TLP: CLEAR

Pesquisa de Cibersegurança
Cyber Threats Actors

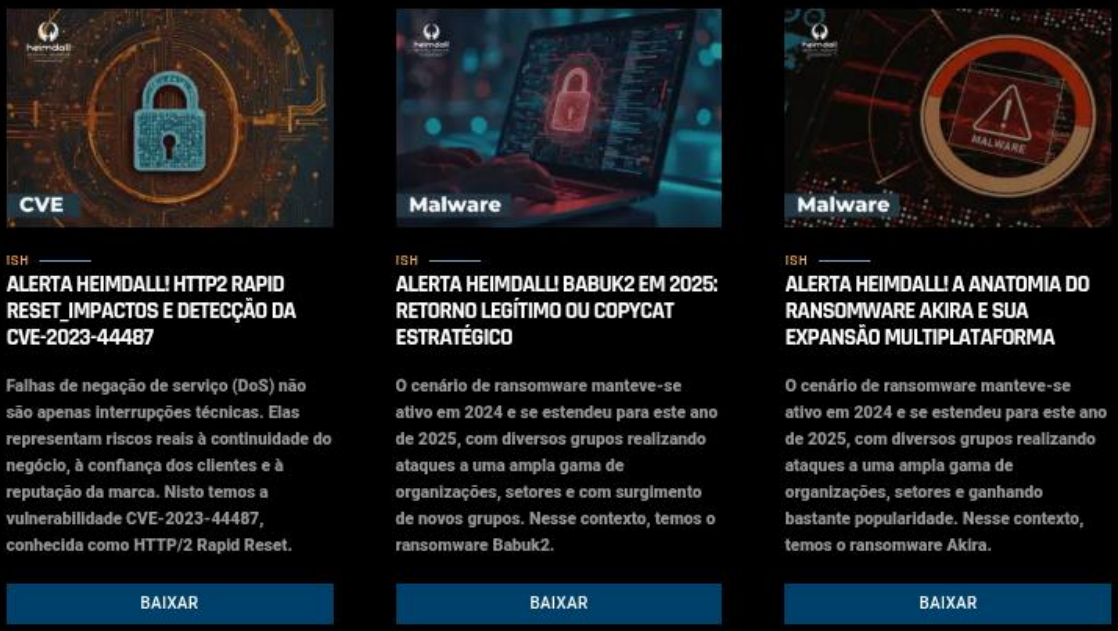
Bloqueando a Restauração:
O Papel dos Backups na Pressão do Ransomware

heimdall
security research

Acesse nossa comunidade no WhatsApp, clicando na imagem abaixo!

heimdall
security research
A DIVISION OF ISH

Acesse a inteligência que produzimos sobre as Táticas, Técnicas e Procedimentos de determinados *Threat Actors*, análises de *malwares* emergentes no cenário de cibersegurança, análises de vulnerabilidades críticas e outras informações no *blog* da ISH Tecnologia, clicando na imagem abaixo.



SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

SUMÁRIO EXECUTIVO: O BACKUP COMO NOVO ALVO ESTRATÉGICO NA GUERRA DO RANSOMWARE

Nos últimos anos, o cenário de ameaças cibernéticas passou por uma transformação profunda. Os ataques de ***Ransomware***, antes vistos como eventos isolados e focados apenas na criptografia de dados, evoluíram para campanhas persistentes, direcionadas e altamente lucrativas. Hoje, os alvos são escolhidos com precisão, explorando vulnerabilidades críticas para maximizar impacto e retorno financeiro. Nesse novo contexto, os *backups* deixaram de ser apenas um recurso de recuperação para se tornarem um alvo estratégico e, muitas vezes, o primeiro a ser comprometido.

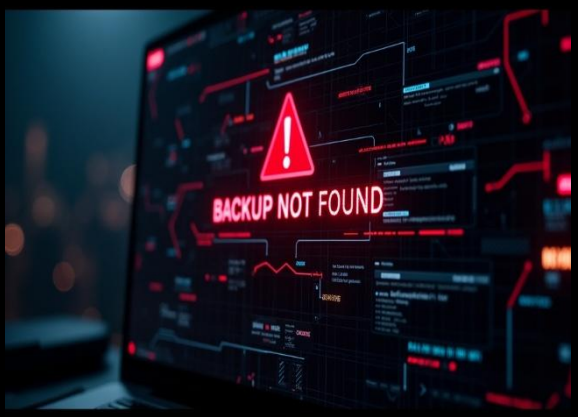


Figura 1 - Backup Corrompido

Proteger *backups* não é mais apenas uma boa prática: é uma linha de defesa vital que pode determinar se uma organização sobrevive ou não a um ataque. Os grupos de ***Ransomware*** entenderam que, ao inviabilizar a restauração, ampliam a pressão para o pagamento e prolongam a interrupção das operações, aumentando drasticamente seus ganhos.

A virada de chave está no modelo de ataques *human-operated*. Diferente das primeiras variantes automatizadas, os operadores modernos atuam de forma meticulosa: podem passar semanas ou até meses infiltrados na rede, roubando credenciais, mapeando a infraestrutura, escalando privilégios e movimentando-se lateralmente, até o momento em que o *payload* de ***Ransomware*** é finalmente disparado. Essa postura estratégica, semelhante à de adversários estatais, coloca os *backups* no centro da guerra.

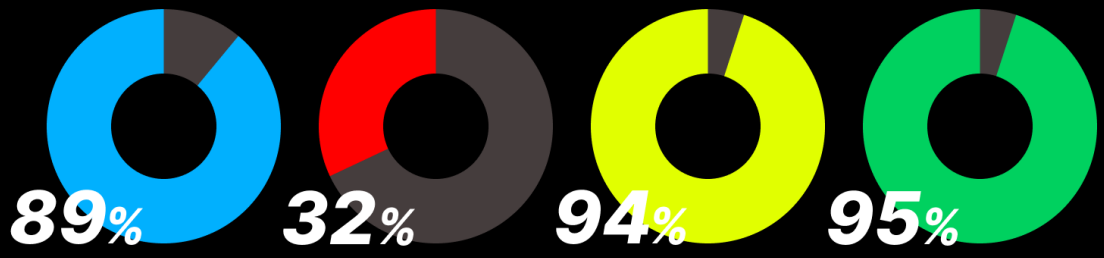
INTELIGÊNCIA ESTRATÉGICA: CONHECENDO OS IMPACTOS

Em **2024**, as campanhas de ***Ransomware*** migraram de ações pontuais para operações contínuas, conduzidas como verdadeiras campanhas militares digitais. O objetivo vai além da criptografia de dados primários: é enfraquecer a infraestrutura de recuperação e tornar a retomada quase impossível sem concessões. Neutralizar os *backups* se tornou a forma mais eficaz de maximizar impacto, pressionar pelo pagamento e estender a interrupção das operações.

Os números são claros:

- **Alvo primário**: Em 2024, segundo relatórios públicos, **94% das organizações atingidas** relataram tentativas de comprometimento de backups, chegando a **99% em setores governamentais e de mídia/entretenimento**.
- **Alta taxa de sucesso** – De forma geral, **57% dessas tentativas funcionaram**, atingindo **79% no setor de energia** e **71% em educação**.
- **Impacto financeiro multiplicado** – Quando backups são comprometidos, a chance de pagamento **quase dobra (67% vs 36%),** o valor mediano de resgate **mais que dobra (US$ 1M vs US$ 2,3M)** e os custos de recuperação podem ser **oito vezes maiores**.

O caso da subsidiária da ***UnitedHealth Group*** foi emblemático: **US$ 872 milhões** de impacto apenas no primeiro trimestre de 2024, somando custos diretos de resposta e perda de produtividade. Outras organizações, em diferentes setores e regiões, também enfrentaram prejuízos expressivos em função da perda ou comprometimento de seus backups, e as estatísticas deixam claro que essa não é uma exceção, mas sim uma tendência consolidada.



89% das empresas que foram atacadas por grupos de *Ransomware* tiveram seus *Backups* como alvo primário.

apenas **32%** das empresas que foram atacadas, usavam repositórios ou serviços com alguma configuração de imutabilidade.

94% das empresas tendem a aumentar seu orçamento de **Recovery** após um ataque de Ransomware.

95% das empresas tendem aumentar seu orçamento de **Prevention** após um ataque de Ransomware.

Os criminosos não miram os *backups* por acaso. Para eles, esses sistemas representam:

- **Última linha de defesa** – Sem cópias viáveis, a vítima perde sua rota de fuga.
- **Pressão máxima** – Sem recuperação, cresce a probabilidade e o valor do pagamento.
- **Dados completos** – *Backups* concentram registros críticos, tornando-se ideais para exfiltração e extorsão dupla.
- **Vulnerabilidade estrutural** – Historicamente, empresas protegem menos seus backups que seus sistemas de produção.
- **Disrupção garantida** – Um *backup* comprometido paralisa a continuidade de negócios de forma imediata.

Para atingir esses objetivos, os operadores de ***Ransomware*** aplicam uma combinação de técnicas que vão muito além da criptografia:

- **Neutralização de agentes e snapshots**, inviabilizando pontos de recuperação.
- **Criptografia direta de volumes de backup**, seja em **NAS**, dispositivos externos ou na nuvem.
- **Comprometimento de credenciais administrativas**, obtendo controle total sobre repositórios.
- **Exploração de vulnerabilidades em softwares de backup**, permitindo adulteração ou exclusão.
- **Movimento lateral** até a infraestrutura de *backup*, muitas vezes via ***Active Directory*** ou *hosts* virtuais.
- **Exfiltração de dados de backup**, ampliando o poder de extorsão e o risco de vazamento.

Apesar da ameaça evidente, muitas empresas ainda cometem erros básicos que abrem caminho para o sucesso dos atacantes:

- **manter backups na mesma rede que os dados primários.**
- **não realizar testes regulares de restauração**.
- **negligenciar controles de acesso**.
- **ignorar práticas como imutabilidade e criptografia**.
- **restaurar diretamente em produção sem validação de integridade**.

Essas falhas não apenas ampliam o risco de perda definitiva e interrupção prolongada, como expõem a organização a **sanções regulatórias (LGPD, GDPR)** e a danos duradouros à reputação e à confiança do mercado.

INTELIGÊNCIA TÁTICA: COMPREENDENDO O ATAQUE

Como acontece na prática

A seguir, acompanhamos uma *Kill Chain* simulada, construída a partir de padrões recorrentes em relatórios de resposta a incidentes. O fluxo mostra como os atacantes, após comprometer um ponto inicial, avançam internamente até neutralizar os mecanismos de backup. Só então executam as etapas de criptografia em larga escala, exfiltração e impacto final, garantindo que a vítima tenha suas opções de recuperação severamente limitadas.

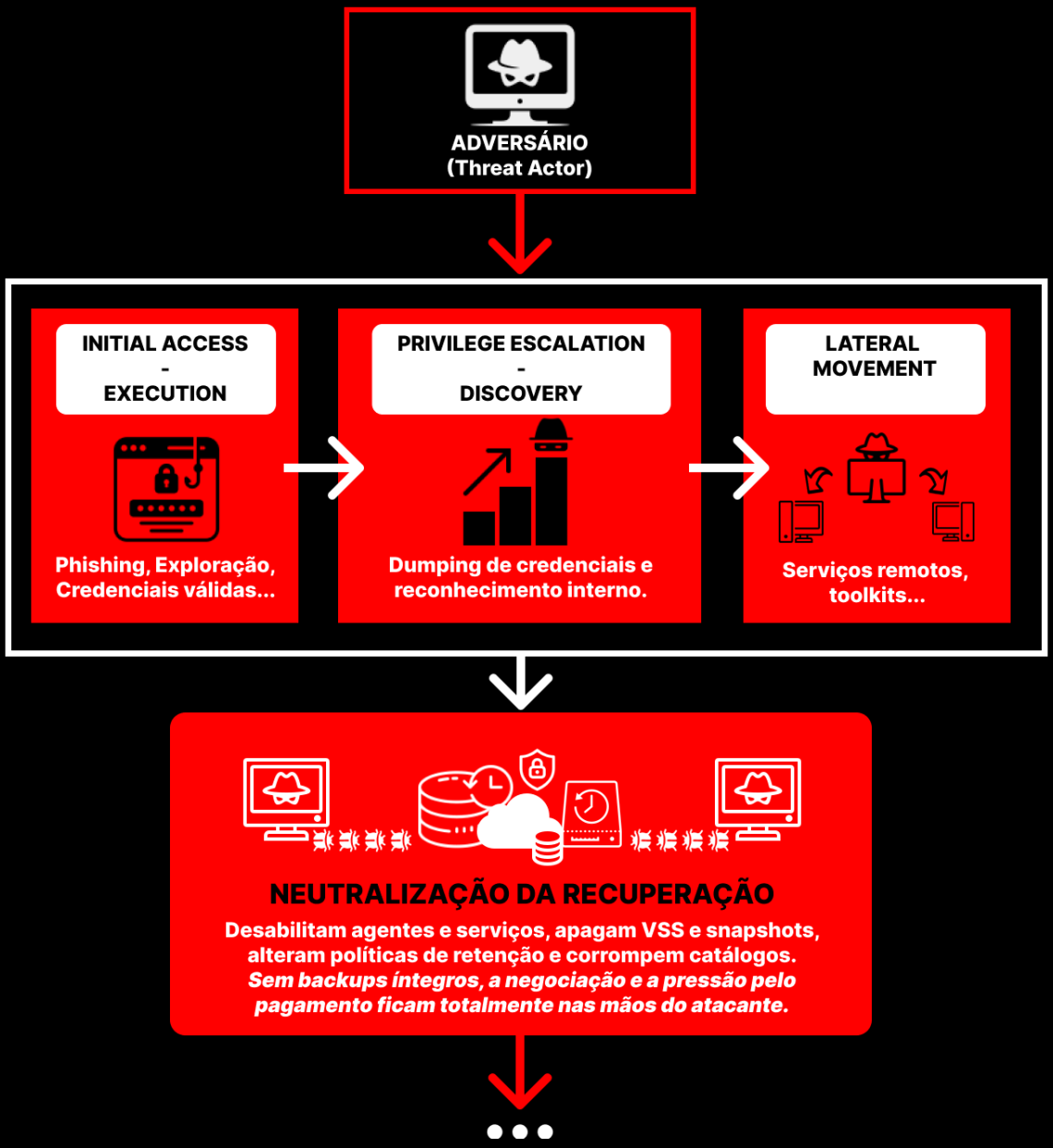


Figura 2 - Kill Chain simulada

Initial Access & Execution:

Os atores entram via *phishing* (**T1566**), exploração de serviços expostos (**T1190**) ou uso de credenciais válidas (**T1078**). A execução é realizada com **PowerShell/CLI** (**T1059**) e a persistência é mantida de forma discreta (**T1547**), minimizando alertas.

Privilege Escalation & Discovery:

Com *dumping* de credenciais (**T1003**) e reconhecimento interno (**T1087**, **T1018**, **T1046**), os atacantes localizam *consoles*, servidores e repositórios de *backup* (**NAS**, **VMs/hipervisores**, *storage* em nuvem).

Lateral Movement & Preparation:

Usam serviços remotos (**T1021**) e transferência de ferramentas (**T1570**). Buscam segredos de *backup* (**T1552**, **T1555**) e contas de serviço com privilégios ampliados.

Neutralização da Recuperação:

Desabilitam agentes/serviços (**T1489**), apagam VSS/snapshots (**T1490**), alteram políticas de retenção (**T1562**) e corrompem catálogos. *Backups* em nuvem são alvo de chaves, *tokens* e operações destrutivas em massa.

Impact & Actions on Objectives:

Criptografam dados (**T1486**) e/ou exfiltram informações (**T1041/T1567**), muitas vezes antes da criptografia.]

A etapa de ataque contra os backups não é apenas uma "tática auxiliar", ela é **o divisor de águas entre uma vítima que consegue se recuperar e outra que fica refém**. Neutralizar a recuperação é o que transforma um incidente grave em uma crise de continuidade. Por isso, proteger e monitorar constantemente ambientes de backup deve ser tratado como prioridade estratégica, não apenas técnica, dentro dos programas de defesa.

MITRE ATT&CK

Abaixo, tabela MITRE ATT&CK contendo a Kill Chain simulada que foi discutida no tópico anterior.

TÁTICA	TÉCNICA	ID	OBSERVAÇÃO
Initial Access	Phishing	**T1566**	Emails direcionados, spear-phishing
	Exploit Public-Facing App	**T1190**	Exploração de serviços expostos
	Valid Accounts	**T1078**	Uso de credenciais legítimas
Execution	Command & Scripting Interpreter	**T1059**	PowerShell, CLI
	Scheduled Task / Job	**T1053**	Execução programada discreta
Persistence	Boot/Logon Autostart	**T1547**	Run Keys, Startup
	Create Account	**T1136**	Contas de serviço temporárias
Privilege Escalation	OS Credential Dumping	**T1003**	Extração de credenciais
Discovery	Account Discovery	**T1087**	Localiza contas privilegiadas
	Remote System Discovery	**T1018**	Identifica servidores de backup
	Network Service Scanning	**T1046**	Varredura de hosts e serviços
Lateral Movement	Remote Services	**T1021**	RDP, SMB, PsExec
	Lateral Tool Transfer	**T1570**	Ferramentas de backup e scripts
Defense Evasion	Impair Defenses	**T1562**	Desabilita agentes/serviços
	Inhibit System Recovery	**T1490**	Apaga snapshots, VSS, corrompe catálogos
Exfiltration	Exfiltration Over C2	**T1041**	Dados críticos exfiltrados
	Exfiltration Over Web Services	**T1567**	Transferência via cloud
Impact	Data Encrypted for Impact	**T1486**	Criptografia de dados primários
	Service Stop	**T1489**	Interrompe serviços de backup

Tabela 1- Táticas e Técnicas MITRE ATT&CK

Inteligência Operacional: Compreendendo o Comportamento dos Adversários

Os padrões observados em múltiplas campanhas recentes confirmam que os operadores seguem uma cadência repetitiva: primeiro eliminam pontos de recuperação (snapshots e cópias sombra), depois atacam serviços de backup, em seguida se movem lateralmente até repositórios críticos e, por fim, realizam compressão e exfiltração massiva.

Ferramentas e Comandos Observados

Técnica MITRE	Ferramentas/Comandos Observados	Observação Prática
T1059 – PowerShell/CLI	- vssadmin delete shadows /all /quiet - wmic shadowcopy delete	Apagar snapshots para inviabilizar restauração rápida.
T1490 – Inhibit System Recovery	Uso do **diskshadow.exe** para manipular cópias de *backup*.	Muito comum em ataques **LockBit** e **BlackCat**.
T1078 – Valid Accounts	Uso de **RDP** com credenciais válidas extraídas do **LSASS**.	Movimentação lateral até servidores de backup.
T1021 – Remote Services	- psexec.exe \\host -u admin -p senha cmd.exe	Execução remota de binários de *ransomware*.
T1562 – Impair Defenses	- net stop "BackupExecAgentAccelerator" - sc stop VeeamBackupSvc	Desabilitação de serviços e agentes de *backup*.
T1570 – Lateral Tool Transfer	- rclone.exe copy - winrar.exe a -hpSenha backup.7z	Exfiltração e movimentação de dados antes da criptografia.
T1041/T1567 – Exfiltração	Conexões **HTTPS** persistentes para **Mega**, **Dropbox**, **Google Drive**, **pCloud**.	Normalmente camuflados em tráfego legítimo de cloud.

Tabela 2 - Ferramentas e Comandos Observados

Observações Operacionais Importantes

1. **Uso de binários nativos do Windows (*Living off the Land*)**
    - Ferramentas como ***vssadmin.exe***, ***wmic.exe*** e ***diskshadow.exe*** aparecem constantemente, pois permitem aos atacantes remover cópias de segurança sem disparar necessariamente alertas de antivírus. Esse comportamento ilustra o padrão ***LOLBins*** (*Living Off the Land Binaries*), onde os adversários usam recursos legítimos do sistema operacional contra a própria defesa.
2. **Neutralização seletiva de serviços de backup**
    - Atacantes identificam os agentes mais comuns em uso, como **Veeam**, **Veritas**, **Commvault** ou mesmo agentes de *backup* nativos em *appliances*, e os desabilitam com comandos simples de ***net stop*** ou ***sc stop***. Essa prática está diretamente alinhada com **T1562** (*Impair Defenses*) e garante que mesmo cópias em andamento sejam corrompidas.
3. **Movimentação lateral até servidores de backup**
    - Com credenciais válidas obtidas via *dumping* de **LSASS** (**T1003**) ou extraídas de cofres mal configurados, os grupos usam **RDP** e ferramentas como **PsExec** para alcançar *hosts* críticos de *backup*. Isso não apenas amplia o raio de impacto, mas também permite que os atacantes implantem *payloads* de ***ransomware*** diretamente nas máquinas que deveriam proteger a continuidade.
4. **Exfiltração camuflada em tráfego legítimo**
    - Ferramentas como ***rclone*** ou mesmo clientes nativos de sincronização são configurados para enviar dados para provedores de nuvem populares (Google Drive, Mega, Dropbox, pCloud). O tráfego **TLS** legítimo dificulta a inspeção por parte de **IDS/IPS** tradicionais, criando um canal discreto de saída de dados (**T1041**, **T1567**).
5. **Compressão com senha antes da exfiltração**
    - Comandos como ***winrar.exe a -hpSenha backup.7z*** ou ***7z a -pSenha backup.7z*** são usados para agrupar grandes volumes em um único pacote protegido. Isso dificulta tanto a detecção de conteúdo sensível durante a exfiltração quanto a análise posterior de incidentes, atrasando o trabalho de resposta.

Exemplos Reais de Observação em Campo

LockBit 3.0 – costuma executar lotes com vssadmin delete shadows /all /quiet e wbadmin DELETE SYSTEMSTATEBACKUP, removendo sistematicamente pontos de restauração antes da ativação do *payload*.

BlackCat (ALPHV) – abusa de contas de serviço ligadas ao **Veeam** *Backup* & *Replication*, explorando permissões privilegiadas para manipular e excluir repositórios de *backup* em nuvem.

Akira – em ambientes **VMware**, já foi observado uso de esxcli vm process kill combinado com deleção de snapshots em ESXi, interrompendo operações de continuidade e impedindo *failover*.

CL0P – frequentemente vincula a etapa de exfiltração ao uso de ***zero-days*** em aplicações de transferência (ex. **MOVEit**). Ao acessar fluxos de replicação, direciona a movimentação de dados também para repositórios de *backup*, garantindo cópia integral antes da destruição.

Play Ransomware – além de desabilitar serviços de *backup*, já foi observado criando tarefas agendadas para remoção periódica de *snapshots*, assegurando que qualquer tentativa de restauração futura falhe.

Na esfera operacional, o que vemos é que os atacantes **não reinventam a roda**: eles exploram ferramentas já existentes, credenciais válidas e serviços expostos, construindo um ciclo destrutivo simples mas altamente eficaz. A neutralização dos backups aparece sempre como **passo obrigatório** para garantir que a negociação se torne inevitável.

MITIGAÇÕES CONTRA COMPROMETIMENTO DE BACKUPS

O foco principal das mitigações é reduzir o risco de comprometimento de *backups* por ***ransomware***, proteger a integridade dos dados e garantir a continuidade dos negócios. As medidas abaixo são recomendadas para organizações que buscam resiliência contra ataques direcionados a *backups* e exfiltração de dados.

Prevenção

1. **Arquitetura de Backup Resiliente**
   - **3-2-1-1-0**: três cópias dos dados, dois tipos de mídia, uma *offsite*, uma imutável, zero erros de *backup*.
   - **Backups baseados em imagem**: captura completa de sistemas, aplicativos e configurações.
   - **Air-gapping ou isolamento lógico/físico**: reduz a exposição a ***ransomware***.
   - **Repositórios imutáveis**: Veeam Hardened Repository, S3 Object Lock, Azure Immutable Blob...
2. **Controle de Acesso**
   - **Princípio do menor privilégio** para todas as contas de *backup*.
   - **MFA** obrigatório em consoles de *backup*, VPNs e plataformas de nuvem.
   - Rotação periódica de credenciais, especialmente para contas administrativas e de serviço.
3. **Segurança de Sistemas**
   - ***Patching*** regular de sistemas, *appliances* e software de *backup*.
   - Desabilitar serviços e portas desnecessárias nos servidores de *backup*.
   - Segregar rede de *backup* e aplicar ***ACLs/firewalls*** para restringir acesso.
4. **Proteção de Credenciais e Segredos**
   - Cofres *offline* ou **HSMs** para armazenamento de chaves de criptografia.
   - Auditoria e monitoramento do uso de credenciais de serviço.

Detecção

1. **Monitoramento Contínuo**
    - Logs de atividades de *backup* e agentes (**Veeam**, **Veritas**, **Commvault**).
    - Monitoramento de alterações em *snapshots*, **VSS**, volumes de *backup* e políticas de retenção.
    - Detecção de uso de binários nativos (***LOLBins***) e execução de comandos suspeitos:

      ```
      Get-EventLog -LogName System | Where-Object {$_.Message -like "*vssadmin*"}
      ```

    - Monitoramento de transferência de arquivos para destinos externos via ***Rclone***, ***WinSCP*** ou clientes *cloud*.
2. **Análise de Comportamento**
    - ***EDR/EDR-Lite*** para detectar scripts e tarefas agendadas suspeitas.
    - Anomalias de tráfego de saída (exfiltração camuflada).
    - Escaneamento de backups pós-criação para identificar malware latente.
3. **Integração com Threat Intelligence**
    - ***IoCs*** de grupos de *ransomware* conhecidos.
    - Alertas de ***CERTs*** e feeds de ameaças focados em exfiltração e comprometimento de backups.

Resposta

1. **Plano de Resposta a Incidentes**
    - Procedimentos claros para isolamento de sistemas afetados.
    - Escalonamento imediato para equipes de TI, SOC e gestão.
    - Registro detalhado de logs de acesso e eventos para forense.
2. **Validação de Backups**
    - Testes regulares de restauração para todos os tipos de *backup*.
    - Restaurar inicialmente em ambientes isolados ***(“cleanroom”)*** para verificação de integridade.
    - Uso de *snapshots offline* e réplicas ***air-gapped*** para recuperação rápida.

3. **Recuperação e Reconstituição**
    - Limpeza de hosts comprometidos antes de restauração em produção.
    - Revalidação de permissões, **ACLs** e regras de *firewall*.
    - Testes pós-restauração de *malware* e vulnerabilidades.

CONCLUSÃO

O avanço dos ataques de *ransomware* exige uma postura de **"assume compromise"**, assumindo que, em algum momento, atores maliciosos poderão penetrar na rede. Dessa forma, proteger e validar *backups* não é apenas uma tarefa operacional, mas um compromisso estratégico com a continuidade e a segurança da organização. Equipes que integram inteligência estratégica, tática e operacional, apoiadas por mitigação prática e testes frequentes, conseguem reduzir drasticamente o risco de perda de dados, exfiltração de informações e impacto financeiro.

Em última análise, os backups não são apenas uma cópia dos dados: são a **última linha de defesa**, a principal ferramenta de recuperação e o elemento que pode decidir se a organização sobrevive ou sucumbe a ataques sofisticados de *ransomware*.

REFERÊNCIAS

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

AUTORES

- **Gustavo Santos – Security Researcher**

heimdall
security research
A DIVISION OF ISH