Lições aprendidas na análise post-mortem de um incidente relevante

FEBRABAN
/CYBER LAB

14° Fórum Brasileiro de CSIRTs

Agenda

Introdução, Objetivo e Disclaimer /

Timeline /

Análise /

Lições Aprendidas /

Considerações Finais /

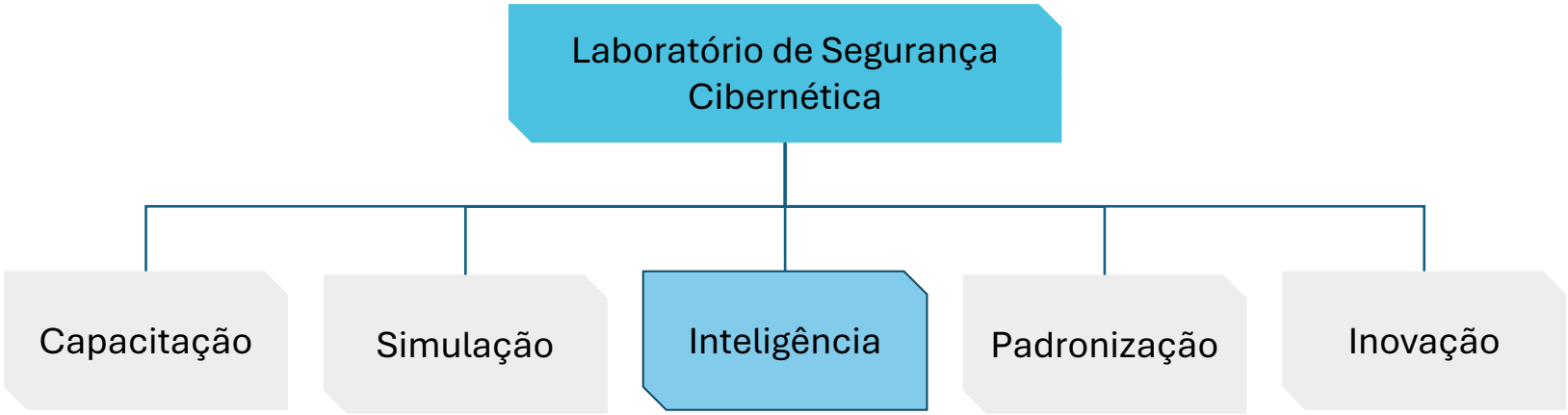
Whoami

FEBRABAN CYBER LAB

Henrique Kodama

Especialista em Segurança Cibernética

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS



De onde vem esta apresentação

Caso concreto de análise post-mortem com lições aprendidas

Reconstrução a partir da análise de logs e históricos de comando

FEBRABAN CYBER LAB

Escopo e limitações

1. **Base documental**

   Análise construída em cima de material disponibilizado. Sem acesso ao contexto interno da organização afetada.

2. **Natureza**

   Não é laudo forense, não substitui investigação interna e não tem caráter probatório.

3. **Inferência**

   Conclusões foram formuladas por correlação de artefatos, não necessariamente 100% dos registros.

4. **Anonimização**

   Datas deslocadas com intervalos preservados. Identificadores e nomes de sistema substituídos.

FEBRABAN
/CYBER LAB

Introdução

Timeline

Análise

Lições Aprendidas

Considerações Finais

FEBRABAN / CYBER LAB

Onde cada máquina apareceu na linha do tempo

	Acesso	Túnel	Dwell	Abuso	Detecção
RELAY nuvem pública		ativo	presente	presente	presente
VM_1 pivô	ativo	ativo	presente	ativo	ativo
VM_2 operacional				ativo	presente
HOST_B borda				ativo	
HOST_C auxiliar				ativo	

VM_1 aparece em todas as fases ativas. Foi o ponto de entrada, o host da chave e o ultimo a ser inspecionado.
➡️ Qual a sua VM_1 do seu ambiente?

FEBRABAN / CYBER LAB

Living of the Land + Oportunismo

O adversário mapeou e adaptou o que encontrou.

Encontrado no ambiente

- Componentes de integração em produção
- Documentação técnica interna
- Estruturas de configuração por canal
- Certificados e chaves em disco

Adicionado pelo operador

- Scanner de rede via gerenciador de pacotes
- Emuladores de terminal para sistema específico
- Navegador headless e automação
- Ambiente de desenvolvimento remoto

Pouca ou nenhuma compilação ou ofuscação. Tudo estava disponível ou já no ambiente.

FEBRABAN CYBER LAB

Da posse da chave ao uso da identidade

Posse

Chave privada e certificado legíveis em disco

→

Assinatura

Mensagem formada e assinada localmente

→

Transporte

Envio pelos mecanismos legítimos

→

Aceitação

Destino valida e processa

Em nenhum ponto desta cadeia houve falha criptográfica.

Do ponto de vista do destino, as mensagens eram indistinguíveis das legitimas.

FEBRABAN
/CYBER LAB

Introdução

Timeline

Análise

Lições Aprendidas

Considerações Finais

TLP:CLEAR

FEBRABAN / CYBER LAB

Oportunidades de detecção

1

Execução em área temporária

Binário extraído e executado a partir de diretório gravável por qualquer usuário, em servidor de produção.

FONTE

EDR ou auditoria de sistema

2

Egress persistente para nuvem

Sessão cifrada de longa duração para provedor externo, em porta não padronizada, mantida por semanas.

FONTE

Fluxo de rede, firewall, proxy

3

Falhas de elevação de privilegio

Três negativas de autorização em sequencia, com comandos apontando para script oculto e canal reverso.

FONTE

Log de autenticação do sistema

4

Ferramentas fora do baseline

Scanner de rede, emuladores de terminal, navegador headless, e bibliotecas incomuns.

FONTE

Gerenciador de pacotes e inventario

5

Volumetria anômala de credenciais

Milhares de operações registradas em log próprio da aplicação, sem limiar e sem painel.

FONTE

Log de aplicação, ausente do SIEM

6

Credencial única, múltiplas origens

A mesma conta de serviço autenticando de endereços distintos, fora do expediente, incluindo madrugada.

FONTE

Correlação de autenticação

FEBRABAN CYBER LAB

Recomendações por camada

Identidade

- Conta de serviço não autenticar interativamente
- Se ainda for necessário, ter visibilidade e revisar frequentemente
- Usar cofre para credencial de automação

Host

- Remover permissão de execução em diretórios desnecessários
- Inventário de software autorizado por perfil
- Registro e auditoria de execução de comandos em servidores críticos

Rede

- Baseline de saída por host: destino, porta, duração
- Sessão longa para nuvem pública pode ser uma anomalia
- Revisão periódica das conexões mais duradouras

Aplicação

- Gestão da chave privada em módulo de hardware ou cofre
- Log de uso de credencial ingerido no SIEM
- Baseline de volumetria por canal e por janela

Os logs que reconstruíram este incidente já existiam. Nenhum foi criado depois.

FEBRABAN
/CYBER LAB

Introdução

Timeline

Análise

Lições Aprendidas

Considerações Finais

Obrigado!

Henrique Kodama

henrique.kodama@febraban.org.br

linkedin.com/in/hskodama/

Laboratório

labsegciber@febraban.org.br

FEBRABAN

TLP:CLEAR