TLP: CLEAR

RELATÓRIO DE PESQUISAS

INC Ransomware:

Perfil, Comportamento e Mitigações

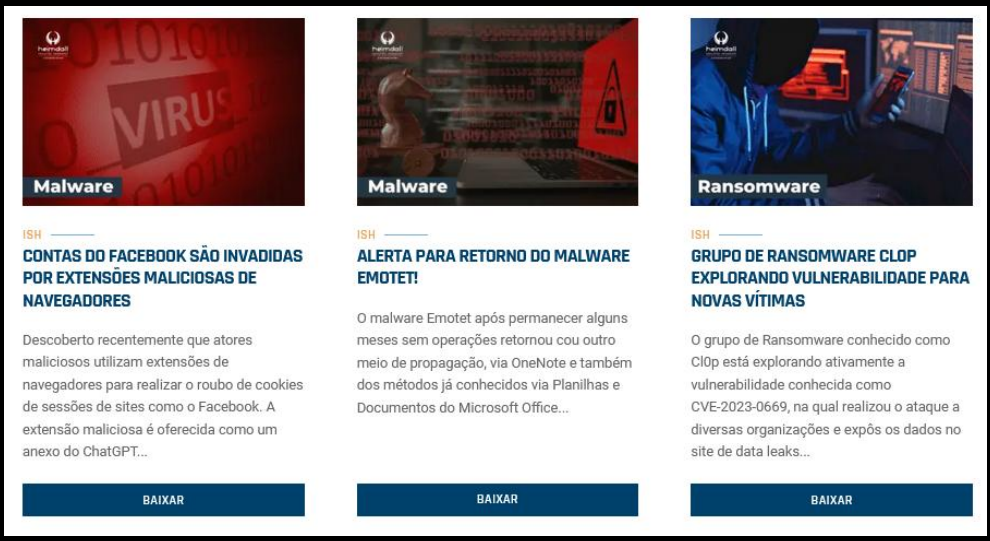
heimdall
security research

Acesse a nossa nova comunidade através do WhatsApp!

Heimdall Security Research

Acesse boletins diários sobre agentes de ameaças, *malwares*, indicadores de comprometimentos, TTPs e outras informações no *site* da ISH.

Boletins de Segurança – Heimdall



SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

1 INTRODUÇÃO EXECUTIVA

Este relatório de segurança, desenvolvido pela equipe de inteligência **Heimdall da ISH Tecnologia**, 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.

2 ESTRATÉGICO

2.1 INTRODUÇÃO SOBRE A AMEAÇA

O cenário global de ransomware segue altamente ativo em 2025, com diversos grupos conduzindo ataques direcionados a organizações de diferentes setores e portes. Nesse contexto, o **INC Ransomware** destaca-se como uma das principais ameaças emergentes, reconhecida por suas operações estruturadas, extorsão dupla e alta capacidade de adaptação. Desde sua aparição em 2023, o grupo tem conduzido campanhas seletivas, priorizando alvos com alto potencial financeiro e dados sensíveis. O modus operandi inclui **exfiltração de informações antes da criptografia**, uso de **ferramentas legítimas de administração remota** e exploração de **vulnerabilidades conhecidas**, visando maximizar impacto e coerção.

O **INC Ransomware** representa, portanto, uma ameaça consolidada e em evolução, exigindo **monitoramento contínuo**, **resposta integrada** e **cooperação entre as áreas estratégica, tática e operacional** para mitigação efetiva.

2.2 VITIMOLOGIA E SEGMENTOS AFETADOS

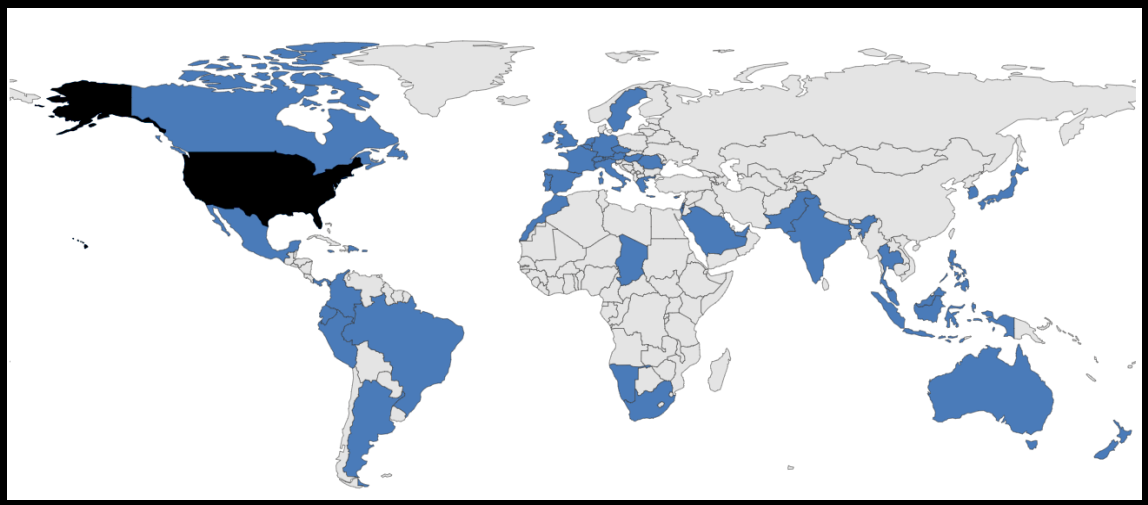


Figura 1 – Países vítimas do INC ransom.

A análise dos incidentes associados ao **INC Ransomware** demonstra um padrão de atuação **global e diversificado**, com registros de ataques distribuídos pela América do Norte, Europa, Ásia e Oceania. Observa-se **maior concentração de vítimas nos Estados Unidos**, seguidos por países da **Europa Ocidental** (Reino Unido, França, Alemanha, Espanha) e regiões estratégicas da **América Latina**, incluindo **Brasil**, **Chile e México**. Também foram identificadas ocorrências na **Austrália**, **África do Sul** e em países do **Sudeste Asiático**, o que reforça o alcance internacional e a flexibilidade operacional do grupo.

Em relação à **vitimologia setorial**, o INC tem direcionado suas campanhas principalmente para organizações pertencentes aos seguintes segmentos:

- **Saúde:** instituições hospitalares e laboratórios clínicos, explorando a criticidade dos serviços e o alto impacto de interrupções.
- **Tecnologia:** empresas de software e provedores de serviços digitais, visando acesso a dados sensíveis e infraestrutura de clientes.
- **Business Services:** consultorias, contabilidade e advocacia, alvos comuns pela alta densidade de informações confidenciais.
- **Educação:** universidades e escolas, aproveitando fragilidades em ambientes híbridos de TI.
- **Manufatura:** indústrias com processos automatizados e baixa tolerância a paradas operacionais.

A distribuição geográfica e a variedade setorial indicam que o INC Ransomware adota uma estratégia oportunista e financeiramente orientada, explorando vulnerabilidades de exposição pública e priorizando vítimas com maior probabilidade de pagamento. O perfil de ataque evidencia **maturidade operacional**, com campanhas adaptáveis e capacidade de atingir múltiplas regiões simultaneamente.

3 TÁTICO

3.1 ANÁLISE DA KILL CHAIN DA AMEAÇA

Reconhecimento

- É realizado o mapeamento de contas, shares e topologia de rede da vítima para identificar caminhos de privilégio e alvos críticos. Esse estágio normalmente precede tentativas de brute-force, phishing ou exploração de aplicações públicas. O grupo realiza tanto **reconhecimento passivo** (coleta de informações públicas e OSINT sobre infraestrutura, e-mails e credenciais vazadas) quanto **reconhecimento ativo** (varreduras de porta, enumeração de shares e serviços expostos, sondagens de Active Directory e testes de autenticação). Além disso, os atacantes costumam executar ações de profiling, identificando contas com privilégios, serviços de backup, pontos de acesso remoto (RDP/VPN) e janelas operacionais (horários de uso), para planejar rotas de invasão, priorizar vetores iniciais e definir o momento de execução que maximize impacto e minimize detecção.

Acesso inicial

- O grupo realiza o acesso inicial por meio de múltiplos vetores coordenados: exploração de aplicações públicas e appliances expostos, por exemplo VPNs, gateways e servidores web com patches pendentes; campanhas de spear-phishing e engenharia social para roubo de credenciais ou execução de payloads; e uso de contas válidas comprometidas, compradas ou reutilizadas para autenticação remota (incl. RDP). Frequentemente combinam a implantação de web shells ou loaders em hosts explorados com logins legítimos para reduzir ruído e evitar detecção, além de tentativas de contornar controles de MFA por meio de técnicas de engenharia social. Em particular, foram observadas explorações de vulnerabilidades públicas conhecidas, por exemplo **CVE-2023-3519** em **appliances Citrix NetScaler/ADC,** usadas como vetor de entrada em campanhas do grupo.

Execução e persistência

- O grupo realiza a execução primária por meio de intérpretes nativos (por exemplo *cmd.exe* e *PowerShell*), usando-os para orquestrar a implantação de payloads e comandos administrativos. Em seguida, costuma criar serviços Windows com nomes aparentemente legítimos (por exemplo ***winupd***, "***Windows Update Service***") para executar binários com privilégios SYSTEM e persistir no ambiente. Paralelamente, os operadores implantam ferramentas de acesso remoto legítimas (AnyDesk, RMMs) e backdoors próprios, estabelecendo canais redundantes, serviços, tarefas agendadas, chaves de registro de inicialização e agentes remotos, para

garantir resiliência operacional. Esse conjunto de técnicas (execução via intérpretes, mascaramento de serviços e uso de ferramentas legítimas) reduz a superfície de detecção, facilita movimentação lateral e prepara o ambiente para a fase de coleta/exfiltração e eventual execução do encryptor.

Descoberta & escalada

- É realizado a enumeração de hosts, shares e contas de domínio; dump de credenciais e escalada usando contas encontradas para obter controle amplo do ambiente. Ferramentas como *AdFind/esentutl* e técnicas de credential dumping foram observadas em campanhas relacionadas.

Movimento lateral

- O grupo realiza movimento lateral rápido e coordenado para ampliar o domínio sobre a rede antes da fase de impacto. Métodos típicos incluem execução remota via **PsExec** (frequentemente renomeado), cópias massivas para shares SMB/admin$, execução por WMI/WMIC, criação remota de serviços e agendamento de tarefas, e uso de RDP/administrative tools para sessões interativas. Para facilitar a propagação, operadores reutilizam credenciais obtidas, exploram permissões de conta e aproveitam ferramentas "*living-off-the-land*" para reduzir ruído.

    - **Sinais de detecção:** picos de conexões SMB/execuções remotas em sequência, criação de serviços/ tarefas com nomes atípicos, uso súbito de PsExec/WMI por contas não usuais.

Exfiltração

- A exfiltração é feita por canais que dificultem a detecção e o bloqueio: sincronizadores de nuvem (*MegaSync, Rclone*), uploads cifrados para armazenamento em nuvem controlado pelos atacantes, túneis SSH/VPN ou uso de contas SaaS comprometidas. Os operadores costumam fracionar transferências, usar contas de terceiros e mascarar tráfego em HTTPS para contornar inspeção. Em alguns casos, dados sensíveis são colocados em repositórios acessíveis publicamente ou anunciados em portais de vazamento como mecanismo de pressão.

    - **Sinais de detecção:** tráfego de saída anômalo para serviços de sincronização/cloud, grandes uploads fora de janela operacional, uso de credenciais de terceiros em fluxos de egress.

Impacto - Criptografia e extorsão

- A fase final combina criptação em larga escala com extorsão: cifra de servidores e estações críticas, remoção de snapshots e backups (p.ex. comandos que limpam cópias de sombra), e publicação/ameaça de

vazamento dos dados exfiltrados (double extortion). Operadores instalam o encryptor em múltiplos pontos quase simultaneamente para maximizar interrupção e costumam deixar notas de resgate com instruções comerciais/contato. Em incidentes onde o risco reputacional é suficiente, o ator pode optar por extorsão pura (ameaça de publicar sem cifrar).

- **Sinais de detecção:** operações massivas de gravação/ciframento de arquivos, exclusão de shadow copies (vssadmin /wbadmin), criação de notas de resgate, acesso massivo a ferramentas administrativas próximo ao evento de impacto.

~~~~ INC Ransom ~~~~

-----> Your data is stolen and encrypted.
If you don't pay the ransom, the data will be published on our TOR darknet sites.
The sooner you pay the ransom, the sooner your company will be safe.

Tor Browser Link:
http://[redacted]onion/
http://[redacted].onion/

Link for normal browser:
[redacted]

-----> What guarantees are that we won't fool you?
We are not a politically motivated group and we want nothing more than money.
If you pay, we will provide you with decryption software and destroy the stolen data.
After you pay the ransom, you will quickly restore your systems and make even more money.
Treat this situation simply as a paid training for your system administrators, because it is due to your corporate network not being properly configured that we were able to attack you.
Our pentest services should be paid just like you pay the salaries of your system administrators. Get over it and pay for it.
If we don't give you a decryptor or delete your data after you pay, no one will pay us in the future.
You can get more information about us on Twitter https://twitter.com/hashtag/incransom?f=live

-----> You need to contact us on TOR darknet sites with your personal ID
Download and install Tor Browser https://www.torproject.org/
Write to the chat room and wait for an answer, we'll guarantee a response from you.
Sometimes you will have to wait some time for our reply, this is because we have a lot of work and we attack tens of companies around the world.

Tor Browser Link for chat:
http://[redacted]onion/

Your personal ID:
[snip]

-----> Warning! Don't delete or modify encrypted files, it will lead to problems with decryption of files!
-----> Don't go to the police or the FBI for help. They won't help you.
The police will try to prohibit you from paying the ransom in any way.
The first thing they will tell you is that there's no guarantee to decrypt your files and remove stolen files.
This is not true, we can do a test decryption before paying and your data will be guaranteed to be removed because it's a matter of our reputation.
Paying the ransom to us is much cheaper and more profitable than paying fines and legal fees.
The police and the FBI don't care what losses you suffer as a result of our attack, and we'll help you get rid of all your problems for a modest sum of money.
If you're worried that someone will trace your bank transfers, you can easily buy cryptocurrency for cash, thus leaving no digital trail that someone from your company paid our ransom.
The police and FBI won't be able to stop lawsuits from your customers for leaking personal and private information.
The police and FBI won't protect you from repeated attacks.

-----> Don't go to recovery companies!
They are essentially just middlemen who will make money off you and cheat you.
We are well aware of cases where recovery companies tell you that the ransom price is $5M dollars, but in fact they secretly negotiate with us for $1M.
If you approached us directly without intermediaries you would pay several times less.

-----> For those who have cyber insurance against ransomware attacks.
Insurance companies require you to keep your insurance information secret.
In most cases, we find this information and download it.

-----> If you do not pay the ransom, we will attack your company again in the future.

Figura 2 – Nota de resgate do INC ransomware.
~~~~

4 CONCLUSÃO

O **INC Ransomware** configura uma ameaça consolidada e de alto impacto, combinando exfiltração prévia de dados com criptografia direcionada para aumentar a pressão sobre as vítimas. Sua capacidade de explorar superfícies públicas, abusar de credenciais válidas e empregar ferramentas legítimas reduz a visibilidade das ações e acelera a penetração em ambientes críticos. Os efeitos esperados vão além da indisponibilidade temporária, incluem divulgação de dados sensíveis, perda de propriedade intelectual, custos forenses e operacionais significativos e potencial exposição a sanções e litígios. Setores com baixa tolerância a interrupções (saúde, manufatura, educação e serviços críticos) estão particularmente em risco. Em suma, o perfil operacional do grupo aponta para uma ameaça de alta probabilidade e grande severidade, com impactos financeiros, reputacionais e regulatórios potencialmente duradouros.

5 TABELA MITRE ATT&CK

Este tópico apresenta as Táticas, Técnicas e Procedimentos (TTPs) identificados 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	(T1566) Phishing	O grupo obtém acesso inicial via campanhas de spear-phishing/engenharia social visando roubo de credenciais ou execução de payloads (documentos, links maliciosos).
Discovery	(T1082) System Information Discovery (T1057) Process Discovery (T1083) File and Directory Discovery (T1135) Network Share Discovery (T1652) Device Driver Discovery (T1120) Peripheral Device Discovery	O grupo realiza uma enumeração abrangente do ambiente para identificar e priorizar alvos de exfiltração/criptação: mapeia informações do sistema e volumes (incluindo partições ou volumes ocultos), varre processos em execução usando o Restart Manager para identificar e encerrar processos que mantenham arquivos abertos e faz buscas dirigidas por pastas e arquivos de alto valor (aceitando parâmetros de linha de comando para focar DBs, backups e documentos). Paralelamente, enumera shares e recursos de rede mapeados para localizar repositórios críticos, verifica drivers instalados que possam ser aproveitados e identifica dispositivos periféricos (USBs, discos externos, impressoras) que possam conter, propagar ou receber dados, tudo com o objetivo de maximizar impacto e bloquear rotas de recuperação.
Execution	(T1047) Windows Management Instrumentation (T1106) Native API	Uso de WMI/WMIC para execução remota de comandos e orquestração de ações em hosts remotos durante a propagação. Chamadas a APIs nativas (ex.: DeviceIoControl, Device/Kernel APIs) para operações de baixo nível, p.ex. manipular snapshots ou evitar ferramentas de alto nível detectáveis.
Lateral Movement	(T1570) Lateral Tool Transfer	Transferência e distribuição do binário/encryptor entre endpoints (push do executável para múltiplos hosts).
Impact	(T1490) Inhibit System Recovery (T1486) Data Encrypted for	O grupo costuma neutralizar mecanismos de recuperação, por exemplo excluindo Volume Shadow Copies, antes ou durante o ataque para

	(T1491.001) ImpactInternal Defacement	dificultar restaurações. Em seguida realiza criptografia massiva de arquivos e volumes, frequentemente multithreaded e seletiva por extensão e tamanho, com o objetivo de tornar dados críticos indisponíveis. Além disso, pode promover desfiguração interna ao alterar o wallpaper ou o background para exibir notas de resgate e aumentar a pressão sobre os operadores. Essas ações combinadas dificultam a recuperação direta e amplificam a coerção por pagamento.

Tabela 1 – Tabela MITRE ATT&CK.

6 RECOMENDAÇÕES

Além dos indicadores de comprometimento elencados abaixo pela ISH, poderão ser adotadas medidas visando a mitigação da infecção da referida *ameaça*, como por exemplo:

Prevenção de acesso inicial

- Autenticação multifator (MFA) para todos os acessos, inclusive sistemas administrativos.
- Senhas fortes, únicas e bem gerenciadas (evitar reutilização entre sistemas)
- Educação e treinamento de usuários para identificar phishing, links suspeitos, anexos maliciosos etc.
- Filtragem de e-mail/ sandboxing de anexos, análise de links, bloqueio de macros não confiáveis.

Fortalecimento de sistemas e rede

- Manter sistemas operacionais, firmware e softwares atualizados com os patches mais recentes.
- Desativar ou remover serviços ou funcionalidades que não são usados ou que representam risco.
- Segmentação de rede (dividir a rede em zonas menores) para prevenir movimento lateral.
- Monitoramento de rede (IDS/IPS), análise de tráfego e uso de logging centralizado com alertas para comportamento suspeito.
- Endpoints protegidos por soluções de antivírus/anti-ransomware modernas (com análise comportamental, heurística etc.).
- Limitar privilégios: aplicar o princípio de menor privilégio (usuários e serviços só têm os acessos estritamente necessários).

Cópias de segurança (backups)

- Fazer backup frequente dos dados críticos.
- Armazenar backups de maneira isolada (offline, air-gapped ou em rede separada) para que não possam ser criptografados junto com o ambiente principal.
- Utilizar backups “imutáveis” ou de escrita única (onde o backup não pode ser alterado ou apagado) quando possível.
- Testar regularmente os backups: verificar se podem ser restaurados com sucesso.
- Criptografar os backups (para proteger contra acesso indevido).

Planejamento de resposta a incidentes

- Ter um plano formal de resposta a ransomware/ plano de incidentes, com responsabilidades, “playbooks” (roteiros de ação) definidos.

- Simular e treinar exercícios de resposta a incidentes (testes de invasão, simulações de ransomware)
- Em caso de ataque: isolar imediatamente sistemas infectados (desconectar da rede) para limitar propagação.
- Monitorar e identificar indicadores de compromisso (IOCs), endereços C2, hashes, domínios usados pelos atacantes.

Outras boas práticas:

- Usar criptografia em repouso para dados sensíveis, sempre que possível.
- Minimizar a "superfície de ataque" desligando funções desnecessárias ou portas de rede expostas.
- Utilizar inteligência de ameaça (Threat Intelligence) para manter-se informado sobre novas variantes, vulnerabilidades ou IOCs relacionados ao INC ou grupos similares.
- Fazer auditorias e avaliações regulares de segurança (pentests, varreduras de vulnerabilidades).
- Monitorar logs de segurança com soluções de SIEM, correlacionando eventos e alertas para detectar anomalias cedo.

7 OPERACIONAL

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.

7.1 INDICADORES DE COMPROMETIMENTO (IOC)

Indicadores do artefato	
md5:	1fb412212359a970be06b9a4578c1e68
sha1:	efa771d6f699c7240c80260d50925ed8baae3cdc
sha256:	fcefe50ed02c8d315272a94f860451bfd3d86fa6ffac215e69dfa26a7a5deced
File name:	Inc_Ransomware

Indicadores do artefato	
md5:	8fe9e6561f467bec7bcafccfb05cef8f
sha1:	009758e1a892f274467602d5db9ea2ae432a579d
sha256:	e2370ef066df692317a5f9d739120e467144cfdcd9a4dd7dd562ebdbf5f0778c
File name:	INC-README.txt

Indicadores do artefato	
md5:	1922a47e467e4185eea0bb003e813dde
sha1:	cd0228e52de03fc2423e22df9840ba5dc707c4b4
sha256:	1754c9973bac8260412e5ec34bf5156f5bb157aa797f95ff4fc905439b74357a
File name:	ais.exe.vir

Indicadores do artefato	
md5:	79803779790dae11cbbef6500dc53391
sha1:	3a3a20e1207a6e4518c9e363a98bce36bd94f7b8
sha256:	f96ecd567d9a05a6adb33f07880eebf1d6a8709512302e363377065ca8f98f56
File name:	ben.exe

Indicadores do artefato	
md5:	092d39b97288886203fa681bb354cca3
sha1:	baa44b68d92836d9005c6829d6d4891d39e1471d
sha256:	11cfd8e84704194ff9c56780858e9bbb9e82ff1b958149d74c43969d06ea10bd
File name:	INC.exe

Indicadores do artefato	
md5:	c64f05781d89a721acf93b31d5301d58
sha1:	6cf651be718abc9be4d8295adb9c425de27a743a
sha256:	3c4e8f6a5dc94966483069b68981b0ad77ff9c547e8ec3d74ed207e3f037ece6
File name:	02bf1514-d3e5-40d1-8267-150337649901

Tabela 2 – Indicadores de Comprometimento.

8 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **CTI Purple Team *by* ISH Tecnologia**
- **MITRE ATT&CK**
- **Ransomware.live**
- **Trendmicro**

9 AUTORES

- **Ismael Rocha – Threat Intelligence Specialist**

heimdall
security research
A DIVISION OF ISH