17/01/2022

cybersecurity360.it

Argomento: Exprivia: si parla di noi

EAV: € 1.497
Utenti unici: 28.467

https://www.cybersecurity360.it/nuove-minacce/sysjoker-il-malware-che-spia-gli-utenti-windows-macos-e-linux-come-difendersi/

SysJoker, il malware che spia gli utenti Windows, macOS e Linux: come difendersi

Gli utenti di Windows, Linux e macOS sono nel mirino di SysJoker: il malware multipiattaforma è attivo dalla seconda metà dell'anno scorso e sfrutta una backdoor per stabilire l'accesso iniziale sulla macchina target. Ecco tutti i dettagli e come difendersi È stato scoperto un nuovo malware multi-piattaforma basato su C++ e ribattezzato SysJoker che sta prendendo di mira Windows, Linux e macOS con la capacità di eludere i sistemi di rilevamento su tutti e tre i sistemi operativi.La campagna di cyber spionaggio risale alla seconda metà dell'anno scorso ed è stata rilevata dai ricercatori di sicurezza Avigayil Mechtinger, Ryan Robinson e Nicole Fishbein di Intezer."Se il mercato delle applicazioni legittime tende a premiare applicazioni multi-piattaforma", commenta Antonio Pontrelli, ricercatore di sicurezza di Exprivia, "il mercato del malware non poteva fare eccezione a questa tendenza che vede e vedrà malware multi-piattaforma sempre più presenti sul mercato del crimine".Indice degli argomenti Come agisce SysJokerIl vettore d'attaccoSysJoker: come avviene l'infezioneTutti i passaggi dell'infezioneSu WindowsSu LinuxSu macOSCome difendersi da SysJoker Come agisce SysJoker "A questa categoria appartiene SysJoker", continua Antonio Pontrelli: "Diffuso nella seconda metà del 2021, è in grado di fare danni su Windows, Linux e macOS". WHITEPAPER Quali sono gli step da seguire per effettuare la corretta progettazione di un ambiente VDI? Sicurezza Smart working Scarica il Whitepaper"SysJoker utilizza una backdoor per stabilire l'accesso iniziale sulla macchina target", ci dice ancora Pontrelli. "Una volta installato, i criminali hanno pieno accesso al dispositivo infetto e pertanto possono eseguire codice, comandi aggiuntivi o cercare di infettare altri dispositivi presenti nella stessa rete locale. Questa tecnica è molto richiesta nel Dark Web, dove molti gruppi di criminali possono acquistarla per organizzare i propri attacchi".In questo caso, l'attacco potrebbe essere stato mirato e specifico. Il vettore d'attacco "Un possibile vettore di attacco per SysJoker è un pacchetto infetto su 'npm', un repository di codice che consente agli sviluppatori JavaScript di condividere e riutilizzare blocchi di codice", mette in evidenza Pontrelli: "Npm ed altri repository di codice pubblico sono delle community in cui qualsiasi utente può caricare e scaricare blocchi di codice da includere nello sviluppo delle applicazioni. Se uno di questi blocchi contiene codice malevolo, esso può essere inserito in un numero elevato di applicazioni, rendendo così l'applicazione vulnerabile". SysJoker: come avviene l'infezione Anche se il comportamento di SysJoker è simile per tutti e tre i sistemi operativi, in realtà esistono "piccole differenze in funzione del sistema operativo", sottolinea Pontrelli. E prosegue

l'esperto di cyber security: "L'infezione avviene mascherandosi come un aggiornamento di sistema. Sulla versione Windows, a differenza della versione per Linux e macOS, l'infezione avviene eseguendo uno step in più, ovvero tramite la libreria style-loader.ts.dll presente su npm, che scarica il file msg.zip da un repository GitHub, lo decomprime e lo esegue sul percorso "C:/ProgramData/RecoverySystem/". Tutte queste azioni avvengono tramite i comandi di PowerShell".PowerShell: il fuoco amico sfruttato dal cyber crime Tutti i passaggi dell'infezione "Una volta che viene eseguito il file msg.exe", spiega Antonio Pontrelli, "SysJoker rimane inattivo per un massimo di due minuti prima e successivamente creerà una nuova directory C:/ProgramData/SystemData/ e si copierà in questa directory, mascherandosi come Intel Graphics Common User Interface Service (igfxCUIService.exe). In seguito, SysJoker raccoglierà informazioni sulla macchina compromessa, come MAC address, indirizzo IP, numero di serie e nome utente. SysJoker creerà la persistenza aggiungendo una voce di registro HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersionRun. Tra ciascuno dei passaggi precedenti, il malware è silente per una durata casuale".Pontrelli illustra i passaggi successivi: "Poi SysJoker inizierà la sua comunicazione con il server Command&Contron(C&C). Il collegamento verso il C&C viene stabilita decodificando una stringa da un file di testo ('domain.txt') disponibile su Google Drive".I criminali aggiornano continuamente il collegamento il file domain.txt per evitare il rilevamento e il blocco. Continua Pontrelli: "Le informazioni di sistema raccolte nella fase precedente dell'infezione vengono inviate al C&C. Il C&C risponde con un token univoco che funge da identificatore dell'endpoint infetto. A questo punto il C&C può controllare host infetto tramite la backdoor, inviandoli il comando per installare malware aggiuntivo, eseguire comandi sul dispositivo infetto". Su Windows Pontrelli delinea alcuni degli IOC (indicators of compromise) per ciascun sistema operativo. "In Windows, i file malware si trovano nella cartella: C:ProgramDataRecoverySystem C:ProgramDataSystemDataigfxCUIService.exe C:ProgramDataSystemDatamicrosoft_Windows .dll. Per la persistenza, il malware crea un valore Run di esecuzione automatica di igfxCUIService che avvia l'eseguibile del malware igfxCUIService.exe". Su Linux Su Linux, "i file e le directory vengono creati in /.Library/ mentre la persistenza viene stabilita creando il seguente processo cron: @reboot (/.Library/SystemServices/updateSystem)" continua Pontrelli. Su macOS Su macOS, mette in guardia Pontrelli, "i file vengono creati su/Library/ e la persistenza viene ottenuta tramite LaunchAgent nel percorso: /Library/LaunchAgents/com.apple.update.plist. I domini C&C condivisi sono i seguenti: https[://]bookitlab[.]tech https[://]winaudio-tools[.]com https[://]aggiornamento grafico[.]com https[://]github[.]url-mini[.]com https[://]aggiornamento-office360[.]com https[://]drive[.]google[.]com/uc?export=download&id=1-NVty4YX0dPHdxkgMrbdCldQCpCaE-Hn https[://]drive[.]google[.]com/uc?export=download&id=1W64PQQxrwY3XjBnv_QaeBQu-ePr537eu". Come difendersi da SysJoker "Se viene rilevata una compromissione", conclude Pontrelli, "le vittime possono eliminare i processi relativi a SysJoker, eliminare il relativo meccanismo di persistenza e tutti i file relativi a SysJoker".@RIPRODUZIONE RISERVATA