COMPARTIMENTO POLIZIA POSTALE E DELLE COMUNICAZIONI "CALABRIA"
NUCLEO OPERATIVO PER LA SICUREZZA CIBERNETICA

Protocollo	MIPG	**Data**	27/08/2021
Destinatari	**Infrastrutture Critiche Informatizzate CALABRIA**		

Oggetto	**Alert compromissione sistemi informatici**
Data evento	Evento in corso
Descrizione evento	• Ricercatori di sicurezza hanno recentemente tracciato una nuova backdoor modulare, SideWalk, utilizzata da un sottogruppo del cluster Axiom denominato SparklingGoblin. Questa minaccia, condivide molteplici somiglianze con CROSSWALK, backdoor proprietaria di Axiom. Secondo i dati ottenuti dai ricercatori, SparklingGoblin ha preso di mira una vasta gamma di organizzazioni in tutto il mondo. SideWalk si presenta come uno shellcode criptato in ChaCha20 che viene caricato in memoria tramite process hollowing da un loader in .NET (offuscato con ConfuserEx) che ottiene la persistenza tramite task. Gli indirizzi dei C2 vengono ottenuti da SideWalk decriptando una stringa presente su un documento Google Docs il cui indirizzo è hardcoded. La backdoor è in grado di esfiltrare informazioni sul sistema e di eseguire payload aggiuntivi inviati dal C2. • È in corso una campagna di smishing (phishing basato su SMS) massivo, lanciata a partire dalla metà giugno 2021. I messaggi sembravano inviati da servizi postali e inducevano i destinatari a cliccare su un link per recuperare un pacco in giacenza. Il link reindirizza a una pagina di phishing mirata a sottrarre informazioni personali e di pagamento. • Si è venuto a conoscenza che in seguito a recenti investigazioni sul ransomware Chaos, sono state rilevate alcune novità; prima tra tutte, la conferma della sua creazione sulla base di Hidden Tear, ransomware opensource risalente all'agosto 2015. La connessione tra i due è visibile nella versione 3.0 di Chaos dove la minaccia ha acquisito la capacità di crittografare i file utilizzando AES/RSA. Infatti, in questa versione il codice per generare la chiave e quello per eseguire l'effettiva crittografia AES sono quasi identici a quelli utilizzati da Hidden Tear. Inoltre, è stato possibile confermare che lo sviluppatore del builder del ransomware Chaos aveva precedentemente creato "bagli ransomware" (una prima versione di Chaos scritta in C#) e lo aveva venduto sul marketplace del dark web "Tor2door". Infine, ricercatori di sicurezza hanno segnalato che molte varianti basate su Chaos 3.0 sono apparse In The Wild utilizzando lo stesso indirizzo di wallet BTC e la stessa nota di riscatto e chiedendo lo stesso importo. Le estensioni utilizzate dalle varianti identificate finora sono "pay us", "gru", "big", "AstraLocker". • Si è venuto a conoscenza che, dalla fine di giugno 2021, sono state tracciate numerose campagne di phishing a tema COVID-19 che distribuiscono i malware RustyBuer, Formbook e Ave Maria e prendono di mira migliaia di organizzazioni a livello globale. L'aumento dell'utilizzo di temi COVID-19 si allinea con l'interesse pubblico per la variante Delta, altamente contagiosa. Nella nuova campagna FormBook, le email (oltre

	7.000) contengono un file .zip malevolo che, se eseguito, porta all'installazione della minaccia. Il malware Ave Maria è stato invece utilizzato per lo più in campagne contro organizzazioni del settore energetico (il 90% degli obiettivi) e industriale. Il contenuto dei messaggi allerta i dipendenti sulle nuove misure preventive COVID-19 incluse nell'allegato Excel. Quest'ultimo sfrutta varie vulnerabilità di Equation Editor. Infine, la campagna RustyBuer risulta essere quella attualmente più attiva. Le email contengono allegati .zip con all'interno file Excel. Questi ultimi sono protetti da password e contengono a loro volta macro malevole che, se abilitate, scaricano ed eseguono il malware. I messaggi non imitano nessuna corrispondenza ufficiale e il più delle volte non hanno senso grammaticale e sembrano contenere frammenti di notizie. Si segnalano inoltre molteplici tentativi di phishing aziendale per rubare credenziali Microsoft e O365. In questo caso, il testo dell'email contiene un URL che reindirizza la vittima a una falsa pagina di autenticazione Microsoft. • Si è venuto a conoscenza che, FormBook è ancora il protagonista di una campagna di phishing che sta colpendo anche in Italia. I target ricevono un email a tema "Purchase Order" con un allegato .Izh. Questo contiene a sua volta un file .exe (ovvero il malware stesso) che, se aperto, avvia la catena d'infezione. • È stata tracciata una nuova campagna di distribuzione del malware Hancitor che sta interessando anche utenze mail italiane. Le email sono a tema DocuSign e contengono in allegato un file .doc. Questo contatta un URL diverso ogni volta ed effettua il download di un documento che varia ad ogni operazione. Il file .doc contiene a sua volta una DLL con il malware stesso. Al momento, non è chiaro quale sia il payload finale. • Si è venuto a conoscenza che il ransomware KARMA, distribuito dall'omonimo gruppo, si presenta come un eseguibile console-based per architetture x86 scritto in C/C++. Per evitare l'esecuzione di più istanze del ransomware viene creata la mutex KARMA; la cifratura avviene grazie alla libreria crypt32.dll inserita in CryptoAPI. I file cifrati – vengono colpiti solo quelli all'interno di specifiche cartelle e di tipologie diverse da .exe, .dll, .ini, .url, .lnk – ricevono l'estensione .KARMA. Alla fine dell'operazione malevola viene scaricata la nota con la richiesta di riscatto KARMA-ENCRYPTED.txt in varie posizioni nei sistemi colpiti. Le vittime sono invitate a contattare degli indirizzi onionmail o protonmail per ricevere indicazioni sul pagamento che va effettuato in bitcoin. • È stata recentemente rilevata una campagna volta a veicolare LokiBot attraverso molteplici tecniche, compreso lo sfruttamento di vecchie vulnerabilità. Tra i metodi di distribuzione figura l'utilizzo di Open Action Object nei PDF, Frameset nei DOCX, sfruttamento della CVE-2017-11882 tramite gli RTF e della CVE-2016-0189 in Internet Explorer e l'utilizzo di OLE Object e Word incorporati in file Excel. In un attacco è stato rilevato l'utilizzo di un PDF a tema fatturazione che, una volta aperto, fa connettere l'host ad un IP hardcoded che risponde con un HTML malevolo il quale, sfruttando la CVE-2016-0189, esegue un PowerShell. Il payload scaricato risulta essere LokiBot, malware utilizzato per rubare informazioni dai browser, dai server FTP e dai client SMTP. • Si continuano a tracciare campagne di spionaggio contro target governativi ad opera dell'APT nordcoreano ScarCruft, noto anche come Kimsuki. L'attacco inizia con un file JavaScript mascherato da PDF contenente dati codificati in Base64. Una volta aperto,

	scarica un PDF e lancia il programma legittimo Adobe Reader per la sua visualizzazione e contemporaneamente scarica un eseguibile. Successivamente, decodifica il payload e lo esegue in modalità stealth. Secondo quanto emerge dalle investigazioni, il payload risulta essere una DLL offuscata con UPX che ha capacità di persistenza nei sistemi. La minaccia, un tool di spionaggio, ha funzionalità di keylogging e può ricercare documenti di diverse estensioni (.hwp, .pdf, .doc, .xls, .ppt, .txt) in tutte le directory, comprese le unità USB, con lo scopo di esfiltrarli. Premesso quanto sopra, si prega di garantire **la riservatezza delle informazioni fornite, astenendosi dal divulgare la presente nota di trasmissione**. Si chiede di fornire riscontro, facendo riferimento al numero di protocollo della presente, **solo in caso di effettiva compromissione dei vostri sistemi informatici**. Si allega copia degli archivi zip cifrati con password "cnaipic", contenente gli indicatori di compromissione afferenti alla presente comunicazione. Si rappresenta che il formato. json è compatibile con la nota piattaforma MISP e, pertanto, direttamente importabile in essa. e si raccomanda la massima cautela della consultazione della corrispondenza e messaggistica digitale, verificando con precisione il mittente prima di aprire allegati e cestinando eventuali messaggi di dubbia provenienza.

IL DIRETTORE DEL 3°SETTORE
MORABITO

ORIGINALE FIRMATO AGLI ATTI

Compartimento Polizia Postale e delle Comunicazioni "Calabria"
Indirizzo: Via S. Anna II tr. snc – Reggio Calabria
Tel. 0965309011 e-mail: polposta.rc@poliziadistato.it
PEC: compartimento.polposta.rc@pecps.poliziadistato.it