



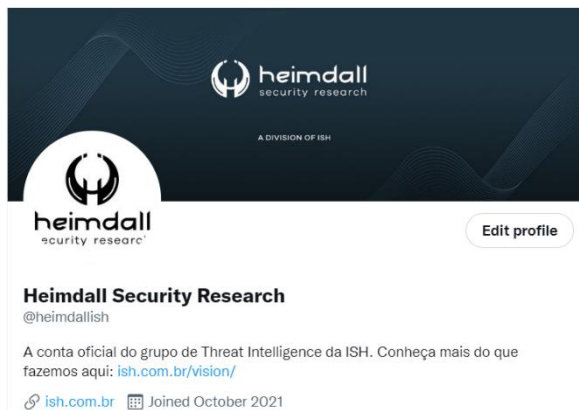
heimdall  
security research

---

A DIVISION OF ISH

# Receba alertas e informações sobre segurança cibernética rapidamente por meio do nosso Twitter:

<https://twitter.com/heimdallish>



**Heimdall Security Research @heimdallish · 3h**  
A CISA adicionou seis novos exploits ao seu Catálogo de Vulnerabilidades Exploradas Conhecidas, com base em evidências de exploração ativa. Esses tipos de vulnerabilidades são um vetor de ataque frequente para agentes cibernéticos mal-intencionados.

CISA:  
[bit.ly/3dphOEt](https://bit.ly/3dphOEt)



**Heimdall Security Research @heimdallish · Sep 9**  
Boletim semanal: Uma das principais ameaças da atualidade são os Malwares do tipo Stealer. Neste boletim trazemos informações e IoCs mostrando como você pode proteger sua empresa deste ataque.  
  
Acesso nosso boletim:  
[bit.ly/3L317ev](https://bit.ly/3L317ev)



**Heimdall Security Research @heimdallish · Sep 14**  
Hoje é o Patch Tuesday de setembro de 2022 da Microsoft, e com ele vem correções para uma vulnerabilidade do Windows explorada ativamente e um total de 63 falhas.

Bleeping Computer:  
[bit.ly/3BEdeII](https://bit.ly/3BEdeII)



**Heimdall Security Research @heimdallish · Sep 15**  
Em nosso Boletim Mensal, acompanhe os endereços IP ofensores, as principais ameaças, entre elas: Malwares, Cryptojacking, SSH Brute Force e TOR Proxy, que afetaram o Brasil no último mês e veja nossas recomendações para proteger sua empresa.

Boletim:  
[bit.ly/3dfvNww](https://bit.ly/3dfvNww)



**Heimdall Security Research @heimdallish · Aug 5**  
Em nosso Boletim Mensal, apresentamos análises de diversas fontes e, principalmente, da nossa plataforma de inteligência: Heimdall Global Threat Intelligence by ISH.

Acesso nosso material:  
[d335iupugy2.cloudfront.net/cms%2Ffiles%2F...](https://d335iupugy2.cloudfront.net/cms%2Ffiles%2F...)



# Relatório de Inteligência e Análise do Ransomware Cuba

Recentemente, a CISA publicou um alerta ([AA22-335A](#)) referente a algumas instruções para combater o Ransomware Cuba. Fato este muito relevante tendo em vista que a equipe de Threat Intelligence da ISH, o HEIMDALL estava realizando o acompanhamento das publicações referente as diversas vítimas afetadas e publicadas junto ao site de Data Leak dos operadores do Ransomware CUBA, sendo que até o presente momento, o ransomware Cuba anunciou o total de 85 (oitenta e cinco) vítimas em seu site de Data Leak, sendo que de acordo com o relatório da CISA os ataques realizados pelo Ransomware já atingiu certa de mais de 100 empresas e organizações.

Diante disto, alinhando o relatório advindo da CISA, traremos informações importantes referente ao Ransomware Cuba, bem como Análise Técnica e principais Indicadores de Comprometimento (IoCs) vinculadas aos operadores deste Ransomware.

## Alerta (AA22-335A) CISA

Diante do Alerta emitido pela CISA, elencaremos os principais pontos a serem observados do Ransomware Cuba. O principal aspecto trazido junto ao relatório fora a incorporação de novas TTPs (Táticas, Técnicas e Procedimentos) adotados pelos operadores, incorporando o Trojan de Acesso Remoto RomCom (RAT) e agentes de espionagem industrial.

Foi realizado o mapeamento das vítimas dos operadores, sendo atuantes no ramo de: Serviços Financeiros, Instalações Governamentais, Saúde e Saúde Pública, Fabricação Crítica e Tecnologia da Informação. Ao total, fora exigido pelos operadores a quantia de 145 milhões de Dólares e recebeu mais de 60 milhões de dólares em pagamentos de resgates.

## Táticas, técnicas e procedimentos dos operadores Cuba Ransomware

Conforme mencionado no relatório, os agentes do Cuba utilizaram as seguintes técnicas para obtenção de acesso inicial:

- Vulnerabilidades conhecidas em softwares comerciais (T1190)
- Utilização de campanhas de phishing (T1566)
- Credenciais comprometidas (T1078)
- Ferramentas legítimas de protocolo de área de trabalho remota (Remote Desktop Protocol – RDP) (T1563.002).

Após a obtenção do acesso inicial, os agentes distribuíram o ransomware Cuba em sistemas comprometidos por meio de outro malware conhecido como Hancitor (ou Chanitor), o qual funciona como um dropper ou download de outros artefatos, tendo em vista realizar a comunicação com seu servidor de comando e controle (C2).

Além da CISA, a Unit 42 da Palo Alto publicou um [relatório](#) detalhado sobre os agentes do Ransomware Cuba, informando ainda que os mesmos estão:

- Explorando a CVE-2022-24521 no driver do Windows Common Log File System (CLFS) para roubar tokens do sistema e elevar privilégios.
- Realizou a utilização de script do PowerShell para identificar e direcionar contas de serviços para o Kerberos ticket do Active Directory. Logo os agentes então coletaram e quebraram os tickets Kerberos offline via Kerberoasting (T1558.003).
- Utilizou ferramenta denominada KerberCache, para extrair tíquetes Kerberos em cache da memória LSASS (Local Security Authority Server Service) de um host (T1003.001).
- Usou uma ferramenta para explorar o CVE-2020-1472 (conhecida como “ZeroLogon”) para obtenção de privilégios administrativos de domínio (T1068). Tais ferramentas e suas tentativas de invasão foram relacionadas ao Hancitor e ao Qbot.

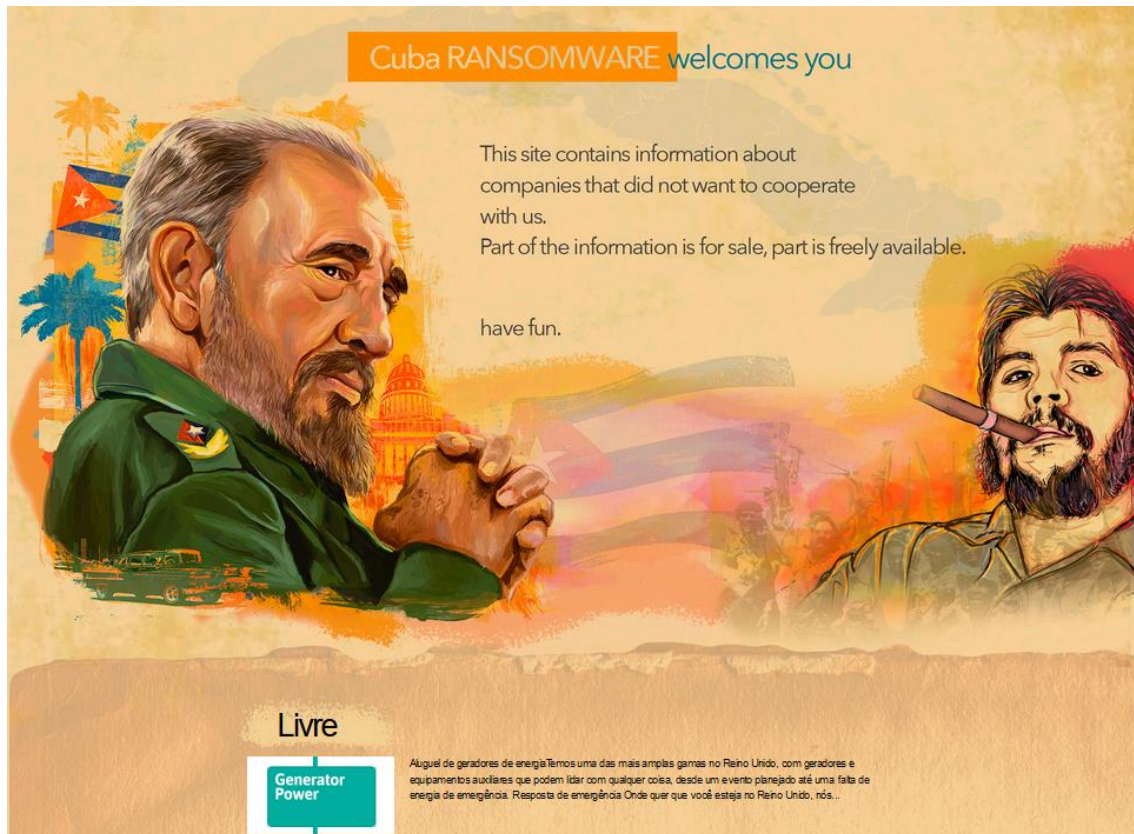
Diante do resumo, abaixo traremos mais informações sobre os agentes do Cuba Ransomware.

## Histórico do Cuba Ransomware

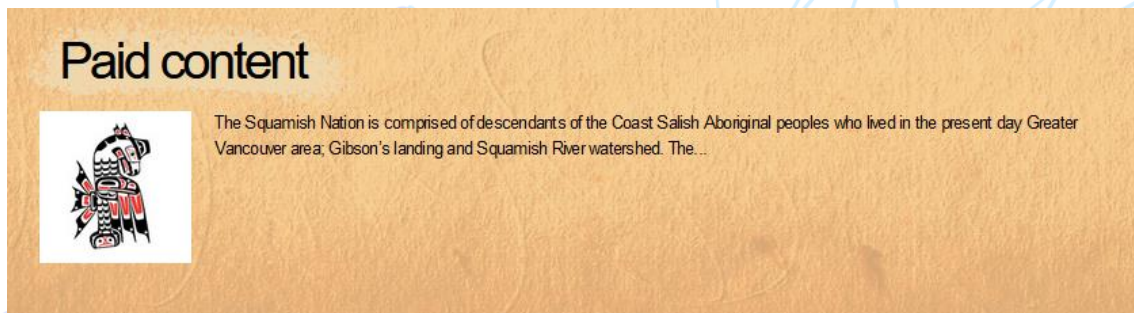
A família Cuba Ransomware surgiu pela primeira vez em dezembro de 2019, sendo que no início, os operadores não informavam as organizações que supostamente foram comprometidas, sendo que tal comportamento evoluiu de acordo com outras famílias que realizavam a divulgação, como o REvil e Maze.

Além de expor as supostas vítimas, expõe também a seção paga onde os agentes de ameaças compartilham vazamentos que foram vendidos a partes interessadas.





(Site de Data Leak do Cuba Ransomware)



(Captura de tela da seção do site de Data Leak onde os dados são oferecidos para venda).

Diante disto, abaixo realizamos a análise de uma amostra do Ransomware Cuba.

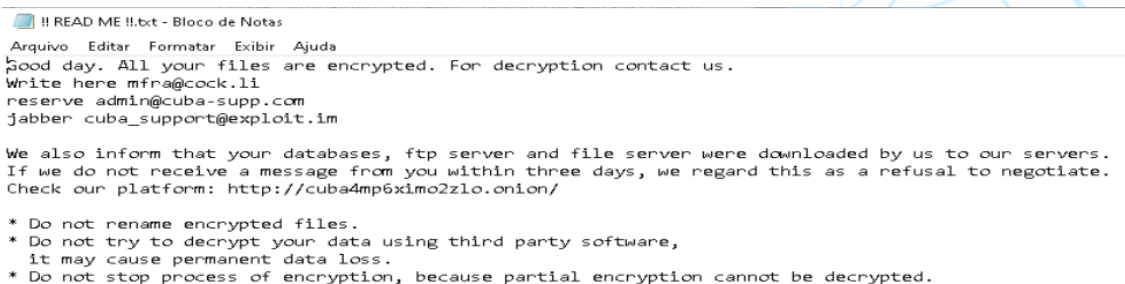
## Análise do Ransomware

Realizada a análise do artefato malicioso do ransomware Cuba sha256: 936119bc1811aeef01299a0150141787865a0dbe2667288f018ad24db5a7bc27, podemos observar que o mesmo fora compilado em C/C++ com a data de compilação em 23/08/2021, às 09:16:56 UTC.

Observado que o Ransomware realiza o “kill” de uma lista de processos, ou seja, se os processos abaixo estiverem em execução, o ransomware encerra-os.

MySQL	MySQL80	SQLSERVERAGENT	MSSQLSERVER	SQLWriter
SQLTELEMETRY	MSDTC	SQLbrowser	Sqlagent.exe	Sqlservr.exe
Sqlwriter.exe	Sqlceip.exe	Msdctc.exe	Sqlbrowser.exe	Vmcompute
Vmms	Vmwp.exe	Vmsp.exe	Outlook.exe	MSEExchangeUM MCR
MSEExchangeUM	MSEExchangeTransportLogSearch	MSEExchangeTransport	MSEExchangeThrottling	MSEExchangeSubmission
MSEExchangeServiceHost	MSEExchangeRPC	MSEExchangeRepl	MSEExchangePOP3BE	MSEExchangePop3
MSEExchangeNotificationsBroker	MSEExchangeMailboxReplication	MSEExchangeMailboxAssistants	MSEExchangeIS	MSEExchangeIMAP4BE
MSEExchangeMap4	MSEExchangeHMRecovery	MSEExchangeHM	MSEExchangeFrontEndTransport	MSEExchangeFastSearch
MSEExchangeEdgeSync	MSEExchangeDiagnostics	MSEExchangeDelivery	MSEExchangeDagMount	MSEExchangeCompliance
MSEExchangeAntispamUpdate	Microsoft.Exchange.Store.Worker.exe			

Após o processo de criptografia, o Ransomware despeja a nota de resgate denominada **!! READ ME !!.txt** nos diretórios e Área de Trabalho, contendo o seguinte conteúdo:



```

!! READ ME !!.txt - Bloco de Notas
Arquivo  Editar  Formatar  Exibir  Ajuda
Good day. All your files are encrypted. For decryption contact us.
Write here mfra@cock.li
reserve admin@cuba-supp.com
jabber: cuba_support@exploit.im

We also inform that your databases, ftp server and file server were downloaded by us to our servers.
If we do not receive a message from you within three days, we regard this as a refusal to negotiate.
Check our platform: http://cuba4mp6xi1mo2z1o.onion/

* Do not rename encrypted files.
* Do not try to decrypt your data using third party software,
  it may cause permanent data loss.
* Do not stop process of encryption, because partial encryption cannot be decrypted.
  
```

(Nota de Resgate despejada pelo Ransomware Cuba)

Porém, a nota variante da família, contém em sua nota de resgate, não apenas o site Tor, mas também oferecem comunicação via TOX:

"Greetings! Unfortunately we have to report you 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 3 next days we will public it in our news site.

You can find it there (

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> )

Our ToxID:

Alternative method is email: [inbox@mail.supports24.net](mailto:inbox@mail.supports24.net)

Mark your messages with your personal ID:

(Nota de resgate descartada obtida do relatório da Unit42)

Quanto a criptografia utilizada pelo Ransomware, permaneceu a mesma desde a sua descoberta de 2019, utilizando os algoritmos criptográficos do repositório de código aberto WolfSSL, especificamente ChaCha para criptografia de arquivos e RSA para criptografia de Chave.

Cada arquivo criptografado também é anexado com um cabeçalho inicial de 1024 bytes contendo o magic number "FIDEL.CA", seguindo por um bloco criptografado **RSA-4096** contendo a chave ChaCha específica do arquivo. Após a criptografia a extensão é alterada para **.cuba** no arquivo.



Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Texto decodificado.
00000000	46	49	44	45	4C	2E	43	41	00	04	00	00	08	00	00	00	FIDEL.CA.....
00000010	A4	00	00	00	10	00	00	00	00	00	00	00	00	00	00	00	.....
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000040	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000050	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000060	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000070	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000080	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000090	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000000A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000000B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000000C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000000D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000000E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000000F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000100	10	4E	C5	BC	99	8D	8E	C3	56	DB	94	22	44	DC	44	01	.NÅ...ZÅV0~"DÜD.
00000110	5E	1E	8A	0B	7F	C7	72	4B	A3	13	97	A7	AC	17	A1	FF	^..Š..ÇrKE.-S~.jŸ
00000120	0E	28	0B	65	19	FB	7A	2C	3B	4D	5C	42	9E	93	13	55	.(.e.ûz,,M\Bž".U
00000130	15	0D	14	DC	73	C5	F5	CE	3E	54	CB	2C	21	52	2C	6B	...ÜsÅöI>TÈ, !R,k
00000140	F6	47	A1	27	4A	CA	24	83	D4	22	A4	F7	B0	33	0C	99	öG;'JÈ\$fo"x÷°3..
00000150	63	6A	BA	4C	C9	1B	4D	00	48	B8	D6	86	C5	50	0D	28	cj°LÈ.M.H,Ö+ÅP.(
00000160	2E	43	3E	20	10	47	98	A1	35	2A	45	1F	68	60	39	5E	.C> .G" ;S*E.h`9^
00000170	3F	A4	90	D0	B4	08	CF	BE	24	64	59	A1	37	D8	A9	C3	?x.D'.I3\$dY;700Å
00000180	66	E1	5E	46	39	6E	4B	F6	FB	D7	92	15	A8	4F	CE	1C	fä°F9nKöûx'..Oî.

Por fim, alguns diretórios e arquivos estão sendo evitados pelo ransomware, como os diretórios:

- \windows\
- \program files\microsoft office\
- \program files (x86)\microsoft office\
- \program files\avs\
- \program files (x86)\avs\
- \\${recycle.bin}\
- \boot\
- \recovery\
- \system volume information\
- \msocache\
- \users\all users\
- \users\default user\
- \users\default\
- \temp\
- \inetcache\
- \google\

E as extensões abaixo também são evitados:

- .exe
- .dll
- .sys
- .ini
- .lnk
- .vbm



- .cuba

Logo, podemos observar que não só a referida amostra se trata de um Ransomware potencialmente lesivo para as organizações, como também demais artefatos localizados em conjunto com o ataque realizado pelos Operadores do Cuba também afetam as organizações, diante disto, listamos as principais IoCs relacionadas coletadas em fontes abertas e fechadas visando auxiliar a comunidade e cliente da ISH para se protegerem da referida ameaça.

## Indicadores de Compromissos

A ISH Tecnologia realiza o tratamento de diversos indicadores de compromissos coletados por meio de fontes abertas, fechadas e também de análises realizadas pela equipe de segurança Heimdall. Diante disto, abaixo listamos todos os Indicadores de Compromissos (IOCs) relacionadas a análise do(s) artefato(s) deste relatório.

**Driver Dropper** utilizado pelos agentes:

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	8539a8aafc49c49465b4af4aee1830cf
sha1:	309068c1d1e8414bed7eabed052805483608ff34
sha256:	07905de4b4be02665e280a56678c7de67652aee318487a44055700396d37ecd0
Imphash:	ec6ba1aefd8ce1eef7c5ed9910dd9c52
Authenthash:	d194ade38d448518f5b2f4249e80342aac1031e4911f0b44916f752fd90ba59a
Size in bytes:	592416 bytes

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	5f2d265f41a00ca041fbb6c99444d275
sha1:	820ba270b0c777347658fab42f1c2f5cddf6adf5
sha256:	af6561ad848aa1ba53c62a323de230b18cfd30d8795d4af36bf1ce6c28e3fd4e
Imphash:	ec6ba1aefd8ce1eef7c5ed9910dd9c52
Authenthash:	0e2d240a924bc4255a12766f8d45843383c18603bc12d7c37c49c6f2436aed86
Size in bytes:	592384 bytes

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	91d650d54ae1442c8900b6e2e4aa284a
sha1:	8ff14e53d77b5e1600d522a09009e2591accfb29
sha256:	24e018c8614c70c940c3b5fa8783cb2f67cb13f08112430a4d10013e0a324eaa
Imphash:	f5e8dfc3b903777152d89d57c9179121
Authenthash:	c5a3cd8943157a7f49deab7f660b12eaf9ba4ff63272355d779afdf7232f3513
Size in bytes:	20400 bytes

Ferramenta **ZeroLogon**:

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	2f46cf0e841677a362d70c8397466698
sha1:	3f82737550fbcc24c5724536b542fd5e6bb50278

sha256:	ab5a3bbad1c4298bc287d0ac8c27790d68608393822da2365556ba99d52c5dfb
lmpash:	3463aa6b67d3f434014f20fc5dd8ad17
Authenthash:	d7efb8fee7087388cc64b7be3f6eaf37a122be649014ae834198d82177e771b
Size in bytes:	178176 bytes

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	499eec3612c0f7597296397fb77b04c8
sha1:	832a9552e786b4ca7c960bc4b1de18e854944c49
sha256:	6866e82d0f6f6d8cf5a43d02ad523f377bb0b374d644d2f536ec7ec18fdaf576
lmpash:	3463aa6b67d3f434014f20fc5dd8ad17
Authenthash:	45cc23d9f68a1743e2ad22b952b5cd88160575aae00b136c0fd3d535824343ed
Size in bytes:	176128 bytes

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	bcf121ba763f4a0c07113046e5103900
sha1:	0e36bcc07c3de7549feafeeb606d4a77dd435c71
sha256:	3febf726ffb4f4a4186571d05359d2851e52d5612c5818b2b167160d367f722c
lmpash:	3463aa6b67d3f434014f20fc5dd8ad17
Authenthash:	1f4dd387a0c78f0ef6d2bdb2af6d8ba3f7f06d2f3ba2a88d03ed24dac8fb3cc
Size in bytes:	178176 bytes

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	25a089f2082a5fcb0f4c1a12724a5521
sha1:	8a06c836c05537fcd8c600141073132d28e1172d
sha256:	3a8b7c1fe9bd9451c0a51e4122605efc98e7e4e13ed117139a13e4749e211ed0
lmpash:	3463aa6b67d3f434014f20fc5dd8ad17
Authenthash:	3639b9b85e2e2d910856926fed047fdd84e53800d471d9b279862a37badecf47
Size in bytes:	178176 bytes

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	91889658f1c8e1462f06f019b842f109
sha1:	33a6b39fbe8ec45afab14af88fd6fa8e96885bf1
sha256:	36bc32becf287402bf0e9c918de22d886a74c501a33aa08dcb9be2f222fa6e24
lmpash:	3463aa6b67d3f434014f20fc5dd8ad17
Authenthash:	37d54b003fbf8eee85f85dc561d16a0f43f48a19880e378127312f06aef0b263
Size in bytes:	178176 bytes

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	63f6e59406f06ac58ff74430fca45301
sha1:	7389d1bd0c44450cfd995956f7470745f1af0bf5
sha256:	1450f7c85bfec4f5ba97bcec4249ae234158a0bf9a63310e3801a00d30d9abcc
lmpash:	777ad6c685de589753a744e38de7bf5c
Authenthash:	0327ac1d812440396d8cb6f1bf2b1d614c8dc6ef5d6064793a736744bdd7df8f
Size in bytes:	2908181 bytes

#### Ferramenta para **escalação de privilégios**:

Indicadores de compromisso de artefato malicioso/ analisado	
sha256:	a4665231bad14a2ac9f2e20a6385e1477c299d97768048cb3e9df6b45ae54eb8

### Ferramenta para KerberCache:

Indicadores de compromisso de artefato malicioso/ analisado	
sha256:	cfe7b462a8224b2fbf2b246f05973662bdabc2c4e8f4728c9a1b977fac010c15

### Ferramenta ROMCOM RAT:

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	69f58753ca65263f8b17bc845d876221
sha1:	e3ab90c4276cb31b071bf59e44213476f48e7e56
sha256:	b5978cf7d0c275d09bedf09f07667e139ad7fed8f9e47742e08c914c5cf44a53
Imphash:	efc2fe9a6a8f3e28ab7d5f31bf931066
Authenthash:	31dafa0322df07571665fe937b89c6e4f3b26ba499857d579514e005b2231868
Size in bytes:	592896 bytes

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	8e3366c06fa4136f43e548c7792b9678
sha1:	7ef6ce25e6a224d4e1a50db037cfd343083293ad
sha256:	324ccd4bf70a66cc14b1c3746162b908a688b2b124ad9db029e5bd42197cfe99
Imphash:	5e6833d41f0b30ee70a2511f4e41ee49
Authenthash:	8874b380369cd3d35acf22714e0e879afc2b9e8ee7d6a3e9cdecfa4b307ac0d1
Size in bytes:	582144 bytes

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	7c003b4f8b3c0ab0c3f8cb933e93d301
sha1:	ddc8dbc20dfe28de6e2495079324cd53354227fe
sha256:	246dfe16a9248d7fb90993f6f28b0ebe87964ffd2dcdb13105096cde025ca614
Size in bytes:	124671897 bytes

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	1a21a1e626fd342e794bcc3b06981d2c
sha1:	a1aa16c9e2dfd74c4470045da1180e015c015de8
sha256:	596eae93bdcd00a3aedaf6ad6d46db4429eeba61219b7e01b1781ebbf6e321b
Size in bytes:	5843388 bytes

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	d1a84706767bfb802632a262912e95a8
sha1:	f0e252eb7fd19f08ee4912e1dfc3f96fa121c8e0
sha256:	9d3b268416d3fab4322cc916d32e0b2e8fa0de370acd686873d1522306124fd2
Imphash:	3565985f928df68b8c3af3b353d04a5b
Authenthash:	c5495dd5a8bc50cce40fc5df78145aafb006b2243d08cdc2cb7147d3046266b5
Size in bytes:	111905784 bytes

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	cb933f1c913144a8ca6cfcfd913d6d28
sha1:	8c14acc05b66fa9c9b34ac8ea349f21df71eb981
sha256:	ac09cbfee4cf89d7b7a755c387e473249684f18aa699eb651d119d19e25bff34
Imphash:	2fd6a700dc3d7b2a027ab5e783746856
Authenthash:	2694c8dd8638295e5b937c6769e02039808daf78b41982e51b8e14e68a026741

Size in bytes:	766464 bytes
----------------	--------------

Indicadores de compromiso de artefato malicioso/ analizado	
md5:	8284421bbb94f3c37f94899cdcd19afd
sha1:	f38665cf13204f915d2efe78658a6dc65c4ca224
sha256:	8b8dff5d30802fd79b76ee1531e7d050184a07570201ef1cd83a7bb8fa627cb0
Imphash:	643c3d5c721741ad5b90c98c48007038
Authenthash:	1f71617165cad745622b09060ddf80e55e57ca64fa7d3b4d3f7dddf85d71e5e
Size in bytes:	752128 bytes

Indicadores de compromiso de artefato malicioso/ analizado	
md5:	6310a2063687800559ae9d65cff21b0a
sha1:	76ba097c0ee4ec561ef90db04358b0dcfc4b5c3f
sha256:	f7013ce417fcbaf0f36c4b9bf5f8f6e0e2b14d6ed33ff4d384c892773508e932e
Imphash:	16150a566bf5e341c7ccacbc00e90ebc
Authenthash:	10bae7e53f71eee6eff28a96dcc2b0207fad3599bec48e68a3f42a0729792dc1
Size in bytes:	78336 bytes

Indicadores de compromiso de artefato malicioso/ analizado	
md5:	550f42c5b555893d171285dc8b15b4b5
sha1:	36fb60b9aa51cf8ad9353b2aea24bc80545a9b93
sha256:	5f187393acdeb67e76126353c74b6080d3e6ccf28ae580658c670d8b6e4aacc1
Imphash:	c8a247ca80236d13e8666489872047d3
Authenthash:	d54bfd04790c5cee0a27386ec8433dc6a2ea086bf9826434064e5c934cd6755d
Size in bytes:	160256 bytes

Indicadores de compromiso de artefato malicioso/ analizado	
md5:	4e4eca58b896bdb6db260f21edc7760a
sha1:	ebcdd838acf310f6977089fe385f0ee27b7f87a0
sha256:	abe9635adbfee2d2fbaea140625c49abe3baa29c44fb53a65a9cda02121583ee
Imphash:	3d9df15f8734d827e2dd3840fdf2650b
Authenthash:	1a27fcd4673c05bfe1c9429bc9fba51d3a9dff8ea23328cd0b8e546e6a3ab75a
Size in bytes:	623616 bytes

Indicadores de compromiso de artefato malicioso/ analizado	
md5:	a7172aef66bb12e1bb40a557bb41e607
sha1:	260ab60e78919a80297c2b2ae461a3a60c43d546
sha256:	3252965013ec861567510d54a97446610edba5da88648466de6b3145266386d9
Imphash:	1ce3d6f5d3e0d6ca5b78e72664fd4c42
Authenthash:	32638559e16146298395060dddc947fc8f145fa43827b7ef48665c909f1f7b75
Size in bytes:	609280 bytes

### Ransomware CUBA:

Indicadores de compromiso de artefato malicioso/ analizado	
md5:	bcd57da0c23eae47f5e5b54db614cbc6
sha1:	064e77464964a9a96ce79b56fe4d8b9e740d4e1f
sha256:	0a3517d8d382a0a45334009f71e48114d395a22483b01f171f2c3d4a9cfdbfbf
Imphash:	fef753040a8ab4b25d3664a44289061e



Authenthash:	7efbd43e60fff0f2a6a189104912f622a5ebc17ac9a90b55b5aabac21cc00b22
Size in bytes:	1629696 bytes

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	286a7aa55ea888813b6df7c047aada5d
sha1:	dce10f420e527bbb7eda14f15fa261b647fb0d56
sha256:	0eff3e8fd31f553c45ab82cc5d88d0105626d0597afa5897e78ee5a7e34f71b3
Imphash:	fef753040a8ab4b25d3664a44289061e
Authenthash:	16685416862c50b6e8c2fb0a96ea922443a4b3e144c03a342386ea39a5600231
Size in bytes:	1629696 bytes

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	23d0033fe765242cbc07ceeab7ba3736
sha1:	d318737c9116dd181c2ec074c1ffc9e2f42bc31b
sha256:	78ce13d09d828fc8b06cf55f8247bac07379d0c8b8c8b1a6996c29163fa4b659
Imphash:	96be6a0fdaed049c36c7e6b23e9a1db3
Authenthash:	8faa8bccfc1662c6e3c3410b20c31e1400e16aa7e87074ec0bea9a43c90c03b5
Size in bytes:	765952 bytes

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	d8fd19fef4605b4217cb2546c470a918
sha1:	79786955d426945054e6d02050b8f9ada01e39ef
sha256:	33352a38454cfc247bc7465bf177f5f97d7fd0bd220103d4422c8ec45b4d3d0e
Imphash:	3dfd6c1844e4962d112479d58d5da410
Authenthash:	bbe1920fd3ec4d9dbf27d4a5351bef6235e7df23f7e00cbbde354a874b92827e
Size in bytes:	164352 bytes

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	b8018958476178596817f734894ff64c
sha1:	e1cae0d2a320a2756ae1ee5d37bfe803b39853fa
sha256:	672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1
Imphash:	d9dc90dd06110fc79f0b74983e7fb09d
Authenthash:	0ffe72edbacc0f72ce47b3d01032158423f409c30cf2f5035711ab53717d66c8b
Size in bytes:	483840 bytes

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	ce9c4f5439c48aeeca3bc9f2cdfaf826
sha1:	8ec10319d7a8f3dc651d4a66d3b8297abf1f895e
sha256:	e942a8bcb3d4a6f6df6a6522e4d5c58d25cdbe369ecda1356a66dacbd3945d30
Imphash:	eb982cdfb623fba4f616075ae03d7b9
Authenthash:	e73852bf3e547027c91dcab9a7197dd680d974b5b11d022b13d318f9c86fd27d
Size in bytes:	658944 bytes

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	7982a49032fd9ff757a60ec271cb4ae5
sha1:	ffdf827347981bf6dfb920a9068cfaefd5328666
sha256:	907f42a79192a016154f11927fbb1e6f661f679d68947bddc714f5acc4aa66eb
Imphash:	96be6a0fdaed049c36c7e6b23e9a1db3

Authenthash:	b28b5af444c4a0a4fdcc9ac72475420654ec2845801b1dde722a0aad36a593f7
Size in bytes:	765952 bytes

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	c3299f7783df63fd1682b5ad63d80325
sha1:	94e256709f30d9f436223113a2e612a3e5eda6d3
sha256:	28140885cf794ffe727f5673ca64bd680fc0b8a469453d0310aea439f7e04e64
Imphash:	56bf04b1246e7bd71ba0bddbd47cd745
Authenthash:	ee06be9d673934f171b5880f626786f3747b6bbc2f3b3010121863519b6771e5
Size in bytes:	1156608 bytes

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	a12e733ddbe6f404b27474fa0e5de61d
sha1:	e8d0c95621a19131ef9480e58a8d6dd3d15c9acd
sha256:	271ef3c1d022829f0b15f2471d05a28d4786abafd0a9e1e742bde3f6b36872ad
Imphash:	56bf04b1246e7bd71ba0bddbd47cd745
Authenthash:	280158d27bbe6ebc7855a59cf0fc1dfac549fb45e3e4087b5da9fb199b9971f
Size in bytes:	1156608 bytes

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	00b2679e73e28343fd153df9858bc910
sha1:	f27390cdca4afea0ffeda89f117931858e7f5a7f
sha256:	6396ea2ef48aa3d3a61fb2e1ca50ac3711c376ec2b67dbaf64eeba49f5dfa9df
Imphash:	80ccc470b5c03f358ac4b90d1cffe605
Authenthash:	b2140de180435e44765356c0c910f9b80e81bd63599896c1a415b3119f06652d
Size in bytes:	733016 bytes

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	d663bd6d72fa66cc0b8e64c205875ef8
sha1:	0de9a0b7f96b02ebd3f03c7a208d3a6041d605fa
sha256:	bda4bddcbd140e4012bab453e28a4fba86f16ac8983d7db391043eab627e9fa1
Imphash:	96be6a0fdaed049c36c7e6b23e9a1db3
Authenthash:	f1f05cc1c81bafb8cc806549d005138be93c2f85b37971deca7613fb65852482
Size in bytes:	765952 bytes

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	5ab2962110135f986777c938ac8bdb67
sha1:	25da0849207beb5695c8d9826b585b8cda435eba
sha256:	7a17f344d916f7f0272b9480336fb05d33147b8be2e71c3261ea30a32d73fecb
Imphash:	88494749b91f8c2f5d74d39e432d8001
Authenthash:	806084742d417edeef23bf387c4e6bbe751b0f2bb7f682871feda03f25fc5d66
Size in bytes:	519168 bytes

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	246b2207cfb8ef03049f11a80fba06bc
sha1:	7e42b668fd2ca96b05f39d5097943a191f1010f4
sha256:	c206593d626e1f8b9c5d15b9b5ec16a298890e8bae61a232c2104cbac8d51bdd
Imphash:	88494749b91f8c2f5d74d39e432d8001

Authenthash:	a4ce7986fad2527bab34019e8b14b4611d30f4f8ab06cd9e8ab3a1d04738f9f9
Size in bytes:	519168 bytes

Indicadores de compromiso de artefato malicioso/ analizado	
md5:	f739977004981fbe4a54bc68be18ea79
sha1:	6732aef6139c086ba62bd907ebdfa191a42529a6
sha256:	9882c2f5a95d7680626470f6c0d3609c7590eb552065f81ab41ffe074ea74e82
Size in bytes:	552073 bytes

Indicadores de compromiso de artefato malicioso/ analizado	
md5:	2af30ca88d11eb0c1a4bd4f0aa0ce685
sha1:	26d8a7cc91b1b047f24e948ec5498057bf37f429
sha256:	00ddbe28a31cc91bd7b1989a9bebd43c4b5565aa0a9ed4e0ca2a5cfb290475ed
Imphash:	d839287a3944866efd1ff751ae6ebaca
Authenthash:	d4bc54fdebd358a27e9f17717538d9eaf9660247476ac36cb862c0b2efc05fa8
Size in bytes:	417112 bytes

Indicadores de compromiso de artefato malicioso/ analizado	
md5:	c0451fd7921342e0d2fbf682091d4280
sha1:	c294ae878aba6aec14bcdf5a84d688fc66597893
sha256:	936119bc1811aef01299a0150141787865a0dbe2667288f018ad24db5a7bc27
Imphash:	0bab8bd0d5a8bc9bcbce47aa8df167a8
Authenthash:	905a1c1ba6ae3677b259bbc9968ad1ef38cc6ce443949c38f8f9527215959828
Size in bytes:	148480 bytes

Indicadores de compromiso de artefato malicioso/ analizado	
md5:	20a04e7fc12259dfd4172f5232ed5ccf
sha1:	82f194e6baeef6eefb42f0685c49c1e6143ec850
sha256:	482b160ee2e8d94fa6e4749f77e87da89c9658e7567459bc633d697430e3ad9a
Imphash:	83de7cbd89e0f17a9c11503452c3da00
Authenthash:	0e70a06819e107b7bf50ec48a62c337867dc553baea4b3c15983e92e693ea442
Size in bytes:	148480 bytes

Indicadores de compromiso de artefato malicioso/ analizado	
md5:	a12e733ddbe6f404b27474fa0e5de61d
sha1:	e8d0c95621a19131ef9480e58a8d6dd3d15c9acd
sha256:	271ef3c1d022829f0b15f2471d05a28d4786abafd0a9e1e742bde3f6b36872ad
Imphash:	56bf04b1246e7bd71ba0bddbd47cd745
Authenthash:	280158d27bbe6ebc7855a59cf0fc1dfac549fb45e3e4087b5da9fb199b9971f
Size in bytes:	1156608 bytes

Indicadores de compromiso de artefato malicioso/ analizado	
sha256:	c4b1f4e1ac9a28cc9e50195b29dde8bd54527abc7f4d16899f9f8315c852afd4
sha256:	944ee8789cc929d2efda5790669e5266fe80910cabf1050cbb3e57dc62de2040
sha256:	c385ef710cbdd8ba7759e084051f5742b6fa8a6b65340a9795f48d0a425fec61
sha256:	54627975c0befee0075d6da1a53af9403f047d9e367389e48ae0d25c2a7154bc
sha256:	1f825ef9ff3e0bb80b7076ef19b837e927efea9db123d3b2b8ec15c8510da647
sha256:	40101fb3629cdb7d53c3af19dea2b6245a8d8aa9f28febd052bb9d792cfbafa6

sha256:	729950ce621a4bc6579957eabb3d1668498c805738ee5e83b74d5edaf2f4cb9e
---------	--

Indicadores de Compromisso de Domínios, URL e IPs considerados maliciosos	
C2	CombinedResidency.org
C2	optasko.com
C2	37.120.193.123
C2	40.115.162.72
C2	157.245.70.127
C2	31.44.184.82
C2	185.153.199.176
C2	kurvalarva.com

**Obs: Os links e endereços de IPs elencados acima podem estar ativos, cuidado ao realizar a manipulação dos referidos IoCs, evitando-se que seja realizado o clique e vítima do conteúdo malicioso hospedado no IoC.**

## Referências

Foram coletadas informações das referências abaixo:

- Heimdall Cyber Threat Group by ISH.
- <https://www.bleepingcomputer.com/news/security/fbi-cuba-ransomware-raked-in-60-million-from-over-100-victims/>
- <https://www.cisa.gov/uscert/ncas/alerts/aa22-335a>
- <https://unit42.paloaltonetworks.com/cuba-ransomware-tropical-scorpius/>
- [https://www.trendmicro.com/en\\_us/research/22/f/cuba-ransomware-group-s-new-variant-found-using-optimized-infect.html](https://www.trendmicro.com/en_us/research/22/f/cuba-ransomware-group-s-new-variant-found-using-optimized-infect.html)
- <https://blogs.blackberry.com/en/2021/07/threat-thursday-hancitor-malware>



