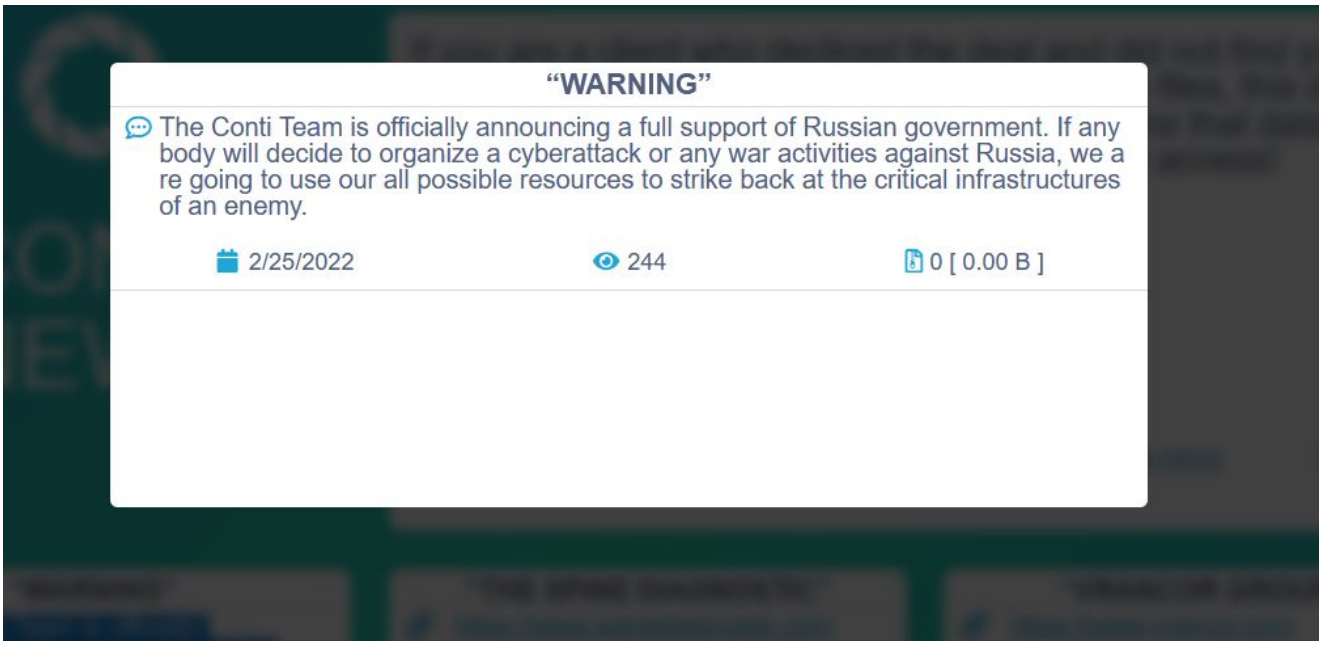
Il ransomware Conti si schiera a favore della Russia nella cyberwar.

redhotcyber.com/post/il-ransomware-conti-si-schiera-a-favore-della-russia

Redazione RHC February 25, 2022

La famigerata cyber-gang Conti, ha pubblicato poco fa un annuncio sul suo data-leak-site (DLS) che riporta **la vicinanza e il sostegno al governo Russo,** riportando quanto segue:*"Il Conti Team annuncia ufficialmente **il pieno sostegno del governo russo**.*

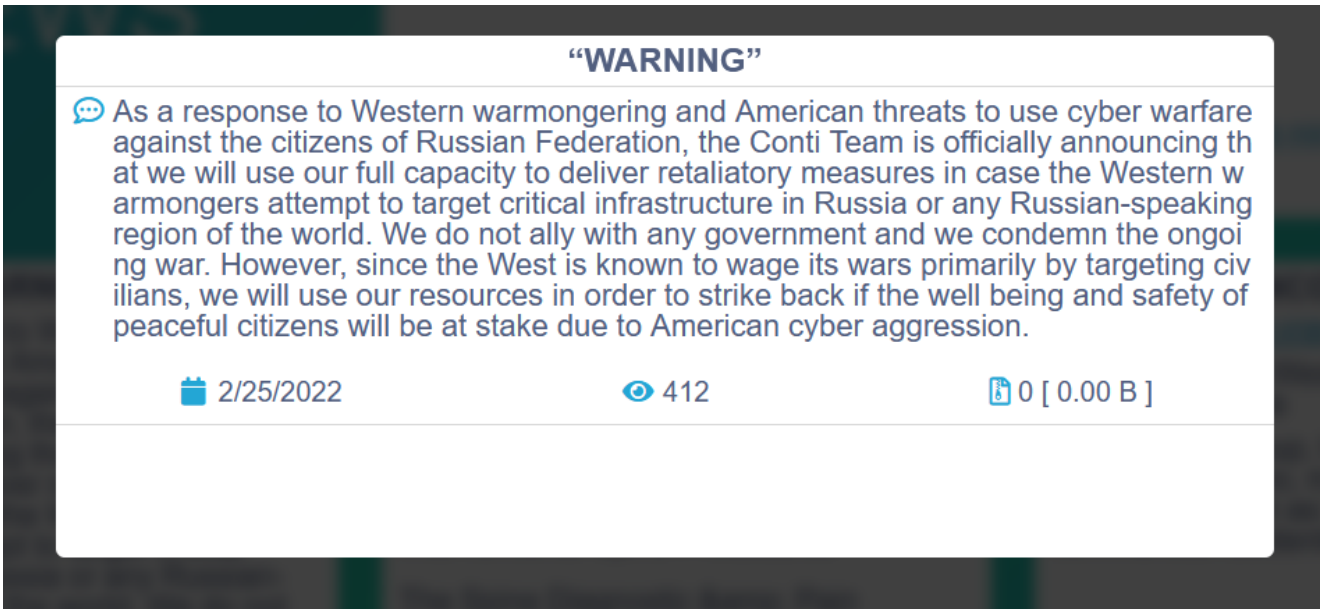


Primo post della cybergang Conti
"*Se qualcuno deciderà di organizzare un attacco informatico o qualsiasi attività bellica contro la Russia, utilizzeremo tutte le nostre risorse possibili per contrattaccare le infrastrutture critiche di un nemico.*"

In effetti, negli ultimi periodi, soprattutto quando erano iniziate le consultazioni tra Biden e Putin e dopo gli arresti dei criminali di REvil, le cybergang da profitto come Conti e LockBit 2.0, avevano iniziato ad avere timore di possibili arresti, pensando anche ad una mancata protezione da parte del governo russo schierato con gli Stati Uniti, il quale storicamente è sempre stato vicino ai criminali informatici con un patto mai scritto ma vero nella sostanza.

Abbiamo in precedenza molto parlato del legame tra le intelligence Russe e i gruppi hacker underground, riportando che molti hacker assoldati dal Cremlino provengono da questi vivai di hacker nationalstate e hacker da profitto.

Poche ore dopo la prima pubblicazione, il collettivo Conti aggiorna il post riportando quanto segue:



Secondo post emesso dalla cybergang Conti
"*In risposta ai guerrafondai occidentali e alle minacce americane di utilizzare la guerra informatica contro i cittadini della Federazione Russa, il Conti Team annuncia ufficialmente che utilizzeremo la nostra piena capacità per fornire misure di ritorsione nel caso in cui i guerrafondai occidentali tenti di prendere di mira infrastrutture critiche in Russia o qualsiasi regione del mondo di lingua russa. Non ci alleiamo con nessun governo e condanniamo la guerra in corso. Tuttavia, poiché è noto che l'Occidente conduce le sue guerre principalmente prendendo di mira i civili, utilizzeremo le nostre risorse per contrattaccare se il benessere e la sicurezza dei cittadini pacifici saranno in gioco a causa dell'aggressione informatica americana.*"

Sicuramente ora il livello di allerta relativamente alla minaccia cyber è massima, pertanto tutte le aziende dovrebbero proteggersi qualora non lo abbiano fatto, per evitare di rimanere vittime di rappresaglie **nei confronti dell'Italia che apertamente si è schierata contro la Russia.**

La cyber war ora entra nel vivo.

La cyber war è una guerra che non ha un confine geografico.

Come proteggersi dal ransomware

Le infezioni da ransomware possono essere devastanti per un'organizzazione e il ripristino dei dati può essere un processo difficile e laborioso che richiede operatori altamente specializzati per un recupero affidabile, anche se in assenza di un backup dei dati, sono molte le volte che il ripristino è stato impossibile. Infatti, si consiglia agli utenti e agli amministratori di adottare delle misure di sicurezza preventive per proteggere le proprie reti dalle infezioni da ransomware e sono:

- Utilizzare un piano di backup e ripristino dei dati per tutte le informazioni critiche. Eseguire e testare backup regolari per limitare l'impatto della perdita di dati o del sistema e per accelerare il processo di ripristino. Da tenere presente che anche i backup connessi alla rete possono essere influenzati dal ransomware; i backup critici devono essere isolati dalla rete per una protezione ottimale;
- Mantenere il sistema operativo e tutto il software sempre aggiornato con le patch più recenti. Le applicazioni ei sistemi operativi vulnerabili sono l'obiettivo della maggior parte degli attacchi. Garantire che questi siano corretti con gli ultimi aggiornamenti riduce notevolmente il numero di punti di ingresso sfruttabili a disposizione di un utente malintenzionato;
- Mantenere aggiornato il software antivirus ed eseguire la scansione di tutto il software scaricato da Internet prima dell'esecuzione;
- Limitare la capacità degli utenti (autorizzazioni) di installare ed eseguire applicazioni software indesiderate e applicare il principio del "privilegio minimo" a tutti i sistemi e servizi. La limitazione di questi privilegi può impedire l'esecuzione del malware o limitarne la capacità di diffondersi attraverso la rete;
- Evitare di abilitare le macro dagli allegati di posta elettronica. Se un utente apre l'allegato e abilita le macro, il codice incorporato eseguirà il malware sul computer;
- Non seguire i collegamenti Web non richiesti nelle e-mail. Per ulteriori informazioni, fare riferimento alle risorse di phishing presenti su questo sito Web.
- Esporre le connessione Remote Desktop Protocol (RDP) mai direttamente su internet. Qualora si ha necessità di un accesso da internet, il tutto deve essere mediato da una VPN;
- Implementare sistemi di Intrusion Prevention System (IPS) e Web Application Firewall (WAF) come protezione perimetrale a ridosso dei servizi esposti su internet.

Sia gli individui che le organizzazioni sono scoraggiati dal pagare il riscatto, in quanto anche dopo il pagamento le cyber gang possono non rilasciare la chiave di decrittazione oppure le operazioni di ripristino possono subire degli errori e delle inconsistenze.

La sicurezza informatica è una cosa seria e oggi può minare profondamente il business di una azienda. Oggi occorre cambiare mentalità e pensare alla cybersecurity come una parte integrante del business e non pensarci solo dopo che è avvenuto un incidente di sicurezza informatica.