A Importância da Conscientização dos Usuários na Prevenção de Incidentes de Segurança

RNP
ORGANIZAÇÃO SOCIAL DO MCTI

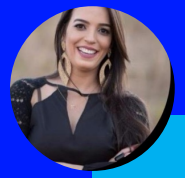
Educação, Pesquisa
e Inovação em Rede

CAIS

CERT.br – 11º Fórum Brasileiro de CSIRTs

31 de julho e 01 de agosto de 2023

Responsáveis



Andressa Cristina Borges Dutra Saberi

- Especialista em Segurança Cibernética, formação em Ciência da Computação pela Universidade Paulista.
- Analista de Segurança do CSIRT CAIS/RNP com foco em tratamento de incidentes desde 2021.

Jessica Araujo Silva Zanatta

- Formada em Segurança da Informação pela Faculdade de Tecnologia São Paulo (FATEC - Americana).
- Atua no CAIS/RNP como Analista de Segurança da Informação, com foco em tratamento de incidentes.

Matheus Nascimento de Camargo

- MBA em Cibersegurança (FIAP), formação em Redes de Computadores pela Universidade do Grande ABC.
- Atua na RNP desde 2015 e focado em segurança ofensiva no CAIS desde 2021 (RedTeam).

TLP:CLEAR

Agenda

RNP
ORGANIZAÇÃO SOCIAL DO MCTI

Educação, Pesquisa
e Inovação em Rede

- Sobre
- Objetivo
- Cenário do ataque
- Análise técnica
- Lições aprendidas

TLP:CLEAR

RNP

A rede brasileira para educação e pesquisa, trabalha para promover e implementar a inovação em aplicações de tecnologia da informação desde 1992, através da Internet.

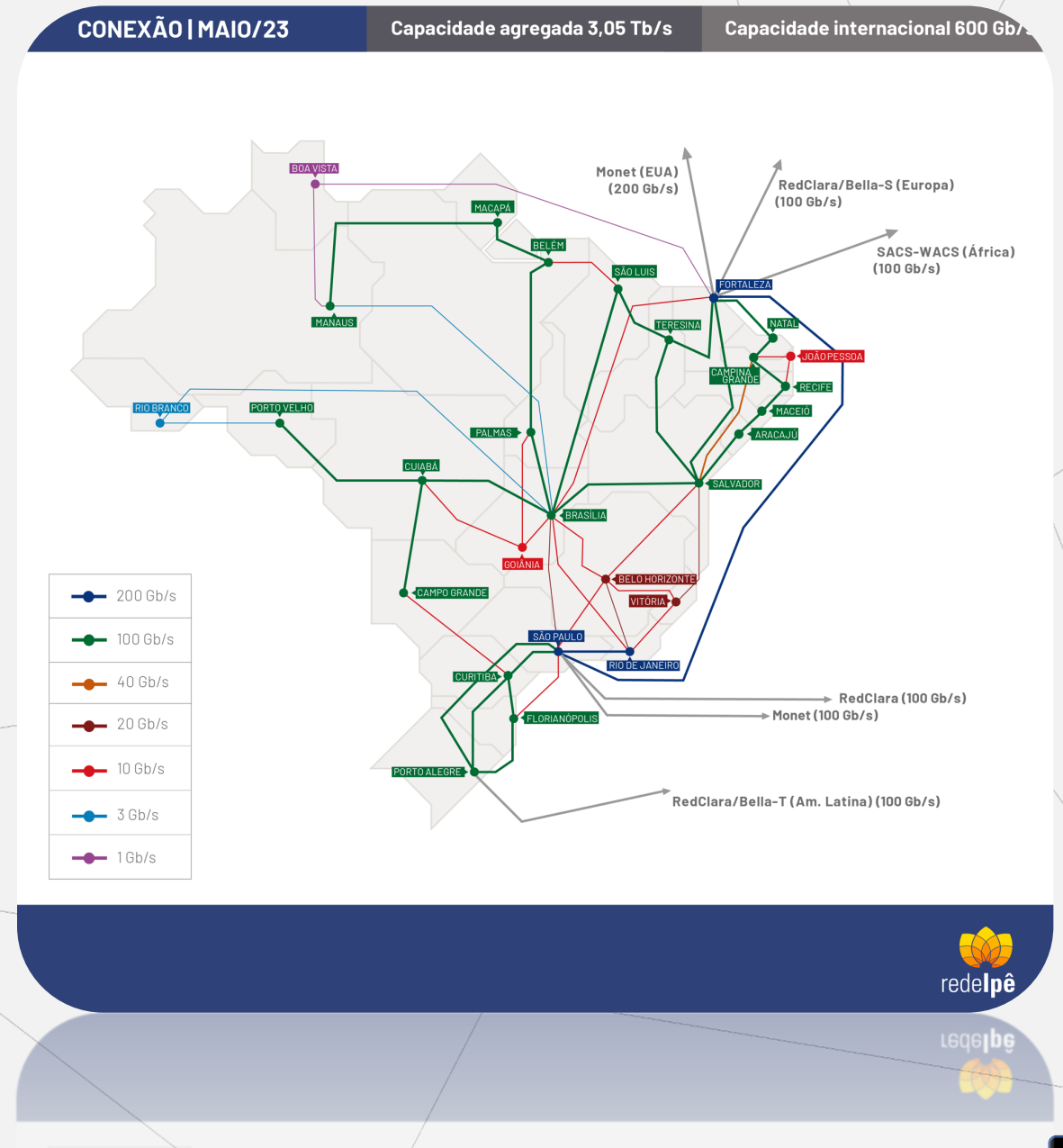
Atualmente conecta mais de 4 milhões de alunos, professores e pesquisadores, em institutos educacionais e culturais, agências de pesquisa, hospitais de ensino, parques e polos tecnológicos.

É uma Organização Social vinculada ao Ministério da Ciência, Tecnologia e Inovações (MCTI), em conjunto com os ministérios da Educação (MEC), das Comunicações (MCom), Saúde (MS) e Defesa (MD), além da Secretaria Especial da Cultura, vinculada ao Ministério do Turismo (SC/MTur), que participam do Programa Interministerial RNP (PRO-RNP).“

CAIS - CSIRT

Time de segurança da informação da RNP e CSIRT de Coordenação do Sistema RNP.

Com 26 anos de atuação, o CAIS foi um dos primeiros **grupos de resposta a incidentes de segurança** a nossa **MISSÃO** é atuar na detecção, resolução e prevenção de incidentes de segurança na rede acadêmica brasileira, além de elaborar, promover e disseminar práticas de segurança em redes.

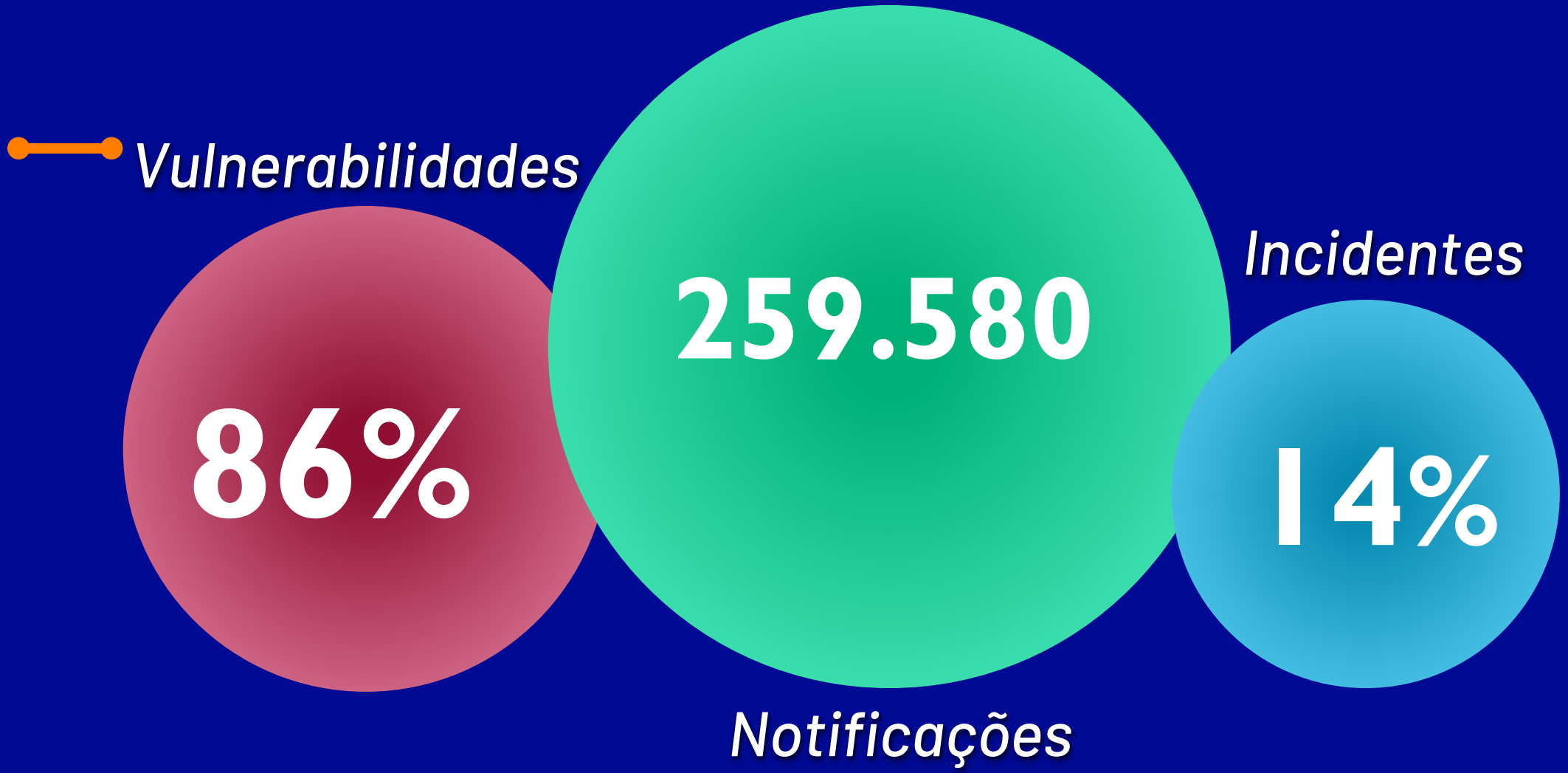


TLP:CLEAR

https://www.rnp.br/cais/25-

TLP:CLEAR

CAIS – Em números (2022)



Objetivo

A Importância da Conscientização dos Usuários na Prevenção de Incidentes de Segurança

O CAIS, Centro de Atendimento a Incidentes de Segurança da RNP, atuou em um recente caso de engenharia social envolvendo uma determinada instituição financeira. Durante o processo de resposta a incidente foi possível observar aspectos técnicos, operacionais e administrativos que poderiam ser melhorados do ponto de vista das equipes técnicas e do ponto de vista dos usuários.

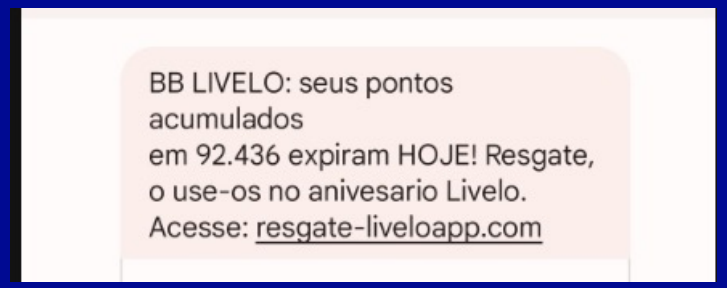
Objetivo

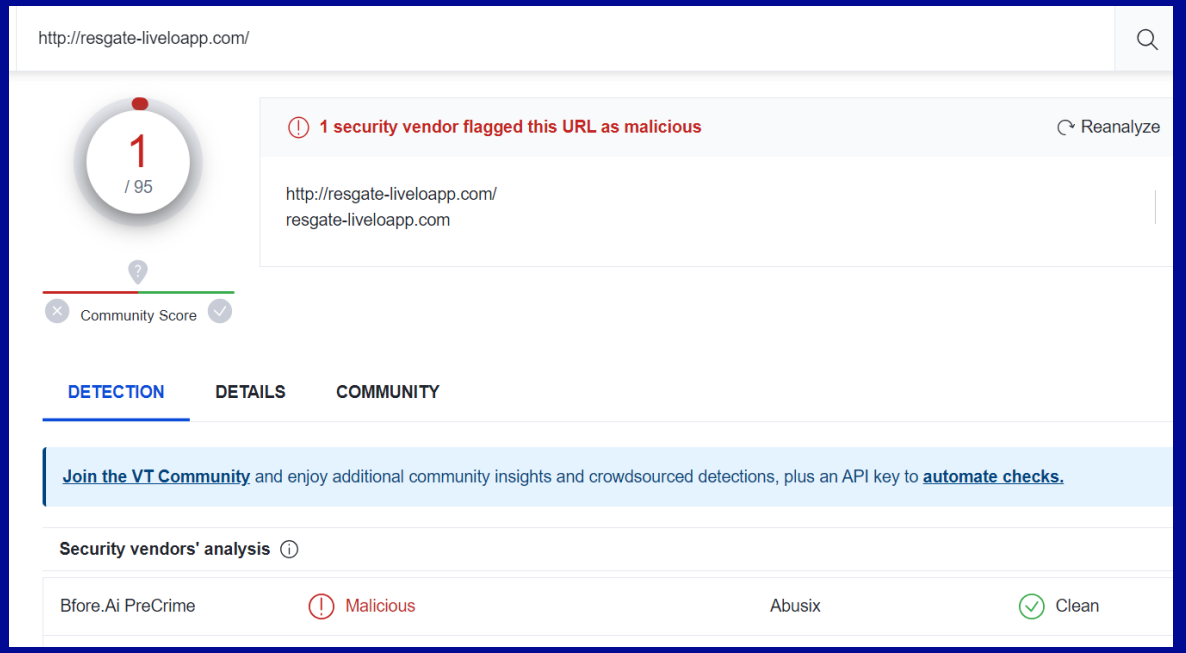
A palestra tem como objetivo compartilhar as etapas da análise do incidente que apresentou técnicas de smishing, falsas centrais de atendimento e interação direta com os usuários afetados, bem como apresentar as lições aprendidas, técnicas e administravas, fomentando a necessidade de conscientização dos usuários e equipes de TI por partes do CSIRTs.

TLP:CLEAR

Eventos

Smishing – Primeiro contato





https://www.virustotal.com/gui/url/380fbcdbd89b62a4f6d9be4c2f5c2260983e541e69b99cdcf3b051372c683c50/detection

TLP:CLEAR

Análise técnica

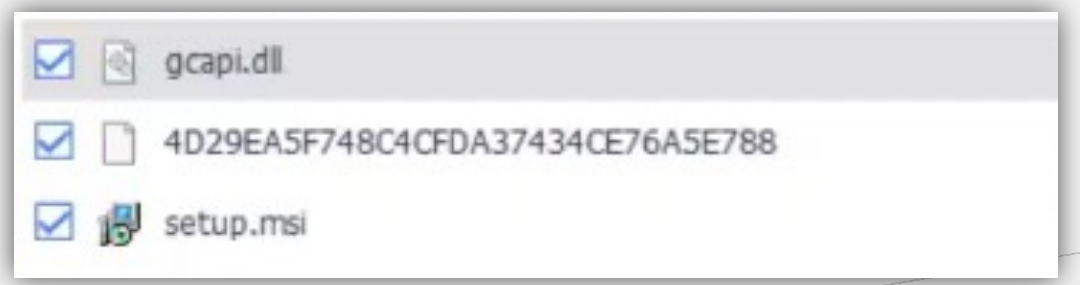
A análise realizada no ativo exposto teve por objetivo avaliar os seguintes pontos:

- Garantir que o ativo não esteja mais vulnerável;
- Análise do fluxo e escala do ataque;
- Obtenção de artefatos;

No segundo momento, realizamos análise em ambiente virtual controlado, com o intuito de:

- Analise do malware suspeito e seu comportamento;
- Por que o antivírus não notificou ou registrou em log a instalação do então possível malware?

Análise técnica - Artefatos



TLP:CLEAR

Análise técnica

Métodos utilizados para analise técnica:

- Visualizador de eventos do Windows 10;
- Gerenciador de Tarefas Windows: Processos/Desempenho/Histórico /usuários/detalhes/serviços;
- Power Shell – Análise de conexões;
- Antivírus SEP;
- Editor do Registro Windows;
- Vírus Total;
- VirtualBox;
- Máquina virtual com sistema Operacional Windows 10;
- Wireshark;
- Proccess Monitor;
- Regshot.

Análise técnica

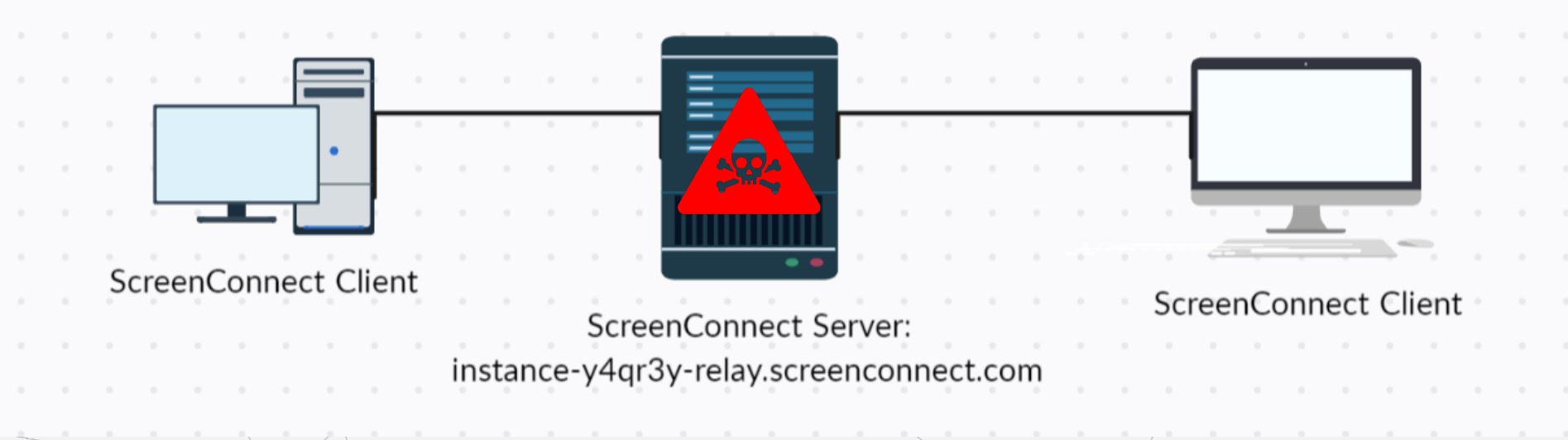
Mitigações :

- Reset de senha;
- Formatação do ativo;
- Conscientização.

Lições apreendidas

ScreenConnect - Características

- É um software de desktop remoto auto-hospedado;
- Assume privilégios do Sistema Operacional (SO);
- Seu processo não é finalizado por usuários sem privilégios;
- Inicializa junto ao SO, reestabelecendo comunicação junto ao Server.



TLP:CLEAR

Lições apreendidas

- Antivírus – Ausência de ‘report’ ou bloqueio por parte do antivírus corporativo: Como vimos o software instalado é um sistema licito, que os atacantes utilizam para transpassar algumas barreiras de defesa, incluindo o antivírus.

CAIS – Ações de Conscientização

Onboarding

Atividade para os novos colaboradores, junto ao processo de integração ao RH.

Campanhas phishing

Envio de e-mail falso para verificar nível de maturidade coorporativo com relação a e-mails maliciosos.

Gamificação

Metodologia com conceitos de jogos em um contexto não-jogo, facilitando o aprendizado, engajamento e motivação em mudanças de comportamento.

Café da Segurança

Encontro da equipe de segurança com outras área, para compreender seus processos e promover SI alinhada a necessidade de cada área.

CAIS – Ações de Conscientização

CISA

Há diversos relatos de utilização indevida deste software no auxilio a ataques e propagação de ransomware.

Em Janeiro de 2023 a CISA (Cybersecurity & Infrastructure Security Agency) publicou um alerta referente ao uso do ScreenConnect e outras soluções que estão sendo objeto de ações maliciosas.

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

AMERICA'S CYBER DEFENSE AGENCY

Search

Topics | Spotlight | Resources & Tools | News & Events | Careers | About

Home / News & Events / Cybersecurity Advisories / Cybersecurity Advisory

CYBERSECURITY ADVISORY

Protecting Against Malicious Use of Remote Monitoring and Management Software

Last Revised: January 26, 2023 **Alert Code:** AA23-025A

Summary

The Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), and Multi-State Information Sharing and Analysis Center (MS-ISAC) (hereafter referred to as the "authoring organizations") are releasing this joint Cybersecurity Advisory (CSA) to warn network defenders about malicious use of legitimate remote monitoring and management (RMM) software. In October 2022, CISA identified a widespread cyber campaign involving the malicious use of legitimate RMM software. Specifically, cyber criminal actors sent phishing emails that led to the download of legitimate RMM software—ScreenConnect (now ConnectWise Control) and AnyDesk—which the actors used in a refund scam to steal money from victim bank accounts.

https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-025a

TLP:CLEAR

Catalogo de fraudes

Serviço de Catálogo de Fraudes catálogo é um repositório de mensagens classificadas como fraudulentas, servindo como uma fonte de informação que auxilia a não propagação de fraudes disseminadas por email e fornecendo informações sobre como se proteger desse tipo de golpe.

- Reporte de mensagens suspeitas
- E-mail: phishing@cais.rnp.br
- https://catalogodefraudes.rnp.br

OBRIGADA

Palestrantes:
Andressa Cristina Borges Dutra Sahori
andressa.sahori@terceiro.rnp.br

Matheus Nascimento de Camargo
matheus.camargo@rnp.br

Jessica Araujo Silva Zanatta
jessica.zanatta@rnp.br