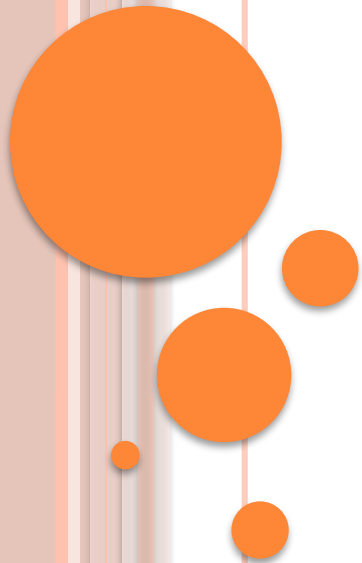


ATAQUE HACKER NA JUSTIÇA DO TRABALHO

- 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 TRI-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

CONDITIONS FOR PARTNERS

[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

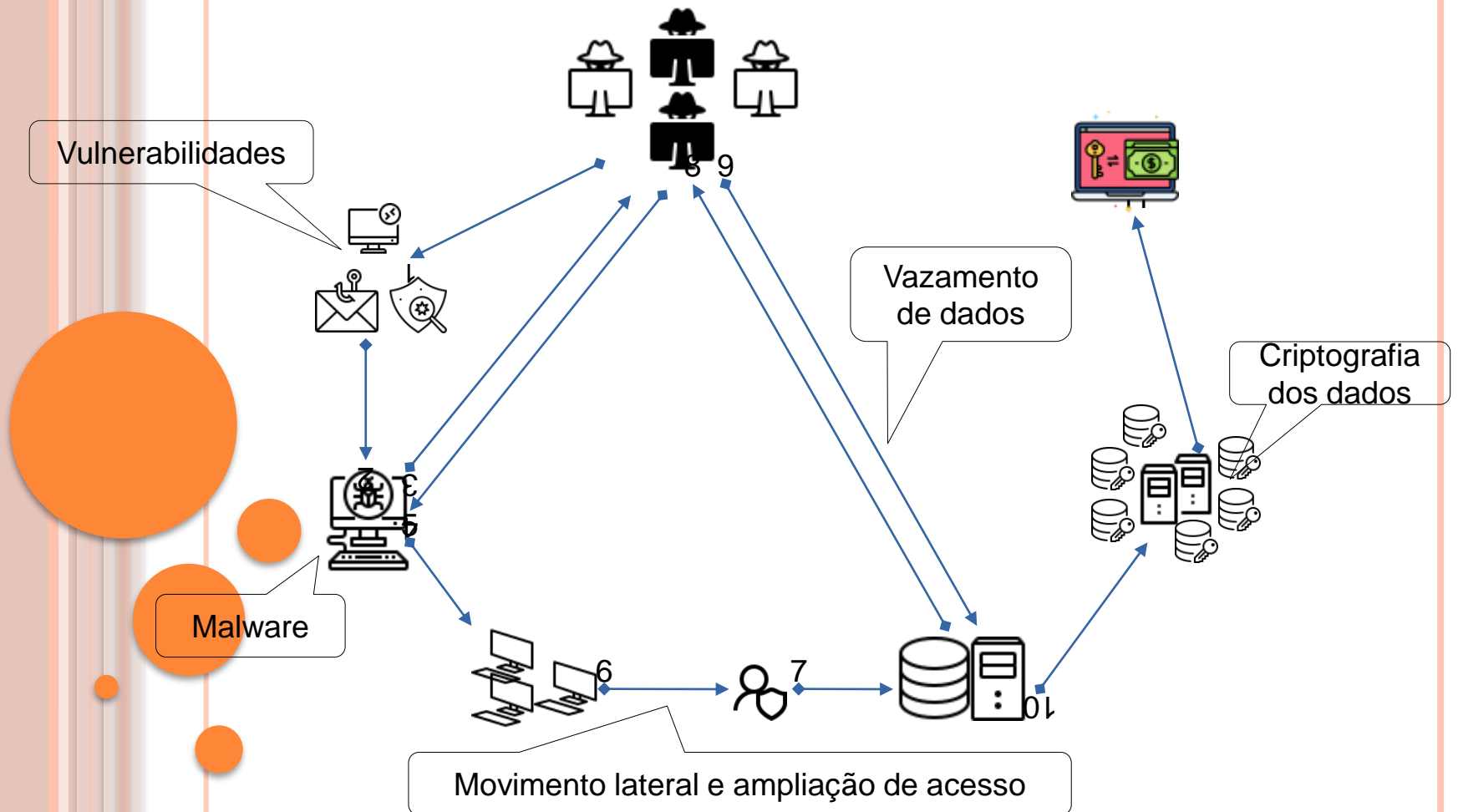
Os principais vetores de ataque usados são:

- 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

Wana Decrypt0r 2.0

English



What Happened to My Computer?

Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Payment will be raised on
5/15/2017 16:32:52
Time Left
02:23:59:49

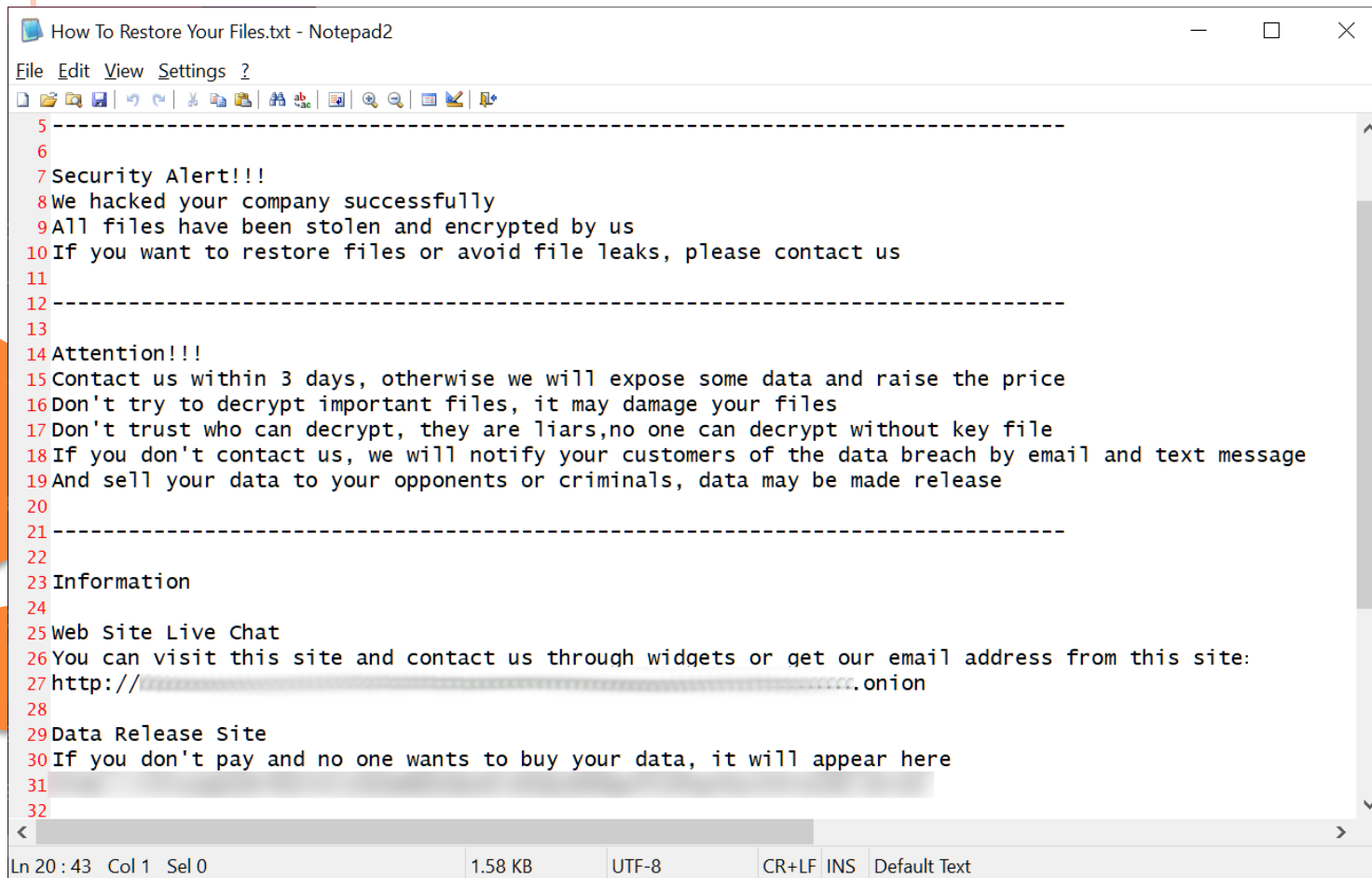
Your files will be lost on
5/19/2017 16:32:52
Time Left
06:23:59:49

[About bitcoin](#)
[How to buy bitcoins?](#)
[Contact Us](#)

Send \$300 worth of bitcoin to this address:

 **12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw**

RESGATE RANSOMWARE



The image shows a Notepad2 window titled "How To Restore Your Files.txt - Notepad2". The window contains a ransomware message with the following text:

```
5 -----  
6  
7 Security Alert!!!  
8 We hacked your company successfully  
9 All files have been stolen and encrypted by us  
10 If you want to restore files or avoid file leaks, please contact us  
11  
12 -----  
13  
14 Attention!!!  
15 Contact us within 3 days, otherwise we will expose some data and raise the price  
16 Don't try to decrypt important files, it may damage your files  
17 Don't trust who can decrypt, they are liars, no one can decrypt without key file  
18 If you don't contact us, we will notify your customers of the data breach by email and text message  
19 And sell your data to your opponents or criminals, data may be made release  
20  
21 -----  
22  
23 Information  
24  
25 Web Site Live Chat  
26 You can visit this site and contact us through widgets or get our email address from this site:  
27 http://[REDACTED].onion  
28  
29 Data Release Site  
30 If you don't pay and no one wants to buy your data, it will appear here  
31 [REDACTED]  
32
```

The status bar at the bottom of the window shows: Ln 20 : 43 Col 1 Sel 0 1.58 KB UTF-8 CR+LF INS Default Text

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

zimbra
A SYMAGOR PRODUCT

Buscar

E-mail Contatos Agenda Tarefas Porta-arquivos Conectar Preferências Status At

Fechar Responder Responder a todos Encaminhar Arquivar Apagar Spam Ações Visualizar

Status Atualizado #62318862130 - Expirado 1 mensagem

De: "#Vendas - Colmare Engenharia e Construcoes LTDA" <luan4yh6@terra.com.br>

Para: spe@positivo.com.br **Destinatário não é você**

Olá

O prazo para o pagamento do pix no valor de **R\$ 1.681,00 expirou**, e por isso, o pedido foi **cancelado**.
Caso ainda não tenha pago, pedimos para **não realizar o pagamento**.

ANEXO: ([Pedido-6231887796-IAP](#))

Por favor, caso ainda tenha interesse em adquirir o(s) produto(s) efetue uma nova compra.

Responder - Responder a todos - Encaminhar - Mais ações

<https://tinyurl.com/y6p2x2ah> **Link desconhecido**

PREVENÇÃO NO DIA A DIA

The screenshot shows the Zimbra web interface. At the top, there is a search bar with the text "Buscar" and a magnifying glass icon. Below the search bar is a navigation menu with tabs for "E-mail", "Contatos", "Agenda", "Tarefas", "Preferências", and "Formulário de C" (with a close icon). A green arrow points to the "Formulário de C" tab. Below the navigation menu is a toolbar with buttons for "Fechar", "Responder", "Responder a todos", "Encaminhar", "Arquivar", "Apagar", "Spam", a printer icon, a pencil icon, and "Ações". To the right of the toolbar are icons for "Imprimir", "Voltar", and "Avançar".

The email header shows the sender as "ADMIN" <isamohamed099@gmail.com> and the recipient as "Recipients" <isamohamed099@gmail.com>. A red arrow points from the text "Destinatário igual ao remetente" to the recipient's email address. The date and time are "10 de maio de 2022 2:55".

The main body of the email contains a warning: "Sua caixa de correio ultrapassou o limite de armazenamento [CLIQUE AQUI PARA DESBLOQUEAR](#) Preencha e clique em ENVIAR para obter mais espaço ou você não poderá enviar mensagens." A blue arrow points from this text to the URL "https://atu-aliz-ação.weebly.com" at the bottom of the email. A red arrow points from the text "Link desconhecido" to the URL.

Destinatário igual ao remetente

Link desconhecido

<https://atu-aliz-ação.weebly.com>

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

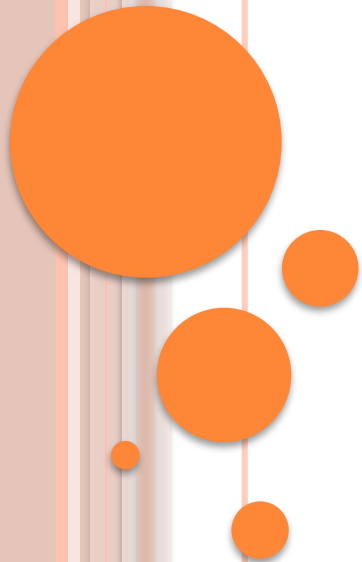
- Varredura de vulnerabilidades em parceria com TJ-MS;
- Migração para novo software antivírus;
- Atualizações de softwares de infraestrutura;
- Bloqueio de acesso ao Gabinete Virtual;
- Bloqueio de acesso de softwares de desenvolvimento;
- Vigilância do servidor de e-mails;

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 expiração 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