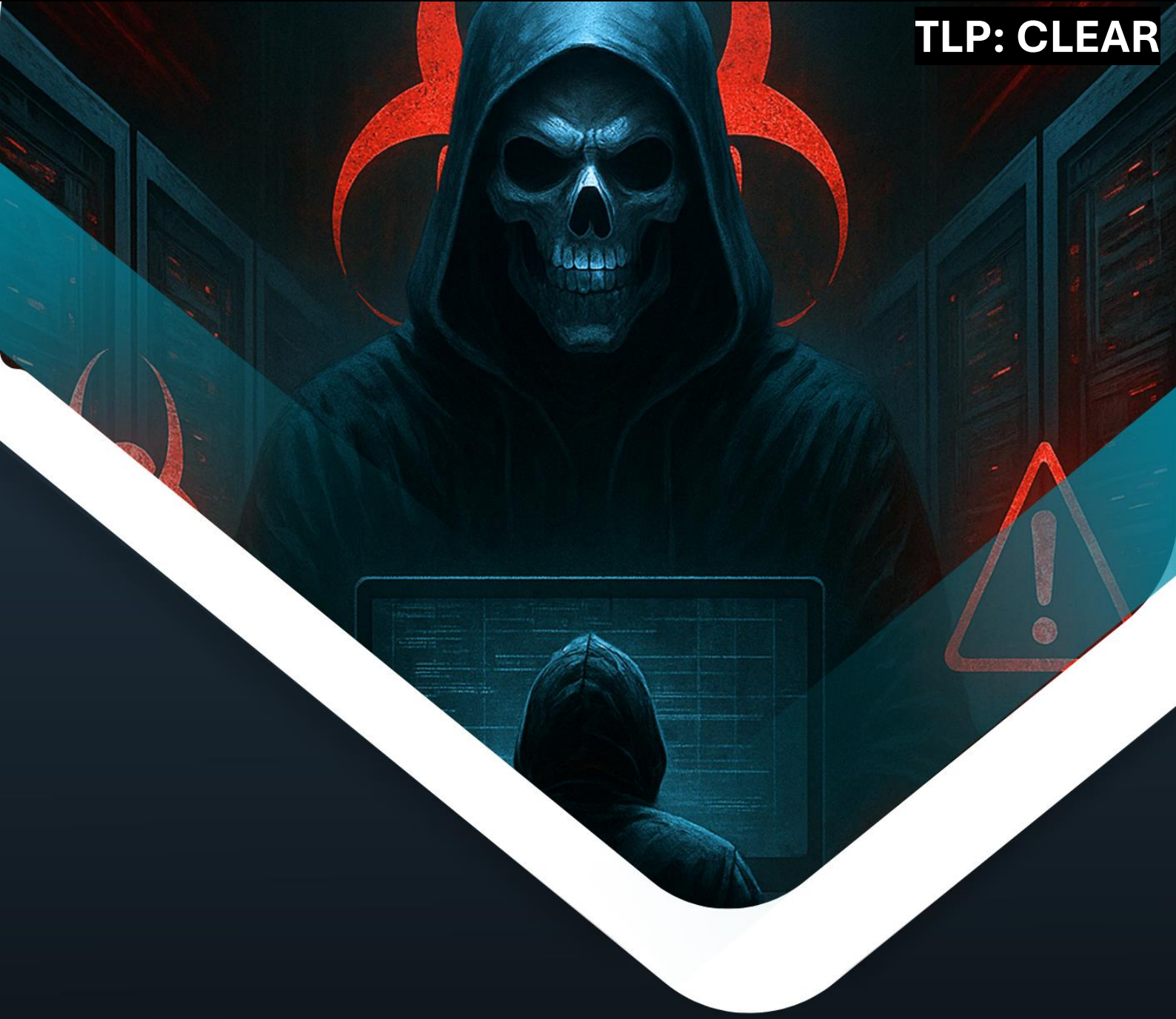
TLP: CLEAR



Pesquisa de Cibersegurança

Cyber Threat Actor

A Análise da Kill Chain do SuperBlack 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.

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 **SuperBlack Ransomware** é uma variante identificada no final de janeiro de 2025, atribuída ao grupo cibercriminoso **Mora_001**, com possíveis vínculos operacionais com o ecossistema ***LockBit***. Essa ameaça tem como principal vetor de acesso inicial a exploração de duas vulnerabilidades críticas em firewalls Fortinet — **CVE-2024-55591** e **CVE-2025-24472** — que permitem a obtenção de privilégios de **superadministrador** em dispositivos **FortiGate** expostos.

O grupo se destaca pelo uso de uma cadeia de ataque sofisticada que inclui **acesso inicial** via **exploração remota**, **escalonamento de privilégios**, **movimentação lateral por VPN**, **WMIC** e **SSH**, **exfiltração de dados** e posterior **criptografia seletiva** com base no **builder** vazado do **LockBit 3.0**. Também foram encontradas semelhanças em **ransom notes**, identificadores **TOX** e infraestrutura de comunicação. Além do ransomware, os atacantes empregam o **WipeBlack**, um componente **wiper** usado para apagar evidências e dificultar a resposta a incidentes. Essa ferramenta já havia sido observada em campanhas anteriores associadas ao ransomware **BrainCipher**, outro derivado do ecossistema **LockBit**.

Com mais de **3.200 dispositivos vulneráveis** identificados no **Brasil** durante o período de atividade, o SuperBlack representa uma ameaça relevante para organizações que utilizam **appliances Fortinet** sem correções recentes. A combinação entre técnicas de **dupla extorsão** e **sofisticação tática** torna essa ameaça crítica no cenário atual, exigindo resposta rápida, monitoramento contínuo e aplicação imediata de atualizações de segurança.

VITIMOLOGIA DO SUPERBLACK RANSOMWARE

A atuação do **SuperBlack Ransomware** apresenta foco global, mas com destaque significativo para o **Brasil**, que figura entre os países mais afetados, com mais de **3.200 dispositivos FortiGate vulneráveis** identificados no momento dos ataques. A distribuição geográfica das vítimas segue um padrão semelhante ao de outras variantes do ecossistema LockBit, com maior incidência em países que utilizam dispositivos **Fortinet** amplamente expostos e sem atualizações de segurança aplicadas.

Embora os ataques sejam considerados **oportunistas**, direcionados a organizações que mantêm firewalls com interfaces administrativas acessíveis pela internet, há indícios de **seleção estratégica de alvos**, priorizando ambientes com maior superfície de ataque e infraestrutura crítica exposta. O grupo por trás do SuperBlack também segue o comportamento típico de grupos **russófonos**, **evitando sistemas configurados com idioma russo** e países da antiga **União Soviética**.

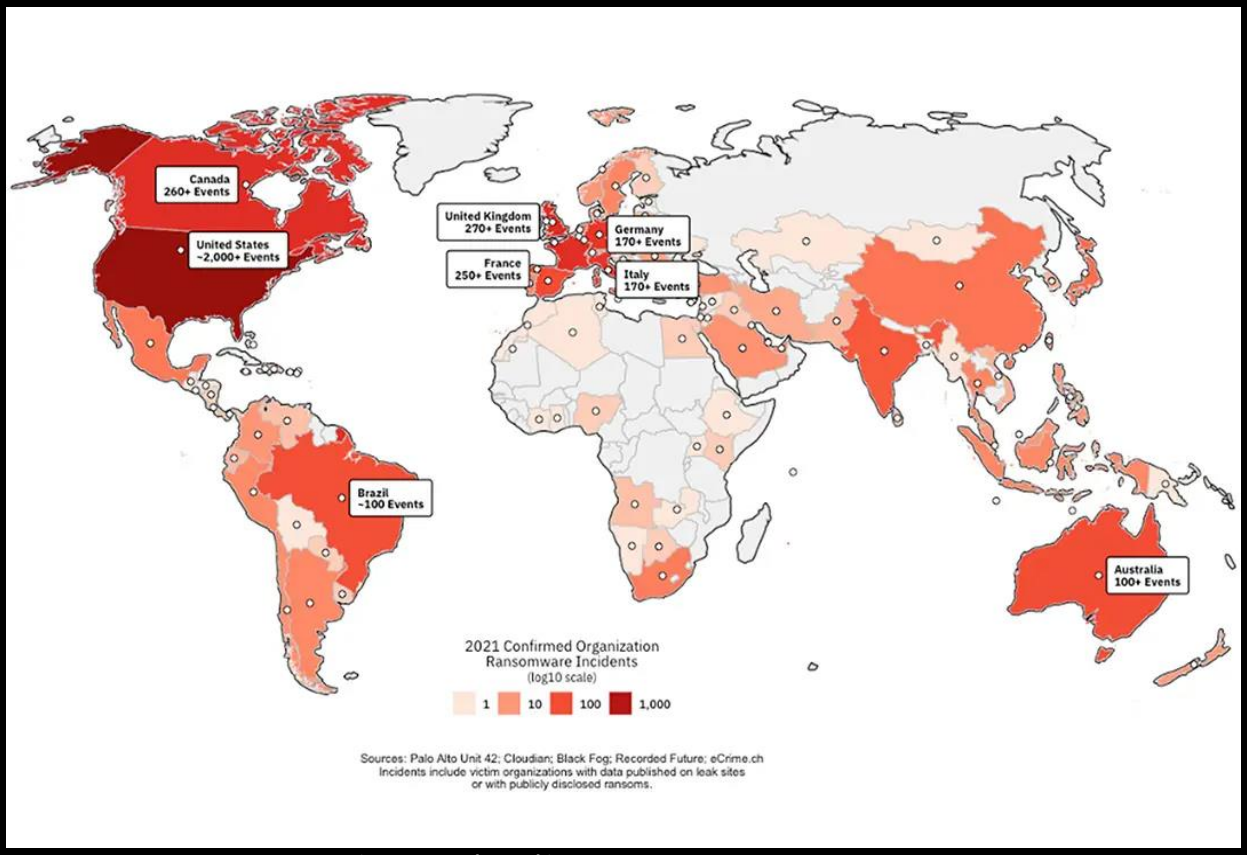


Figura 1 - Países Vítimas do Superblack Ransomware.

As vítimas têm perfil variado, mas o grupo demonstra preferência por **ambientes corporativos com uso intensivo de infraestrutura Fortinet**, explorando brechas para comprometer servidores, controladores de domínio, bancos de dados e sistemas de autenticação.

Regiões com alto impacto: Brasil (destaque na América Latina), EUA, Índia, entre outros.

Setores visados:

- Serviços de tecnologia da informação;
- Infraestrutura e telecomunicações;
- Setores financeiros e corporativos;
- Manufatura e logística;
- Empresas com forte dependência de conectividade remota (VPNs corporativas).

A abordagem dos operadores envolve **dupla extorsão**, com **exfiltração de dados sensíveis antes da criptografia,** e posterior ameaça de divulgação pública em caso de não pagamento. Além disso, a presença do módulo **WipeBlack** evidencia a intenção de dificultar a recuperação e a análise forense, ampliando os danos e o tempo de resposta das vítimas.

O modelo operacional do grupo **Mora_001**, responsável pelo SuperBlack, é compatível com o padrão **RaaS** *(Ransomware as a Service),* podendo ser conduzido por **afiliados especializados** em diferentes fases da cadeia de ataque — do acesso inicial à monetização. Esse formato contribui para a expansão rápida e modular da ameaça.

A vitimologia do SuperBlack, portanto, revela uma ameaça **altamente direcionada**, com **motivações financeiras claras**, uso de **técnicas avançadas de intrusão**, e **potencial impacto severo sobre a continuidade operacional e reputacional** das organizações comprometidas.

INCIDENTES ENVOLVENDO O MALLOX RANSOMWARE

Desde sua identificação em **janeiro de 2025**, o ransomware **SuperBlack** tem sido responsável por uma série de incidentes de alto impacto. A ameaça, atribuída ao grupo **Mora_001**, explora vulnerabilidades críticas em dispositivos **Fortinet**, com foco em **FortiGate** e **FortiProxy**, a partir de uma cadeia de ataque bem estruturada e rápida execução — em alguns casos, com **implantação de ransomware em menos de 48 horas**.

Linha do Tempo de Atividades

- **Novembro de 2024:** Primeiros sinais de exploração da vulnerabilidade **CVE-2024-55591**, como **zero-day**.
- **14 de Janeiro de 2025:** Fortinet divulga comunicado oficial sobre a falha (Advisory).
- **27 de janeiro de 2025:** PoC (Proof of Concept) é publicada publicamente.
- **31 de janeiro a 3 de março de 2025:** Período de exploração ativa com múltiplas vítimas confirmadas.
- **8 de fevereiro de 2025:** É acrescentada a falha **CVE-2025-24472** ao advisory oficial da Fortinet.

Evolução Técnica e Estratégica

O **SuperBlack** evidencia uma evolução tática sofisticada, marcada por seu **rápido desenvolvimento**, uso de recursos reutilizados do ecossistema cibercriminoso e adaptação a múltiplos ambientes.

A ameaça foi construída com base no **builder vazado do LockBit 3.0**, demonstrando como operadores como o grupo **Mora_001** reutilizam ferramentas previamente divulgadas para criar variantes com identidade própria. A personalização inclui a **remoção de marcas visuais do LockBit** nas notas de resgate, adoção de exfiltradores customizados, e mudanças nos vetores de persistência — tornando cada ataque mais difícil de rastrear ou associar diretamente ao ransomware original.

A arquitetura do ataque é apoiada por automações em diversas fases. Scripts personalizados são utilizados para:

- Criar contas **administrativas locais** e **VPNs persistentes**;
- Automatizar a **restauração de privilégios elevados**, caso removidos;
- Efetuar **backup** e **exportação** de configurações de dispositivos Fortinet;
- **Manter acesso contínuo** mesmo após reinicializações do sistema.

Essa estrutura técnica revela um **modus operandi** orientado por **eficiência, ofuscação e resiliência**. Além disso, foram observadas **duas técnicas distintas de exploração** das falhas críticas da Fortinet (**WebSocket** e **HTTPS**), o que reforça a capacidade de adaptação da ameaça ao ambiente-alvo.

Por fim, o uso do módulo **WipeBlack** — um componente wiper que apaga rastros e dificulta a análise forense — consolida a natureza destrutiva e altamente evasiva da operação, com foco em comprometer a continuidade das vítimas e acelerar o impacto do ataque.

Impacto e Implicações

Os ataques associados ao **SuperBlack** têm provocado **interrupções operacionais críticas** e **exposição de dados sensíveis** em diversas organizações, especialmente aquelas que utilizam dispositivos **Fortinet** com interfaces de gerenciamento expostas à internet.

A atuação do grupo **Mora_001** destaca-se pela agressividade e eficiência, com **movimentação lateral rápida**, **exfiltração de dados estruturada** e posterior criptografia, o que caracteriza um modelo de **dupla extorsão**. A presença do componente **WipeBlack**, utilizado para apagar logs e arquivos sensíveis, agrava ainda mais o impacto ao dificultar investigações forenses e a recuperação do ambiente comprometido.

O padrão observado nos incidentes evidencia um **modelo de ataque contínuo e automatizado**, com ações coordenadas que incluem:

- Comprometimento de infraestrutura crítica (VPNs, controladores de domínio, bancos de dados);
- Inviabilização de recuperação de sistemas via backups tradicionais;
- Ameaças explícitas de **vazamento de dados em sites de *leak* na dark web**;
- Demandas de resgate com valores elevados, direcionadas a organizações com maior capacidade financeira.

O impacto dos ataques ultrapassa os danos técnicos, resultando em **perdas financeiras**, **danos à reputação institucional** e **possíveis sanções legais** relacionadas à violação de dados. A combinação entre **sofisticação técnica**, **velocidade de execução** e **intenção destrutiva** posiciona o SuperBlack como uma ameaça de alto risco que exige resposta rápida, medidas preventivas eficazes e reforço contínuo nas defesas cibernéticas.

TÁTICO

MODELO DE NEGÓCIO DA AMEAÇA

O **SuperBlack** opera dentro de um modelo que reflete características do **Ransomware como Serviço (RaaS)**, embora com nuances que indicam um controle mais centralizado e direcionado pelo grupo **Mora_001**. Essa estrutura híbrida combina elementos de **profissionalismo técnico**, **customização de payloads** e **operações orientadas a lucro**, adotando práticas semelhantes às de grandes gangues como a LockBit.

Ao reutilizar e modificar o **builder vazado do LockBit 3.0**, o **Mora_001** consegue gerar variantes personalizadas do SuperBlack, excluindo marcas explícitas do LockBit e utilizando ferramentas próprias de exfiltração. Essa abordagem sugere uma operação autônoma ou afiliada altamente especializada, com conhecimento avançado em **engenharia reversa** e **desenvolvimento de malware.**

Embora ainda não haja evidências claras de uma campanha aberta de recrutamento de afiliados, como visto em fóruns clandestinos por grupos típicos de RaaS, os ataques indicam uma estrutura de operação replicável e organizada, com padrões técnicos consistentes e reutilização de infraestrutura — incluindo **ID TOX** associado anteriormente ao LockBit, o que sugere possível **reaproveitamento de canais de comunicação ou colaboração com ex-membros** da gangue.

O SuperBlack também adota o modelo de **dupla extorsão**, com **exfiltração prévia de dados sensíveis** antes da criptografia. Caso a vítima não pague o resgate, há ameaça de divulgação pública dos dados, potencialmente em fóruns da dark web ou plataformas controladas pelos operadores.

Em síntese, o modelo de negócio por trás do SuperBlack revela uma operação bem financiada, tecnicamente madura e com alto potencial de impacto, mesmo sem seguir o formato clássico de RaaS. Sua eficácia está ancorada na **velocidade, discrição e sofisticação técnica**, o que torna sua detecção e contenção um desafio significativo para equipes de segurança.

INFRAESTRUTURA DE VAZAMENTO

Uma das peças centrais na operação do **SuperBlack** é o uso de uma infraestrutura dedicada para vazamento de dados — típica do modelo de **dupla extorsão**. Até o momento, os operadores associados ao grupo **Mora_001** utilizam plataformas na **dark web** como forma de pressionar as vítimas a efetuarem o pagamento do resgate, ameaçando a exposição pública das informações sensíveis exfiltradas durante o ataque.

Embora ainda não tenha sido identificado **um Dedicated Leak Site** (***DLS***) exclusivo e consolidado com a marca "SuperBlack", evidências indicam que os dados roubados são publicados ou referenciados em sites ***.onion* temporários**, **fóruns clandestinos** e **plataformas utilizadas anteriormente por grupos como o LockBit** — o que reforça a conexão operacional entre **Mora_001** e ecossistemas RaaS mais amplos.

As publicações normalmente seguem o formato padrão de vazamentos cibercriminosos, incluindo:

- *Nome da organização vítima;*
- *País ou setor de atuação;*
- *Volume estimado dos dados exfiltrados;*
- *Provas públicas (ex.: capturas de tela, documentos, tabelas);*
- *Contadores regressivos para divulgação completa;*
- *Links para arquivos hospedados em repositórios temporários na dark web.*

Esse modelo serve como mecanismo de coerção psicológica e financeira, amplificando o impacto do ataque por meio da exposição reputacional e do risco de **sanções legais e regulatórias** relacionadas à violação de dados. A ausência de um domínio fixo também pode ser uma estratégia deliberada de evasão e mobilidade, dificultando o rastreio da infraestrutura pelos defensores e pelas forças de segurança. A utilização de **IDs TOX** para contato direto e canais criptografados reforça a confidencialidade das negociações e dificulta a interceptação da comunicação entre operadores e vítimas.

Em suma, a infraestrutura de vazamento do SuperBlack está alinhada às práticas modernas de ransomware avançado, adotando táticas de pressão sofisticadas e utilizando recursos herdados ou compartilhados com operações como a do LockBit, mesmo sem uma identidade visual própria totalmente consolidada.

CADEIA DE ATAQUE DA AMEAÇA

O **SuperBlack** Ransomware, operado pelo grupo **Mora_001**, segue uma cadeia de ataque altamente estruturada e executada com precisão, evidenciando um modus operandi profissional e com forte capacidade de adaptação. As campanhas conhecidas até o momento demonstram consistência nos padrões táticos e operacionais, com foco na exploração de vulnerabilidades críticas em dispositivos de borda para acesso inicial, seguidas por movimentações laterais rápidas e técnicas de persistência avançadas.

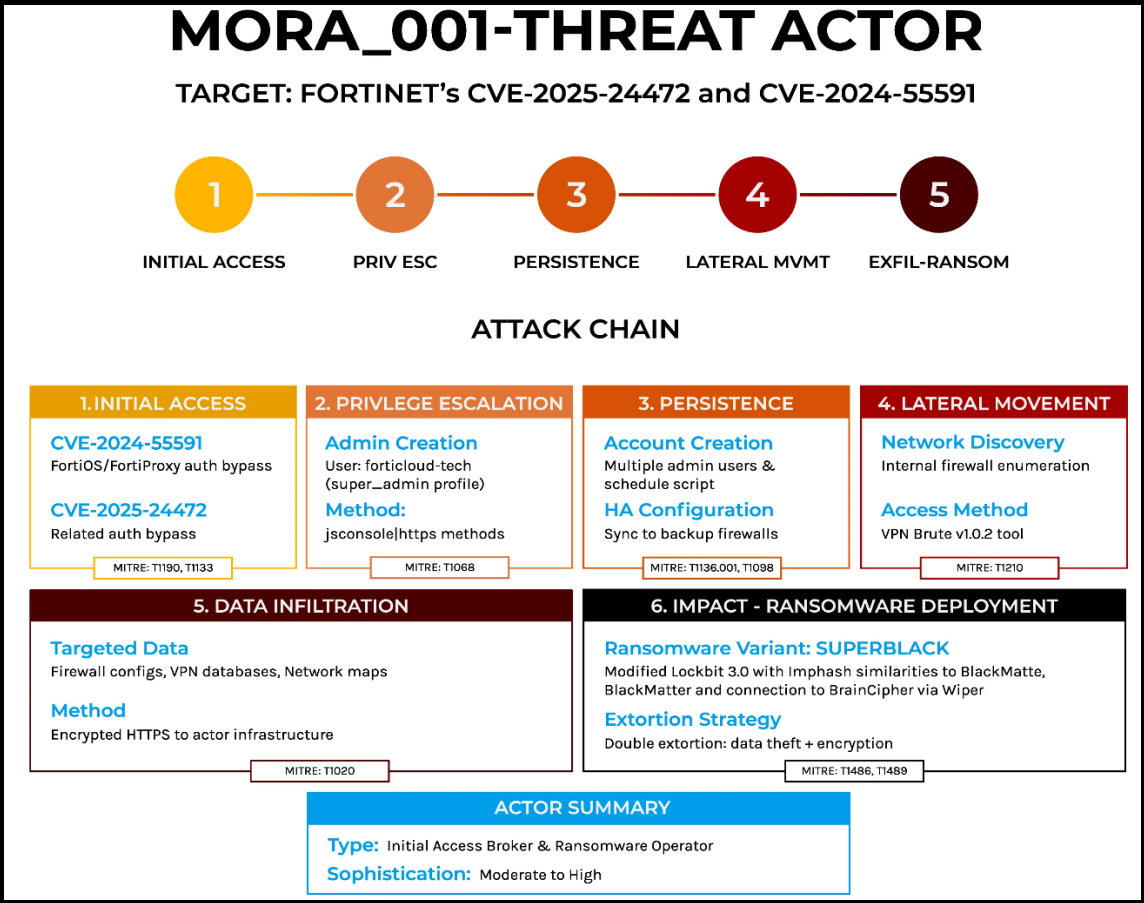


Figura 2 - Figura 2 - Diagrama da cadeia de ataque do SuperBlack – Fonte: Forescout Research

TARGET RECOGNITION AND IDENTIFICATION

Na fase inicial de suas campanhas, os operadores do **SuperBlack**, atribuídos ao grupo **Mora_001**, realizam **varreduras automatizadas em larga escala** com o objetivo de identificar **dispositivos Fortinet vulneráveis expostos na internet**, principalmente firewalls **FortiGate** e **FortiProxy**.

Essa etapa de reconhecimento é altamente sistematizada e evidencia o uso de ferramentas automatizadas capazes de:

- *Detectar dispositivos com firmware* ***FortiOS vulnerável****;*
- *Verificar a exposição de interfaces administrativas;*
- *Realizar requisições automatizadas com* ***nomes de usuário gerados aleatoriamente*** *(com cinco caracteres), indicando a execução de ataques de autenticação por força bruta ou fuzzing de interfaces.*

Entre os principais vetores explorados para acesso inicial, destacam-se duas vulnerabilidades críticas:

- **CVE-2024-55591**: *falha de autenticação via WebSocket na interface administrativa do FortiOS, permitindo* ***elevação de privilégios para super_admin;***
- **CVE-2025-24472**: *vulnerabilidade de autenticação adicional, que quando encadeada com a anterior, amplia o controle do invasor sobre o dispositivo comprometido.*

Essas falhas são particularmente graves por permitirem o **comprometimento completo do firewall**, que atua como ponto estratégico de entrada para redes corporativas. Após a identificação de um alvo vulnerável, o operador inicia o processo de exploração utilizando dois métodos distintos:

- **Solicitações HTTPS customizadas**, simulando tráfego legítimo para contornar sistemas de detecção;
- **Conexões via WebSocket**, explorando diretamente a interface **jconsole** dos dispositivos afetados.

Em alguns casos, foram observadas tentativas iniciais de login e posterior criação de **usuários administrativos locais**, possibilitando o acesso persistente mesmo após reinicializações ou tentativas de remediação.

Essa fase também pode incluir:

- ***Enumeração da topologia da rede alvo****;*
- ***Identificação de ativos críticos*** *(controladores de domínio, servidores de autenticação, bases de dados e repositórios de arquivos);*
- *Preparação para movimentações laterais com base no mapeamento da infraestrutura.*

A sofisticação do reconhecimento realizado pelo grupo **Mora_001** permite não apenas a seleção eficaz de alvos, mas também o planejamento estruturado das etapas seguintes da cadeia de ataque, reduzindo o tempo entre o comprometimento inicial e a ativação do ransomware.

Esta fase pode envolver:

- ***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 e domínio. Essas informações ajudam a identificar sistemas prioritários, como servidores de arquivos ou controladores de domínio.
- ***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.
- ***T1046* – *Network Service Discovery***
  Execução de varreduras internas com ferramentas nativas ou scripts personalizados para descobrir serviços e portas em uso dentro da rede, com foco em RDP (3389), SMB (445), e portas de autenticação (389/636). Isso permite identificar pontos com acesso remoto ativo ou interfaces de administração.
- ***T1135* – *Network Share Discovery***
  Enumeração de compartilhamentos de rede utilizando **net view**, **net share** ou **PowerShell**, com o objetivo de localizar pastas compartilhadas em servidores e estações, geralmente visando servidores de arquivos para futura exfiltração e criptografia.
- ***T1201* – Password Policy Discovery**
  Consulta a políticas de senha locais por meio do comando **net accounts** ou consultas via **PowerShell**, a fim de entender complexidade de senhas e frequência de expiração, o que auxilia na criação de credenciais persistentes ou na engenharia de contas com senhas fracas.
- ***T1033* – System Owner/User Discovery**
  Identificação de usuários atualmente logados com query **user**, **whoami**, **tasklist /v e PowerShell**, usada para reconhecer contas privilegiadas ou usuários ativos com perfil de administrador, que possam ser alvo de hijack ou movimentação lateral.
- ***T1482* – Domain Trust Discovery**
  Utilização de **nltest /domain_trusts** e **dsquery** para explorar relações de confiança entre domínios, com o objetivo de entender o alcance da infraestrutura do AD e as possibilidades de expansão do ataque para outros ambientes confiáveis.

Initial Access and Establishing Persistence

Após identificar um dispositivo Fortinet vulnerável, o grupo **Mora_001**, associado ao ransomware **SuperBlack**, executa a exploração das falhas **CVE-2024-55591** (bypass de autenticação via WebSocket) e **CVE-2025-24472** (elevação de privilégio). Essas vulnerabilidades, quando combinadas, permitem acesso não autenticado com privilégios de **super_admin** em dispositivos FortiOS (versões anteriores à 7.0.16).

Logo após o comprometimento, os invasores criam contas administrativas locais com nomes camuflados, como:

- ***forticloud-tech*;**
- ***fortigate-firewall*;**
- ***adnimistrator*** *(com erro ortográfico propositall);*

Essas contas são utilizadas para consolidar o controle e, em alguns casos, para implementar um encadeamento de contas, em que cada nova conta criada gera outras automaticamente. Esse método complica os esforços de detecção e remoção, retardando a resposta da equipe de segurança.

Métodos de Exploração Observados

A exploração foi registrada por meio de dois vetores distintos:

- ***WebSocket (jsconsole):*** *acessos à interface de administração via jsconsole, frequentemente mascarados com IPs comuns como* ***127.0.0.1****,* ***8.8.8.8*** *e* ***13.73.13.73****.*
- ***Solicitações HTTPS diretas****: comunicação maliciosa via portas padrão (ex.:* ***443*** *ou* ***80****), realizando chamadas diretas à API de administração.*

Além disso, os atacantes:

- *Realizam tentativas automatizadas de login com usuários gerados aleatoriamente (5 caracteres), sugerindo o uso de scripts de varredura e fuzzing.*
- *Criam e deletam contas PoC, como* ***watchTowr****, para testar acessos e confirmar a exploração bem-sucedida.*

Ações Pós-Explotação

Uma vez estabelecido o acesso privilegiado, o agente:

- *Baixa a configuração completa do firewall, incluindo políticas, rotas, chaves e VPNs.*
- *Modifica parâmetros do sistema por meio de sessões autenticadas (ex.: **via jsconsole** ou **https**), conforme evidenciado em logs forenses.*
- *Cria contas VPN locais com nomes semelhantes aos de usuários legítimos, adicionando-as ao grupo VPN para manter acesso furtivo e contínuo.*

Persistência Automatizada

Para garantir persistência, os operadores implementam tarefas automatizadas utilizando o recurso **system.automation-action.** Um exemplo recorrente envolve a recriação diária da conta forticloud-sync com perfil **super_admin** e senha predefinida. A automação é ativada por um **automation-trigger** agendado, configurado para executar um script CLI que recria a conta mesmo após sua exclusão.

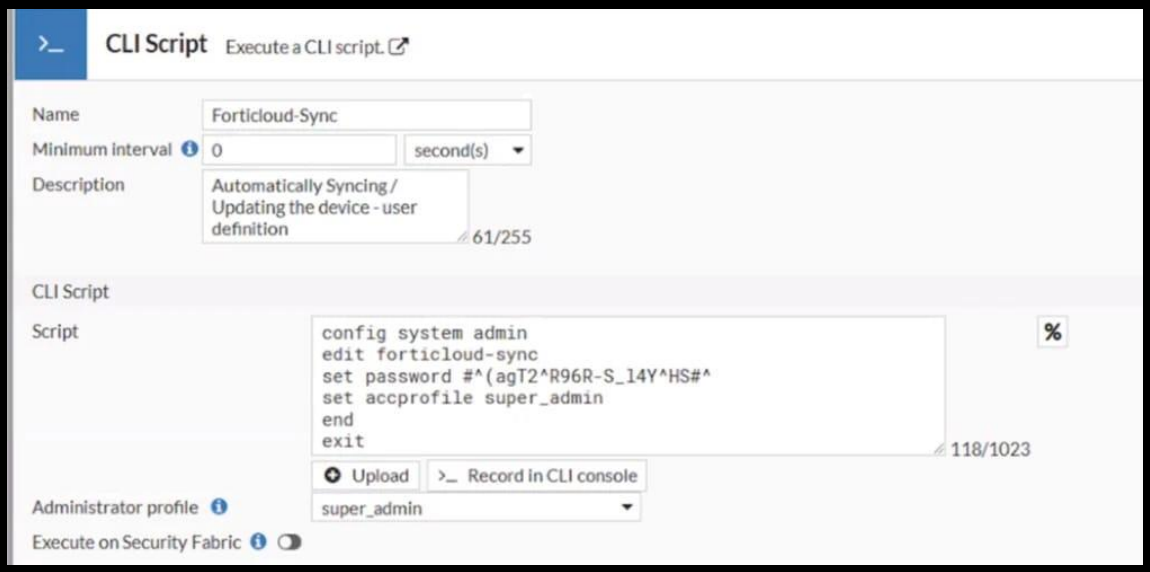


Figura 2 - Script CLI automatizado para manter a persistência - Fonte: Forescout Research

A exploração altamente automatizada e encadeada, combinada à manipulação dos mecanismos nativos de administração do FortiOS, evidencia uma campanha sofisticada com foco em persistência de longo prazo e evasão de detecção.

Esta fase pode envolver:

- ***T1190* – Exploit Public-Facing Application**
  Exploração de falhas críticas **(CVE-2024-55591 e CVE-2025-24472)** em interfaces expostas do Fortinet FortiOS. Os atacantes utilizaram exploits

públicos (PoC) para obter privilégios de *super_admin* por meio do **WebSocket (jsconsole) ou via HTTPS**, mesmo sem autenticação prévia.

- ***T1078* – *Valid Accounts***
  Uso de credenciais válidas obtidas via criação manual ou reaproveitamento de contas existentes. As contas eram nomeadas de forma a imitar nomes legítimos como **forticloud-tech**, **fortigate-firewall** ou **adnimistrator** (com erro proposital). Também foram criadas contas com nomes próximos a usuários reais acrescidos de dígitos.
- ***T1136.001* – *Create Account: Local Account***
  Criação de contas locais usando o comando **config system admin**, **script CLI** ou automação via **system.automation-action**. Essas contas tinham privilégios de administrador e eram usadas para manter acesso persistente ao sistema.
- ***T1098* – *Account Manipulation***
  Modificação de privilégios das contas recém-criadas, elevando-as ao perfil **super_admin** e adicionando-as a grupos de VPN ou administrativos.
  A manipulação era feita via comandos no CLI ou pela interface **jsconsole**.
- ***T1053.005* – *Scheduled Task/Job: Scheduled Task***
  Criação de tarefas agendadas de automação **(automation-trigger)** para recriar automaticamente a conta **forticloud-sync** com senha fixa e perfil **super_admin**, caso fosse deletada. O script CLI de persistência foi embutido em tarefas agendadas diariamente (ex: às 15h30) no FortiOS.
- ***T1562.001* – *Impair Defenses: Disable or Modify Tools***
  Modificação de configurações de segurança no FortiOS, como alteração de logs e políticas de acesso, visando ocultar a atividade maliciosa. O atacante manipulava atributos como **accprofile**, **logdesc**, e **permissões administrativas nos objetos do sistema**.
- ***T1210* – *Impair Defenses: Disable or Modify Tools***
  Modificação de configurações de segurança no FortiOS, como alteração de logs e políticas de acesso, visando ocultar a atividade maliciosa. O atacante manipulava atributos como **accprofile**, **logdesc**, e **permissões administrativas nos objetos do sistema**.
- ***T1562.001* – *Exploitation of Remote Services***
  Acesso a outros dispositivos Fortinet via **configuração HA (High Availability),** onde o invasor forçava a replicação das suas contas e scripts para outros firewalls do cluster.
  A sincronização HA foi usada para mover persistência entre múltiplos nós da rede.
- ***T1505.003* – *Server Software Component: Web Shell***
  Utilização indireta da interface **jsconsole** como vetor para comandos maliciosos, semelhante a um web shell improvisado. Através dessa interface, os invasores executavam comandos administrativos como se estivessem interagindo localmente via terminal.

- ***T1609* – *Container Administration Command***
  Uso da CLI administrativa (**config system admin, edit, set, end**) para manipulação da configuração interna, adicionar contas, alterar perfis e agendar tarefas no FortiOS. Essa CLI era acessada via interface remota.

Internal Recognition and Privilege Escalation

Após obter acesso inicial por meio da exploração das falhas **CVE-2024-55591** e **CVE-2025-24472** em firewalls Fortinet, o grupo **Mora_001** direciona suas ações para o mapeamento da rede interna e a escalada de privilégios. Essa fase demonstra não apenas a sofisticação técnica do grupo, mas também um profundo entendimento de topologias corporativas e falhas recorrentes em configurações de rede.

Mapeamento e Acesso Expandido

Os invasores utilizam as interfaces administrativas dos dispositivos FortiGate para:

- *Identificar ativos críticos, como controladores de domínio e servidores sensíveis.*
- *Criar contas VPN locais com nomes semelhantes aos de usuários legítimos, adicionando um caractere numérico ao final, como **usuario1**, para evitar detecção casual.*
- *Adicionar essas contas ao grupo "**VPN Users**", garantindo persistência via VPN mesmo após a descoberta dos pontos de entrada originais.*

As atividades são registradas em logs como:

{"itime": "xxx", "date": "2025-02-xx", "time": "18:04:01", "devid": "xxx", "vd": "root", "type": "event", "subtype": "system", "action": "Add", "cfgattr": "type[password]passwd[ENC]", "cfgobj": "xxx1", "cfgpath": "user.local", "cfgtid": "11075652", "devname": "xxxx", "eventtime": "xxx", "idseq": "xxxx", "level": "information", "logdesc": "Object attribute configured", "logid": "xxxx", "logver": "xxxx", "msg": "Add user.local xxx1", "tz": "-xxx", "ui": "GUI(89.248.192.55)", "user": "fortigate-firewall"}

{"itime": "xxx", "date": "2025-02-xx", "time": "xx:04:01", "devid": "xxxx", "vd": "root", "type": "event", "subtype": "system", "action": "Edit", "cfgattr": "member[xxx1]", "cfgobj": "VPN Users", "cfgpath": "user.group", "cfgtid": "xxx", "devname": "xxxx", "eventtime": "xxx", "idseq": "xxx", "level": "information", "logdesc": "Object attribute configured", "logid": "xxx", "logver": "xxx", "msg": "Edit user.group VPN Users", "tz": "-xx", "ui": "GUI(89.248.192.55)", "user": "fortigate-firewall"}

Além disso, as conexões VPN com endereços de IP russos foram registradas, indicando o uso da infraestrutura comprometida para comunicação remota com a rede interna.

tunnel-up Russia vpn XX1 event 89.248.192.55 89.248.192.55

tunnel-up Russia vpn XX1 event 89.248.192.55 10.1.1.1 89.248.192.55

PROPAGAÇÃO LATERAL

Em ambientes com **alta disponibilidade (HA),** o grupo explora a funcionalidade de sincronização de configuração entre dispositivos do cluster. Dessa forma, **contas de backdoor e tarefas de automação maliciosas são replicadas em múltiplos dispositivos**, ampliando o alcance do comprometimento:

```
Feb 27 xx:13:49 xxx CEF:0|Fortinet|FortiGate-101E|7.0.12,build0523 (GA)|xxx|system event Add|4|start=Feb 27 2025 xx:13:49 logver=xx deviceExternalId=xxx dvchost=xxxx vd=root eventtime=xxx tz=-xxx logid=xxx cat=event subtype=system deviceSeverity=information logdesc=Object attribute configured duser=forticloud-tech sproc=ha_daemon act=Add cfgtid=xxx cfgpath=system.automation-stitch cfgobj=Automatically Syncing cfgattr=description[Automatically Syncing / Updating the device]trigger[Forticloud-Sync] msg=Add system.automation-stitch Automatically Syncing tz="-xxx"
```

Em redes com autenticação centralizada via **TACACS+ ou RADIUS**, o grupo tenta autenticar suas contas VPN locais reutilizando credenciais sincronizadas com o **Active Directory** ou explorando segredos compartilhados do RADIUS. Quando bem-sucedido, esse acesso garante presença prolongada mesmo em casos de rotação de senhas locais.

```
network policy server denied access to a user. contact the network policy server administrator for more information. user: security id: s-1-0-0 account name: admin account domain: xxx fully qualified account name: xxx\admin client machine: security id: s-1-0-0 account name: - fully qualified account name: - called station identifier: xx.xxx.xx.xx calling station identifier: xxx.xxx.xxx.xxx nas: nas ipv4 address: xx.xxx.xxx.xx nas ipv6 address: - nas identifier: xxxxx nas port-type: virtual nas port: 5 radius client: client friendly name: xxx client ip address: xxx.xxx.xx.xx authentication details: connection request policy name: virtual private network (vpn) connections network policy name: - authentication provider: windows authentication server: xxx.xxx.xx@local authentication type: extension eap type: - account session identifier: xxxx logging results: accounting information was written to the local log file. reason code: 21
```

reason: an nps extension dynamic link library (dll) that is installed on the nps server rejected the connection request.

Acesso a Painéis de Administração

Para guiar sua movimentação lateral e expandir o reconhecimento interno, o ator acessa diversos painéis integrados da interface FortiGate:

- **Painel de Status**: *informações sobre desempenho do sistema e disponibilidade.*
- **Painel de Segurança**: *dados de vulnerabilidades, ameaças ativas e ativos comprometidos.*
- ***Painel de Rede**: topologia, rotas, sessões VPN e status de interfaces.*
- **Painel de Dispositivos e Usuários**: *sessões FortiClient, autenticações e dispositivos em quarentena.*
- **Painel WiFi:** *dados sobre redes sem fio, pontos de acesso e alertas relacionados.*

Essas interações são refletidas em logs como:

{"itime": "xx","date": "2025-02-xx","time": "xx:07:59","devid": "xxx","vd": "root","type": "event","subtype": "system","action": "Edit","cfgattr": "gui-dashboard:--------","cfgobj": "fortigate-firewall","cfgpath": "system.admin","cfgtid": "xxx","devname": "xxx","eventtime": "xxxx","idseq": "xxxx","level": "information","logdesc": "Object attribute configured","logid": "xxx","logver": "xxxx","msg": "Edit system.admin fortigate-firewall","tz": "-xx","ui": "GUI(80.66.88.90)","user": "fortigate-firewall"}

O uso coordenado de **painéis administrativos, criação furtiva de contas, abuso de infraestrutura de autenticação e replicação em clusters** revela um operador altamente experiente, com manual de operação bem definido e foco em persistência sigilosa e expansão interna rápida.

Esta fase pode envolver:

- ***T1550.002 – Use Alternate Authentication Material: Pass the Hash:*** Autenticação lateral sem necessidade da senha em texto claro, utilizando o hash NTLM de contas privilegiadas obtido previamente. Isso permite escalar privilégios e se mover lateralmente sem disparar alertas tradicionais.
- ***T1484.001 – Domain Policy Modification: Group Policy Modification:*** Alterações nas políticas de grupo (GPO) via scripts ou acesso administrativo local, utilizadas para manter persistência, como configurar

scripts de login ou ajustes no UAC (User Account Control) que facilitam execuções subsequentes.

- ***T1203 – Exploitation for Privilege Escalation:*** Exploração de vulnerabilidades locais **(CVE-2024-55591 e CVE-2025-24472)** em sistemas Fortinet com configuração incorreta ou software desatualizado, para elevar privilégios diretamente em firewalls e replicar as alterações via HA.

Lateral Movement and Ransomware Deployment

Na fase final da intrusão, o grupo Mora_001, intensifica sua presença na rede comprometida por meio de **movimentação lateral e execução controlada do processo de criptografia**. Essa etapa é marcada por ações furtivas, seleção estratégica de alvos e foco em maximizar o impacto da dupla extorsão.

Movimentação Lateral Silenciosa

Com acesso privilegiado já estabelecido (via VPN, credenciais comprometidas ou replicação de contas), os invasores priorizam:

- ***Servidores de arquivos, controladores de domínio, servidores de autenticação, bancos de dados e dispositivos de rede.***
- ***Ferramentas nativas do sistema operacional*** *para evitar detecção, como:*
  - ***WMIC (Windows Management Instrumentation Command-line):*** *para reconhecimento e execução remota de comandos em hosts Windows.*
  - ***SSH (Secure Shell):*** *para movimentação em servidores Linux e appliances de rede.*

As ações são apoiadas por dados coletados nos painéis administrativos dos FortiGates comprometidos, permitindo que os operadores mapeiem detalhadamente a topologia da rede e priorizem ativos sensíveis.

- ***Exfiltração de Dados e Desativação de Defesas***

Antes da execução do ransomware, os invasores realizam:

- ***Exfiltração de dados confidenciais*** *para infraestrutura controlada externamente, preparando o terreno para a segunda fase da extorsão.*
- ***Neutralização de mecanismos de defesa****, como:*
  - *Desativação ou exclusão de agentes EDR/AV.*
  - *Interrupção de serviços de backup.*

CRIPTOGRAFIA DIRECIONADA E ORQUESTRADA

Diferente de abordagens amplas e destrutivas, o SuperBlack adota uma estratégia de **criptografia seletiva e orquestrada**:

- *A **criptografia é disparada somente após a exfiltração**, alinhando-se à tática de dupla extorsão (T1486 + T1530).*
- *O **foco recai sobre servidores de arquivos críticos**, contendo documentos sensíveis e bases de dados operacionais, aumentando a pressão pelo pagamento sem comprometer serviços que poderiam alertar prematuramente a equipe de resposta.*

Essa abordagem híbrida de movimentação lateral furtiva, exfiltração estratégica e criptografia seletiva evidencia a maturidade técnica do grupo, que opera com foco em **impacto operacional e psicológico**, buscando dificultar a resposta das vítimas enquanto maximiza sua capacidade de extorsão.

Esta fase pode envolver:

- ***T1021.001* – Remote Services: Remote Desktop Protocol (RDP):**
  Uso do RDP para movimentação lateral entre sistemas comprometidos. Após garantir acesso administrativo, os invasores se conectam a outros hosts da rede usando RDP, aproveitando contas previamente criadas ou comprometidas. O tráfego de RDP é liberado em firewalls e as conexões são automatizadas via scripts.
- ***T1021.002* – Remote Services: SMB/Windows Admin Shares:**
  Movimentação lateral por meio de compartilhamentos administrativos (C$, ADMIN$). Utilização de credenciais privilegiadas para copiar binários maliciosos por meio do protocolo SMB, preparando a execução remota em hosts remotos.
- ***T1053.005* – Scheduled Task/Job: Scheduled Task:**
  Implantação do ransomware usando tarefas agendadas do Windows. Criação de tarefas com schtasks.exe para executar o binário do ransomware em horários específicos, sincronizando a criptografia em múltiplos sistemas.
- ***T1562.001* – Impair Defenses: Disable or Modify Tools:**
  Desativação de soluções de segurança e backup. Ferramentas como sc, taskkill ou PowerShell são usadas para encerrar processos de antivírus (AV), EDRs e agentes de backup, assegurando que a criptografia ocorra sem interferência.
- ***T1486* – Data Encrypted for Impact:**
  Execução do ransomware SuperBlack para criptografar arquivos. O binário é executado localmente ou remotamente após a exfiltração de dados. A criptografia é seletiva: prioriza servidores de arquivos com dados

confidenciais, maximizando impacto e dificultando recuperação sem pagamento.

- ***T1047* – *Windows Management Instrumentation (WMI):***
  Execução remota via WMI para comando e controle interno.
  Com wmic ou PowerShell, os atacantes executam comandos remotamente em sistemas conectados, incluindo execução do ransomware ou scripts auxiliares.
- ***T1041* – *Exfiltration Over C2 Channel:***
  Exfiltração de dados sensíveis antes da criptografia.
  Utilização de scripts automatizados para enviar dados críticos a servidores externos via HTTP, FTP ou canais criptografados, visando extorsão dupla.
- ***T1560* – *Archive Collected Data:***
  Compressão de arquivos exfiltrados com ferramentas como WinRAR ou 7-Zip. Dados coletados são compactados e protegidos com senha antes do envio externo, otimizando volume e dificultando a detecção.
- ***T1112* – *Modify Registry:***
  Modificações no registro do Windows para persistência e evasão.
  Exemplos incluem ativar RDP, permitir senhas em branco, ou modificar configurações de UAC, garantindo acesso contínuo e menor visibilidade.

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	Utilização de credenciais legítimas, frequentemente obtidas de dumps ou extraídas de servidores comprometidos.
	T1190 – Exploit Public-Facing Application	Exploração de vulnerabilidades conhecidas em dispositivos Fortinet (ex: CVE-2023-27997) para acesso inicial à rede.
Execution	T1059.001 – Command and Scripting Interpreter: PowerShell	Execução de payloads por scripts PowerShell com **-EncodedCommand** e **-ExecutionPolicy** Bypass.
	T1053.005 – Scheduled Task	Utilização de tarefas agendadas do Windows para ativar o ransomware em momentos estratégicos.
Persistence	T1136.001 – Create Account: Local Account	Criação de contas locais maliciosas, adicionadas aos grupos “Administrators” e “Remote Desktop Users”.
Privilege Escalation	T1547.001 – Registry Run Keys / Startup Folder	Registro de chaves de inicialização para persistência pós-reboot.
	T1068 – Exploitation for Privilege Escalation	Exploração de configurações incorretas ou permissões excessivas para obter privilégios de administrador.
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.

Discovery	T1602.002 – Network Information Discovery: Domain Trust Discovery	Identificação de relações de confiança entre domínios via ferramentas nativas e FortiGate GUI.
Lateral Movement	T1021.001 – Remote Desktop Protocol	Movimento lateral utilizando RDP, com contas válidas e configurações alteradas no registro.
	T1021.004 – SSH	Uso de SSH para acesso lateral em dispositivos de rede e servidores Linux.
	T1028 – Windows Remote Management (WinRM)	Execução remota em sistemas Windows via WinRM (em ambientes habilitados).
Command & Control	T1071.001 – Application Layer Protocol: Web Protocols	Comunicação com C2 via HTTPS para download de payloads ou comandos.
Exfiltration	T1041 – Exfiltration Over C2 Channel	Extração de dados sensíveis antes da criptografia final, visando dupla extorsão.
Impact	T1486 – Data Encrypted for Impact	Criptografia seletiva de servidores com dados críticos para maximizar impacto.
	T1490 – Inhibit System Recovery	Deleção de shadow copies e interrupção de serviços de backup.
	T1489 – Service Stop	Interrupção de processos de proteção como antivírus, EDR, backup e banco de dados.

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.

Vulnerability	Product	Type
CVE-2018-13379	Fortinet FortiOS	Path Traversal /Credential Disclosure
CVE-2019-5591	Fortinet FortiOS	Information Disclosure (Hardcoded Certificate)
CVE-2020-12812	Fortinet FortiOS	Improper Authentication
CVE-2022-40684	Fortinet FortiOS / FortiProxy	Authentication Bypass via HTTP Requests
CVE-2023-27997	Fortinet FortiGate SSL VPN	Remote Code Execution (RCE) via Heap Overflow
CVE-2024-21762	Fortinet FortiOS	Heap-Based Buffer Overflow (RCE)
CVE-2021-34473	Microsoft Exchange Server	Remote Code Execution
CVE-2021-34523	Microsoft Exchange Server	Elevation of Privilege
CVE-2021-31207	Microsoft Exchange Server	Security Feature Bypass
CVE-2020-1472	Microsoft Netlogon	Elevation of Privilege (Zerologon)
CVE-2021-43890	Windows App Installer	Spoofing Vulnerability

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 **SuperBlack**. A seguir, são listadas recomendações que fortalecem a postura defensiva das organizações frente a esse tipo de ameaça:

MANTENHA SISTEMAS E SOFTWARES ATUALIZADOS

- Garanta a aplicação contínua de patches de segurança em sistemas operacionais, dispositivos de rede (como firewalls e VPNs) e softwares corporativos.
- Dê atenção especial a produtos Fortinet e Microsoft Exchange Server, frequentemente explorados pelo SuperBlack.

Implemente autenticação forte e segregação de privilégios

- Ative autenticação multifator (MFA) para todos os acessos remotos e privilegiados.
- Limite o uso de contas com privilégios administrativos e monitore alterações em grupos como Administrators e Remote Desktop Users.

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, 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:	5c082bc67a61c822877dab10226044c8
sha1:	c5105a6247dca72a66c0db16d7d88c723acdde12
sha256:	c994b132b2a264b8cf1d47b2f432fe6bda631b994ec7dcddf5650113f4a5a404
File name:	RjqUGZi0a.README.txt

Indicadores do artefato	
md5:	4bcc3589bbbbaa013bebf38d28d442ac
sha1:	a418e1e8ee0195e662d103a7a779aa91ae2ab368
sha256:	f383bca7e763b9a76e64489f1e2e54c44e1fd24094e9f3a28d4b45b5ec88b513
File name:	ni8pxbvnx.README.txt

Indicadores do artefato	
md5:	7f4bc62e2a6457b94509ae8f4a91d4b9
sha1:	25695d47ae4052b2922ac63fa26c932c66b861be
sha256:	813ad8caa4dcbd814c1ee9ea28040d74338e79e76beae92bedc8a47b402dedc2
File name:	813ad8caa4dcbd814c1ee9ea28040d74338e79e76beae92bedc8a47b402dedc2.unknown

Indicadores do artefato	
md5:	046b64c08f66f1820ae4ce5dd170e761
sha1:	f43fe4d81c29abafb8b34d4cacf3ac9930fd9694
sha256:	782c3c463809cd818dadad736f076c36cdea01d8c4efed094d78661ba0a57045
File name:	fB1SZ2i3X.README.txt

Indicadores do artefato	
md5:	e09dd7cca0c6c147ba21b4062e723c5b
sha1:	ff6333bdda824e4c13bcd13351bd4bb14aaeab11
sha256:	d9938ac4346d03a07f8ce8b57436e75ba5e936372b9bfd0386f18f6d56902c88
File name:	d9938ac4346d03a07f8ce8b57436e75ba5e936372b9bfd0386f18f6d56902c88.exe 2024-10-06_e09dd7cca0c6c147ba21b4062e723c5b_darkside

Indicadores do artefato	
md5:	294e9f64cb1642dd89229fff0592856b
sha1:	97b148c27f3da29ba7b18d6aee8a0db9102f47c9
sha256:	917e115cc403e29b4388e0d175cbfac3e7e40ca1742299fbdb353847db2de7c2
File name:	D44B.tmp, D7A3.tmp, 4692.tmp, d8d.tmp, 52ab.tmp, adf2.tmp, 5673.tmp, 3052.tmp, A7B3.tmp, 6180.tmp, 36B8.tmp, 926F.tmp, A5C0.tmp, DEE9.tmp, 494a.tmp, 6fb9.tmp, D929.tmp, CD91.tmp, FB1A.tmp, 2BE0.tmp, 363F.tmp, 81EB.tmp, 470D.tmp, 6EF7.tmp, 642E.tmp, B940.tmp, EBD7.tmp, A811.tmp, EF8C.tmp, C15B.tmp, 7B02.tmp, 6CC9.tmp, F745.tmp, 6A78.tmp, DCD3.tmp, 5697.tmp, 4B13.tmp, 1381.tmp, 1250.tmp, 4089.tmp, edad.tmp, 8ebb.tmp, 6382.tmp, fd2c.tmp, 69BC.tmp, 2ED6.tmp, 7FC5.tmp, 7277.tmp, 3449.tmp, E80A.tmp, 584D.tmp, CF67.tmp, e85e.tmp, 42BC.tmp, 7891.tmp, 4A29.tmp, E8B8.tmp, a4d0.tmp, C196.tmp, 4E64.tmp, 891D.tmp, 6930.tmp, 551B.tmp, 94E2.tmp, A896.tmp, ACCB.tmp, B816.tmp, 23D9.tmp, 5CAC.tmp, 83da.tmp, 2D56.tmp, 76C9.tmp, 2B3B.tmp, 5489.tmp, 3399.tmp, 8003.tmp, 7DF5.tmp, 4E35.tmp, 1121.tmp, D030.tmp, 35DB.tmp, D51B.tmp, 47CD.tmp, 5961.tmp, 46E8.tmp, BAA1.tmp, C957.tmp, D514.tmp, 6874.tmp, 696E.tmp, 9a35.tmp, EF0.tmp, 2CD9.tmp, 5B84.tmp, 8DFD.tmp, 42C9.tmp, 1E23.tmp, D88.tmp, 6A75.tmp, 4D92.tmp

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