RedHot Cyber

WWW.REDHOTCYBER.COM

La cybersecurity è condivisione.
Riconosci il rischio, combattilo,
condividi le tue esperienze ed
incentiva gli altri a fare meglio di te.

Black Basta: Il Dossier Segreto – Retroscena Inediti di un'Organizzazione Ransomware

DARKLAB
RHC INTELLIGENCE LABORATORY

DakLab è un laboratorio di Intelligence all'interno della vasta community di Red Hot Cyber, specializzato nel monitoraggio delle minacce informatiche. nasce con l'obiettivo di diffondere la conoscenza sulle cyber minacce, contribuendo a rafforzare la consapevolezza e le difese digitali del paese.

DARKLAB COMMUNITY

Dark Lab è una community eterogenea che unisce talenti da vari settori della cybersecurity. I nostri membri includono analisti di minacce, ricercatori, ethical hackers e consulenti di sicurezza, tutti uniti dalla passione per la difesa contro le minacce informatiche. Grazie alla nostra diversità di background e competenze, siamo in grado di affrontare le sfide della cybersecurity da molteplici prospettive.

Pietro Melillo
Esperto di Cyber Threat Intelligence e professore universitario, è il coordinatore del gruppo Dark Lab

Edoardo Faccioli
Esperto di Cyber Threat Intelligence.

Alessio Stefan
Studente magistrale di AI & Cybersecurity e CTF player

Inva Malaj
Appassionata di Cyber Security e Cyber Threat Intelligence

INDEX OF CONTENTS

ABSTRACT

Abstract

Il gruppo ransomware Black Basta è recentemente divenuto il centro dell'attenzione a seguito della pubblicazione di un vasto archivio di oltre 196.000 messaggi interni trapelati dal canale Telegram ExploitWhispers. Questi dati forniscono un'opportunità unica per comprendere il funzionamento interno del gruppo, offrendo dettagli sulla sua struttura gerarchica, le dinamiche organizzative, le strategie di attacco, le tensioni interne e le implicazioni economiche.

Attraverso un'analisi approfondita delle conversazioni interne, questo studio esamina il modus operandi di Black Basta, identificando ruoli chiave, tattiche di intrusione e metodi di monetizzazione. L'indagine evidenzia come il gruppo operi con un'elevata specializzazione, adottando strumenti avanzati come Cobalt Strike, Metasploit e DarkGate, nonché tecniche di social engineering come phishing tramite Microsoft Teams e attacchi brute force su VPN e RDP.

Il leak rivela inoltre le fragilità del gruppo, tra cui conflitti interni, problemi economici e rischi legali derivanti dagli attacchi contro infrastrutture russe, che hanno generato dissidi tra i membri. L'analisi delle transazioni finanziarie mostra un uso sofisticato di criptovalute, tra cui Bitcoin (BTC), Monero (XMR) e Tether (TRC-20), con operazioni di riciclaggio attraverso piattaforme come Binance, Kraken e Bitfinex.

Le informazioni estratte permettono una valutazione dettagliata delle implicazioni per la cybersecurity, fornendo dati preziosi per la threat intelligence e il contrasto alle minacce ransomware. Il report si conclude con una discussione sui possibili sviluppi futuri, inclusa la frammentazione del gruppo, l'assimilazione di alcuni membri in altre organizzazioni cybercriminali (come Lockbit e Akira) e il rischio di una crescente azione repressiva da parte delle forze dell'ordine.

Come Leggere Questo Report

Questo report è strutturato in diverse sezioni che permettono di comprendere a fondo il funzionamento di Black Basta, dalla sua organizzazione interna alle implicazioni operative e strategiche derivanti dal recente leak di informazioni. Ogni sezione si concentra su un aspetto specifico del gruppo, fornendo un'analisi dettagliata basata sulle conversazioni trapelate.

Le sezioni principali del report sono:

Analisi Preliminare: Questa parte introduce i principali dati emersi dal leak, fornendo un contesto generale sulle attività del gruppo e sulle strategie utilizzate per portare avanti le operazioni ransomware.

Analisi Dettagliata del Team e della Leadership: Qui vengono esaminati i ruoli chiave all'interno del gruppo, la gerarchia interna e le dinamiche tra i membri, con particolare attenzione alle tensioni e ai conflitti emersi dalle conversazioni trapelate.

Ipotesi sulla Disgregazione di Black Basta e il Rilevamento della Chat: Questa sezione esplora le motivazioni dietro la possibile dissoluzione del gruppo, considerando sia fattori interni (come dissidi e problemi economici) che fattori esterni (come l'azione delle forze dell'ordine e il rischio di infiltrazioni).

Metodi di Attacco e Tecniche Utilizzate: Una panoramica sulle strategie di compromissione adottate da Black Basta, tra cui phishing, attacchi brute force su VPN e RDP, utilizzo di malware avanzati e strumenti di persistenza.

Movimenti Finanziari e Riciclaggio di Denaro: Analisi delle transazioni in criptovaluta, delle piattaforme utilizzate per il riciclaggio e delle strategie adottate dal gruppo per monetizzare le attività criminali.

Analisi sui Wallet Utilizzati e Movimenti di Denaro: Approfondimento sulle transazioni finanziarie di Black Basta, identificazione dei wallet utilizzati e delle piattaforme di scambio di criptovalute coinvolte nel riciclaggio di fondi.

Evidenze sull'Attacco di Black Basta a Synlab (Aprile-Maggio 2024): analisi delle chat e ricostruzione delle attività nell'attacco contro Synlab, con focus sulle modalità di intrusione e di esfiltrazione dei dati.

L'enigma Dei 28 Milioni Di Dollari Di Riscatto: valutazione delle strategie di negoziazione adottate da Black Basta nei confronti delle vittime e delle somme richieste.

Attacchi di Social Engineering: Le Chiamate al Dipartimento IT: Studio dell'uso delle tecniche di social engineering per ottenere accesso ai sistemi delle vittime attraverso chiamate fraudolente al dipartimento IT.

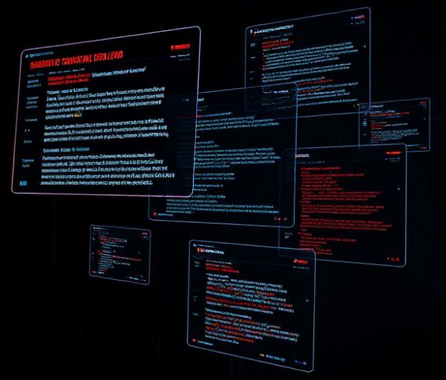
Cosa sta Succedendo Dopo il Leak di Black Basta?: Analisi degli sviluppi successivi alla pubblicazione del leak, inclusa la possibile frammentazione del gruppo e la risposta delle forze dell'ordine.

Implicazioni per la Cybersecurity e Conclusioni: Questa sezione riassume le principali scoperte del report e discute le implicazioni per la threat intelligence, suggerendo possibili contromisure per contrastare gruppi simili in futuro.

ANALISI PRELIMINARE

1. Introduzione

- I gruppi ransomware rappresentano una delle minacce più rilevanti nel panorama della sicurezza informatica. Negli ultimi anni, il fenomeno ha subito un'escalation sia in termini di volume di attacchi sia per l'evoluzione delle tecniche impiegate. Black Basta si è distinto per la sofisticazione delle campagne e per l'ampiezza degli obiettivi colpiti, inclusi settori critici come banche e infrastrutture governative.



- La recente pubblicazione di messaggi interni del gruppo su ExploitWhispers ha reso disponibili informazioni preziose, consentendo di comprendere la composizione gerarchica, le criticità finanziarie, i meccanismi di reclutamento e le strategie di attacco. Questo lavoro presenta un'analisi strutturata di tali contenuti, evidenziando le implicazioni per la cybersecurity e fornendo una panoramica dei possibili sviluppi futuri delle attività del gruppo.

2. Metodologia

L'approccio adottato per la presente analisi si articola in tre fasi principali:

- **Raccolta dei dati:** Sono stati esaminati i messaggi trapelati (oltre 196.000) provenienti dal canale Telegram ExploitWhispers. I dati sono stati raccolti in un database testuale, rimuovendo duplicati e spam.
- **Elaborazione e categorizzazione:** I messaggi sono stati analizzati utilizzando tecniche di text mining e suddivisi in categorie tematiche (ruoli nel gruppo, modalità di attacco, conflitti interni, etc.). Eventuali elementi tecnici (e.g. indirizzi IP, credenziali di accesso) sono stati isolati per valutazioni di cyber threat intelligence.
- **Interpretazione:** I risultati sono stati confrontati con fonti di intelligence aperta (ad es. VX Underground e segnalazioni di PRODAFT) per validarne la credibilità e contestualizzarli all'interno del panorama ransomware globale.

3. Risultati dell'Analisi

3.1. Struttura Organizzativa e Ruoli Chiave

Dallo studio dei messaggi emergono diverse figure centrali:

- **Lapa:** Amministratore principale, sottoposto a forti pressioni interne e compensato meno rispetto ai colleghi.
- **Cortes:** Presunto ex membro del gruppo Qakbot, contrario agli attacchi contro banche russe per timore di ripercussioni legali.
- **YY:** Amministratore con responsabilità strategiche nella gestione delle infrastrutture compromesse.
- **Trump e Bio (Pumba):** Entrambi ex membri del gruppo Conti; Bio è stato arrestato e poi rilasciato, ora in condizioni finanziarie precarie e sotto sorveglianza.

Le dinamiche interne evidenziano tensioni crescenti, soprattutto di natura economica. Il rischio di frammentazione del gruppo è alto, con possibili scenari di riorganizzazione sotto altri nomi o dispersione dei membri in ulteriori gruppi ransomware.

3.2. Attacchi alle Banche Russe e Reazione delle Autorità

Uno degli elementi di maggiore rilevanza riguarda gli attacchi contro infrastrutture bancarie russe:

- Gli attacchi sono stati eseguiti tramite bruteforce di sistemi critici. Alcuni membri (come Cortes) hanno espresso disaccordo, preferendo evitare bersagli russi per non attirare l'attenzione delle autorità nazionali.
- La risposta ufficiale da parte delle istituzioni russe non è stata divulgata, ma i messaggi trapelati lasciano intendere l'avvio di indagini in corso.

La decisione di violare il tacito "codice di non aggressione" verso entità russe potrebbe aver innescato ripercussioni legali e intensificato le tensioni interne al gruppo.

3.3. Indicatori Tecnici: IP Compromessi e Accessi ai Server

Dall'analisi delle chat emergono anche dettagli tecnici fondamentali per le attività di cyber threat intelligence:

```
makefile
CopiaModifica

IP: 194.26.29.188
User: root
Pass: rH5a2f*yIMI@>–^

IP: 45.141.87.189
User: root
Pass: mc5_}4!821N/Tyb

IP: 194.26.25.111
User: root
Pass: )xvMZg48n6bX}5A
```

La disponibilità di tali credenziali rappresenta un'opportunità importante per gli analisti di sicurezza. Le infrastrutture identificate possono essere messe sotto monitoraggio, consentendo di migliorare le strategie di difesa e di mitigazione degli attacchi.

Queste sono solo alcune delle macchine trovate all'interno delle chat trapelate, ma sembra che sotto il servizio di hosting russo Media Land LLC, con ASN AS206728, Black Basta avesse costruito una vera e propria infrastruttura dedicata alle attività di brute force. Inoltre, si trattava di un'infrastruttura di rete che comportava costi elevati per il gruppo, tanto che all'interno delle chat sono presenti discussioni su come ottimizzare i costi, ridurre i consumi di rete e migliorare le performance hardware.

3.4. L'Arresto di Bio

Uno dei passaggi più significativi del leak è il messaggio in cui Bio (noto anche come Pumba) riferisce di essere stato arrestato e successivamente rilasciato. Secondo la sua testimonianza, le forze dell'ordine hanno confiscato beni personali, e Bio rimane sotto sorveglianza. Non è chiaro se l'operazione sia stata condotta da autorità russe o internazionali; si ipotizza che egli possa essere stato costretto a collaborare con le autorità.

3.5. Nuove Evidenze: VX Underground e Altre Fonti

Ulteriori elementi di interesse sono emersi incrociando i dati con le segnalazioni di VX Underground e PRODAFT:

- Diffidenza verso il gruppo Lockbit, considerato "inaffidabile" e potenzialmente incline a truffare gli affiliati.
- Rifiuto di un'offerta di fusione da parte del gruppo DISPOSESSOR per sospetti di infiltrazione.

- Presenza di affiliati molto giovani (età 17 anni), segno di un crescente coinvolgimento di minori nelle attività cybercriminali.
- Investimenti mirati nello sfruttamento di vulnerabilità VPN, al fine di ottenere accessi non autorizzati a reti aziendali.
- Tecniche di social engineering avanzate, con la presenza di un operatore dedicato (Nur) specializzato nel contatto di personale chiave nelle aziende vittime.
- Legami con i gruppi ransomware Cactus e Akira, con possibili ipotesi di riorganizzazione post-Black Basta in questi due gruppi dopo il malcontento all'interno di un luogo di lavoro altamente tossico con presenza di abusi verbali e mancati pagamenti.

4. Discussione e Implicazioni per la Cybersecurity

La pubblicazione del leak offre un raro scorcio sulle dinamiche interne di un gruppo ransomware, svelando non solo l'apparato tecnico ma anche i rapporti di potere, le dispute economiche e i timori legali che influenzano le strategie criminali.

1. **Frammentazione e riorganizzazione**: Le tensioni interne suggeriscono una possibile scissione. È plausibile che alcuni membri confluiscano in altri gruppi (Lockbit, Akira, Cactus) o che formino nuove entità.

2. **Impatto sulla threat intelligence:** La disponibilità di credenziali, IP e tecniche di attacco consente alle organizzazioni di migliorare il proprio threat hunting, aggiornare gli indicatori di compromissione (IoC) e rafforzare le difese.

3. **Risposte delle forze dell'ordine**: L'arresto di Bio e la probabile apertura di indagini sulle operazioni contro banche russe dimostrano una crescente attenzione investigativa. Non è da escludere un intervento coordinato a livello internazionale.

4. **Evoluzione dei gruppi ransomware:** I legami tra Black Basta e altre organizzazioni mostrano come l'ecosistema ransomware sia fluido e in costante evoluzione. Le conoscenze apprese da un singolo gruppo possono rapidamente migrare altrove, contribuendo allo sviluppo di nuove campagne di attacco.

5. Aspetti Tecnici

BlackBasta mostra, nelle chat, una buona coordinazione ed organizzazione degli attacchi. Il gruppo tende ad essere molto cauto nelle prime fasi di attacco arrivando persino ad eseguire un singolo comando al giorno. Durante alcune operazioni il gruppo si tende a dividere in team con diversi obiettivi sulle stesse vittime, inoltre il gruppo tende a lavorare su più vittime al giorno (circa 5).

Nelle prime fasi della chat notiamo una discussione su un rinnovamento della loro infrastruttura, in particolare quella per l'accesso iniziale con un forte utilizzo di JavaScript e del protocollo WebDAV/FileZilla per trasferimento file. Un altro metodo utilizzato è il phishing tramite Microsoft Teams, il gruppo sembrerebbe avere un pretext "standard" da inviare ad una serie di contatti con installazione di default (che quindi permette di ricevere messaggi anche fuori dalla propria organizzazione). Il gruppo disincentiva fortemente di focalizzarsi su organizzazioni che implementano il 2FA sottolineando come questa semplice pratica sia un forte repellente per gli attaccanti.

Gli step per questa metodologia di Initial Access sono i seguenti:

- Invio del messaggio
- Accettazione del messaggio da parte della vittima
- Download del file PDF
- Click su link per installazione file .MSI (signed)
- Esecuzione del .MSI

Gli attacchi tramite Microsoft Teams vengono inviati in massa in maniera tale da avere più probabilità di successo su vittime che eseguono la killchain nella sua completezza. All'interno del gruppo è presente scetticismo riguardo l'efficienza di tale approccio notando però come determinate regioni (eg:/ regione pacifico-orientale) sia più vulnerabile a questa procedura.

Rimanendo in tema di regioni, BlackBasta porta la concentrazione su specifiche regioni (eg:/ regione Europea) in diversi giorni, l'intero team inizia a lavorare con diverse tecniche di ricognizione, collezione di informazioni e informazioni sulle organizzazioni trovate per poi iniziare le fasi di accesso iniziale. In una di queste fasi (non è chiaro esattamente con quale metodologia) mentre si stava focalizzando gli attacchi sull'Europa, in una sola manche di phishing ben 5 vittime italiane diverse sono state compromesse con successo portando il gruppo ad iniziare le attività di enumeration (11 vittime in totale su circa 1000 tentativi di phishing, 4 francesi, 2 tedesche). Tra la chat ottenute si può notare un uso massiccio di Cobalt Strike e Meterpeter/Metasploit nelle loro operazioni, indipendentemente dalle vittime le fasi di enumeration rimangono uguali con primo step l'identificazione dell'organizzazione impattata. In un caso il gruppo è riuscito ad ottenere una copia piratata di Brutel Ratel C4.

Parte del team utilizza Mulvad come VPN prima di connettersi a qualsiasi macchina della loro infrastruttura, nel mese di Ottobre uno server C2 di BlackBasta è stato individuato da forze dell'ordine tedesche che hanno inviato una richiesta di informazioni. Nel gruppo di discuteva come tale evento potesse avere delle ripercussioni negative sul gruppo ma il responsabile di tale macchina ha rassicurato che non si connetteva mai direttamente e che aveva preso delle precauzioni per poter mascherare il suo IP durante le operazioni. Sotto consiglio di altri membri, tale individuo ha poi cambiato gestore di VPN.
Tra i principali tool utilizzati abbiamo anche DarkGate utilizzato come dropper per i beacon di Cobalt Strike sulle macchine delle vittime, ottenuto tramite abbonamento (MaaS). In uno degli attacchi il gruppo ha avuto la necessità di rendere offline i Domain Controller e per evitare la detection hanno inviato una finta email di servizio all'interno della azienda fingendo il tutto come una procedura di supporto tecnico interno.

6. Conclusioni

L'analisi delle chat trapelate fornisce elementi di grande valore per comprendere le dinamiche interne di Black Basta e, più in generale, il modus operandi dei gruppi ransomware.

Tra i punti di maggiore rilievo si evidenziano:
Tensioni interne e potenziale dissoluzione: Il gruppo sembra attraversare una fase di instabilità organizzativa che potrebbe condurre a una cessazione delle attività o a una riorganizzazione sotto nuove sigle.

Rischi di escalation legale: Gli attacchi contro banche russe potrebbero intensificare la reazione delle autorità, aumentando la probabilità di arresti o di interventi repressivi mirati.

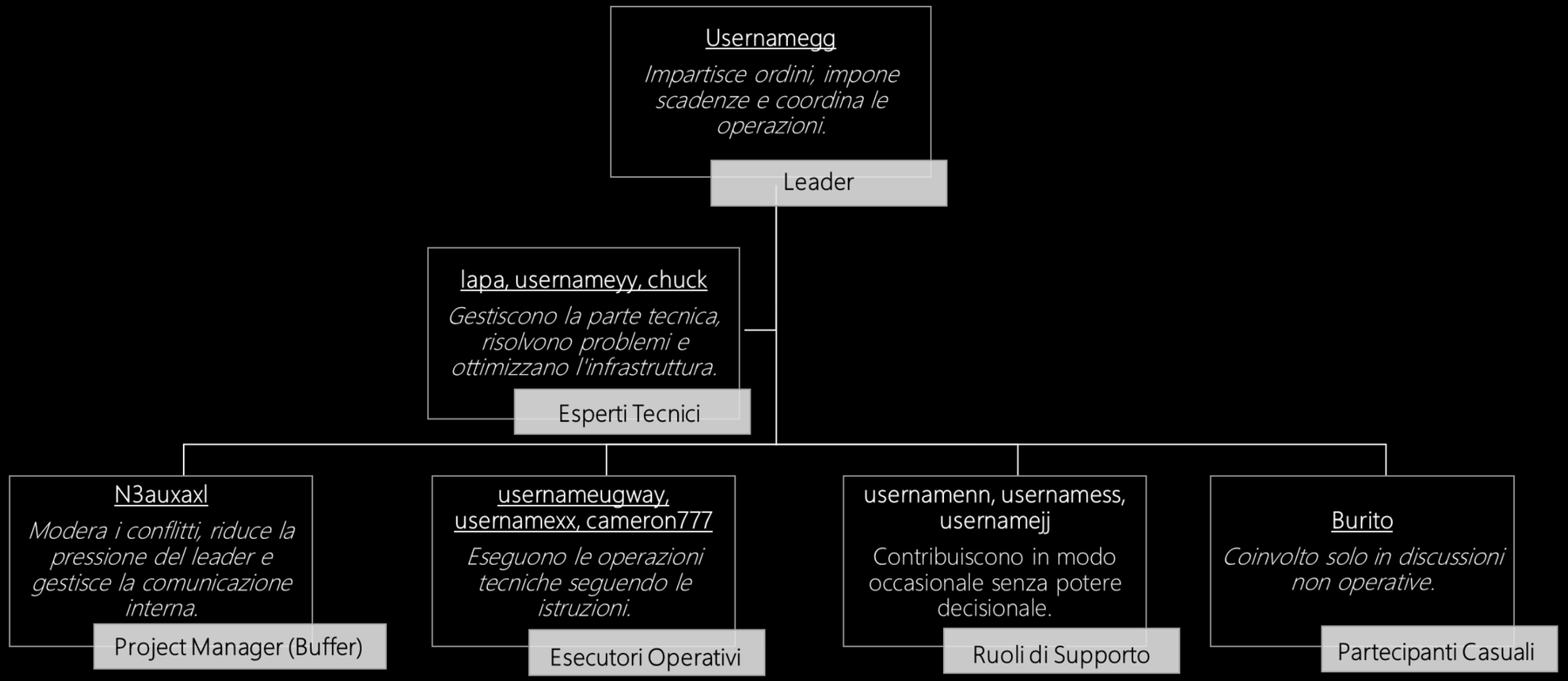
Opportunità di intelligence: Le informazioni contenute nel leak (IP, credenziali, metodi di intrusione, strutture gerarchiche) offrono una base concreta per migliorare le strategie difensive a livello aziendale e governativo.

È auspicabile un costante monitoraggio di ulteriori pubblicazioni e delle mosse dei principali gruppi affiliati (Lockbit, Akira, Cactus), al fine di prevenire e contrastare efficacemente le minacce ransomware.

ANALISI DETTAGLIATA DEL TEAM E DELLA LEADERSHIP

Struttura del Team

La gerarchia è rigida e ben strutturata



La gerarchia è rigida e ben strutturata: Analisi della Leadership: Come usernamegg Gestisce il Gruppo.

Dall'analisi dei messaggi emerge che usernamegg opera in modo gerarchico, impartendo ordini, imponendo scadenze e monitorando attentamente l'esecuzione. Non è aperto a negoziazioni; si aspetta "impegno e massima efficienza". Esprime frequentemente "insoddisfazione" quando il team non rispetta le scadenze.

Esempi:

Ты знал это еще неделю назад.

Я всех подгоню под это время.

Ну как сейчас это полная хуета.

Все этого парня я пиздец как боюсь.

Lo sapevi già una settimana fa.

Radunerò tutti per quest'ora.

Beh, adesso è una completa merda.

Di questo ragazzo ho una fottuta paura.

Clima del Team: Stress, Efficienza e Paura del Fallimento

L'ambiente di lavoro è caratterizzato da un'alta pressione sul risultato, il team lavora con un'urgenza costante e gli errori non sono tollerati.

Le principali attività del team includono:

Tipo di Operazione	Evidenze dal Chat Log	Utenti Coinvolti
Sfruttamento delle Reti	Discussioni su proxy SOCKS, bot e accessi remoti.	chuck, cameron777
Gestione delle Credenziali	Menzioni di login e credenziali di accesso.	usernamegg, lapa
Configurazione dell'Infrastruttura	Setup di server, RDP e testing.	usernameyy, usernamexx
Distribuzione di Malware	Utilizzo di script VBS e tool automatizzati.	usernamegg, lapa
Coordinazione Operativa	Gestione di scadenze e monitoraggio delle attività.	usernamegg, n3auxaxl

Momenti di Maggior Tensione nel Chat Log

I momenti di maggiore conflitto e pressione includono:

Data	Evento	Livello di Tensione
30 gennaio 2024	Ritardo su una scadenza critica, leader furioso.	**Alta**
1 marzo 2024	Problemi tecnici nell'infrastruttura, discussioni accese.	**Media**
22 aprile 2024	Preoccupazioni sulla sicurezza e rischio di esposizione.	**Media**
3 giugno 2024	Inefficienze di rete che causano ritardi operativi.	**Alta**

Conclusioni Finali

La struttura gerarchica rigida porta ad una gestione del gruppo in modo autoritario, generando un clima lavorativo tossico caratterizzato da: elevato stress, aspettative irrealistiche, e tensioni costanti. Si può evidenziare una inefficienza nelle operazioni: i problemi vengono risolti solo dopo che si verificano, denotando una mancanza di pianificazione e organizzazione. invece di essere prevenuti.

Ipotesi sulla Disgregazione di Black Basta e il Rilevamento della Chat

Sulla base dell'analisi delle chat interne e dei pattern operativi del gruppo, possiamo formulare alcune ipotesi su ciò che ha portato alla disgregazione di Black Basta e al rilevamento delle loro comunicazioni. Non è stata un'unica causa, ma probabilmente un insieme di fattori interni ed esterni.

Esempi:

@usernamegg: matrix.bestflowers247.online
ну как сейчас это полная хуета

@usernamegg:matrix.bestflowers247.online
я давно хожу с мыслями о том что так работать не должно

Conflitti interni e malcontento tra i membri, l'ipotesi di un insider che ha tradito il gruppo

Come evidenziato nella nostra analisi precedente, ci sono stati chiari segnali di tensioni interne e frustrazione tra i membri del gruppo. Questi conflitti possono essere stati determinanti per la loro caduta. Si evidenziano continui dissapori e messaggi che criticano il lavoro degli altri.

@usernamegg: matrix.bestflowers247.online
Beh, adesso è una totale schifezza

@usernamegg:matrix.bestflowers247.online
È da un po' che mi gira in testa l'idea che così non dovrebbe funzionare

Non si può escludere che, col tempo, si sia creata una certa sfiducia tra i membri, magari accompagnata da visioni contrastanti sugli obiettivi e le strategie da adottare. Se così fosse, la conseguenza più plausibile potrebbe essere un insider che abbia scelto di tradire il gruppo, passando informazioni alle autorità o a qualche team di cybersecurity.

Ci sono molte indicazioni che suggeriscono che un insider possa aver tradito il gruppo:

- troppe lamentele tra i membri
- discussioni pubbliche su errori tecnici
- alcuni membri sembrano non fidarsi tra loro

Analisi Su I Wallet Utilizzati E Movimenti Di Denaro

Analisi Su I Wallet Utilizzati E Movimenti Di Denaro

I principali movimenti di criptovalute su differenti wallet sono stati effettuati sulle blockchain BTC (Bitcoin), XMR (Monero) ed ETH (Ethereum). Inoltre, dall'analisi delle chat, è emerso anche l'utilizzo di TRON (TRC-20), spesso impiegato dal cybercrime per trasferire ingenti somme di denaro a costi di commissione ridotti.

La blockchain TRC-20, ancora poco controllata e con strumenti di analisi limitati, ha favorito una sua significativa diffusione negli ambienti criminali.

Bitcoin (BTC) Wallets
• bc1qfn6vndc6mhlvvtx54ehyq7z6vel8kkctj0e0sa • bc1qvwntvw5sxtsavaya85up958pjn2eysaqcflffe • bc1qn0z8etys62cljzwjxl80k9y5nag7pq42s9lyes • bc1qsvukyqlpxpnzhedsxeyp7mmza3d9c43fslvs5e • bc1qyu9vwxthn2s0zhe8rqae5m2mg0w7lct3fxkk96 • bc1qj8k6hx9xz2rv5usvt4r2fs5agyudhr5uzxcle8 • bc1qyvaa2uwwgf34m3qggzmptcrm45tppfppyhhhde

Monero (XMR):
• 84JskFBoUddXz1bUn329NeSLw7rfxZkbJiQN7eJdtkDvZDHTPMvHEJkDGNaW47sQfC9jaQ4EDFkgxGJxof4uEgonCdY2HnK • 88M7PZfDZSs3DWB6BY99uKVcnSFAsHr6eEhPmBD2psSyU6hv4EHYB6cGjpysZwEbQKTHCz3JfsiWMZLiDMoZZMSKQddFS66 • 86e6VhUFFHdZDrm4QJHag915m4zGxuXsi3UAyGpTDsPR4CLCnvmJ7zzanmx7Q7KJg846ZrmT911TBEMAZQq24Kqn2xpPqVZ

Ethereum (ETH):
• 0x010165F27A933Ac77534Ee72CE58550dC241AB16 • 0x2b48f85312a7e6F952A773e1234cB340FD472D9e

Tether (USDT – TRC-20):
• TCws332kET8czTuhcBemmmeSrCbTDb2nyD • TNgjeQgr8dPSwK2UkhFtNpGK795cJ3yKjL

Movimenti, riciclaggio e guadagni

Inoltre, dalle analisi effettuate, possiamo evidenziare che i movimenti di denaro erano molteplici, sia per quanto riguarda i guadagni ottenuti dalle loro attività illecite, sia per le spese sostenute per il mantenimento dell'infrastruttura utilizzata.

All'interno delle chat sono presenti messaggi come il seguente:

Я создал щас ETH кошель, можешь на него закинуть баксов 500, что бы ночью было чем платить челу который найдется.	Ho appena creato un wallet ETH, puoi inviarmi 500$ così stanotte avrò i fondi per pagare il tizio che troveremo?

Che fa pensare anche a un reclutamento temporaneo di alcuni individui dedicati a svolgere alcune mansioni. Inoltre sembrerebbe che abbiano persone dedicate al riciclaggio di denaro come si può dedurre da questo messaggio:

у меня есть кому мыть. ахуеешь мыть такой объем сам	Ho persone che si occupano del lavaggio. Tu impazziresti a lavare un volume del genere da solo.

Alcuni messaggi parlano dei riscatti richiesti che raggiungono somme anche molto significative, ecco un esempio:

1750 мы предложили а они предложили миллион	Abbiamo proposto 1.750.000$, ma loro hanno offerto un milione

E, infine, è presente anche un messaggio che riporta alcune query, probabilmente eseguite sul database utilizzato per registrare l'intero bilancio. Queste query mostrano i valori delle somme delle transazioni ricevute in diverse criptovalute, come Bitcoin e Litecoin. Il valore riportato è il seguente:

```
SELECT SUM(amount_received) amount_received from bitcoin_bitcoinpayment;
38372.14453684 BTC

SELECT SUM(amount_received) amount_received from litecoin_litecoinpayment;
51592.82979973 LTC

SELECT SUM(balance) balance from userprofile_user; 630735.1433867989 USDT
```

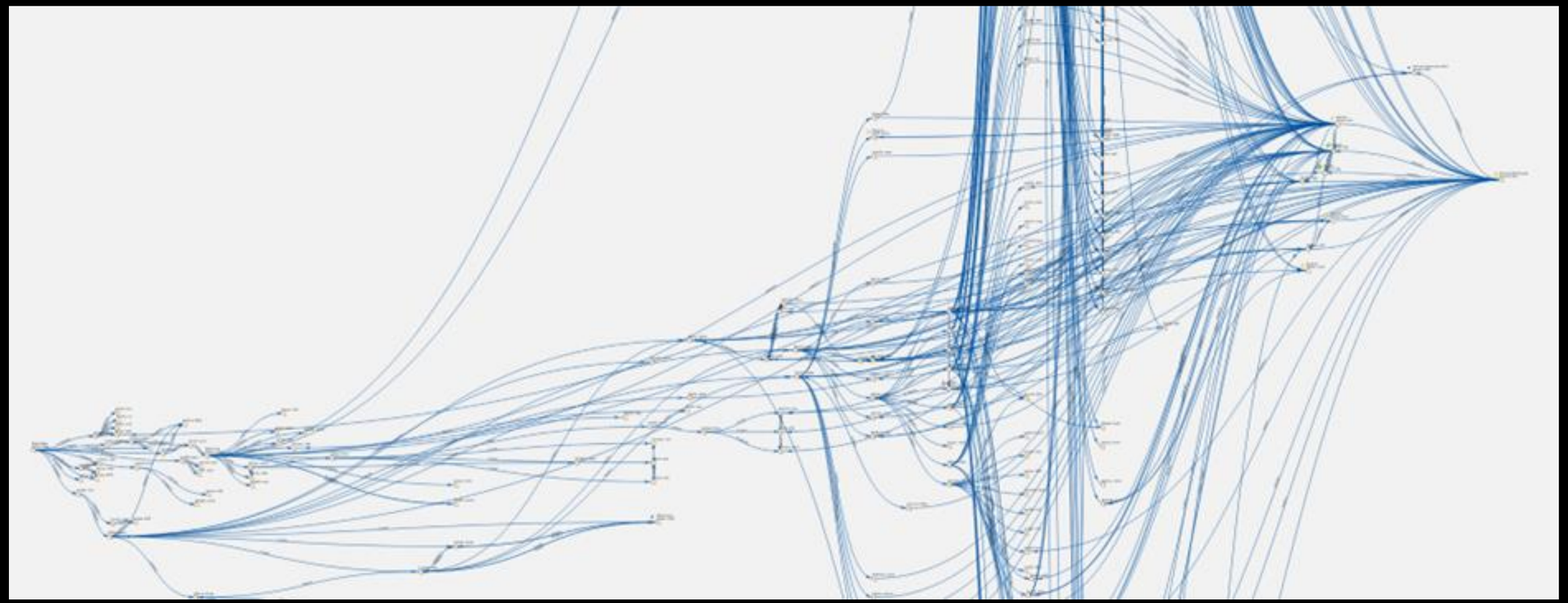
Tutto questo insieme di comunicazioni lascia dedurre che BlackBasta, come molti altri gruppi ransomware altamente strutturati, abbia sviluppato un'infrastruttura di gestione del denaro molto sofisticata, in grado di far fronte a:

- Guadagni enormi provenienti dai riscatti
- Negoziazioni aggressive per accelerare i pagamenti
- Spese operative significative per hardware, collaboratori e servizi di riciclaggio
- Metodi di riciclaggio evoluti per garantire l'anonimato e la liquidità

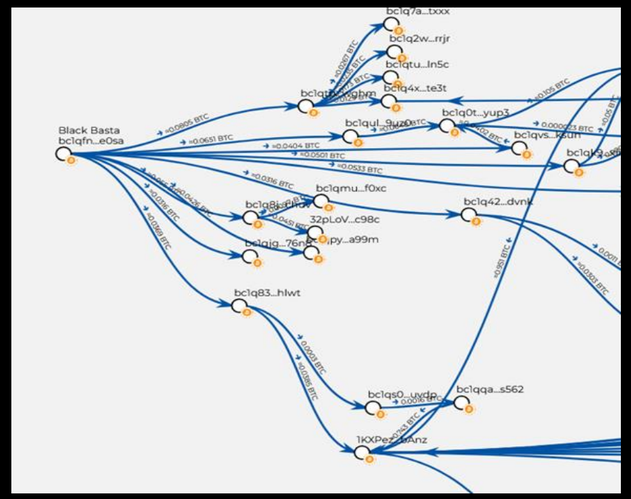
Questa infrastruttura è fondamentale per la sostenibilità e l'efficacia delle operazioni illecite del gruppo, permettendo loro di gestire flussi finanziari complessi e di adattarsi rapidamente a nuovi scenari.

Analisi dei movimenti cripto collegati ai wallet trovati all'interno delle Chat

Analizzando i flussi di denaro generati da un indirizzo wallet trovato all'interno delle chat, in particolare l'indirizzo BTC: bc1qfn6vndc6mhlvvtx54ehyq7z6vel8kkctj0e0sa, si nota immediatamente un'elevata quantità di transazioni e spostamenti di fondi tra numerosi portafogli.

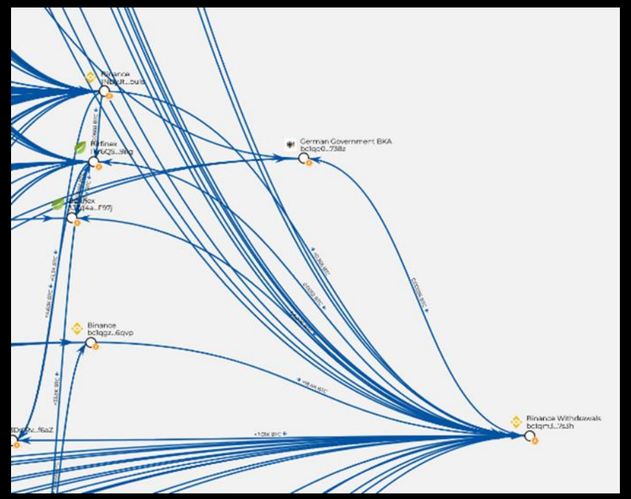


Dall'immagine seguente emerge come BlackBasta frammenti il denaro su diversi wallet, una pratica volta a rendere più complessa l'analisi delle transazioni.



Ciò che rende particolarmente interessante questo insieme di transazioni è il fatto che la maggior parte del denaro movimentato dai wallet individuati seguendo i flussi finanziari sembra confluire principalmente in due exchange: Binance e Bitfinex, entrambi già segnalati come "Bitcoin Abuse."

Provando a seguire altri wallet anche di blockchain differenti come etherium si nota che gli strumenti DeFi i più utilizzati sono:



- Kraken
- Binance
- Bitfinex
- FixedFloat
- Switchcain

Questi sono tutti strumenti che grazie al loro poco controllo e ai servizi di scambio offerti fanno gola a criminali come BlackBast per poter riciclare e prelevare in sicurezza le loro criptovalute.

Evidenze sull'Attacco di Black Basta a Synlab (Aprile-Maggio 2024)

Nel periodo Aprile-Maggio 2024, il gruppo ransomware Black Basta ha condotto un attacco mirato contro Synlab, una delle più grandi aziende europee di diagnostica medica. L'attacco ha portato alla crittografia dei sistemi e all'esfiltrazione di oltre 1,5 terabyte di dati sensibili. Il gruppo ha poi minacciato di rendere pubbliche le informazioni rubate, se il riscatto non fosse stato pagato.

Dai log della chat il primo messaggio relativo a questo attacco appare il 15 aprile da parte dell'utente usernamezz.

```
timestamp: 2024-04-15 19:55:46,
chat_id:
!nRvudzmlyqjkcSxYzO:matrix.bestflowers247.online,
sender_alias:
@usernamezz:matrix.bestflowers247.online,
message: `www.synlab.com`
```

Il 16 aprile un messaggio interessante può far pensare ad un accesso pubblico sfruttato per l'accesso remoto alla rete.

```
chat_id:
!nPsXVNwvPnfPbfsDcD:matrix.bestflowers247.online,
sender_alias:
@usernamegg:matrix.bestflowers247.online,
timestamp: 2024-04-16 10:53:18
message: synlab https://5.97.70.2:443 Default [
XXXXXXXXX
```

Nelle ore e nei giorni successivi vengono scambiati moltissimi messaggi con dump di tutto lo schema di Active Direcorrty con relativi utente e password. Vengono menzionate delle VPS (Virtual Private Server) e molto altro.

Poi si arriva al 4 maggio 2024 quando l'utente usernamegg dichiara che synlab.com è pubblicato! Data effettiva di rivendicazione sul Data Leak Site di Black Basta. Dal 4 maggio parte il countdown di 7 giorni che porterà poi alla pubblicazione dei dati l'11 maggio 2024.

timestamp: 2024-05-04 11:20:50,
chat_id:
!kXjWEDtqiVBjWINNxZ:matrix.bestflowers247.online,
sender_alias:
@usernamegg:matrix.bestflowers247.online,
message:synlab.com - опубликовал

Il 21 maggio, ben oltre la data di pubblicazione dei dati, accade qualcosa di strano che non riusciamo a capire ma possiamo fare delle ipotesi. Viene postato un messaggio sempre da parte dell'utente usernamegg che esprime entusiasmo per il leak eseguito e la grande quantità di dati. Chiede anche di fare un upload della struttura dei file e directory per "così da poter scaricare solo i dati di suo interesse". Si lamenta inoltre di come i file erano organizzati all'interno della rete.

Da questo messaggio possiamo ipotizzare che i dati siano di interesse di altri e quindi ci possa essere un mercato parallelo? Dal 21 maggio in poi non troviamo più nessuna evidenza dell'evoluzione.

chat_id:
!nPsXVNwvPnfPbfsDcD:matrix.bestflowers247.online,
sender_alias:
@usernamegg:matrix.bestflowers247.online,
timestamp: 2024-05-21 09:47:26
message: "Hi guys, the synlab leak is fireee, thanks for sharing it. can you upload a file tree with folder paths? so I can download only the files I am interested cause the leak is huge and synlab workers keep the files like shit. thanks boys, keep it cool"

Conseguenze e Impatti dell'attacco

Sistemi IT bloccati con impossibilità di accedere a strumenti critici per le analisi diagnostiche. Interruzione delle operazioni cliniche, causando ritardi nella gestione dei pazienti. Necessità di ripristinare i sistemi da backup, se disponibili e non compromessi dal ransomware.

Conclusione

L'attacco di Black Basta a Synlab è stato un esempio di ransomware moderno basato su double extortion, con una combinazione di esfiltrazione dati, crittografia dei sistemi e minacce di esposizione pubblica.

L’enigma dei 28 milioni di dollari di riscatto

Hello, We are Black Basta Syndicate. We were able to access you local networks and encrypt as well as exfiltrate data.
As a result, we've downloaded over 1.5 Tb of sensitive information and data from your network.
Right now we are keeping everything confidential and are making sure that only you and us know about this incident.
However, if we will not able come to an agreement within 10 days, all of your data will be posted on our news board.

In case you do not pay, this data exposure and our own efforts will lead to other bad entities being able to connect to your network and end up attacking you and your customers.
The price to resolve this situation is **$28,720,000 USD**. In case of successful negotiations we guarantee you will get:

1) Decryptor for all your Windows.
2) Non recoverable removal of all downloaded data from our side, as well as any other sources (in other words you will get your data back and nobody else will have access to it).
3) Security report on how you were hacked to fix your vulnerabilities and avoid such situations in future.
4) A guarantee from us that neither us nor our allies will ever target you again.

Hope you can correctly assess the risks for your company and make a right decision.
You can find more information about Black Basta syndicate in Google.

In questa sezione del report cerchiamo di fornire un'analisi delle negoziazioni di riscatto. L'analisi include dettagli su richieste di riscatto, strategie di pressione, aziende colpite e possibili controfferte da parte delle vittime.
Uno dei casi più significativi riguarda una richiesta di $28.720.000 USD avanzata nei confronti di una vittima. Il messaggio inviato da Black Basta contiene minacce di pubblicazione dei dati rubati se il riscatto non viene pagato entro 10 giorni. La richiesta include anche un decryptor e la garanzia che i dati rubati verranno eliminati dopo il pagamento.

Black Basta utilizza diverse strategie per forzare il pagamento, tra cui:

- presentarsi come 'businessmen' per giustificare il riscatto.
- minacce di divulgazione dei dati
- enfasi sui costi operativi giornalieri derivanti dal downtime.

> If you do not pay, this data exposure and our own efforts will lead to other bad entities being able to connect to your network and end up attacking you and your customers.

Alcune vittime cercano di negoziare offerte inferiori al riscatto richiesto. In un caso specifico, una vittima ha dichiarato che le proprie compagnie assicurative si sono rifiutate di pagare il riscatto e ha offerto solo $125.000 USD invece della somma richiesta.

> We are also running out of options. All our insurance companies have refused to pay any ransom.
> The second lender has turned us down. They said we are 'damaged goods' because some of our confidential data has been made public.
> All we can pay now is $125,000. We have told you honestly what we can pay. We are not bluffing.

Black Basta ha respinto l'offerta, affermando che non accetteranno riduzioni significative del riscatto e che chiunque tenti di abbassare il pagamento sarà considerato un 'ostacolo alla conclusione dell'accordo'.

Aziende colpite e possibili vittime

Diversi nomi di aziende sono emersi durante l'analisi dei messaggi di Black Basta, tra cui:

- DYWIDAG-Systems International USA
- Nuclear Waste Management Organization (NWMO)
- Hanson Bridgett LLP
- Trade-Mark Industrial Inc.
- Volex

Dall'analisi emerge che Black Basta utilizza una combinazione di minacce, pressione psicologica e rigidità nelle trattative.
Nelle chat del gruppo emergono moltissime aziende ed enti governativi vittime di Black BAsta ma non ci sono prove definitive di abbia ricevuto la richiesta di riscatto da $28.720.000 USD.

Attacchi di social engineering: le chiamate al Dipartimento IT.

Black Basta utilizza tecniche avanzate di social engineering, tra cui l'impersonificazione del dipartimento IT, per ottenere accesso ai sistemi delle vittime. In questa sezione del report analizziamo i messaggi intercettati nel dataset e cerchiamo di capire come questa tecnica viene utilizzata nei loro attacchi.

2024-06-03 18:10:02 - @usernamegg
Messaggio: можно сделать что бы звонок проходил от it департамента?
2024-06-03 18:10:12 - @usernameugway
Messaggio: да, сейчас как раз делаем
2024-06-03 18:10:15 - @usernameugway
Messaggio: скину скрины что получится
2024-06-03 18:13:32 - @usernameugway
Messaggio: да пока звоним на доступы которые у нас есть, проверить идет ли дозвон
2024-06-03 18:13:44 - @usernameugway
Messaggio: сначала разбирались как позвонить еще..
2024-06-03 18:13:49 - @usernameugway
Messaggio: тоже не сразу получилось
2024-06-03 18:14:21 - @usernameugway
Messaggio: сейчас под тестовый прозвон через кол центр подговлю аки тоже, надо с ними сработаться

2024-06-03 18:10:02 - @usernamegg
Messaggio: Può essere fatta una chiamata che sembri provenire dal dipartimento IT?
2024-06-03 18:10:12 - @usernameugway
Messaggio: Sì, lo stiamo facendo proprio ora.
2024-06-03 18:10:15 - @usernameugway
Messaggio: Ti invierò screenshot di come risulterà.
2024-06-03 18:13:32 - @usernameugway
Messaggio: Sì, stiamo chiamando gli accessi che abbiamo per verificare se la chiamata va a buon fine.
2024-06-03 18:13:44 - @usernameugway
Messaggio: Prima abbiamo dovuto capire come effettuare la chiamata...
2024-06-03 18:13:49 - @usernameugway
Messaggio: Non è andata subito a buon fine.
2024-06-03 18:14:21 - @usernameugway
Messaggio: Ora sto preparando chiamate di test attraverso il call center, dobbiamo coordinarci con loro.

Interpretazione dei Messaggi

Questi messaggi indicano che Black Basta utilizza l'impersonificazione del dipartimento IT per manipolare gli impiegati e ottenere accesso ai sistemi interni. Le strategie principali includono:

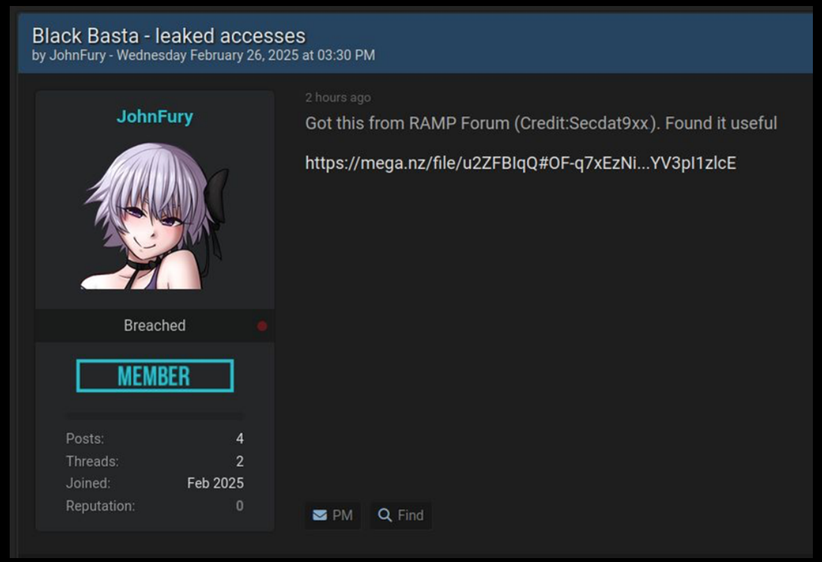
- preparare chiamate che sembrino provenire dall'IT per ottenere credenziali o accesso remoto
- testare attivamente l'efficacia di queste chiamate per migliorare la loro credibilità
- usare un call center per gestire più chiamate e rendere la truffa più convincente
- verificare se le chiamate vengono ricevute e migliorare i metodi per renderle più efficaci

Conclusione

Black Basta utilizza avanzate tecniche di social engineering per sfruttare la fiducia degli impiegati e ottenere accesso a sistemi aziendali. Il loro uso di chiamate false da parte del dipartimento IT indica un alto livello di organizzazione e adattabilità alle difese di sicurezza moderne.

Cosa succede dopo il leak di Black Basta?

Gli avvoltoi si avventano sulla carcassa. Il 26 febbraio 2025, sul noto forum underground *BreachForums*, un utente con lo pseudonimo *JohnFury* ha pubblicato un post intitolato *"Black Basta - Leaked Access"*. *JohnFury* afferma di aver recuperato, da un altro altrettanto noto forum underground, *RAMP* (ringraziando l'utente *Secdat9xx*), un file che rende disponibile gratuitamente per il download.



Cosa contiene il file trapelato?

Dopo averlo analizzato, possiamo confermare che si tratta di un file di testo contenente migliaia di accessi a portali VPN, con relativi nomi utente e password in chiaro. Questo tipo di informazione è estremamente sensibile, poiché un accesso VPN compromesso può consentire a un attaccante di infiltrarsi direttamente nelle reti aziendali senza dover sfruttare vulnerabilità nei sistemi.

Tuttavia, restano molte domande aperte:
- si tratta di una delle armi dell'arsenale interno di Black Basta esfiltrato insieme alle chat?
- è un semplice database costruito raccogliendo credenziali rubate attraverso infostealer e poi organizzato per apparire come un leak autentico?

Se il file trapelato fosse effettivamente stato utilizzato da Black Basta, significherebbe che le credenziali compromesse potrebbero essere state usate in attacchi precedenti e potrebbero ancora essere valide.
Il leak di Black Basta, reale o meno, dimostra ancora una volta la pericolosità delle informazioni rubate e condivise nei forum underground.

CONCLUSIONI GENERALI

L'analisi del leak di Black Basta evidenzia con chiarezza la fragilità intrinseca dei gruppi ransomware, i quali, nonostante un'organizzazione apparentemente strutturata, sono spesso afflitti da instabilità interna, conflitti di leadership e problematiche logistiche. L'utilizzo di infrastrutture compromesse, tecniche di attacco non sempre efficienti e la dipendenza da strumenti di terze parti hanno reso Black Basta vulnerabile a una potenziale infiltrazione e disgregazione.

Dal punto di vista della threat intelligence, il leak fornisce un'opportunità senza precedenti per comprendere le dinamiche interne dei gruppi ransomware, aggiornare gli indicatori di compromissione (IoC) e rafforzare le strategie difensive a livello enterprise. Le informazioni trapelate evidenziano il crescente utilizzo di tecniche di social engineering avanzate, l'integrazione di strumenti di attacco automatizzati e l'impiego di schemi finanziari sofisticati per il riciclaggio di denaro.

Guardando al futuro, la disgregazione di Black Basta non implica la fine della minaccia ransomware, ma piuttosto una probabile riconfigurazione degli attori coinvolti. La migrazione di affiliati verso gruppi più consolidati, come Lockbit o Akira, rappresenta un rischio concreto, poiché garantisce una continuità operativa delle tecniche e delle strategie già sperimentate.

In conclusione, la resilienza della comunità cybercriminale rende fondamentale un approccio proattivo da parte delle aziende e delle forze dell'ordine, con investimenti mirati nella threat intelligence, monitoraggio costante dei canali underground e sviluppo di strategie di difesa avanzate per contrastare le minacce emergenti.

RIFERIMENTI

1.Anderson, R., Barton, C., Bohme, R., Clayton, R., van Eeten, M. J. G., & Levi, M. (2020). *Measuring the cost of cybercrime*. In R. Clayton & F. Stajano (Eds.), Proceedings of the Workshop on the Economics of Information Security.
2.VX Underground. (n.d.). https://vx-underground.org/
3.PRODAFT Threat Intelligence. (n.d.). https://www.prodaft.com/

(Nota: I riferimenti sopra elencati includono fonti generalmente riconosciute in ambito di ricerca sulla sicurezza informatica. Ulteriori fonti specifiche possono essere integrate sulla base di future pubblicazioni o aggiornamenti di ExploitWhispers.)