La cassetta degli attrezzi del bravo hacker



Dic 09, 2019 Giancarlo Calzetta Approfondimenti, Hacking, In evidenza, RSS, Software 0

Sergio Caruso è un esperto di sicurezza che abbiamo già avuto il piacere di intervistare in occasione di una sua breve ricerca sulle truffe online via cellulare. Il video, che svela cosa succede quando si clicca su una pubblicità malevola o una pagina solitamente fornita all'utente tramite browser-jacking, era molto interessante e lo trovate qui sotto:
[embedded content]
Adesso, Sergio ci ha fatto un gran regalo: una guida, devo dire molto completa, sugli strumenti "di base" che vengono usati dagli hacker per gestire le quotidiane chiamate che spaziano dall'analisi dei malware all'investigazioni forensi, passando per reverse engeneering e sfide di Capture the Flag.

Ha diviso per noi l'elenco in macro categorie, aggiungendo una breve descrizione ad ogni strumento. Questo articolo è solo un punto di partenza, ma chi ha voglia di approfondire ha da fare per mesi. Grazie Sergio!

STRUMENTI DI REVERSE ENGINEERING,

DECOMPILATORI E DEBUGGER

OllyDbg – Disponibile solo in versione a 32 bit, per sistemi Microsoft Windows.
OllyDbg traccia i registri, riconosce le funzioni e i parametri passati alle principali librerie standard, le chiamate alle API del sistema operativo, eventuali salti condizionali, tabelle, costanti, variabili e stringhe.

Immunity Debugger – Nuovo modo efficace per scrivere exploit, analizzare malware e decodificare file binari. Si basa su una solida interfaccia utente con funzione grafica, il primo strumento di analisi heap del settore costruito appositamente per la creazione di heap e un'API Python ampia e ben supportata per una facile estensibilità.

GDB – GNU debugger è un programma libero sviluppato dal progetto GNU. È il debugger predefinito del sistema operativo GNU, gira su molte piattaforme ed è capace di analizzare numerosi linguaggi di programmazione, tra cui Ada, C, C++ e Fortran.

IDA Pro – L'Interactive Disassembler, più comunemente conosciuto con il nome IDA, è un disassembler largamente usato per il reverse engineering. Supporta numerosi formati di file eseguibili per diversi processori e sistemi operativi.

WinDbg – Debugger di Windows. Può essere utilizzato per eseguire il debug del codice in modalità kernel e in modalità utente, per analizzare i dump di arresto anomalo e per esaminare i registri della CPU durante l'esecuzione del codice.

PE Tools – Consente di ricercare attivamente file e processi PE. Sono inclusi Process Viewer e Editor di file PE, Dumper, Rebuilder, Comparatore, Analizzatore.

UPX – Ultimate Packer per eXecutables è un packer eseguibile

open source che supporta numerosi formati di file da diversi sistemi operativi.

Radare2 – Framework completo per il reverse engineering e l'analisi dei binari; composto da un insieme di piccole utility che possono essere utilizzate insieme o indipendentemente da riga di comando.

Strace – Utility di debugging per Linux e altri sistemi Unix-like che esamina le chiamate di sistema usate da un programma e tutti i segnali che esso riceve, analogamente all'utility truss presente in altri sistemi Unix. Ciò è reso possibile da una funzionalità chiamata ptrace.

CFF Explorer – Suite di strumenti freeware che include un editor PE chiamato CFF Explorer e un visualizzatore di processi.

Barf – Binary Analysis and Reverse engineering Framework è un framework open source multipiattaforma per l'analisi binaria e il reverse engineering

Binary Ninja – Framework di Reverse Engineering

Hopper – Strumento di reverse engineering per OSX e Linux

Apktool – Strumento per il reverse engineering di app Android. Può decodificare le risorse in una forma quasi originale e ricostruirle dopo aver apportato alcune modifiche.

dex2jar – Strumento per lavorare con i file Android .dex e java .class

Androguard – Reverse engineering, analisi di malware e goodware di applicazioni Android

Apk2Gold – Strumento CLI per la decompilazione di app Android in Java.

Jadx – Strumenti da riga di comando e GUI per produrre codice

sorgente Java da file Dex e Apk Android

Java Decompilers – Decompilatore online per APK Java e Android

RABCDAsm – Raccolta di utilità incluso un assemblatore/disassemblatore ActionScript 3.

Swftools – Raccolta di utility per lavorare con file SWF

Xxxswf – Uno script Python per l'analisi dei file Flash.

Detox – Strumento per supportare l'analisi manuale di codice Javascript dannoso.

Krakatau – Decompilatore e disassemblatore Java

STRUMENTI PER L'ANALISI DEL CODICE STATICO

RIPS – Software di analisi del codice statico per il rilevamento automatico delle vulnerabilità della sicurezza nelle applicazioni PHP e Java. Lo strumento iniziale è stato scritto da Johannes Dahse e rilasciato durante il mese di PHP Security nel maggio 2010 come software open source.

OWASP Code Crawler – È uno strumento di revisione del codice statico che cerca argomenti chiave all'interno del codice .NET e J2EE / JAVA.

OWASP LAPSE Project – Security scanner per rilevare le vulnerabilità di data injection nelle applicazioni Java EE.

Flawfinder – Analizzatore di codice sorgente statico per C / C ++. Segnala possibili punti deboli di sicurezza

ANALISI FORENSE

SANS Investigative Forensic Toolkit (SIFT) – Distribuzione di informatica forense che installa tutti gli strumenti necessari

su Ubuntu per eseguire un esame digitale forense dettagliato e di risposta agli incidenti. È compatibile con i formati dei testimoni esperti, i formati forensi avanzati, i formati di prove di analisi non elaborate e di memoria.

Volatility – Framework di Memory Forensics open source per la risposta agli incidenti e l'analisi dei malware. È scritto in Python e supporta Microsoft Windows, Mac OS X e Linux.

Sleuth Kit – Raccolta di utility basate su Unix e Windows per facilitare l'analisi forense dei sistemi informatici. È stato scritto ed è gestito principalmente dall'investigatore digitale Brian Carrie.

Xplico – Network Forensic Analysis Tool (NFAT), ovvero un software che ricostruisce i contenuti dalle acquisizioni eseguite con packet sniffer (ad esempio Wireshark o tcpdump).

Binwalk – Strumento veloce e facile da usare per l'analisi, il reverse engineering e l'estrazione di immagini del firmware.

ExifTool – Software gratuito e open source per la lettura, la scrittura e la manipolazione di metadati di immagini, audio, video e PDF. È indipendente dalla piattaforma, disponibile sia come libreria Perl sia come applicazione da riga di comando.

CAINE – Computer Aided INvestigative Environment è una distribuzione live GNU / Linux italiana creata come progetto Digital Forensics. Offre un ambiente forense completo organizzato per integrare strumenti software esistenti come moduli software e fornire un'interfaccia grafica intuitiva.

DEFT Linux – Distribuzione GNU/Linux live di software libero basata su Ubuntu per usi legati alla Computer Forensics e alla sicurezza informatica.

Aircrack-Ng – Suite completa di strumenti per valutare la sicurezza della rete WiFi 802.11 WEP e WPA-PSK

Ophcrack – Software di password cracking, dedicato al cracking

di password di sistemi Windows. E’ gratuito, open source e basato su Rainbow Tables. E’ disponibile anche sotto forma di Live CD, una volta fatto il boot, in automatico preleva i file SAM di windows e avvia le procedure di cracking.

Creddump – Strumento in Python per estrarre varie credenziali dal registro di Windows

Strumento Exif – Legge, scrive e modifica i metadati dei file

Extundelete – Utilizzato per il recupero di dati persi da immagini montabili

Fibratus – Strumento per l’esplorazione e la traccia del kernel di Windows

Fsck.ext4 – Usato per riparare filesystem corrotti

Malzilla – Strumento per l’hunting di malware

NetworkMiner – Strumento di analisi forense della rete

PDF Streams Inflater – Trova ed estrae file zlib compressi in file PDF

ResourcesExtract – Estrae vari tipi di file dagli ex

Shellbags – Esamina i file NT_USER.dat

UsbForensics – Tool che contiene molti strumenti per la analisi forense su dispositivi USB

RegistryViewer – Utilizzato per visualizzare i registri di Windows

John The Ripper – Strumento per il cracking delle password. Supporta il riconoscimento automatico degli hash e vari tipi di attacco: vocabolario o forza bruta. Attualmente può essere eseguito su 15 differenti piattaforme.

Hashcat – Strumento per il cracking delle password. Contiene

tutte le funzioni di John The Ripper, ma è pensato per velocizzare le operazioni di cracking sfruttando il calcolo parallelo con le GPU.

FeatherDuster – Strumento di crittografia modulare automatizzato

PkCrack – Uno strumento per rompere la crittografia PkZip

RSACTFTool – Uno strumento per recuperare la chiave privata RSA con vari attacchi

RSATool – Genera chiave privata con conoscenza di p e q

XORTool – Uno strumento per analizzare la crittografia xor multi-byte

John The Jumbo – Versione migliorata di John the Ripper

Nozzlr – Framework di brute force modulare e intuitivo.

STEGANOGRAFIA

Exif – Mostra le informazioni EXIF □□nei file JPEG

Exiv2 – Strumento di manipolazione dei metadati di immagine

ImageMagick – Strumento per manipolare le immagini

Outguess – Strumento steganografico universale

Pngtools – Per varie analisi relative ai PNG

SmartDeblur – Utilizzato per eseguire il deblur e correggere immagini sfocate

Steganabara – Strumento per analisi stegano scritto in Java

Stegbreak – Lancia attacchi brute force con dizionario sulle immagini JPG

StegCracker – Utilità di forza bruta Steganography per

scoprire dati nascosti all’interno dei file

stegextract – Rileva file e testo nascosti nelle immagini

Steghide – Strumento eccezionale che può essere utilizzato per incorporare o estrarre dati in vari tipi di file di immagini e audio

Stegsolve – Applica varie tecniche di steganografia alle immagini

Zsteg – Analisi dei file PNG / BMP per la rilevazione di tecniche di steganografia

MP3Stego – Consente di nascondere del testo nei file MP3

STRUMENTI UTILIZZATI PER ESEGUIRE VARI TIPI DI ATTACCHI

Exploit-db – Database sulle vulnerabilità con libero accesso.

Burp Suite – Strumento per testare la sicurezza delle applicazioni Web. Scritto in Java e sviluppato da PortSwigger Web Security.

OWASP ZAP – Progetto di sicurezza delle applicazioni Web, simile a Burp ma gratuito e open source

WPScan – Scanner per vulnerabilità WordPress

Reaver – Strumento d’attacco di brute force contro i PIN del Wifi Protected Setup (WPS) al fine di recuperare le passphrase WPA/WPA2.

Nmap – Portscanner Open Source con plug-in per la valutazione delle vulnerabilità e il rilevamento della rete

Wireshark – Sniffer di rete e analizzatore di protocolli per Unix e Windows

Netcat – Programma open source a riga di comando di comunicazione remota, utilizzabile sia col protocollo TCP sia col protocollo UDP. Netcat è stato pensato per essere utilizzato facilmente da altri programmi o scripts.

Masscan – Scanner per IP massivo.

Raccoon – Strumento di sicurezza ad alte prestazioni per la scansione di vulnerabilità.

Sqlmap – Software Open Source per il penetration testing, che permette di automatizzare il rilevamento e lo sfruttamento delle SQL injection e prendere così il controllo dei server DBMS. Il software lavora a linea di comando.

W3af – Attacco alle applicazioni Web e framework di audit.

XSSer – Tool per attacchi di tipo XSS automatizzato

Metasploit Framework – Oltre ad essere un framework di test di penetrazione, Metasploit ha moduli per lo sfruttamento automatico e strumenti per la creazione di exploit.

Bettercap – Framework per eseguire attacchi MITM (Man in the Middle).

DLLInjector – Inietta dll nei processi

libformatstr – Semplifica lo sfruttamento delle stringhe di formato.

Pwntools – CTF Framework per scrivere exploit

Gadget ROP – Framework per lo sfruttamento ROP

V0lt – Security CTF Toolkit

Monit – Strumento Linux per controllare un host sulla rete (e altre attività non di rete).

Nipe – Script per rendere Tor Network il gateway predefinito.

Zmap – Scanner di rete open source.

Position Grabber – Strumento per la creazione di link di cattura personalizzati. Quando verrà aperto dal bersaglio automaticamente arriverà una mail con un link ad una Mappa interattiva con la posizione.

OSINT – OPEN SOURCE INTELLIGENCE TOOLS

Maltego – Tool sviluppato dalla società Paterva, che offre la possibilità di raccogliere informazioni tramite la consultazione di dati pubblicamente accessibili e raggrupparle in formato grafico.

Google Dorks – Query, utilizzate principalmente sul motore di ricerca Google, che utilizza operatori di ricerca avanzati al fine di trovare informazioni che non sono prontamente disponibili su un sito Web. Google Dorking, noto anche come Google hacking, può restituire informazioni difficili da individuare tramite semplici query di ricerca.

Metagoofil – Strumento di raccolta di informazioni progettato per l'estrazione di metadati di documenti pubblici (pdf, doc, xls, ppt, docx, pptx, xlsx) appartenenti a un'azienda target.

Recon-ng – Framework di ricognizione progettato con l'obiettivo di fornire un ambiente potente e open source.

Check Usernames – Controlla l'uso di un marchio o nome utente su 160 Social Network

TinEye – Motore di ricerca di reverse image. È il primo motore di ricerca di immagini sul Web a utilizzare la tecnologia di identificazione delle immagini anziché parole chiave, metadati o filigrane.

Searchcode – Motore di ricerca gratuito di documentazione e

codici sorgente. Gli snippet di codice e i repository open source (software libero) sono indicizzati e ricercabili.

Recorded Future – Soluzione basata sull'intelligenza artificiale per la previsione delle tendenze e l'analisi dei big data. Utilizza vari algoritmi AI e dati strutturati e non strutturati per prevedere il futuro. Gli utenti possono ottenere dati OSINT sulle tendenze passate e sulle tendenze future.

SpiderFoot – Strumento di ricognizione open source disponibile per Linux e Windows. Si integra con una GUI semplice e interattiva con una potente interfaccia a riga di comando.

Wayback Machine – Archivio digitale del World Wide Web e altre informazioni su Internet. Contenente una copia cache della Internet pubblica.

VirusTotal – Sito web che permette l'analisi gratuita di files e/o URLs per scovarne virus o malwares all'interno. Utilizza più di 70 software di antivirus tra cui Kaspersky, Avira, BitDefender, AVG, ESET, G-Data, Comodo, Malwarebytes e McAfee. VirusTotal permette l'invio di files di dimensione massima di 128 MB

GeoTweet – Programma per la ricerca di tweet, tag, hashtag e utenti, con posizioni e mappe

RedditInvestigator – Raccoglie i dati che Reddit rende disponibili e li elabora per ottenere alcune nuove informazioni utili.

Spokeo – Aggregatore di social network che raccoglie e accorpa dati da fonti online e offline. Questi dati aggregati possono contenere dati demografici, proprietà e indici di ricchezza.

theHarvester – Strumento per ottenere email e informazioni relative a domini.

Shodan – Motore di ricerca che fornisce molte informazioni

sulle risorse che sono state connesse alla rete. I dispositivi possono variare da computer, laptop, webcam, segnali stradali e vari dispositivi IOT.

Creepy – Strumento open source che raccoglie informazioni sulla geolocalizzazione utilizzando varie piattaforme di social network e servizi di hosting di immagini che sono già pubblicati altrove.

Social Mention – Piattaforma di ricerca e analisi sui social media che aggrega i contenuti generati dagli utenti provenienti da tutto il mondo in un unico flusso di informazioni.

NameCHK – Applicazione web gratuita che consente di visualizzare la disponibilità di un determinato nome utente.

PasteLert – Sistema semplice per cercare "paste" e impostare avvisi (come gli avvisi di Google) per le voci di pastebin.com.

Whoisology – Un database consultabile con riferimenti incrociati dei record di proprietà dei nomi di dominio correnti e storici.

GlobalFileSearch – Motore di ricerca FTP con ricerca file avanzata su server ftp in tutto il mondo. software gratuito,

OneMillionTweetMap – Strumento di social media che può essere utilizzato per visualizzare tweet e dati aggregati di Twitter in una mappa del mondo.

GitRob – Strumento che aiuta a trovare file potenzialmente sensibili inviati a repository pubblici su Github.

Sublist3r – Strumento Python progettato per enumerare i sottodomini di siti Web utilizzando OSINT.

Knowem – Consente di verificare immediatamente l'uso di un marchio, prodotto, nome personale o nome utente su oltre 500

siti Web di social media popolari ed emergenti.

Tinfoleak – Sito Web in cui è possibile ottenere informazioni dettagliate su un utente di Twitter. Utilizza le informazioni geografiche visualizzate nei tweet e nelle immagini caricate per individuare il luogo in cui si trovava l'utente.

InSpy – Strumento di enumerazione LinkedIn basato su Python

Domain Hunter – Controlla i domini scaduti per la categorizzazione/reputazione e la storia su Archive.org per determinare i candidati idonei per phishing e nomi di dominio C2.

DNS Twist – Generatore di nomi di domini simili a quello che viene inserito, con controllo dell'effettiva registrazione. Utile per rilevare errori di battitura, attacchi di phishing, frodi e spionaggio aziendale.

CignoTrack – Strumento di spionaggio aziendale per testare la privacy e la sicurezza utilizzando OSINT e il social engineering.

UINames – Strumento per generare nomi falsi da utilizzare in progetti e modelli. (incluse imagini da associare alle persone).

Condividi l'articolo

- Analisi forenze, attacchi, capture the flag, Codice Statico, Debugger, Decompiulatore, Hacker etico, Hacking, Osint, reverse engineering, Seganografia, Sergio Caruso

Mosca: i poliziotti vendono l'accesso alle telecamere di controllo

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2019/12/09/la-cassetta-degli-attrezzi-del-bravo-hacker/

Mosca: i poliziotti vendono l’accesso alle telecamere di controllo

Dic 09, 2019 Marco Schiaffino Gestione dati, In evidenza, Leaks, News, RSS, Scenario 0

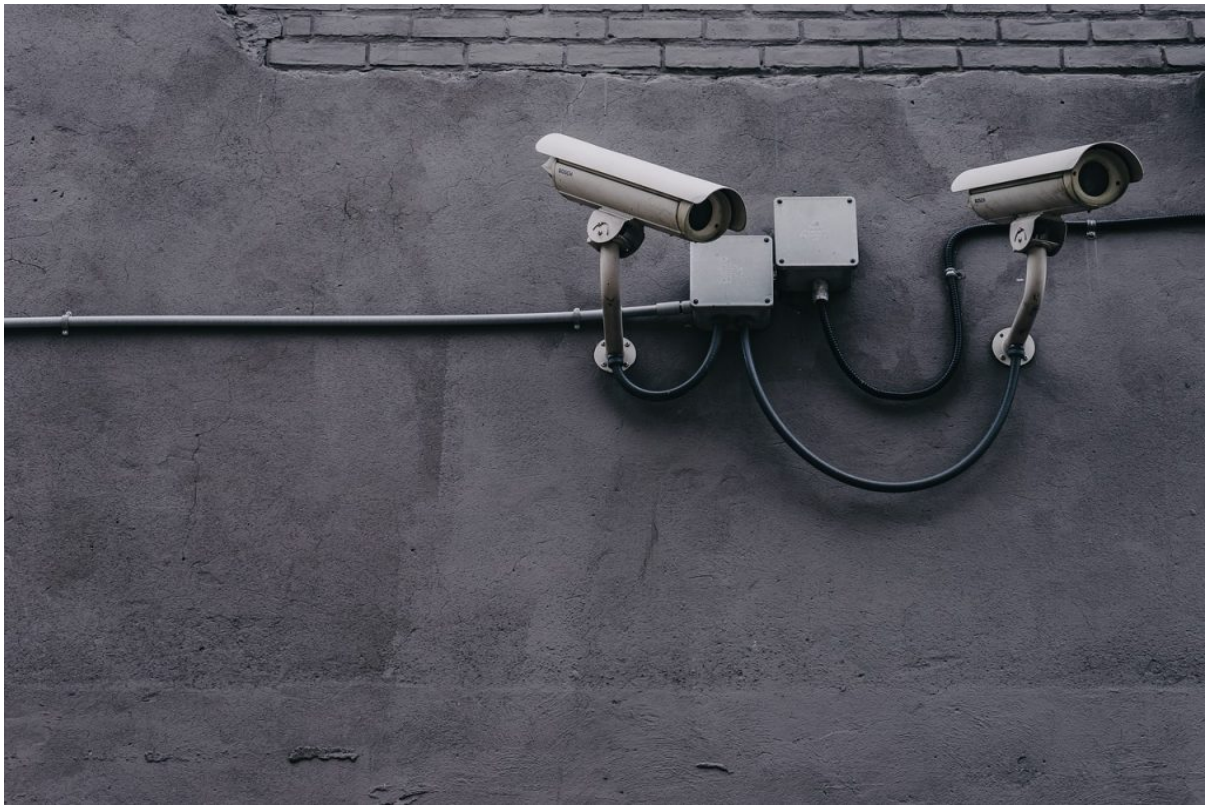
Nei bassifondi del Web è possibile acquistare per pochi spiccioli un accesso alle migliaia di telecamere sparse per la città.

Il problema di privacy legato alla sorveglianza video può assumere diversi aspetti. Mosca, però, sotto questo punto di vista batte veramente tutti. Nella capitale russa esistono decine di migliaia di telecamere come in altre metropoli nel mondo, ma il vero problema è che ad accedervi non sono solo le forze di polizia. **Il sistema è letteralmente aperto a chiunque**.

Secondo quanto riporta **MBKh Media**, infatti, per avere accesso

alle **175.000 telecamere** sparse per la città e alle registrazioni memorizzate basta trovare il giusto forum o partecipare a una chat room dedicata, in cui vengono messi in vendita dei collegamenti "a tempo" al **Centro Integrato per l'Elaborazione e la Conservazione dei Dati (YTKD)**.

Andrey Kaganskikh, autore dell'articolo disponibile qui in lingua russa, lo definisce "il mercato nero della città sicura" e spiega che i collegamenti in vendita al sistema di telecamere a circuito chiuso di Mosca hanno una durata di 5 giorni.



A quanto pare, poi, poliziotti e membri della pubblica amministrazione mettono regolarmente in vendita le loro credenziali di accesso a prezzi che partono dai **470 dollari** (30.000 rubli) che permettono anche di utilizzare **i sistemi di riconoscimento facciale** implementati dal governo russo su alcune delle telecamere.

Insomma: pagando una cifra ridicola chiunque può utilizzare i sistemi di controllo moscoviti per rintracciare chiunque, contando anche sul fatto che il sistema di registrazione

conserva i filmati per 5 giorni (30 giorni per alcuni luoghi considerati particolarmente sensibili) e consente quindi di tracciarne gli spostamenti.

Paradossalmente, secondo quanto emerge dall'inchiesta **i forum in cui avviene la compravendita degli accessi sono addirittura indicizzati da Google** e, di conseguenza, facilmente rintracciabili. Una ciliegina sulla torta che la dice lunga sul livello di tutela della privacy garantito dalle forze di polizia russe.

Condividi l'articolo

La cassetta degli attrezzi del bravo hacker Una vulnerabilità nei sistemi Unix mette a rischio le VPN

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/12/09/mosca-i-poliziotti-si-vendono-gli-account-per-laccesso-alle-telecamere-di-controllo/

Una vulnerabilità nei sistemi Unix mette a rischio le VPN

Dic 06, 2019 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

I ricercatori hanno trovato il modo per analizzare il traffico e "dirottare" la VPN sui sistemi Linux, macOS, iOS e Android.

È possibile violare una **VPN**? Sui sistemi operativi basati su **Unix** parrebbe proprio di sì. A dirlo è un gruppo di ricercatori del team di ricerca **Breakpointing Bad** dell'università del **New Mexico**.

Gli accademici hanno pubblicato un report in cui spiegano che i sistemi Unix soffrono di una vulnerabilità che permette di "sondare" il traffico delle VPN per raccogliere informazioni e, in buona sostanza, dirottare la connessione. La falla di sicurezza (CVE-2019-14899) consente infatti di iniettare del codice a livello TCP.

Per farlo, un pirata informatico deve essere collegato alla stessa rete locale della vittima. L'attacco avviene attraverso l'invio di speciali pacchetti ai sistemi basati su Unix (**Linux, FreeBSD, OpenBSD, macOS, iOS e Android**) e l'analisi delle risposte.



Sulla base di queste, è possibile determinare se l'utente è

connesso a una VPN, individuare l’indirizzo IP virtuale assegnato dal server VPN e (in alcuni casi) l’esatta sequenza dei pacchetti nella connessione. Il team ha sperimentato la tecnica su diverse tecnologie VPN come **OpenVPN**, **WireGuard** e **IKEv2/IPSec** e ha confermato la sua efficacia.

Secondo i ricercatori, la vulnerabilità può essere mitigata introducendo alcuni accorgimenti non tanto a livello dei sistemi operativi interessati, quanto dei server VPN. La tecnica, infatti, è basata principalmente sull’analisi dei pacchetti inviati dalla vittima, un aspetto su cui è più facile intervenire lato server.

Nel loro report iniziale, in ogni caso, spiegano di aver redatto un white paper completo sulla falla di sicurezza che verrà pubblicato, però, **solo quando sarà stata trovata una soluzione per correggere la vulnerabilità**.

Condividi l’articolo

BlackDirect espone alla violazione degli account Microsoft Azure

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/12/06/una-vulnerabilita-nei-sistemi-unix-mette-a-rischio-le-vpn/

BlackDirect espone alla violazione degli account Microsoft Azure

Dic 05, 2019 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

Il sistema di autenticazione usato da Microsoft lascia aperta la strada a un attacco che potrebbe consentire il furto dell'account.

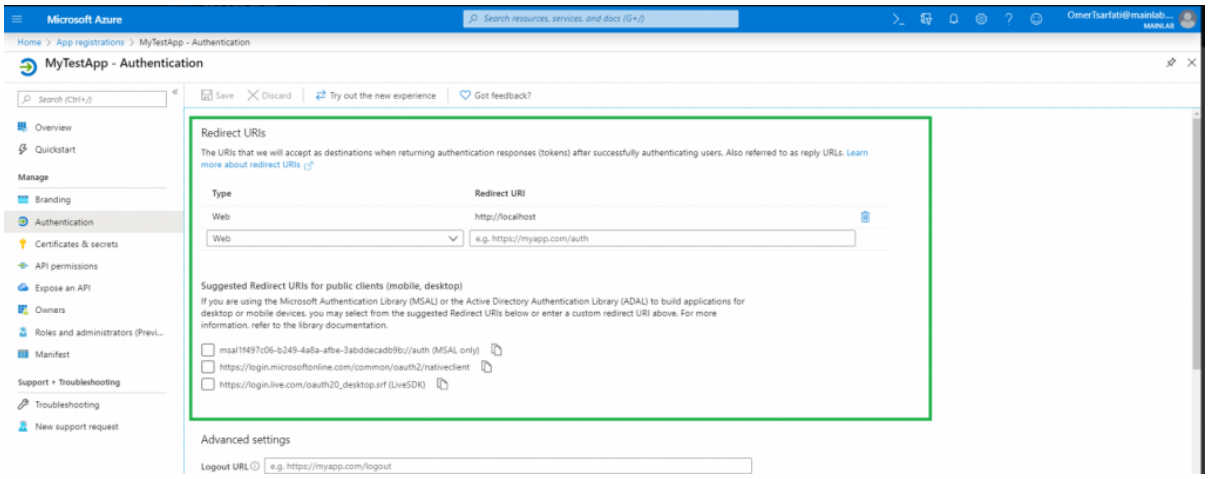
È stata battezzata con il nome i **BlackDirect** ed è una tecnica di attacco che permette di eseguire operazioni con elevati privilegi di amministrazione sugli account **Microsoft Azure**.

A individuare la falla di sicurezza sono stati i ricercatori di **CyberArk**, che ne descrivono i dettagli in un report pubblicato sul sito ufficiale della società di sicurezza.

Ma di cosa si tratta nel dettaglio? Tutto prende le mosse da **OAuth 2**, la nuova versione del sistema di autenticazione utilizzato dai sistemi Microsoft. OAuth, infatti, prevede la possibilità di prevedere una forma di interazione che permette di eseguire l'accesso da un'applicazione di terze parti.

La procedura è gestita attraverso la creazione di un **token** che, in pratica, garantisce l'utilizzo delle funzionalità legate all'account.

Come spiega **Omer Tsarfati**, autore del report,, il sistema in sé è strutturato in maniera solida e quello individuato da CyberArk non è una vulnerabilità di OAuth, quanto un problema legato a un'impostazione "debole" delle procedure che sfruttano il sistema di autenticazione.



Le terze parti autorizzate a eseguire l'accesso attraverso il redirect comprendono infatti URL definite attraverso una white list che elenca i domini e i sottodomini a cui è consentito utilizzare OAuth. Alcuni di questi, fanno notare i ricercatori, non sono registrati da Microsoft e potrebbero, di conseguenza, rappresentare un fattore di rischio.

Se un pirata informatico riuscisse a prenderne il controllo, potrebbe infatti sfruttare il sistema di autenticazione attraverso token per eseguire operazioni come se fosse il legittimo proprietario dell'account.

Per mettere a segno l'attacco, sarebbe sufficiente attirare la vittima sul sito Web attraverso tecniche di social engineering, per esempio attraverso un semplice messaggio di posta elettronica.

Il problema è che ci sono almeno tre applicazioni Microsoft che prevedono, all'interno della lista, una serie di domini che i ricercatori considerano "a rischio". Si tratta di **Portfolios**, **O365 Secure Score** e **Microsoft Service Trust**. In seguito alla segnalazione di CyberArk, Microsoft ha corretto il problema.

Per quanto riguarda invece altre applicazioni, è possibile eseguire un controllo attraverso uno strumento sviluppato dalla stessa società di sicurezza e che può essere utilizzato gratuitamente attraverso la pagina Web dedicata

https://black.direct/.

Condividi l’articolo

Hacker tentano un attacco 51% contro Vertcoin, ma ci perdono soldi

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/12/05/blackdirect-espone-alla-violazione-degli-account-microsoft-azure/

Hacker tentano un attacco 51% contro Vertcoin, ma ci perdono soldi

Dic 04, 2019 Marco Schiaffino Attacchi, In evidenza, News, RSS 0

I pirati informatici hanno cercato di portare un attacco “double spending” alterando la blockchain della cripto-valuta. Il fallimento gli è costato 4.000 dollari.

Per i pirati informatici, Bitcoin e cripto-valute in generale

non sono solo uno strumento. Spesso possono essere un bersaglio. La cronaca recente, infatti, ha registrato decine di attacchi (riusciti e falliti) nei confronti degli exchange che si occupano di compravendita di cripto-monete.

Di solito si tratta di classici attacchi che puntano a infiltrare i sistemi per ottenerne il controllo. **Più raramente si verificano attacchi che prendono di mira direttamente la struttura delle cripto-valute, puntando per esempio a "inquinare" la blockchain**.

Nel caso dell'attacco a **Vertcoin (VTC)**, però, i pirati informatici hanno fallito e secondo gli operatori di **Bittrex** il loro tentativo di attacco gli sarebbe costato almeno 4.000 dollari.

Com'è possibile? Presto detto: l'attacco tentato ai danni di Bittrex (l'exchange che tratta prioritariamente Vertcoin) è del tipo "51%", una modalità di attacco che punta ad alterare la blockchain per consentire ai pirati di usare due volte la stessa cripto-valuta.

La tecnica (per i curiosi c'è una spiegazione più dettagliata consultabile su questa pagina Web) fa leva sul principio di "democrazia" che ispira i sistemi di blockchain, per cui la veridicità dei dati è affidata alla maggioranza.

Semplificando il concetto, il sistema considera affidabile la blockchain più lunga, partendo dal presupposto che sia quella a cui ha contribuito il maggior numero di persone. Se i cyber-

criminali riescono in questo intento, possono cancellare l’acquisto che hanno fatto e, in pratica, usare due volte la stessa cripto-valuta.

Inquinare la blockchain, però, non è facile. I pirati devono infatti immettere nel circuito una sua versione che sembri più completa di quella originale e, per farlo, devono riuscire a elaborare i blocchi più velocemente del resto del circuito.

Ed è qui che vanno incontro a dei costi. Secondo quanto ha scritto in un report **James Lovejoy**, che si occupa della manutenzione di Vertcoin, gli autori dell’attacco avrebbero “affittato” della potenza di calcolo tramite **Nicehash** spendendo tra 0,5 e 1 Bitcoin.

Quando i gestori di Bittrex hanno bloccato i wallet sospetti, infatti, i pirati erano riusciti a raggranellare solo 13.825 VTC, corrispondenti a circa 0,44 BTC. Insomma: facendo i conti, nell’operazione avrebbero perso tra i 400 e i 4.000 dollari.

Condividi l’articolo

Emergenza StrandHogg: il nuovo exploit per Android già usato dai pirati

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/12/04/hacker-tentano-un-attacco-51-contro-vertcoin-ma-ci-perdono-soldi/

Emergenza StrandHogg: il nuovo exploit per Android già usato dai pirati

Dic 03, 2019 Marco Schiaffino Attacchi, Emergenze, Hacking, In evidenza, Malware, News, RSS 0

Sfrutta una falla del sistema Google e permette di violare qualsiasi app senza nemmeno eseguire il root del telefono.

Una vulnerabilità devastante, che i pirati informatici stanno già sfruttando attivamente per colpire gli utenti Android. SI chiama **StrandHogg** ed è stata individuata dai ricercatori di **Promon**.

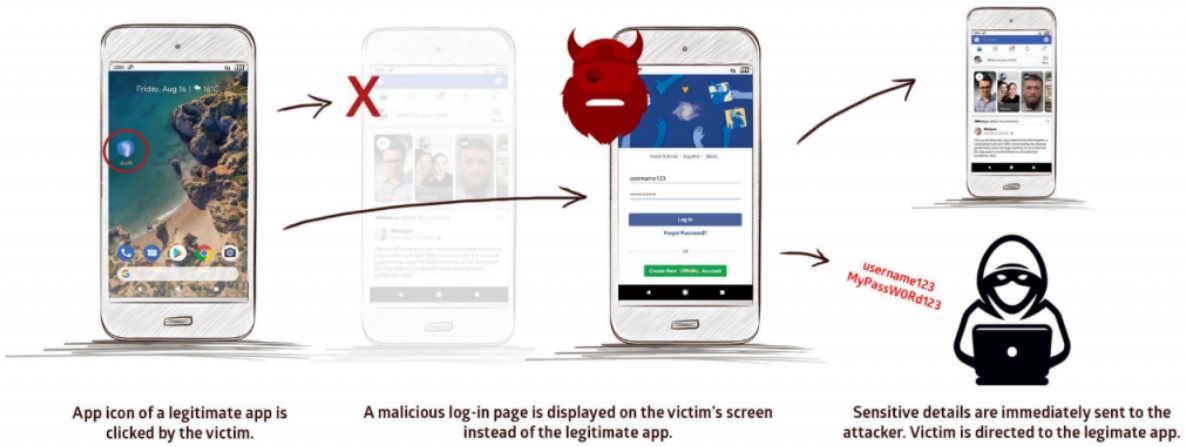
Come si legge nel report pubblicato dalla società di sicurezza, StrandHogg fa leva su una falla di sicurezza nel sistema multitasking del sistema operativo di **Google** e consente a un malware di compiere una serie pressoché infinita di attività malevole **senza che sia necessario nemmeno eseguire il root del telefono**.

Nel dettaglio, la tecnica sfrutta il comando **taskAffinity**, che permette di "impersonare" qualsiasi applicazione su Android. Come spiegano i ricercatori, questo consente di mettere a punto malware che sono in grado di **rubare qualsiasi tipo di informazione o indurre la vittima a concedere permessi estremamente ampi**, con conseguenze facilmente immaginabili.

[embedded content]

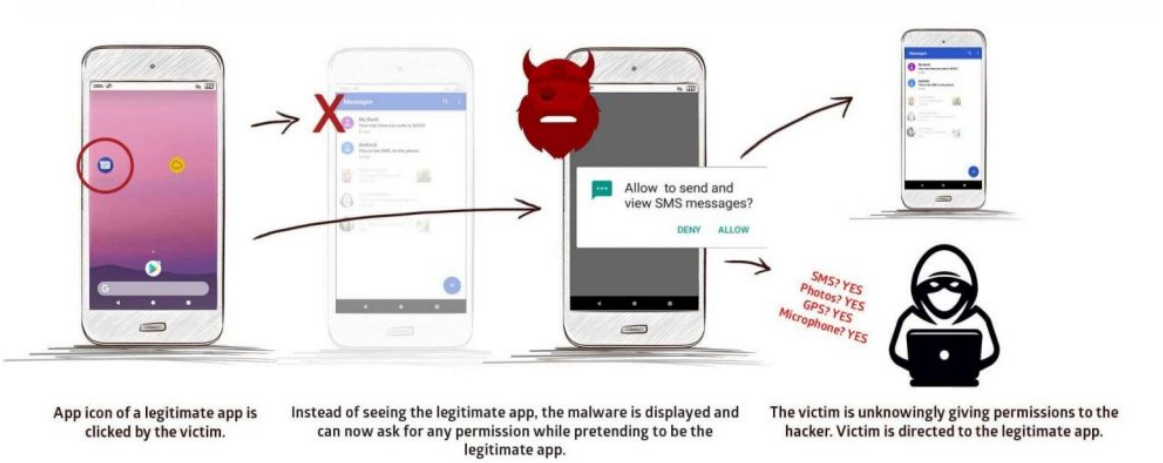
Ma come funziona nella pratica? Quando l'utilizzatore dello smartphone esegue un'applicazione legittima, il malware è in grado di visualizzare una schermata del tutto identica a quella dell'app originale. Qualsiasi comando inviato in quella schermata, però, farà riferimento all'applicazione malevola.

I possibili utilizzi hanno come unico limite la fantasia dei cyber-criminali. È possibile per esempio sfruttarla per visualizzare una schermata di login che permetterebbe ai pirati informatici di **ottenere facilmente le credenziali di accesso a qualsiasi servizio, compresi i codici utilizzati per l'autenticazione a due fattori**.



C'è di peggio: agendo sul sistema dei permessi, il malware potrebbe garantirsi una libertà d'azione senza precedenti. Tutto quello che deve fare è richiedere quello che gli serve quando l'utente avvia un'applicazione di cui si fida. **La vittima penserà di aver fornito il permesso all'app che aveva attivato, mentre in realtà il permesso viene assegnato a quella infetta**.

In questo modo, un malware che sfrutta StrandHogg può per esempio ottenere l'accesso alle funzioni per l'invio di SMS a pagamento, o alla fotocamera e al microfono per spiare la vittima.



Per gli utenti, accorgersi che c'è qualcosa di strano è estremamente difficile. Gli unici indizi potrebbero essere la richiesta di login che di solito non compaiono o richieste di permessi incongruenti con le funzionalità di un'app. Se i pirati pianificano bene il funzionamento del malware, però, è probabile che le vittime non notino nulla di strano.

Secondo quanto riportano i ricercatori di Promon, la tecnica funzionerebbe con tutte le app per Android più popolari. Per la precisione, i tecnici avrebbero testato StrandHogg con le 500 applicazioni più scaricate da **Google Play**. Peggio ancora, gli stessi analisti avrebbero individuato almeno **36 applicazioni malevole** che utilizzano questa tecnica.

Condividi l'articolo

Database di TrueDialog espone milioni di SMS. E non solo…

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/12/03/emergenza-strandhogg-il-nuovo-exploit-per-android-viene-gia-usato-dai-pirati/

Database di TrueDialog espone milioni di SMS. E non solo…

Dic 02, 2019 Marco Schiaffino Gestione dati, In evidenza, Leaks, News, RSS 0

Il server "dimenticato" online con dati sensibili conservati in chiaro e senza alcuna protezione. Ben 604 gigabyte di dati accessibili a chiunque.

Questa volta il potenziale leak di dati non riguarda dati medici o elenchi di utenti, ma milioni di SMS "dimenticati", come al solito, su un server cloud aperto a chiunque.

A scovarli sono stati i ricercatori di **vpnMentor**, che lo scorso 26 novembre hanno individuato il database su un server della piattaforma **Microsoft Azure**.

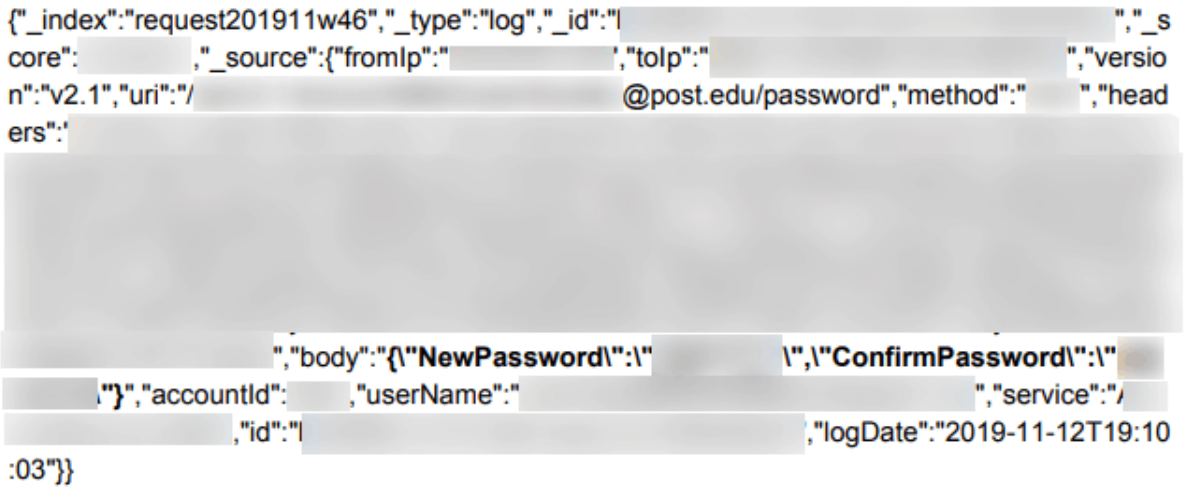
Come spiegano gli stessi esperti di sicurezza in un report pubblicato sul blog dell'azienda, il server è collegato a **TrueDialog**, una società specializzata in comunicazione operante negli Stati Uniti con sede in Texas. L'azienda, nel dettaglio, si occupa di campagne di marketing e comunicazione attraverso l'uso di SMS.

A livello globale, TrueDialog collabora con più di 900 operatori telefonici e ha un bacino di circa 5 miliardi di sottoscrizioni. Insomma: non stiamo parlando propriamente di una "startup", ma di un vero colosso del settore.



Stando a quanto scrivono gli autori del report, TrueDialog ha dimostrato un'ottima reattività nel rispondere alla segnalazione, riuscendo a "tappare" la falla nel giro di 24 ore. **Se sotto questo profilo l'azienda merita un 10 e lode, le cose cambiano decisamente per quanto riguarda le sue policy nella gestione dei dati personali**.

I 604 GB di dati, infatti, contenevano oltre 1 miliardo di record tra cui dati anagrafici, numeri di telefono, indirizzi di posta elettronica e **password memorizzate in chiaro**. Le uniche password protette in qualche modo erano inoltre codificate in base64 e, di conseguenza, facilmente decrittabili.



L'impatto del leak è amplificato dal fatto che una buona parte dei dati contenuti riguardano i clienti di TrueDialog (quindi altre aziende) che a questo punto sono esposte al rischio che qualcuno utilizzi le informazioni per scopi fraudolenti.

Non solo: secondo i ricercatori di vpnMentor il database conteneva anche i log con gli errori registrati nei sistemi interni, che potrebbero essere utilizzati da un pirata

informatico come materiale di “intelligence” per pianificare un attacco ai sistemi della stessa TrueDialog.

Condividi l’articolo

RevengeHotels: attacchi mirati agli alberghi colpiscono anche l’Italia

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/12/02/database-di-truedialog-espone-milioni-di-sms-e-non-solo/

RevengeHotels: attacchi mirati agli alberghi colpiscono anche l’Italia

Nov 29, 2019 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS 0

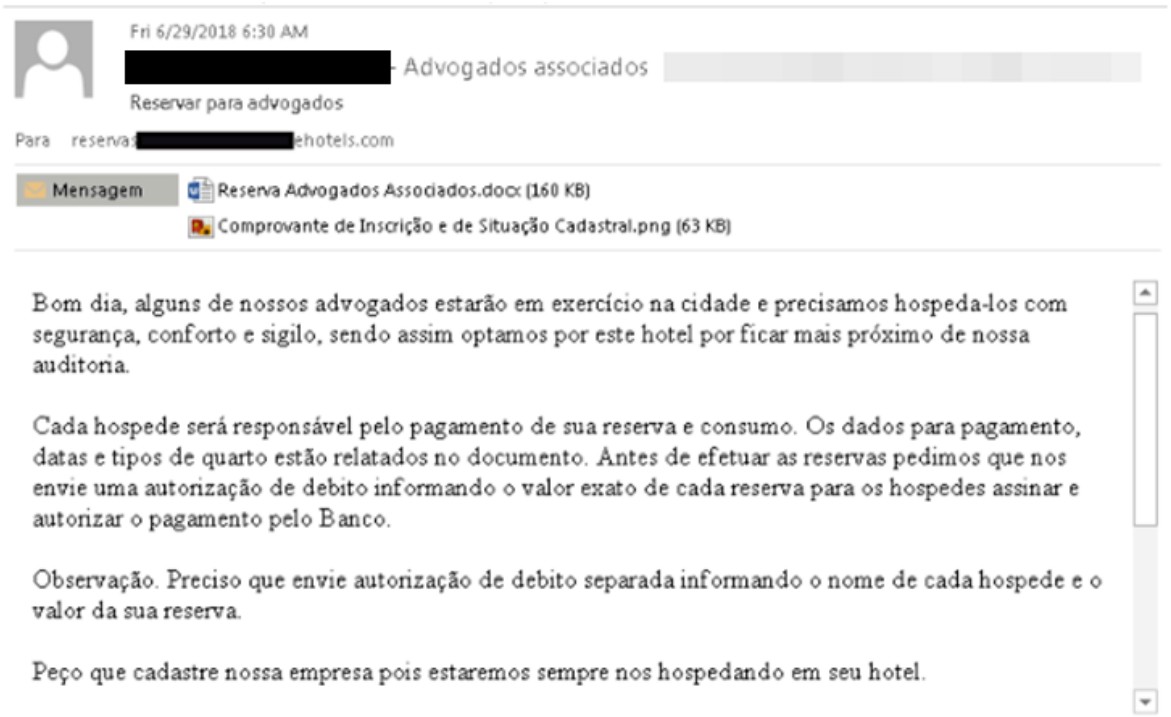
I pirati informatici utilizzano email di phishing per compromettere i sistemi delle strutture alberghiere e rubare i dati delle carte di credito dei clienti.

Hotel, alberghi e bed and breakfast sembrano essere diventati

un obiettivo privilegiato per i cyber-criminali. A confermarlo è un rapporto di **Kaspersky** che accende i riflettori su una campagna di pirateria informatica battezzata **RevengeHotels**.

Gli attacchi, spiegano i ricercatori della società di sicurezza, avvengono attraverso email di phishing che i pirati realizzano con estrema cura, cercando di impersonare aziende e partner commerciali che hanno rapporti con la vittima.

Allegato al messaggio, di solito, c'è un allegato che contiene i trojan utilizzati per infiltrare i sistemi della struttura alberghiera. I formati preferiti sono quelli **Office** e, in particolare, i ricercatori hanno individuato l'utilizzo di file che sfruttano una vulnerabilità (CVE-2017-0199) conosciuta fin dal 2017.

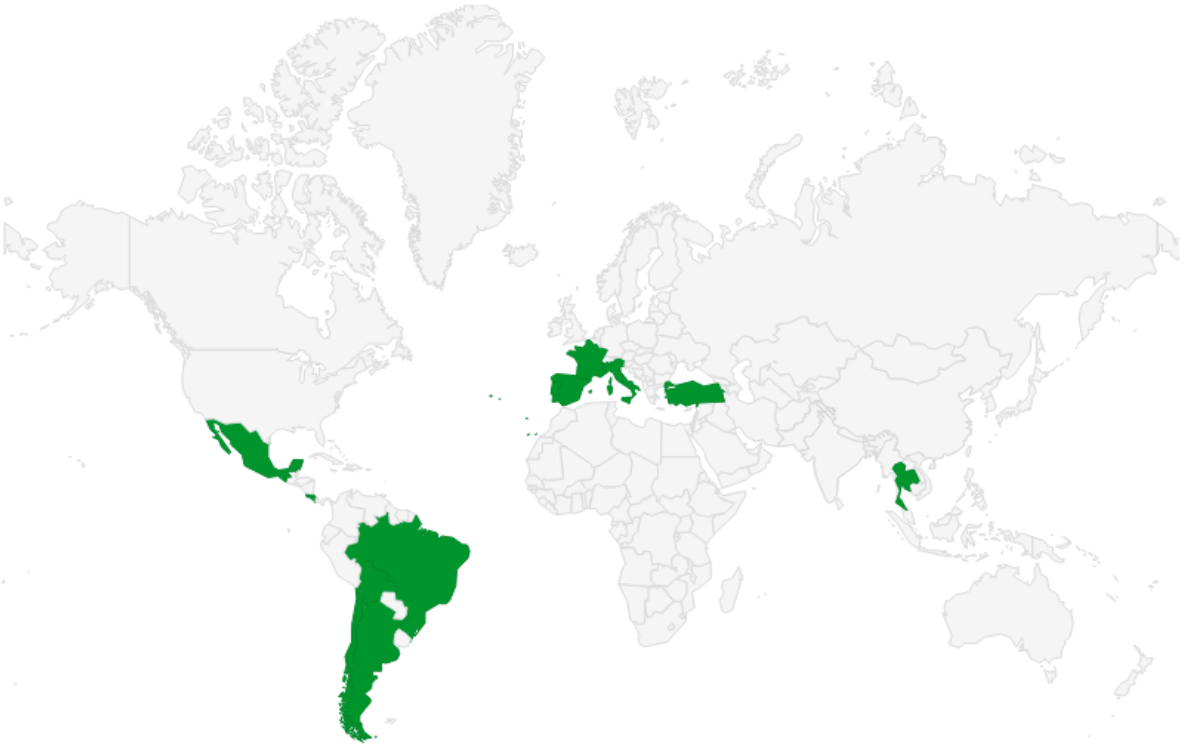


I malware utilizzati sono tutti conosciuti e, probabilmente, acquistati dai pirati informatici sul mercato nero. Tra questi ci sono **RevengeRAT**, **NjRAT**, **NanoCoreRAT** e **ProCC**. I cyber-criminali, però, utilizzerebbero anche un modulo "fatto in casa" chiamato **ScreenBooking**.

Insomma: il modus operandi non è nulla di particolarmente

originale e l’uso di vulnerabilità conosciute conferma ancora una volta il problema relativo al livello di sicurezza dei sistemi informatici utilizzati nel settore turistico.

Il gruppo, attivo in Argentina, Bolivia, Cile, Costa Rica, Francia, **Italia**, Messico, Portogallo, Spagna, Tailandia e Turchia è interessato principalmente ai dati delle carte di credito dei clienti degli alberghi, ma utilizza anche tecniche che gli permettono di accedere ai dati di pagamento comunicati attraverso le piattaforme di prenotazione online, come **Booking.com**.



In alcuni casi, spiegano i ricercatori, l’accesso tramite trojan ai sistemi degli alberghi vengono addirittura venduti attraverso la formula del “malware as a service”. **In pratica, chiunque può “affittare” una backdoor che gli consente di accedere ai dati registrati**.

Tra i suggerimenti che gli esperti di Kaspersky rivolgono ai turisti per evitare di finire vittima di attacchi simili c’è anche quello di usare per i pagamenti wallet virtuali come **Apple Pay** o **Google Pay**.

Condividi l’articolo

Google: in 3 mesi dodicimila attacchi a Gmail da “hacker di stato”

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/11/29/revengehotels-attacchi-mirati-agli-alberghi-colpiscono-anche-litalia/

Google: in 3 mesi dodicimila attacchi a Gmail da “hacker di stato”

Nov 28, 2019 Marco Schiaffino Attacchi, In evidenza, News, Phishing, Prodotto, RSS, Scenario, Tecnologia 0

I dati dell’azienda statunitense fotografano un’impressionante numero di attacchi mirati. Protagonisti i pirati informatici al soldo dei servizi segreti.

Se c’è una cosa che **Google** cura con molta attenzione (a volte addirittura esagerando) è la sicurezza degli account **Gmail**. L’azienda di Mountain View, nel corso del tempo, ha messo a

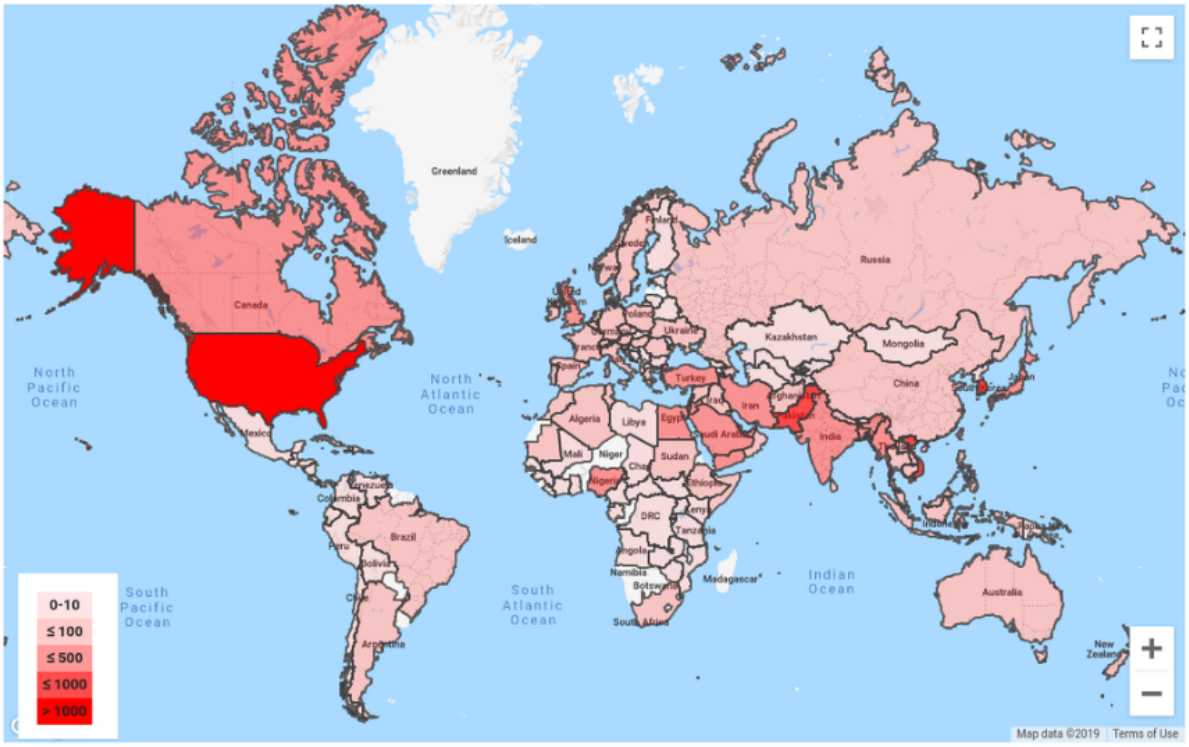
punto un sistema puntuale di notifiche per avvisare i suoi iscritti quando individua attività sospette che hanno a che fare con gli account Gmail.

Tra queste, però, ce n'è una molto specifica. Si tratta di un sistema di notifica che avvisa gli utenti Gmail quando il loro account viene preso di mira da un attacco che rientra nella categoria del "hacking di stato".

Stiamo parlando di quella sorta di élite composta dai cosiddetti **APT (Advanced Persistent Threat)** che agiscono per conto di governi e servizi segreti portando attacchi a bersagli selezionati, solitamente attraverso tecniche si spear phishing.

La funzionalità di Gmail, introdotta nel 2012, è stata progressivamente ampliata e, dal 2018, copre anche gli account forniti attraverso **G Suite**.

In un comunicato stampa pubblicato sul suo blog ufficiale, Google svela adesso che nel trimestre compreso tra luglio e settembre 2019 ha individuato la bellezza di **12.000 attacchi** di questo tipo rivolti ad account Gmail, con picchi a livello geografico negli **Stati Uniti** e in **Pakistan**.



A prima vista il numero può sembrare modesto, ma non è così. Se nel settore della sicurezza informatica siamo abituati a cifre da capogiro, con statistiche che parlano di milioni di attacchi al giorno, la statistica fornita da Google offre uno spaccato preoccupante.

In questo caso, infatti, non stiamo parlando di attacchi "a tappeto" che colpiscono gli utenti casualmente. **Si tratta invece di tentativi di compromissione attentamente pianificati e studiati, che non si esauriscono di certo in un singolo episodio**.

Per dirlo con altre parole significa che gli hacker di stato, nel corso di soli tre mesi, hanno avviato 12.000 operazioni di spionaggio che hanno preso di mira dei bersagli specifici. Gli attacchi rilevati da Google, quindi, sono probabilmente soltanto un tentativo all'interno di una strategia più ampia e persistente di colpire quei bersagli.

Se poi consideriamo che il dato riguarda solo gli account Gmail (anche aziendali) ma non comprende le potenziali vittime che usano una casella di posta di un altro fornitore di servizi, possiamo ipotizzare che la portata del fenomeno sia

ben più ampia. Insomma: il pericolo APT è sempre più rilevante e, soprattutto per le aziende, rappresenta un rischio concreto e reale.

Condividi l’articolo

Due SDK registrano informazioni di utenti Facebook e Twitter

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/11/28/google-in-3-mesi-dodicimila-attacchi-a-gmail-da-hacker-di-stato/

Due SDK registrano informazioni di utenti Facebook e Twitter

Nov 27, 2019 Marco Schiaffino In evidenza, News, Privacy, RSS, Vulnerabilità 0

I kit di sviluppo permetterebbero di creare app che raccolgono informazioni sugli utenti quando eseguono il login utilizzando le credenziali dei social network.

L’ennesimo epic fail in tema di privacy sui social network

coinvolge le applicazioni mobile (**Android** e **iOS**) sviluppate utilizzando due particolari **SDK (Software Development Kit)** di terze parti.

A denunciarlo sono **Facebook** e **Twitter**, che hanno segnalato la presenza di funzionalità che violerebbero le condizioni d'uso dei rispettivi social network, consentendo in buona sostanza agli sviluppatori di raccogliere informazioni a cui no dovrebbero avere accesso.

I Software Development Kit sono "pacchetti" di sviluppo che i programmatori utilizzano per creare le loro applicazioni sfruttando parti di codice e funzionalità già pronte per l'uso. Tra queste, ad esempio, i sistemi che permettono di impostare il login all'app utilizzando le credenziali di Facebook o Twitter. Il sistema, in teoria, non dovrebbe però consentire all'app di accedere ad alcuna informazione sull'account.



A quanto pare, però, gli SDK commercializzati da **OneAudience** e

MobiBurn lascerebbero un varco che consente agli sviluppatori di raccogliere informazioni come email, account e nome degli iscritti. Nel caso di Twitter, poi, la falla permetterebbe anche di registrare l'ultimo tweet pubblicato. **Tutto senza alcuna notifica e, di conseguenza, senza alcuna autorizzazione da parte dell'utente**.

A quanto pare, le violazioni registrate riguarderebbero soltanto i dispositivi Android, ma

La risposta delle due società non si è fatta attendere ed è arrivata attraverso dei comunicati in cui, in buona sostanza, **le aziende scaricano la responsabilità sui singoli sviluppatori**. La loro tesi, in pratica, è di non aver mai utilizzato la funzione per raccogliere dati sensibili degli utenti Facebook e Twitter. Se questo è accaduto, è solo perché qualche sviluppatore ha abusato delle funzioni messe a disposizione dal loro SDK.

Una ricostruzione tutto sommato plausibile, che lascia aperta però la questione del controllo dei dati condivisi attraverso i sistemi di accesso "delegati" ai social network, che troppo spesso aprono la strada ad abusi e cortocircuiti di ogni genere.

Condividi l'articolo

Notifiche pericolose sui siti Web

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/11/27/due-sdk-registrano-informazioni-di-utenti-facebook-e-twitter/