| 1. **Identificação** |
| --- |
| | **Evento ID:** | INC-259109 | | --- | --- | | **Data / hora:** | 23/11/2021 19:52:25 | | **Meio de Notificação:** | Nível 1 (SOC) | | **Tipo de Ameaça** | Acesso indevido (VPN) | | **IOC :  (Indicadores de Comprometimento)** | VPN - Host ID malicioso | | **Período analisado:** | 23/11/2021 19:52:25 | | **Resumo:** | Acesso de HostID c97ef43e-af4d-49d4-8bae-776666810232  Incluído na lista de HostID maliciosos por acesso indevido previamente | |

| 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) | | --- | --- | --- | --- | | melissa.kreling@agu.gov.br | 10.253.1.38 | 177.25.203.123 |  | | | | **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** | | --- | --- | --- | | melissa.kreling@agu.gov.br | 56528833400 | melissa.kreling@agu.gov.br | | | | **2.3 Principais sistemas acessados / volumetria:  (Firewall de VPN)** | | **Credencial** | **Top 3 Sistemas mais acessados** | **Volumetria** | | --- | --- | --- | | melissa.kreling@agu.gov.br | vip-pmeuinss-api.inss.gov.br | 46.82 KB | | estatisticaswebatualiza.dataprev.gov.br | 32.89 KB | | vip-pmeuinss-web.inss.gov.br | 32.21 KB | | | | **2.4 Usuário de VPN utilizado :** | | **Usuário VPN** | **IP VPN** | **Hostid (Palo Alto)** | | --- | --- | --- | | melissa.kreling@agu.gov.br | 10.253.1.38 | c97ef43e-af4d-49d4-8bae-776666810232 | | | | **2.5 Evidências coletadas (abaixo) :** | | | | Baixa reputação    Palo Alto – Atividade por IP de origem    Palo Alto - Actividade por Destination IP    Monitor > GlobalProtect | | | |

| 1. **Contenção, erradicação e recuperação** |
| --- |
| | **Contenção:** | Bloqueio de endereçamento IP  Data/hora: 23/11/2021 20:42 | | **Endereço IP ou subrede** | | --- | | 177.25.203.123 | | | --- | --- | --- | --- | --- | | **Comentários adicionais:** |  |  | | **Existe caso de reincidência?** | Houve reincidencia para o hostID c97ef43e-af4d-49d4-8bae-776666810232 | | | **Encaminhamento:** |  |  | |

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