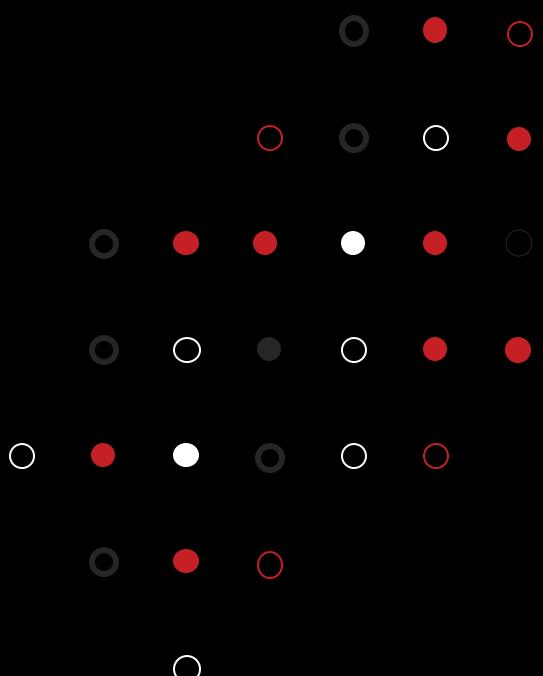
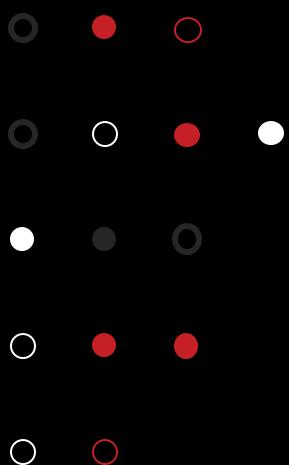


# SOC iT.eam Report



## Ransomware afeta Data Center Tier III Em Goiás

Cyber Threat Intelligence



# Ransomware Report

**Author:** Gabriel Alves

**Audience:** SOC

**Key Decisions:** Determinar e correlacionar IOC's, contextualizando sobre concorrente direto afetado na cidade de Goiânia (GO).

**Decision-Enabling Data Points:** Contexto e relevância da ameaça para a organização; Comportamento do adversário e objetivos potenciais; Enriquecimento de informações de Intelligence com o auxílio na tomada de decisão.

 Deltta + Unique data center

### Deltta + Unique data center

Description of the publication

Unique DataCenter provides tailored cloud computing solutions designed to enhance business operations through high performance, security, scalability, and unmatched agility. Their services include cloud backup, dedicated servers, SD-WAN solutions, and advanced firewalls, aimed at businesses of all sizes seeking reliable IT infrastructure. With a focus on 24/7 technical support and compliance with Tier 3 standards, they ensure data security and seamless connectivity. Unique DataCenter emphasizes sustainability and flexibility, enabling clients to control their IT resources effectively.

Publication category	Income
Encrypted	6000000 \$
Date of publication	Views
27/10/2025	50

---

**Disclosures**

Title: Data Categories: Financial data, Customer's data, Contracts

Description: 50 Gb

3d : 5h : 35m : 19s



## Executive Summary

O time de Threat Intelligence da **iT.team** identificou, por meio de fontes internas de inteligência, que o **Unique Data Center**, sediado em Goiânia, foi comprometido pelo **Ransomware Sinobi**, com evidências confirmadas de publicação no fórum oficial do grupo na Dark Web. Considerando que a Unique é um data center Tier III e concorrente direta de um de nossos clientes, este relatório foi elaborado para ciência do time de Segurança da Informação da **Everest Digital**, bem como para atualização das regras de detecção com os IOCs identificados.

O **Sinobi Ransomware** surgiu em junho de 2025, utilizando criptografia **AES** e **RSA** para bloquear arquivos e adicionar a extensão **.SINOBI**. Após o ataque, as vítimas recebem um arquivo **README.txt** com instruções de contato via site Tor para negociação do resgate. O grupo afirma agir com motivação financeira, fornecendo prova de descriptografia e lista de dados exfiltrados hospedados em **cdn.sinobi.us.org**, concedendo um prazo de sete dias para resposta.

A principal técnica de acesso inicial identificada envolve o comprometimento de **credenciais de VPN SonicWall SSL (CVE-2024-53704)**, embora também haja tentativas por outros serviços de VPN e movimentação lateral via RDP. Após a invasão, os operadores criam contas administrativas e desativam ferramentas de segurança, incluindo **EDRs** e **VeeamBackup**, além de exfiltrarem dados via **RClone**.

O grupo também realiza campanhas de **phishing** e **spear-phishing** para coleta de credenciais adicionais, reforçando a necessidade de políticas rígidas de conscientização e atualização de sistemas. Como medidas preventivas, recomenda-se manter **clients de VPN atualizados**, bloquear **IPs associados ao ataque** e revisar **ativos expostos na internet**, com foco em serviços críticos identificados via **Shodan**.

Good afternoon, we are Sinobi Group.

As you can see you have been attacked by us! We offer you to make a deal with us. all you need to do is contact us by following the instructions below. We are not politically motivated group, we are interested only in money, we always keep our word. You have a possibility to decrypt your files and save your reputation in case we find good solution! You have to know we do not like procrastination. You have 7 days to come to the chat room and start negotiations.

- 1 Communication Process:  
In order to contact with us you need to download Tor Browser.  
You can download Tor Project from this link:  
<https://www.torproject.org/download/>

After you joined to chat room you have the opportunity to request several things from us for free:  
1. make a test decrypt.  
2. get a list of the files stolen from you.

At the end, we should agree on the price for our services. Keep in mind that we got your income/insurance documents.

- 2 Access to the chat room:  
To access us please use one of the following links:  
1. <http://sinobi7yuoppj76qnkwuobwc2qve2xkv2ckvzzyjb1w7ucptl62ad.onion/login>  
2. <http://sinobi57mfegeov2naiufk1dkpz263jtb1dkinfj7qmk2mye6syqd.onion/login>  
3. <http://sinobi1bzduzhujkl0fkxziz3ueyedfh6bed21zjz2z6pafw5jeptsid.onion/login>  
4. <http://sinobi1bjqytwqxu24zuerqcjd3hou6zia7z6kzuvaauivam7nqayd.onion/login>  
5. <http://sinobi1crh73ongfruxja3mlyha1okhlcgtxxxaxz2qsgsdccfg76uigd.onion/login>  
6. <http://sinobi1dxogdt4jsr3tlnf2r4okjuvrf5gh3irpxqnuonmcx62srxhqd.onion/login>  
7. <http://sinobi4snfqtkc43paunap04i7vxcy5u7zfoalunsnuzehozhfhpypd.onion/login>

If Tor is blocked in your country you can use this link: <http://chat.sinobi.us.org/login>  
Your unique ID: [REDACTED] - use it to register in the chat room.

- 3 Blog:  
To access us please use one of the following links:  
1. <http://sinobi6ftrg27d6gkjstdt65mlsd56cfptlnjuw52rskakqjda6ubv7yd.onion/leaks>  
2. <http://sinobi6flec6f2bgn6rd72x07hds4a5aji2u1f4oubzut7fg3gomqd.onion/leaks>  
3. <http://sinobi6yugmwmq2jg2yygb2hxbimaxpqyk27ut5jwhfc1dhackid.onion/leaks>  
4. <http://sinobi713vet3uqn4cagjiesuonw75au3bvgah4jp43od7ndb7kad.onion/leaks>  
5. <http://sinobi71sukclb3ygtorysbtrogdbnrngbhov45rpubbbzhu5jvqd.onion/leaks>  
6. <http://sinobi23l75c3znmqgxxyuzquhx15ar7actgv4nqeuhgcn5yu23zqd.onion/leaks>  
7. <http://sinobi1dmnht2ocdjpmess59py7pn2y4dyqd740gobgj4gybcmkqd.onion/leaks>

If Tor is blocked in your country you can use this link: <http://blog.sinobi.us.org/leaks>

- 4 Recommendations:  
Do not try to recover your files with third-party programs, you will only do harm.  
Do not turn off / reboot your computer.  
Do not procrastinate.

## Sinobi Ransomware

O time de Threat Intelligence da iTteam detectou através de fontes internas de inteligência que o data center sediado em Goiânia, Unique Data Center, foi comprometido pelo Ransomware Sinobi, com publicação ativa no fórum oficial do grupo na DarkWeb.

A Unique também é um data center Tier III, devido à este motivo, estamos enviando este report para ciência dos colaboradores envolvidos no setor de Segurança da Informação da Everest Digital, assim como estaremos adicionando os IOCs aqui apresentados nas nossas regras de detecção.

## Analysis Summary

Este tópico tem o intuito de resumir a ameaça e elencar os IoC's que compõem este Ransomware, juntamente com suas TTP's baseada no MITRE ATT&CK.

Até então, o ransomware emergiu no final de junho de 2025. Ele emprega uma combinação de algoritmos de criptografia AES e RSA para bloquear os arquivos das vítimas, anexando a eles a extensão .SINOBI. Após a infecção, as vítimas recebem uma nota de resgate intitulada README.txt, instruindo-as a contatar os atacantes através de um site de chat baseado em Tor para negociar o pagamento. A nota enfatiza que o grupo é motivado financeiramente, e não politicamente, e oferece prova da descriptografia dos dados e uma lista dos arquivos exfiltrados que se dão através de uma conexão com o servidor de arquivos dos atacantes (<http://cdn.sinobi.us.org>). As vítimas têm sete dias para iniciar a comunicação, com avisos contra o uso de ferramentas de recuperação de terceiros ou a reinicialização de seus sistemas.

Diante dos estudos feitos, os atores de ameaça têm como principal acesso inicial o comprometimento de credenciais VPN's SonicWall SSL (CVE-2024-53704), porém, há indícios da tentativa de comprometimento através de outros serviços de VPN, mapeando o ambiente e habilitando portas RDP, após o comprometimento, os atores utilizam comandos para criar novas contas usadas subsequentemente para movimentação lateral.

---

Após o acesso inicial e a infecção, o dropper do ransomware executa também a exclusão das Shadow Copies do Windows, abaixo, seguem alguns comandos utilizados durante o processo de criação de contas pós acesso inicial.

```
cmd/c net localgroup administrators Assistance /add
cmd/c net user Assistance /add
cmd/c net localgroup "domain admins" Assistance /add

sc config cbdefense start= disabled
cmd/c sc config cbdefense binpath= "C:\programdata\bin.exe" & shutdown /r/t
```

Durante o processo de comprometimento interno, os operadores podem tentar desativar ferramentas do ambiente com softwares legítimos como o Revo Uninstaller seguindo com a exfiltração via RClone (também legítimo), combinando isso com a desativação de ferramentas como VeeamBackup e até mesmo bancos de dados SQL, e de EDR's.

Além do comprometimento de credenciais expostas de VPN's, os atores também utiliza de técnicas de phishing e spear-phishing via email, com o envio de arquivos diversos.

## IoC's

### IP's

45.135.194.0/24  
83.150.218.93  
83.150.218.236  
83.150.218.230  
83.150.218.188  
14.103.145.211  
14.103.145.242  
14.103.145.146  
14.103.145.202  
154.91.254.95  
150.241.114.140 (servidor para exfiltração) - AS199785  
10.246.112.59 (servidor para exfiltração)  
150.241.114.168  
78.153.149.90  
78.153.149.208  
78.153.149.133  
78.153.149.124  
78.153.149.77

### SHA256

c88f60dbae08519f2f81bb8efa7e6016c6770e66e58d77ab6384069a515e451c  
eb3e2a6a50f029fc646e2c3483157ab112f4f017406c3aabedaae0c94e0969f6  
f4cd7ab04b1744babef19d147124bfc0e9e90d557408cc2d652d7192df61bda9  
e3c080e322862d065649c468d20f620c3670d841c30c3fe5385e37f4f10172e7  
e62df17150fc7fea32ff459ef47cdd452a21269efe9252bde70377fd2717c10  
43d4847bf237c445ed2e846a106e1f55abefef5c3a8545bd5e4cad20f5deb9a4  
53e2c2d83813d1284ddb8c68b1572b17cca95cf36a55a7517bf45ff40828be5  
4c2429fc8b8ec61da41cbba1b8184ec45fa93a9841b4ca48094bba7741b826b8  
694d729d67f1b0c06702490bfb1df3a96fe040fe5d07efa5c92356c329757be  
0814a0781ab30fca069a085dba201d6fd0f414498fafaf4bb42859786d91d4781

**Arquivos**

invoice.pdf  
invoice.pdf.SINOBI  
Sinobi  
Ransom.Lynx!gen1  
SONAR.Ransomware!g  
SONAR.Ransom!gen98  
README.txt

**Extensão principal**

.SINOBI

**SHA256**

edae3b75deb8013bd48ac4534cca345b90938a2abb91672467c2bf9ae81ff683  
59b4deee977e9e27b60e7e179d54a1ce8e56624e73b799523416eee828bfaf76  
9f916a552efc6775367a31357a633dc0be01879830d3fddccdf3c40b26e50afd  
0a9ebbecc8ec58c253039520304ca373cfb8d1674d67993e6485e244a77d6ec9  
6c81fd73b4bef6fef379cbefdcce7f374ea7e6bf1bf0917cf4ca7b72d4cee788  
a55a3859a203ca2bae7399295f92aaeae61d845ffa173c1938f938f5c148eef99  
57573779f9a62eeeb80737d41d42165af8bb9884579c50736766abb63d2835ba  
c123a91fdacd9a4c0bcf800d6b7db5162cf11cb71e260647ef0f2c60978ebfc  
3daa53204978b7797bd53f5c964eed7a73d971517a764785ce3ab65a9423c2e7  
a197f60d5f5641f2c56576b4c867d141612c6e00db29c512f266835510b8a62d  
8250d289c5ec87752cec1af31eed0347cf2dd54dc0fbeea645319c4dae238ee2  
937e6ab0dfcedfa23eced7b52d3899b0847df3fc7a9c326b71027a7ab5f5b93

**MD5**

3ebf5f01ac8ca704f4ab9e12acd11139f3ff838f  
2101541061fb52b178165e7ef22244ec42601aea  
3055b209cfdd3bd297029ef4270b77b50f76dc03  
86233a285363c2a6863bf642deab7e20f062b8eb

**Onions**

http://sinobi6ftrg27d6g4sjdt65malds6cfptlnjyw52rskakqjda6uvb7yd.onion/  
http://sinobi6rllec6f2bgn6rd72xo7hvds4a5ajiu2if4oub2sut7fg3gomqd.onion/  
http://sinobi6ywgmmpvg2gj2yygkb2hxbimaxpqkyk27wti5zjwhfcldhackid.onion/  
http://sinobi7l3wet3uqn4cagiessuomv75aw3bvgah4jpj43od7xndb7kad.onion/  
http://sinobi7sukclb3ygtorysbtrdgdbnrmgbhov45rwzipubbzhiu5jvqd.onion/  
http://sinobi23i75c3znmqqxyuzqvhxnjsar7actgvc4nqeuhgcn5yvz3zqd.onion

**Exfiltração:**

http://cdn.sinobi.us.org/  
http://sinobihmkmncjubqin5u44vs03z2zongdmmtgle7eglskjmf6u74rad.onion/

## MITRE ATT&CK

**TA0001 - Initial Access:** Consiste na soma de diversas técnicas utilizadas para ganhar acesso indevido à rede do alvo, neste caso, podendo ser por phishing, spear-phishing e credenciais comprometidas de VPN Clients.

**TA0003 - Persistence:** Uma ou várias técnicas que visam a permanência dentro da rede ou em uma máquina dentro da rede do alvo.

[Create or Modify System Process / Service](#) — T1543

[Account Manipulation](#) — T1098

### **TA0003 - Execution**

[Command and Scripting Interpreter](#) — T1059

[Shared Modules](#) — T1129

### **TA0004 - Privilege Escalation**

[Access Token Manipulation](#) — T1134

[Abuse Elevation Control Mechanism](#) — T1548

**TA0005 – Defense Evasion:** Métodos que atacantes usam para evitar a detecção durante suas ações, detecções essas que podem vir de um programa AV até EDR's ou SIEMs.

[Disable or Modify Tools / Impair Defenses](#) — T1562

[Obfuscated Files or Information](#) — T1027

[File Permissions Modification](#) — T1222

**TA0008 – Lateral Movement:** Movimentação lateral consiste em técnicas que adversários usam para acessar e controlar sistemas remotos em uma rede, neste caso, usando o PSEexec.

[Remote Services](#) — T1021

[WMI](#) — T1047

[Remote Desktop](#) — T1021.001



## Recomendations

- Não abrir emails suspeitos de qualquer origem, principalmente emails que contenham arquivos desconhecidos.
- Manter atualizado todos os clients de VPN's, bem com soluções de backup internas.
- Bloquear comunicações em Firewall relacionados com IP's identificados.
- Verificação de ativos expostos na internet, encontrados via Shodan. (query = country:"br" org:"EVEREST DIGITAL SOLUCOES EM TECNOLOGIA LTDA")

[View Report](#) [View on Map](#) [Advanced Search](#)

**Product Spotlight:** We've Launched a new API for Fast Vulnerability Lookups. Check out [CVEDB](#)

**177.105.249.18** 

EVEREST DIGITAL SOLUOES EM TECNOLOGIA LTDA  
 Brazil, Esmeraldas

HTTP/1.1 200 OK  
Accept-Ranges: bytes  
Cache-Control: max-age=31536000  
Content-Length: 22734  
Content-Security-Policy: script-src 'self' cdn.matomo.cloud js.hsforms.net https://www.google.com/recaptcha/, https://www.gstatic.com/recaptcha/; object-src '

**400 Bad Request** 

177.105.249.38  
EVEREST DIGITAL SOLUOES EM TECNOLOGIA LTDA  
 Brazil, Belo Horizonte

HTTP/1.1 400 Bad Request  
Date: Tue, 28 Oct 2025 22:16:04 GMT  
Server: Apache/2.4.6 () OpenSSL/1.0.2k-fips PHP/7.4.33  
Content-Length: 362  
Connection: close  
Content-Type: text/html; charset=iso-8859-1

**IS Windows Server** 

177.105.249.22  
EVEREST DIGITAL SOLUOES EM TECNOLOGIA LTDA  
 Brazil, Esmeraldas

 IIS

HTTP/1.1 200 OK  
Content-Type: text/html  
Last-Modified: Tue, 13 May 2025 13:03:47 GMT  
Accept-Ranges: bytes  
ETag: "8b371b777c4db1:0"  
Server: Microsoft-IIS/10.0  
X-Powered-By: ASP.NET  
Date: Tue, 28 Oct 2025 21:17:14 GMT  
Content-Length: 703

177.105.249.26 - Apache Tomcat (possivelmente crítico)

177.105.249.22 - IIS Windows Server

177.105.249.11 - IIS Windows Server

177.105.249.18 Login page – MaximaSistemas

177.105.249.24 - Login Page – Clinical Force

177.105.249.29 - Apache2

177.105.249.9 - Login Page A2O Sistemas

177.105.249.44 - Payara Server

177.105.249.133 - Apache

177.105.249.231 - Login Page EAP 6

177.105.249.17 - Login Page Totvs

---

## Referências

Disponível em: <https://www.cyfirma.com/news/weekly-intelligence-report-11-july-2025/>