



RELATÓRIO DE PESQUISAS

**Kerberoasting em Ambientes Windows: Mecanismos de
Ataque e Estratégias de Defesa**



heimdall
security research




Acesse a nossa nova comunidade através do WhatsApp!

Heimdall Security Research



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

Boletins de Segurança – Heimdall

 <p>Malware</p>	 <p>Malware</p>	 <p>Ransomware</p>
<p>ISH</p> <p>CONTAS DO FACEBOOK SÃO INVADIDAS POR EXTENSÕES MALICIOSAS DE NAVEGADORES</p> <p>Descoberto recentemente que atores maliciosos utilizam extensões de navegadores para realizar o roubo de cookies de sessões de sites como o Facebook. A extensão maliciosa é oferecida como um anexo do ChatGPT...</p> <p>BAIXAR</p>	<p>ISH</p> <p>ALERTA PARA RETORNO DO MALWARE EMOTET!</p> <p>O malware Emotet após permanecer alguns meses sem operações retornou com outro meio de propagação, via OneNote e também dos métodos já conhecidos via Planilhas e Documentos do Microsoft Office...</p> <p>BAIXAR</p>	<p>ISH</p> <p>GRUPO DE RANSOMWARE CLOP EXPLORANDO VULNERABILIDADE PARA NOVAS VÍTIMAS</p> <p>O grupo de Ransomware conhecido como Clop está explorando ativamente a vulnerabilidade conhecida como CVE-2023-0669, na qual realizou o ataque a diversas organizações e expôs os dados no site de data leaks...</p> <p>BAIXAR</p>

SUMÁRIO

1	Introdução executiva	5
2	Estratégico.....	5
2.1	Introdução	5
2.2	Vitimologia e Segmentos afetados	5
3	Tático	7
3.1	Funcionamento do protocolo Kerberos em ambiente Windows.....	7
3.2	Glossário rápido do protocolo Kerberos no ambiente Windows.....	7
3.3	O que é, como funciona e por que o Kerberoasting acontece.....	8
3.4	Fluxo do ataque	8
3.5	Por que o Kerberoasting acontece	9
4	Operacional.....	10
4.1	Emulação	10
4.2	Métodos de Detecção: Kerberoasting.....	11
4.3	Mitigação de ataque: Kerberoasting.....	12
4.4	Tabela MITRE ATT&CK.....	13
5	Conclusão	14
6	Recomendações.....	15
6.1	Indicadores de Comprometimento (IoC).....	17
7	Referências	18
8	Autores.....	18

LISTA DE TABELAS

Tabela 1 – Tabela MITRE ATT&CK.	13
--------------------------------------	----

LISTA DE FIGURAS

Figura 1 – Fluxo do protocolo Kerberos.	8
Figura 2 – SPN: Usuário de serviço.	10
Figura 3 – Evento 4769.	11
Figura 4 – GPO para Habilitar protocolos do Kerberos.	12

1 INTRODUÇÃO EXECUTIVA

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

2 ESTRATÉGICO

2.1 INTRODUÇÃO

A exploração de falhas nos mecanismos de autenticação é uma das táticas mais **utilizadas por agentes maliciosos** para obter acesso privilegiado em ambientes corporativos. Dentre essas técnicas, o **Kerberoasting** tem se destacado pela sua eficácia e dificuldade de detecção, explorando a arquitetura do protocolo Kerberos, amplamente adotado em domínios Windows. O Kerberoasting permite a extração de hashes de contas de serviço associadas a SPNs (Service Principal Names) e o subsequente ataque offline desses hashes, visando obter senhas em texto claro. Por não exigir acesso ao controlador de domínio nem gerar grandes alertas na rede.

Este relatório busca oferecer uma visão estratégica sobre a ameaça representada pelo Kerberoasting, contextualizando os riscos para a infraestrutura organizacional, os segmentos mais afetados e os **possíveis impactos operacionais**, além de fundamentar as decisões de segurança voltadas à mitigação da técnica.

2.2 VITIMOLOGIA E SEGMENTOS AFETADOS

A técnica de Kerberoasting, apesar de sua complexidade técnica moderada, tem sido amplamente adotada por cibercriminosos por sua eficácia contra ambientes mal configurados. Os principais setores impactados incluem:

- **Financeiro:** corporações com grandes domínios, contas de serviço antigas e exposição a ataques de movimentação lateral. O acesso privilegiado pode levar a fraudes internas e sequestro de dados.
- **Infraestrutura crítica e governo:** redes governamentais com domínios extensos e heranças legadas de Active Directory são alvos por razões geopolíticas e de espionagem.
- **Educação e pesquisa:** universidades com ambientes heterogêneos e falta de controle rígido de SPNs estão entre os alvos mais suscetíveis.

- **Saúde:** hospitais e operadoras frequentemente mantêm contas de serviço desatualizadas e são expostos por meio de técnicas de lateralização.
- **Empresas de tecnologia:** organizações com múltiplos serviços internos, scripts automatizados e contas de serviço compartilhadas tendem a acumular alvos ideais para Kerberoasting.

Em geral, qualquer ambiente *Windows* baseado em Active Directory pode ser impactado, principalmente quando:

- SPNs estão configurados em contas com senhas fracas ou estáticas;
- A criptografia RC4 está habilitada (em vez de AES);
- Não há mecanismos de rotação periódica de senhas de contas de serviço.

Diversos grupos avançados de *ameaças persistentes (APTs)*, como o **APT29 (Nobelium)**, **APT10** e **FIN6**, têm explorado a técnica Kerberoasting para escalar privilégios internamente após comprometimento inicial. A popularidade da técnica também se reflete no uso frequente por equipes de Red Teaming que empregam ferramentas como **Impacket**, **mimikatz** e variantes furtivas como **SharpRoast** e **Orpheus' Roaster**. Seu uso permite o comprometimento de contas de serviço privilegiadas com mínima visibilidade, representando alto risco para infraestruturas Windows mal configuradas.

3 TÁTICO

3.1 FUNCIONAMENTO DO PROTOCOLO KERBEROS EM AMBIENTE WINDOWS

Kerberos é um protocolo de autenticação que garante a comunicação segura entre usuários e serviços em redes como o **Active Directory**. Ele funciona com um sistema de tickets gerenciado pelo KDC (*Key Distribution Center*), que atua no controlador de domínio como o responsável por autenticar usuários e serviços e emitir tickets que comprovam suas identidades.

Quando um usuário faz login no domínio, ele recebe um ticket inicial chamado TGT (*Ticket-Granting Ticket*), que permite solicitar acesso a outros serviços. Para acessar um serviço específico, o usuário envia o TGT junto com uma solicitação ao KDC, que emite um novo ticket, o "*ticket de serviço*" (ou TGS), criptografado com o hash da senha do usuário de serviço de destino. Esse ticket é então apresentado ao serviço, que autentica o usuário e libera o acesso ao recurso.

3.2 GLOSSÁRIO RÁPIDO DO PROTOCOLO KERBEROS NO AMBIENTE WINDOWS

KDC (*Key Distribution Center*)

- Centro de Distribuição de Chaves que autentica usuários e serviços e gera tickets para acesso. Funciona no controlador de domínio.

TGT (*Ticket-Granting Ticket*)

- Ticket inicial concedido ao usuário após autenticação com o KDC. Usado para solicitar acesso a serviços no domínio.

TGS (*Ticket-Granting Service*)

- Serviço do KDC que recebe o TGT do usuário e emite um ticket de serviço (TGS) para acessar recursos específicos.

Ticket de Serviço (TGS)

- Ticket emitido pelo KDC para autenticação em um serviço específico. É criptografado com o hash da senha da conta do serviço alvo.

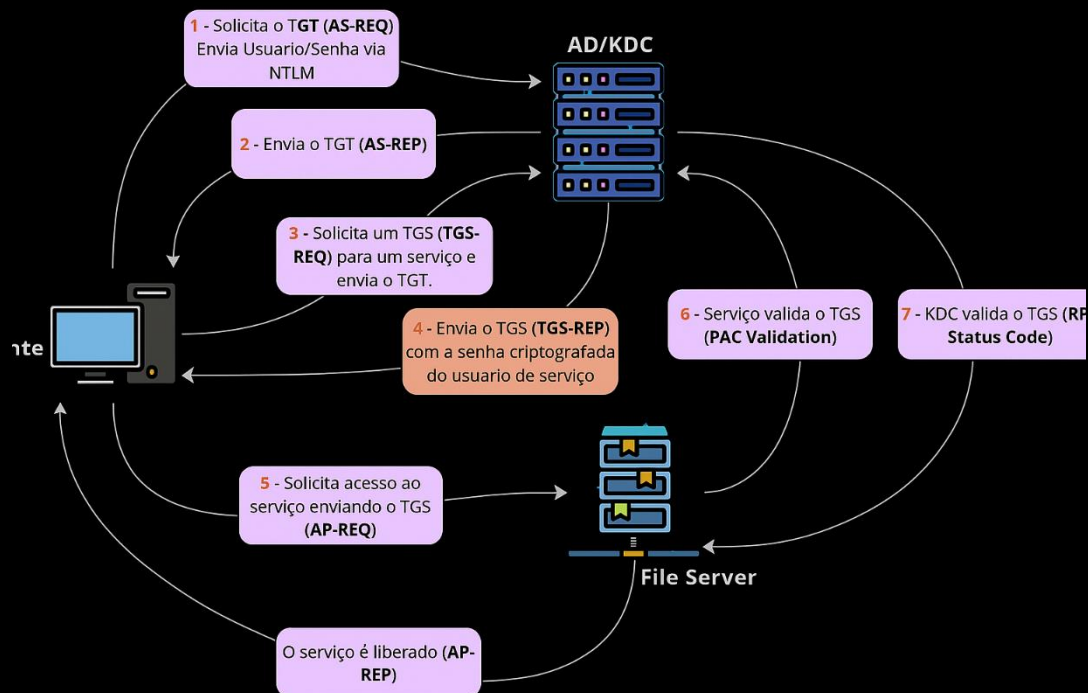


Figura 1 – Fluxo do protocolo Kerberos.

3.3 O QUE É, COMO FUNCIONA E POR QUE O KERBEROASTING ACONTECE

Kerberoasting é uma técnica utilizada por adversários para explorar o protocolo de autenticação **Kerberos** em ambientes Windows baseados em **Active Directory**. Nesse ataque, o invasor autentica-se normalmente no domínio e, em seguida, solicita **tickets de serviço (TGS)** para contas associadas a **Service Principal Names (SPNs)** — geralmente vinculadas a contas de serviço. Esses tickets TGS são criptografados com o **hash da senha da conta de serviço correspondente**. Como qualquer usuário autenticado pode solicitar esses tickets, o adversário consegue extraí-los da memória ou da rede e, posteriormente, realizar um **ataque offline de força bruta ou dicionário** para tentar descobrir a senha em texto claro.

O objetivo principal da técnica é **comprometer credenciais privilegiadas**, frequentemente associadas a serviços críticos, o que permite ao atacante escalar privilégios e ampliar seu controle sobre o ambiente interno da organização.

3.4 FLUXO DO ATAQUE

Geralmente o ataque acontece nas seguintes etapas:

1. Uma conta de domínio é comprometida (existem diversas técnicas para alcançar esse objetivo).

2. Após a autenticação, o adversário procura por alvos com contas que possuem *Service Principal Names* (SPNs).

- SPN (Service Principal Name) é um identificador que vincula uma instância de serviço específica a uma conta de logon de serviço. Um exemplo de SPN é: HTTP/webserver.purple.com.

3. O adversário utiliza a conta comprometida para obter um Ticket de Serviço (TGS), passando por todo o fluxo de autenticação do KDC.

Normalmente, o TGS é solicitado com um algoritmo de criptografia mais fraco. A mais utilizada para esse técnica é a 0x17 (RC4-HMAC).

4. O adversário captura o ticket e extrai o hash da conta.

5. Um ataque de força bruta é realizado para quebrar o hash da conta e obter a senha em texto claro.

6. O adversário utiliza essa credencial para se autenticar na rede e acessar outros recursos.

3.5 POR QUE O KERBEROASTING ACONTECE

Existem alguns pontos importantes no funcionamento padrão do protocolo Kerberos que permitem a ocorrência do Kerberoasting, incluindo:

1. Todos os serviços são associados a uma conta, seja uma conta de máquina ou de usuário.
2. Os tickets TGS (Ticket-Granting Service) são criptografados com o hash da senha da conta de serviço, o que é um dos fatores principais que tornam o Kerberoasting possível.
3. O KDC (Key Distribution Center) não verifica se o usuário tem permissão para acessar o serviço solicitado; essa verificação de permissão é feita pelo próprio serviço.

4 OPERACIONAL

4.1 EMULAÇÃO

Pré-requisito: *Credenciais de usuário do domínio.*

Diversas ferramentas podem ser utilizadas para esse ataque, como Mimikatz, Impacket e Rubeus. No nosso exemplo, será utilizada a ferramenta GetUserSPNs.py do conjunto de ferramentas Impacket. A primeira coisa após o comprometimento de uma conta é buscar com contas que **possuem SPN** (contas de serviço).

```
$ python3 GetUserSPNs.py DOMINIO/USER:SENHA [REDACTED]
```

```
Impacket v0.12.0.dev1 - Copyright 2023 Fortra
```

ServicePrincipalName	Name	MemberOf	PasswordLastSet	LastLogon	Delegation
http/app01.servico.purple.local	app01.servico	CN=Administrators,CN=Builtin,DC=purple,DC=local	2024-10-29 22:52:20.811331	<never>	

Podemos confirmar essa informação no AD, conforme imagem abaixo:

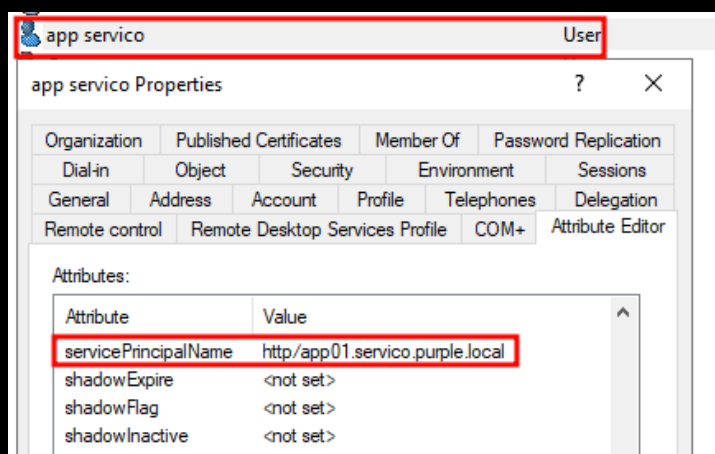


Figura 2 – SPN: Usuário de serviço.

Após enumerar as contas, pode ser solicitado o TGS para esse serviço.

```
$ python3 GetUserSPNs.py PURPLE.local/purple:Lab@2024 [REDACTED]
```

```
Impacket v0.12.0.dev1 - Copyright 2023 Fortra
```

ServicePrincipalName	Name	MemberOf	PasswordLastSet	LastLogon	Delegation
http/app01.servico.purple.local	app01.servico	CN=Administrators,CN=Builtin,DC=purple,DC=local	2024-10-29 22:52:20.811331	<never>	

```
[-] CCache file is not found. Skipping...
$krb5tgs$23$app01.servico$PURPLE.LOCAL$PURPLE.local/app01.servico*$02de899c8258bcecc0111cd5677b4f6cf$...<hash truncado>...
```

Com o Ticket salvo, pode ser realizado o processo de força bruta de forma offline para a quebra do hash e obter a senha em texto claro.

4.2 MÉTODOS DE DETECÇÃO: KERBEROASTING

Os ataques de Kerberoasting são difíceis de detectar, pois exploram o funcionamento padrão do Kerberos. No entanto, existem algumas maneiras eficazes de identificação. Para isso, é necessário habilitar os logs de Audit Kerberos Service Ticket Operations, Evento [4769](#).

Abaixo é apresentado um evento quando o Kerberoasting é executado na rede.

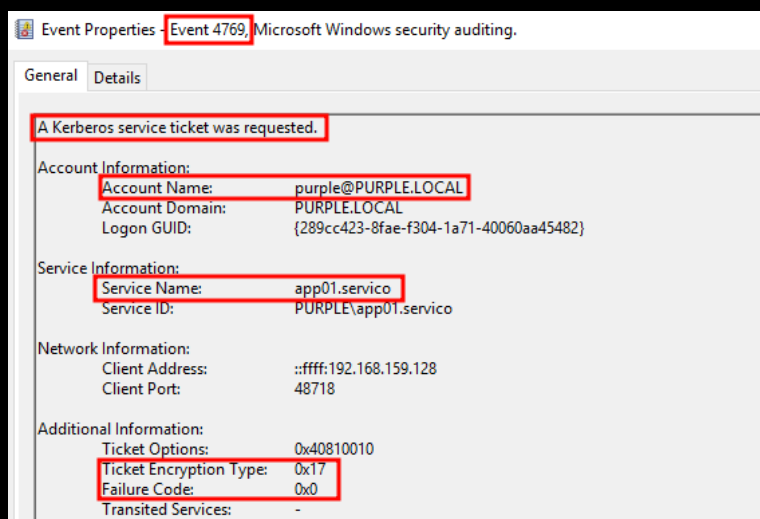


Figura 3 – Evento 4769.

Em um ambiente Active Directory, inúmeras solicitações de geração de tickets são geradas, o que pode dificultar a análise. No entanto, alguns parâmetros podem ajudar a filtrar falsos positivos, entre eles:

- **Account Name:** Contas que terminam com o símbolo \$ podem ser descartadas, pois geralmente são usadas por contas de serviço e de máquina.
- **Service Name:** Assim como no Account Name, serviços terminados com \$ e o serviço krbtgt também podem ser filtrado.
- **Ticket Encryption Type:** O uso de 0x17 (RC4-HMAC) é suspeito, pois trata-se de uma criptografia fraca geralmente associada a sistemas legados. O padrão costuma ser 0x12 (AES256-CTS-HMAC-SHA1-96).
- **Failure Code:** Um valor de 0x0 indica que o ticket foi gerado com sucesso.

Com esses filtros, a criação de regras de detecção ou o processo de hunting se torna mais assertivo, reduzindo falsos positivos e focando em atividades potencialmente maliciosas.

4.3 MITIGAÇÃO DE ATAQUE: KERBEROASTING

Uma das maneiras mais eficazes de fortalecer o ambiente contra ataques de Kerberoasting é implementar uma política de senhas robusta para contas de serviço, incluindo senhas complexas e alteração periódica. Além disso, seguir o princípio do menor privilégio.

Embora não elimine totalmente o risco, utilizar apenas criptografias mais robustas, como AES 128 e AES 256, pode dificultar o trabalho do adversário. É possível desabilitar protocolos de criptografia inseguros por meio das Políticas de Grupo (GPO). Abaixo está o caminho para configurar essa opção.

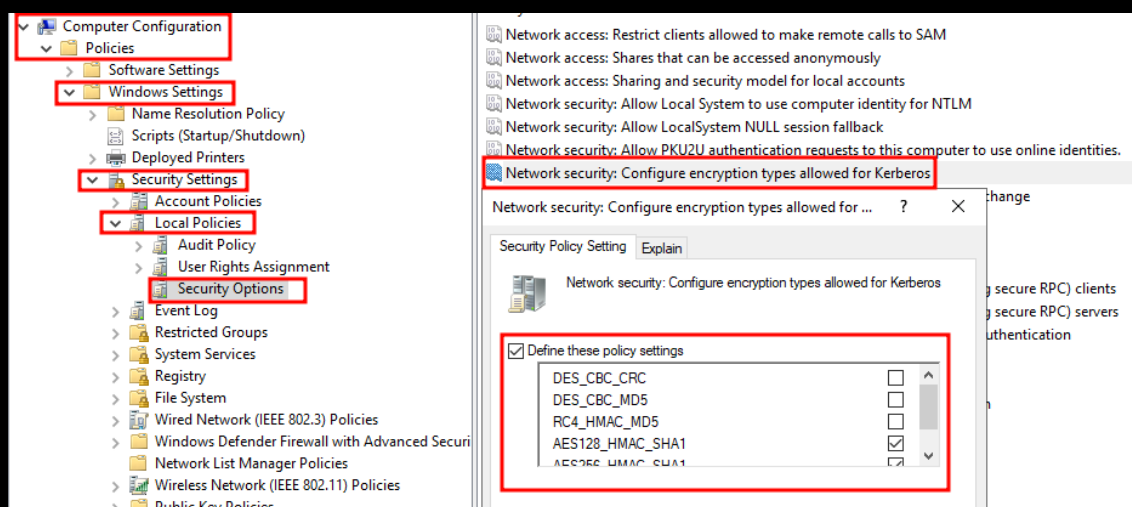


Figura 4 – GPO para Habilitar protocolos do Kerberos.

4.4 TABELA MITRE ATT&CK

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

Tática	Técnica	Detalhes
Credential Access	T1158 Steal or Forge Kerberos Tickets	Adversários autenticados no domínio podem solicitar tickets de serviço (TGS) para contas associadas a SPNs.

Tabela 1 – Tabela MITRE ATT&CK.

5 CONCLUSÃO

O Kerberoasting permanece como uma das técnicas mais eficazes para escalonamento de privilégios em ambientes Windows baseados em Active Directory. Sua simplicidade de execução aliada à dificuldade de detecção torna a ameaça especialmente perigosa em redes mal configuradas ou com políticas de segurança deficientes. Este relatório demonstrou não apenas como o ataque ocorre, mas também como pode ser detectado, mitigado e prevenido por meio de práticas consolidadas de cibersegurança. Políticas robustas de senhas, eliminação de algoritmos legados, controle rigoroso de SPNs e visibilidade operacional são pilares essenciais para proteção eficaz contra esse vetor.

Reforçamos que a defesa contra ameaças como o Kerberoasting não deve se limitar à configuração técnica, mas envolver uma postura contínua de monitoramento, validação de controles e resposta a incidentes. A integração entre inteligência de ameaças, equipes técnicas e governança de TI é fundamental para reduzir riscos e garantir resiliência cibernética no longo prazo.

6 RECOMENDAÇÕES

São elencadas abaixo pela ISH, medida que poderão ser adotadas visando a mitigação da referida ameaça, como por exemplo:

Fortalecimento de contas de serviço

- Estabeleça políticas rigorosas de criação de senhas para contas de serviço, com exigência de alta complexidade e comprimento mínimo de 25 caracteres.
- Implemente mecanismos automatizados de **gerenciamento e rotação periódica de senhas**, especialmente para contas sensíveis e privilegiadas.
- Evite o uso de contas de usuário padrão como contas de serviço, separando identidades operacionais de identidades técnicas.

Controle de criptografia

- Desabilite algoritmos obsoletos como **RC4** nas políticas de autenticação Kerberos.
- Garanta que apenas algoritmos modernos e seguros, como **AES**, estejam habilitados para emissão de tickets de serviço.

Redução da superfície de ataque

- Faça revisões regulares das contas associadas a **nomes principais de serviço (SPNs)** e elimine SPNs não utilizados, duplicados ou vinculados a contas desnecessárias.
- Restrinja os privilégios das contas de serviço ao **mínimo necessário para a execução de suas funções**, evitando associações com grupos administrativos ou de alto privilégio.

Monitoramento e Detecção

- Ative a auditoria de autenticação Kerberos e configure alertas para comportamentos anômalos, como:
 - Múltiplas solicitações de tickets de serviço (TGS) em curto intervalo.
 - Solicitações de TGS utilizando algoritmos de criptografia mais fracos.
- Mantenha visibilidade sobre contas que nunca realizam logon, mas continuam com SPNs ativos.

Validação de controles e simulação

- Realize exercícios regulares para testar a eficácia dos controles de autenticação e resposta a incidentes envolvendo extração e quebra de tickets.
- Integre equipes de defesa e simulação ofensiva (Blue Team e Red Team) em ciclos coordenados para avaliar vulnerabilidades e refinar alertas.

6.1 INDICADORES DE COMPROMETIMENTO (IoC)

Para verificar comprometimentos em contas de serviço, alguns dados podem ser úteis, além dos eventos e parâmetros destacados na seção de detecção, outros dados podem contribuir para a análise, como logs de execução do PowerShell, que permitem verificar atividades maliciosas no host que realizou a solicitação.

- **Evento 4104:** Registra scripts do PowerShell executados na máquina, facilitando a identificação de comandos suspeitos e potenciais atividades maliciosas.
- **Arquivos Prefetch:** Programas como o Rubeus podem gerar arquivos Prefetch, armazenados no diretório *C:\Windows\Prefetch*, ajudando a rastrear execuções recentes de programas e possíveis ações suspeitas no sistema.

7 REFERÊNCIAS

- Heimdall *by* ISH Tecnologia
- [MITRE ATT&CK](#)
- [Microsoft](#)

8 AUTORES

- Cleriston de Freitas Santos Portela – Threat Researcher
- Ismael Rocha – Threat Intelligence Specialist



heimdall
security research

A DIVISION OF ISH