

Guerra digitale: il gruppo russo Trident Ursa non interrompe le sue attività cyber



Trident Ursa: minaccia avanzata persistente della Russia contro il dominio cibernetico dell'Ucraina

Dalla pubblicazione dell'ultimo blog di Unit 42, a inizio febbraio, dedicato al gruppo APT Trident Ursa (alias Gamaredon, UAC-0010, Primitive Bear, Shuckworm), l'Ucraina e il suo dominio cibernetico hanno dovuto affrontare minacce sempre più gravi da parte della Russia. Il Servizio di sicurezza ucraino collega il gruppo Trident Ursa al Servizio di sicurezza federale russo.

Gli attacchi cyber di Trident Ursa continuano in Ucraina

Durante il conflitto in corso sul territorio e nel cyberspazio, Trident Ursa ha operato come creatore di accessi e collettore di informazioni. Il gruppo rimane una delle Advanced Persistent Threat più pervasive, invadenti, costantemente attive e concentrate sull'Ucraina. Data la situazione geopolitica in corso e l'obiettivo specifico di questo gruppo, i ricercatori di Unit 42 continuano a monitorare attivamente gli indicatori delle loro operazioni. In questo modo, sono stati mappati oltre 500 nuovi domini, 200 campioni e altri Indicatori di Compromissione (IoC) utilizzati negli ultimi 10 mesi che supportano diversi obiettivi di

phishing e malware di Trident Ursa.

Nuove informazioni sull'operatività e sulle tattiche di Trident Ursa

Unit 42 fornisce questo aggiornamento insieme a IoC noti per evidenziare e condividere l'attuale conoscenza e comprensione delle operazioni di Trident Ursa. Monitorando questi domini e l'intelligence open source, sono stati identificati diversi elementi rilevanti:

- Un tentativo fallito di compromettere una grande azienda di raffinazione del petrolio all'interno di un Paese membro della NATO il 30 agosto.
- Un individuo, che sembra essere coinvolto con Trident Ursa, ha minacciato di fare del male a un ricercatore di sicurezza informatica con sede in Ucraina subito dopo l'invasione iniziale.
- Numerosi cambiamenti nelle tattiche, tecniche e procedure.

Tradizionalmente, Trident Ursa ha preso di mira soprattutto entità ucraine con esche scritte in ucraino. Sebbene questo sia ancora lo scenario più comune per questo gruppo, sono stati anche osservati alcuni casi di utilizzo dell'inglese. Unit 42 ritiene che questi esempi indichino che Trident Ursa stia cercando di incrementare la raccolta di informazioni e l'accesso alla rete contro gli alleati ucraini e della NATO.

Adattabilità di Trident Ursa e utilizzo di strumenti e script pubblici

Trident Ursa si conferma un gruppo agile e adattabile che non utilizza tecniche troppo sofisticate o complesse nelle sue operazioni. Nella maggior parte dei casi, per eseguire con successo le attività si affida a strumenti e script pubblici disponibili, insieme a un livello significativo di

offuscamento e tentativi di phishing di routine.

Persistenza e successo di Trident Ursa negli attacchi cyber

Le operazioni di questo gruppo vengono regolarmente rilevate da ricercatori e organizzazioni governative, ma i cybercriminali non sembrano preoccuparsene. Semplicemente aggiungono ulteriori offuscamenti, nuovi domini e nuove tecniche e ci riprovano, spesso riutilizzando anche sample precedenti. Operando in questo modo almeno dal 2014, e senza alcun segno di rallentamento durante questo periodo di conflitto, Trident Ursa continua ad avere successo.

Per tutti questi motivi, Trident Ursa rimane una minaccia significativa per l'Ucraina, dalla quale il paese e i suoi alleati devono difendersi attivamente.

Tutti i dettagli sono disponibili qui
<https://unit42.paloaltonetworks.com/trident-ursa>

Condividi sui Social Network:

<https://www.ictsecuritymagazine.com/notizie/guerra-digitale-il-gruppo-russo-trident-ursa-non-interrompe-le-sue-attivita-cyber/>