Bitdefender

# La nuova campagna malware BellaCiao

**Milano, 27 Aprile 2023** - Bitdefender rilascia oggi una ricerca che illustra una nuova (e ancora in corso) campagna di malware, denominata BellaCiao, che sta prendendo di mira aziende negli Stati Uniti, in Europa, Israele, Turchia e India.

BellaCiao è gestita da Charming Kitten (alias Mint Sandstorm, APT35/42), noto gruppo di criminali informatici sostenuto dal governo iraniano. Il nuovo malware è altamente sofisticato e adattato a ogni tipologia di obiettivo; utilizza un approccio di comunicazione specifico che utilizza la sua infrastruttura di comando e controllo (C2).

La funzione di BellaCiao è quella di operare come backdoor e dropper e può essere utilizzato per distribuire qualsiasi tipo di malware a scopo di spionaggio, furto di dati, ransomware ed estorsione. Una volta infettato il sistema, BellaCiao si nasconde come se fosse un processo legittimo che non viene rilevato e attende ulteriori istruzioni dai criminali informatici.

La ricerca sottolinea come l'elemento di novità che contraddistingue BellaCiao sia il modo in cui riceve le istruzioni dal server C2 degli hacker. BellaCiao chiede al computer infetto di eseguire una richiesta DNS per suo conto ogni 24 ore per la risoluzione di un sottodominio tramite una stringa hardcoded unica per ogni vittima.

Bitdefender ritiene che questa campagna sia la fase successiva agli attacchi opportunistici. Charming Kitten cerca indiscriminatamente sistemi vulnerabili (utilizzando exploit di vulnerabilità), quindi sviluppa un malware personalizzato (BellaCiao) per l'azienda compromessa e lo distribuisce da remoto.

Dal momento che la campagna è ancora in Corso, Bitdefender invita le aziende a mantenere un elevato livello di attenzione e a condividere con i CIO le informazioni di questa ricerca.

Per difendersi dagli attacchi di ultima generazione - come BellaCiao – è nceessario adottare soluzioni di sicurezza informatica complete che includano funzionalità di prevenzione, rilevamento e neutralizzazione delle minacce. Bitdefender consiglia inoltre di implementare la reputazione di IP/URL/Dominio su tutti gli endpoint.

La ricerca completa è disponibile qui.

**Informazioni su Bitdefender**

Bitdefender è una società leader nella sicurezza informatica che offre le migliori soluzioni di prevenzione, rilevamento e risposta alle minacce del mondo. Proteggendo milioni di consumatori, aziende e ambienti governativi, Bitdefender è considerata uno degli esperti più affidabili del settore per eliminare le minacce, proteggere la privacy e i dati, e ottenere la resilienza informatica. Grazie a notevoli investimenti in ricerca e sviluppo, Bitdefender Labs scopre centinaia di nuove minacce ogni minuto e convalida miliardi di query sulle minacce al giorno. L'azienda ha aperto la strada a innovazioni rivoluzionarie in varie tecnologie, come anti-malware, sicurezza IoT, analisi comportamentale e intelligenza artificiale. La sua tecnologia è usata su licenza da più di 150 dei marchi tecnologici più noti al mondo. Fondata nel 2001, Bitdefender ha clienti in oltre 170 paesi con uffici in tutto il mondo. Per maggiori informazioni, visitare https://www.bitdefender.it.

**Per ulteriori informazioni**

Prima Pagina Comunicazione

02/91339820

Tania Acerbi, Monica Fecchio, Elisa Pagano

tania@primapagina.it

monica@primapagina.it

elisa@primapagina.it