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

POLIZIA POSTALE E DELLE COMUNICAZIONI
COMPARTIMENTO REGGIO CALABRIA
Prot.: 0011637 del 01/09/2021 Uscita Cod. Amm. m_it
AOO: RCPH10 uor: RCPH10
Data: 01/09/2021 08:40:23

Protocollo	MIPG	**Data**	01/09/2021
Destinatari	**<u>Infrastrutture Critiche informatizzate CALABRIA</u>**		

Oggetto	**Alert compromissione sistemi informatici.**
Data evento	Evento in corso
Descrizione evento	• Una campagna globale di distribuzione del malware FormBook sta interessando anche l'Italia. Un'email a tema "Request for Quotation" apparentemente inviata da una compagnia cinese riporta in allegato un file lzh contenente l'eseguibile della minaccia. • Si è venuto a conoscenza che un messaggio di posta elettronica scritto in inglese che sembra provenire da una compagnia realmente esistente con base a Brema (Germania) sta distribuendo FormBook anche in Italia. L'oggetto della mail fa riferimento ad una fattura e in allegato compare un file .doc; quest'ultimo, all'apertura, avvia l'infezione dell'host. • Si è venuto a conoscenza che il ransomware LockFile, attivo da luglio 2021, continua ad essere oggetto di analisi. Una condotta su uno specifico sample ha messo in luce alcuni nuovi dettagli. Il binario è offuscato per due volte con UPX e modificato per eludere le analisi statiche da parte di software presenti negli endpoint. Anche i nomi di sezione originali sono stati alterati: UPX0 e UPX1 sono stati sostituiti, rispettivamente, con OPEN (che non contiene alcun dato) e CLSE (che si compone di 286Kb; la prima parte del codice verrà traslata in OPEN, mentre nell'ultima pagina sono presenti 3 funzioni). Una volta avviata, la minaccia termina processi pericolosi per la propria attività, come macchine virtuali, database MySQL e servizi di sicurezza Oracle. La libreria utilizzata per la cifratura deriva dal progetto open source Crypto++ Library, presente su GitHub. Da questa operazione sono esclusi file il cui nome contenga le seguenti stringhe: ".lockfile", "\Windows", "LOCKFILE", "NTUSER". Inoltre, LockFile dispone di due ampie blacklist di estensioni che comprendono anche .gif .ini .iso .jpeg .jpg .m4a .mov .mp3 .mp4 .mpeg .msi .mui .php. Lo schema di cifratura intermittente consente di eludere sistemi di detection come chi-squared (chi^2), presente in alcuni software. Al termine del processo, i record ricevono l'estensione .lockfile. La nota con la richiesta di riscatto 'LOCKFILE-README-[hostname]-[id].hta' somiglia a quella utilizzata da LockBit 2.0; al suo interno compare un indirizzo di contatto registrato sul dominio contipauper, il cui nome sembra allusivo al ransomware Conti. L'intera procedura si conclude con la cancellazione del malware dai sistemi. • Si è venuto a conoscenza che la botnet Mirai ha iniziato a sfruttare la vulnerabilità CVE-2021-32305 di WebSVN poco dopo il rilascio della PoC dell'exploit. WebSVN è un'applicazione web open-source e cross-platform basata su PHP e viene utilizzata per la gestione del codice sorgente. La falla, scoperta e corretta nel maggio 2021 con la versione 2.6.1, è di tipo command injection. La PoC è stata resa pubblica il 26 giugno. Gli avversari stanno approfittando di questo bug per scaricare uno shell script capace di sottrarre informazioni di sistema e sull'architettura del processore che verranno utilizzate da uno

	shell script di secondo livello allo scopo di scaricare ed eseguire un binario malevolo (una variante della botnet). Mirai, in questo frangente, è stata utilizzata per lanciare attacchi DDoS. • È stata rilevata una campagna che sfrutta la CVE-2021- 35394, una delle vulnerabilità RealTek divulgate la scorsa settimana. Nello specifico, è in corso la distribuzione di varianti della botnet Mirai. Tale bug, di tipo Command Injection, è sfruttabile inviando pacchetti UDP malevoli. Questo attacco prende di mira i chipset Realtek RTL8xxx SoC – utilizzati in molti dispositivi embedded, in particolare i router wireless – e le seguenti architetture: ARM (v5 e v7), MIPS e SuperH. Al momento, tutti i server di download utilizzati in questa campagna sono online e gli attacchi sono in corso. La vulnerabilità è stata apparentemente risolta, ma alcuni analisti hanno scoperto che la correzione consiste semplicemente nel verificare che tutte le stringhe di comando abbiano il prefisso "orf". Questa mitigazione è facilmente aggirabile aggiungendo il suddetto prefisso a qualsiasi stringa di comando. • Si è venuto a conoscenza che IL RAT NanoCore viene attualmente distribuito anche ad utenze email italiane. Il messaggio – scritto in inglese e apparentemente spedito da una compagnia con sedi negli Emirati Arabi e in Pakistan – ha come oggetto "RE: Payment". 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