TJCE
Tribunal de Justiça
do Estado do Ceará

Corregedoria Geral da Justiça

Ofício Circular nº 118/2024 – CGJUCGJ

Fortaleza, data da assinatura digital.

Aos(as) Excelentíssimos(as) Senhores(as) Juízes(as) Corregedores(as) Permanentes do Estado do Ceará
Aos(as) Senhores(as) Notários(as) e Registradores(as) do Estado do Ceará

Assunto: Suposta falsificação de documentos

Excelentíssimos(as) Senhores(as),

Com os cumprimentos de estilo, venho por meio deste, COMUNICAR ao público em geral e às autoridades interessadas, especialmente aos(às) Excelentíssimos(as) Senhores(as) Juízes(as) Corregedores(as) Permanentes, bem como aos(às) Senhores(as) Notários(as) e Registradores(as) das Serventias Extrajudiciais do Estado do Ceará, o inteiro teor do Ato Ordinatório (Id. 4037032) oriundo do Poder Judiciário de Santa Catarina, a respeito de possível extravio de dados eletrônicos do 1° Tabelionato de Notas e de Protesto de Títulos da Comarca de Blumenau/SC, em decorrência de ataque cibernético (Ransonware).

Atenciosamente,

Desembargadora Maria Edna Martins
Corregedora-Geral da Justiça do Estado do Ceará

Avenida General Afonso Albuquerque Lima, s/n, Cambeba, Fortaleza CE, 60822-325, Brasil, 85 3108 1573, cgj.extrajudicial@tjce.jus.br

Autos SEI n. 0012627-60.2024.8.24.0710 - Providências

TJSC/Divisão Administrativa <cgj@tjsc.jus.br>

Qui, 07/03/2024 13:20

Para:Corregedoria Alagoas <chefia_cgj@tjal.jus.br>;TJAP - Corregedoria <corregedoria@tjap.jus.br>;Corregedoria Amazonas <protocolo.corregedoria@tjam.jus.br>;TRIBUNAL DE JUSTIÇA DO ESTADO DO CEARÁ - CORREGEDORIA <corregedoria@tjce.jus.br>;Corregedoria Espírito Santo <gabinete@tjes.jus.br>;Corregedoria Goiás <corregsec@tjgo.jus.br>;Corregedoria Maranhão <chefgab_cgj@tjma.jus.br>;Corregedoria Mato Grosso <coordenadoria.corregedoria@tjmt.jus.br>;Corregedoria Mato Grosso do Sul <corregedoria@tjms.jus.br>;Corregedoria Minas Gerais <gacor@tjmg.jus.br>;Corregedoria Paraíba <cgj.protocolo@tjpb.jus.br>;Corregedoria Paraná <sei@tjpr.jus.br>;Corregedoria Pernambuco <corregedoria@tjpe.jus.br>;Corregedoria Piauí <corregedoria@tjpi.jus.br>;Corregedoria Rio de Janeiro <cgjdipac@tjrj.jus.br>;Corregedoria Rio Grande do Norte <corregedoria@tjrn.jus.br>;Corregedoria Rio Grande do Sul <cgj@tjrs.jus.br>;Corregedoria Rondônia <cgj@tjro.jus.br>;Corregedoria Roraima <corregedoria@tjrr.jus.br>;Corregedoria São Paulo <corregedoria@tjsp.jus.br>

5 anexos (2 MB)

Ato_Ordinatorio_7990630.pdf; Comprovante_7984223_1___Comprovante.pdf; Expediente_7984226_2___Expediente.pdf; Oficio_7984231_3___Oficio_n._011_2024.pdf; Relatorio_7984251_4___Relatorio_de_incidente_de_seguranca.pdf;

Excelentíssimos(as) Senhores(as) Corregedores(as),

Por solicitação do Núcleo IV da Corregedoria-Geral do Foro Extrajudicial, encaminho o expediente anexo para as providências que entenderem necessárias.

Respeitosamente,

Seção Expediente
Divisão Administrativa

_____

Corregedoria-Geral da Justiça
Tribunal de Justiça de Santa Catarina

ESTADO DE SANTA CATARINA
PODER JUDICIÁRIO

ATO ORDINATÓRIO

Extrajudicial/Comunicação de interesse geral n. 0012627-60.2024.8.24.0710

Unidade: Núcleo IV - Extrajudicial

Assunto: Ataque cibernético - possível extravio de dados - comunicação

Trata-se de procedimento administrativo de comunicação de interesse geral instaurado em razão do Ofíco de n. 11/2024, proveniente do 1º Tabelionato de Notas e de Protesto de Títulos da Comarca de Blumenau, deste Estado de Santa Catarina, por meio do qual comunica o possível extravio de dados eletrônicos da serventia em decorrência de ataque cibernético sofrido, diante de vulnerabilidade do sistema de automação utilizado. Tão logo identificado o ataque, os sevidores da serventia foram derrubados, para fins de análise da extensão dos possíveis danos e reestabelecimento seguro da atividade extrajudicial, o qual ocorreu no mesmo dia, sem qualquer perda de informações/dados (docs. ns. 7984231 e 7984251).

Nos termos do artigo 54 do Regimento Interno da Corregedoria-Geral da Justiça, bem como da Ordem de Serviço n. 4 (SEI 0014940-62.2022.8.24.0710), que delega atribuições de atos ordinatórios aos servidores do Núcleo IV (Extrajudicial), encaminho os autos à Divisão Administrativa para que se dê conhecimento do fato ocorrido às Corregedorias dos demais Estados da Federação, para cumprimento do artigo 132 do Novo Código de Normas desta Corregedoria-Geral do Foro Extrajudicial.

Ad cautelam, intime-se o interino responsável pela serventia extrajudicial, ora comunicante, para que, no prazo de 10 (dez) dias, demonstre o cumprimento do art. 132 do CNCGFE, *in verbis: O notário ou registrador deverá comunicar ao Corregedor-Geral do Foro Extrajudicial e* ***às demais serventias extrajudiciais do Estado, por meio do Sistema Hermes – Malote Digital, situações de interesse geral****, não alcançados por central de informações especializada, tais como: I – extravio de livros relacionados às atividades notariais e registrais [...]****.***

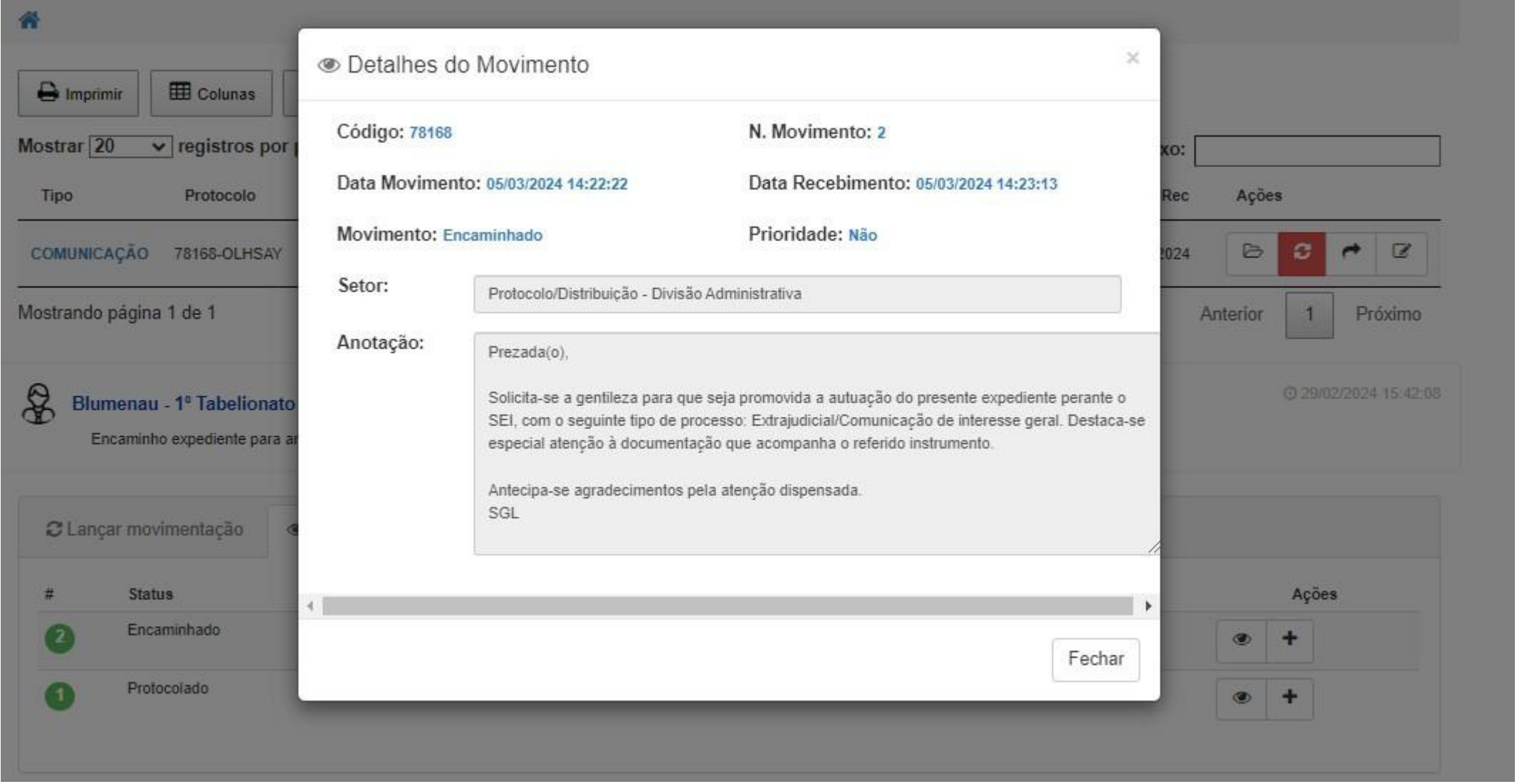
Na oportunidade, importante esclarecer que qualquer informação relacionada a esse assunto deverá ser encaminhada diretamente ao comunicante.

Comprovado o cumprimento do disposto pelo art. 132 do CNCGFE pelo responsável da serventia extrajudicial, convém registrar ser desnecessária a comunicação acerca de outras medidas adotadas.

Cumprida a determinação, a tramitação processual deverá ser encerrada nesta unidade.

Documento assinado eletronicamente por **Lucas Nicolau Guimaraes**, **Assessor Correicional**, em 06/03/2024, às 18:46, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site http://sei.tjsc.jus.br/verificacao informando o código verificador **7990630** e o código CRC **C09383B1**.


Imprimir
Colunas
Mostrar 20 registros por
Tipo
Protocolo
Rec
Ações
COMUNICAÇÃO
78168-OLHSAY
Mostrando página 1 de 1
Anterior
1
Próximo
Blumenau - 1º Tabelionato
Encaminho expediente para ar
29/02/2024 15:42:08
Lançar movimentação
#
Status
Ações
2
Encaminhado
1
Protocolado
Detalhes do Movimento
Código: 78168
N. Movimento: 2
Data Movimento: 05/03/2024 14:22:22
Data Recebimento: 05/03/2024 14:23:13
Movimento: Encaminhado
Prioridade: Não
Setor:
Protocolo/Distribuição - Divisão Administrativa
Anotação:
Prezada(o),
Solicita-se a gentileza para que seja promovida a autuação do presente expediente perante o SEI, com o seguinte tipo de processo: Extrajudicial/Comunicação de interesse geral. Destaca-se especial atenção à documentação que acompanha o referido instrumento.
Antecipa-se agradecimentos pela atenção dispensada.
SGL
Fechar

Protocolo: 78168-OLHSAY **Data:** 29/02/2024 15:42:08 **Tipo:** Comunicação

Nome:

Blumenau - 1º Tabelionato de Notas E Protestos de Titulos

C.I.:

0

CNPJ:

Endereço:

Nº:

0

Bairro:

CEP:

Cidade:

UF:

Email:

tabeliao@primeirotabelionato.org

Tel:

N. Processo:

OAB:

Assunto:

Selecione um Assunto

Comarca:

Selecione uma Comarca

Vara:

Lotação:

Comarca atendimento:

Foro Unificado

Vara atendimento:

Destinatário:

Selecione um Destinatário

Serventia:

Município da serventia:

Origem:

Setorial

Mensagem:

Encaminho expediente para análise.

Resposta:

REPÚBLICA FEDERATIVA DO BRASIL
PODER JUDICIÁRIO

MALOTE DIGITAL

Tipo de documento: Administrativo

Código de rastreabilidade: 824202411499793

Nome original: Ofício 011_2024 Comunicação Corregedor Geral - Hackers ASS.pdf

Data: 29/02/2024 12:43:21

Remetente:

Blumenau - 1º Tabelionato de Notas E Protestos de Titulos

Blumenau - 1º Tabelionato de Notas E Protestos de Titulos

TJSC

Assinado por:

Não foi possível recuperar a assinatura

Prioridade: Normal.

Motivo de envio: Para conhecimento.

Assunto: Comunicado de Ataque RANSONWARE.

REPÚBLICA FEDERATIVA DO BRASIL

ESTADO DE SANTA CATARINA - COMARCA DE BLUMENAU

1º TABELIONATO DE NOTAS E PROTESTO DE TÍTULOS

LIO OGÊ GAYA JUNIOR

Tabelião Interino

Rua São Paulo, 21, Centro, 89.010-175, Blumenau/SC

Horário de Atendimento: 2ª a 6ª das 9h às 18h - Tel.: (47) 3321-1200

Ofício 1TAB/011/2024

Blumenau, 29 de fevereiro de 2024.

Excelentíssimo Senhor
Desembargador ARTUR JENICHEN FILHO
MM. Corregedor-Geral do Foro Extrajudicial
Florianópolis - SC

Senhor Corregedor,

Cumprimentando-o cordialmente, venho, respeitosamente, à presença de Vossa Excelência, em cumprimento ao Art. 132 do Código de Normas da Corregedoria-Geral do Foro Extrajudicial deste Estado, comunicar que no dia 27/02/2024, um computador desta serventia foi invadido por hackers, sofrendo um ATAQUE RANSONWARE, conforme relatório anexo, elaborado por nosso suporte técnico.
Informo ainda, que em razão do ocorrido, por segurança, a serventia não praticou nenhum ato no horário das 10:00 às 11:25h., tempo necessário para identificação do computador, análise de extensão do ataque e solução do problema.
Atenciosamente,

Lio Ogê Gaya Junior
Tabelião Interino

REPÚBLICA FEDERATIVA DO BRASIL
PODER JUDICIÁRIO

MALOTE DIGITAL

Tipo de documento: Administrativo

Código de rastreabilidade: 824202411499794

Nome original: Ofício 011_2024Relatório de incidente de segurança.pdf

Data: 29/02/2024 12:43:21

Remetente:

Blumenau - 1º Tabelionato de Notas E Protestos de Titulos

Blumenau - 1º Tabelionato de Notas E Protestos de Titulos

TJSC

Prioridade: Normal.

Motivo de envio: Para conhecimento.

Assunto: Comunicado de Ataque RANSONWARE.

ADVANCE
SOLUÇÕES EM TI

Relatório de incidente de segurança

CONFIDENCIALIDADE

Todas as informações contidas neste documento são consideradas de uso privilegiado e pertencente à Primeiro Tabelionato de Notas de Blumenau.

Sua divulgação só deverá ser praticada com a finalidade específica de avaliação de seu conteúdo para aprovação e condução das atividades desse projeto.

Sendo assim, nenhuma parte deste documento poderá ser reproduzida ou divulgada, por quaisquer meios, sem a autorização prévia da Advance Comércio e Serviços de Informática Ltda.

EMPRESA

A Advance Soluções em TI atua no mercado desde 2005, levando soluções específicas para empresas com diferentes necessidades e realidades. Formada por um quadro de profissionais com larga experiência, especializados e atentos às principais inovações tecnológicas disponíveis, estão aptos a definir e acompanhar os projetos desde sua prospecção até sua total implantação.

Altamente qualificada na implantação, monitoramento e gerenciamento de soluções de infraestrutura de TI on-premisse ou Cloud, especializando-se assim em fornecedores de alto nível de confiabilidade e de valor agregado como Microsoft, AWS, Bitdefender, Fortinet, Dell entre outros.

Missão
Prestar consultoria em tecnologia da informação potencializando negócios para a empresa e seus clientes.

Visão
Ser referência nacional no mercado onde atua.

Valores
Ter a confiança do cliente, integridade com todos os públicos, excelência com simplicidade, ética, transparência e solidez.

09:50 – Recebido ligação da Sra. Simone Pavan informando que as máquinas da rede estavam sem acesso a pastas no servidor e que havia uma mensagem em inglês.

Imediatamente todos os servidores foram desligados e repassamos a orientação de que todos os Switches fossem desligados.

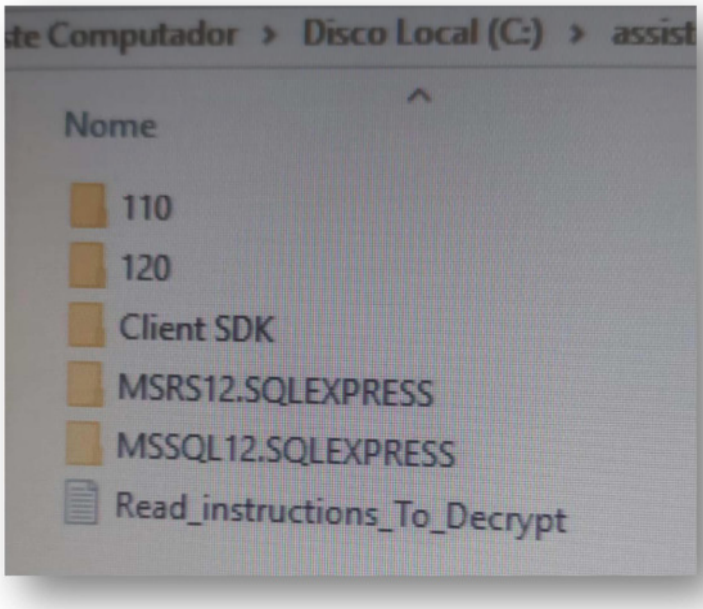
10:00 - Iniciado o deslocamento até a serventia.

10:15 – No local foi identificado se tratar de ataque Ransonware realizado pelo grupo bl00dy.

Iniciado procedimento para análise de extensão do ataque, identificado que apenas pastas compartilhadas nos servidores AD, Ponto e Hyper-v foram infectadas, nenhum compartilhamento em estação de trabalho foi infectado.

Com ajuda do Sr Maicon, iniciado procedimento de localização e identificação do agente de entrada do ataque, após inspeção em todos os computadores, identificamos que o ataque foi originado na máquina chamada e-selo.

A máquina foi desligada e isolada, separada para formatação pelo Sr Rogério.



Conteúdo do arquivo ***Read_Instructions_To_Decrypt***

Hello

We are a team of high-level competent team of Pentesters but NOT a THREAT to your reputable organization

We secure networks of companies to avoid complete destruction and damages to companies

We encrypted all files on Your servers to show sign of breach / network intrusion

To resolve this Continue reading !!!!

ALL files oN Your Entire Network Servers and Connected Devices are Encrypted.

Means , Files are modified and are not usable at the moment.

Don't Panic !!!

All Encrypted files can be reversed to original form and become usable .

This is Only Possible if you buy the universal Decryption software from me.

Price for universal Decryption Software : $ Contact us either through email or tox chat app for the ransom price $

You Have 72 hours To Make Payment As Price of Universal Decryption software increases by $1000 dollars every 24 hours.

Contact on this email: bl00dyadmin@dnmx.org

copy email address and write message to bl00dyadmin@dnmx.org

You can write me on tox:

Download tox app from https://tox.chat

Create new Account ..

Send me friend request using my tox id:

E5BBFAD2DB3FB497EA03612B2428F927FD8A9B3333D524FD51D43B029B7870571CEB0166CB03

copy and paste it as it is

Before You Pay me ... I will Decrypt 3 files for free To proof the universal Decryption software works

Failure to Pay Me :

Kindly RESPECT my Rules

Note: Huge amounts of Data / documents has been stolen from your Network servers and will be published online for free

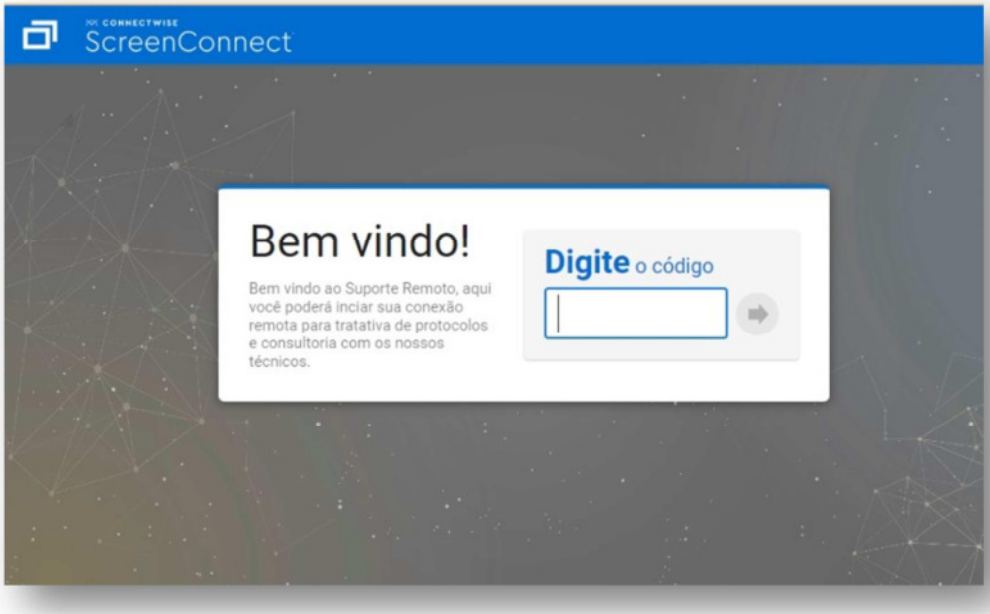
I have stolen All Your Databases ; DAta on your shared drives ; AD users Emails(Good for Spam) ;

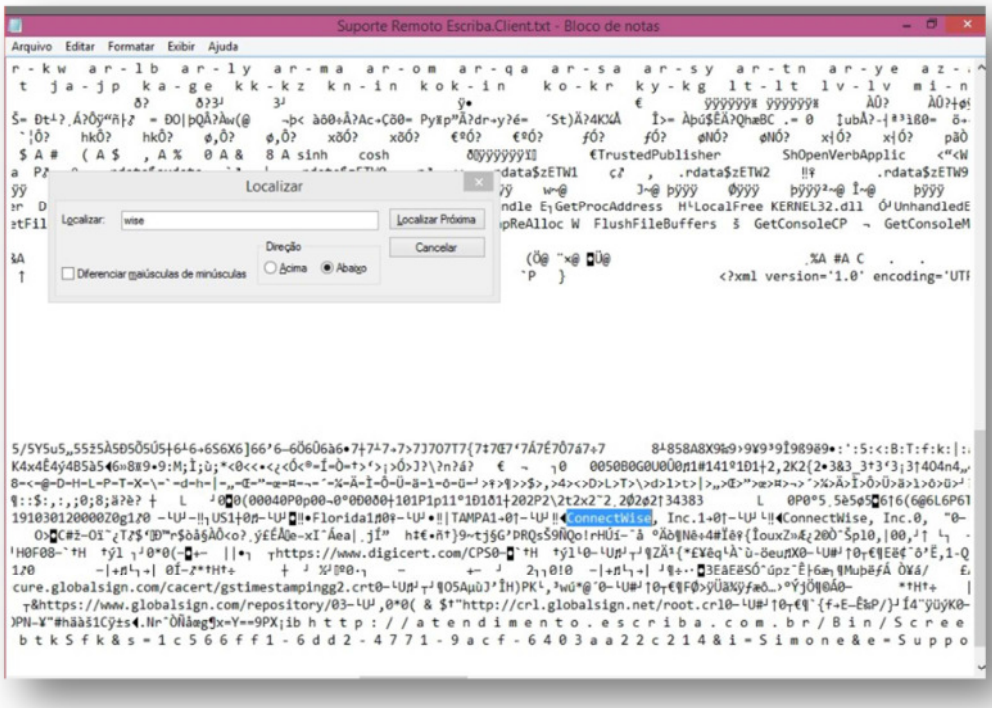
i have stolen huge amount of critical data from your servers

** I keep the breach private only if your cooperate **

Após conversa com a Sra Simone, a mesma informou que a máquina em questão havia sido utilizada para acesso remoto pela empresa fornecedora do sistema de gestão “Escriba” na noite anterior ao episódio e ainda no mesmo dia pela manhã para resolver um problema de envio de selos.

Para o acesso remoto, a empresa Escriba utiliza uma solução chamado Screen Connect da empresa Conectwise, conforme detalhamento abaixo:


CONNECTWISE
ScreenConnect
Bem vindo!
Bem vindo ao Suporte Remoto, aqui você poderá inciar sua conexão remota para tratativa de protocolos e consultoria com os nossos técnicos.
Digite o código


Suporte Remoto Escriba.Client.txt - Bloco de notas
Arquivo Editar Formatar Exibir Ajuda
Localizar
Localizar:
wise
Localizar Próxima
Cancelar
Direção
Acima
Abaixo
Diferenciar maiúsculas de minúsculas
ConnectWise, Inc.
https://www.digicert.com/CPS0
cure.globalsign.com/cacert/gstimestampingg2.crt0
https://www.globalsign.com/repository/03
http://crl.globalsign.net/root.crl0
http://atendimento.escriba.com.br/Bin/Scree
btkSfk&s=1c566ff1-6dd2-4771-9acf-6403aa22c214&i=Simone&e=Suppo

Após a identificação do agente causador do ataque Ransonware, iniciamos os procedimentos de restauração do ambiente, religamento dos servidores, exclusão dos arquivos infectados e restauração do backup.

Por volta das 11:20 o ambiente foi parcialmente restabelecido, e por volta das 13:30 totalmente operacional.

Com relação ao agente causador do ataque Ransonware, após pesquisa, identificado que o Software de acesso remoto utilizado pela fornecedora Escriba, apresentou uma falha grave de segurança descoberta em 22/02/2024, podendo ser o possível causador do ataque Ransonware.

Black Basta, Bl00dy Ransomware Exploiting Recent ScreenConnect Flaws - SecurityWeek

Falhas:

CVE-2024-1709 (CVSS score of 10)

Base Score: 10.0 CRITICAL

CVE-2024-1708 (CVSS score of 8.4)

Base Score: 8.4 HIGH

MALWARE & THREATS

Black Basta, BlOOdy Ransomware Exploiting Recent ScreenConnect Flaws

The Black Basta and BlOOdy ransomware gangs have started exploiting two vulnerabilities in ConnectWise ScreenConnect.

By Ionut Arghire
February 27, 2024

TRENDING

1. State-Sponsored Group Blamed for Change Healthcare Breach
2. NIST Cybersecurity Framework 2.0 Officially Released
3. LockBit Ransomware Gang Resurfaces With New Leak Site
4. Apple Shortcuts Vulnerability Exposes Sensitive Information
5. 'SlashAndGrab' ScreenConnect Vulnerability Widely Exploited for Malware Delivery
6. Microsoft Releases Red Teaming Tool for Generative AI