Rotary
Commissione informatica
e anagrafe distrettuale

Cybersecurity

Manuale di intervento per il virus denominato Kasidet-URSNIF

0 Premessa

Il presente documento riporta indicazioni e istruzioni per l'intervento di pulizia dai virus Kasidet e Dridex (fra i peggiori in assoluto) chiamato anche URSNIF.
Il manuale è stato redatto con l'aiuto di esperti di sicurezza digitale e di alcuni Soci del Distretto.

Sommario

1 Modalità di 'contaminazione'

È ben documentato che gli 'untori digitali' hanno riacceso la loro storia d'amore utilizzando le macro di Office come corriere per diffondere malware bancari e persino il Trojan BlackEnergy negli ultimi tempi.
Secondo i ricercatori della società di sicurezza di San Jose zScaler, anche il bot Kasidet, noto anche come Neutrino, ha adottato questa tecnica. Gli aggressori che hanno passato il bot lo hanno intensificato nelle ultime settimane.
I ricercatori sostengono che le stesse macro VBA (Visual Basic Applications Edition) nei file di Microsoft Office che vengono sfruttate per eliminare Dridex possono essere utilizzate per eliminare anche Kasidet. Entrambi utilizzano gli allegati mascherati da documenti scansionati nelle e-mail di spearphishing.
Dopo aver scaricato il malware, questo particolare ceppo di Kasidet ruba le informazioni dalle macchine degli utenti in due modi:

- Scraping della memoria.
- Hook del browser.

La tecnica di **scraping** della memoria consente agli aggressori di rubare i dati delle carte di credito dai sistemi di punti vendita; secondo zScaler analizza la memoria dai processi in esecuzione e la inoltra tramite una stringa di caratteri URI (Uniform Resource Identifier).
Il bot **Kasidet** è in circolazione dal 2013 ed è noto principalmente per le sue funzionalità DDoS. A quanto pare, il bot ha aggiunto un modulo per il recupero dei dati a settembre.
Kasidet è in grado di intercettare il traffico proveniente dalla macchina della vittima e browser come Firefox, Chrome e IE tramite l'aggancio del browser. Secondo i ricercatori, il malware utilizza la stessa funzione di hash utilizzata da Carberp per crittografare i nomi dei browser.
Kasidet può emettere una manciata di richieste una volta che è attiva e in esecuzione, anche chiedendo il nome del sistema, la versione del sistema e se ci sono antivirus sul sistema, per citarne alcuni.
I ricercatori stanno ammonendo che potrebbe non esserci una connessione netta tra le due famiglie di malware. Solo perché la stessa campagna sembra stia facendo cadere Dridex e Kasidet, non significa che stiano lavorando insieme, affermano. Riesce a "riaffermare il fatto" che alcuni dei meccanismi sono condivisi dagli attaccanti, Yadav, Kumar e Singh.
Il file di **documento di Office malevolo** (vedi seguente immagine) è un vettore popolare per gli autori di malware che forniscono i loro carichi utili.

Gli autori di Dridex hanno sfruttato questa tecnica per oltre un anno ed è stato interessante vedere la stessa campagna e gli stessi URL sfruttati per fornire i payload di Kasidet.
Nel mese di marzo 2018, gli aggressori hanno iniziato a spingere Dridex via macro in file XML e sembra che la tecnica non sia ancora invecchiata.
I ricercatori di Invincea hanno notato che gli Hacker hanno abbandonato il malware sugli utenti francesi in ottobre 2017, mentre IBM ha osservato una campagna di spam centrata sulle vittime nel Regno Unito nel febbraio 2018. Ogni incidente ha comportato l'utilizzo di macro, solitamente disabilitate di default in Office, suggerendo che il vettore rimane popolare, indipendentemente da ciò che gli aggressori stanno spingendo.

2 Campagna malware "URSNIF"

Famiglia malware: URSNIF
VirIT: Trojan.Win32.Ursnif.ET, Trojan.DOC.Dropper.OV, 97M.Downloader.DU

Descrizione: La campagna di mail è partita questa la mattina del 20 marzo 2018.

2.1 Come si diffonde

Sfrutta gli account di posta elettronica configurati nel PC infettato, inviando finte risposte infette, a dei messaggi che sono stati GIA RICEVUTI in precedenza dalla vittima stessa.
Il corpo del messaggio è sempre lo stesso (visibile a destra), invece l'oggetto è diverso proprio perché rispondendo a dei messaggi che la vittima ha ricevuto, nei giorni precedenti, varia in base ad essi.

Oggetto: [cambia in base alla mail che si riceve]

Buongiorno,

Vedi allegato e di confermare.

In allegato si trova un file Word .DOC con nome "**Richiesta.DOC**" oppure termina con "-Richiesta.Doc" (esempio "info-Richiesta.doc").
L'allegato malevole presente nella mail è un file DOC che al suo interno contiene una MACRO AutoOpen che appena viene avviata scarica il malware e lo mette in esecuzione.
La macro AutoOpen prima esegue il file CMD.EXE passandogli come parametro la seguente stringa per eseguire PowerShell (campagna del 2018-03-20).

2.2 Come agisce il virus

Il malware che viene scaricato (parte della famiglia degli URSNIF) ha come obiettivo rilevare le password di accesso a siti importanti come possono essere home banking, posta, ftp, altro.
Non è possibile cancellarlo da Login; se ne crea un altro con questo Path:

- "HKCU\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN"; Key: "API-GSVC"; Value: "%APPDATA%\Microsoft\Cmdisvc6\adprtext.exe").

2.3 Come cercare di riconoscere una falsa mail

L'esperienza ed il buon senso sono le prime armi per non rimanere vittima di questo tipo di truffe.
È fondamentale un'attenta lettura della mail, in tutti i suoi elementi.
Diffidare da subito di allegati in formato ZIP e, se possibile in alcun modo, **NON abilitare l'esecuzione automatica delle macr**o.
È fortemente sconsigliato impostare l'esecuzione automatica delle macro poiché la semplice apertura di file Word ed Excel vedrà l'immediata esecuzione delle macro senza alcun segnale ed alert preventivo.

2.4 Consiglio utile

Nel caso in cui si fosse stati infettati da un Banker, il consiglio da parte del C.R.A.M. di TG Soft è quello di:

- Prendere opportuni accorgimenti di sicurezza anche dopo la bonifica del/dei sistemi coinvolti come il **cambio delle password più comunemente utilizzate nel Web**.

Nel caso in cui la postazione coinvolta fosse stata utilizzata per operazioni di Home-banking è consigliato anche un accertamento con il proprio Istituto di Credito.

2.5 Analisi di possibili virus

È possibile inviare eMail sospette per l'analisi come possibili virus/malware/ransomware e/o tentativi di Phishing; tale materiale da analizzare deve essere inoltrato al Centro Ricerche Anti-Malware di TG Soft per l'analisi che è sempre e comunque gratuito può avvenire in tutta sicurezza in due modalità:

- Qualsiasi e-mail che sia da considerarsi sospetta può essere inviata direttamente dalla posta elettronica del ricevente scegliendo come modalità di invio "INOLTRA come ALLEGATO" e inserendo nell'oggetto "Possibile Phishing da verificare" piuttosto che "Possibile Malware da verificare" alla mail lite@virit.com.
- Salvare come file esterno al programma di posta elettronica utilizzato la mail da inviare al C.R.A.M. di TG Soft per l'analisi. Il file che ne risulterà dovrà essere inviato facendone l'Upload dalla pagina di INVIO File Sospetti (http://www.tgsoft.it/italy/file_sospetti.asp). Naturalmente per avere un feed-back rispetto al responso dell'analisi dei file infetti inviati sarà necessario indicare un indirizzo e-mail e sarà gradita una breve descrizione del motivo dell'invio del file (ad esempio: possibile/probabile phishing; possibile/probabile malware o altro).

Tutto questo per aiutare ad aiutarvi cercando di evitare che possiate incappare in furti di credenziali, virus/malware o ancor peggio Ransomware / Crypto-Malware di nuova generazione.

2.6 Maggiori dettagli

Per maggiori dettagli consultare il seguente link
https://www.tgsoft.it/italy/news_archivio.asp?id=912

3 Interventi

Non si cancella da Login.
Ne crea immediatamente un altro con questo Path:

- "HKCU\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN"; Key: "API-GSVC"; Value: "%APPDATA%\Microsoft\Cmdisvc6\adprtext.exe").

Per maggiori info:

- https://www.hybridanalysis.com/sample/c9b634ec09cb54f8de2fd3eabcc9ef37c65352ae261980b7cdce2fd204c6e31c/5ab56f377ca3e101f2518674
- https://www.joesandbox.com/analysis/51629/1/html

Modificare tutti i Browser.
Se si utilizza Firefox è necessario cambiare il Java script, in quanto probabilmente carica un'estensione sua; conviene cancellare il profilo di Firefox e reinstallare Firefox se si utilizza Mozilla.
Naturalmente legge le Password salvate in Explorer dei vari portale etc.

Scrive questo comando
%APPDATA%\Mozilla\Firefox\Profiles\a0u7kz53.default-1460755681908\prefs.js
che modifica profilo e carica estensioni senza autorizzazione.

Gli antivirus consigliati sono:

- https://www.virustotal.com/en/file/ae65f67f93319e94ed56c13018b984bdb7ae83a32ea72e595ceb531835da67bf/analysis/
- https://www.hybrid-analysis.com/sample/c9b634ec09cb54f8de2fd3eabcc9ef37c65352ae261980b7cdce2fd204c6e31c/5ab56f377ca3e101f2518674

Molti utilizzano Kaspersky e Malwarebytes.