	183
1024	8
Synology	3
HTTP (8080)	1

Fig.4 – *Servizi FTP senza autenticazione in Italia*

La situazione per il protocollo SMB è ancora più disastrosa: nel mondo abbiamo circa 545.000 servizi esposti e circa 35.000 nel territorio italiano.

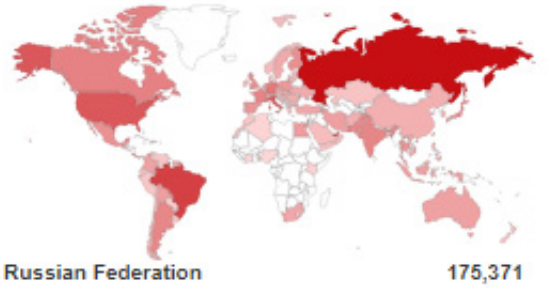
Query per i servizi SMB:

SMB "Authentication: disabled"

TOTAL RESULTS

545,013

TOP COUNTRIES



Russian Federation	175,371
United Arab Emirates	65,641
Brazil	59,000
Italy	34,240
United States	32,189

TOP ORGANIZATIONS

OJSC Sibirtelecom	92,596
Rostelecom	68,562
Emirates Telecommunications ...	64,890
Algar Telecom	43,807
Vodafone Italia DSL	11,643

Fig.5 – *Servizi SMB senza autenticazione nel mondo*

Servizi SMB in Italia:

SMB "Authentication: disabled" country:"IT"

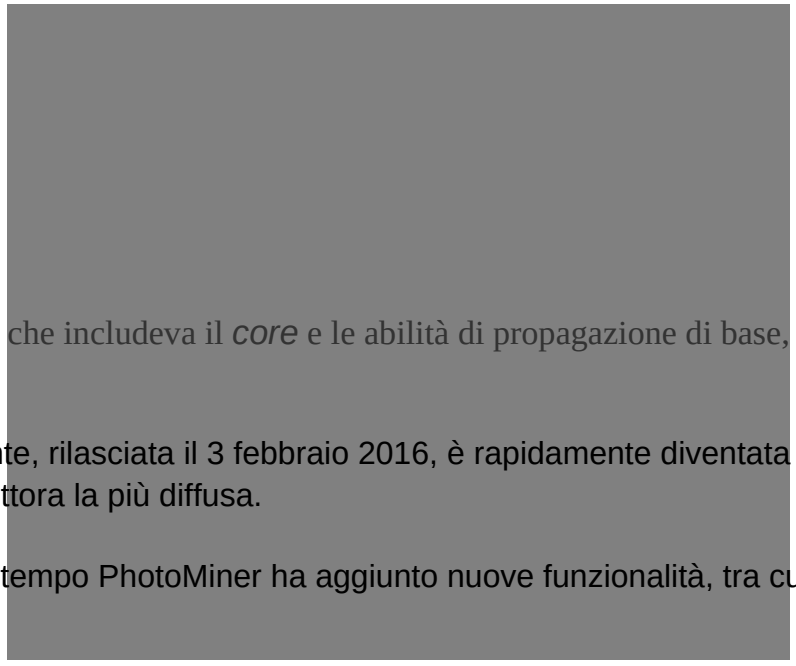
Fig.6 – ***Servizi SMB senza autenticazione nel territorio italiano***

Ho ripercorso l'evoluzione del malware per capire se la minaccia è ancora attiva o se è circoscritta a pochi server.

La sua prima comparsa ha destato molta curiosità, sia per la tipologia di diffusione - che non si avvaleva di nessun exploit specifico - sia perché offriva un meccanismo di infezione unico per propagarsi su NAS (con protocolli SMB e FTP) e su server FTP, allo scopo di estrarre Monero.

DESCRIZIONE DELL'ATTACCO

Fig.7 – *Schema d'attacco di PhotoMiner* [2]



La prima variante, che includeva il *core* e le abilità di propagazione di base, è stata compilata il 9 dicembre 2015.

La seconda variante, rilasciata il 3 febbraio 2016, è rapidamente diventata la versione dominante ed è tuttora la più diffusa.

In questo lasso di tempo PhotoMiner ha aggiunto nuove funzionalità, tra cui un esclusivo

meccanismo di infezione multistadio.

Sono stati in primo luogo compromessi i server FTP senza autenticazione o con autenticazione di default.

Esempi di autenticazione di default:

Usernames: *anonymous, www-data, administrator, ftp, user, user123*

Passwords: *password, pass1234, 123456, 1234567, 12345678, 123456789, 1234567890, qwerty, 000000, 111111, 123123, abc123, admin123, derok010101, windows, 123qwe, 000000*

Con essi anche i siti Web ospitati sono diventati vettori di infezione e di conseguenza, a causa della tipologia di minaccia, anche gli stessi visitatori infettati sono divenuti vettore d'infezione.

PhotoMiner utilizza principalmente due tipi di attacco.

Il primo prevede la scansione di IP casuali, allo scopo di accedere ai servizi con attacchi a dizionario *utente/password*, in modo da caricare una copia di se stesso sul server, compromettendo tutti quei file che possono essere sfruttati ai danni di un utente (come HTML, PHP, XML ecc...).

Con l’utilizzo di un Google Dork creato *ad hoc*, ho potuto constatare come molte pagine web abbiano inserito nel codice sorgente un “iframe” che provvede a generare in automatico il download del malware al caricamento delle stesse.

Ricerca per singolo file:

intitle:'index of' "photo.scr"

intitle:'index of' "IMG001.scr"

intitle:'index of' " IMG001.exe "

Ricerca globale:

intitle:'index of' photo.scr | IMG001.scr | IMG001.exe

Fig.8 – *Sorgente della Homepage con l'iframe al suo interno*

Successivamente al download e al click sul file eseguibile, il nuovo processo creato provvederà a inviare alla struttura di C&C, l'IP del server, le sue credenziali e l'elenco dei file infetti.
Con queste informazioni gli aggressori possono in seguito accedere ai server FTP compromessi in modo da infettare più file e vittime possibili.

Il secondo metodo si basa sull'attacco di endpoint e server Windows raggiungibili nella rete locale.

PhotoMiner utilizza strumenti di sistema integrati in Windows, tentando di forzare la connessione sul protocollo SMB e rilasciando copie di se stesso in ogni posizione accessibile.

Alcune varianti aprono di nascosto un punto di accesso Wi-Fi pubblico con SSID "*Free_WIFI_abc12345*".

Da analisi approfondite, si evince come il malware sia progettato in modo modulare, creando un eseguibile *standalone* focalizzato sull'estrazione di Monero e un *wrapper* complesso che è responsabile del meccanismo di persistenza.

- La prima variante **img001.scr** è unica nel suo uso di NSIS (Nullsoft Scriptable Install System), un linguaggio di scripting personalizzato costruito per gli installatori. NSIS è perfetto per la scrittura di semplici programmi di installazione, incluso malware. Il codice è facile da leggere ed eseguire il debug, consentendo agli aggressori di aggiungere funzionalità facilmente.
- La seconda variante **photo.scr** è un binario nativo che implementa la funzionalità **img001.scr** nel codice nativo.

All'esecuzione viene creata la cartella *NsMiner* in *%AppData%,* con all'interno i seguenti file e cartelle:

- Un file di testo chiamato *pools.txt* che contiene un elenco con URL e le porte dei pool di mining Bitcoin;

- Un'altra copia del sample originale chiamato IMG001.exe;

- Una versione a 32 bit di un bitcoin miner chiamato NsCpuCNMiner32.exe;

- Una versione a 64 bit di un bitcoin miner chiamato NsCpuCNMiner64.exe.

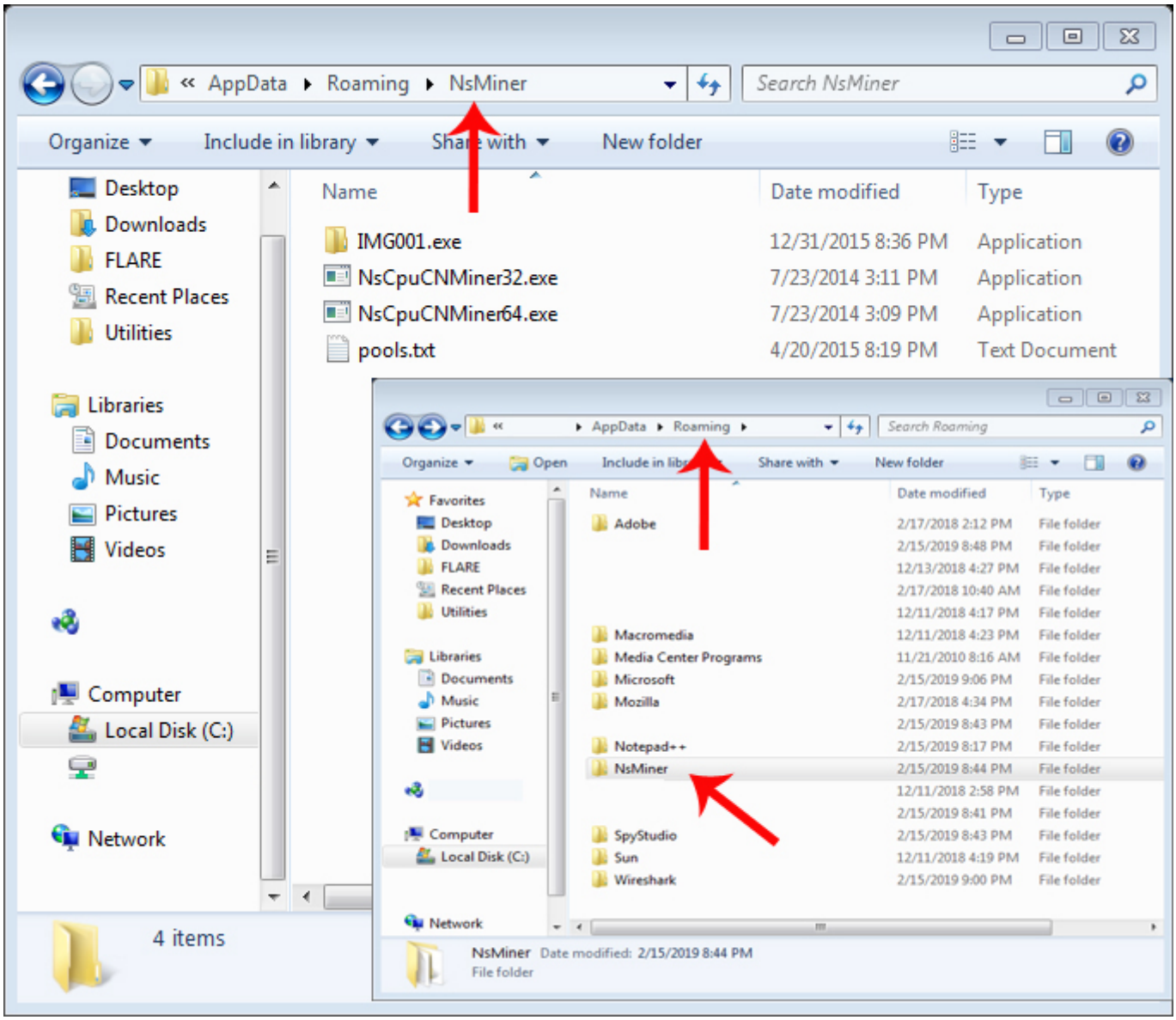


Fig.9 – *Posizione della cartella "NsMiner" con i file contenuti al suo interno*

Il file *pool.txt* contiene il pool dei domini per il mining dei Monero.

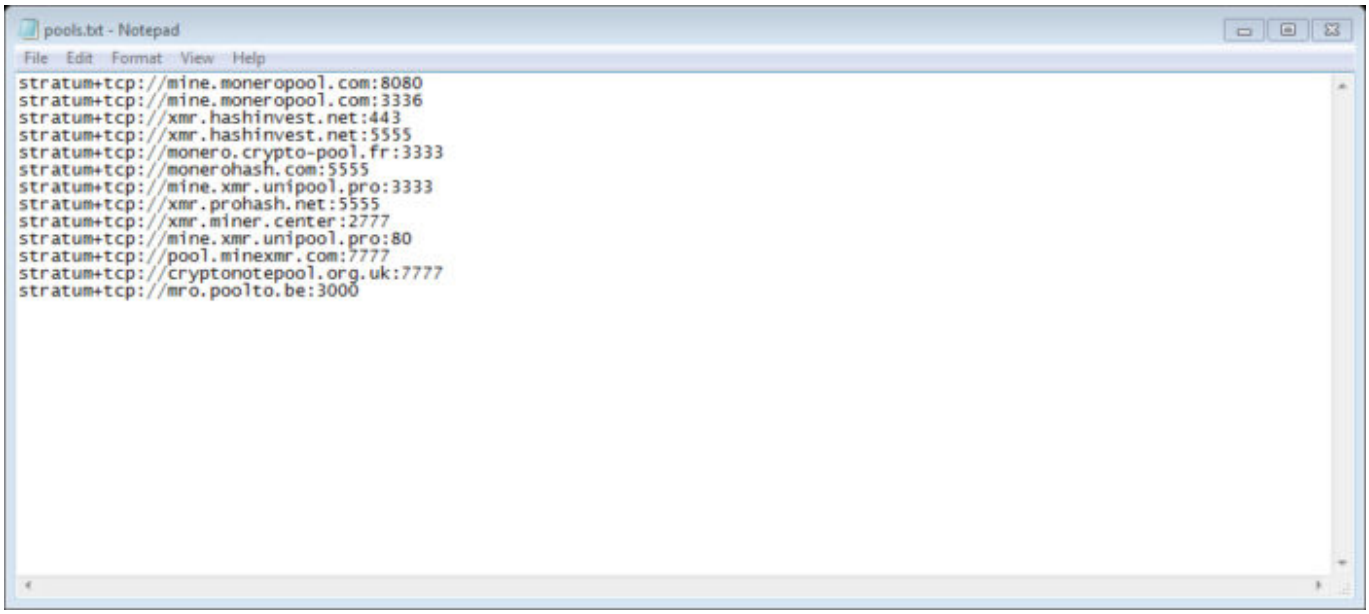


Fig.10 – *File pool.txt con domini e porte di comunicazione*

Il malware utilizza l'algoritmo ***CryptoNight*** per estrarre i bitcoin, come si evidenzia con l'analisi effettuata con il tool Binary Ninja.

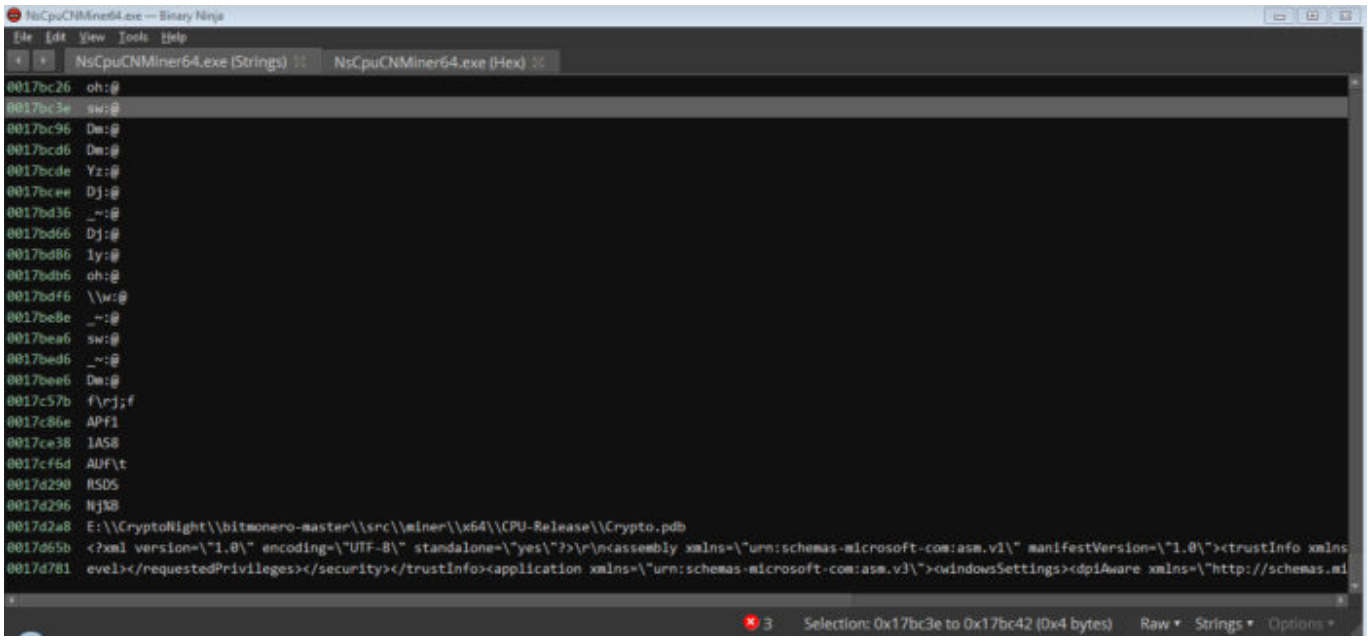


Fig.11 - *Il malware utilizza l'algoritmo CryptoNight per estrarre i bitcoin*

Durante la fase di inizializzazione, PhotoMiner crea il meccanismo di persistenza ed esegue la raccolta dei dati di configurazione per il miner.

Per installare dunque un meccanismo di persistenza, lo si posiziona nell'avvio automatico di Windows, modificando anche le seguenti chiavi di registro:

HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

%ALLUSERSPROFILE%\Microsoft\Windows\Start Menu\Programs\Startup\

%HOMEPATH%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\

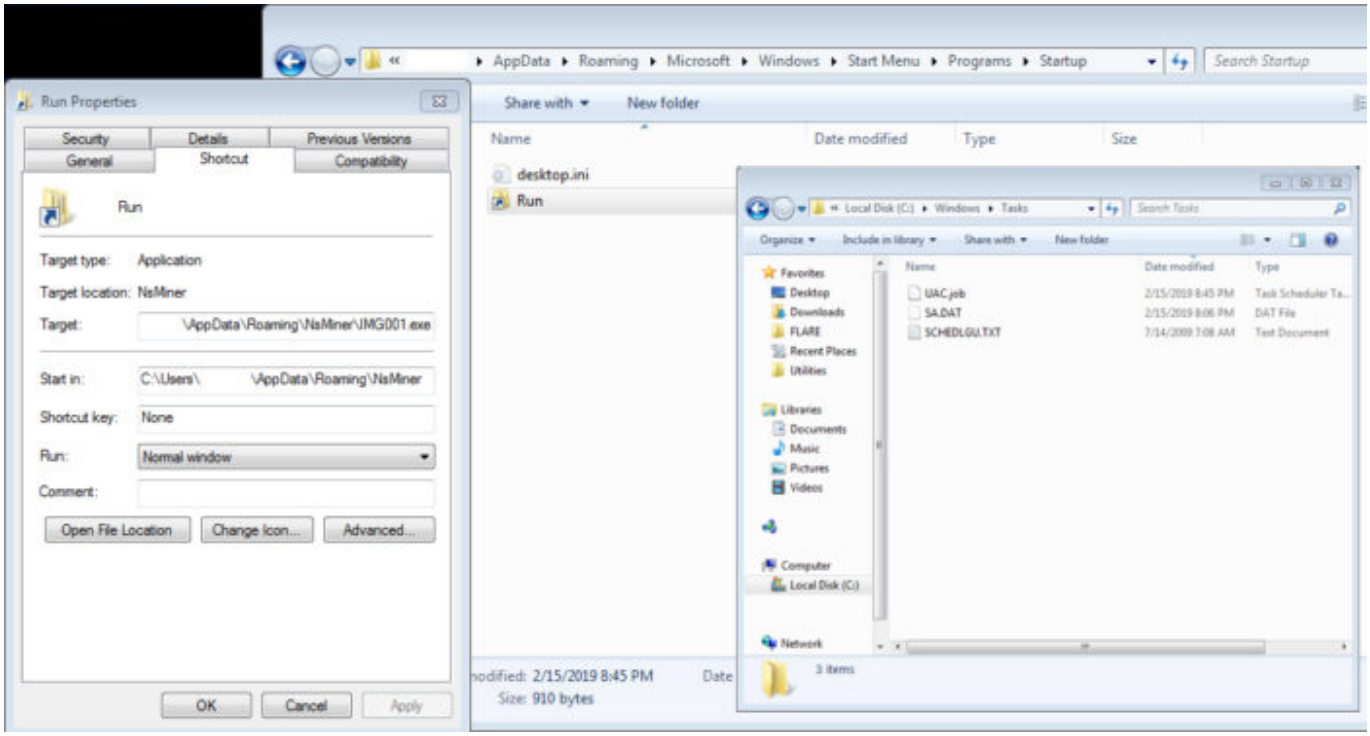


Fig.12 – *Collegamento creato in C:\Users\\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup*

Tutti i dati di configurazione raccolti durante l'attività vengono inviati verso diversi domini predefiniti su protocollo HTTP.

PhotoMiner si connette ai server C&C esclusivamente per comunicare i propri progressi senza includere nessuna funzionalità di accesso remoto.

In conclusione è possibile affermare che tutt'ora la botnet è viva e vegeta.

I file trovati nelle directory risultano aggiornati a 2\3 giorni prima della stesura di quest'articolo.

Buona parte dell'infrastruttura (contenuta nel file pool.txt) risulta ancora attiva e da analisi su Virustotal continua a ricevere traffico relativo a nuove infezioni.

Qualora fossero stati rispettati i requisiti minimi di sicurezza dei servizi FTP e SMB, la botnet non avrebbe avuto modo di svilupparsi a macchia d'olio, poiché ha sfruttato la debolezza delle password di default e la mancanza di autenticazione.

Note

[1]

https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/27000/PD27402/en_US/McAfee_Labs_Threat_Advisory-Photominer.pdf

[2] https://www.guardicore.com/wp-content/uploads/2016/06/drawing-e1465891322649.png

Articolo a cura di **Sergio Caruso**