Ataque hacker na justiça do trabalho

- Invasões por cibercriminosos e seus efeitos na JT
- Entenda os casos reais e como se prevenir

Conteúdo

- Casos reais;
- Principal ameaça, sua forma de atuação e as possíveis consequências;
- Prevenção no dia a dia;
- Ações que o TRT24 está tomando para não se tornar vítima;

Casos reais de ataques na justiça do trabalho

PF investiga ataque hacker ao TRT-ES; alguns serviços seguem suspensos

O ataque cibernético foi identificado no dia 20 de fevereiro. Por causa disso, audiências e prazos processuais da Justiça do Trabalho seguem suspensos

Tempo de leitura: 2min

Isaac Ribeiro | Repórter
iribeiro@redegazeta.com.br

Publicado em 11/03/2022 às 17h20

Sistema do TRT-RS é alvo de ataque hacker

Corte afirma que não há indícios de comprometimento ou vazamento dos dados processuais e pessoais

04/10/2021 - 12h11min

COMPARTILHE:

EDUARDO MATOS
Enviar E-mail

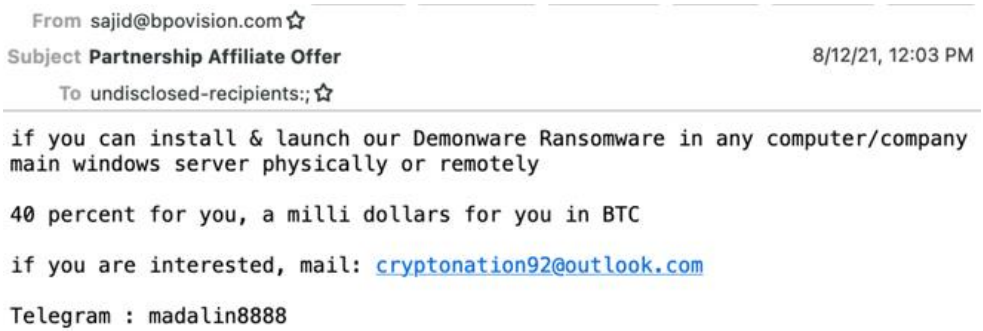
Hackers invadem sessão do TRT-20 e tocam funk obsceno e "gemidão"

Sessão foi interrompida após a invasão. "Autoridades policiais serão devidamente notificadas", informou o TRT-20, em nota

Principal ameaça

- Ramsonware (sequestro de dados).
- Virou um negócio (ramsonware-as-a-service);
- Existem várias gangues de ransomware que desenvolvem e vendem os serviços na DarkWeb;

- Exemplo de recrutamento de afiliados;


From sajid@bpovision.com
Subject **Partnership Affiliate Offer** 8/12/21, 12:03 PM
To undisclosed-recipients:;

if you can install & launch our Demonware Ransomware in any computer/company main windows server physically or remotely

40 percent for you, a milli dollars for you in BTC

if you are interested, mail: cryptonation92@outlook.com

Telegram : madalin8888

RAMSONWARE-AS-A-SERVICE

[Ransomware] LockBit 2.0 is an affiliate program.

Affiliate program LockBit 2.0 temporarily relaunch the intake of partners.

The program has been underway since September 2019, it is designed in origin C and ASM languages without any dependencies. Encryption is implemented in parts via the completion port (I/O), encryption algorithm AES + ECC. During two years none has managed to decrypt it.

Unparalleled benefits are encryption speed and self-spread function.

The only thing you have to do is to get access to the core server, while LockBit 2.0 will do all the rest. The launch is realized on all devices of the domain network in case of administrator rights on the domain controller.

Ramsonware-as-a-service

Ransomware as a Service - HimalayA

We offer ransomware for free!
We take a commission of 30% of all ransoms paid
We send the part of your ransom maximum 24 hours after confirmation of the transaction
We manage communication with victims

VERY IMPORTANT WARNING :
PROHIBITION OF ATTACKING HEALTH FACILITIES
PROHIBITION OF ATTACKING ANY PUBLIC ORGANIZATION OR NON-PROFIT ASSOCIATION
ONLY ATTACK PRIVATE COMPANIES OR INDIVIDUALS

Already configured and compiled FUD Ransomware.
AES 256 Encryption
x86 / x64 for Windows

Vetores de ataque

Os principais vetores de ataque usados são:

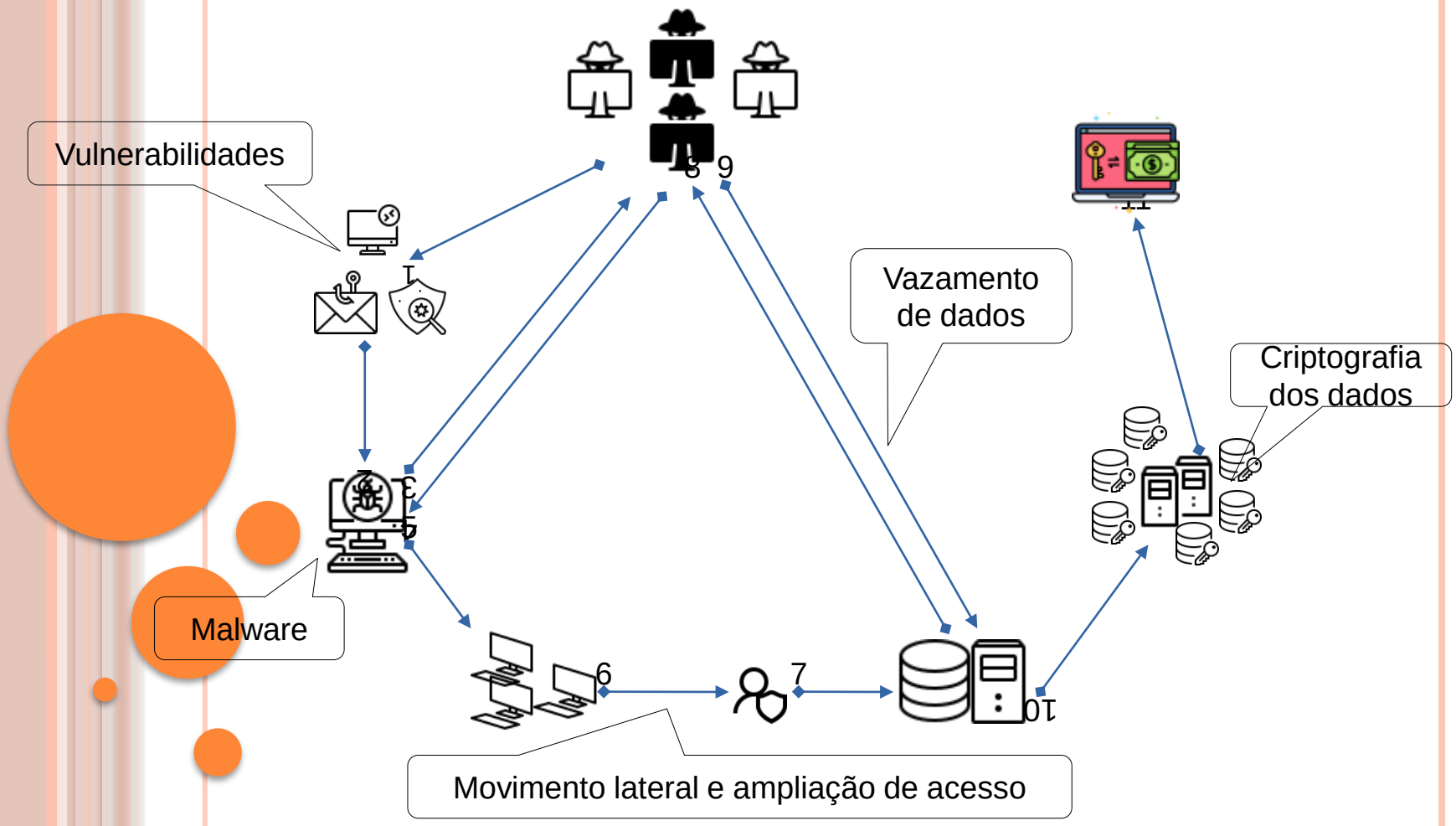
- RDP = Conexão com área de trabalho remota.
- Phishing = E-mail falso com objetivo de obter informações confidenciais, como login e senha.
- Vulnerabilidades de software = software com brecha de segurança não corrigida.

- Tendência de aumento de vishing (phishing por voz) combinado com outras técnicas para dar mais credibilidade.

Fases do ataque ransomware

1) Acesso inicial: envolve vetores de acesso inicial como phishing, exploração de vulnerabilidades e Remote Desktop Protocol estabelecendo acesso persistente.
2) Pós-exploração: implanta uma ferramenta de acesso remoto ou malware para estabelecer o acesso interativo.
3) Compreensão e ampliação: triagem do sistema local e ampliação do acesso para movimentação lateral.
4) Coleta e exfiltração de dados: identificando dados valiosos e exfiltrando-os.
5) Implantação de ransomware: distribuição de carga útil de ransomware (criptografia dos dados).

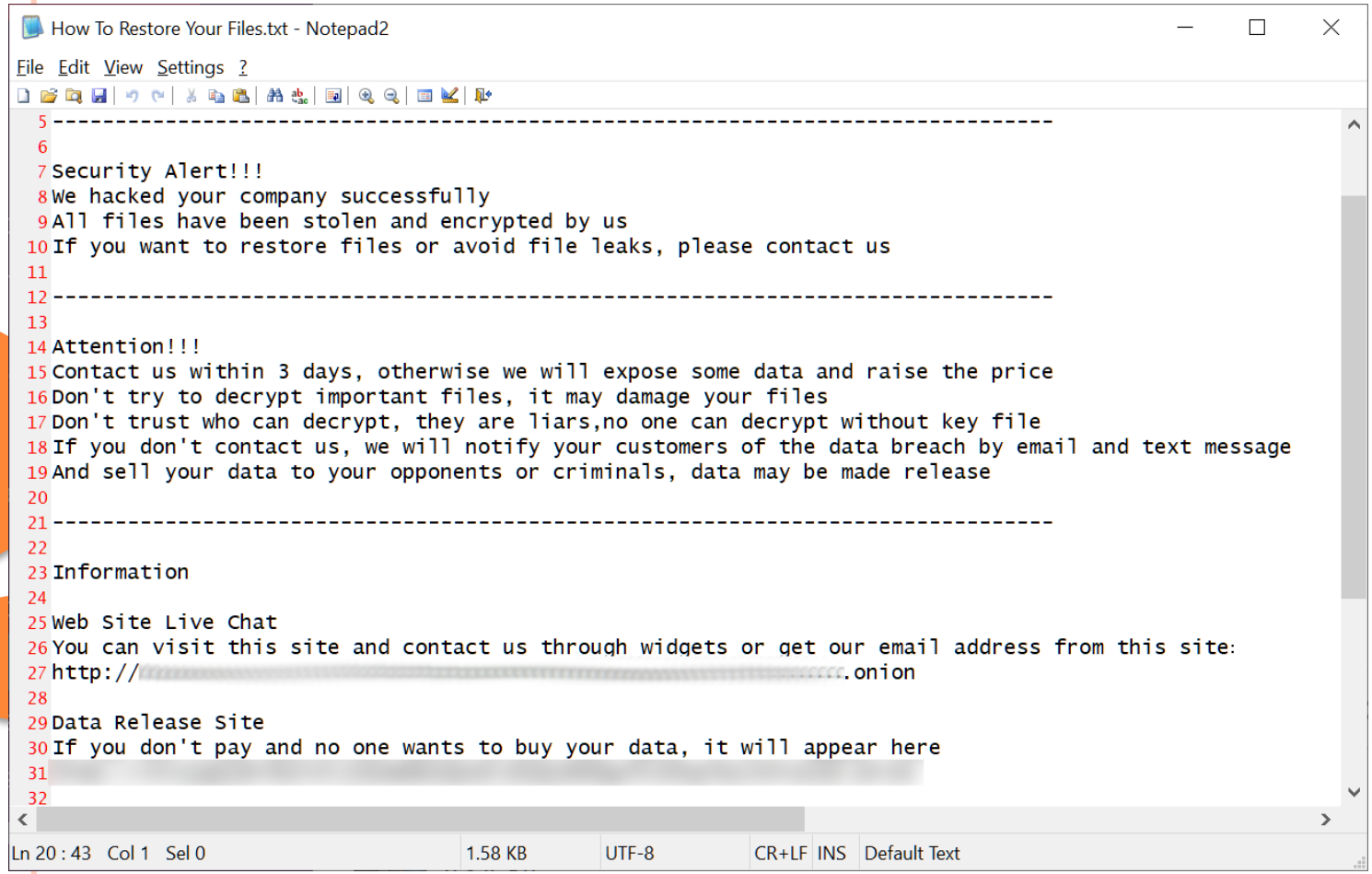
Fases do ataque ransomware



Fases do ataque ransomware

RESGATE RANSOMWARE

RESGATE RANSOMWARE



Características dos ataques à JT

- Ramsonware;
- Utilizaram phishing;
- Explorou vulnerabilidade no Gabinete Virtual;
- Atacantes ficaram semanas dentro do ambiente da organização entre a invasão inicial até criptografia dos dados;
- Atacantes trabalhavam no período noturno;
- Senha de 8 dígitos foi quebrada poucas horas;
- Dados foram criptografados;
- Banco de dados não foi atingido;

Ações em caso de ataque

- Equipe de Tratamento e Resposta a Incidentes (ETIR);
- Acionamento da PF;
- Busca de ajuda com empresas experientes;
- Isolamento do ambiente;
- Grupo de Gestão de Crise de Cibernética (GGCC);
- Comunicação interna e externa;
- Transparência;
- Análise da extensão do ataque;
- Restauração do ambiente;

Ações em caso de ataque

- Isolamento do ambiente: para interromper a comunicação com o atacante e conter a propagação do vírus;
- Análise da extensão do ataque: verificação de integridade dos dados nos diversos sistemas como servidores de rede, bancos de dados, backups, etc.
- Análise de logs de atividades: verificação dos arquivos de log de atividades dos sistemas para rastrear as ações do atacante.
- Preservação do ambiente: preservação para análise forense da PF.
- Restauração dos serviços;

Recuperação e restabelecimento dos sistemas

- Análise da disponibilidade de equipamentos para recuperação: quais equipamentos podem ser utilizados sem que interfira na investigação Policial.
- Restauração dos dados: backup em disco, nuvem, fita de backup.
- Recuperação dos servidores de rede e aplicações: restauração de backup ou instalação e reconfiguração dos sistemas.

CONSEQUÊNCIAS

- Sistemas ficaram fora por mais de 20 dias;
- Sistemas em plataformas conhecidamente vulneráveis não voltarão a ser publicados;
- Implantação de Segundo Fator de Autenticação (2FA) em todos os serviços;
- Grandes prejuízos financeiros;
- Prejuízo à imagem da instituição;
- Sobrecarga de trabalho;
- Estresse nas equipes envolvidas;

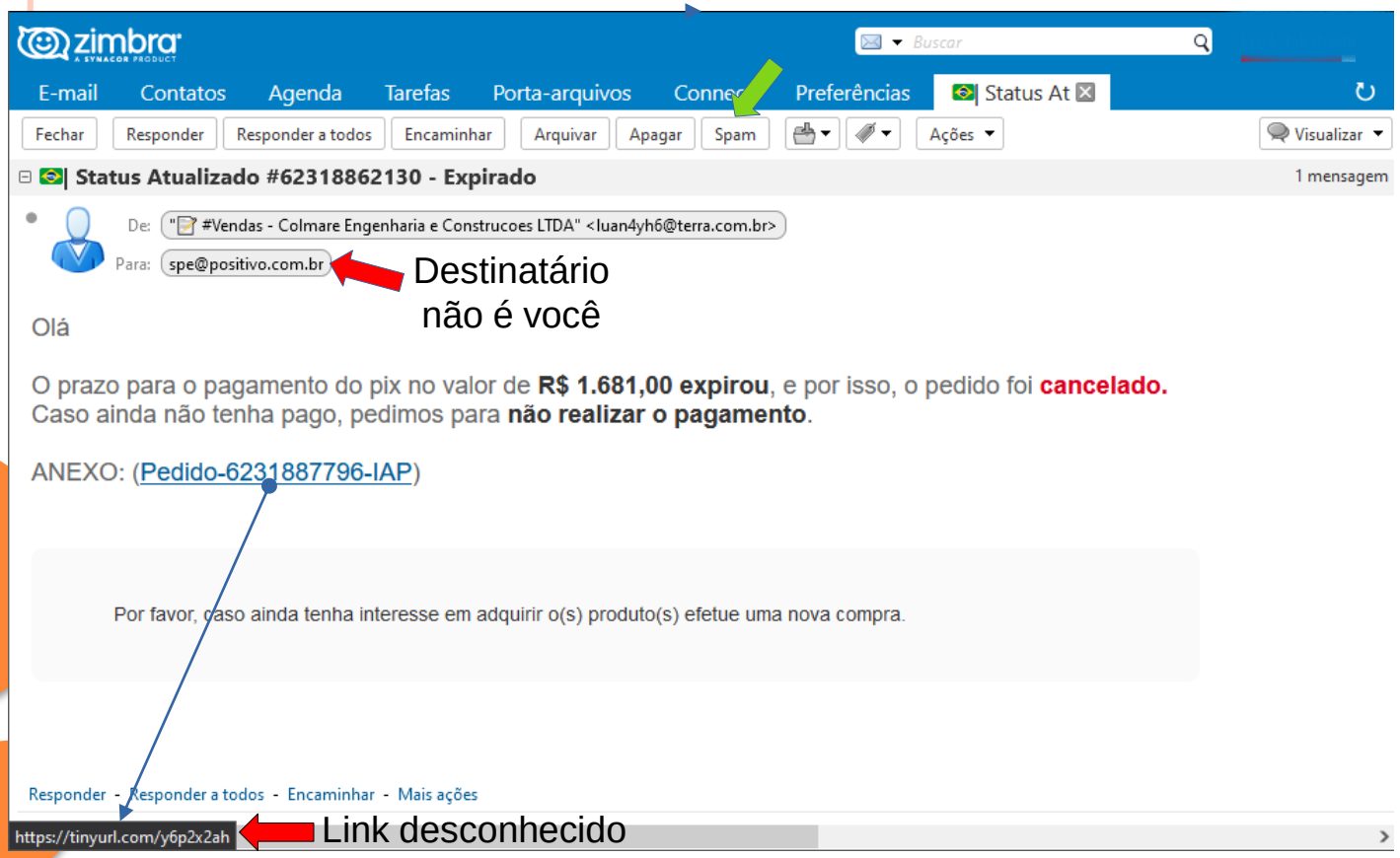
Prevenção

- Palestras;
- Campanhas;
- Treinamentos;
- Revisão das políticas;
- Contratação de serviços especializados;

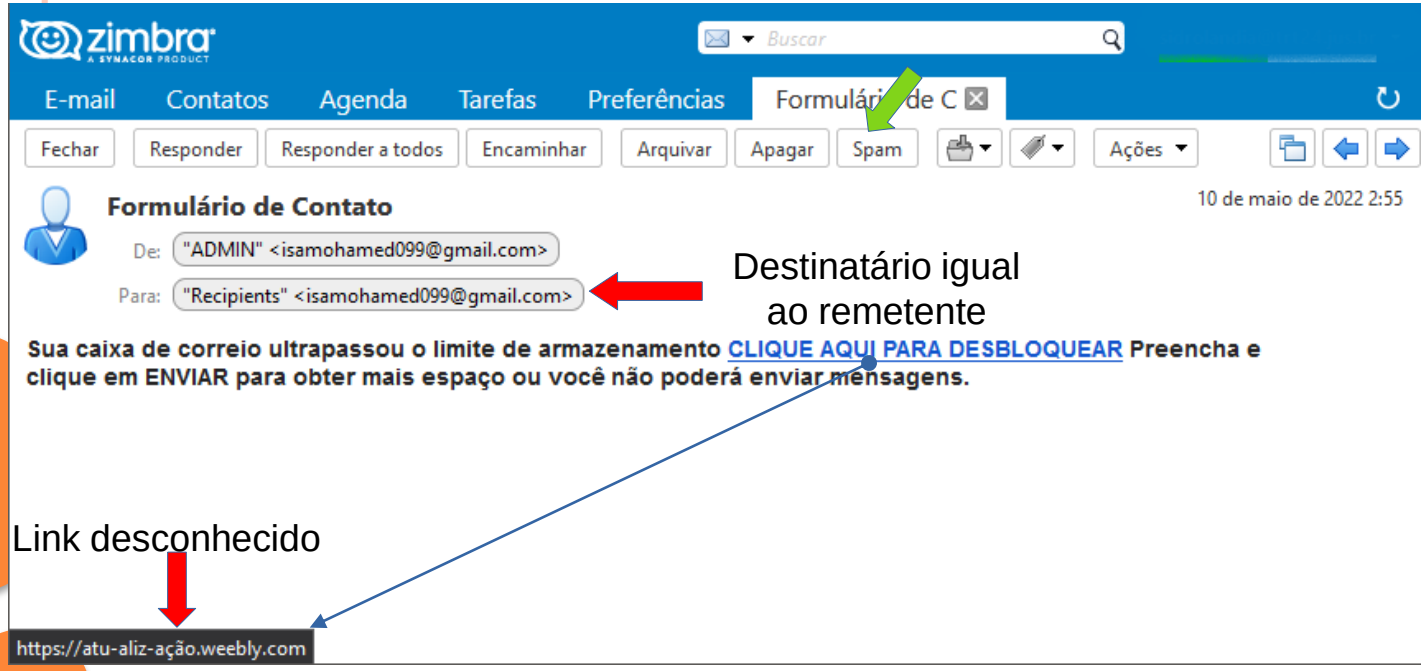
Prevenção no dia a dia

- Cuidado com e-mails suspeitos;
- Cuidado com anexos suspeitos;
- Cuidado com arquivos suspeitos;
- Cuidado com telefonemas suspeitos;
- Utilização de senhas fortes;
- Utilização segundo fator de autenticação (2FA);
- Manter softwares atualizados;

PREVENÇÃO NO DIA A DIA



Prevenção no dia a dia



Prevenção no dia a dia

Antivírus desativado

Antivírus desatualizado

Antivírus ativo

Reinicialização necessária para instalar atualizações do Windows

Indicação de leitura

- Golpes:
- Whatsapp;
- Instagram;
- Instituições financeiras;
- Pix;
- E-mail;
- Compras na internet;
- Boletos;
- Relacionamento;
- Criptomoedas;
- Outros.

Ações realizadas nos últimos 12 meses

- Varredura de vulnerabilidades em parceria com TJ-MS;
- Migração para novo software antivírus;
- Atualizações de softwares de infraestrutura;
- Bloqueio de acesso ao Gabinete Virtual;
- Bloqueio de acesso de softwares de desenvolvimento;
- Vigilância do servidor de e-mails;

Ações em andamento

- Mapeamento de riscos críticos;
- Atualização do Windows;
- Revisão de políticas de antivírus;
- Revisão de políticas de acesso privilegiado;
- Cancelamento de páginas do antigo portal;
- Gerenciamento de vulnerabilidades;
- Troca de experiências com outros TRTs;
- Contratação de software de proteção de dados não estruturados e em nuvem;
- Aquisição de software de gerenciamento de acesso privilegiado;

Preparação para incidente catastrófico

- Revisão de rotinas de backup;
- Aquisição de novo software de backup;
- Atualização de políticas e manuais de restauração;
- Parceria com TRE-MS para abrigar o site backup;

Próximas Ações

- Mudança de senha: senhas trocadas na última campanha expirarão 30/06/2022;
- Utilizar senha forte de no mínimo 12 dígitos: novo requisito mínimo (outros requisitos continuam valendo);
- Proteção de notebooks: alteração de configurações para proteção e controle dos equipamentos (abrir Siate até dia 13/07/2022);
- Proteção da intranet: exigência de conexão VPN para acesso (Recuperação de senha terá novo endereço e Holerit deverá ser acessados no Sigep-Online);

Referências

Ramsonware

- https://itforum.com.br/noticias/ransomware-e-o-principal-tipo-de-ataque-cibernetico-enquanto-manufatura-e-a-mais-atingida/
- https://www.kaspersky.com.br/resource-center/threats/ransomware-attacks-and-types
- https://www.uol.com.br/tilt/noticias/redacao/2022/06/09/ransomware-o-que-e-e-por-que-esta-na-modo-o-sequestro-de-dados-e-sistemas.htm
- https://www.cisoadvisor.com.br/prejuizo-em-ataque-pode-custar-7-vezes-o-valor-do-resgate/

Phishing

- https://prodest.es.gov.br/entenda-o-que-e-phishing-e-adote-medidas-para-evita-lo
- https://www.avast.com/pt-br/c-phishing

Gerenciades de senhas

- https://tecnoblog.net/responde/10-aplicativos-gerenciadores-de-senhas/
- https://www.tecmundo.com.br/seguranca/216650-10-gerenciadores-senhas-gratuitos.htm
- https://www.uol.com.br/tilt/noticias/redacao/2021/08/25/gerenciador-de-senhas-veja-5-aplicativos-para-voce-usar.htm

Dúvidas?

SETIC

Seção de Proteção de Dados e Segurança da Informação

Contatos: spdseg@trt24.jus.br

- etakahashi@trt24.jus.br
- geslaine@trt24.jus.br
- fnsilva@trt24.jus.br