Yoroi ha scoperto una serie di attacchi che stanno infettando le aziende manifatturiere italiane con finti documenti Microsoft Office ed Excel attraverso la botnet Dridex

https://yoroi.company

nota per la stampa del 16 Novembre 2021

Contrastare i cyber-attacchi è sempre più difficile. Gli aggressori informatici modificano e migliorano costantemente le loro tecniche, ma una tendenza rimane costante: i documenti Microsoft Office ed Excel sono gli strumenti di diffusione preferiti da molti criminali informatici per inoculare malware nelle aziende.

Si tratta infatti di una tecnica estremamente flessibile e abusata sia da attori opportunisti che dalle APT, le così dette Minacce Avanzate Persistenti che fanno capo a gruppi criminali ben finanziati e organizzati e spesso supportati da governi canaglia.

Negli ultimi mesi il **Malware ZLAB di Yoroi** (gruppo Tinexta) ha monitorato con particolare attenzione le **ondate di attacchi** che adottano però una nuova tecnica: librerie binarie caricate direttamente da Microsoft Excel, **in un solo click**. Questa tecnica di diffusione emergente sfrutta i file XLL, un particolare tipo di file contenente un'applicazione Microsoft Excel pronta per essere caricata.

Questo metodo di sfruttamento di Microsoft Office viene silenziosamente abusato in molte ondate di attacchi in tutto il mondo, ma recentemente questa tecnica emergente è stata usata **per colpire le aziende manifatturiere italiane**.

E i criminali informatici stanno utilizzando massicciamente queste particolari applicazioni Excel XLL perché rendono inefficaci i motori di scansione antivirus per i documenti ricevuti nelle caselle di posta aziendali.

Gli **attacchi** sono infatti basati su **email e documenti Microsoft Office**, i file XLL, un tipo di documento Excel che non è però un documento Office, ma una libreria eseguibile che viene utilizzata dai cybercriminali per iniettare malware in grado di rubare le credenziali salvate nel browser e agli attaccanti di accedere remotamente al computer.

Il **CERT di Yoroi** sta monitorando la nuova tecnica dall'estate del 2021. Già osservata originariamente in attacchi sporadici, nell'ultimo mese attori criminali hanno cominciato ad abusare della nuova tecnica anche ai danni di realtà italiane.

La campagna di malspam – cioè un invio massiccio di email per infettare le vittime -, che veicola il file dannoso camuffato da documento Excel, utilizza le infrastrutture di **Discord**, la piattaforma statunitense per chiamate vocali e messaggistica istantanea progettata per la comunicazione tra comunità di videogiocatori.

Il codice malevolo in questo caso è **particolarmente pericoloso** in quanto è associato a tecniche di evasione che ne rendono difficile l'individuazione anche con VirusTotal, la piattaforma di Google per l'analisi dei file potenzialmente infetti.

In questo momento almeno **due campagne d'attacco** che lo utilizzano hanno l'Italia come **bersaglio**.

La pericolosa tecnica risulta attualmente utilizzata dalla **botnet criminale Dridex** nel corso di attacchi su larga scala, indice di una potenziale esplosione di questa tecnica di attacco nel corso dei prossimi mesi del 2022. Dridex è uno dei malware bancari più pericolosi e resistenti al mondo, dal 2010 sfrutta le macro di Word e Excel, e la sua botnet, cioè la rete di computer zombie che utilizza per diffondere il suo carico malevolo, è tra le più estese tra quelle conosciute. Gli attacchi provenienti da questa botnet possono portare a una infezione ransomware di tipo double-extortion come è già accaduto in aprile ai danni di molti comuni italiani del Nord-Ovest.

Secondo i coordinatori dello Zlab di Yoroi: "Le aziende oggetto di questa campagna in Italia sono una decina nel settore manifatturiero e l'attenzione va tenuta alta. La campagna è particolarmente pericolosa perché inganna i sistemi di difesa tradizionali e il suo livello di sofisticazione suggerisce che gli attaccanti, di provenienza russa e asiatica, si stanno organizzando per affinare i loro attacchi via email".

Di seguito il link diretto all'analisi che Yoroi ha realizzato in inglese per la comunità internazionale:

https://yoroi.company/research/office-documents-may-the-xll-technique-change-the-threat-landscape-in-2022/

Yoroi Srl – Tinexta Cyber SpA

Yoroi Srl è un'azienda che gestisce Sistemi Integrati Adattivi e Dinamici di Difesa Cibernetica e sviluppata tecnologie proprietarie che hanno ottenuto significativi riconoscimenti anche sul mercato internazionale. Coniugando esperienza e vocazione all'innovazione tecnologica, conta più di 40 cyber analisti qualificati, più di 50 sviluppatori e uno dei più importanti team di ethical hacking formato da oltre 20 specialisti tra i più qualificati e riconosciuti sia a livello nazionale che Internazionale.

Dal 2020, Yoroi è parte di **TinextaCyber (Tinexta Group)**, il polo italiano della cybersecurity con forti competenze verticali e soluzioni custom proprietarie per la mitigazione e la governance dei rischi legati alla sicurezza digitale. L'azienda agisce con e attraverso le società controllate Corvallis, Swascan, oltre che Yoroi. Con 900 dipendenti complessivi, Tinexta Cyber opera dalla sede di Roma e da 22 uffici in Italia.

@yoroisecurity www.linkedin.com/company/yoroi/	Media Advisor Arturo Di Corinto (+39) 335 6785259	https://www.yoroi.company https://blog.yoroi.company/ https://yomi.yoroi.company