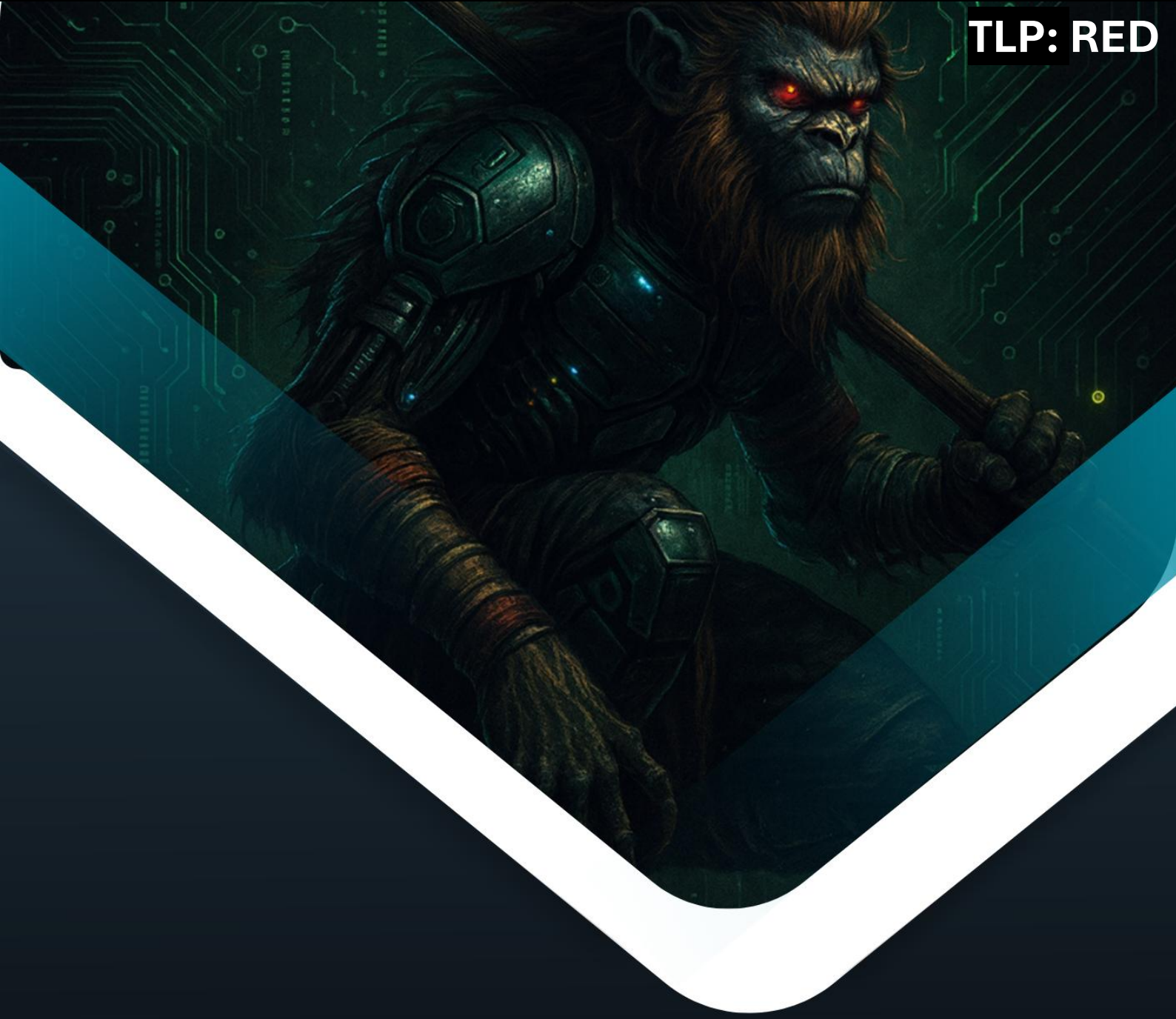
TLP: RED



Pesquisa de Cibersegurança

Cyber Threat Actor

A Análise da Kill Chain do Gunra Ransomware

Nova Variante Linux

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.

ISH

ALERTA HEIMDALL! HTTP2 RAPID RESET_IMPACTOS E DETECÇÃO DA CVE-2023-44487

Falhas de negação de serviço (DoS) não são apenas interrupções técnicas. Elas representam riscos reais à continuidade do negócio, à confiança dos clientes e à reputação da marca. Nisto temos a vulnerabilidade CVE-2023-44487, conhecida como HTTP/2 Rapid Reset.

BAIXAR

ISH

ALERTA HEIMDALL! BABUK2 EM 2025: RETORNO LEGÍTIMO OU COPYCAT ESTRATÉGICO

O cenário de ransomware manteve-se ativo em 2024 e se estendeu para este ano de 2025, com diversos grupos realizando ataques a uma ampla gama de organizações, setores e com surgimento de novos grupos. Nesse contexto, temos o ransomware Babuk2.

BAIXAR

ISH

ALERTA HEIMDALL! A ANATOMIA DO RANSOMWARE AKIRA E SUA EXPANSÃO MULTIPLATAFORMA

O cenário de ransomware manteve-se ativo em 2024 e se estendeu para este ano de 2025, com diversos grupos realizando ataques a uma ampla gama de organizações, setores e ganhando bastante popularidade. Nesse contexto, temos o ransomware Akira.

BAIXAR

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 **ransomware Gunra** foi identificado pela primeira vez em **10 de abril de 2025**, em uma campanha voltada a sistemas **Windows** e com forte inspiração no código e nas táticas do infame **Conti**. Assim como outras famílias surgidas após o vazamento do código-fonte do Conti em fevereiro de 2022 — como Black Basta e Royal —, o Gunra parece ter reutilizado e aprimorado essa base, focando em **acelerar negociações e refinar técnicas de engenharia social.** Entre suas estratégias mais marcantes está a **pressão baseada em tempo**, que exige que a vítima inicie **negociações em até cinco dias**, aumentando o estresse e a urgência do ataque.

O grupo ganhou notoriedade rapidamente, reivindicando o vazamento de **40 TB de dados** de um hospital em Dubai, **em maio de 2025**. Segundo dados de inteligência da Trend Micro, atividades do Gunra foram detectadas em organizações da **Turquia, Taiwan, Estados Unidos e Coreia do Sul**, abrangendo alvos governamentais e empresas dos setores de **saúde, manufatura e transporte**. Já o site de vazamentos do grupo indica vítimas no **Brasil, Japão, Canadá, Turquia e Estados Unidos**, incluindo também os segmentos de **direito, consultoria, TI e agricultura**. Desde sua primeira aparição, o grupo publicou e reivindicou **14 vítimas** em sua página de vazamentos.

Recentemente, o **Gunra** expandiu suas operações para o **Linux**, demonstrando uma clara estratégia de ataque multiplataforma. Ao contrário de outros ransomwares, cujo número de threads é fixo ou limitado pelo hardware da vítima, o Gunra permite configuração manual desse parâmetro, potencializando a velocidade do ataque.

Esta análise apresenta o contexto, **os recursos técnicos e o impacto dessa variante Linux,** além de situar sua evolução no cenário de ameaças atual. Informações sobre vetores de acesso inicial e métodos de propagação serão adicionadas em atualizações futuras, à medida que novos dados forem disponibilizados.

VITIMOLOGIA DO GUNRA RANSOMWARE

A distribuição geográfica das vítimas do **Gunra Ransomware** é ampla, abrangendo diferentes continentes, mas com registros notáveis em países como **Brasil, Japão, Canadá, Turquia e Estados Unidos**, segundo informações divulgadas no próprio site de vazamentos do grupo. Dados de telemetria e inteligência de ameaças da **Trend Micro** indicam ainda detecção de atividades associadas ao Gunra em **Turquia, Taiwan, Coreia do Sul e Estados Unidos,** incluindo ataques a órgãos governamentais e empresas privadas. No contexto latino-americano, o **Brasil** desponta como um dos países mais impactados.

Assim como diversos grupos de ransomware, os operadores do Gunra parecem **evitar alvos em países da antiga União Soviética** ou sistemas configurados com idioma russo como padrão, comportamento possivelmente vinculado a laços geográficos ou acordos tácitos entre grupos cibercriminosos. Desde sua primeira aparição em abril de 2025, o **Gunra tem mostrado rápida expansão operacional**, agora com uma **variante voltada para Linux**, o que amplia seu alcance a servidores e ambientes corporativos críticos. Essa evolução reflete uma estratégia mais distribuída e profissionalizada, possivelmente com recrutamento de afiliados e adaptação de campanhas a diferentes idiomas, regiões e setores econômicos.

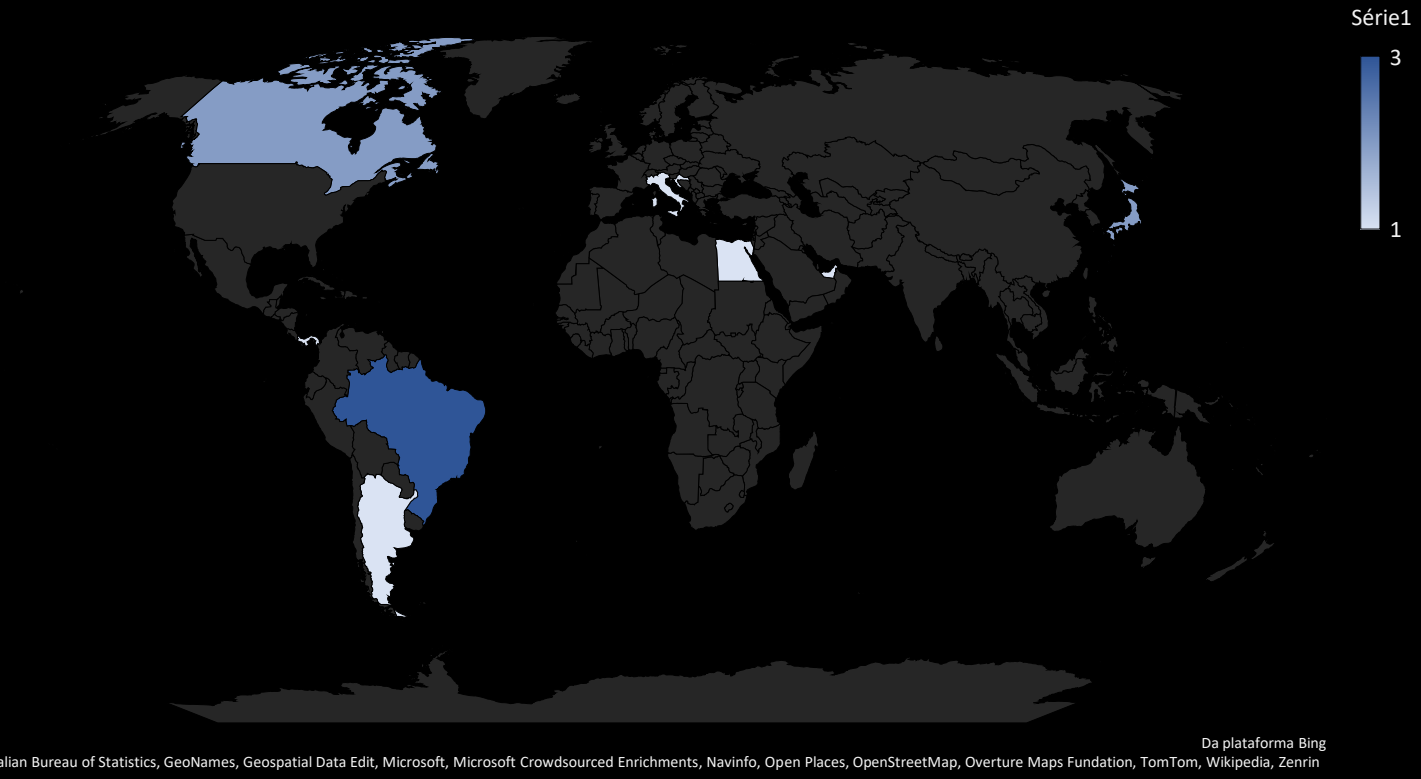


Figura 1 - Ransomware Victims by Country for group

O **foco primário do Gunra** é o ganho financeiro, com resgates que podem variar de dezenas a centenas de milhares de dólares, dependendo do porte e da capacidade de pagamento da vítima. **Observa-se preferência por organizações com alta receita anual ou detentoras de informações sensíveis de alto valor comercial**. A escolha de setores estratégicos levanta ainda a hipótese de **interesses secundários em espionagem industrial** ou sabotagem direcionada.

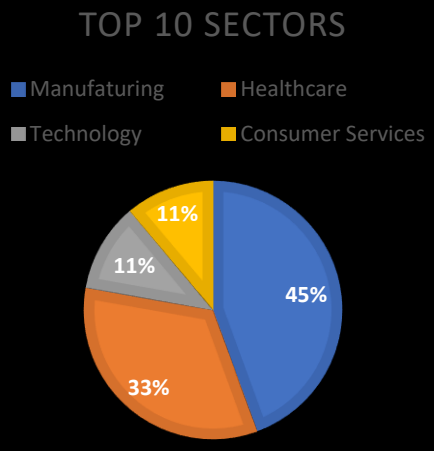
Entre os **setores mais visados** pelo Gunra, destacam-se:

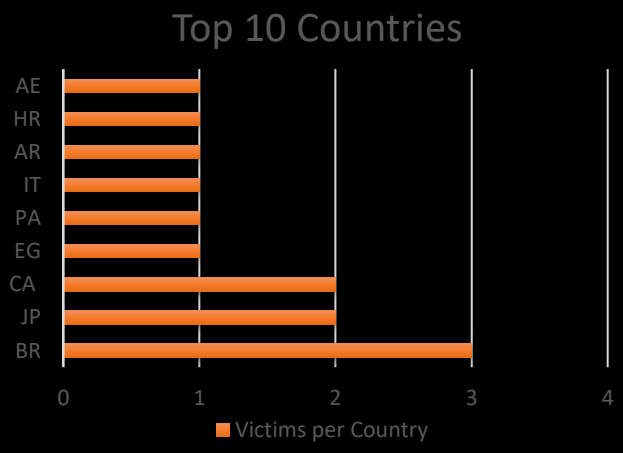
- *Saúde;*
- *Manufatura;*
- *Transporte;*
- *Tecnologia da Informação;*
- *Consultoria e serviços jurídicos;*
- *Agricultura*.

O grupo **não demonstra restrições explícitas** contra setores como educação ou governo — diferentemente de alguns concorrentes —, o que reforça seu caráter **oportunista** e **versátil** na seleção de alvos.

Além da criptografia de arquivos, o Gunra emprega **técnicas de dupla extorsão**, exfiltrando dados antes da cifragem e ameaçando publicá-los em seu site na dark web caso o resgate não seja pago. Essa abordagem aumenta a pressão sobre as vítimas, causando não apenas **interrupções operacionais severas**, mas também **danos reputacionais** e **exposição a responsabilidades legais**, especialmente em setores regulamentados.

A combinação de **criptografia multithread de alta performance**, **capacidade multiplataforma** e **pressão psicológica por tempo** posiciona o Gunra como uma ameaça sofisticada, persistente e adaptável, com potencial para impactar severamente organizações de diversos perfis e regiões.





INCIDENTES ENVOLVENDO O GUNRA RANSOMWARE

Desde sua primeira detecção em **abril de 2025**, o **Gunra Ransomware** apresentou uma rápida evolução operacional, combinando elementos técnicos herdados do **Conti** com inovações próprias, e expandindo sua atuação para sistemas **Linux**, ampliando o alcance a servidores e ambientes críticos. A seguir, estão os principais marcos e eventos conhecidos que evidenciam a sofisticação e a agressividade desse grupo.

Linha do Tempo de Atividades

- **10 de abril de 2025:** Primeiros ataques identificados contra sistemas **Windows**, com código e táticas inspiradas no Conti. Utilização de técnicas de pressão baseadas em tempo, exigindo o início das negociações em até cinco dias.
- **Maio de 2025**: Reivindicação do vazamento de **40 TB de dados** de um hospital em Dubai, marcando um dos maiores incidentes atribuídos ao grupo e consolidando sua presença no cenário global.
- **Maio–Junho de 2025**: Dados de inteligência da **Trend Micro** registram tentativas de ataque contra organizações na **Turquia, Taiwan, Estados Unidos e Coreia do Sul**, abrangendo setores como saúde, transporte, manufatura e governo.
- **Junho de 2025:** Confirmação da **variante Linux**, com capacidade de **criptografia multithread** configurável de até **100 threads**, criptografia parcial de arquivos e armazenamento de chaves RSA em *keystores* separados.
- **Julho de 2025**: O site de vazamentos do Gunra lista vítimas no **Brasil, Japão, Canadá, Turquia e Estados Unidos**, expandindo para setores como consultoria, TI, direito e agricultura.

- **Agosto de 2025:** Relatos não confirmados indicam incidentes em ambientes **VMware ESXi**, sugerindo possíveis testes ou adaptação da variante Linux para infraestrutura virtualizada.

Evolução Técnica e Estratégica

O **Gunra Ransomware** apresentou, desde seu surgimento uma evolução técnica acelerada e direcionada para ampliar sua eficácia e abrangência. Inicialmente focado em sistemas Windows, o grupo rapidamente desenvolveu uma **variante para Linux**, capaz de explorar ambientes corporativos críticos e,

possivelmente, **infraestruturas VMware ESXi**, conforme indicam relatos recentes.

Essa nova versão incorpora **criptografia multithread altamente configurável**, permitindo até **100 threads simultâneas**, superando o limite adotado por outros ransomwares conhecidos, e oferecendo controle refinado sobre a quantidade de dados cifrados por arquivo. O mecanismo de **criptografia parcial** acelera a execução do ataque e reduz a janela de reação das equipes de resposta. Outro avanço significativo é o **armazenamento separado das chaves RSA** em *keystores* dedicados, dificultando a recuperação sem pagamento do resgate. Essa abordagem demonstra conhecimento técnico avançado e preocupação em tornar a reversão do ataque mais complexa.

Além da sofisticação técnica, há sinais de que o Gunra adota um **modelo de operação próximo ao Ransomware como Serviço (RaaS)**, o que possibilita a **personalização das campanhas** conforme idioma, região e setor-alvo. Essa estratégia aumenta o alcance e diversifica o perfil das vítimas, explorando ao máximo as capacidades de seus afiliados ou colaboradores. A combinação de **alta performance**, **flexibilidade tática** e **amplo espectro de alvos** posiciona o Gunra como uma ameaça emergente, mas já adaptada para competir com grupos estabelecidos no cenário global de ransomware.

Impacto e Implicações

Os incidentes atribuídos ao **Gunra**, têm provocado **interrupções operacionais severas**, comprometendo a continuidade de negócios e causando prejuízos financeiros significativos às organizações afetadas. O modelo de **dupla extorsão**, que combina criptografia de dados e vazamento de informações sensíveis, amplia o impacto ao gerar **danos reputacionais** e **exposição a ações legais**, especialmente em setores regulamentados como saúde, jurídico e transporte.

A rápida capacidade de execução da variante Linux — impulsionada pela criptografia multithread e parcial — reduz drasticamente o tempo disponível para resposta e contenção, aumentando a taxa de sucesso dos ataques. Esse fator, somado à pressão psicológica imposta pelo prazo curto para negociações, intensifica o poder coercitivo do grupo.

Embora o Gunra seja um ator recente, o volume de vítimas publicadas em seu site de vazamentos desde abril de 2025 demonstra **atividade constante** e **expansão geográfica contínua**. A presença de vítimas em setores estratégicos e países com infraestrutura crítica reforça o potencial disruptivo dessa ameaça.

No cenário atual, o Gunra já se posiciona como um risco de alto impacto, combinando **sofisticação técnica**, **versatilidade tática** e **capacidade de adaptação** para explorar vulnerabilidades tanto em sistemas Windows quanto Linux. Essa convergência de fatores o coloca entre os grupos de ransomware com maior potencial de crescimento e periculosidade no curto prazo.

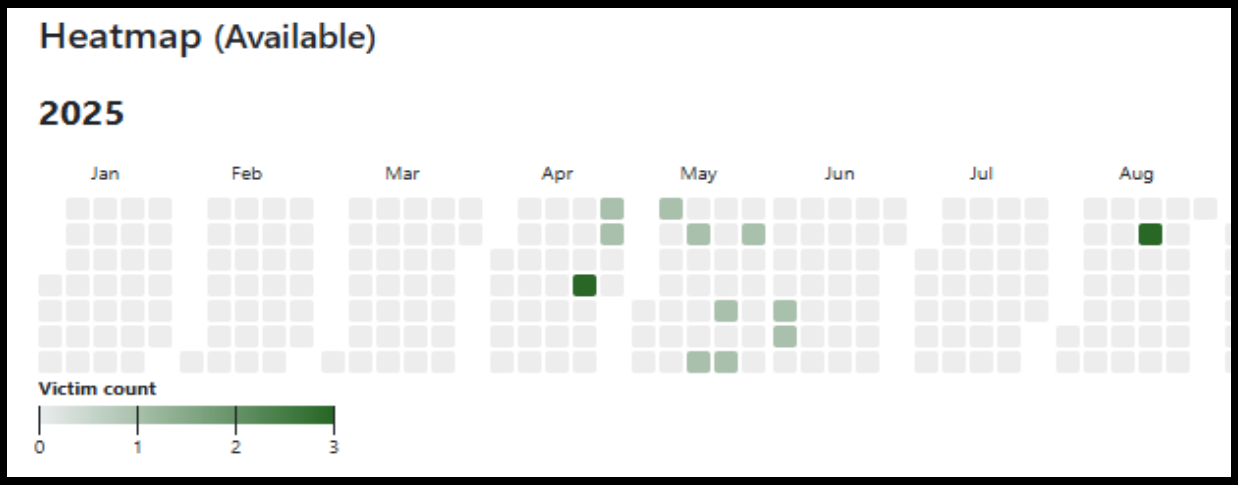


Figura 2 - Incidentes envolvendo o Gunra Ransomware desde 2025

TÁTICO

MODELO DE NEGÓCIO DA AMEAÇA

O **Gunra Ransomware** opera sob um modelo semelhante ao **Ransomware como Serviço (RaaS)**, no qual o núcleo do grupo é responsável pelo desenvolvimento, manutenção e atualização do malware, enquanto afiliados ou parceiros realizam as intrusões e conduzem as campanhas maliciosas. Essa estrutura descentralizada **amplia o alcance geográfico** das operações e dificulta a **atribuição direta** aos desenvolvedores originais.

Embora seja um ator recente, há fortes indícios de que o Gunra já estabeleceu **mecanismos de recrutamento** em fóruns clandestinos, atraindo indivíduos com diferentes níveis de especialização técnica. Esse modelo permite a personalização de ataques conforme idioma, localização e setor econômico, tornando as campanhas mais direcionadas e eficazes.

A estratégia central do grupo combina **dupla extorsão** e **pressão baseada em tempo**:

- **Exfiltração de dados sensíveis** antes da criptografia, ameaçando publicá-los em seu site de vazamentos na dark web caso o resgate não seja pago.
- **Imposição de prazos curtos para negociação** — geralmente até cinco dias —, aumentando o estresse e a urgência para forçar o pagamento.

O Gunra demonstra **capacidade de adaptação contínua**, incorporando recursos como criptografia **multithread configurável** (até 100 threads), **criptografia parcial** para maior agilidade e **armazenamento separado de chaves RSA** para dificultar a recuperação sem pagamento. Essas melhorias técnicas, aliadas à flexibilidade operacional do modelo RaaS, tornam o grupo uma ameaça persistente e desafiadora, capaz de explorar tanto sistemas **Windows** quanto **Linux**.

A combinação de **infraestrutura robusta de vazamento de dados**, **estratégias psicológicas de coerção** e **técnicas avançadas de evasão** reforça o Gunra como um ator emergente, mas com potencial para se consolidar rapidamente entre as operações de ransomware mais relevantes do cenário cibernético global.

INFRAESTRUTURA DE VAZAMENTO

Um dos elementos centrais da operação do **Gunra Ransomware** é o uso de um **Dedicated Leak Site (DLS)** hospedado na **dark web** em um endereço “

“.onion”, acessível exclusivamente por meio do navegador **Tor**. Essa plataforma funciona como o principal mecanismo de **pressão psicológica e operacional** contra as vítimas, sustentando o modelo de **dupla extorsão** adotado pelo grupo.

O site do Gunra apresenta uma **interface organizada e funcional**, similar à utilizada por outros operadores RaaS, transmitindo uma imagem de profissionalismo e controle. A estrutura de navegação normalmente inclui:

- ***Lista de vítimas*** *que não atenderam às exigências de resgate;*
- ***Área de contato*** *para negociação com os operadores.*
- ***Sessão de provas públicas*** *com amostras de dados exfiltrados.*
- ***Painel administrativo*** *de uso restrito aos integrantes do grupo.*

Cada registro na lista de vítimas geralmente contém:

- *Nome da organização afetada.*
- *País ou região da vítima.*
- *Setor de atuação.*
- *Volume estimado de dados roubados.*
- *Contagem regressiva para a divulgação completa dos dados.*
- *Links para os arquivos exfiltrados, liberados após o prazo final.*
- *Provas visuais como capturas de tela, planilhas, documentos financeiros ou e-mails corporativos.*

Essa infraestrutura é projetada para **amplificar o poder de coerção** do grupo, combinando exposição pública, dano reputacional e risco de sanções legais para forçar o pagamento do resgate. O contador regressivo serve como ferramenta de intimidação, colocando as vítimas sob **pressão temporal extrema**.

Relatos indicam que o Gunra mantém **atualizações constantes** no DLS, incluindo a adição rápida de novas vítimas e a publicação parcial de dados como forma de prova. Essa dinâmica sugere um fluxo contínuo de operações e uma estrutura logística robusta para o gerenciamento e distribuição de dados roubados.

CADEIA DE ATAQUE DA AMEAÇA

O **Gunra Ransomware** adota uma **cadeia de ataque modular e multifásica**, permitindo que seus operadores e afiliados personalizem as campanhas conforme o alvo e a infraestrutura disponível. Essa flexibilidade aumenta o alcance e a eficácia da ameaça, facilitando tanto intrusões oportunistas quanto ataques direcionados.

Embora detalhes completos sobre **acesso inicial** ainda estejam em investigação, evidências sugerem que o Gunra utiliza métodos variados, incluindo:

- **Exploração de vulnerabilidades conhecidas** em serviços expostos à internet, especialmente em ambientes Linux e possivelmente VMware ESXi.
- **Ataques de força bruta ou dicionário** contra credenciais SSH e painéis de administração remota.
- **Phishing e spear-phishing** com anexos ou links maliciosos, adaptados ao idioma e contexto da vítima.

Uma vez estabelecido o acesso inicial, o grupo tende a empregar **técnicas para elevação de privilégios** e **movimento lateral** dentro da rede corporativa, explorando credenciais comprometidas e vulnerabilidades locais.

Entre as táticas observadas ou inferidas para a variante Linux, destacam-se:

- Implantação direta do binário de ransomware em servidores comprometidos.
- Uso de criptografia **multithread** altamente configurável (até 100 threads simultâneas) para acelerar o processo e reduzir o tempo de detecção.
- Criptografia parcial de arquivos para otimizar o desempenho e manter a ameaça menos perceptível durante as fases iniciais.
- Armazenamento de chaves RSA em **keystores** separados, dificultando a recuperação sem pagamento do resgate.

*O **estágio final da cadeia** envolve a execução do ransomware, criptografando dados críticos e deixando mensagens de resgate que instruem as vítimas a acessar o **Dedicated Leak Site (DLS)** do grupo na dark web para negociações. Essa etapa é acompanhada de um prazo rígido — geralmente de cinco dias — para aumentar a pressão psicológica.*

*A **natureza flexível e descentralizada** dessa cadeia de ataque torna o Gunra particularmente perigoso, pois permite que afiliados escolham combinações distintas de vetores e ferramentas, adaptando-se rapidamente a novas defesas e explorando múltiplas superfícies de ataque.*

Initial Access

As campanhas do **Gunra** utilizam uma combinação de vetores para comprometer ambientes corporativos, especialmente servidores Linux e, potencialmente, VMware ESXi. O grupo adota tanto métodos de exploração técnica quanto abordagens de engenharia social, adaptando-se ao perfil do alvo.

Principais vetores de intrusão

- **Exploração de vulnerabilidades em serviços expostos**: focada em interfaces administrativas de sistemas Linux e painéis de virtualização, aproveitando falhas conhecidas ou zero-days para execução remota de código.
- **Ataques de força bruta ou dicionário contra credenciais SSH**: utilizados contra servidores com autenticação fraca ou sem restrições de acesso por IP.
- **Uso de credenciais comprometidas**: obtidas em fóruns clandestinos ou após infecções anteriores, permitindo acesso direto sem gerar tráfego suspeito.
- **Phishing e spear-phishing direcionados**: e-mails maliciosos com anexos ou links para download de scripts/bibliotecas trojanizadas, ajustados ao idioma e ao setor da vítima.

Fluxo típico observado

1. **Enumeração de serviços expostos** e verificação de versões vulneráveis.
2. **Comprometimento via exploração** (RCE ou falha de autenticação) ou **quebra de credenciais**.
3. **Implantação de scripts de preparação**, que configuram persistência, limpam rastros iniciais e realizam reconhecimento do ambiente.
4. **Entrega do payload do ransomware** diretamente no servidor alvo, preparado para execução multithread e criptografia seletiva.

Essa abordagem híbrida, combinando exploração de falhas, credenciais válidas e phishing direcionado, oferece ao Gunra flexibilidade para ajustar a intrusão conforme o nível de segurança da vítima, tornando a detecção precoce mais difícil e aumentando a taxa de sucesso das campanhas.

Esta fase pode envolver:

- ***T1190* – *Exploit Public-Facing Application***
  Exploração de vulnerabilidades em serviços expostos (interfaces Linux, painéis de administração e virtualização/ESXi) para execução remota de código.
- ***T1110* – *Brute Force***
  Ataques de força bruta e dicionário contra credenciais SSH e serviços remotos expostos.
- ***T1078* – *Valid Accounts***
  Uso de credenciais previamente comprometidas, obtidas em vazamentos, mercados clandestinos ou campanhas anteriores, para acesso direto sem acionar alertas.
- ***T1566* – *Phishing***
  Campanhas de e-mail malicioso (phishing e spear-phishing) contendo anexos ou links trojanizados, ajustados ao idioma e setor da vítima.

Execution and Establishment of Persistence

Após obter acesso inicial, o **Gunra Ransomware** executa uma série de ações para **consolidar sua presença no ambiente comprometido** e preparar o terreno para a fase de impacto. Essa etapa é caracterizada pelo uso de **scripts automatizados**, configuração de persistência em nível de sistema e ajustes para garantir a execução estável do binário malicioso.

Métodos de Execução

- **Transferência e execução do payload:** o binário do Gunra é carregado diretamente no servidor, seja em disco ou memória, pronto para iniciar o processo de criptografia.
- **Execução de scripts em Bash ou Python**: utilizados para manipular permissões, apagar rastros iniciais e configurar o ambiente antes da ativação do ransomware.
- **Execução em múltiplas threads**: o Gunra pode ser configurado para operar com até **100 threads simultâneas**, garantindo maior velocidade na criptografia e reduzindo a chance de detecção precoce.

Persistência no Ambiente Linux

- **Agendamento de tarefas via cron**: criação de tarefas programadas para garantir reexecução automática do binário após reinicializações.
- **Alteração de scripts de inicialização do sistema**: modificação de arquivos como “.bashrc”, “.profile” ou serviços em “/etc/init.d/” para reinfecção persistente.
- **Criação de usuários ou chaves SSH maliciosas**: em alguns cenários, operadores podem implantar contas adicionais ou inserir chaves SSH para manter acesso contínuo.

Fluxo típico observado

1. Drop do binário malicioso em diretórios estratégicos do servidor.
2. Execução inicial via scripts de automação (Bash/Python) para preparar o ambiente e configurar parâmetros de criptografia.
3. Configuração de persistência através de cron jobs ou manipulação de arquivos de inicialização. Entrega do payload do ransomware.
4. Validação do ambiente (arquitetura, permissões, diretórios prioritários) antes do início da criptografia em larga escala.

Essa fase reflete a preocupação do Gunra em garantir que o ransomware **permaneça ativo mesmo diante de reinicializações ou tentativas de contenção**, explorando técnicas comuns no ecossistema Linux, mas combinadas com **recursos avançados de performance e customização**, como o controle manual do número de threads e a criptografia parcial de arquivos.

Esta fase pode envolver:

- ***T1059* – *Command and Scripting Interpreter***
  Execução de scripts em Bash, Python ou Shell para manipular permissões, apagar rastros e acionar o binário malicioso.
- ***T1059.004* – *Command and Scripting Interpreter: Unix Shell***
  Uso de comandos nativos do Linux (ex: sh, bash) para iniciar ou automatizar a execução do ransomware.
- ***T1105* – *Ingress Tool Transfer***
  Transferência do binário do ransomware para o servidor comprometido, via SCP, wget, curl ou upload direto em sessão SSH.
- ***T1204.002* – *User Execution: Malicious File***
  Em cenários de phishing, a execução pode depender de o usuário abrir um arquivo malicioso ou script trojanizado.
- ***T1027* – *Obfuscated Files or Information***

Arquivos e scripts podem ser ofuscados para evitar a detecção por antivírus ou EDR.

- ***T1053.003* – *Scheduled Task/Job: Cron***
  Criação de cron jobs para garantir que o ransomware seja reexecutado após reinicializações.
- ***T1547.004* – *Boot or Logon Autostart Execution: Unix Shell Configuration Modification***
  Alteração de arquivos como "~.bashrc", "~.profile" ou scripts em "/etc/init.d/" para execução automática.
- ***T1136.001* – *Create Account: Local Account***
  Criação de contas adicionais para garantir acesso persistente ao sistema.
- ***T1098* – *Account Manipulation***
  Inserção de chaves SSH maliciosas no "~/.ssh/authorized_keys" ou modificação de contas existentes para manter o acesso.
- ***T1543.002* – *Create or Modify System Process: Systemd Service***
  Criação de serviços maliciosos no **systemd** para garantir persistência de longo prazo.
- ***T1505.003* – *Server Software Component: Web Shell***
  Implantação de web shells em servidores expostos, garantindo acesso remoto contínuo mesmo após resets de senha ou patches.

Discovery & Lateral Movement

Após garantir execução inicial e persistência, o **Gunra** passa à fase de **reconhecimento do ambiente interno** e **movimentação lateral**. O objetivo é identificar ativos críticos, ampliar o alcance do ataque e preparar a exfiltração e criptografia de dados em múltiplos sistemas.

Atividades de Reconhecimento

- **Enumeração de arquivos e diretórios:** identificação de volumes, diretórios prioritários e repositórios de dados sensíveis.
- **Mapeamento de rede e descoberta de hosts**: levantamento de servidores disponíveis, sistemas de backup e máquinas com dados estratégicos.
- **Coleta de informações de contas e credenciais**: análise de permissões e privilégios para facilitar a escalada de acesso.
- **Verificação de serviços em execução**: busca por portas abertas e aplicações vulneráveis em sistemas internos.

MOVIMENTAÇÃO LATERAL

- ***Acesso remoto via SSH**: uso de credenciais válidas ou obtidas por força bruta para se mover entre servidores Linux.*
- ***Abuso de chaves SSH**: inserção de chaves maliciosas em authorized_keys para manter acesso e movimentar-se de forma furtiva.*
- ***Transferência de ferramentas adicionais**: upload de utilitários e scripts auxiliares para movimentação lateral e coleta de informações.*
- ***Uso de protocolos administrativos legítimos** para evitar alertas e mascarar a atividade maliciosa.*

FLUXO TÍPICO OBSERVADO

1. Mapeamento da rede interna e enumeração de sistemas críticos (servidores de arquivos, bancos de dados, VMs e backups).
2. Aquisição de credenciais adicionais por meio de exploração, coleta ou manipulação de contas locais.
3. Conexão via SSH a outros servidores, expandindo o raio de comprometimento.
4. Posicionamento estratégico do ransomware em múltiplos hosts para garantir impacto generalizado durante a fase de criptografia.

Essa fase demonstra a capacidade do Gunra de **agir como uma ameaça multiplataforma e persistente**, utilizando técnicas comuns em ambientes Linux, mas com um nível de automação e agressividade que acelera a expansão do ataque antes que medidas defensivas sejam acionadas.

Esta fase pode envolver:

- ***T1083 – File and Directory Discovery***
  Enumeração de diretórios e arquivos críticos para identificar dados sensíveis.
- ***T1018 – Remote System Discovery***
  Descoberta de hosts e servidores ativos na rede.
- ***T1046 – Network Service Scanning***
  Escaneamento de portas e serviços internos para localizar alvos vulneráveis.
- ***T1087 – Account Discovery***
  Identificação de contas de usuário e permissões para facilitar elevação de privilégios.
- ***T1069 – Permission Groups Discovery***

Enumeração de grupos de privilégios (ex.: sudoers, grupos administrativos).

- ***T1057* – *Process Discovery***
  Identificação de processos em execução para determinar quais podem ser encerrados antes da criptografia.
- ***T1021.004* – *Remote Services: SSH***
  Uso de credenciais válidas ou roubadas para se mover entre servidores Linux via SSH.
- ***T1098* – *Account Manipulation***
  Inserção de chaves SSH maliciosas no ~/.ssh/authorized_keys ou modificação de contas existentes para manter o acesso.
- ***T1078* – *Valid Accounts***
  Uso de credenciais comprometidas obtidas em dumps, vazamentos ou força bruta para expandir acesso.
- ***T1105* – *Ingress Tool Transfer***
  Transferência de ferramentas auxiliares ou binários adicionais para novos hosts durante o movimento lateral.
- ***T1570* – *Lateral Tool Transfer***
  Copiar o binário do ransomware entre sistemas comprometidos, garantindo execução simultânea em múltiplos servidores.
- ***T1563.002* – *Remote Service Session Hijacking: SSH Hijacking***
  Sequestro de sessões SSH legítimas já estabelecidas, evitando a criação de novos logins visíveis em logs.

EXFILTRATION

O **Gunra Ransomware** adota uma abordagem sistemática para a exfiltração de dados, etapa fundamental para sustentar seu modelo de **dupla extorsão**. Antes de acionar a criptografia, os operadores coletam e enviam informações sensíveis para servidores controlados pelo grupo, reforçando a ameaça de exposição pública em seu **Dedicated Leak Site (DLS)** caso a vítima se recuse a pagar o resgate.

PRINCIPAIS MÉTODOS DE EXFILTRAÇÃO

- **Compressão e arquivamento de dados locais:** uso de ferramentas nativas ou scripts personalizados em Linux para agrupar grandes volumes de informação em pacotes organizados **(ZIP, TAR, GZ).**

- **Transferência de dados via canais de comando e controle:** envio direto para infraestrutura controlada pelo grupo, em muitos casos sobre conexões criptografadas para dificultar detecção.
- **Uso de protocolos alternativos não criptografados:** upload de dados por HTTP/HTTPS POST ou SCP, mascarado como tráfego legítimo.
- Publicação de amostras no DLS como comprovação da posse dos dados, ampliando a pressão psicológica sobre as vítimas.

FLUXO TÍPICO OBSERVADO

1. **Identificação de dados sensíveis** – documentos financeiros, registros médicos, bases de dados corporativas e arquivos confidenciais priorizados durante a fase de reconhecimento.
2. **Coleta e organização** – consolidação dos arquivos em diretórios temporários, muitas vezes renomeados para evitar fácil identificação.
3. **Compressão e preparação para envio** – uso de utilitários nativos do Linux (tar, gzip) ou ferramentas customizadas.
4. **Transferência para infraestrutura externa** – envio para servidores do Gunra em nuvem comprometida ou para infraestrutura dedicada em rede Tor.
5. **Prova de posse** – publicação parcial de arquivos no DLS com contador regressivo para liberação total, reforçando a coerção.

Essa estratégia reforça a **eficácia coercitiva** do Gunra, combinando danos técnicos com forte impacto psicológico e reputacional, tornando a exfiltração um dos pontos centrais de sua cadeia de ataque.

Esta fase pode envolver:

- ***T1560* – *Archive Collected Data***
  Compactação de arquivos antes da exfiltração.
- ***T1041* – *Exfiltration Over C2 Channel***
  Envio de dados por canais de comunicação controlados.
- ***T1048.003* – *Exfiltration Over Alternative Protocol : Unencrypted Non-C2 Protocol***
  Transferência via protocolos HTTP/SCP fora de canais tradicionais de C2.
- ***T1074* – *Data Staged***
  Preparação e armazenamento de arquivos exfiltrados em diretórios temporários.
- ***T1537* – *Transfer Data to Cloud Account***
  Possível uso de serviços legítimos de armazenamento para ocultar a movimentação de dados.

CRYPTOGRAPHY AND IMPACT

A fase de impacto do Gunra representa o estágio mais crítico da cadeia de ataque, quando os operadores consolidam o dano, impossibilitando a recuperação dos dados sem o pagamento do resgate. O grupo combina **velocidade de execução**, **parâmetros customizáveis de criptografia** e **técnicas de evasão** para maximizar a eficácia e pressionar as vítimas.

PRINCIPAIS MÉTODOS DE CRIPTOGRAFIA

- **Criptografia multithread altamente configurável**, permitindo até 100 threads simultâneas, acelerando o processo e reduzindo a janela de reação.
- **Criptografia parcial de arquivos**, que aumenta a eficiência do ataque e dificulta métodos de recuperação parcial.
- Extensão adicionada aos arquivos criptografados: .ENCRT.
- Armazenamento de chaves RSA em keystores separados, aumentando a complexidade da engenharia reversa.
- **Nota de resgate entregue**, direcionamento direto ao Dedicated Leak Site (DLS) na versão Linux, impondo prazo médio de **cinco dias** para início da negociação.

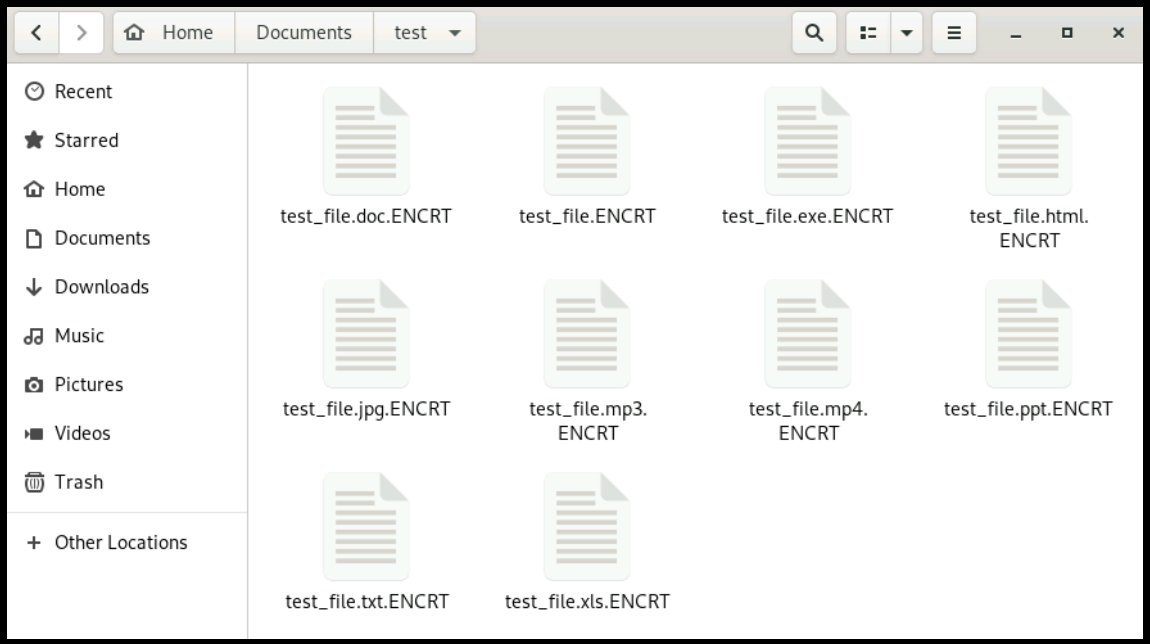


Figura 3 - Arquivos encriptografados com extensão .ENCRT

FLUXO TÍPICO OBSERVADO

1. **Enumeração de arquivos e processos** em execução para identificar alvos prioritários e evitar corromper o próprio sistema operacional.
2. **Encerramento de processos críticos** (como bancos de dados, serviços de backup e aplicações abertas) para liberar arquivos bloqueados.
3. **Remoção de cópias de segurança locais e snapshots**, impossibilitando restauração simples.
4. **Execução do módulo de criptografia**, aplicando ChaCha20 para cifrar blocos de 1 MB e protegendo as chaves com RSA.

5. Adição da extensão .ENCRT a todos os arquivos comprometidos.
6. **Comunicação de impacto**: inserção de nota de resgate (no Windows) ou direcionamento ao DLS no Linux, com contagem regressiva para o vazamento dos dados.

Essa estratégia reforça a **eficácia coercitiva** do Gunra, combinando danos técnicos com forte impacto psicológico e reputacional, tornando a exfiltração um dos pontos centrais de sua cadeia de ataque.

Esta fase pode envolver:

- ***T1486* – *Data Encrypted for Impact***
  Criptografia massiva de arquivos locais e compartilhados.
- ***T1490* – *Inhibit System Recovery***
  Exclusão de snapshots e cópias de sombra.
- ***T1070.001* – *Indicator Removal on Host: Clear Windows Event Logs***
  Em variantes Windows, limpeza de logs de eventos para dificultar a análise.
- ***T1562.001* – *Impair Defenses: Disable or Modify Tools***
  Desativação de serviços de backup, AV/EDR e processos que poderiam impedir a criptografia.
- ***T1027* – *Obfuscated Files or Information***
  Uso de técnicas de ofuscação no binário para reduzir detecção por antivírus.

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 comprometidas obtidas em fóruns clandestinos.
	T1190 – Exploit Public-Facing Application	Exploração de falhas em serviços Linux ou painéis VMware ESXi expostos.
	T1110 – Brute	Ataques de força bruta contra
	T1566 – Phishing	Campanhas de phishing com anexos ou links
Execution	T1059 – Command and Scripting Interpreter	Execução de scripts em Bash, Python ou Shell para manipular permissões, apagar rastros e acionar o binário malicioso.
	T1059.004 – Unix Shell	Uso de comandos nativos do Linux (sh, bash) para iniciar ou automatizar a execução do ransomware.
	T1204.002 – User Execution: Malicious File	Execução depende do usuário abrir um arquivo malicioso ou script trojanizado.
Commnd and Control	T1105 – Ingress Tool Transfer	Transferência do binário via SCP, wget, curl ou upload direto em sessão SSH.
Defense Evasion	T1027 – Obfuscated Files or Information	Arquivos e scripts ofuscados para evitar a detecção.
	T1078 – Valid Accounts	Uso de credenciais comprometidas para acesso lateral.
Persistence	T1053.003 – Scheduled Task/Job: Cron	Criação de cron jobs para reexecutar o ransomware após reinicializações.
	T1547.004 – Unix Shell Configuration Modification	Alteração de arquivos como “.bashrc”, “.profile” para execução automática.
	T1136.001 – Create Account: Local Account	Criação de contas adicionais para persistência.
	T1098 – Account Manipulation	Inserção de chaves SSH maliciosas ou modificação de contas existentes.
	T1543.002 – Systemd Service	Criação de serviços maliciosos no systemd para persistência.
	T1505.003 – Web Shell	Implantação de web shells para acesso remoto contínuo.

Discovery	T1083 – File and Directory Discovery	Enumeração de diretórios e arquivos críticos.
	T1018 – Remote System Discovery	Descoberta de hosts e servidores ativos na rede.
	T1046 – Network Service Scanning	Escaneamento de portas e serviços internos.
	T1087 – Account Discovery	Identificação de contas de usuário e permissões.
	T1069 – Permission Groups Discovery	Enumeração de grupos de privilégios como sudoers.
	T1057 – Process Discovery	Identificação de processos em execução.
Lateral Movement	T1021.004 – Remote Services: SSH	Uso de SSH para movimentação lateral.
	T1570 – Lateral Tool Transfer	Cópia do binário entre sistemas para execução simultânea.
	T1563.002 – SSH Hijacking	Sequestro de sessões SSH legítimas ativas.
Collection	T1560 – Archive Collected Data	Compactação de arquivos antes da exfiltração.
	T1074 – Data Staged	Armazenamento temporário dos arquivos exfiltrados.
Exfiltration	T1041 – Exfiltration Over C2 Channel	Envio de dados por canais de C2.
	T1048.003 – Exfiltration Over Alt. Protocol	Transferência via HTTP/SCP fora de C2 tradicional.
	T1537 – Transfer Data to Cloud Account	Uso de serviços de nuvem legítimos para esconder exfiltração.
Impact	T1486 – Data Encrypted for Impact	Criptografia massiva de arquivos locais e compartilhados.
	T1490 – Inhibit System Recovery	Exclusão de snapshots e cópias de sombra.
	T1070.001 – Clear Windows Event Logs	Limpeza de logs para dificultar análise.
	T1562.001 – Disable or Modify Tools	Desativação de AV/EDR e serviços de backup.
	T1027 – Obfuscated Files or Information	Ofuscação de binário para evitar detecção.

Tabela 1 - MITRE ATT&CK TTPs

VULNERABILIDADES EXPLORADAS PELA AMEAÇA

Durante a elaboração deste relatório, identificamos que os operadores do ransomware **SuperBlack** exploraram diversas vulnerabilidades críticas em ambientes corporativos para obter acesso inicial, realizar movimentações laterais e, posteriormente, implantar ransomware. A atuação do grupo evidencia uma estratégia sofisticada, com foco em explorar falhas conhecidas em produtos amplamente utilizados — especialmente em firewalls e soluções de VPN.

Essa abordagem ressalta a importância de manter sistemas atualizados, aplicar patches de segurança de forma contínua e monitorar ativamente a exposição de serviços críticos à internet.

CVE-2019-5544**Vulnerability**	**Product**	**Type**
CVE-2019-5544	VMware ESXi	**Information Disclosure** via OpenSLP
CVE-2020-3992	VMware ESXi	Use After Free vulnerability leading to RCE
CVE-2021-21972	VMware vCenter Server	Remote Code Execution (RCE) via vRealize Plugin
CVE-2021-21974	VMware ESXi	Heap Overflow in OpenSLP, enabling remote execution
CVE-2022-22947	VMware Spring Cloud Gateway	RCE via actuator endpoints
CVE-2022-22960	VMware Workspace ONE Access	Privilege Escalation via improper permissions
CVE-2022-22954	VMware Workspace ONE Access	RCE via command injection in log-related component
CVE-2023-20867	VMware Aria Operations	Authentication Bypass via hardcoded secrets
CVE-2021-3156	Sudo (Unix/Linux)	Privilege Escalation via buffer overflow (“Baron Samedit”)
CVE-2019-0211	Apache HTTP Server	Local Privilege Escalation
CVE-2021-4034	Polkit (pkexec)	Privilege Escalation via memory corruption (“PwnKit”)
CVE-2022-0847	Linux Kernel	Privilege Escalation via Dirty Pipe

CVE-2022-36537	ZK Framework (usado em NAS QNAP)	RCE via deserialização
CVE-2021-26084	Atlassian Confluence	RCE via template injection
CVE-2023-22515	Atlassian Confluence	Authentication Bypass + Privilege Escalation
CVE-2021-36260	Huawei Devices (web interfaces)	Command Injection via web components
CVE-2020-25078	Netgear Routers	Stack Overflow for unauthenticated users

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

RECOMENDAÇÕES

Além dos indicadores de comprometimento apresentados neste relatório, é essencial adotar práticas de segurança que visem mitigar os riscos associados ao ransomware **Gunra**. A seguir, são listadas recomendações que fortalecem a postura defensiva das organizações frente a esse tipo de ameaça:

MANTENHA SISTEMAS E SOFTWARES ATUALIZADOS

- Aplique regularmente patches de segurança em **sistemas operacionais Linux**, servidores expostos à internet e aplicações de banco de dados.
- Priorize a atualização de serviços críticos como **MS-SQL** e outros sistemas frequentemente explorados pelo Gunra em ataques oportunistas.

Implemente autenticação forte e segregação de privilégios

- Ative autenticação multifator (MFA) para todos os acessos remotos e privilegiados.
- Restringa o uso de contas privilegiadas apenas a operações necessárias e monitore inclusões em grupos de administradores locais.

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.

Monitore e análise atividades da rede

- Implemente soluções de **SIEM e NDR** com regras específicas para detectar **varredura de rede, execução de binários maliciosos em Linux e uso anômalo de comandos shell**.
- Monitore a execução de **scripts bash, python ou comandos administrativos** que possam indicar tentativas de persistência ou movimentação lateral.

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:	9a7c0adedc4c68760e49274700218507
sha1:	77b294117cb818df701f03dc8be39ed9a361a038
sha256:	854e5f77f788bbbe6e224195e115c749172cd12302afca370d4f9e3d53d005fd
File name:	854e5f77f788bbbe6e224195e115c749172cd12302afca370d4f9e3d53d005fd.exe

Indicadores do artefato	
md5:	7dd26568049fac1b87f676ecfaac9ba0
sha1:	bb79502d301ba77745b7dbc5df4269fc7b074cda
sha256:	a82e496b7b5279cb6b93393ec167dd3f50aff1557366784b25f9e51cb23689d9
File name:	.packed

Indicadores do artefato	
md5:	ae6f61c0fc092233abf666643d88d0f3
sha1:	79e19d3d8405425735e4b3cd36a8507d99dfee20
sha256:	944a1a411abb97f9ae547099c4834beb49de0745740ba450efb747bd62d8d83b
File name:	_944a1a411abb97f9ae547099c4834beb49de0745740ba450efb747bd62d8d83b.exe

Indicadores do artefato	
md5:	f6664f4e77b7bcc59772cd359fdf271c
sha1:	0c3c878b678c7254446e84cca6f0d63caeb51880
sha256:	5530363373dfe8fa474c9394184d2c56a0682c6a178d6f1c3536a1a3796dff42
File name:	5530363373dfe8fa474c9394184d2c56a0682c6a178d6f1c3536a1a3796dff42.exe

Tabela 3 - Indicadores de Comprometimento

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