ACESSO LEGÍTIMO, COMPORTAMENTO SUSPEITO

Investigação de Incidentes com Credenciais Válidas

TLP:CLEAR

Everson Probst
Head de Cibersegurança – Grant Thornton

Especialista em Resposta a Incidentes.

Profissional com 16 anos de atuação em segurança da informação, com foco em investigação de incidentes, análise forense digital e suporte a litígios.

Formado em sistemas de informação com especialização em Engenharia de redes e telecomunicações e Cibersegurança.

Atuou em diversos casos envolvendo vazamentos de dados, comprometimento interno, movimentação lateral silenciosa e fraudes com uso de credenciais legítimas.

A ILUSÃO DO ACESSO CONFIÁVEL

ATAQUES MODERNOS NÃO PRECISAM MAIS DE EXPLOITS — BASTA UM LOGIN VÁLIDO.

TLP:CLEAR

TLP:CLEAR

INCIDENTE PIX (JUL/2025)

- **No início de julho de 2025, uma PSTI, fornecedora crítica de infraestrutura para o sistema PIX devidamente autorizada e homologada pelo BACEN, foi alvo de um ataque que resultou no desvio de mais de R$ 800 milhões, afetando diferentes bancos.**
- **O Banco Central suspendeu temporariamente três participantes do sistema e abriu investigação.**
- O mais alarmante? Não houve brecha técnica sofisticada.
- Tudo indica que o ataque foi conduzido com credenciais válidas - vendidas por um Access Broker.
- Novo paradigma: Nem todo comportamento suspeito vem de fora. E nem todo acesso legítimo é confiável.

Mas esse não é um caso isolado. Vamos olhar o cenário maior de exposição.

MEGA VAZAMENTO DE 16 BILHÕES DE CREDENCIAIS (JUN/2025)

- Em junho de 2025, foi divulgado um compilado contendo ~16 bilhões de credenciais (usuário+senha), colhidas por infostealers e brechas antigas, organizadas em 30 bases distintas .

- Essas credenciais incluem contas de plataformas como Apple, Google, Facebook, GitHub, VPNs e até portais governamentais .

- Embora não seja um ataque concentrado a uma empresa específica, esses dados estão frescos, bem estruturados e podem ser usados em escala para credential stuffing e account takeover.

Se apenas **0,01%** dessas credenciais ainda estiver ativa, **são 1,6 milhão de combinações válidas em circulação**.

Usuários que reutilizam senhas entre pessoal e corporativo aumentam exponencialmente o risco.

Isso significa que milhares de empresas podem estar vulneráveis a ataques com credenciais válidas, que são extremamente difíceis de detectar.

DADOS QUE CONTEXTUALIZAM O RISCO

- 30% das intrusões globais em 2024 começaram com uso de credenciais legítimas (IBM X-Force).

- 79% dos ataques detectados não usaram malware - exploraram identidade, automação e comportamento esperado (Crowdstrike 2025).

- Fóruns na dark web registraram aumento de 90% na oferta de acessos corporativos válidos (Cyberint IAB Report).

- O Brasil aparece com destaque nesse cenário: 7% das credenciais à venda têm origem em empresas brasileiras

Esses números mostram o tamanho do problema. Mas como esses acessos são explorados na prática?

TLP:CLEAR

EXEMPLO DE INCIDENTE

Imagine o funcionário do financeiro:

- Acessa a plataforma bancária toda segunda às 9h.

Agora imagine:

- A mesma conta usada às 3h da manhã,
- A partir de uma máquina nova,
- Realizando transações grandes,
- De forma perfeitamente autenticada.

O sistema de monitoramento vê normalidade. Mas você, como analista, precisa ver o absurdo.

TLP:CLEAR

A CREDENCIAL NÃO É A IDENTIDADE.

O LOGIN NÃO É GARANTIA DE LEGITIMIDADE.

E O SIEM, SOZINHO, NÃO VAI ENXERGAR ESSE TIPO DE ATAQUE.

TÉCNICAS MODERNAS COM LOGIN LEGÍTIMO

TÁTICA	TÉCNICA (ID)	AÇÃO DO ATACANTE
Initial Access	T1078	Uso de credenciais legítimas
Lateral Movement	T1021.002 (SMB)	Uso de PsExec entre hosts
Persistence	T1053.005 (Scheduled Task)	Criação de tarefas agendadas
Collection	T1119	Coleta automatizada de arquivos
Exfiltration	T1048.003 (Exfil via Cloud)	Upload para OneDrive

Tudo nativo, nada malicioso.

O atacante hoje não instala nada. Ele age com o que já existe no sistema. Quando o atacante tem a senha, ele não precisa do exploit.

DADOS DE MERCADO QUE CONFIRMAM O PADRÃO

- Infostealers (como RedLine e Vidar) coletaram mais de 3,2 bilhões de credenciais em 2024.
- Um Access Broker cobra de US$ 200 a 3.000 por acesso a rede corporativa com RDP ou VPN válidas.
- Ataques “malware-free” já são maioria em ambientes corporativos - o “novo normal” é invasão por identidade, não por binário.

Ex. Um atacante compra na dark web o login de um coordenador de TI. Ele entra pelo VPN, executa um script PowerShell para extrair senhas de rede via LSASS, acessa arquivos sigilosos no servidor de RH e sobe tudo para o OneDrive.

Tudo isso sem usar nenhuma ferramenta maliciosa.

Para o SIEM: rotina de trabalho.

EXEMPLO DE MOVIMENTAÇÃO LATERAL COM PSEXEC

Conta: suporte.local

Permissão: leitura em endpoints de usuários

Atividades detectadas:

1. Logon remoto via RDP em máquina de marketing às 18h45
2. Execução de net group "Domain Admins" e whoami
3. Uso de PsExec para pivotar lateralmente

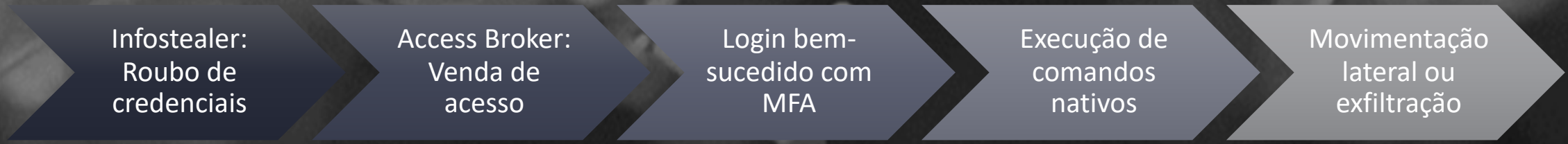
Resultado:

- Sem alertas de EDR
- Sem erros de autenticação
- Sem comportamento ostensivo

O que um bom analista veria aqui?

- Isolado, cada evento parece inofensivo.
- Juntos, eles contam uma história.

REFLITA SOBRE ESTE FLUXO:



Sem correlação de logs, esse fluxo parece legítimo do início ao fim.

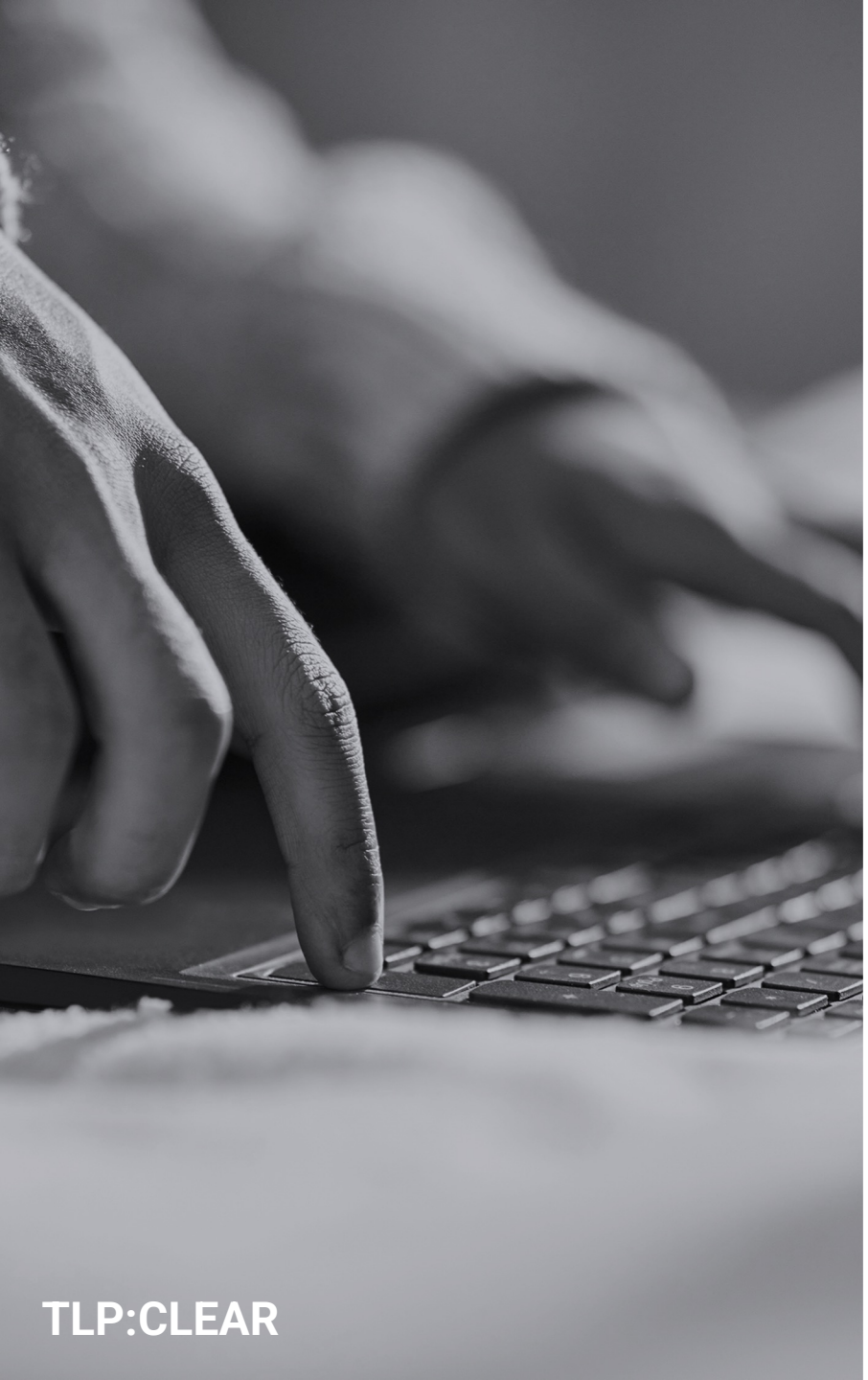
Nenhuma dessas etapas depende de malware.

Cada uma delas parece "comportamento normal", sem contexto.

QUANDO O ATACANTE TEM A SENHA, O SISTEMA ESTÁ DO LADO DELE.

SÓ A INVESTIGAÇÃO CONTEXTUAL É CAPAZ DE INVERTER O JOGO.

TLP:CLEAR



INSIDER VS CONTA COMPROMETIDA

CRITÉRIO	INSIDER	CONTA COMPROMETIDA
Conhecimento do negócio	Alto: sabe onde mexer	Baixo: tenta e erra, ou age com padrão genérico
Comportamento no sistema	Cauteloso, metódico, previsível	Errático, com saltos entre sistemas
Disfarce de ações	Costuma mascarar como rotina	Usa comandos de forma abrupta
Horário de atividade	Dentro do expediente	Fora de horário, ou com “impossible travel”
Ferramentas usadas	Sistemas corporativos regulares	Cmd, PowerShell, exportações em massa
Persistência	Planejada (ex: exfiltra aos poucos)	Mais imediatista

Quando um comportamento anômalo parte de uma conta legítima, o analista precisa formular hipóteses.

Existem dois cenários principais:

- Insider malicioso: O próprio colaborador age intencionalmente contra a organização
- Conta comprometida: A conta foi usada por terceiros (ex: via malware, phishing ou venda)

EXEMPLO DE CONTA COMPROMETIDA POR ACCESS BROKER

Cenário:

Credencial de gerente de operações vendida na dark web por US$ 1.400.

Comportamento detectado:

- Logon via VPN de IP argentino (conta normalmente usada no Brasil).
- Tentativa de acesso a 6 sistemas diferentes, em 10 minutos.
- Download massivo de planilhas com prefixo “comercial_2023*”.
- Logoff em seguida.

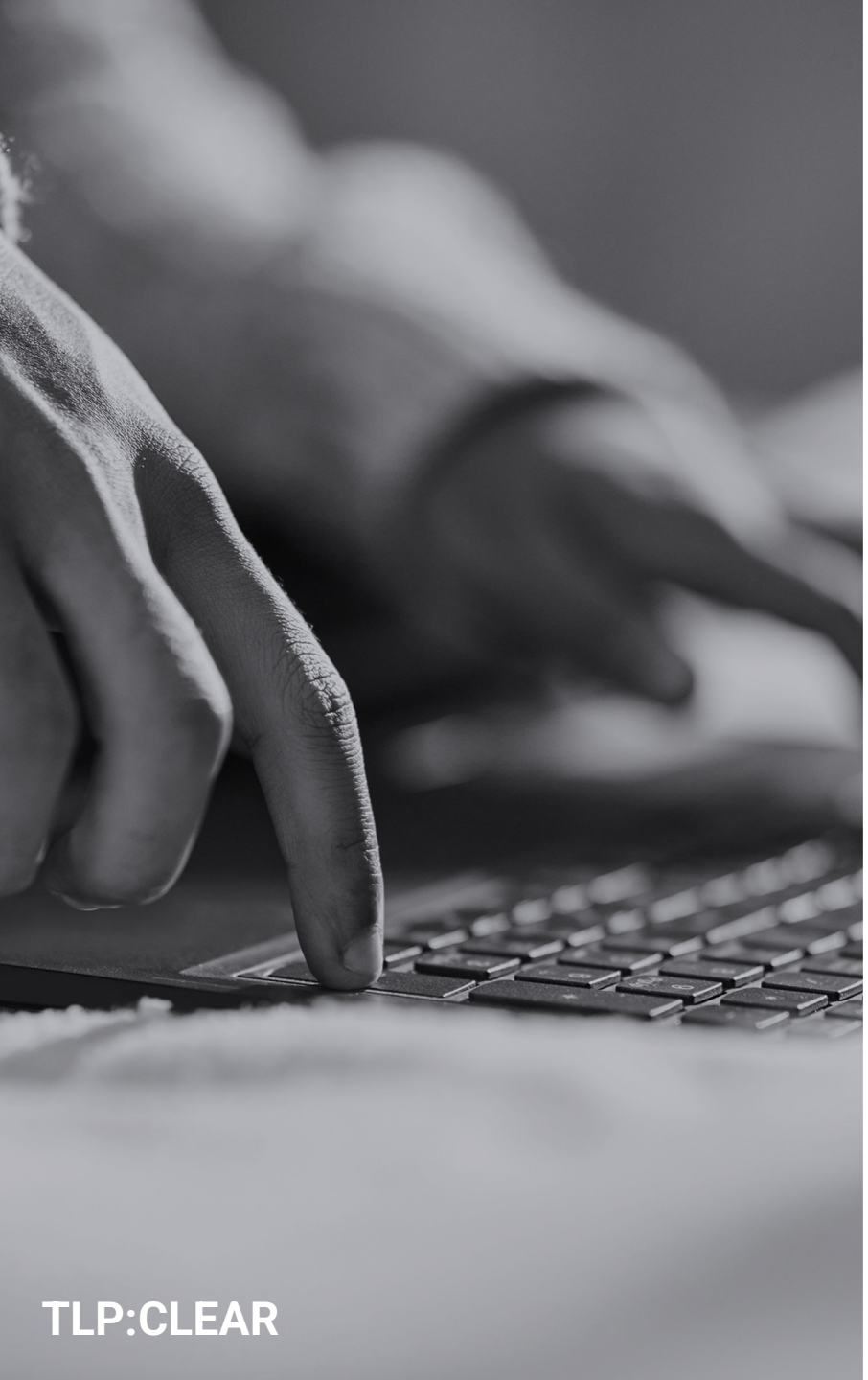
Esse padrão chama atenção por:

- Volume e variedade.
- Dispositivo e origem inéditos.
- Sequência não típica do usuário.

TLP:CLEAR

A CONTA É A MESMA. MAS O COMPORTAMENTO CONTA UMA HISTÓRIA DIFERENTE.

PARA INVESTIGAR, É PRECISO SAIR DA LÓGICA BINÁRIA DE ‘FOI OU NÃO FOI HACKEADO’ - E PASSAR PARA HIPÓTESES BASEADAS EM CONTEXTO.



FERRAMENTAS NECESSÁRIAS PARA UMA INVESTIGAÇÃO EFICAZ

COMPONENTE	PAPEL NA INVESTIGAÇÃO
SIEM com correlação contextual	Identifica ações isoladas que só fazem sentido em conjunto
UEBA	Detecta desvios de padrão por identidade
EDR + Proxy + VPN + AD	Fontes de log obrigatórias para análise de movimentação lateral
MFA adaptativo	Detecta novos dispositivos, localizações, horários
PAM / Vaulting	Ajuda a identificar uso não autorizado de credenciais sensíveis

Se seus logs não têm timestamp sincronizado e dados padronizados, sua investigação vai falhar — mesmo com SIEM.

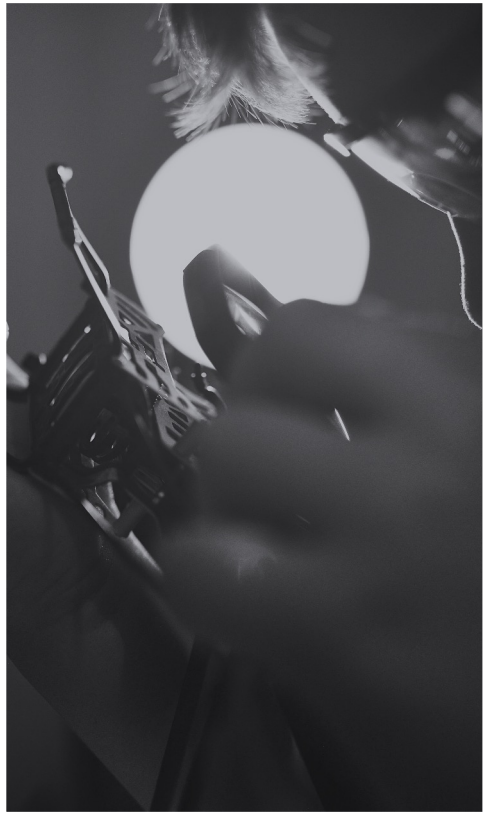
A tecnologia ajuda a detectar indicadores, mas as anomalias conectadas com incidentes mais avançados ou silenciosos são detectadas por analistas que interpretam logs de forma contextual.

INDICADORES ÚTEIS PARA INVESTIGAÇÃO

- Logon bem-sucedido fora do país
- Logon em horário incomum.
- Mudança de regras de e-mail .
- Conexões RDP entre máquinas de setores distintos.
- Atividade intensa durante férias do titular.
- PowerShell em máquina sem histórico técnico.

Esses sinais, isolados, são fracos.
Mas correlacionados, eles entregam o invasor.
O SIEM vê eventos. O analista vê o absurdo.

DEZ SINAIS DE COMPORTAMENTO SUSPEITO COM LOGIN VÁLIDO



1. Novo device com MFA aprovado
2. Logon bem-sucedido mas fora do perfil
3. Horário de atividade anômalo
4. Ferramenta nova usada pelo usuário
5. Acesso a sistema fora da rotina (whoami a partir da máquina do RH)
6. Atividade intensa durante férias
7. RDP/WinRM entre áreas distintas
8. Criação de tarefa agendada incomum
9. Script com comandos obfuscados
10. Alterações em configurações de e-mail

ENCERRAMENTO

O verdadeiro analista não procura o erro.

Procura o que não faz sentido.

O atacante de hoje quer parecer legítimo. Seu trabalho é identificar o que não faz sentido; mesmo que tudo tenha passado pelo MFA.

Everson Probst – Sócio de Cibersegurança

Grant Thornton

E-mail: everson.probst@br.gt.com

Checklist final com 5 perguntas:

- Isso faz sentido para esse usuário?
- Esse dispositivo é conhecido?
- O horário é compatível?
- Há histórico semelhante?
- Há contexto para esse padrão?

TLP:CLEAR