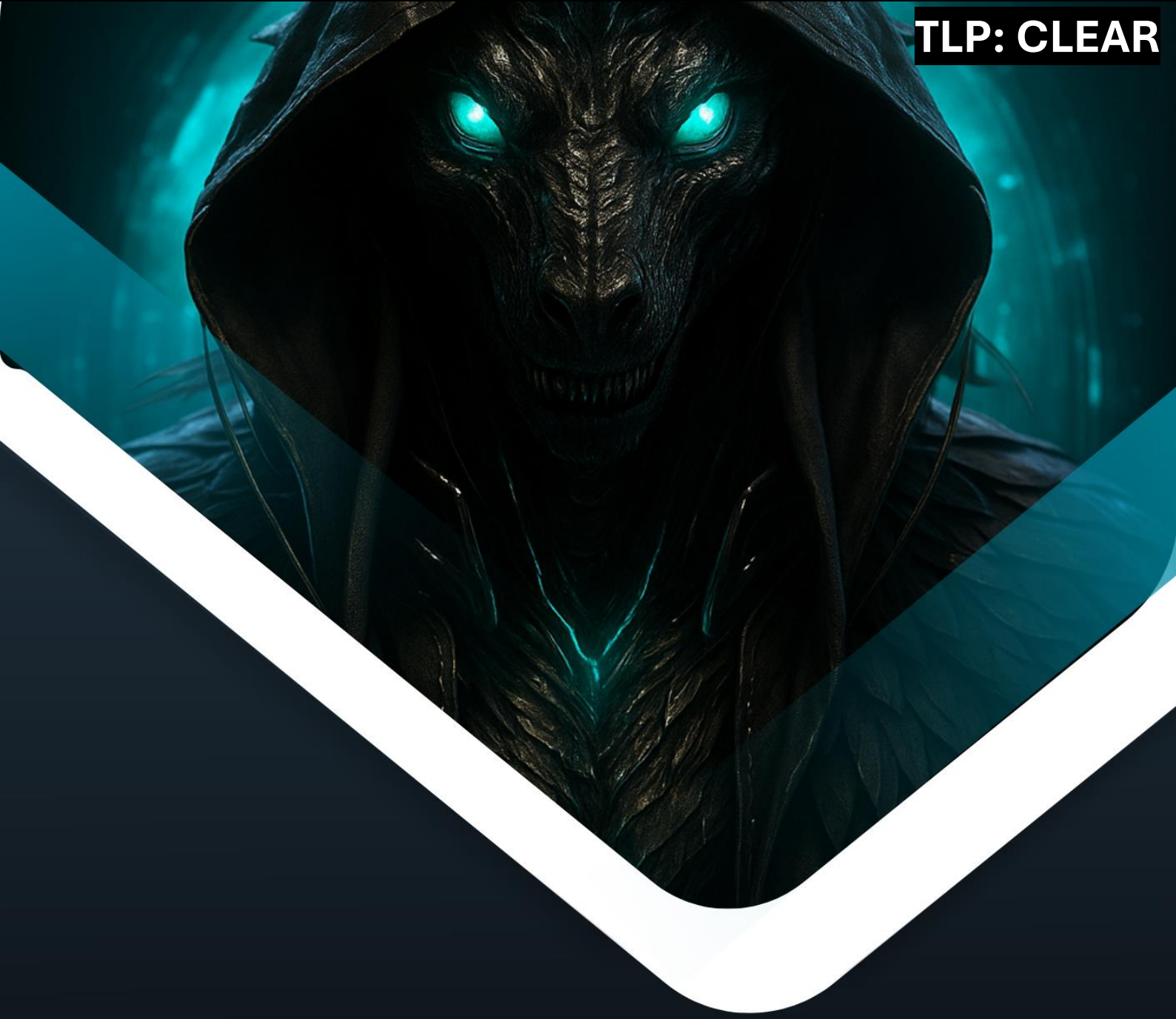
TLP: CLEAR



Pesquisa de Cibersegurança
Cyber Threat Actor

Análise da Kill Chain do Mallox Ransomware

heimdall
security research

Acesse nossa comunidade no WhatsApp, clicando na imagem abaixo!

heimdall
security research
A DIVISION OF ISH

Acesse as análises produzidas pela ISH Tecnologia sobre Táticas, Técnicas e Procedimentos (TTPs) de Threat Actors, malwares emergentes, vulnerabilidades críticas e outros temas relevantes em cibersegurança. Clique na imagem abaixo para conferir nosso blog.

SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

SUMÁRIO EXECUTIVO: CONHECENDO A AMEAÇA

Este relatório de segurança, desenvolvido pela equipe de **Inteligência de Ameaças da ISH, *Heimdall***, tem como objetivo proporcionar uma compreensão aprofundada e um dimensionamento preciso das ameaças cibernéticas identificadas. O documento está estruturado em três níveis de abordagem: ***Estratégico***, ***Tático*** e ***Operacional***, garantindo uma visão completa e integrada das ameaças e ações recomendadas.

ESTRATÉGICO

INTRODUÇÃO SOBRE AMEAÇA

O **Mallox Ransomware** — também identificado como **TargetCompany**, **FARGO**, **Tohnichi** ou **XOLLAM** — é uma variante ativa desde **junho de 2021**, conhecida por explorar **servidores Microsoft SQL (MS-SQL)** desprotegidos como vetor de acesso inicial. Pesquisas recentes apontam um crescimento acentuado das atividades do grupo, com aumento de mais de **174% em incidentes** no último ano conforme relatado pela Unidade 42 da Palo Alto Networks. Esse crescimento está ligado à **expansão das operações do grupo**, incluindo o **recrutamento ativo de afiliados** por meio de **fóruns clandestinos** em ambientes de dark web, o que reforça seu modelo de negócios baseado em RaaS. Os atacantes frequentemente utilizam **scripts automatizados**, **ferramentas de varredura de rede** e realizam **exfiltração de dados** antes da criptografia.

Além de **criptografar dados** com algoritmos robustos como **ChaCha20**, o grupo também adota a prática de **dupla extorsão**, ameaçando divulgar os dados exfiltrados das vítimas em **sites de vazamento na dark web**, caso o pagamento do resgate não seja realizado. Essa abordagem agressiva e altamente lucrativa torna o Mallox uma ameaça crítica para organizações de diversos setores, incluindo **governo, serviços jurídicos, tecnologia da informação, manufatura e transporte**.

Diante desse cenário, o ransomware Mallox representa hoje uma das ameaças mais ativas e resilientes no panorama cibernético global, exigindo ações coordenadas de prevenção, detecção e resposta rápida por parte de organizações e equipes de segurança.

VITIMOLOGIA DO MALLOX RANSOMWARE

A distribuição geográfica das vítimas do Mallox é **global**, mas apresenta maior concentração em países como **Brasil**, **Vietnã**, **China**, **Estados Unidos**, **Canadá**, **Reino Unido**, **Alemanha** e **Austrália**. De acordo com dados de telemetria e fontes abertas de inteligência, **o Brasil destaca-se na América Latina** como um dos países mais atingidos. Assim como outros grupos, os operadores do Mallox parecem evitar alvos na antiga União Soviética, e não há registros de ataques a sistemas configurados com idioma russo como padrão.

A atuação do Mallox expandiu-se rapidamente, especialmente a partir de 2023, com um **aumento de aproximadamente 174% nos ataques** em comparação ao segundo semestre de 2022. Essa intensificação coincide com a transição do grupo para um modelo mais distribuído de operação e **recrutamento de afiliados** em fóruns clandestinos, permitindo a personalização de campanhas conforme o idioma, a região e o setor das vítimas.

Figura 1 - Países Vítimas do Mellox Ransomware.

A estratégia de direcionamento do ransomware **Mallox** tem sido majoritariamente orientada pelo ganho financeiro, com pedidos de resgate que variam entre milhares e dezenas de milhares de dólares. O grupo por trás da ameaça tende a priorizar organizações com **receita anual superior a 10 milhões de dólares**, evidenciando um foco claro em alvos com maior capacidade de pagamento. Além disso, embora a motivação central seja financeira, os padrões

de ataque sugerem um possível interesse secundário em **espionagem comercial**, dada a escolha de setores estratégicos e sensíveis.

O ransomware Mallox tem demonstrado uma abordagem **ampla e oportunista**, atingindo empresas com **posturas de segurança frágeis** em setores diversos, incluindo:

- *Manufatura;*
- *Serviços profissionais e jurídicos;*
- *Atacado e varejo;*
- *Transporte;*
- *Tecnologia da Informação;*
- *Logística;*

Apesar dessa versatilidade, o grupo **evita explicitamente alvos nos setores de educação, governo** e **saúde**, o que pode indicar tanto considerações éticas quanto estratégias de evasão de investigações mais intensas. A escolha dos setores-alvo também levanta a hipótese de que a ameaça possa, em certos contextos, estar associada a **interesses geopolíticos** ou **de espionagem industrial**.

O impacto das campanhas do Mallox vai além da simples criptografia de arquivos. Os operadores executam técnicas de **dupla extorsão**, exfiltrando dados sensíveis antes da criptografia e **ameaçando publicá-los em sites de vazamento na dark web** caso o resgate não seja pago. Esse modelo causa **graves interrupções operacionais**, danos à reputação e possíveis implicações legais às vítimas, especialmente em setores regulamentados. A complexidade técnica e a velocidade de execução observadas nas amostras analisadas evidenciam uma ameaça que combina **sofisticação**, **persistência** e **capacidade de adaptação** às defesas modernas.

INCIDENTES ENVOLVENDO O MALLOX RANSOMWARE

Desde sua primeira detecção em junho de 2021, o ransomware Mallox tem evoluído significativamente, com uma série de incidentes notáveis que evidenciam sua crescente sofisticação e adaptabilidade. Abaixo, destacam-se os principais marcos e eventos associados a essa ameaça:

Linha do Tempo de Atividades

- **Junho de 2021:** Emergência do Mallox com ataques direcionados a organizações específicas, utilizando extensões de arquivo personalizadas como *.architek*, *.avast* e *.bitenc*, indicando uma abordagem adaptada às vítimas.
- **2022:** Transição para o modelo de Ransomware como Serviço *(RaaS),* com a adoção da marca "Mallox" e o início de campanhas de multiextorsão, incluindo a ameaça de vazamento de dados em sites na dark web.
- **Julho de 2023:** Relato de um aumento significativo (174%) nas atividades do Mallox em comparação ao segundo semestre de 2022, destacando sua crescente ameaça global.
- **Meados de 2023:** Descoberta de uma variante do Mallox para sistemas Linux, marcando a expansão da ameaça para além do ambiente Windows.
- **Novembro de 2024:** Ataque de grande repercussão à empresa Blue Yonder, fornecedora de soluções de gerenciamento da cadeia de suprimentos, afetando operações de empresas como a Starbucks, que teve que recorrer a métodos manuais para rastrear horas de trabalho de funcionários.
- **Dezembro de 2024:** Surgimento do grupo de ransomware FunkSec, que começou a assumir a responsabilidade por diversos ataques utilizando o ransomware Mallox, indicando uma possível fragmentação ou rebranding dentro do ecossistema de ameaças.

Evolução Técnica e Estratégica

O Mallox demonstrou uma notável capacidade de adaptação, expandindo seu alcance para sistemas Linux e VMware ESXi. Pesquisadores identificaram que afiliados do Mallox utilizaram uma versão modificada do código-fonte do ransomware Kryptina para desenvolver variantes voltadas para Linux, evidenciando a reutilização e adaptação de ferramentas existentes no cibercrime. Além disso, a descoberta de scripts personalizados em Python, como o *web_server.py*, indica o desenvolvimento de painéis web para a criação e

gerenciamento de cargas maliciosas, facilitando a operação por parte de afiliados e ampliando o alcance das campanhas.

Impacto e Implicações

Os incidentes associados ao Mallox têm causado interrupções significativas nas operações das organizações afetadas, além de potenciais exposições de dados sensíveis, isso é demonstrado na imagem abaixo, destacando em azul os dias que atividades maliciosas foram registradas ou atribuídas ao grupo. De 2020 para 2022, a ameaça estava em uma atividade contínua durante alguns meses, ao longo dos anos foi reduzindo gradativamente até o meio de 2023. De 2024 para início de 2025 ele se mantém ativo e constante.

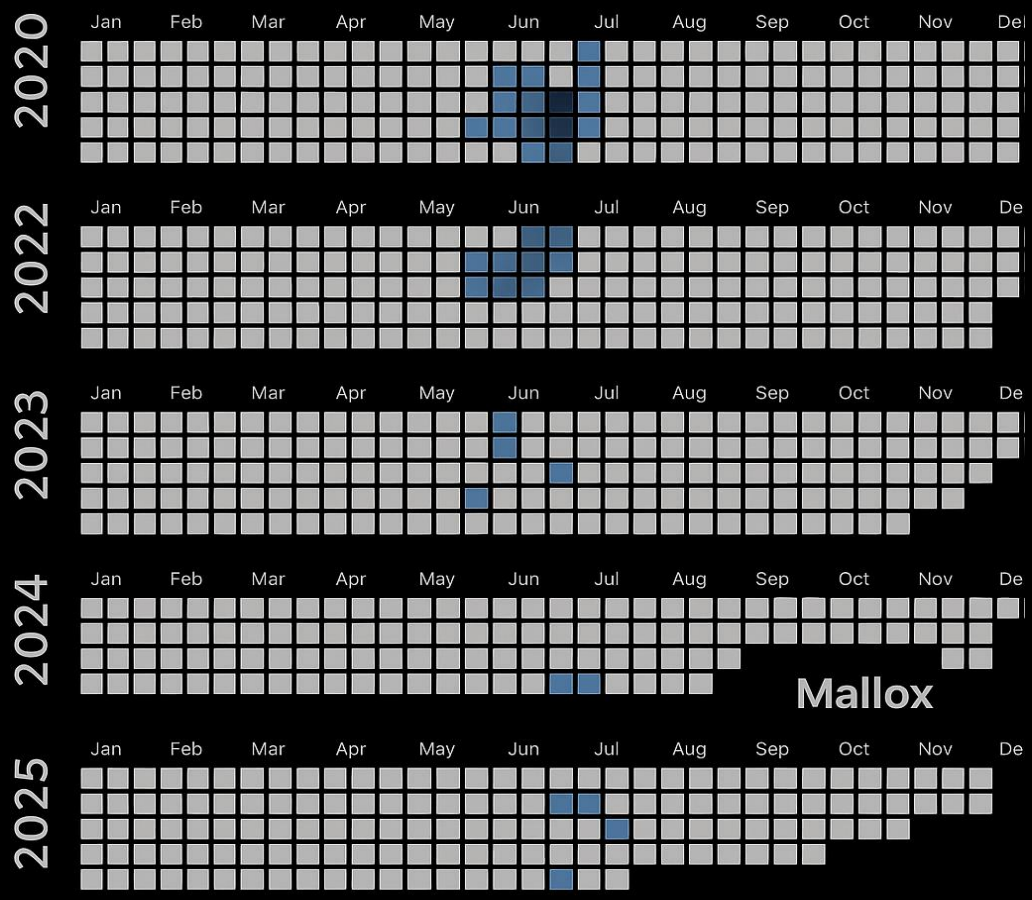


Figura 2- Incidentes envolvendo o Mallox ransomware desde 2020.

TÁTICO

MODELO DE NEGÓCIO DA AMEAÇA

O modelo de negócio do ransomware Mallox é estruturado sob o paradigma de Ransomware como Serviço (RaaS), permitindo que operadores centrais desenvolvam e mantenham a infraestrutura do malware, enquanto afiliados realizam os ataques. Essa abordagem descentralizada amplia o alcance das operações maliciosas e dificulta a atribuição direta dos responsáveis.

Desde sua transição para o modelo RaaS em 2022, o Mallox tem recrutado afiliados por meio de fóruns clandestinos, como Nulled e RAMP, oferecendo acesso ao ransomware em troca de uma porcentagem dos lucros obtidos com os resgates pagos pelas vítimas. Essa estratégia permite que indivíduos com diferentes níveis de habilidade técnica participem das operações, aumentando a frequência e a diversidade dos ataques. O Mallox emprega uma estratégia de dupla extorsão, onde os dados das vítimas são exfiltrados antes da criptografia. Caso o resgate não seja pago, os operadores ameaçam divulgar as informações roubadas em um site dedicado na dark web, aumentando a pressão sobre as vítimas para que efetuem o pagamento.

O Mallox tem demonstrado uma capacidade significativa de adaptação, com atualizações frequentes que incluem melhorias nos algoritmos de criptografia e na eficácia das técnicas de evasão. Essa evolução contínua torna o ransomware uma ameaça persistente e desafiadora para as defesas cibernéticas tradicionais. O modelo de negócio do Mallox, baseado em RaaS e dupla extorsão, representa uma ameaça significativa no cenário de segurança cibernética atual. Sua estrutura descentralizada, combinada com técnicas avançadas de ataque e uma infraestrutura robusta para vazamento de dados, exige uma abordagem proativa e multifacetada por parte das organizações para mitigar os riscos associados.

INFRAESTRUTURA DE VAZAMENTO

Uma das características mais marcantes da operação do ransomware Mallox é o uso de um Dedicated Leak Site (DLS) na dark web, hospedado em um endereço *.onion* acessível por meio do navegador *Tor*. Esse site funciona como uma plataforma de pressão psicológica e operacional sobre as vítimas, reforçando o modelo de dupla extorsão adotado pelo grupo. O site do Mallox é semelhante ao de outros grupos RaaS, apresentando uma estética limpa e focada em demonstrar profissionalismo. Ele contém páginas de navegação dedicadas para:

- Lista *de vítimas;*
- *Contato com operadores;*
- *Provas públicas de dados;*
- *Painel de administração (restrito).*

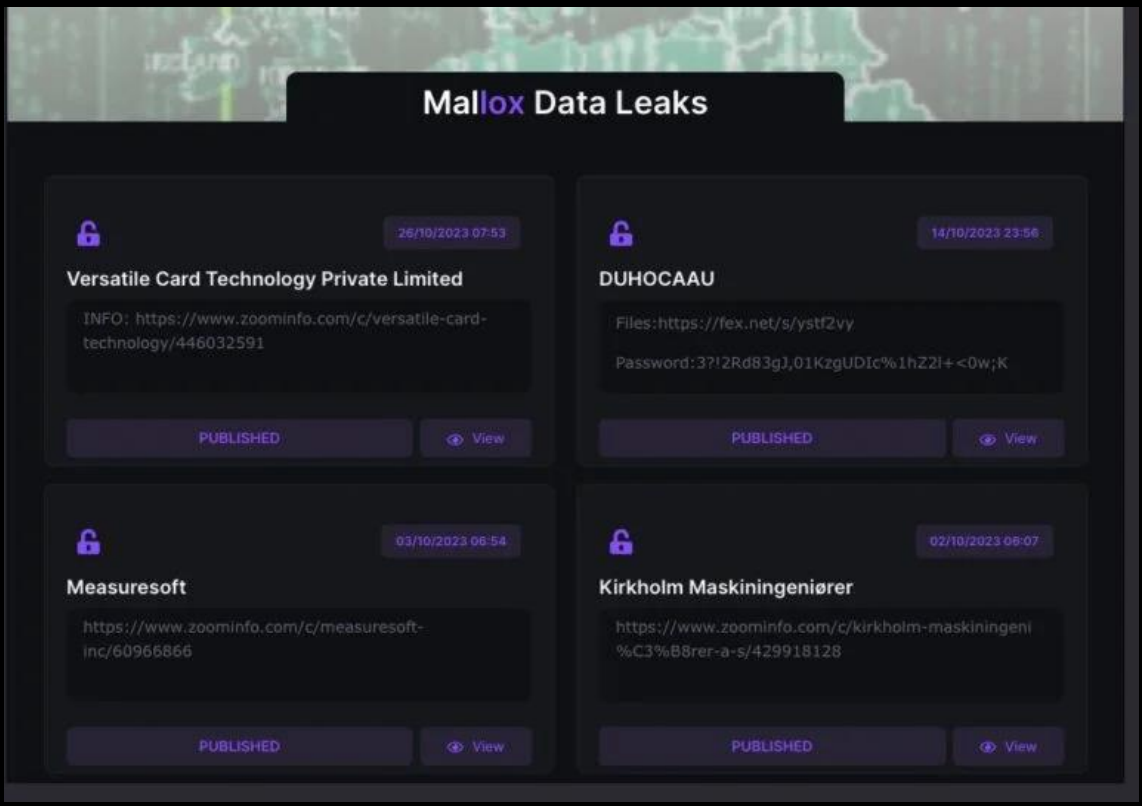


Figura 3 - Site Tor do Ransomware Mallox.

O site do Mallox na dark web apresenta uma interface que lista as vítimas que não pagaram o resgate exigido após a criptografia de seus arquivos. Cada entrada de vítima normalmente inclui:

- *Nome da organização;*
- *País ou região;*

- *Volume estimado de dados roubados;*
- *Contador regressivo para a publicação completa;*
- *Links diretos para os arquivos exfiltrados (quando o prazo se encerra);*
- *Provas dos dados (ex: planilhas, e-mails, documentos financeiros).*

Essa estrutura tem o objetivo de forçar as vítimas a pagar o resgate antes que seus dados sejam totalmente expostos, usando a ameaça de vazamento público como mecanismo de coerção.

Cadeia de Ataque da Ameaça

O ransomware Mallox adota uma cadeia de ataque sofisticada e estruturada em múltiplas fases, combinando diversas técnicas para obter acesso, garantir persistência e, por fim, criptografar os dados das vítimas, permitindo que afiliados conduzam ataques com autonomia e variabilidade nos métodos de infecção. Os afiliados têm liberdade para escolher suas táticas de comprometimento, e campanhas observadas até o momento envolveram desde envio de e-mails com anexos maliciosos (spam) até exploração de vulnerabilidades específicas, como no caso de uma campanha na China, em que foi utilizada uma falha no software IP-Guard para obter acesso inicial.

A análise de telemetria da Kaspersky (KSN) indicou que uma das formas mais comuns de infecção do Mallox envolve a invasão de servidores *MS-SQL* ou *PostgreSQL* expostos à internet. Os atacantes geralmente exploram vulnerabilidades conhecidas de execução remota de código *(RCE)* — como as CVE-2019-1068 e CVE-2020-0618 — em servidores desatualizados, ou lançam ataques de força bruta/dicionário para descobrir credenciais válidas.

Initial Access & Execution – Implantação de Payload

O acesso inicial em campanhas do ransomware **Mallox** ocorre principalmente por meio da **exploração de serviços vulneráveis e expostos publicamente**, com ênfase em **instâncias *MS-SQL* (Microsoft SQL Server)** e conexões ***ODBC* (Open Database Connectivity)** mal configuradas. Os operadores do Mallox exploram vulnerabilidades conhecidas de execução remota de código (RCE), com destaque para falhas antigas não corrigidas como:

- ***CVE-2019-1068*** – Execução remota no Microsoft SQL Server;
- ***CVE-2020-0618*** – Vulnerabilidade no SQL Server Reporting Services.

Além das falhas técnicas, o grupo também utiliza **ataques de força bruta** e **dicionário** para comprometer servidores com credenciais fracas ou configurações inseguras expostas à internet. Em diversos casos recentes, a entrada inicial foi realizada através da **quebra de autenticação em serviços MS-SQL**, seguida do uso de scripts personalizados em PowerShell.

Durante a intrusão, os afiliados do Mallox comumente utilizam **scripts PowerShell codificados em base64** executados com o parâmetro *-EncodedCommand*, contornando restrições com a política de execução (ExecutionPolicy Bypass). Esses scripts são utilizados como **droppers** para carregar a carga maliciosa do ransomware, geralmente armazenada em diretórios como AppData da conta de serviço SQL. Um exemplo observado foi o script "*alta.ps1*".

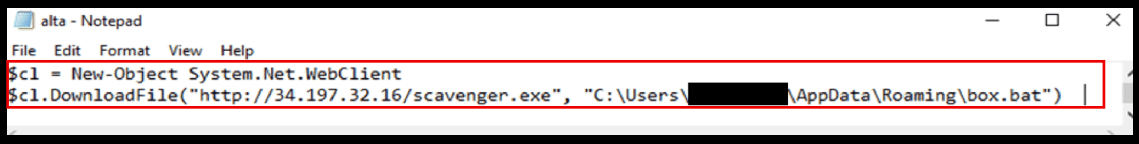


Figura 4 - Script "alta.ps1"

Após o drop da amostra, o ransomware é executado na máquina-alvo utilizando a **Instrumentação de Gerenciamento do Windows (WMI)**, permitindo a criação de novos processos sem levantar alertas imediatos.

A fase de entrega também pode envolver:

- ***T1105* – *Ingress Tool Transfer***: download da carga maliciosa diretamente na memória ou disco, dependendo do nível de controle de rede e endpoint detectado.
- ***T1059.001* – *Command and Scripting Interpreter: PowerShell***: execução de comandos remotos e scripts com codificação em base64, garantindo evasão e flexibilidade na entrega.
- ***T1047* – *Windows Management Instrumentation:*** ativação do payload a partir de processos legítimos do Windows, dificultando a detecção.

Em campanhas complementares, os afiliados do Mallox também foram observados utilizando **phishing via e-mail** como vetor secundário, incorporando ferramentas como **Cobalt Strike** e **Sliver** após o acesso inicial, para reconhecimento interno e movimentação lateral.

DISCOVERY & PERSISTENCE – CRIAÇÃO DE CONTA LOCAL

Figura 5 - Discovery & Persistence

Nesta fase, o Mallox executa atividades de reconhecimento e estabelece persistência no ambiente comprometido. A cadeia de ações se inicia com a execução de um **script batch (.BAT)**, responsável por coletar informações do sistema e da rede, além de **criar uma nova conta de usuário local**. Essa conta é, em seguida, adicionada automaticamente aos grupos **"Administrators"** e **"Remote Desktop Users"**, garantindo privilégios elevados e acesso remoto contínuo ao sistema.

Além disso, foi observada a instalação do software legítimo **AnyDesk**, imediatamente após o comprometimento inicial do servidor web. Essa técnica, semelhante à usada por grupos como o ransomware Akira, permite ao atacante **estabelecer uma backdoor persistente** utilizando ferramentas legítimas, dificultando a detecção por soluções tradicionais de segurança. O uso do AnyDesk oferece uma forma prática de controlar o sistema remotamente, sem a necessidade de deixar traços diretos de malware ativo.

- ***T1082* – *System Information Discovery***
  Execução do comando systeminfo para coletar informações detalhadas sobre o sistema comprometido, como versão do sistema operacional, arquitetura e tempo de atividade.

- ***T1016* – *System Network Configuration Discovery***
  Utilização de comandos como route, ipconfig, nltest, net e arp para obter dados sobre a configuração de rede, rotas, interfaces e domínio.

- ***T1136.001* – *Create Account: Local Account***
  Criação de uma nova conta de usuário local utilizando o comando net user, com credenciais definidas diretamente pelo script malicioso.

- ***T1098* – *Account Manipulation: Administrators Group***
  Adição da conta recém-criada ao grupo de administradores locais por meio do comando net localgroup Administrators.

- ***T1098*** **– Account Manipulation: Remote Desktop Users Group**
  Inclusão da conta no grupo “Remote Desktop Users” usando o comando net localgroup, habilitando o acesso via RDP.

DEFENSE EVASION & LATERAL MOVEMENT – HABILITAÇÃO DE CONEXÕES RDP

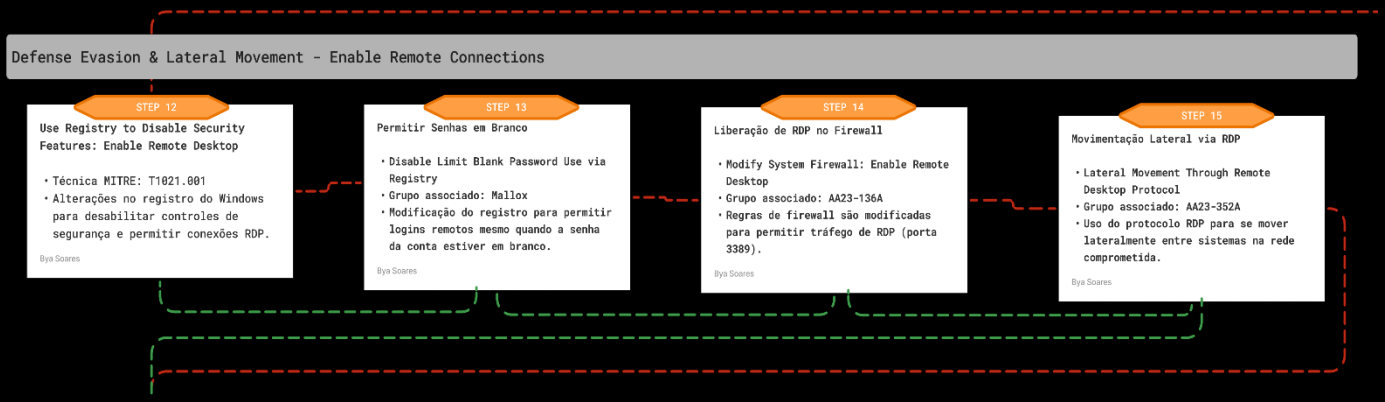


Figura 6 - Defense Evasion & Lateral Movement

Nesta fase, o agente de ameaça do Mallox realiza ajustes no sistema para habilitar conexões via Remote Desktop Protocol (RDP) e, com isso, facilitar a movimentação lateral dentro da rede comprometida. O processo se inicia com a modificação de chaves do Registro do Windows relacionadas ao Terminal Services e à política de senhas em branco. Em seguida, o agente cria uma regra personalizada no firewall utilizando o utilitário *netsh*, permitindo o tráfego na porta 3389/TCP, usada pelo RDP. Com o ambiente preparado, o próximo passo é iniciar a movimentação lateral para outras máquinas na rede via RDP.

Durante a análise, foi identificada a criação de uma conta chamada SystemUI, aparentemente automatizada por um script nomeado *system.bat*. O script, que foi “deixado para trás” pelo atacante, possuía um comentário final curioso: "**REMOVA ESTE ARQUIVO**", evidenciando a intenção de ocultar vestígios da atividade maliciosa, mas indicando falhas operacionais do invasor.

Esta fase pode envolver:

- ***T1562.001*** **– *Impair Defenses: Disable or Modify Tools:***
  Modificação da chave de registro:
  HKLM\SYSTEM\CurrentControlSet\Control\Terminal Services\fDenyTSConnections para 0, habilitando conexões RDP no sistema.
- *T1562* **– *Impair Defenses: Disable or Modify Tools:***
  Desativação da política que impede o uso de senhas em branco, via alteração da chave de registro:

HKLM\SYSTEM\CurrentControlSet\Control\Lsa\LimitBlankPasswordUse para 0.

- *T1562.001* – ***Impair Defenses: Disable or Modify Tools:***
  Criação de uma nova regra no firewall do sistema operacional com netsh, permitindo conexões RDP na porta 3389.
- ***T1021.001*** – ***Remote Services: Remote Desktop Protocol:***
  Tentativa de **movimentação lateral** usando RDP para acessar sistemas vizinhos na rede.

DISCOVERY & EXFILTRATION – RECONHECIMENTO DO SISTEMA LOCAL

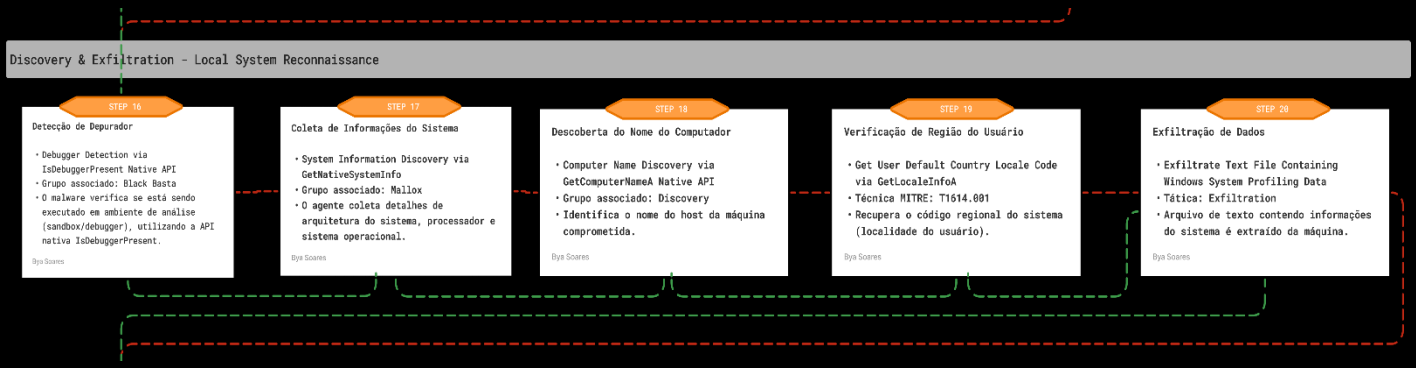


Figura 7 - Discovery & Exfiltration

Nesta fase, o ransomware **Mallox** realiza atividades de **reconhecimento local do sistema** com o objetivo de **coletar informações detalhadas** sobre o ambiente comprometido, como nome da máquina, arquitetura, localização geográfica e indícios de execução em ambientes de análise (sandbox/debugger). Essas ações são realizadas por meio de **chamadas diretas à API do Windows**, o que permite executar os comandos de forma discreta e eficiente.

Após a coleta dos dados, um arquivo de texto contendo os resultados dos comandos de descoberta é criado e, posteriormente, **exfiltrado por meio de uma requisição HTTP POST** para um servidor remoto controlado pelos operadores da ameaça. Esse tráfego não utiliza canais de comando e controle tradicionais, o que dificulta a detecção por soluções de segurança.

Além disso, foi observado o uso da ferramenta **Mimikatz** para a extração de credenciais no servidor inicialmente comprometido. Com essas credenciais, o agente de ameaça conseguiu **acesso privilegiado ao domínio**, elevando significativamente o impacto do ataque. O uso do *netscan.exe* — uma ferramenta legítima de varredura de rede da SoftPerfect — foi outro elemento importante, utilizado para mapear o ambiente. A versão 6.2.1.0 foi empregada com o nome modificado para ***netscanold.exe***, visando dificultar sua identificação.

Esta fase pode envolver:

- ***T1497* – *Virtualization/Sandbox Evasion:***
  Uso da função IsDebuggerPresent da API do Windows para verificar se o processo atual está sendo executado em um ambiente de análise ou depuração, como sandboxes.
- ***T1082* – *System Information Discovery:***
  Chamada da função GetNativeSystemInfo para coletar dados sobre o sistema operacional, arquitetura e hardware da máquina.
- ***T1614* – *System Location Discovery:***
  Execução da função GetLocaleInfoA para identificar o código de localização regional configurado no sistema da vítima, permitindo ao malware evitar alvos específicos, como países da CEI (Comunidade dos Estados Independentes).
- ***T1048.003* – *Exfiltration Over Alternative Protocol: Unencrypted Non-C2 Protocol:***
  Exfiltração de um arquivo de texto contendo as informações coletadas, utilizando uma requisição HTTP POST para um servidor remoto. O uso de um protocolo não criptografado e fora dos canais C2 tradicionais visa dificultar a detecção do tráfego malicioso.

IMPACTO – CRIPTOGRAFIA DO MALLOX RANSOMWARE

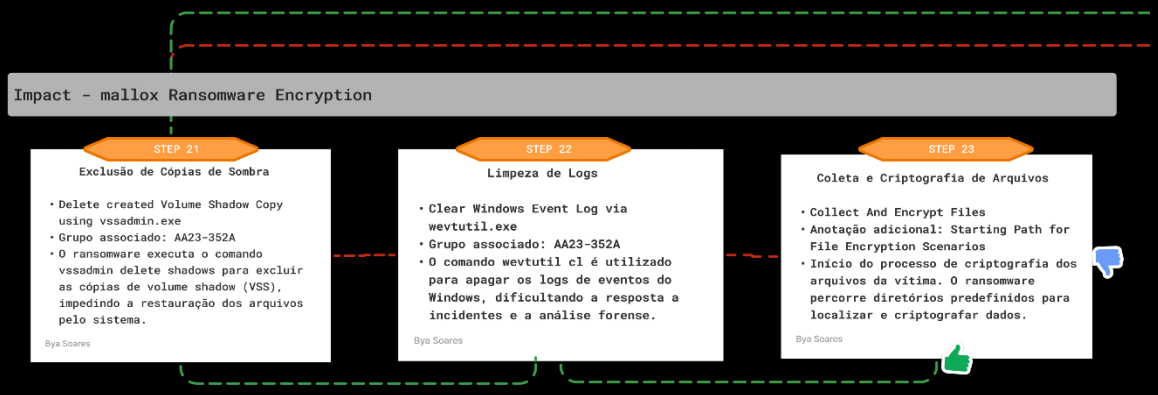


Figura 8 - Impacto – Criptografia do Mallox Ransomware

A fase de impacto do ransomware **Mallox** é marcada por uma sequência de ações que visam **maximizar os danos** e dificultar a recuperação dos dados pela vítima. O processo é cuidadosamente elaborado para eliminar rastros, impedir restauração do sistema e iniciar a **criptografia massiva de arquivos**.
Inicialmente, o ransomware **remove as Cópias de Sombra de Volume (VSS)** usando o utilitário legítimo *vssadmin.exe*, anulando tentativas de recuperação via pontos de restauração do sistema. Em seguida, são apagados os **logs de eventos**

do Windows com o comando *wevtutil.exe*, ocultando as atividades realizadas durante o ataque. Por fim, os arquivos da vítima são **identificados e criptografados localmente** com base em uma lista de extensões predefinidas, usando algoritmos semelhantes aos de outras famílias de ransomware.

Durante a análise do incidente, foi observado o uso do software **FileZilla**, uma ferramenta legítima de FTP/SFTP, para **exfiltrar dados antes da criptografia**, fortalecendo o modelo de **dupla extorsão**.

A investigação de duas amostras nomeadas *ozon.exe* e *net_[CUSTOMER_ID].exe* revelou comportamento padronizado no pré-criptografia, com as seguintes etapas:

- Desativação de recursos de recuperação do sistema com *bcdedit*.
- Verificação da **localização e idioma** do sistema. Caso seja identificado como **Rússia ou região próxima**, o processo é interrompido.
- Alteração do **plano de energia do Windows** para "Desempenho Máximo", otimizando os recursos para a tarefa de criptografia.
- Realização de uma requisição DNS para verificar conectividade com a internet.
- Envio de uma **requisição HTTP POST** para o servidor C2, contendo dados sobre o sistema e o **ID da vítima**, que também aparece no nome do executável e na nota de resgate.

Esta fase pode envolver:

- ***T1490*** - ***Inhibit System Recovery:*** Este cenário executa o vssadmin.exeutilitário para excluir uma cópia de sombra de volume recente criada pelo modelo de avaliação.
- ***T1070.001*** - ***Indicator Removal: Clear Windows Event Logs:*** O cenário usará o wevtutil.exebinário para limpar logs de eventos do sistema.
- ***T1486*** - ***Data Encrypted for Impact***: Este cenário executa as rotinas de criptografia de arquivos usadas por famílias comuns de ransomware. Arquivos que correspondem a uma lista de extensões são identificados e criptografados no local usando algoritmos de criptografia semelhantes.

TABELA MITRE ATT&CK

Este tópico apresenta as *TTPs* identificadas nesta ameaça, conforme o framework MITRE ATT&CK, oferecendo uma visão tática detalhada sobre o comportamento do adversário. O objetivo é permitir o mapeamento das técnicas utilizadas pelos atacantes, facilitando a implementação de contramedidas eficazes e o aprimoramento das defesas de segurança.

Tática	Técnica	Detalhes
Initial Access	T1078 – Valid Accounts	Uso de credenciais obtidas via força bruta ou phishing para acesso a servidores MS-SQL expostos.
	T1566 – Phishing	E-mails maliciosos com anexos ou links levando a scripts PowerShell ou executáveis para obter acesso inicial.
Execution	T1059.001 – PowerShell	Execução de payloads por scripts PowerShell com **-EncodedCommand** e **-ExecutionPolicy** Bypass.
Persistence	T1136.001 – Create Account: Local Account	Criação de contas locais para persistência, adicionadas a grupos como "Administrators" e "Remote Desktop Users".
Privilege Escalation	T1547.001 – Registry Run Keys / Startup Folder	Inserção de entradas no registro para garantir execução persistente após reinicialização.
Defense Evasion	T1070.001 – Clear Windows Event Logs	Uso do wevtutil.exe para apagar logs e dificultar investigações forenses.
	T1562.001 – Impair Defenses: Modify Tools	Modificação de chaves de registro (**fDenyTSConnections**, **LimitBlankPasswordUse**) e regras de firewall para liberar RDP.
	T1027 – Obfuscated Files or Information	Scripts e binários ofuscados para evitar detecção por antivírus.
Credential Access	T1003.001 – LSASS Memory	Uso do Mimikatz para extração de credenciais da memória do sistema (incluindo acesso a domínio).
Discovery	T1082 – System Information Discovery	Uso da API **GetNativeSystemInfo** e comandos como **systeminfo**.
	T1016 – System Network Configuration Discovery	Comandos **ipconfig**, **net**, **nltest**, **route** e ferramentas como **netscan** para mapear o ambiente de rede.
	T1614 – System Location Discovery	API **GetLocaleInfoA** para identificar região e evitar alvos em países da CEI.
	T1497 – Virtualization/Sandbox Evasion T1497 – Virtualization/Sandbox Evasion	API **IsDebuggerPresent** para detectar ambientes de análise (sandbox/debugger).

Tática	Técnica	Detalhes
Lateral Movement	T1021.001 – Remote Desktop Protocol	Acesso lateral via RDP após habilitação do serviço, criação de conta local e liberação de firewall.
Command & Control	T1041 – Exfiltration Over C2 Channel	Envio de dados via requisições HTTP POST contendo informações do sistema e ID da vítima para servidor controlado pelos operadores.
Exfiltration	T1048.003 – Exfiltration Over Unencrypted Non-C2 Protocol	Exfiltração de arquivos de texto com dados do sistema coletados durante a fase de reconhecimento, usando HTTP sem criptografia.
Impact	T1486 – Data Encrypted for Impact	Criptografia de arquivos com base em extensões predefinidas, usando algoritmos robustos como ChaCha20.
	T1490 – Inhibit System Recovery	Exclusão de Cópias de Sombra de Volume via vssadmin.exe.

Tabela 1 - MITRE ATT&CK TTPs

VULNERABILIDADES EXPLORADAS PELA AMEAÇA

No momento da elaboração deste relatório, foi identificado que os operadores e afiliados do ransomware **Mallox** vêm explorando ativamente vulnerabilidades conhecidas em **servidores Microsoft SQL** e outros softwares amplamente utilizados em ambientes corporativos. Essas explorações são empregadas para obter **acesso inicial aos sistemas** e, em muitos casos, implantar scripts e ferramentas que facilitam o **movimento lateral, exfiltração de dados e execução da carga maliciosa de criptografia**.

A escolha por **falhas públicas e frequentemente negligenciadas** revela um padrão de atuação oportunista, porém estratégico, voltado para sistemas desatualizados ou mal configurados. Isso reforça a importância de manter uma postura proativa de segurança, incluindo **aplicação contínua de patches**, **monitoramento de serviços expostos** e **redução da superfície de ataque**.

Vulnerability	Product	Type
CVE-2019-1068	Microsoft SQL Server	Execução Remota de Código (RCE)
CVE-2020-0618	Microsoft SQL Server Reporting Services	Execução Remota de Código (RCE)
CVE-2021-31206	Microsoft Exchange Server	Arbitrary File Write
CVE-2021-34473	Microsoft Exchange Server	Pre-auth Path Confusion leading to RCE
CVE-2021-34523	Microsoft Exchange Server	Privilege Escalation
CVE-2022-41040	Microsoft Exchange Server (ProxyNotShell)	Server-Side Request Forgery (SSRF)
CVE-2022-41082	Microsoft Exchange Server (ProxyNotShell)	RCE via PowerShell

Tabela 2 - Vulnerabilidades exploradas pelos operadores do ransomware em seus ataques.

RECOMENDAÇÕES

Além da atenção aos **Indicadores de Comprometimento (IoCs)** descritos neste relatório, é essencial adotar medidas proativas para **mitigar o risco de infecção** pelo ransomware **Mallox** e suas variantes. As seguintes recomendações visam fortalecer a postura defensiva das organizações contra campanhas ativas de ransomware que exploram vulnerabilidades em servidores, credenciais fracas e configurações indevidas:

6.1 MANTENHA SISTEMAS E SOFTWARES ATUALIZADOS

- Aplique patches de segurança regularmente, especialmente em servidores Microsoft SQL, Exchange Server, e softwares de terceiros amplamente explorados.
- Corrija vulnerabilidades como CVE-2019-1068 e CVE-2020-0618, comumente exploradas pelo Mallox.

6.2 Implemente soluções de segurança confiáveis

- Utilize **EDR, antivírus corporativo e firewall de próxima geração** com capacidades de detecção de comportamento anômalo.
- Bloqueie a execução de scripts maliciosos via **GPO** e restrinja o uso de ferramentas como PowerShell e WMI.

6.3 Realize backups regulares

- Mantenha **backups criptografados e offline**, testados periodicamente, com versões históricas armazenadas em ambientes isolados.
- Verifique se os backups não estão acessíveis diretamente a partir de contas administrativas comuns.

6.4 Monitore e analise atividades da rede

- Implemente soluções de **SIEM, NDR e análise de logs** com regras específicas para detectar movimentação lateral, exfiltração e execução via PowerShell.
- Monitore atividades incomuns, como uso de vssadmin, wevtutil, ou alterações no registro (regedit).

INDICADORES DE COMPROMETIMENTO

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 do artefato	
md5:	ad938c8aa558ff9a2332ac6a3e24705a
sha1:	4ff0e55a42bfe34e27f33cbdc4cdf3fbccd793ba
sha256:	e292806b534bcc2fd2d965b17dafc502b1aed3eb2882edb3c60dd20d2fd5da7a
File name:	Win32 EXE, 2025-05-07_ad938c8aa558ff9a2332ac6a3e24705a_black-basta_cobalt-strike

Indicadores do artefato	
md5:	ce9742ce6f771663ff82c57b72ef90e4
sha1:	84b056504600477936cc19e9fe7004bce2778b9b
sha256:	2803c8b487421075c4751ae6f4f137033c7c1da6706afac1fad68eb9c4ad8293
File name:	sync.exe

Indicadores do artefato	
md5:	ba59e1d90d8ff1763e9afbb627553d81
sha1:	f363fbb01db5efe8f8dad5bc1bf74a9e403a8e93
sha256:	5eee1d167dfc901714cf007a5d2cba6c05e9078b39914adcab0e7ee3fc52535c
File name:	2025-04-24_ba59e1d90d8ff1763e9afbb627553d81_black-basta_cobalt-strike

Indicadores do artefato	
md5:	3a5be9663e8f105cf77cad03bb0671da
sha1:	d626e264dc2fe8be3c75e36d892e39e46dceb6f0
sha256:	32be900bcf0bfdb213ee96e953cd4fe159f15f55b9b107b07d6fcf57a1c24f7c
File name:	OneDrive.exe

Indicadores do artefato	
md5:	b859fc33281054900595598330ba86f3
sha1:	d3af272fb4a3da27a4a2a155182046c6661e0743
sha256:	02fb490eb62c2dc8061d7bc81f47207f137e4b77a2b1228443bc405581e06563
File name:	FPGGuJqN.exe

Indicadores do artefato	
md5:	91798710166ed4e63d8ed8432aa9b905
sha1:	a3f7221caa73ab4c39c6c447adf957dbc9fa61fd
sha256:	0d249861eecafc7fbb246de87325da7f122f09dda29b809e1310160406ed6c3f
File name:	AV-Mark_241101_R1_45.exe

Indicadores do artefato	
md5:	e9b0bc2afd0451c70e4ce10705383672
sha1:	5030266646293c5eea3673b6821d51fe00fd9599
sha256:	e068e915e998b1def7d54684c4259236f021aa2a2335afec438a45839e18efc0
File name:	cry.exe

Indicadores do artefato	
md5:	a74ee50d2f91f77f010ecb154aa6b30b
sha1:	90138ac54f4002803b7a88137da5ed2c5e46460c
sha256:	40b75aa3c781f89d55ebff1784ff7419083210e01379bea4f5ef7e05a8609c38
File name:	1windows.exe

Tabela 3 - Indicadores de Comprometimento

Indicadores de URL, IPs e Domínios

Abaixo, podemos observar o *Dedicated Leak Site* ativo do **Cl0p**, aonde os dados exfiltrados de suas vítimas, serão publicados, caso eles não paguem o resgate solicitado pelos afiliados.

Dedicated Leak Site	
TOR Link:	mallox7mk3xvjqh7vbj5j7ixn5dsqax7vpz7h5cfwzfyus3znmn7haqd[.]onion
Tipo:	Data Leak Site
Descrição:	Site de vazamento de dados utilizados pelo grupo Mallox para extorsão pública das vítimas.

Tabela 4 - Dedicated Leak Site ativo do Mallox.

REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **CTI Purple Team *by* ISH Tecnologia**
- **MITRE ATT&CK**

AUTORES

- **Bryenne Soares – Threat Researcher**

heimdall
security research

A DIVISION OF ISH