07/01/2022

cybersecurity360.it

EAV: € 1.521
Utenti unici: 28.467

Argomento: Exprivia: si parla di noi

https://www.cybersecurity360.it/nuove-minacce/zloader-il-malware-ora-sfrutta-un-exploit-su-un-certificato-microsoft-per-diffondersi-come-proteggersi/

ZLoader, il malware ora sfrutta un exploit su un certificato Microsoft per diffondersi: come proteggersi

Il gruppo criminale Malsmoke sta conducendo una campagna malevola mirata al furto di dati sensibili mediante una nuova variante del malware Zloader, diffuso mediante l'exploit di un certificato di verifica Microsoft e già usato in passato per diffondere i ransomware Conti e Ryuk. Ecco come difendersi Il gruppo di cyber criminali Malsmoke sta abusando di un certificato di verifica e-Signature di Microsoft, attraverso il malware ZLoader: l'obiettivo dei criminal hacker è di rubare le credenziali degli utenti e informazioni sensibili.Check Point Research (CPR) avverte che il banking malware sfrutta l'exploit degli strumenti di monitoraggio da remoto e una vulnerabilità che compie nove anni nel certificato di Microsoft di verifica di firma digitale."Parliamo di una nuova campagna malware che di fatto non ha nulla di diverso rispetto a tante altre", commenta Pierguido Iezzi, esperto di cybersecurity e CEO di Swascan: "Il vettore di diffusione è tramite la solita ed evergreen tecnica del social engineering. Il software installato opera attraverso exploit che fanno leva su programmi "standard" o più "diffusi" degli endpoint e l'attacco è completato in base alle finalità e obiettivi più comuni oggi: diffusione di ransomware, furto delle credenziali e sottrazione di dati".Indice degli argomenti Il ritorno di ZloaderCome avviene l'attacco con ZloaderI dettagli dell'attaccoLe osservazioni di Check PointCome proteggersi dalla campagna Malsmoke Il ritorno di Zloader Zloader conduce da novembre una campagna che conta già duemila vittime in 111 Paesi, fra cui USA, Canada, India, Indonesia ed Australia. Il malware Zloader è stato in precedenza usato per diffondere i ransomware Ryuk e della banda Conti. WEBINAR 25 Gennaio 2022 - 12:00Il cybercrime non si ferma: proteggi i tuoi dati anche nel 2022! Sicurezza Sicurezza dei dati Iscriviti al WebinarAntonio Pontrelli, ricercatore di sicurezza di Exprivia, delinea l'identikit di ZLoader: "ZLoader è un trojan bancario individuato per la prima volta nel 2015 in grado di rubare le credenziali dell'account e vari tipi di informazioni private sensibili". Come avviene l'attacco con Zloader "ZLoader è stato utilizzato per veicolare ulteriori payload sui dispositivi infetti, inclusi payload ransomware come Ryuk ed Egregor", continua Pontrelli: "Zloader è stato distribuito dal gruppo criminale noto come MalSmoke utilizzando diverse modalità, dalla posta indesiderata al malvertising fino all'utilizzo di esche di contenuti per adulti. I criminali inducono le vittime ad installare strumenti di gestione remoti per ottenere accesso e controllo del dispositivo tramite un file 'Java.msi'. Diverse sono le modalità utilizzate, da crack su software pirati o e-mail di spear-phishing. Un approccio simile è stato utilizzato dal gruppo ransomware Conti. Gli script 'defenderr.bat' e 'load.bat', inclusi nel programma di installazione 'Java.msi'

eseguono alcuni controlli per assicurarsi di disporre dei privilegi necessari per aggiungere esclusioni a Windows Defender e disabilitare strumenti come 'cmd.exe' e il task manager". I dettagli dell'attacco Pontrelli entra nei dettagli: "Successivamente, i seguenti file aggiuntivi vengono scaricati dal seguente dominio "teamworks455[.]com" e aggiunti nella cartella %AppData%: 9092.dll –payload Zloader appContast.dll – utilizzato per eseguire 9092.dll e new2.bat reboot.dll – utilizzato anche per eseguire 9092.dll new2.bat – disabilita la "Modalità di approvazione dell'amministratore" e spegne il computer auto.bat – posizionato nella cartella di avvio per la persistenza dell'avvioQuindi, lo script invoca il file di Windows mshta.exe, utilizzando come parametro la DLL malevola "appContast.dll". Infine il malware Zloader viene eseguito, iniziando a comunicare con il server C&C (lkjhgfgsdshja[.]com). Confrontando la DLL modificata (appContast.dll) con quella originale (programma di gestione IT remoto), sono state identificate lievi modifiche nel checksum e nella dimensione della firma. Queste semplici modifiche non sono sufficienti per revocare la validità della firma elettronica, ma allo stesso tempo consentono a qualcuno di aggiungere codice (in questo caso) malevolo nella sezione dedicata alla firma del file. Pertanto appContast.dll, che esegue il payload Zloader, contenendo una firma del codice valida, potrebbe sfuggire ai controlli di sistemi di endpoint protection.Infine, lo script "new2.bat" modifica il registro per impostare i privilegi di tutte le applicazioni al livello di amministratore. Affinché questa modifica abbia effetto, è necessario un riavvio, quindi il malware forza il riavvio del sistema infetto", continua Pontrelli. Le osservazioni di Check Point "La catena dell'infezione incorpora tecniche che includono l'uso del software legittimo di remote management software (RMM) per ottenere un accesso iniziale alla macchina nel mirino", spiega Golan Cohen di Check Point in un report. "Il malware poi effettua l'exploit del certificato di verifica di digital signature di Microsoft per iniettare i payload in un sistema DLL per bypassare i sistemi di difesa".L'utilizzo di uno dei file aggiunge l'esclusione di Windows Defender. Intanto un secondo file recupera ed esegue i payload successivi, compreso il DLL "appContast.dll" che serve a far girare ZLoader ("9092.dll"). L'appContast.dll porta la firma legittima di Microsoft con e-signature valida. Inoltre, l'attacco prevede l'iniezione del file, in origine un'app resolver module ("AppResolver.dll"), con uno script per caricare il malware responsabile dell'ultima fase.Infine, l'attacco usa la vulnerabilità CVE-2013-3900 nella WinVerifyTrust signature validation (che risale a nove anni fa), una falla che consente agli attaccanti di eseguire code arbitrario attraverso "eseguibili portatili", artefatti di proposito, in modo tale da modificare il file solo quanto serve per non revocare la validità della firma digitale. Come proteggersi dalla campagna Malsmoke "Partiamo da presupposto che non esistono e non esisteranno software o applicativi completamente sicuri", mette in guardia Iezzi: "Ecco che quindi diventa necessario adottare framework di sicurezza efficaci ed efficienti. Un'architettura di sicurezza basata per layer: predittivo, preventivo e proattivo".L'esperto di cyber security spiega come proteggersi: "Nel caso specifico, questi layer avranno lo scopo di "compensare e proteggere" attraverso un sistema di patching virtuale le criticità e le minacce che quotidianamente incontriamo e siamo costretti a fronteggiare. È evidente che il social engineering sarà sempre

maggiormente il vettore di attacco preferito dai criminal hacker. Diventa quindi necessario e indispensabile prevedere attività di formazione e awareness per i propri dipendenti, ma allo stesso tempo effettuare attività di phishing simulation per misurare costantemente il livello di attenzione e conoscenza dei propri colleghi. Ma non è sufficiente".“Dobbiamo operare per strati di difesa ulteriori. Uno di questo è sicuramente l'adozione di sistemi di EDR (Endpoint Detection & Response) e/o XDR unitamente a servizi di SOC as a Service permettono di creare quella linea di difesa necessaria per ridurre drasticamente il rischio cyber di queste tipologie di attacchi", conclude Iezzi.Infine, il ricercatore Pontrelli invita gli utenti di Microsoft ad applicare l'update per la verifica Authenticode: "Per evitare che le vittime eseguano file modificati con le tecniche descritte è possibile abilitare la funzione di Authenticode che contrassegna tutti i file lievemente manipolati. Maggiori informazioni si trovano sul sito di Microsoft".@RIPRODUZIONE RISERVATA