Un nuovo attacco prende di mira i software pirata di Microsoft Office e Adobe Photoshop CC

Si tratta di un potente malware attivo dal 2018 e scoperto dai ricercatori di Bitdefender che causa furto di dati personali e di denaro. Utenti e aziende italiane tra le vittime colpite da questi attacchi ancora in corso

Milano, 13 aprile 2021 - Bitdefender, azienda leader nella cybersicurezza che protegge centinaia di milioni di endpoint e sistemi in tutto il mondo, pubblica oggi una nuovo report su un attacco eseguito attraverso software "craccati" per Microsoft Office e Adobe Photoshop CC. Oltre all'illegalità nell'utilizzo di simili strumenti, le analisi dei ricercatori di Bitdefender mostrano come questi software, comunemente utilizzati da utenti privati e aziende, siano in realtà una potente e pericolosa porta d'ingresso per infettare i dispositivi permettendo così ai criminali informatici di accedervi, prenderne totalmente il controllo e rubarne dati sensibili, informazioni e denaro.

Secondo le indagini svolte da Bitdefender, gli attacchi che sfruttano questa modalità sono iniziati nella seconda metà del 2018 e sono tuttora attivi. Il report è stato elaborato sulla base delle analisi della threat intelligence di Bitdefender che, per il momento, è anche l'unico vendor in ambito sicurezza ad aver individuato questa campagna di malware.

Eseguire il crack di un software significa modificarlo per rimuovere o disabilitare le caratteristiche non desiderate, soprattutto, per esempio, quelle relative alla protezione dalla copia. Sebbene siano illegali, utenti e aziende usano ancora software craccati o piratati per ridurre i costi, ma allo stesso tempo, così facendo introducono seri rischi per la sicurezza informatica, oltre al fatto che la produzione, vendita e diffusione di software pirata è chiaramente un'attività illegale, perseguita dalla legge.

Principali pericoli relativi all'utilizzo dei software craccati per Microsoft Office e Adobe Photoshop CC:

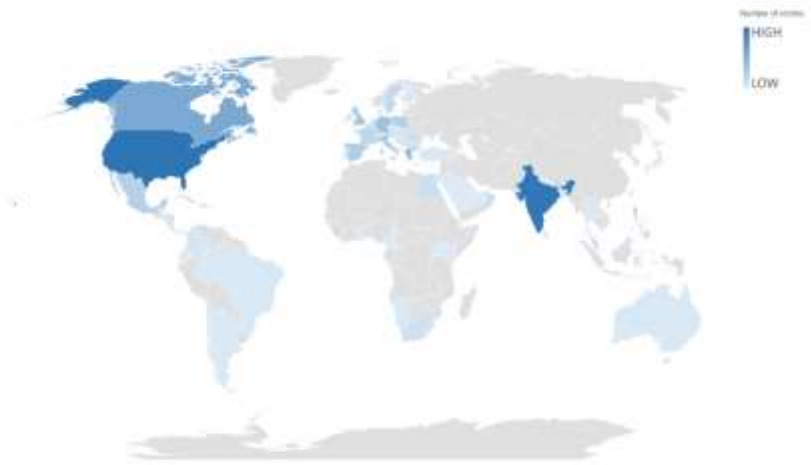
- **Il malware finale è una backdoor** - Questo significa che il criminale informatico assume il pieno controllo del dispositivo e può ordinargli di fare qualsiasi cosa: rubare password, file locali, codici PIN o qualsiasi altra credenziale sensibile.
- **Furto dei wallet Monero** - Qualora l'hacker riesca a individuare un wallet Monero memorizzato sul dispositivo, sarà in grado di assumerne il controllo e di impadronirsi quindi delle criptovalute in esso contenute.
- **Furto dei profili utente del browser Firefox** - Il furto del profilo dell'utente include le password di accesso memorizzate, la cronologia di navigazione, i segnalibri e i cookie di sessione registrati.
- **Hijacking dei cookie delle sessioni di navigazione -** I cookie di sessione sono importanti perché chi se ne impadronisce può semplicemente importarli all'interno del proprio browser e venire così direttamente connesso ai servizi internet dell'utente a cui li ha rubati, senza domande relative a password di accesso o autentificazione a due fattori.

Questa lista di pericoli non è esaustiva; poiché i criminali informatici assumono il controllo completo del dispositivo in cui riescono ad inserirsi, possono adattare le campagne in base ai loro interessi del momento.

Distribuzione geografica

- **US, India, Germany and UK are the most infected countries** – see the attached map for distribution. The infection rate is most likely coordinated with the appetite for pirated software in each geography.

- **Stati Uniti, India, Italia, Spagna, Germania e Regno Unito sono i paesi più colpiti** - La mappa qui di seguito fornisce utili indicazioni per capire la distribuzione geografica degli attacchi. Il tasso di infezione è molto probabilmente legato alle preferenze di utilizzo di software pirata a livello geografico.



L'installazione di un antivirus può aiutare, ma questa modalità di attacco rappresenta una ragione in più per evitare di usare software craccati o pirata. Anche se può essere allettante utilizzare software piratati, per risparmiare a livello economico, si rischia di compromettere totalmente il proprio computer.

A proposito di Bitdefender

Bitdefender, leader riconosciuto nel settore della cybersecurity, offre le migliori soluzioni di prevenzione, rilevamento e risposta alle minacce in tutto il mondo. Responsabile della protezione di milioni di sistemi in ambienti consumer, business e governativi, Bitdefender è l'esperto più affidabile del settore* per eliminare le minacce, proteggere la privacy e i dati per favorire la resilienza informatica. Grazie agli investimenti in ricerca e sviluppo, Bitdefender Labs rileva 400 nuove minacce ogni minuto con 30 miliardi di query giornaliere. L'azienda ha rilasciato innovazioni rivoluzionarie in materia di antimalware, IoT, analisi comportamentale e intelligenza artificiale e la sua tecnologia viene concessa in licenza a oltre 150 brand di cybersecurity, i più conosciuti al mondo. Fondata nel 2001, Bitdefender vanta clienti in 170 paesi e ha uffici in tutto il mondo. Per maggiori informazioni https://www.bitdefender.it.

*Bitdefender si è classificata al primo posto nel 54% di tutti i test di AV-Comparatives 2018-2021 per protezione del mondo reale, prestazioni, protezione dai malware & protezione dalle minacce avanzate.

###

Per ulteriori informazioni

Prima Pagina Comunicazione

02/91339820

Tania Acerbi, Monica Fecchio, Elisa Pagano

tania@primapagina.it

monica@primapagina.it

elisa@primapagina.it