****

**Rischio di attacchi omografici per tutti i programmi**

**di Microsoft Office**

Milano, xx giugno 2022 - Bitdefender Labs annuncia che tutti i programmi MS Office (inclusi Outlook, Word, Excel, OneNote e PowerPoint) sono vulnerabili agli attacchi omografici ai nomi di dominio internazionalizzati (IDN).

Un attacco omografico consiste nell’utilizzare domini con nomi molto simili agli originali, appartenenti a marchi noti o all’azienda obiettivo dell’attacco del criminale informatico ( l'attacco omografico più semplice consiste nel sostituire "o" con "0" ad esempio g00gle.com), con la finalità di attirare gli utenti su siti fasulli e di ottenere così dati personali, di diffondere malware o rendere più credibile una mail di phishing, facendo credere al malcapitato di wessere nel sito web originale. Tuttavia, gli attacchi omografici IDN possono essere irriconoscibili dai domini a cui stanno facendo spoofing, perché le lettere dei vari alfabeti sono quasi identiche.

Sebbene il rischio di attacchi omografici IDN sia stato rilevato nei browser web, Bitdefender ha riscontrato che i nomi di dominio oggetto di spoofing utilizzati nelle applicazioni MS Office rimangono cammuffati, rendendo elevata la probabilità di clic da parte dell’utente.

**Principali rilevazioni**

* Bitdefender ha scoperto che tutte le applicazioni di Microsoft Office rimangono vulnerabili agli attacchi di tipo omografico IDN.
* Bitdefender ha testato altre applicazioni di produttività e ha riscontrato un comportamento incoerente: alcune applicazioni visualizzano sempre l'indirizzo reale, mentre altre visualizzano un nome internazionale.
* Bitdefender ha segnalato questo problema a Microsoft nell'ottobre 2021 e il Microsoft Security Response Center ha confermato la validità dei risultati del vendor. Ad oggi non è ancora chiaro se e quando Microsoft risolverà il problema.
* Gli attacchi al nome di dominio internazionalizzato sono uno strumento efficace che gli avversari di alto livello (APT o RaaS) possono utilizzare contro obiettivi di alto valore (aziende o persone). Bitdefender ha osservato attacchi di spoofing che hanno preso di mira istituzioni finanziarie e borse di criptovalute.

**Le raccomandazioni di Bitdefender**

* Considerare la possibilità di attacchi omografici nei momenti di formazione e di sensibilizzazione degli utenti, compresa la possibilità di attacchi omografici contro la supply chian dell’azienda.
* Implementare una soluzione di sicurezza per gli endpoint che rilevi e blocchi i siti web dannosi.
* Utilizzare i servizi di reputazione di IP e URL per tutti i dispositivi aziendali. Una semplice regola da tenere in considerazione: se l'URL inizia con xn--, il sito è sospetto.

Ogni mese Bitdefender esamina i dati della sua telemetria per ottenere maggiori informazioni sul panorama delle minacce in merito agli attacchi omografici. Analizzando queste informazioni emerge una chiara tendenza a prendere di mira le operazioni finanziarie, con un focus primario sui mercati delle criptovalute.

La ricerca completa è disponibile [qui](https://businessinsights.bitdefender.com/homograph-phishing-attacks-when-user-awareness-is-not-enough).

**Informazioni su Bitdefender**

Bitdefender fornisce efficaci soluzioni di sicurezza informatica che garantiscono alte prestazioni e facilità d'uso alle PMI, alle medie aziende e ai consumatori. Con una vision incentrata sul fornire le soluzioni di sicurezza informatica più affidabili al mondo, la missione di Bitdefender è difendere le aziende e le persone in tutto il mondo dagli attacchi informatici per trasformare e migliorare la loro esperienza digitale. Per maggiori informazioni, è possibile visitare la pagina <https://www.bitdefender.com>

**Per ulteriori informazioni**

Prima Pagina Comunicazione

02/91339820

Tania Acerbi, Monica Fecchio, Elisa Pagano

tania@primapagina.it

monica@primapagina.it

elisa@primapagina.it