|  |
| --- |
| 1. **Identificação** |
| |  |  | | --- | --- | | **Evento ID:** |  | | **Data / hora:** |  | | **Meio de Notificação:** | Nível 1 (SOC) | | **Tipo de Ameaça** | Acesso indevido (VPN) | | **IOC :  (Indicadores de Comprometimento)** | |  |  | | --- | --- | | VPN - utilização de SO Server VPN – conexões simultâneas | VPN - hostid malicioso  Gerid – utilização de credencial de terceiros | | Troca de senha - credencial de terceiros (alerta4) Endereço IP diferente da localização do usuário | Endereço IP público (hosting/má reputação) Outro: | | | **Período analisado:** |  | | **Resumo:** | |  | | --- | | (escreva um breve resumo do evento sobre o que foi encontrado) | | |

| 1. **Detecção e Análise** |
| --- |
| |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | | **Ferramentas de Análise :** | |  |  |  | | --- | --- | --- | | Netwitness | Firewall | Acesso (LDAP) | | ELK | Cisco Talos | Outro: | | | **2.1 Credenciais envolvidas :** (incluir o domínio no usuário ex. @inss.gov.br) | |  |  |  |  | | --- | --- | --- | --- | | **Usuário(s)** | **End. IP VPN - Privado (caso exista)** | **Endereço IP da conexão (Público)** | **Data/hora da última Troca de Senha (www-acesso)** | |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  | | | **(EXCLUSIVO VPN) 2.2 Credenciais utilizadas (VPN/Gerid) :** incluir domínio no e-mail dos usuários,  ex. @inss.gov.br | |  |  |  | | --- | --- | --- | | **Usuário VPN** | **Credencial GerID** | **E-mail usuário GerID** | |  |  |  | |  |  |  | |  |  |  | |  |  |  | |  |  |  | | | **(EXCLUSIVO VPN)**  **2.3 Principais sistemas acessados / volumetria :  (Firewall de VPN)** | |  |  |  | | --- | --- | --- | | **Credencial** | **Top 3 Sistemas mais acessados** | **Volumetria** | |  |  |  | |  |  | |  |  | |  |  |  | |  |  | |  |  | |  |  |  | |  |  | |  |  | |  |  |  | |  |  | |  |  | | | **(EXCLUSIVO MONITORAMENTO TROCA SENHA)**  **2.2 Informações LDAP :**   |  |  |  |  |  | | --- | --- | --- | --- | --- | | **Usuário** | **Nome** | **CPF** | **Status** | **Localidade** | |  |  |  |  |  | |  |  |  |  |  | |  |  |  |  |  | |  |  |  |  |  | |  |  |  |  |  |   **2.3 Usuário de VPN utilizado :**  (Se a troca de senha for por meio de IP de VPN, informar também qual foi o hostid utilizado no firewall de VPN.)   |  |  |  | | --- | --- | --- | | **Usuário VPN** | **IP VPN** | **Hostid (Palo Alto)** | |  |  |  | |  |  |  | |  |  |  | | | | **2.4 Evidências anexadas :** | Coloque o nome dos arquivos csv | | **2.5 Evidências coletadas (abaixo) :** | | | **\*\*\* Todo o texto ABAIXO deve ser apagado \*\*\*\***  Tela do Cisco Talos com endereço IP público e possíveis bloqueios [apenas se estiver com má reputação])  **[SE FOR MONITORAMENTO DE VPN]**  (Tela do Palo Alto “[Source IP Activity” + “Destination IP Activity” + “Monitor > GlobalProtect”]  Tela do Gerid [apenas se encontrar divergências de acesso];  (ATENÇÃO: Caso a ameaça seja de “hostid malicioso”, favor informar também os outros usuarios que utilizaram do mesmo hostids)  **[SE FOR MONITORAMENTO DO TROCA SENHA, incluir as telas do ELK abaixo]**   * + 1. “[WAF] IPs x Usuarios Trocas com Sucesso”;     2. “[WAF] IPs x Numero de Trocas”;     3. “[WAF] Tentativas de Troca x IPs Distintos” (Reset/sucesso/falha);     4. “[WAF] Troca-Senha – Falha.” Observação: essa informação, caso exista, é importante para que se verifique quais outros usuários podem ser futuros alvos;     5. Timeline Troca de Senhas;     6. “[Palo Alto] VPN Correio - Troca senha”. Observação: esta informação se aplica no caso de conexão por VPN. Se a informação não estiver disponível no dashboard, ela deverá ser pesquisada no Palo Alto; | | |

|  |
| --- |
| 1. **Contenção, erradicação e recuperação** |
| |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | **Contenção:** | |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | | Bloqueio de credenciais no **firewall**  **Data/hora:** | |  | | --- | | **Credenciais de VPN** | |  | |  | |  | |  | |  | | | |  | |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | | Bloqueio no **firewall de aplicação**  **Data/hora:** | |  | | --- | | **E-mail usuários GerID** | |  | |  | |  | |  | |  | | | |  | |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | | Bloqueio de **endereçamento IP**  **Data/hora:** | |  | | --- | | **Endereço IP ou subrede** | |  | |  | |  | |  | |  | | | |  | |  |  |  | | --- | --- | --- | | Outro  **Data/hora:** | |  | | --- | |  | | | |  |  | | **Comentários adicionais:** |  | | **Existe caso de reincidência?** | (informar se possível caso o usuário ou hostid seja reincidente) | | **Encaminhamento:** |  | |

|  |
| --- |
| 1. **Atividade Pós-Notificação** |
| **(A ser preenchido pela IRIS / DMPR)** |