

Ransomware Lynx: saiba detalhes da operação e como mitigar essa ameaça

By Rebecca Bezerra

Published: 2025-03-26 · Archived: 2026-04-05 21:44:55 UTC

Por [Ícaro Cesar](#) e [Ismael Rocha](#): A crescente sofisticação dos ataques cibernéticos exige que empresas estejam sempre um passo à frente na proteção de seus dados. O **Lynx Ransomware** se destaca como uma das ameaças mais avançadas da atualidade, explorando vulnerabilidades para comprometer infraestruturas críticas.

Para ajudar organizações a entender e mitigar esse risco, apresentamos o Ransomware Lynx sob três perspectivas essenciais: **Estratégica, Tática e Operacional**. Neste artigo, apresentamos os principais insights desse estudo, trazendo uma visão completa sobre os métodos do malware, seus impactos e as melhores práticas para proteção.

Continue a leitura e descubra como fortalecer sua defesa cibernética contra essa ameaça emergente!

O **ransomware** continua sendo uma das maiores ameaças à **segurança cibernética** global, com ataques cada vez mais sofisticados e direcionados a empresas e instituições. Nos últimos anos, a frequência e a complexidade dessas investidas cresceram exponencialmente, e essa tendência se intensifica em 2025, com **novas variantes explorando vulnerabilidades inéditas**.

Dentro desse cenário, o **Ransomware Lynx** se destaca como uma ameaça emergente, utilizando **técnicas avançadas de evasão e criptografia** para tornar a recuperação dos sistemas afetados extremamente difícil. Seu impacto já foi observado em diversos ataques documentados, reforçando a necessidade de **estratégias de defesa eficazes, monitoramento constante e resposta rápida a incidentes**.

Para aprofundar o conhecimento sobre essa ameaça, a equipe **CTI-Purple Team da ISH Tecnologia** realizou uma **análise detalhada do Ransomware Lynx**, explorando seu funcionamento, vetores de ataque e recomendações de mitigação. Continue a leitura e descubra como proteger sua organização contra essa nova onda de ataques cibernéticos.

Setores e regiões mais afetadas pela ameaça

O **Lynx Ransomware** tem como alvo principal **empresas que lidam com dados críticos** e possuem **infraestruturas digitais essenciais para suas operações**. Esse ransomware foca ataques em setores estratégicos, onde a **interrupção de serviços pode causar grandes prejuízos operacionais e financeiros**.

Principais setores mais afetados pelo Ransomware Lynx:

- **Financeiro** – Instituições bancárias e empresas de pagamentos digitais.
- **Manufatura** – Indústrias que dependem de processos automatizados.
- **Arquitetura e Construção** – Organizações com projetos e dados estratégicos.

- **Energia** – Infraestruturas críticas que garantem fornecimento elétrico e combustíveis.

Além de **explorar vulnerabilidades em empresas de diferentes portes**, o **Ransomware Lynx tem alcance global**, atingindo organizações em diversas regiões. Sua capacidade de **se adaptar a diferentes ambientes digitais** amplia o potencial de lucro dos cibercriminosos, tornando essa ameaça ainda mais preocupante para empresas de todos os tamanhos.

Quer saber mais sobre as táticas desse ransomware e como proteger sua empresa? Continue a leitura para entender a abrangência global do Lynx e como mitigar os riscos.

Países vítimas do Lynx Ransomware

O **Lynx Ransomware** Group surgiu em meados de 2024 e tem sido amplamente reconhecido como uma evolução do [INC ransomware](#) que surgiu em meados de 2023, operando por meio de um modelo **Ransomware-as-a-Service**.

Atividades do Lynx desde seu surgimento

Essa abordagem permite que afiliados utilizem sua infraestrutura e ferramentas para lançar ataques de forma rápida e em larga escala, sem a necessidade de desenvolver o malware do zero.

Como já mencionado, o grupo tem direcionado seus ataques para setores considerados críticos, essa seleção de alvos se deve à sensibilidade dos dados e ao potencial de causar impactos significativos nas operações, fazendo com que as vítimas se vejam pressionadas a pagar o resgate. Abaixo, podemos observar o website de Vazamentos de Dados das vítimas, onde ocorre o processo de dupla extorsão.

Leak Site do Lynx

Diversas empresas de grande porte já saíram na mídia como vítimas dos ataques do **Lynx**. Relatos de incidentes envolvendo estas organizações demonstram a abrangência das operações, evidenciando como o grupo consegue alcançar empresas que atuam em mercados nacionais e internacionais, causando prejuízos não apenas financeiros, mas também à reputação dos envolvidos.

Abaixo podemos observar um exemplo de dados vazados, com um alto preço de resgate, onde destaca-se a categoria de dados vazados:

Exemplo de Vazamento no Leak Site do Lynx

Embora o grupo afirme evitar alvos considerados “**socialmente importantes**” (conforme podemos observar na imagem abaixo), como hospitais e órgãos governamentais, a visibilidade dos ataques e a divulgação de informações sensíveis demonstram o potencial devastador de suas operações.

A atuação do Lynx ressalta a necessidade de uma postura de defesa cibernética robusta, capaz de mitigar os riscos e proteger os dados críticos das organizações.

Discurso de imprensa do grupo

Modelo de negócio da ameaça

O **Lynx Ransomware** opera no modelo **Ransomware-as-a-Service (RaaS)**, permitindo que cibercriminosos afiliados utilizem uma **infraestrutura pronta e constantemente atualizada** para realizar ataques sem precisar desenvolver o malware do zero.

Como funciona o RaaS do Lynx?

- O grupo centraliza o **desenvolvimento e manutenção do ransomware**.
- Afiliados recebem um **kit completo** para lançar ataques.
- A plataforma inclui **interfaces de gerenciamento de vítimas e suporte via rede Tor**.
- O monitoramento dos ataques acontece **em tempo real**, maximizando a eficiência da operação.

Essa abordagem acelera a **expansão do ransomware**, tornando-o mais acessível e perigoso. Enquanto os afiliados se concentram na execução dos ataques, o grupo responsável pelo Lynx garante **atualizações constantes** e suporte tecnológico, aumentando a sofisticação e a letalidade da ameaça.

Modelo de RaaS com afiliados

O **Lynx Ransomware** adota a perigosa estratégia de **dupla extorsão**, na qual os dados das vítimas são **criptografados e exfiltrados**. Isso significa que, além de bloquear o acesso às informações, os cibercriminosos ameaçam **vazar ou vender os dados roubados**, aumentando a pressão para o pagamento do resgate.

Por que a dupla extorsão é tão eficaz?

- **Maior chance de pagamento:** As vítimas temem não apenas a perda dos dados, mas também a exposição de informações sigilosas.
- **Pressão psicológica e reputacional:** Empresas afetadas podem sofrer danos irreparáveis à imagem e à confiança de clientes e parceiros.
- **Lucros ampliados para cibercriminosos:** O modelo gera ganhos expressivos tanto para os operadores do ransomware quanto para seus afiliados.

A **dupla extorsão** tem se tornado uma das táticas mais utilizadas por grupos de **ransomware**, tornando a proteção contra **vazamento de dados e criptografia maliciosa** ainda mais crucial para empresas de todos os portes.

Modelo de Dupla Extorsão

O **Lynx Ransomware** opera com um rigoroso processo de **seleção e monitoramento de afiliados**, garantindo que apenas operadores experientes tenham acesso à sua infraestrutura. Para incentivar ataques bem-sucedidos, o grupo oferece uma **participação expressiva nos lucros**, chegando a **80% do valor do resgate**.

Por que esse modelo fortalece o Ransomware Lynx?

- **Alto incentivo financeiro:** Afiliados altamente motivados devido aos grandes lucros.
- **Escalabilidade do ataque:** Expansão rápida da ameaça sem necessidade de novos desenvolvedores.
- **Maior eficiência operacional:** O grupo central mantém o ransomware atualizado enquanto os afiliados executam os ataques.

Esse modelo de **Ransomware-as-a-Service (RaaS)** garante a **resiliência e escalabilidade** do Lynx, tornando-o uma das ameaças **mais lucrativas e persistentes** do cenário cibernético.

Análise do Lynx Ransomware

Nesta seção iremos explorar as principais características do Lynx Ransomware. Abaixo, podemos observar o fluxo macro da execução do Lynx Ransomware.

Falta de presença e ofuscação

O **Lynx Ransomware** se diferencia de outras variantes por não utilizar **técnicas de ofuscação** em seu código, tornando sua análise mais acessível para pesquisadores de segurança. Com ferramentas simples, como o **'strings'**, é possível extrair informações valiosas sobre seu funcionamento, sem a necessidade de técnicas avançadas de engenharia reversa.

O que isso significa para especialistas em segurança?

- **Facilidade na detecção:** A ausência de ofuscação permite identificar padrões e indicadores de comprometimento (IoCs) rapidamente.
- **Extração de informações cruciais:** Com ferramentas básicas, é possível acessar comandos, menus de ajuda e dados codificados.
- **Resposta mais ágil a incidentes:** A identificação rápida do malware possibilita estratégias eficazes de mitigação.

Na análise do Lynx Ransomware, foi possível extrair facilmente seu **menu de 'help'** e **um bloco de string codificado em Base64**, demonstrando como sua falta de camuflagem facilita investigações.

Identificação de Strings valiosas pela falta de Ofuscação

Com o uso do *PowerShell* somos capazes de decodificar o Base64, permitindo que tenhamos extraído a Nota de Ransomware, conforme podemos observar abaixo.

Decodificação de Nota de Ransomware

Com a *flag* **help**, somos capazes de observarmos de fato o menu de ‘help’ do Lynx Ransomware, podemos assim observar todas as capacidades que o Lynx pode implementar em sua execução.

Menu de ajuda do Lynx

Engenharia reversa do Lynx Ransomware

A partir desta seção, analisamos de forma técnica utilizando Engenharia Reversa para analisar as principais capacidades do Lynx. Abaixo podemos observar que a função main, também não há nenhuma ofuscação de alteração de fluxo do malware, sendo assim bem fácil de seguir o seu fluxo.

Função 'Main' do Lynx Ransomware

Decodificação de BASE64 da nota do Ransomware

Após checar se o Lynx foi executado com algum argumento (as *flags* descritas acima), o Lynx realiza o processo de decodificação do bloco de dados em *Base64*, conforme vimos anteriormente e anexo *do ID da Vítima* na **Nota de Ransomware**.

Funções de decodificação e construção da Nota de Ransomware

Abaixo, podemos observar que o Lynx não implementa nenhuma técnica de ofuscação de API, utilizando de maneira clara para seus propósitos. No caso abaixo, o Lynx utiliza o [CryptStringToBinaryA](#) para realizar o processo de *decode* da Nota de Ransomware.

Função de decodificação Base64 por meio de WinAPIs

Abaixo podemos observar a função, que adiciona o ID da Vítima à Nota de Ransomware (após a decodificação da Nota de Ransomware em *Base64*) identificado para esta amostra como “**66ed20b7c8dfe0f702f199dd**”.

Função de adição do ID da vítima na Nota de Ransomware

Execução paralela de criptografia via threads

Após isso, o Lynx irá executar uma *Thread* independente para criptografar os arquivos, enquanto executa as capacidades indicadas pelas *flags* utilizadas para executá-lo. Abaixo, podemos observar o uso da criação de uma nova *Thread* por meio da API [CreateThread](#), e tendo como endereço de início do que será executado nesta *Thread* a função de criptografia, na qual será utilizado o algoritmo AES.

Criação de Thread para criptografia paralela

Abaixo, podemos observar o fluxo da função principal que implementa o algoritmo de criptografia de arquivos através de um *loop*.

Loop de criptografia

Também fomos capazes de identificar o algoritmo, por conta da identificação das constantes referente à tabela **S-Box** do AES, conforme podemos observar abaixo:

Constantes do S-Box do AES

Montagem de discos “ocultos” para aumentar o impacto

O **Lynx Ransomware** adota técnicas avançadas para **localizar e criptografar discos ocultos** no sistema, tornando a recuperação de dados ainda mais difícil para as vítimas. Ao ser executado com a flag `--load-drives`, o malware inicia um processo automatizado para detectar **backups escondidos**, impedindo que os usuários restaurem suas informações.

Como funciona essa técnica?

- **Identificação de discos ocultos:** O Lynx usa as APIs `FindFirstVolumeW` e `GetVolumePathNamesForVolumeNameW` para localizar unidades escondidas.
- **Montagem automática:** O ransomware percorre um array de possíveis volumes, montando cada um deles.
- **Criptografia de dados:** Após a montagem, os discos são criptografados, eliminando qualquer possibilidade de recuperação manual.

Essa abordagem aumenta significativamente o impacto do ataque, pois **neutraliza backups armazenados em unidades ocultas**, forçando a vítima a considerar o pagamento do resgate.

Array de letras para montagem de disco

Em sequência, o código executa um *loop* neste *array*, com o objetivo de tentar montar cada um destes possíveis Discos no sistema.

Loop de montagem de discos para futura criptografia

Implementação não comum da exclusão do Volume Shadow Copy

O **Lynx Ransomware** adota uma técnica avançada para **excluir backups do Volume Shadow Copy (VSS)** sem utilizar os binários nativos do Windows, dificultando a detecção por soluções de segurança. Em vez de comandos tradicionais como `vssadmin delete shadows`, o Lynx manipula o **tamanho do VSS para zero** por meio da **API DeviceIoControl**, eliminando completamente os pontos de restauração do sistema.

Por que essa técnica é eficaz?

- **Evita detecção por ferramentas de segurança** que monitoram comandos tradicionais de exclusão de backup.
- **Impossibilita restauração manual**, forçando a vítima a buscar alternativas mais custosas.
- **Aumenta a taxa de sucesso do ransomware**, já que as vítimas perdem o acesso a seus dados sem chance de recuperação.

Ao remover silenciosamente os backups do sistema, o Lynx **maximiza o impacto do ataque** e pressiona as vítimas a pagar o resgate. Essa abordagem reforça a necessidade de **estratégias de backup offline e soluções avançadas de segurança** para evitar perdas irreversíveis.

Implementação de técnica de exclusão do VSS via WinAPI

Assim, o Lynx implementa de maneira peculiar a técnica de Impacto [Inhibit System Recovery \[T1490\]](#) do MITRE ATT&CK, de maneira que evade qualquer tentativa de implementar uma detecção através de Logs.

Criação e configuração do Wallpaper padrão

O **Lynx Ransomware** adota uma estratégia visual para **intimidar as vítimas e reforçar a pressão pelo pagamento do resgate**. Caso a flag `--no-background` não seja utilizada, o malware **altera automaticamente o wallpaper do sistema**, exibindo a **Nota de Ransomware** na tela do usuário.

Como funciona essa técnica?

- **Criação dinâmica do wallpaper:** O Lynx gera um arquivo chamado `background-image.jpg` na pasta Temporária do Windows.
- **Uso de APIs para escrita da imagem:** O ransomware escreve a nota de resgate na imagem antes de defini-la como fundo de tela.
- **Impacto psicológico imediato:** A vítima é confrontada visualmente com a exigência do resgate assim que acessa o computador.

Essa abordagem **aumenta a sensação de urgência** e diminui o tempo de resposta das vítimas, tornando-as mais propensas a considerar o pagamento. A alteração do wallpaper também **sinaliza claramente a infecção** , reforçando a necessidade de estratégias proativas de defesa contra o **Lynx Ransomware** .

Criação dinâmica de um Bitmap para a criação do Wallpaper

Basicamente, o fluxo acima irá criar um Wallpaper preto tendo a Nota de Ransomware centralizada na imagem, do tamanho exato da tela de Desktop do dispositivo infectado. Após criar o Wallpaper, o Lynx modifica a Chave de Registro HKU\\Control Panel\Desktop\Wallpaper para forçar a configurar o Wallpaper padrão do dispositivo, por meio da API [RegOpenKeyW](#) e [RegSetValueExW](#).

Alteração do Wallpaper padrão do dispositivo infectado

Abaixo, podemos observar a tela do dispositivo infectado após a execução desta técnica.

Wallpaper criado dinamicamente configurado pelo Lynx

Envio de nota através das impressoras locais

Uma capacidade interessante e única do grupo, é o envio de *jobs* para Impressoras locais da Nota de Ransomware do Lynx, através das APIs [OpenPrinter](#) e [StartDocPrinterW](#).

Scan de Impressoras Locais e Impressão de Nota de Ransomware

Por meio desta técnica, o adversário acrescenta um fator psicológico que pode aumentar o impacto e induzir o cliente a ter mais disposição para realizar o pagamento pelos dados.

MITRE ATT&CK – TTPs

Mapeamento Tático do Lynx Ransomware segundo MITRE ATT&CK

O Lynx Ransomware utiliza diversas técnicas de evasão, descoberta e impacto para maximizar os danos e dificultar a recuperação do sistema. A tabela abaixo apresenta um resumo das principais táticas e técnicas identificadas, com base na matriz MITRE ATT&CK:

Tática	ID	Técnica	Descrição
Defense Evasion	T1140	Deobfuscate/Decode Files or Information	Com o objetivo de dificultar a análise estática, o Lynx codifica a nota de resgate em Base64 e realiza sua decodificação de forma dinâmica.
Discovery	T1083	File and Directory Discovery	Utiliza APIs do Windows para percorrer recursivamente diretórios e identificar arquivos para criptografia. Evita arquivos com extensões <code>.exe</code> , <code>.msi</code> e <code>.lynx</code> , além dos diretórios <code>Program Files</code> , <code>Program Files (x86)</code> e <code>AppData</code> .
Discovery	T1082	System Information Discovery	Coleta informações do sistema, como a quantidade de núcleos da CPU, com o objetivo de otimizar a criação de múltiplas threads.
Discovery	T1135	Network Share Discovery	Enumera diretórios compartilhados na rede, ampliando o impacto ao criptografar recursos disponíveis em outros dispositivos.
Discovery	T1057	Process Discovery	Detecta e, se configurado com a flag <code>--stop-processes</code> , encerra processos específicos durante a execução do ataque.
Impact	T1486	Data Encrypted for Impact	Utiliza o algoritmo AES para criptografar os arquivos do sistema, exigindo pagamento de resgate para a restauração dos dados.
Impact	T1491.001	Internal Defacement: Wallpaper	Altera o wallpaper da máquina comprometida para exibir a nota de resgate, deixando claro que o sistema foi infectado.
Impact	T1490	Inhibit System Recovery	Remove silenciosamente cópias de sombra (Volume Shadow Copy), dificultando a restauração do sistema sem pagamento de resgate.
Impact	T1489	Service Stop	Se configurado com a flag <code>--kill</code> , finaliza serviços e processos específicos para facilitar a criptografia de arquivos em uso.

Malware Behavior Catalog (MBC)

Análise Comportamental do Lynx Ransomware segundo o MBC (Malware Behavior Catalog)

A seguir, apresentamos um mapeamento das táticas e técnicas utilizadas pelo Lynx Ransomware com base no catálogo MBC (Malware Behavior Catalog). Este levantamento visa destacar as ações executadas pela ameaça em

diferentes fases de sua operação maliciosa:

Tática	Técnica	Descrição
Anti-Static Analysis	Obfuscated Files or Information::Encoding – Standard Algorithm	O Lynx codifica a nota de resgate em Base64 para dificultar a análise estática e realiza a decodificação de forma dinâmica.
Cryptography	Encrypt Data::AES	Utiliza o algoritmo Rijndael/AES para criptografar os arquivos da vítima.
Collection	Screen Capture::WinAPI	Captura informações sobre as dimensões da tela com o objetivo de gerar o wallpaper da nota de resgate.
Discovery	System Information Discovery	Coleta informações do sistema, como o número de núcleos da CPU, para otimizar o uso de threads paralelas.
Discovery	File and Directory Discovery	Percorre o sistema recursivamente usando APIs do Windows para localizar arquivos a serem criptografados. Evita arquivos com extensões <code>.exe</code> , <code>.msi</code> e <code>.lynx</code> , além dos diretórios <code>Program Files</code> , <code>Program Files (x86)</code> e <code>AppData</code> .
File System	Create/Write/Delete File	Cria notas de resgate, criptografa arquivos e altera suas extensões para <code>.LINX</code> em loops contínuos.
Process	Create Thread	Utiliza múltiplas threads para executar tarefas paralelas, evitando que a amostra fique limitada a uma única atividade.
Operating System	Registry::Set Registry Value	Altera a chave de registro responsável pelo wallpaper para exibir a nota de resgate.
Operating System	Wallpaper	Define um novo wallpaper com a nota de resgate, como tática de intimidação e pressão psicológica.
Impact	Data Encrypted for Impact	Criptografa os dados da vítima com o objetivo de exigir pagamento pelo resgate.

Indicadores de Comprometimento (IOCs)

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 Comprometimento (IoCs) relacionadas a análise do(s) artefato(s) deste relatório.

Indicadores de Comprometimento (IoCs)

Tabela 1 – Indicadores de Comprometimento

MD5	57f45c0738af9cd49c61984ea99f83ca
SHA-1	5338cae40e5419a0567b8162c52484f390284f15
SHA-256	b378b7ef0f906358eec595777a50f9bb5cc7bb6635e0f031d65b818a26bdc4ee
Nome do Arquivo	b378b7ef0f906358eec595777a50f9bb5cc7bb6635e0f031d65b818a26bdc4ee.exe

Tabela 2 – Indicadores de Comprometimento

MD5	65c0c7c9fe6bc1d5296447aae6c6c14c
SHA-1	67217e5c6859afb1b2c736625fcf8bee9ad158cc
SHA-256	4e5b9ab271a1409be300e5f3fd90f934f317116f30b40eddc82a4dfd18366412
Nome do Arquivo	win.exe

Tabela 3 – Indicadores de Comprometimento

MD5	0e521e0452f113cdf8b5c2fa6580db1f
SHA-1	4182106fbec3d3fcecde5056b8246b6db317c2a3
SHA-256	f71fc818362b1465fc1deb361de36badc73ac4dd9e815153c9022f82c4062787
Nome do Arquivo	build.exe

Tabela 4 – Indicadores de Comprometimento

MD5	ff458208c49836cdec92f0a4a7ba6afd
SHA-1	c0b013fd8a38c0e7ffa8394de49f401ac7625773
SHA-256	5da4f51e3ced3166336277bb04c32d0cd20f3e28db3d4f02826fee88b7583040
Nome do Arquivo	windows.exe

Tabela 5 – Indicadores de Comprometimento

MD5	a20886a5b378624d16972db66bd4e7e1
SHA-1	89d84ab72b2e5116f4a46b19f4d8096a0a9c7a88
SHA-256	31de5a766dca4eaae7b69f807ec06ae14d2ac48100e06a30e17cc9accfd5193

Nome do Arquivo	dd.exe
------------------------	--------

Tabela 6 – Indicadores de Comprometimento

MD5	f16238836909d07f86154c5ccbade96a
SHA-1	558f259459d0ed1b30cbeaee71aa46eb5e40b090
SHA-256	3e68e5742f998c5ba34c2130b2d89ca2a6c048feb6474bc81ff000e1eaed044e
Nome do Arquivo	build.exe

Tabela 7 – Indicadores de Comprometimento

MD5	b1d81e8bbecccc547645d17395538a2d
SHA-1	637728e7bd41bb100a5730547e53960d2bab9b29
SHA-256	0315dbb793f855f154aa8d227151f1098bd9b580a4f85064648b85bac1321663
Nome do Arquivo	0315dbb793f855f154aa8d227151f1098bd9b580a4f85064648b85bac1321663.exe

Tabela 8 – Indicadores de Comprometimento

MD5	146d350fd6271b4411714c630d8cda87
SHA-1	f22bda5fa8a632e7d2dd2982300b4374168f8f32
SHA-256	589ff3a5741336fa7c98dbcef4e8aecea347ea0f349b9949c6a5f6cd9d821a23
Nome do Arquivo	589ff3a5741336fa7c98dbcef4e8aecea347ea0f349b9949c6a5f6cd9d821a23.exe

Tabela 9 – Indicadores de Comprometimento

MD5	571684f28ce1cf4d8236dbd46ef6f7f0
SHA-1	d758d1f048ace4547dd3c22357aa2cf223426a50
SHA-256	468e3c2cb5b0bbc3004bbf5272f4ece5c979625f7623e6d71af5dc0929b89d6a
Nome do Arquivo	468e3c2cb5b0bbc3004bbf5272f4ece5c979625f7623e6d71af5dc0929b89d6a.exe

Tabela 10 – Indicadores de Comprometimento

MD5	d972bbbb3edb0e5ab5751b911f3dda17
------------	----------------------------------

SHA-1	c632223f5f7a8a469bbf07eb017863bb83564b84
SHA-256	571f5de9dd0d509ed7e5242b9b7473c2b2cbb36ba64d38b32122a0a337d6cf8b
Nome do Arquivo	11.exe

Recomendações para manter seu negócio seguro

Além dos indicadores de comprometimento elencados acima pela ISH, poderão ser adotadas medidas visando a mitigação da infecção do referido *malware*, como por exemplo:

Mantenha sistemas e softwares atualizados

- Garanta que todos os sistemas operacionais, aplicativos e softwares de segurança estejam atualizados com os patches mais recentes. Isso corrige vulnerabilidades que podem ser exploradas por atacantes.

Implemente soluções de segurança confiáveis

- Utilize ferramentas de segurança robustas, como antivírus e firewalls, para detectar e bloquear ameaças potenciais.

Realize backups regulares

- Mantenha backups atualizados e armazenados em locais seguros, preferencialmente offline ou em ambientes isolados, para garantir a recuperação de dados sem necessidade de pagar resgates.

Eduque e treine funcionários

- Promova treinamentos regulares sobre segurança cibernética para que os colaboradores reconheçam e evitem e-mails de phishing e outras tentativas de ataque.

Restrinja privilégios de acesso

- Adote o princípio do menor privilégio, garantindo que usuários tenham apenas as permissões necessárias para suas funções, limitando o potencial de movimentação lateral de atacantes na rede.

Monitore e analise atividades da rede

- Implemente ferramentas de monitoramento para identificar atividades suspeitas ou não autorizadas, permitindo respostas rápidas a possíveis incidentes.

Desenvolva um plano de resposta a incidentes

- Estabeleça e teste regularmente um plano de resposta a incidentes específico para ataques de ransomware, assegurando que sua equipe saiba como agir rapidamente para conter ameaças e restaurar operações.

Utilize autenticação Multifator (MFA)

- Implemente MFA para adicionar uma camada extra de segurança, dificultando o acesso não autorizado, mesmo que credenciais sejam comprometidas.

Desative serviços e protocolos não utilizados

- Reduza a superfície de ataque desativando serviços e protocolos desnecessários que podem ser explorados por cibercriminosos.

Realize avaliações de vulnerabilidades

- Conduza avaliações regulares para identificar e corrigir pontos fracos em sua infraestrutura de TI antes que sejam explorados.

Referências:

- **Heimdall by ISH Tecnologia**
- **CTI Purple Team by ISH Tecnologia**
- [MITRE ATT&CK](#)
- [Ransomware.live](#)

Source: <https://ish.com.br/en/blog/ransomware-lynx-saiba-como-mitigar-essa-ameaca/>