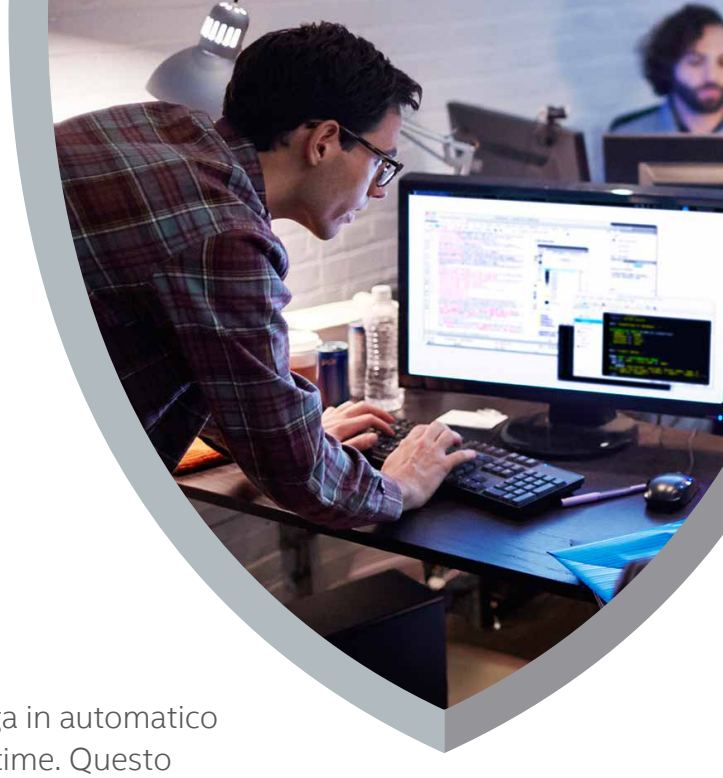
Panoramica sulla soluzione



Proteggersi da Pinkslipbot

W32/Pinkslipbot è una famiglia di malware che si propaga in automatico creata per sottrarre dati personali e finanziari alle sue vittime. Questo malware permette il controllo completo dei sistemi infetti tramite una backdoor basata su comandi e azionata dal server di controllo, oltre che attraverso una backdoor basata sul network computing virtuale. Tramite le condivisioni di rete Pinkslipbot può inoltre diffondersi ad altri sistemi nell'ambiente e può comunicare con il proprio server di controllo per scaricare le versioni aggiornate di se stesso.

Pinkslipbot è stato identificato inizialmente nel 2007, ma il gruppo che l'ha creato ha mantenuto il codice aggiungendo degli aggiornamenti incrementali prima di rilasciare una nuova versione ogni pochi mesi.

I dati sottratti da Pinkslipbot consentono all'autore dell'attacco di determinare posizione geografica, azienda e titolare del sistema infettato. L'aggressore può poi vendere queste informazioni (soprattutto se provengono da un'azienda di rilievo) a una terza parte e, dopo il pagamento, distribuire il malware mirato nel sistema compromesso.

Per un approfondimento tecnico su Pinkslipbot, consulta il *Report McAfee Labs sulle minacce: giugno 2016*. Il report spiega il processo iniziale dell'infezione, i meccanismi di propagazione, i dati tecnici e i generali metodi di protezione.

Policy e procedure per proteggersi da Pinkslipbot

Ecco alcune policy e procedure generali che ti aiuteranno a proteggerti da Pinkslipbot.

Per proteggere il perimetro bisogna bloccare le porte inutilizzate in tutti i punti di uscita dalla rete e le richieste di connessione da e verso gli indirizzi IP notoriamente associati al malware. Interrompendo l'uso delle condivisioni di rete si ferma il movimento laterale di Pinkslipbot. Nella maggior parte degli ambienti si deve anche disattivare la funzionalità AutoRun di Microsoft Windows. È fondamentale aggiornare i sistemi operativi e le applicazioni Windows agli ultimi livelli di patch, oltre che il software antimalware all'ultima versione.

I sistemi privi di patch consentono lo sfruttamento delle vulnerabilità. Per ogni ambiente è indispensabile una corretta gestione delle patch. Quando vengono emesse delle patch, queste vanno immediatamente testate, verificate e implementate. Quando l'applicazione delle patch non è possibile a causa di dipendenze da una vecchia versione, dev'essere presente un altro meccanismo per mitigare lo sfruttamento delle vulnerabilità note. Una gestione aggressiva delle patch è uno dei metodi più efficaci per mitigare gli effetti di Pinkslipbot e degli altri malware.

intel Security

Panoramica sulla soluzione

Anche se Pinkslipbot viene inviato principalmente tramite i download guidati dai siti web compromessi dai kit di exploit, le vittime vengono solitamente dirette a tali siti dalle email di phishing. Contrassegnando le email come “interne” o “esterne”, gli utenti hanno maggiori probabilità di identificare le email falsificate o di phishing e di trattenersi dal fare clic sui collegamenti sconosciuti e pericolosi.

Pinkslipbot si esegue parzialmente in memoria, pertanto l’applicazione delle patch ai sistemi, le scansioni complete e l’utilizzo di uno strumento di rimozione del malware non sono sufficienti. Per rimuovere il malware dalla memoria dei sistemi infetti occorre il riavvio e poi una nuova scansione per assicurare che il sistema sia pulito. Per bloccare gli attacchi dictionary consigliamo l’uso di password sicure, la disattivazione dell’esecuzione automatica e la messa in pratica del principio del “minimo privilegio”.

Pinkslipbot è un evoluzione aggressiva del famigerato trojan Zeus. Una password elementare per accedere a un sistema Windows è sufficiente per venire infettati da Pinkslipbot, anche senza l’esposizione a un kit di exploit o l’interazione dell’utente. Quando un sistema è stato infettato, qualsiasi attività eseguita nel sistema viene registrata e inviata all’autore dell'attacco. Dato che in Pinkslipbot sono state introdotte comunicazioni sicure e personalizzate con i propri server di controllo, il rilevamento e l’analisi sta diventando sempre più difficile. La sua storia suggerisce che diventerà sempre più pericoloso alla riuscita di ogni iterazione. Comprendendo il tuo ambiente e mettendo in pratica le policy e procedure consigliate, puoi ridurre al minimo i danni che Pinkslipbot può causare.

Cosa può fare la tecnologia di Intel Security per proteggerti da Pinkslipbot

McAfee VirusScan Enterprise (VSE) e McAfee Endpoint Security (ENS) 10

McAfee VirusScan Enterprise e McAfee Endpoint Security 10 offrono un’avanzata protezione antimalware per i sistemi endpoint. McAfee VirusScan Enterprise è stato superato da McAfee Endpoint Security 10, che ha prestazioni più veloci su una piattaforma ottimizzata. I DAT Intel Security per McAfee VirusScan Enterprise e McAfee Endpoint Security 10 contengono funzioni di rilevamento e rimozione dei componenti di Pinkslipbot. McAfee VirusScan Enterprise e McAfee Endpoint Security 10 proteggono su numerosi livelli tramite rilevamento in memoria, antirootkit e meccanismi comportamentali e statici. Per aggiungere livelli di protezione contro le nuove varianti, puoi applicare le regole di protezione dell'accesso e impedire a Pinkslipbot di infettare i sistemi.

- Crea e testa una regola di protezione dell'accesso per prevenire l’esecuzione di qualsiasi processo e la creazione di qualsiasi file eseguibile in C:\Users*\AppData\Roaming\Microsoft**.exe.
- Crea e testa una regola di protezione dell'accesso per impedire ai processi cscrpit.exe e wscript.exe di leggere, eseguire e creare i file WPL nella cartella %LOCALAPPDATA%\Microsoft\. Il blocco di questi file, solitamente in JavaScript, impedisce al malware di scaricare le nuove versioni.
- Crea e testa una regola di protezione dell'accesso per impedire ai processi cscrpit.exe e wscript.exe di leggere ed eseguire i file nella cartella %UserProfile%, dove fattibile.
- Crea e testa una regola di protezione dell'accesso per impedire a “updates_*new.cb”, “upd_*.cb” e “updates*_new.cb” di eseguire e creare dei nuovi file. Questi sono solitamente utilizzati dai file di configurazione di Pinkslipbot e il blocco di tali file può impedire al malware di aggiornarsi.
- Crea e testa una regola di protezione dell'accesso per le porte da 65200 a 65400 relativa ai processi iexplorer.exe ed explorer.exe. Dato che Pinkslipbot si inietta in questi processi, impedendo loro l’utilizzo delle porte si impedisce a Pinkslipbot di comunicare con il proprio server di controllo.
- Implementa e testa le regole di protezione dell'accesso per impedire l’esecuzione remota dei file autorun.inf.

Panoramica sulla soluzione

McAfee Host Intrusion Prevention (HIPS)
McAfee Host Intrusion Prevention protegge i sistemi dalle minacce zero-day combinando un sistema di prevenzione delle intrusioni basato su firme e comportamenti con un firewall stateful e dinamico. Gli aggiornamenti pianificati dei contenuti proteggono i sistemi dalle vulnerabilità di applicazioni e sistemi operativi anche prima che siano disponibili le patch. Rinforza la sicurezza di un ambiente consentendo alle firme di bloccare molti dei metodi comunemente usati dal malware per introdursi nei software più diffusi.

- Testa e attiva la firma McAfee HIPS 6010 (Protezione generica dall'hooking delle applicazioni).
- Testa e attiva la firma McAfee HIPS 6011 (Protezione generica dal richiamo delle applicazioni).
- Isola i sistemi infettati da Pinkslipbot assegnando loro una policy in cui la regola del firewall blocca tutte le porte eccetto quelle di amministrazione.

McAfee Endpoint Security 10 e McAfee Host Intrusion Prevention sono inclusi in McAfee Complete Endpoint Protection.

McAfee Web Gateway (MWG)
I download guidati e i collegamenti contenuti nelle email sono i modi più comuni usati da Pinkslipbot per diffondersi. McAfee Web Gateway offre una sicurezza web ad alte prestazioni, proteggendo i sistemi dai siti web pericolosi. La si può distribuire come appliance hardware dedicata o come immagine in un computer virtuale.

- Configura McAfee Web Gateway per il filtraggio antispam.
  - Il filtraggio antispam protegge contro:
    - IP nocivi
    - URL pericolosi
    - Email di spam.
- Attiva l'ispezione GAM.
- Attiva McAfee GTI per la reputazione di URL e file.
- Si integra con McAfee Advanced Threat Defense per l'analisi nella sandbox e il rilevamento delle minacce zero-day.

McAfee Active Response (MAR)
McAfee Active Response offre rilevamento e risposta continui per i sistemi presi di mira dalle minacce avanzate come Pinkslipbot. Il monitoraggio automatizzato degli eventi ti consente di trovare gli indicatori di compromissione, che segnalano l'infezione del malware.

- La presenza dei seguenti domini in una cache DNS può indicare un'infezione da parte di Pinkslipbot:
  - gpfbvtuz.org
  - hsdmoyrkeqpcyrtw.biz
  - lgzmtkvnijeaj.biz
  - mfrlilcumtwieyzbfdmpdd.biz
  - hogfpicpoxnp.org
  - qrogmwmahgcwil.com
  - enwgzzthfwhdm.org

  - vksslxpxaoql.com
  - dxmhcvxcmdewthfbnaspnu.org
  - mwtfngzkadeviqtlfrrio.org
  - jynsrklhmaqirhjrtygjx.biz
  - uuwgdehizcuuucast.com
  - gyvwkxfxqdargdooqql.net
  - xwcjchzq.com
  - tqxllcfn.com
  - feqsrxswnumbkh.com
  - nykhliicqv.org
  - ivalhlotxdyvzyxrb.net
  - bbxrsgsuwksogpktqydlkh.net
  - rudjqypvucwwpfejdxqsv.org
- Per determinare se i sistemi hanno comunicato con uno qualsiasi dei domini di Pinkslipbot sopra elencati eseguire la seguente interrogazione della cache DNS:
  - DNSCache where DNSCache hostname equals “[Dominio di Pinkslipbot]”
- Questa interrogazione restituisce l’elenco delle comunicazioni stabilite dai sistemi dell’ambiente con i domini di Pinkslipbot. Puoi facilmente individuare quali sono i sistemi in comunicazione con questi domini facendo clic su una voce e visualizzando i sistemi correlati.
- Usare un firewall locale come McAfee ENS 10 o McAfee HIPS per mettere in quarantena i sistemi colpiti da Pinkslipbot. Per mettere in quarantena un sistema, in McAfee ePO assegna una policy firewall di blocco al sistema stesso.
- Eseguire una scansione completa su richiesta con McAfee ENS 10 o McAfee VSE assegnando al sistema un’attività di scansione su richiesta da eseguire immediatamente in McAfee ePO. Attiva l’agente per avviare la scansione.

Ulteriori letture

Avviso sulle minacce McAfee Labs: W32/Pinkslipbot
Questo avviso fornisce una dettagliata analisi tecnica di Pinkslipbot.

Serie di webinar di Intel Security sul malware: Pinkslipbot
Questo video fornisce una panoramica di Pinkslipbot, le cifre a livello regionale e di settore, caratteristiche e sintomi, oltre alle raccomandazioni per la prevenzione.

McAfee. Part of Intel Security.
Via Fantoli, 7
20138 Milano
Italia
(+39) 02 554171
www.intelsecurity.com