Relatório Prévio da Invasão à Rede da Prefeitura de Amparo

Em 10 de julho deste ano, foi constatado pelos Analista de Sistemas lotados neste Departamento que houve uma invasão nas estações de trabalho remoto (computadores) da municipalidade, bem como aos Servidores Computacionais de armazenamento de dados e arquivos lotados no *Data Center,* localizados no Paço Municipal "Carlos Piffer". O ataque efetivado basea-se na implantação de códigos maliciosos, que podem ser enviados por e-mail ou por exploração de falhas de segurança de sistemas operacionais legados, como Windows XP, Vista, Server 200x, onde este código é um tipo de *malware* que cifra/codifica os arquivos dos computadores e os liberam para acesso e leitura somente mediante pagamento de resgate através de "criptomoeda", que na ocasião, o famigerado *BitCoin.* Este tipo de ataque denomina-se *Ransomware.*

Segundo a Rede Nacional de Ensino e Pesquisa (RNP), órgão que provê a integração global e a colaboração apoiada em tecnologias de informação e comunicação para a geração do conhecimento e a excelência da educação e da pesquisa, a principal característica desses ataques é capacidade de propagação que eles possuem, graças à exploração de vulnerabilidades do sistema operacional Microsoft Windows, utilizado para compartilhamentos de arquivos e impressoras, que permite ao *malware* acesso administrativo ao sistema e a execução de comandos para infectar outros computadores e se propagar. Além disto, existe outros serviços ativos de rede, como RDP (Serviços de Área de Trabalho Remota), que podem ser explorados para uma invasão inicial da rede. Outra maneira muito recorrente de infecção é dada por usuários que acessam sites comprometidos solicitando que seja realizado o *download* de documentos, fotos ou qualquer outro tipo de arquivo falso, que se executado, realiza a cifragem dos dados do computador e tenta se propagar através da rede.

Em uma célere análise preliminar na referida invasão, a ação de criptografia dos arquivos disponíveis e compartilhados em rede tiveram início da manifestação no dia 08 de julho, onde até o dia 10, boa parte da massa de arquivos disponíveis e compartilhados em rede e diversos computadores remotos tiveram seus arquivos criptografados pelo *malware*

PAÇO MUNICIPAL "PREFEITO CARLOS PIFFER"
AV. BERNARDINO DE CAMPOS, Nº 705 – CENTRO – AMPARO/SP – CEP 13.900-400 – TEL: (19) 3817-9300
suporte@amparo.sp.gov.br | http://www.amparo.sp.gov.br

identificado como ***Phobos, Dharma (.cezar Family) - Figura 01 - ,*** que até presente data momento não possui decriptação aberta, segundo o site **nomoreransom.org**[1].

Análise da identificação do tipo do *malware* está disponível em https://id-ransomware.malwarehunterteam.com/identify.php?case=711a85b64b5da9ceafa7187664c058be30736224

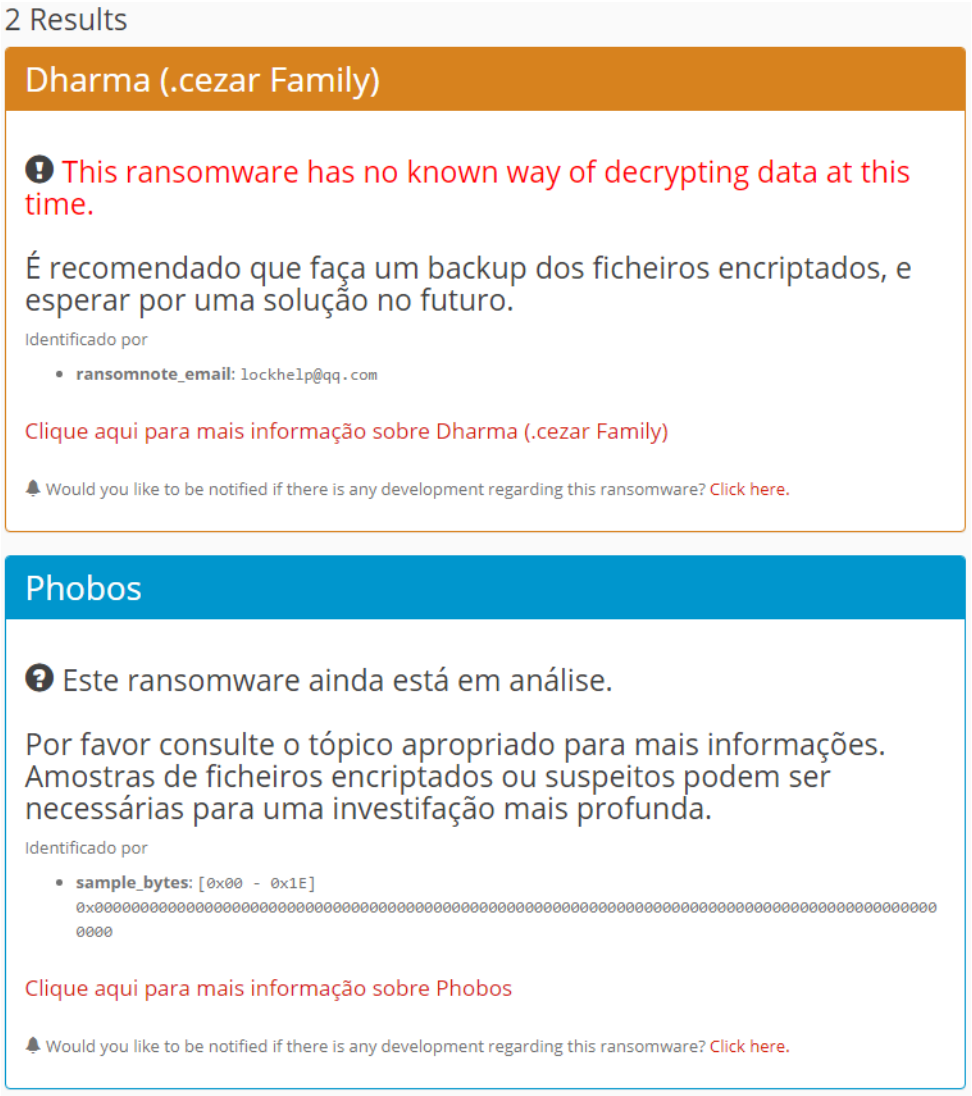


Figura 1 - Tipo do Ransomware

PAÇO MUNICIPAL "PREFEITO CARLOS PIFFER"
AV. BERNARDINO DE CAMPOS, Nº 705 – CENTRO – AMPARO/SP – CEP 13.900-400 – TEL: (19) 3817-9300
suporte@amparo.sp.gov.br | http://www.amparo.sp.gov.br

Como medida contingencial, o Departamento de Tecnologia isolou as redes comprometidas para evitar a sua propagação, como supra citado, para controlar seu alastramento, e após, verificação *in loco* de todas estações para constatação da sua infecção ou não. Nos casos **positivos**, as máquinas permanecerão **desligas, isoladas e identificadas** para futura **perícia**, análise e possível reparo e recuperação dos arquivos armazenados. Nos casos que foram dados como **negativos**, estes foram integrados novamente a rede física e lógica, além da sua atualização de um antivírus corporativo com proteção total, incluindo proteção anti *ransomware.* Devido ao fato do ocorrido ter se dado em um hiato de vacância, considerando a automatização da rotina de cópia de segurança, por infortúnio, as cópia processadas, outrossim, foram comprometidas. Estima-se, previamente, que isto corresponda a 2TB (dois terabytes) de dados. Concomitantemente, as ações descritas, algumas em empresas especializadas em segurança digital foram contactadas no ensaio de uma possível reversão do quadro debuxado.

Por derradeiro, em levantamento prévio, após a análise em todo o parque de máquinas do Paço Municipal e seus anexos, existem 30 (trinta) computadores de diversas secretarias, 04 Servidores Computacionais de Rede e 02 NAS (network attached storage) de arquivos com arquivos criptografados e ilegíveis, onde alguns não mais inicializam.

Este documento, possui 01 (um) anexo com duas imagens.

Nada mais,

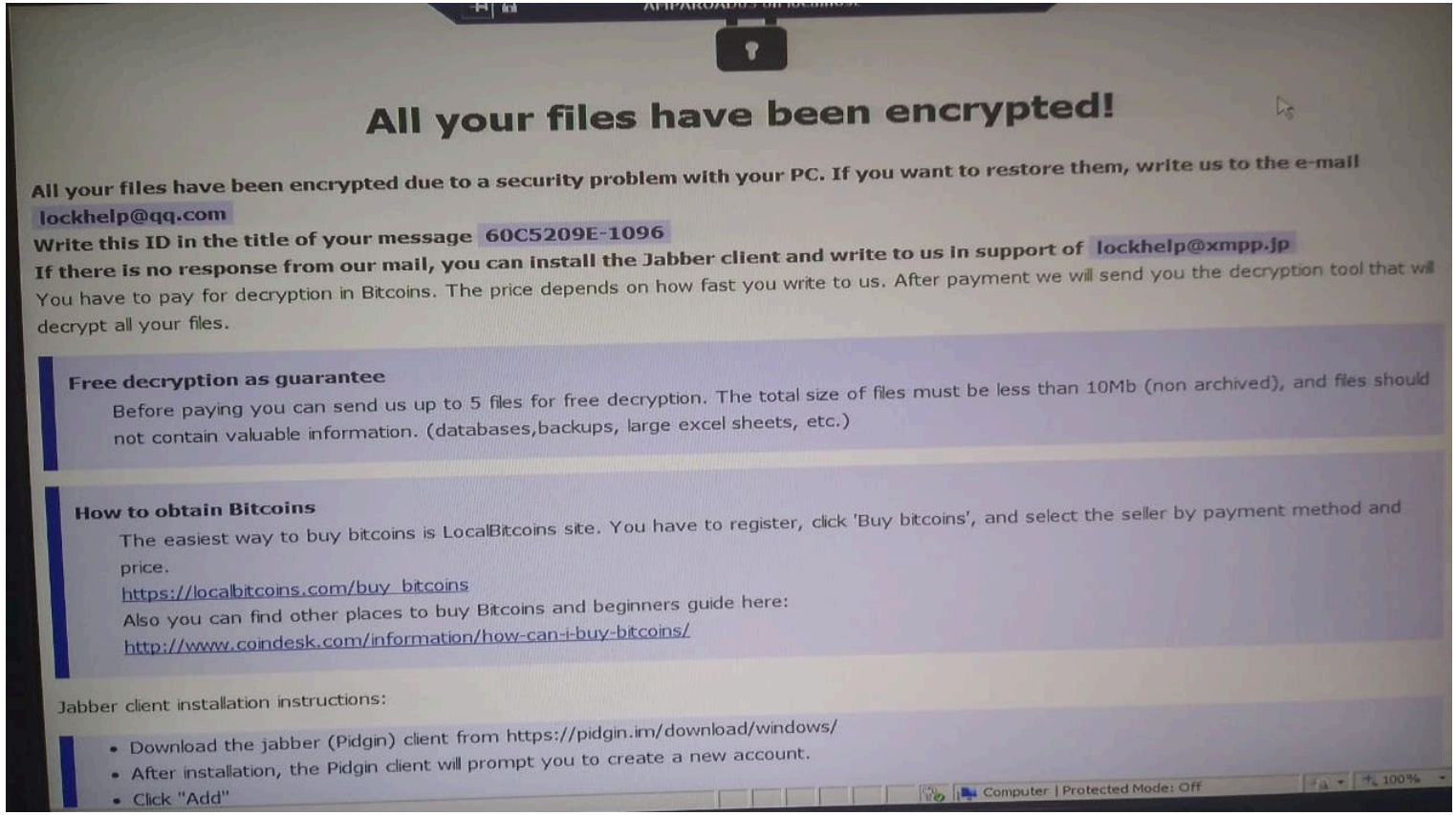
Amparo, 24 de julho de 2019

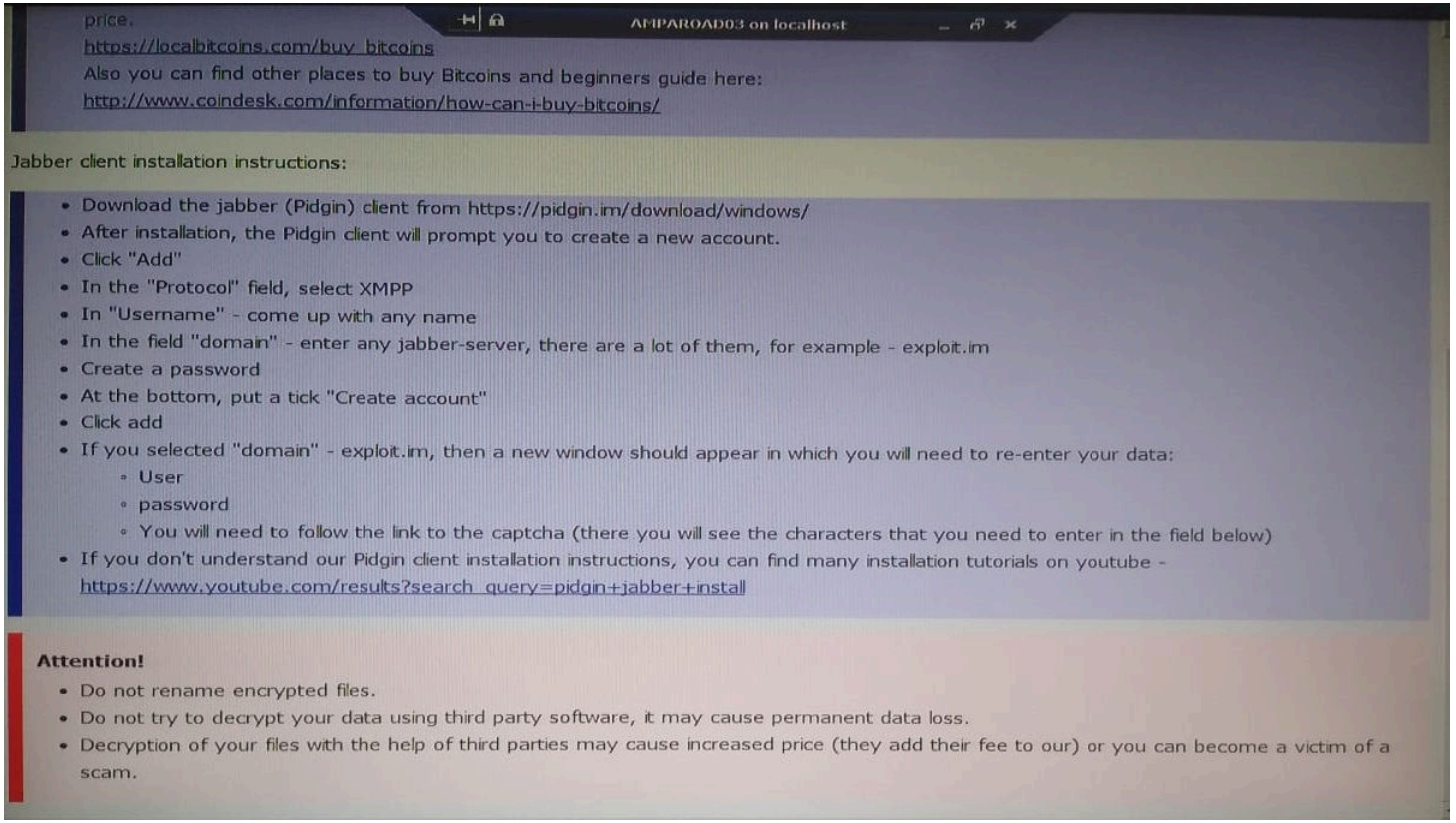
Glauber D Macedo
Analista de Sistemas
Departamento de Tecnologia
Secretaria Municipal de Administração

1 - "No More Ransom" é uma iniciativa da Unidade de Crime de Alta Tecnologia da Polícia Holandesa, do European Cybercrime Centre (EC3) da Europol e McAfee com o objetivo de ajudar as vítimas de *ransomware* a recuperar os seus ficheiros cifrados sem terem que pagar a criminosos (https://www.nomoreransom.org).

PAÇO MUNICIPAL "PREFEITO CARLOS PIFFER"
AV. BERNARDINO DE CAMPOS, Nº 705 – CENTRO – AMPARO/SP – CEP 13.900-400 – TEL: (19) 3817-9300
suporte@amparo.sp.gov.br | http://www.amparo.sp.gov.br

Anexo I





Dependência: DEL.POL.PLANTÃO AMPARO FOLHA:1
Boletim No.: 1414/2019 INICIADO:11/07/2019 10:25 e EMITIDO: 11/07/2019 10:53

1ª Via JRLVQTCBDMEEGK

Boletim de Ocorrência de Autoria Desconhecida.

Natureza(s):
Espécie: L 12737/12 - Delitos de Informática
Natureza: Delitos de Informática
Consumado

Local: AVENIDA BERNARDINO DE CAMPOS, 705 - BAIRRO DO SILVESTRE AMPARO - SP
Tipo de local: Repartição Pública - Prefeitura Municipal
Circunscrição: 01 D.P. - AMPARO

Ocorrência: 10/07/2019 EM HORA INCERTA
Comunicação: 11/07/2019 às 10:25 horas
Elaboração: 11/07/2019 às 10:25 horas
Flagrante: Não

Empresa / Vítima: - Razão social: PREF.MUN. DA ESTANCIA H. DE AMPARO
CNPJ: 43.465.459/0001-73 - Telefone:(19)38179300
Endereço: AV. BERNARDINO DE CAMPOS, 705 - CENTRO - AMPARO - SP
Representante: GLAUBER DANTAS MACEDO - Cargo: ANALISTA DE SISTEMAS

Representante:
- GLAUBER DANTAS MACEDO - Presente ao plantão - RG: [redacted] emitido em [redacted] Exibiu o RG original: Sim
Pai: [redacted] - Mãe: [redacted]
Natural de: S.PAULO -SP - Nacionalidade: BRASILEIRA - Sexo: Masculino
Nascimento: [redacted] - Estado civil: [redacted]
Profissão: FUNCION.PUBLICO MUNICIPAL - Instrução: Superior completo
CPF: [redacted] Advogado Presente no Plantão: Não - Cutis: Branca
Endereço Comercial: AVENIDA BERNARDINO DE CAMPOS, 705 PREFEITURA
BAIRRO DO SILVESTRE - AMPARO - SP - Telefones: (19)3817-9300 (Comercial)

Autor:
- AUTOR 1 - DESCONHECIDO - Não presente ao plantão
Exibiu o RG original: Não - Sexo: Ignorado
Advogado Presente no Plantão: Não

Histórico:
Presente nesta Unidade o representante da vítima, noticiando que é responsável pel centro de Tecnologia de Informação (TI), da prefeitura deste município e, na data dos fatos, ao verificar o sistema de informática local, acabou por constatar que indivíduo(s) desconhecido(s), havia(m) invadido o sistema de informática local através de hackeamento deste, implantando um vírus denominado RANSOMWARE, que tem a função de sequestrar dados existentes no sistemas a fim de solicitar pagamento de resgates em forma de (BITCOINS) às vítimas da invasão. O representante informa que não possui suspeitos de quem possa ter praticado tal delito e informa que não tem como, "com os meios disponíveis no momento", providenciar o rastreio dos autores

Dependência: DEL.POL.PLANTÃO AMPARO FOLHA:
Boletim No.: 1414/2019 INICIADO:11/07/2019 10:25 e EMITIDO: 11/07/2019 10:5

1ª Via JRLVQTCBDMEEGI

através de seu ponto de ataque. O declarante informa que o ataque, provavelmente deve ter ocorrido na data de 08/07/2019. Nada mais.

Solução: BO PARA INVESTIGAÇÃO

ANTONIO FERNANDO MOZZER
ESCRIVÃO AD HOC

LEISE SILVA NEVES
DELEGADA DE POLÍCIA

Endereço da delegacia : RUA POLÔNIA , 318 - JDIM SILVESTRE-AMPARO-SP. CEP: 13901-002
Telefone: (19)3807-4222

SECRETARIA DE ESTADO DA SEGURANÇA PÚBLICA

POLÍCIA CIVIL DO ESTADO DE SÃO PAULO

Dependência: DEL.POL.PLANTÃO AMPARO

RDO Nº: 1414/2019

AUTO DE EXIBIÇÃO E APREENSÃO

Aos 5 dias do mês de agosto de dois mil e dezenove, nesta cidade de AMPARO, Estado de São Paulo, n sede da(o) DEL.POL.PLANTÃO AMPARO , onde presente se achava o(a) Exmo(a) Sr(a) Doutor(a) LEIS SILVA NEVES, Delegado(a) de Polícia respectivo(a), comigo Escrivão(ã) de seu cargo ao final nomeado(a) assinado(a), na presença das TESTEMUNHAS ao final assinadas: Lucas Avancini Mantovani e Raquél d Cássia Pavan, ambos localizáveis na Praça da Bandeira, 55, centro, nesta, aí compareceu o(a) EXIBIDOR(A): Glauber Dantas Macedo, de RG 33.221.437-0 SSP/SP, localizável na Av. Bernardino d Campos, 705, centro, nesta, que exibiu à Autoridade o(s) objeto(s) abaixo especificado(s) encontrado(s), n dia 5 de agosto de 2019, às 16:02 horas em , relacionado(s) com o delito de L 12737/12 - Delitos d Informática / Delitos de Informática(Consumado) sendo determinada pela Autoridade sua apreensão:

Objetos apreendidos:

01 HD (UM) MODELO : HD321HJ, HDD P/N HD 321HJ/SRB INSTAURADO NOPATRIMONIO 42682 LACRE Nº 008064.

Nada mais havendo a tratar, determinou a Autoridade o encerramento do presente auto que, após lido achado conforme, vai por todos devidamente assinado, inclusive por mim Escrivão(ã) de Polícia qu parcialmente o digitei.

LEISE SILVA NEVES
Delegada de Polícia

Testemunha

Testemunha

Exibidor(a)

WILLIAN MACEDO
Escrivão ad hoc de Polícia