Relatório Técnico de Incidente – Sistema Windows

Título: Investigação de Incidente: Credencial Comprometida em Ambiente Windows
Analista Responsável: Mari
Data: Abril de 2025

---

1. Resumo

Durante uma análise de rotina, foi identificado um login fora do horário usual em uma estação Windows. A partir desse evento, observou-se uma sequência de comportamentos anômalos, incluindo uso de ferramenta de extração de credenciais, alteração de arquivos críticos do sistema e atividades que indicam a instalação de um canal de comunicação remoto (C2). A investigação confirmou a ocorrência de comprometimento da máquina, com evidências consistentes de acesso não autorizado, escalonamento de privilégios e persistência maliciosa.

---

2. Descrição do Incidente

O evento inicial consistiu em um logon bem-sucedido registrado fora do padrão de horário da conta. Foram coletadas evidências no sistema afetado que apontam para os seguintes vetores de ataque:

- Execução da ferramenta Mimikatz para extração de senhas em texto claro.
- Modificação do arquivo hosts redirecionando domínios legítimos para endereços IP maliciosos.
- Upload de arquivos .jsp em diretório web, configurando possível webshell.
- Criação de regra personalizada no firewall permitindo conexões pela porta 1337.

Estes elementos demonstram uma tentativa clara de estabelecer persistência no sistema e comunicação externa com controle remoto.

---

3. Linha do Tempo

- Login suspeito identificado em evento de autenticação (Event ID 4624)
- Execução de ferramenta de extração de credenciais (Mimikatz)
- Modificação do arquivo hosts
- Upload de arquivo .jsp indicando webshell no servidor
- Criação de regra de firewall liberando comunicação por porta incomum (porta 1337)

---

4. Técnicas MITRE ATT&CK Identificadas

Fase	Técnica	ID	Descrição
Acesso Inicial	Valid Accounts	T1078	Uso de credenciais legítimas para acessar o sistema
Execução	Command and Scripting Interpreter	T1059.001	Execução de comandos via linha de comando
Credential Access	Credential Dumping (Mimikatz)	T1003.001	Extração de credenciais da memória
Persistência	Web Shell	T1505.003	Instalação de webshell no servidor web
Defesa Evasão	Modify System Configuration	T1562.001	Manipulação do arquivo hosts para redirecionamento de tráfego
Comunicação C2	Non-Standard Port	T1571	Porta 1337 liberada no firewall para comunicação externa

---

5. Conclusão e Recomendações

O incidente foi confirmado por meio da correlação entre logs do sistema, artefatos maliciosos encontrados e análise das técnicas empregadas pelo atacante. O objetivo aparente foi o acesso não autorizado, extração de credenciais, persistência e comunicação remota com o sistema.

Recomendações:

- Revogar imediatamente as credenciais comprometidas e exigir redefinição de senha.
- Bloquear os endereços IP maliciosos identificados.
- Restaurar o arquivo hosts e aplicar monitoramento sobre alterações futuras.
- Remover arquivos maliciosos e regras de firewall personalizadas.
- Realizar varredura em outros ativos da rede para identificar possíveis propagadores ou novos comprometimentos.
- Implementar monitoramento contínuo de logs de eventos e comportamento anômalo.