GATE7
IT SOLUTIONS

# Informativo
# GATE7


# Novo Ransomware Akira ataca empresas em todo o mundo.

A nova operação de ransomware Akira vem lentamente construindo uma lista de vítimas à medida que invadem redes corporativas em todo o mundo, criptografam arquivos e exigem resgates de milhões de dólares.

Lançado em março de 2023, o Akira afirma já ter realizado ataques a dezesseis empresas. Essas empresas estão em vários setores, incluindo educação, finanças, imóveis, manufatura e consultoria. Embora outro ransomware chamado Akira tenha sido lançado em 2017, não se acredita que essas operações estejam relacionadas.

Ao criptografar arquivos, o ransomware criptografa os arquivos e anexa a extensão .akira ao nome do arquivo. Akira também usa a API do Windows Restart Manager para fechar processos ou desligar serviços do Windows que podem estar mantendo um arquivo aberto e impedindo a criptografia.

Cada pasta do computador conterá uma nota de resgate chamada akira_readme.txt que inclui informações sobre o que aconteceu com os arquivos da vítima e links para o site de vazamento de dados Akira e o site de negociação.

Como outras operações de ransomware, o Akira viola uma rede corporativa e se espalha lateralmente para outros dispositivos. Depois que os agentes de ameaças obtêm credenciais de administrador de domínio do Windows, eles implantam o ransomware em toda a rede.

## O criptografador Akira

Uma amostra do ransomware Akira foi descoberta pelo MalwareHunterTeam, que compartilhou uma amostra com o BleepingComputer para que pudéssemos analisá-la.

***Quando executado, o Akira excluirá as Cópias de Volume Sombra do Windows no dispositivo executando o seguinte comando do PowerShell:***

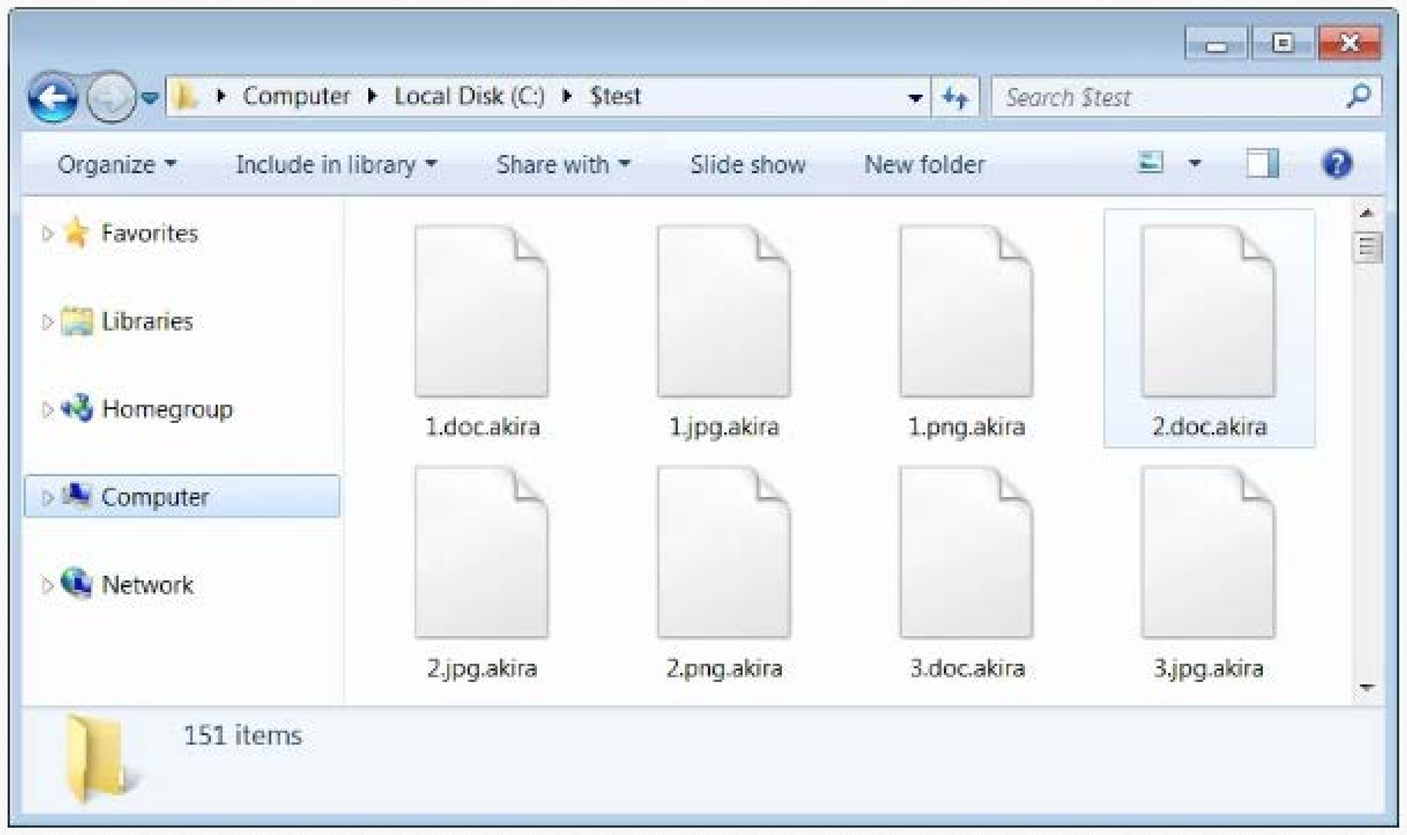
```
powershell.exe -Command "Get-WmiObject Win32_Shadowcopy | Remove-WmiObject"
```

***O ransomware irá então proceder a encriptar ficheiros que contêm as seguintes extensões de ficheiros:***

.accdb, .accde, .accdc, .accdt, .accdr, .adb, .accft, .adf, .ade, .arc, .adp, .alf, .ora, .btr, .ask, .cat, .bdf, .ckp, .cdb, .cpd, .cma, .dad, .dacpac, .daschema, .dadiagrams, .db-shm, .db-wal, .dbf, .dbc, .dbt, .dbs, .dbx, .dbv, .dct, .dcb, .ddl, .dcx, .dlis, .dsk, .dqy, .dtsx, .dsn, .eco, .dxl, .edb, .ecx, .exb, .epim, .fdb, .fcd, .fmp, .fic, .fmpsl, .fmp12, .fol, .fpt, .gdb, .frm, .gwi, .grdb, .his, .hdb, .idb, .itdb, .ihx, .jet, .itw, .kdb, .jtx, .kexic, .kexi, .lgc, .kexis, .maf, .lwx, .mar, .maq, .mav, .mas, .mdf, .mdb, .mrg, .mpd, .mwb, .mud, .ndf, .myd, .nrmlib, .nnt, .nsf, .nyf, .nwdb, .oqy, .odb, .owc, .orx, .pdb, .pan, .pnz, .pdm, .qvd, .qry, .rctd, .rbf, .rodx, .rod, .rsd, .rpd, .sbf, .sas7bdat, .sdb, .scx, .sdf, .sdc, .spq, .sis, .sqlite, .sql, .sqlitedb, .sqlite3, .temx, .tps, .tmd, .trm, .trc, .udl, .udb, .usr, .vpd, .vis, .wdb, .vvv, .wrk, .wmdb, .xld, .xdb, .abcddb, .xmlff, .abx, .abs, .adn, .accdw, .icg, .hjt, .kdb, .icr, .maw, .lut, .mdt, .mdn, .vhd, .vdi, .pvm, .vmdk, .vmsn, .vmem, .nvram, .vmsd, .raw, .vmx, .subvol, .qcow2, .vsv, .bin, .vmrs, .avhd, .avdx, .vhdx, .iso, .vmcx

Durante a criptografia, o criptografador ignorará os arquivos encontrados nas pastas Lixeira, Informações do Volume do Sistema, Inicialização, ProgramData e Windows. Ele também evitará criptografar os arquivos de sistema do Windows com extensões de arquivo .exe, .lnk, .dll, .msi e .sys.
Ao criptografar arquivos, o ransomware criptografa arquivos e anexa a extensão .akira será anexada ao nome do arquivo.

Por exemplo, um arquivo chamado 1.doc seria criptografado e renomeado para 1.doc.akira, conforme mostrado na pasta criptografada abaixo.




O Akira também usa a API do Gerenciador de Reinicialização do Windows para fechar processos ou desligar serviços do Windows que podem estar mantendo um arquivo aberto e impedindo a criptografia.

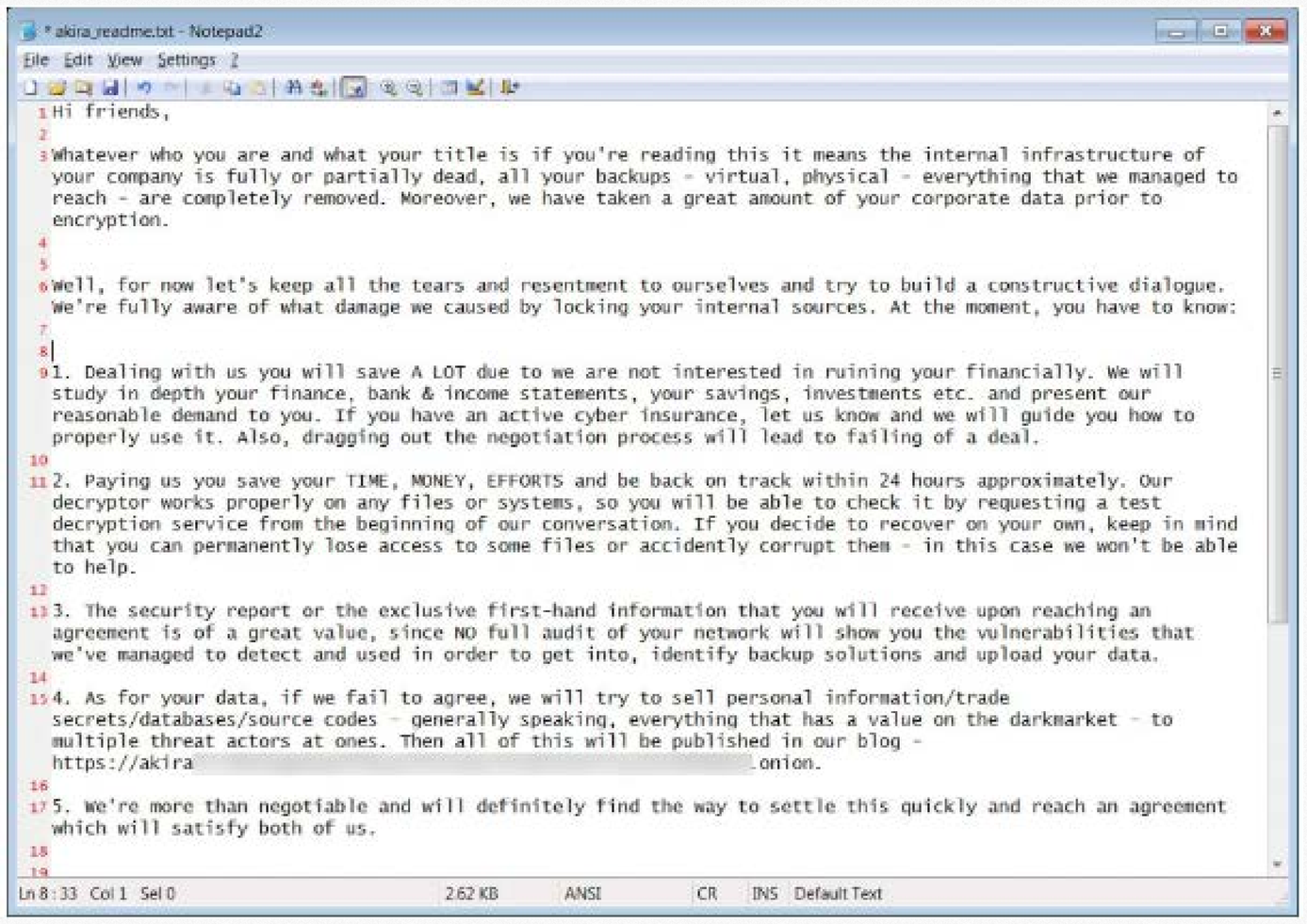
Cada pasta de computador conterá uma nota de resgate chamada akira_readme.txt que inclui informações sobre o que aconteceu com os arquivos de uma vítima e links para o site de vazamento de dados Akira e site de negociação.

NOTA:

> Quanto aos seus dados, se não chegarmos a um acordo, tentaremos vender informações pessoais/ segredos comerciais/bancos de dados/códigos-fonte – em geral, tudo o que tem um valor no mercado escuro – para vários autores de ameaças ao mesmo tempo. Então tudo isso será publicado em nosso blog.

*Ameaça a nota de resgate de Akira.*

Cada vítima tem uma senha de negociação exclusiva que é inserida no site Tor do agente da ameaça. Ao contrário de muitas outras operações de ransomware, este site de negociação inclui apenas um sistema de bate-papo que a vítima pode usar para negociar com a gangue de ransomware.




**Confira na próxima página a tradução da nota de resgate:**

Tradução da nota de resgate:

Olá amigos,
Seja quem for quem você é e qual é o seu título, se você estiver lendo isso, significa que a infraestrutura interna da sua empresa está total ou parcialmente morta, todos os seus backups – virtuais, físicos – tudo o que conseguimos alcançar – são completamente removidos. Além disso, pegamos uma grande quantidade de seus dados corporativos antes da criptografia.
Bem, por enquanto vamos guardar todas as lágrimas e ressentimentos para nós mesmos e tentar construir um diálogo construtivo. Estamos plenamente cientes dos danos que causamos ao bloquear suas fontes internas. No momento, você tem que saber:

1. Lidando conosco você vai economizar MUITO devido a nós não estamos interessados em arruinar o seu financeiramente. Vamos estudar a fundo suas finanças, demonstrações bancárias e de rendimentos, suas poupanças, investimentos etc. e apresente nossa demanda razoável a você. Se você tem um seguro cibernético ativo, avise-nos e nós o orientaremos como usá-lo corretamente. Além disso, arrastar o processo de negociação levará ao fracasso de um acordo.

2. Pagando-nos você economiza seu TEMPO, DINHEIRO, ESFORÇOS e estará de volta aos trilhos dentro de 24 horas aproximadamente. Nosso decodificador funciona corretamente em quaisquer arquivos ou sistemas, então você poderá verificá-lo solicitando um serviço de descriptografia de teste desde o início de nossa conversa. Se você decidir recuperar por conta própria, tenha em mente que você pode perder permanentemente o acesso a alguns arquivos ou corrompê-los acidentalmente – neste caso, não seremos capazes de ajudar.

3. O relatório de segurança ou as informações exclusivas em primeira mão que você receberá ao chegar a um acordo é de grande valor, já que NENHUMA auditoria completa de sua rede mostrará as vulnerabilidades que conseguimos detectar e usar para entrar, identificar soluções de backup e carregar seus dados.

4. Quanto aos seus dados, se não chegarmos a acordo, tentaremos vender informações pessoais/segredos comerciais/bancos de dados/códigos-fonte – em geral, tudo o que tem um valor no mercado escuro – para vários fatores de ameaças em um só. Então tudo isso será publicado em nosso blog -.

5. Somos mais do que negociáveis e definitivamente encontraremos o caminho para resolver isso rapidamente e chegar a um acordo que satisfaça a ambos.

*Se você está realmente interessado em nossa assistência e nos serviços que fornecemos, você pode entrar em contato conosco seguindo instruções simples*:

1. Instale o navegador TOR para ter acesso à nossa sala de bate-papo – hxxps://www.torproject.org/download/.

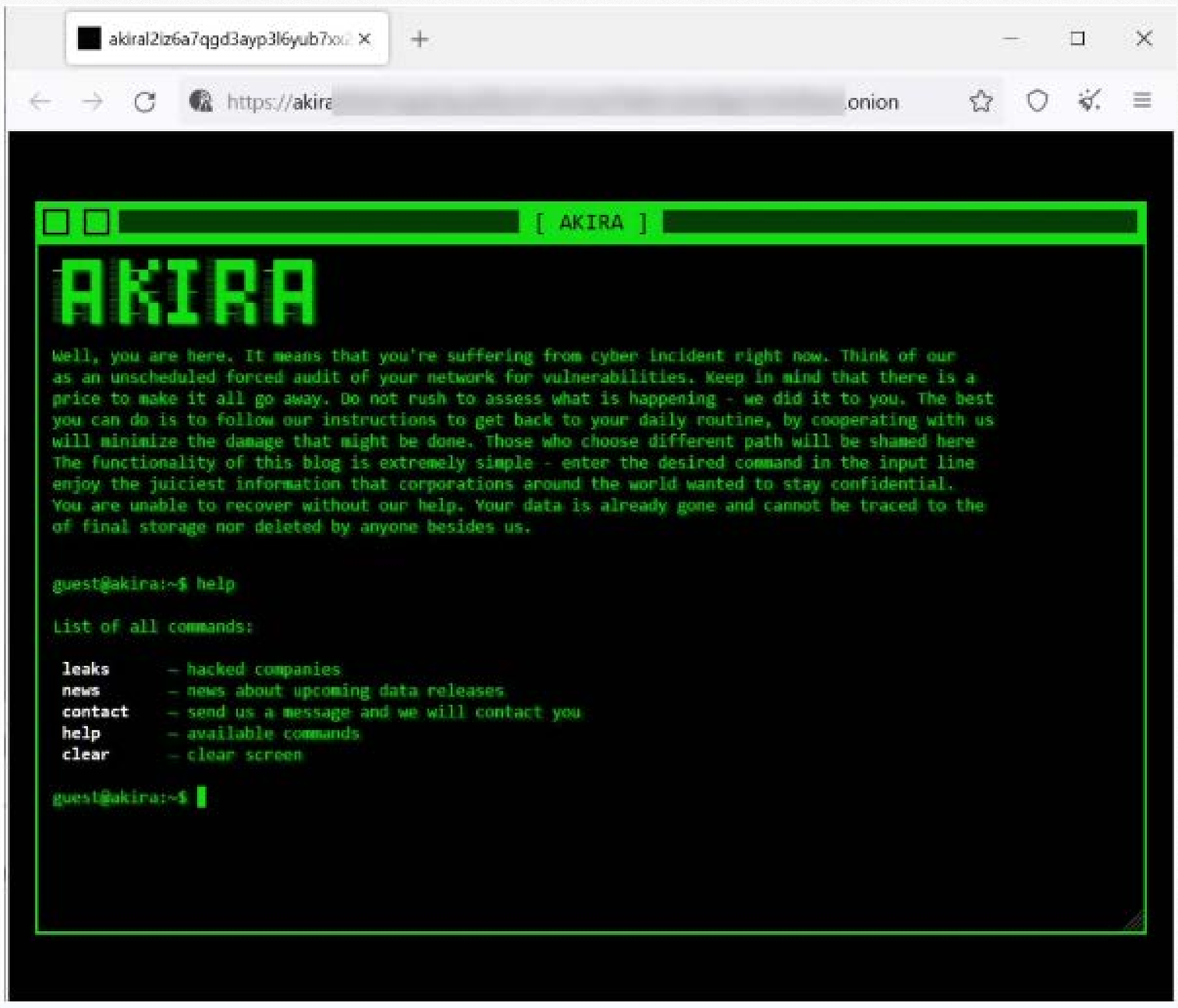
2. Cole este link – -.

3. Use este código – – – para entrar em nosso bate-papo.

Tenha em mente que quanto mais rápido você entrar em contato, menos danos causamos.

# Site de vazamento de dados usado para extorquir vítimas

Como outras operações de ransomware, Akira violará uma rede corporativa e se espalhará lateralmente para outros dispositivos. Depois que os agentes de ameaças obtiverem credenciais de administrador de domínio do Windows, eles implantarão o ransomware em toda a rede.
No entanto, antes de criptografar arquivos, os agentes de ameaças roubarão dados corporativos para alavancar em suas tentativas de extorsão, alertando as vítimas de que eles serão divulgados publicamente se um resgate não for pago.
A gangue Akira colocou muito esforço em seu site de vazamento de dados, dando-lhe um visual retrô onde os visitantes podem navegar digitando comandos, como mostrado abaixo.




Site de vazamento de dados / Foto: BleepingComputer.

No momento em que este artigo foi escrito, Akira vazou os dados de quatro vítimas em seu site de vazamento de dados, com o tamanho dos dados vazados variando de 5,9 GB para uma empresa a 259 GB para outra.

A partir de negociações vistas pelo BleepingComputer, a gangue de ransomware exige resgates que variam de US$ 200 mil a milhões de dólares.

Fontes: pcrisk / BlackHatEthicalHackig / bleepingcomputer / boletimsec.com.br/

Gate7 - Diego Rodrigues - Cyber Security

GATE7
IT SOLUTIONS

# Informativo
# GATE7

comercial@gate7.com.br (41) 3073-1403 https://gate7.com.br