Raport consolidat eveniment cibernetic

Informații suplimentare

Denumire	**Cuba Ransomware**
Tip	Ransomware
Tacticile utilizate MITRE ATT&CK	**Accesul inițial** T1584 - Utilizează rețele compromise pentru a se răspândi T1190 - Exploatează vulnerabilitățile în sistemele orientate spre public. T1566 - Expediază e-mailuri de phishing pentru a obține accesul inițial la sisteme. T1078 - Folosește acreditări compromise pentru a intra într-o rețea de victime. **Execuție** T1569 – Utilizează PsExec pentru a rula comenzi și pentru a instala malware pe alte sisteme compromise. **Evaziuni Defensivă:** T1562 – Utilizează un încărcător care dezactivează instrumentele de securitate din rețeaua victimelor. T1480 - Cuba.Ransomware se va autodistruge dacă este detectat o configurație a tastaturii rusești **Acces Credențiale** T1003 - Actorii folosesc memoria LSASS pentru a prelua acreditările compromise stocate. T1558 – Utilizează tehnica Kerberoasting pentru a identifica conturile de servicii legate de directorul activ. Mișcarea Laterală T1570 - Folosește Cobeacon (posibil o variantă modificată a Cobalt Strike) pentru a facilita mișcarea laterală. T1021.001 - Uilizează RDP pentru a se deplasa lateral. T1021.002 - SMB este utilizat pentru a accesa fișiere și directoare partajate în rețea, ceea ce poate ajuta la livrarea și executarea ransomware-ului pe alte mașini. T1072 - Utilizează Hancitor ca instrument de răspândire a fișierelor rău intenționate într-o rețea de victime.

	C&C T1090 - Ransomware utilizează proxy HTTP/HTTPS prin intermediul unui server C2 pentru a direcționa traficul, pentru a evita conexiunea directă. **Impact** T0881 – Stoparea serviciilor T1486 – Criptarea datelor
Algoritmul de criptare:	Malware-ul utilizează algoritmul de criptare simetrică ChaCha20 pentru a cripta fișierele și algoritmul de criptare asimetrică RSA pentru a proteja Cheia ChaCha20 și Vectorul de inițializare. Autorul a folosit o versiune personalizată a WolfSSL, o bibliotecă SSL/TLS open source, pentru a implementa această capacitate. Pot exista și alte implementări care nu sunt descrise aici. Ransomware-ul alocă o structură personalizată mare numită bloc, care conține toate informațiile de criptare necesare. Apoi inițializează o structură RsaKey cu wc_InitRsaKey și decodează o cheie publică RSA 4096 bit încorporată în format DER utilizând wc_RsaPublicKeyDecode pe care o salvează pentru a bloca.PubRsaKey.
Exemplu de notă	Greetings! Unfortunately we have to report that your company were compromised. All your files were encrypted and you can't restore them without our private key. Trying to restore it without our help may cause complete loss of your data. Also we researched whole your corporate network and downloaded all your sensitive data to our servers. If we will not get any contact from you in the next 3 days we will public it in our news site. You can find it there (https[:]//cuba4ikm4jakjgmkeztyawtdgr2xymvy6nvgw5cglswg3si76icnqd.onion/) Tor Browser is needed (https[:]//www.torproject.org/download/) Also we respect your work and time and we are open for communication. In that case we are ready to discuss recovering your files and work. We can grant absolute privacy and compliance with agreements by our side. Also we can provide all necessary evidence to confirm performance of our products and statements. Feel free to contact us with quTox (https[:]//tox.chat/download.html)
IoC	**SHA256:** f1103e627311e73d5f29e877243e7ca203292f9419303c661aec57745eb4f26c 141b2190f51397dbd0dfde0e3904b264c91b6f81febc823ff0c33da980b69944 02a733920c7e69469164316e3e96850d55fca9f5f9d19a241fad906466ec8ae8 32beefe2c5e28e87357813c0ef91f47b631a3dff4a6235256aa123fc77564346 0f385cc69a93abeaf84994e7887cb173e889d309a515b55b2205805bdfe468a3 bcf0f202db47ca671ed6146040795e3c8315b7fb4f886161c675d4ddf5fdd0c4 **E-mailuri asociate:** admin@cuba-supp[.]com admin@encryption-support[.]com inbox@mail.supports24[.]net cuba_support@exploit[.]jim

Resurse externe

	https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-335a