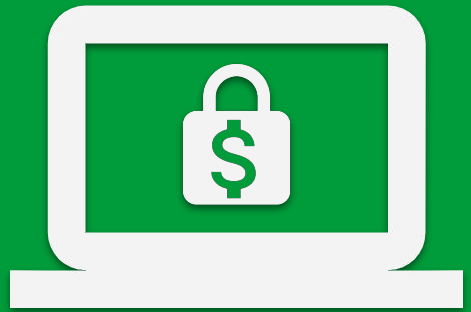
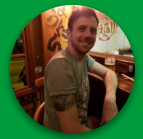
SECRET | UFPR
UNIVERSIDADE FEDERAL DO PARANÁ

SECurity & Reverse Engineering Team (SECRET)
SECRET.INF.UFPR.BR

Integridade, confidencialidade, disponibilidade, ransomware





André Grégio
Federal University of Paraná, BR
@abedgregio

Marcus Botacin
Federal University of Paraná, BR
@MarcusBotacin

GTER 49 | GTS 35
30 DE NOVEMBRO A 1º DE DEZEMBRO DE 2020
EDIÇÃO ON-LINE

Agenda

- Motivação
- Histórico de ransomware
- Funcionamento com *hands-on*
  - Demonstração de exemplares
- Lições aprendidas

Introdução

Motivar é preciso...

RANSOMWARE - Definição

- Código malicioso que **viola a disponibilidade** de arquivos ou dispositivos de suas vítimas (cifrando-os) e demanda quantia para decifragem.

- Tipos principais:
  - ***CRYPTO ransomware:*** criptografa arquivos/diretórios selecionados do usuário comprometido e solicita um resgate, geralmente em criptomoeda, para liberação de chave
  - ***LOCKER ransomware****:* tranca o usuário para fora de seu dispositivo, impedindo que a vítima o utilize. O resgate demandado é para liberar o acesso ao dispositivo.

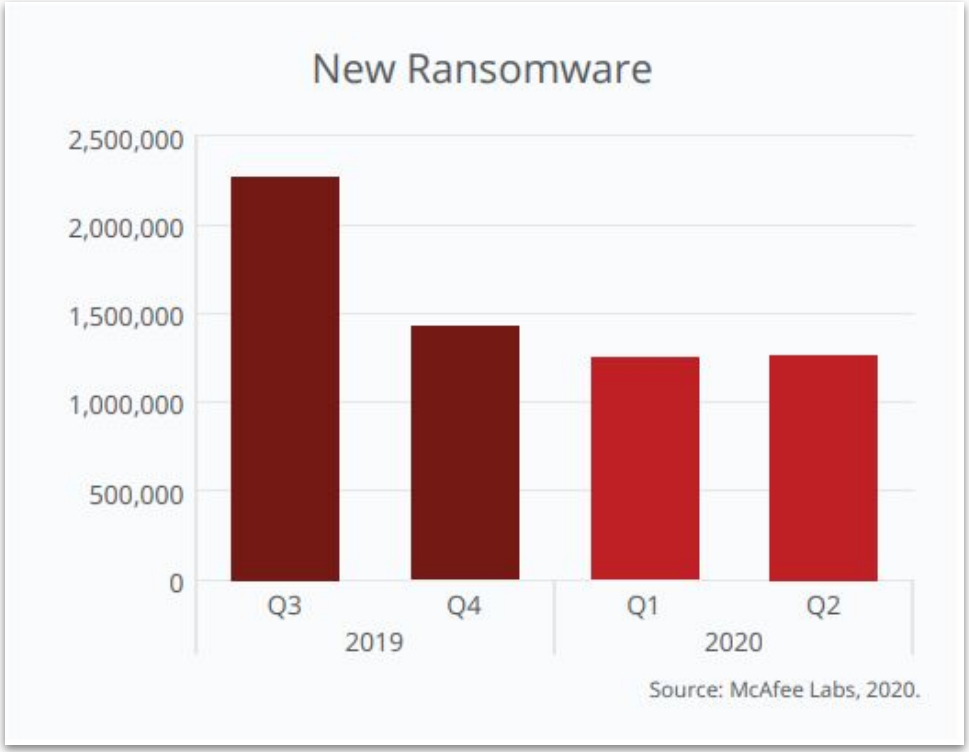
https://www.kaspersky.com/resource-center/threats/ransomware-examples

RANSOMWARE - Comportamento padrão

1. **ENTREGA**
   a. *Phishing* (links, anexos), *Ads* (inclusive em mídias sociais e grandes sites), *Pay-per-Install,* exploração de vulnerabilidades (Java, Windows, etc.) para se propagar
2. **EXECUÇÃO**
   a. Procura arquivos de determinados tipos, nomes de diretórios, *drives* de rede
   b. Acessa e criptografa os objetos-alvo e exibe o aviso de resgate
3. **PAGAMENTO**
   a. Em geral, em USD ou BTC, com destino a uma ou mais carteiras virtuais
   b. **Não é garantido que a chave (ou outro meio de decifragem) seja fornecida**
4. **DECIFRAGEM**
   a. Se houver, pode ser feita por um binário a ser baixado após confirmação de pagamento

https://ieeexplore.ieee.org/abstract/document/8418627

RANSOMWARE - Estatísticas



https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-nov-2020.pdf

Name	Gen.	CAT.	Year	Paid Ransoms	Platform
AIDS	2nd Gen.	*CAT2*	1989	-	Windows
CryptoDefense	3rd Gen.	*CAT4*	2014	> $65,000	Windows
CryptoLocker	3rd Gen.	*CAT4*	2014	>$ 3 million	Windows
CryptoWall	3rd Gen.	*CAT4*	2015	$18 million	Windows
DMA-Locker	3rd Gen.	*CAT4*	2015	> $180,000	Windows
Linux.Encoder	3rd Gen.	*CAT3*	2015	-	Linux
TeslaCrypt	3rd Gen.	*CAT4*	2015	> $80,000	Windows
AnonPop	1st Gen.	*CAT1*	2016	-	Windows
Cerber	3rd Gen.	*CAT5*	2016	> $500,000	Windows
Jigsaw	3rd Gen.	*CAT3*	2016	> $2,000	Windows
KeRanger	3rd Gen.	*CAT4*	2016	> $5,000	Mac OS
Locky	3rd Gen.	*CAT4*	2016	>$ 1 million	Windows
Petya	3rd Gen.	*CAT5*	2016	> $30,000	Windows
VenusLocker	3rd Gen.	*CAT5*	2016	> $6,500	Windows
ZCryptor	3rd Gen.	*CAT5*	2016	-	Windows
Bad Rabbit	2nd Gen.	*CAT2*	2017	-	Windows
Erebus	3rd Gen.	*CAT5*	2017	> $1 million	Linux
NotPetya	3rd Gen.	*CAT3*	2017	> $10,000	Windows
WannaCry	3rd Gen.	*CAT5*	2017	> $140,000	Windows
SamSam	3rd Gen.	*CAT5*	2018	> $850,000	Windows

https://www.researchgate.net/publication/330734778_Understanding_the_Evolution_of_Ransomware_Paradigm_Shifts_in_Attack_Structures

Malware x Não-Malware

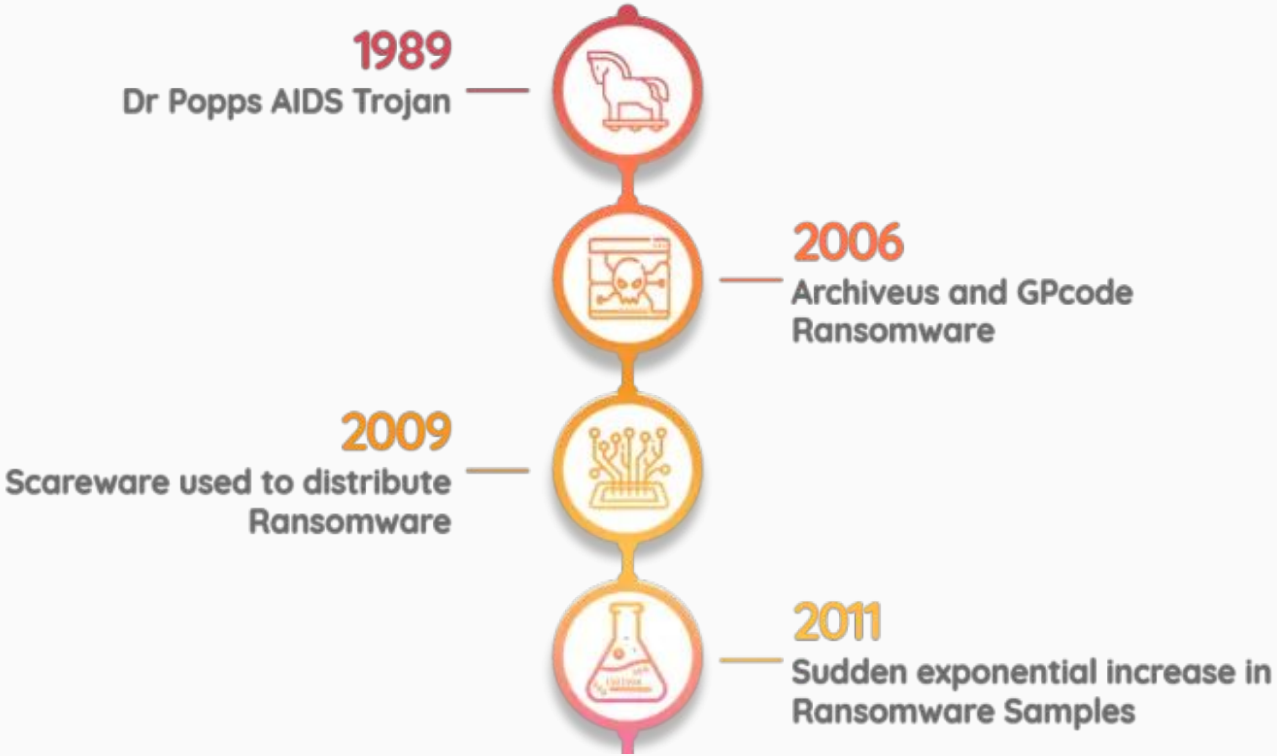
- Tudo é código, a diferença é a intenção…
- Detecção acadêmica vs. Detecção industrial
  - Teoria é offline
  - Prática é inexistente
- Há décadas sabemos os princípios básicos
  - Proteger a integridade, disponibilidade, confidencialidade
  - Realizar prevenção, detecção, reação
  - Implantar políticas, manter tudo atualizado, compartimentalizar

Por que isso não tem funcionado?

De Onde Viemos

Evolução de *ransomware* ao longo do tempo

Linha do Tempo



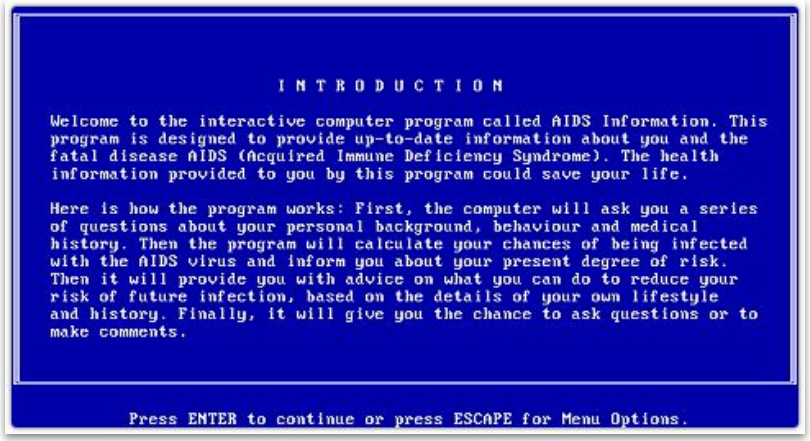
https://www.immersivelabs.com/resources/blog/the-evolution-of-ransomware/

A primeira vez a gente nunca esquece...

Autor: Dr. Popps, biólogo

Nome, Ano: PC Cyborg, 1989

Vetor: (!e-)mail + disquete com questionário sobre AIDS



Comportamento:

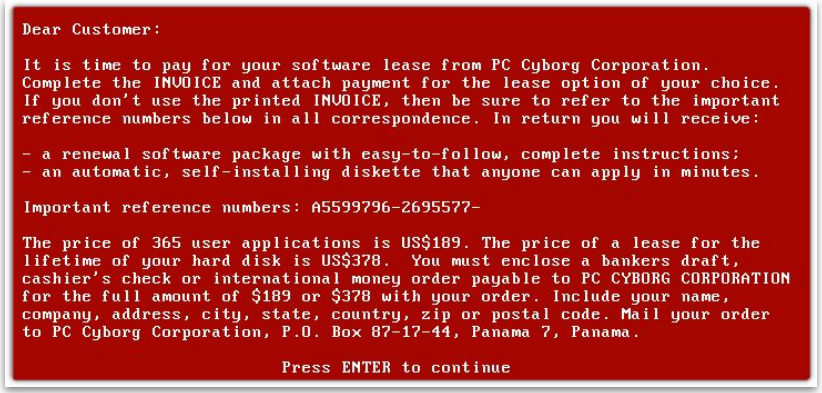
1. 2 arquivos (1 questionário, 1 instalador)
2. Infecta C:\ e sequestra AUTOEXEC.BAT
3. Implementa contador de *reboot* (90x)
4. Criptografa simetricamente **os nomes** de todos os arquivos do *drive*
   a. Alteração na extensão impedia a execução dos arquivos

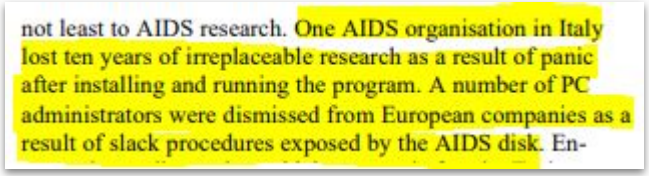
FONTES:
https://www.sdxcentral.com/security/definitions/case-study-aids-trojan-ransomware/
https://www.vice.com/en/article/nzpwe7/the-worlds-first-ransomware-came-on-a-floppy-disk-in-1989

A primeira vez a gente nunca esquece...

Resultado:

1. ~20k pessoas infectadas)
2. Envio de $ para Caixa Postal no Panamá
3. Pânico fez com que usuários e organizações médicas/de pesquisa apagassem HDs

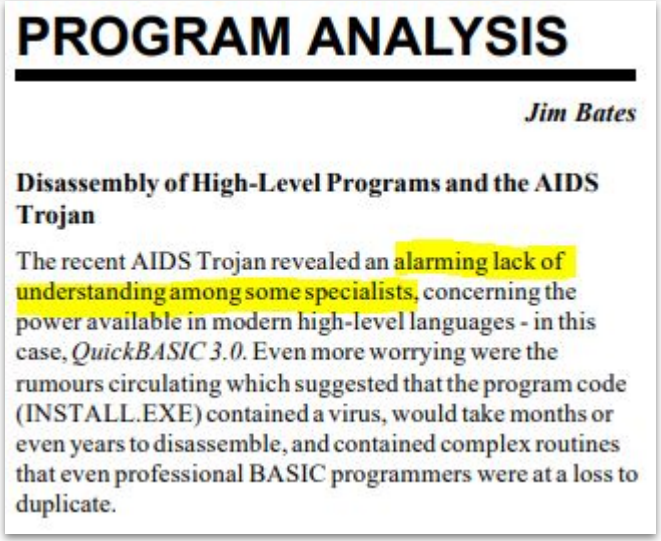



not least to AIDS research. One AIDS organisation in Italy lost ten years of irreplaceable research as a result of panic after installing and running the program. A number of PC administrators were dismissed from European companies as a result of slack procedures exposed by the AIDS disk. En-

FONTES:
https://en.wikipedia.org/wiki/AIDS_(Trojan_horse)
https://www.virusbulletin.com/uploads/pdf/magazine/1992/199201.pdf

4. **Malware como peça de influência**
5. Autor indiciado à prisão/processado, mas considerado não-julgável...
6. Jim Bates criou "vacinas" AIDSOUT e CLEARAIDS em 1990 (VirusBulletin)

Saudades do AIDS Trojan!



PROGRAM ANALYSIS

Jim Bates

Disassembly of High-Level Programs and the AIDS Trojan

The recent AIDS Trojan revealed an alarming lack of understanding among some specialists, concerning the power available in modern high-level languages - in this case, *QuickBASIC 3.0*. Even more worrying were the rumours circulating which suggested that the program code (INSTALL.EXE) contained a virus, would take months or even years to disassemble, and contained complex routines that even professional BASIC programmers were at a loss to duplicate.

https://www.virusbulletin.com/uploads/pdf/magazine/1990/199002.pdf

Análises do *Trojan* explicitaram falhas e melhoraram a área (de *ransomware*):

- IEEE S&P 1996, Yong e Yung implementaram um vírus com criptografia de chaves públicas
- *Cryptovirology: extortion-based security threats and countermeasures*
- https://ieeexplore.ieee.org/document/502676

Lições Aprendidas

- Desenvolvedores de *malware*:
  - Não usar criptografia simétrica!
- Usuários/organizações:
  - **Backup** é importante!

Dados sobre Ransomware

Family	Family Description			
	Samples	Variants	First Seen	Most Recent
Reveton	244(17.95%)	14	2012	2014
Cryptolocker	32 (2.35%)	4	2013	2014
CryptoWall	11(0.8)	2	2014	2014
Tobfy	122 (8.97%)	12	2010	2014
Seftad	23 (1.69%)	4	2006	2010
Winlock	308(22.66%)	27	2008	2013
Loktrom	4 (0.29%)	2	2012	2013
Calelk	9 (0.663%)	2	2009	2010
Urausy	523 (38.48%)	16	2009	2014
Krotten	17 (1.25%)	3	2008	2009
BlueScreen	4 (0.29%)	1	2008	2009
Kovter	8 (0.58%)	2	2013	2013
Filecoder	9 (0.66%)	3	2012	2014
GPcode	21 (1.54%)	4	2004	2008
Weelsof	24 (1.76%)	3	2012	2013
No. of Samples	1,359	-	-	-
No. of Variants	-	99	-	-

Types of Attacks			
Encypting Files	Changing MBR	Deleting Files	Stealing Info
		✓	✓
✓			✓
✓			
		✓	
	✓		
		✓	
		✓	✓
			✓
✓		✓	
✓			
73(5.37%)	23(1.69%)	484(35.61%)	44(3.23%)
13(13.13%)	4(4.04%)	29(21.33%)	6(6.06%)

Table 5: Summary of types of charges in 15 ransomware families.

Families	Type of Charge			
	Premium Number	Untraceable Payments	Online Shopping	Bitcoin Transactions
Reveton		✓	✓	
Cryptolocker		✓		✓
CryptoWall				✓
Tobfy		✓		
Seftad	✓			
Winlock				
Loktrom	✓			
Calelk	✓			
Urausy		✓	✓	
Krotten		✓		
BlueScreen		✓		
kovter		✓	✓	
Filecoder		✓		
GPcode		✓		
Weelsof		✓		
Number of Samples	132 (9.71%)	1,199 (88.22%)	14(1.03%)	28 (2.86%)
Number of Variants	18 (19.35%)	75 (80.64%)	4 (4.30%)	4 (4.3%)

Kharraz et al. *Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks*. DIMVA, 2015.
http://www.eurecom.fr/en/publication/4548/download/rs-publi-4548.pdf

CryptoLocker e CryptoLocker 2.0

Vetor de entrada: e-mail

Comportamento:

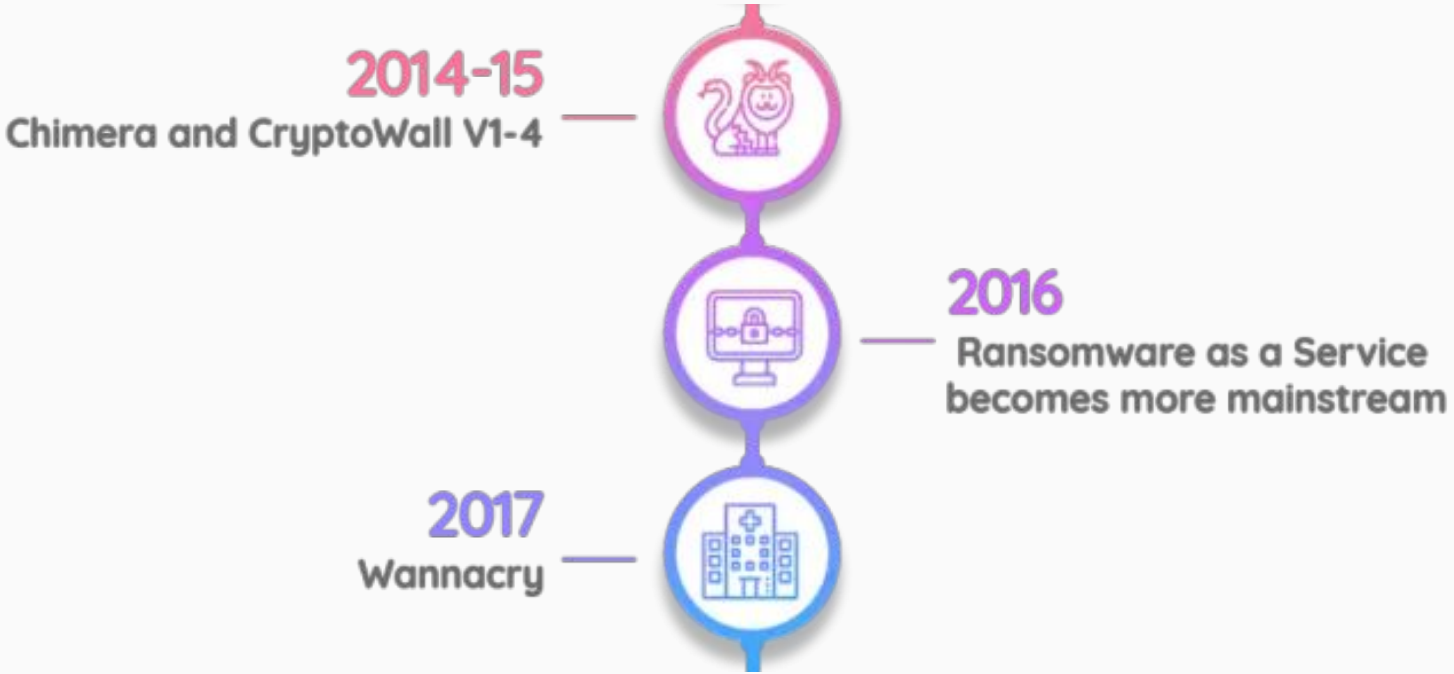
1. Usuário executa o artefato
2. Processo inicia varredura em busca de *drives* de rede
3. Arquivos e diretórios são renomeados e cifrados

Diferenças:

1. De C++ foi para C# (grupos diferentes? Imitação?)
2. 2.0 criptografa mais tipos de arquivo (música, imagem, vídeo)
3. Inflação (USD 300 para 500)

FONTE: https://www.knowbe4.com/cryptolocker-2

Linha do Tempo



https://www.immersivelabs.com/resources/blog/the-evolution-of-ransomware/

Cryptowall

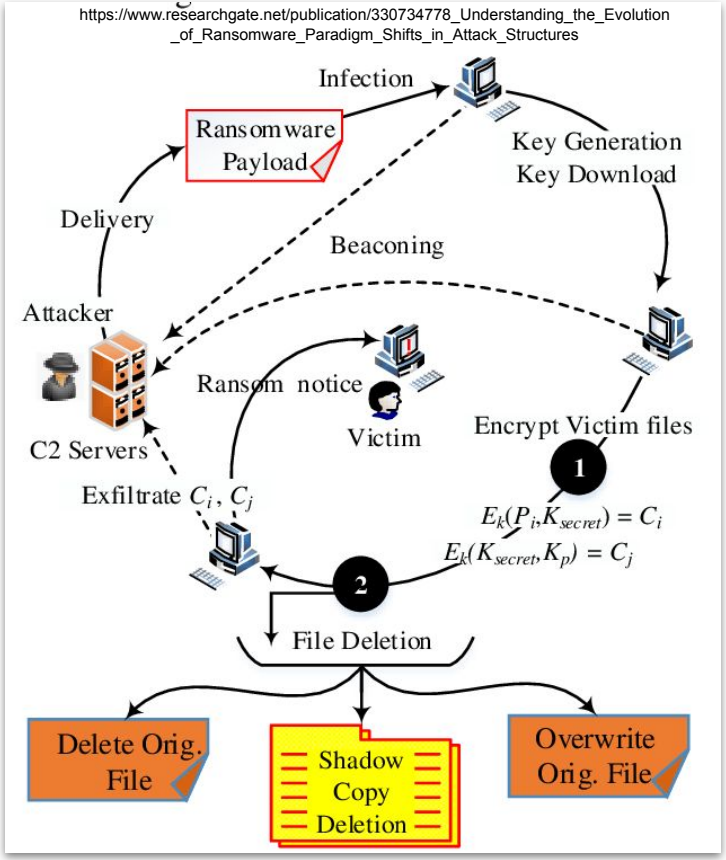
Vetor de entrada: *phishing*, *exploit kits*, propagandas maliciosas

Comportamento:

1. **Injeta código** no Explorer.exe[a] e SVCHost.exe[b] para manutenção
   a. Instala *malware*, **remove *shadow copies***, desabilita serviços, inicializa um novo svchost...
   b. Comunica com a "base" via rede, cifra arquivos, **remove o malware** após serviço feito!
2. Persiste via Registro e *Startup*

FONTE:
https://www.varonis.com/blog/cryptowall/

Ransomware as a Service



- Similar aos malware kits em **usabilidade**
  - Qualquer pessoa pode extorquir outras!

- Criador **é comissionado** com o resgate
  - Provê o código, leva 5-30%

FONTE: https://www.businessinsider.com/ransomware-as-a-service-is-the-next-big-cyber-crime-2015-12

Chimera

Tipo de chantagem: *doxing* (autores prometeram disponibilizar publicamente os arquivos das vítimas caso o resgate não fosse pago...)

Vem pro time, fera!

https://blog.malwarebytes.com/threat-analysis/2015/12/inside-chimera-ransomware-the-first-doxingware-in-wild/

Linha do Tempo

https://www.immersivelabs.com/resources/blog/the-evolution-of-ransomware/

Tendências de 2020

	Initial infection vector	Encryption method	Command and control?	Payment method	Exfiled data?
Maze	Malicious email Exploit kits RDP brute force	Encrypted files using RSA-2048 and ChaCha20	Yes	Bitcoin	Yes
Dharma	Malicious email RDP brute force	Encrypted files using RSA-1024 and AES-128	Yes	Bitcoin	No
Snake	Malicious email RDP brute force Exposed vulnerable systems	Encrypted files using RSA-2048 and AES-256	Sometimes	Email an address for further information	Yes
Sodinokibi	RDP brute force Malicious documents Exposed vulnerable systems Drive by compromise on websites	Encrypted files using AES and Salsa20	Yes	Bitcoin	Yes

https://www.immersivelabs.com/resources/blog/the-evolution-of-ransomware/

Brasil, Novembro de 2020

Notícias | Ransomware | Especiais

STJ é vítima de ransomware e tem seus dados e os backups criptografados

Guilherme M. Petry — há 16 dias — 4 min

Notícias | Ransomware | Especiais

STJ é vítima de ransomware e seus dados e o backups criptografados

Guilherme M. Petry — há 16 dias — 4 min

RansomExx: vírus que atingiu STJ tamb

TJ-PE e outros países

Imagem: iStock

Lucas Carvalho
De Tilt, em São Paulo
07/11/2020 10h01

HOME / SEGURANÇA

Ransomware que afeta STJ já atingiu empresas e governos fora do Brasil

Conhecido como RansomExx, a ameaça se camufla na rede, rouba dados e só então cifra os arquivos e cobra pelo resgate

Renato Santino 05/11/2020 21h10

ransomware e

backups criptografados

Guilherme M. Petry — há 16 dias — 4 min

Início » Antivírus e Segurança » STJ confirma ataque de ransomware e recebe ajuda da Microsoft

STJ confirma ataque de ransomware e recebe ajuda da Microsoft

Empresas que prestam serviços de tecnologia ao STJ estão colaborando com a restauração dos sistemas após invasão

Por Victor Hugo Silva
06/11/2020 às 10:40

RansomExx: vírus que atingiu STJ tamb

TJ-PE e outros países

Imagem: iStock

Lucas Carvalho
De Tilt, em São Paulo
07/11/2020 10h01

Ransomware: saiba como funciona o vírus que invadiu a rede do STJ

Um ataque hacker criptografou dados do STJ e causou a suspensão de atividades do tribunal

por: Ana Marques, em: 06/11/2020

HOME / SEGURANÇA

Ransomware que afeta STJ já atingiu empresas e governos fora do Brasil

Conhecido como RansomExx, a ameaça se camufla na rede, rouba dados e só então cifra os arquivos e cobra pelo resgate

Renato Santino 05/11/2020 21h10

Possíveis falhas no caso do Ransomware do STJ

10/11/2020 mindsecblog Notícias 1

RansomExx: vírus que atingiu STJ tamb

TJ-PE e outros países

ransomware e

seu

backups

criptografa

Guilherme M. Petry — há 16 dias — 4 min

Início » Antivírus e Segurança » STJ confirma ataque de ransomware e recebe ajuda da Microsoft

STJ confirma ataque de ransomware e recebe ajuda da Microsoft

Empresas que prestam serviços de tecnologia ao STJ estão colaborando com a restauração dos sistemas após invasão

Por Victor Hugo Silva
06/11/2020 às 10:40

Ransomware: saiba como funciona o vírus que invadiu a rede do STJ

Um ataque hacker criptografou dados do STJ e causou a suspensão de atividades do tribunal

por: Ana Marques, em: 06/11/2020

HOME / SEGURANÇA

STJ se restabelece após ransomware; PF investiga cópia de dados

Provável malware utilizado no ataque é conhecido por copiar arquivos sigilosos antes de se manifestar

Renato Santino 13/11/2020 18h50

Links

- https://thehack.com.br/stj-e-vitima-de-ransomware-e-tem-seus-dados-e-os-backups-criptografados/
- https://www.uol.com.br/tilt/noticias/redacao/2020/11/07/ransomexx-virus-que-atingiu-stj-tambem-atacou-tj-pe-e-outros-paises.htm
- https://olhardigital.com.br/fique_seguro/noticia/ransomware-que-afeta-stj-ja-atingiu-empresas-e-governos-fora-do-brasil/109866
- https://tecnoblog.net/381722/stj-confirma-ataque-de-ransomware-e-recebe-ajuda-da-microsoft/
- https://minutodaseguranca.blog.br/possiveis-falhas-no-caso-do-ransomware-do-stj/
- https://olhardigital.com.br/fique_seguro/noticia/stj-se-restabelece-apos-ransomware-mas-pf-investiga-copia-de-dados/110209

Modus Operandi

Simplicidade acima de tudo...

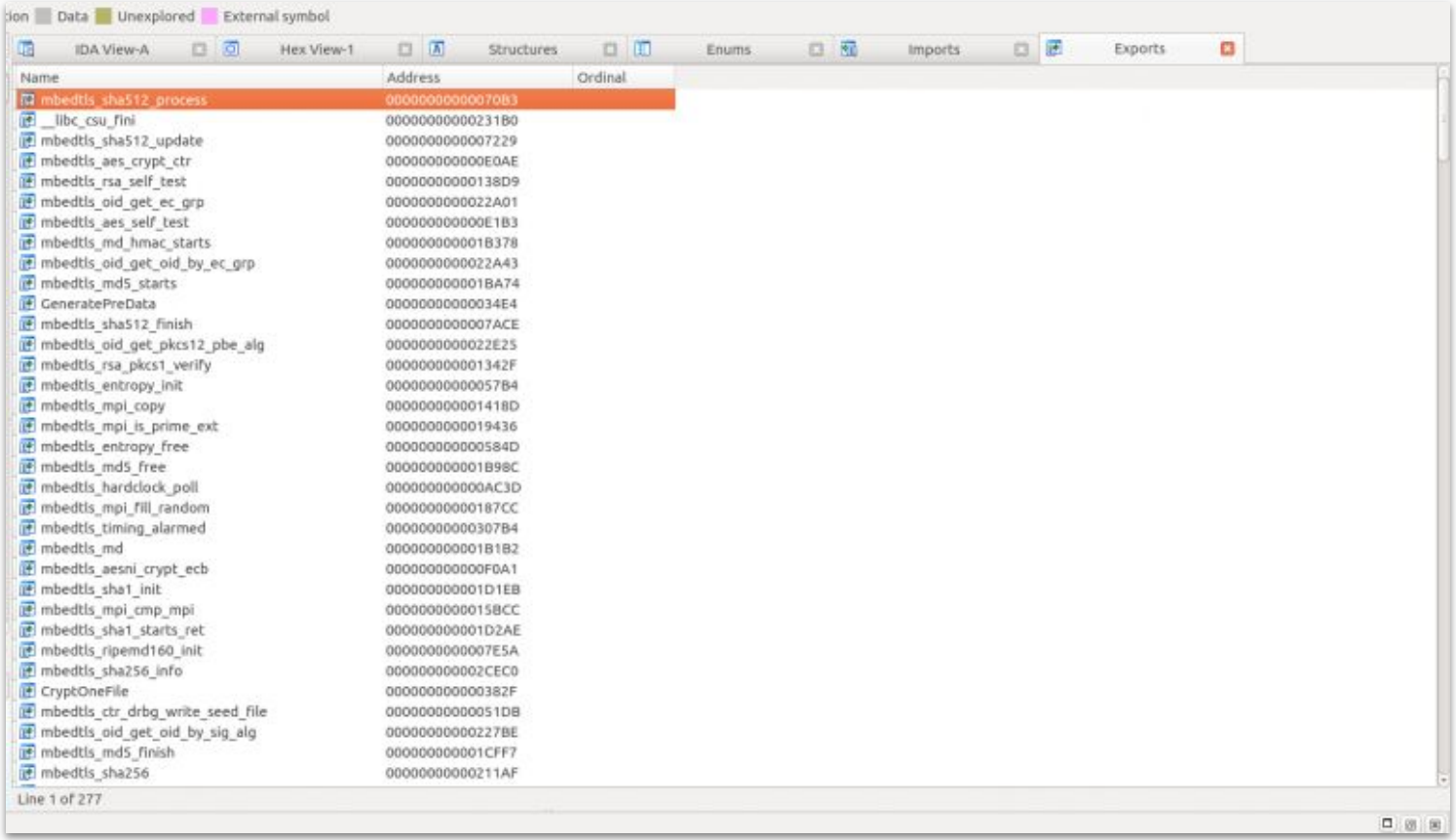
Modus Operandi

- Obtivemos dois exemplares:
  - Notepad.exe (https://corvus.inf.ufpr.br/reports/12243/)
    - **MD5:** 80cfb7904e934182d512daa4fe0abbfb
    - **SHA1:** 9df15f471083698b818575c381e49c914dee69de
  - Arquivo ELF (https://corvus.inf.ufpr.br/reports/12244/)
    - **MD5:** aa1ddf0c8312349be614ff43e80a262f
    - **SHA1:** 91ad089f5259845141dfb10145271553aa711a2b
- O PE é um *loader*
  - Detalhes a seguir...
- **O ransomware é o arquivo ELF, com execução "manual"**
  - Ao se passar um diretório como argumento, a cifragem acontece...
  - Mesmo artefato (RansomEXX) esteve envolvido nos ataques ao TXDoT em maio/2020!
    - https://www.bleepingcomputer.com/news/security/new-ransom-x-ransomware-used-in-texas-txdot-cyberattack/

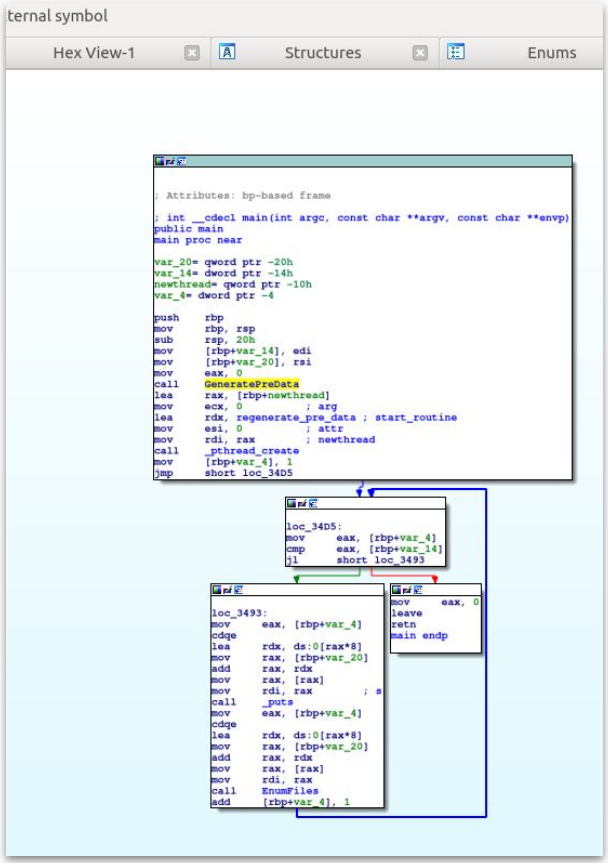
Demonstração & Análise

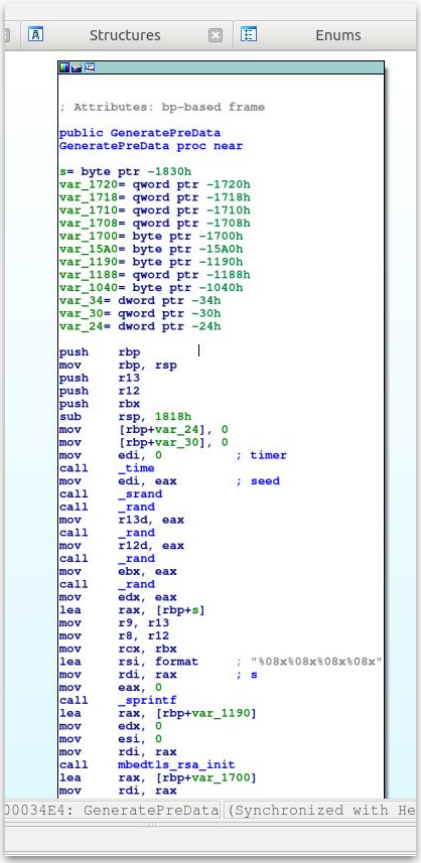
Proof of Concept or...

RansomExx

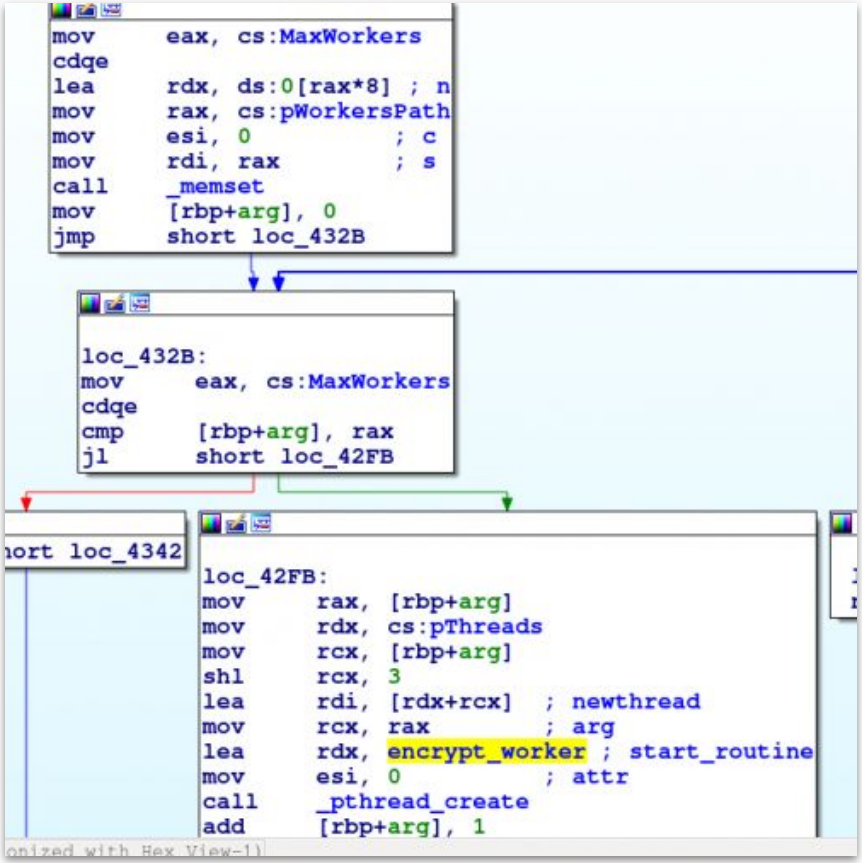

ion Data Unexplored External symbol
IDA View-A
Hex View-1
Structures
Enums
Imports
Exports
Name
Address
Ordinal
mbedtls_sha512_process 00000000000070B3
__libc_csu_fini 00000000000231B0
mbedtls_sha512_update 0000000000007229
mbedtls_aes_crypt_ctr 000000000000E0AE
mbedtls_rsa_self_test 00000000000138D9
mbedtls_oid_get_ec_grp 0000000000022A01
mbedtls_aes_self_test 000000000000E1B3
mbedtls_md_hmac_starts 000000000001B378
mbedtls_oid_get_oid_by_ec_grp 0000000000022A43
mbedtls_md5_starts 000000000001BA74
GeneratePreData 00000000000034E4
mbedtls_sha512_finish 0000000000007ACE
mbedtls_oid_get_pkcs12_pbe_alg 0000000000022E25
mbedtls_rsa_pkcs1_verify 00000000000001342F
mbedtls_entropy_init 00000000000057B4
mbedtls_mpi_copy 000000000001418D
mbedtls_mpi_is_prime_ext 0000000000019436
mbedtls_entropy_free 000000000000584D
mbedtls_md5_free 000000000001B98C
mbedtls_hardclock_poll 000000000000AC3D
mbedtls_mpi_fill_random 00000000000187CC
mbedtls_timing_alarmed 00000000000307B4
mbedtls_md 000000000001B1B2
mbedtls_aesni_crypt_ecb 000000000000F0A1
mbedtls_sha1_init 000000000001D1EB
mbedtls_mpi_cmp_mpi 00000000000158CC
mbedtls_sha1_starts_ret 000000000001D2AE
mbedtls_ripemd160_init 0000000000007E5A
mbedtls_sha256_info 000000000002CEC0
CryptOneFile 00000000000382F
mbedtls_ctr_drbg_write_seed_file 00000000000051DB
mbedtls_oid_get_oid_by_sig_alg 00000000000227BE
mbedtls_md5_finish 000000000001CFF7
mbedtls_sha256 00000000000211AF
Line 1 of 277

RansomExx

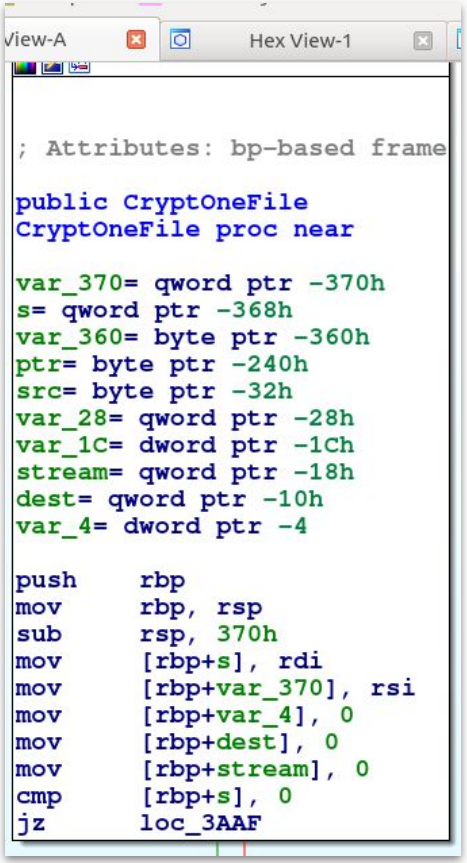

ternal symbol
Hex View-1
Structures
Enums
; Attributes: bp-based frame
; int __cdecl main(int argc, const char **argv, const char **envp)
public main
main proc near
var_20= qword ptr -20h
var_14= dword ptr -14h
newthread= qword ptr -10h
var_4= dword ptr -4
push rbp
mov rbp, rsp
sub rsp, 20h
mov [rbp+var_14], edi
mov [rbp+var_20], rsi
mov eax, 0
call GeneratePreData
lea rax, [rbp+newthread]
mov ecx, 0 ; arg
lea rdx, regenerate_pre_data ; start_routine
mov esi, 0 ; attr
mov rdi, rax ; newthread
call _pthread_create
mov [rbp+var_4], 1
jmp short loc_34D5
loc_34D5:
mov eax, [rbp+var_4]
cmp eax, [rbp+var_14]
jl short loc_3493
loc_3493:
mov eax, [rbp+var_4]
cdqe
lea rdx, ds:0[rax*8]
mov rax, [rbp+var_20]
add rax, rdx
mov rax, [rax]
mov rdi, rax ; s
call _puts
mov eax, [rbp+var_4]
cdqe
lea rdx, ds:0[rax*8]
mov rax, [rbp+var_20]
add rax, rdx
mov rax, [rax]
mov rdi, rax
call EnumFiles
add [rbp+var_4], 1
mov eax, 0
leave
retn
main endp

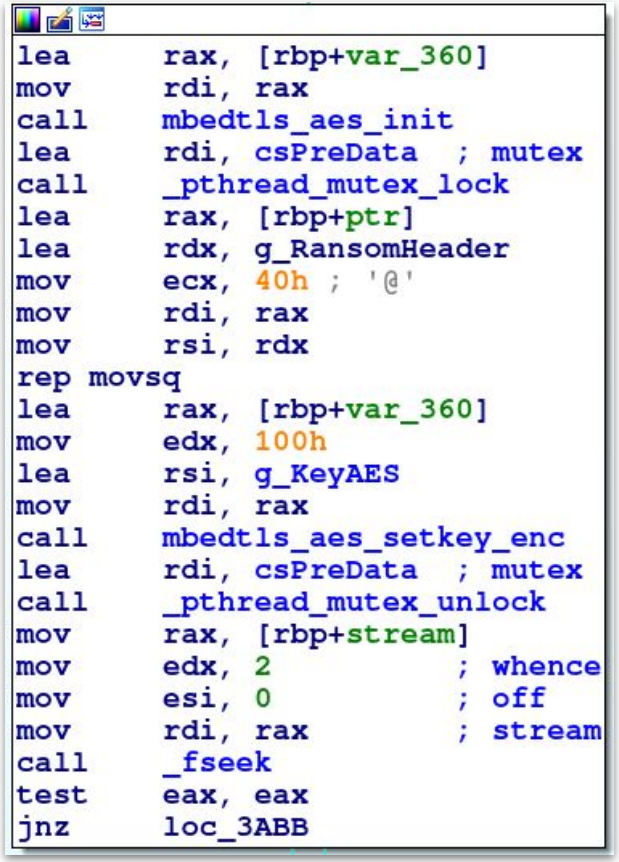

Structures
Enums
; Attributes: bp-based frame
public GeneratePreData
GeneratePreData proc near
s= byte ptr -1830h
var_1720= qword ptr -1720h
var_1718= qword ptr -1718h
var_1710= qword ptr -1710h
var_1708= qword ptr -1708h
var_1700= byte ptr -1700h
var_15A0= byte ptr -15A0h
var_1190= byte ptr -1190h
var_1188= qword ptr -1188h
var_1040= byte ptr -1040h
var_34= dword ptr -34h
var_30= qword ptr -30h
var_24= dword ptr -24h
push rbp
mov rbp, rsp
push r13
push r12
push rbx
sub rsp, 1818h
mov [rbp+var_24], 0
mov [rbp+var_30], 0
mov edi, 0 ; timer
call _time
mov edi, eax ; seed
call _srand
call _rand
mov r13d, eax
call _rand
mov r12d, eax
call _rand
mov ebx, eax
call _rand
mov edx, eax
lea rax, [rbp+s]
mov r9, r13
mov r8, r12
mov rcx, rbx
lea rsi, format ; "%08x%08x%08x%08x"
mov rdi, rax ; s
mov eax, 0
call _sprintf
lea rax, [rbp+var_1190]
mov edx, 0
mov esi, 0
mov rdi, rax
call mbedtls_rsa_init
lea rax, [rbp+var_1700]
mov rdi, rax
00034E4: GeneratePreData (Synchronized with He

RansomExx


mov eax, cs:MaxWorkers
cdqe
lea rdx, ds:0[rax*8] ; n
mov rax, cs:pWorkersPath
mov esi, 0 ; c
mov rdi, rax ; s
call _memset
mov [rbp+arg], 0
jmp short loc_432B
loc_432B:
mov eax, cs:MaxWorkers
cdqe
cmp [rbp+arg], rax
jl short loc_42FB
ort loc_4342
loc_42FB:
mov rax, [rbp+arg]
mov rdx, cs:pThreads
mov rcx, [rbp+arg]
shl rcx, 3
lea rdi, [rdx+rcx] ; newthread
mov rcx, rax ; arg
lea rdx, encrypt_worker ; start_routine
mov esi, 0 ; attr
call _pthread_create
add [rbp+arg], 1

RansomExx

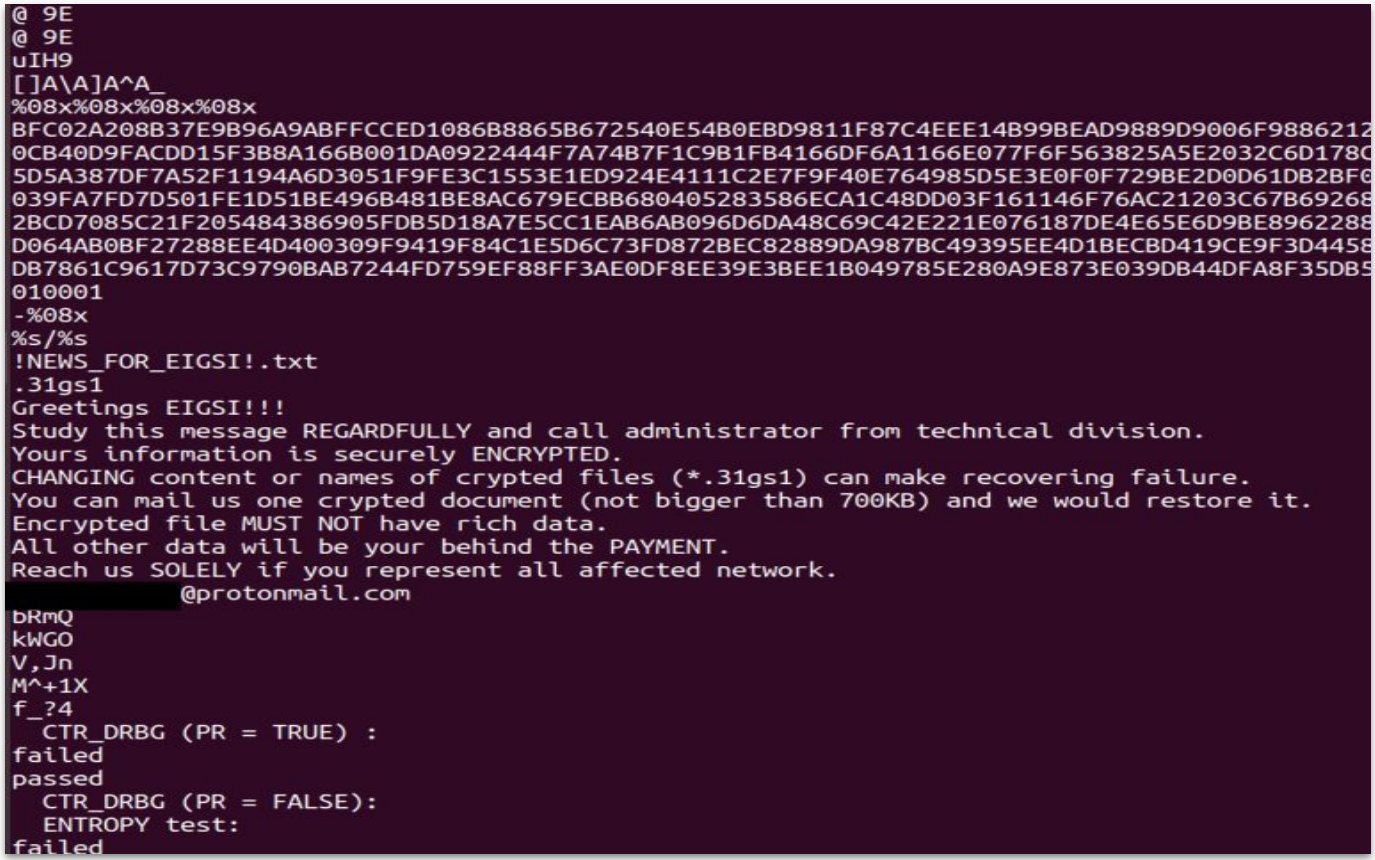

View-A
Hex View-1
; Attributes: bp-based frame
public CryptOneFile
CryptOneFile proc near
var_370= qword ptr -370h
s= qword ptr -368h
var_360= byte ptr -360h
ptr= byte ptr -240h
src= byte ptr -32h
var_28= qword ptr -28h
var_1C= dword ptr -1Ch
stream= qword ptr -18h
dest= qword ptr -10h
var_4= dword ptr -4
push rbp
mov rbp, rsp
sub rsp, 370h
mov [rbp+s], rdi
mov [rbp+var_370], rsi
mov [rbp+var_4], 0
mov [rbp+dest], 0
mov [rbp+stream], 0
cmp [rbp+s], 0
jz loc_3AAF


lea rax, [rbp+var_360]
mov rdi, rax
call mbedtls_aes_init
lea rdi, csPreData ; mutex
call _pthread_mutex_lock
lea rax, [rbp+ptr]
lea rdx, g_RansomHeader
mov ecx, 40h ; '@'
mov rdi, rax
mov rsi, rdx
rep movsq
lea rax, [rbp+var_360]
mov edx, 100h
lea rsi, g_KeyAES
mov rdi, rax
call mbedtls_aes_setkey_enc
lea rdi, csPreData ; mutex
call _pthread_mutex_unlock
mov rax, [rbp+stream]
mov edx, 2 ; whence
mov esi, 0 ; off
mov rdi, rax ; stream
call _fseek
test eax, eax
jnz loc_3ABB

RansomExx

```
ubuntu@ubuntu-VirtualBox:~/Documentos$ cat > honeyfile.txt
This is a test file
ubuntu@ubuntu-VirtualBox:~/Documentos$ ./teste2.exe .
.
ubuntu@ubuntu-VirtualBox:~/Documentos$ ls
 honeyfile.txt.31gs1-4aa9b9dd  '!NEWS_FOR_EIGSI!.txt'   teste2.exe
ubuntu@ubuntu-VirtualBox:~/Documentos$ cat honeyfile.txt.31gs1-4aa9b9dd
[illegible]
[illegible]
[illegible]
[illegible]

ubuntu@ubuntu-VirtualBox:~/Documentos$ cat \!NEWS_FOR_EIGSI\!.txt
Greetings EIGSI!!!

Study this message REGARDFULLY and call administrator from technical division.
Yours information is securely ENCRYPTED.
CHANGING content or names of crypted files (*.31gs1) can make recovering failure.

You can mail us one crypted document (not bigger than 700KB) and we would restore it.
Encrypted file MUST NOT have rich data.
All other data will be your behind the PAYMENT.

Reach us SOLELY if you represent all affected network.
```

RansomExx


@ 9E
@ 9E
uIH9
[]A\A]A^A_
%08x%08x%08x%08x
BFC02A208B37E9B96A9ABFFCCED1086B8865B672540E54B0EBD9811F87C4EEE14B99BEAD9889D9006F9886212
0CB40D9FACDD15F3B8A166B001DA0922444F7A74B7F1C9B1FB4166DF6A1166E077F6F563825A5E2032C6D178C
5D5A387DF7A52F1194A6D3051F9FE3C1553E1ED924E4111C2E7F9F40E764985D5E3E0F0F729BE2D0D61DB2BF0
039FA7FD7D501FE1D51BE496B481BE8AC679ECBB680405283586ECA1C48DD03F161146F76AC21203C67B69268
2BCD7085C21F205484386905FDB5D18A7E5CC1EAB6AB096D6DA48C69C42E221E076187DE4E65E6D9BE8962288
D064AB0BF27288EE4D400309F9419F84C1E5D6C73FD872BEC82889DA987BC49395EE4D1BECBD419CE9F3D4458
DB7861C9617D73C9790BAB7244FD759EF88FF3AE0DF8EE39E3BEE1B049785E280A9E873E039DB44DFA8F35DB5
010001
-%08x
%s/%s
!NEWS_FOR_EIGSI!.txt
.31gs1
Greetings EIGSI!!!
Study this message REGARDFULLY and call administrator from technical division.
Yours information is securely ENCRYPTED.
CHANGING content or names of crypted files (*.31gs1) can make recovering failure.
You can mail us one crypted document (not bigger than 700KB) and we would restore it.
Encrypted file MUST NOT have rich data.
All other data will be your behind the PAYMENT.
Reach us SOLELY if you represent all affected network.
[redacted]@protonmail.com
bRmQ
kWGO
V,Jn
M^+1X
f_?4
CTR_DRBG (PR = TRUE) :
failed
passed
CTR_DRBG (PR = FALSE):
ENTROPY test:
failed

RansomExx

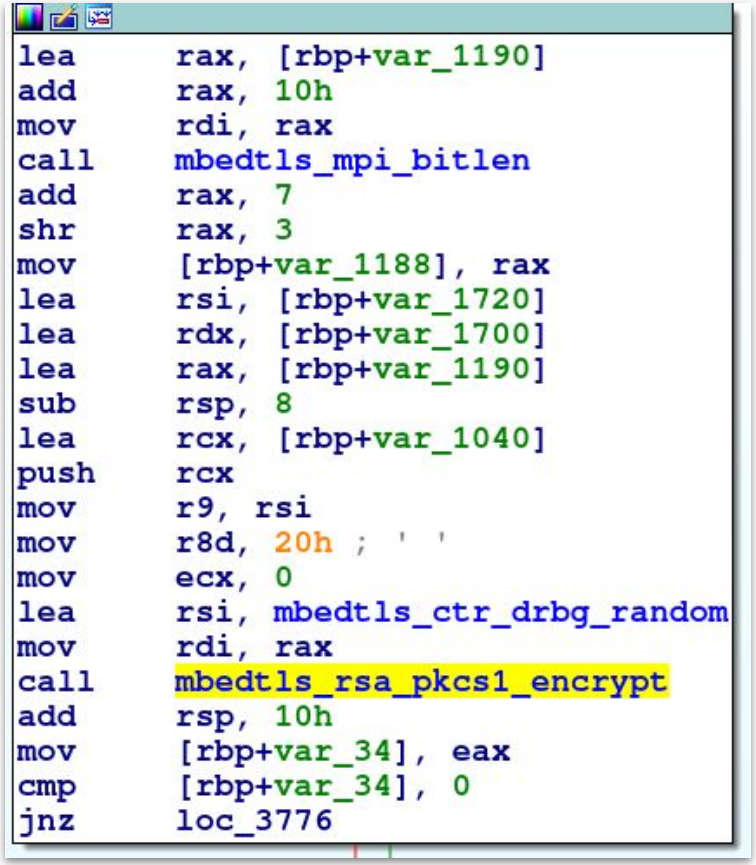
```
ubuntu@ubuntu-VirtualBox:~/Documentos$ hexdump -C honeyfile.txt.31gs1-4aa9b9dd
00000000  04 e0 da 0e 72 1e 9f f4  b7 53 e9 7c ab bd 76 23  |....r....S.|..v#|
00000010  69 6c 65 0a 85 ca 14 ef  81 03 a0 b6 2a 2a 3f 65  |ile.........**?e|
00000020  bd 5d 09 a5 2e c0 cc b9  96 13 0f ae b1 bb d6 37  |.]...........7|
00000030  4a 96 3f 02 25 cd 0a 1b  78 c0 4d bf 7e a1 12 15  |J.?.%...x.M.~...|
00000040  98 ea 71 18 26 f4 e1 cf  27 16 9c c0 b8 84 a4 98  |..q.&...'.......|
00000050  6c 29 e3 52 f1 b3 42 b4  20 6b 83 d3 97 42 55 1e  |l).R..B. k...BU.|
00000060  9d 70 b4 de 28 55 9d 2c  e2 ec 9f e0 a2 3b 69 08  |.p..(U.,.....;i.|
00000070  2a a5 50 86 7e 63 78 61  84 d1 a0 48 1b 59 ba f9  |*.P.~cxa...H.Y..|
00000080  e3 9b 2d 13 7f 40 1e 82  07 ad 2a c3 ab 26 5e 7e  |..-..@....*..&^~|
00000090  69 fd 73 32 35 69 4e 12  7c 77 92 5e df 8d 0a 2b  |i.s25iN.|w.^...+|
000000a0  40 79 ff d4 e7 d4 57 a3  cc ab df 05 c2 4e 61 ca  |@y....W......Na.|
000000b0  01 5c c1 98 4f f6 c7 0c  0a 31 db 28 59 78 85 98  |.\..O....1.(Yx..|
000000c0  36 3c bf 63 01 73 44 c0  84 aa 0e 58 14 f7 9d 3b  |6<.c.sD....X...;|
000000d0  ed 25 ee 1d 13 32 c5 40  f1 bb 18 d2 42 09 d6 2d  |.%...2.@....B..-|
000000e0  5a dd 84 9a cc 17 3c ca  c4 b9 27 49 12 29 d1 a2  |Z.....<...'I.)..|
000000f0  cf df da bd 3a d4 4f 8a  dd 81 08 1b 03 f1 f4 27  |....:.O........'|
00000100  7c ff a5 fc 50 3c ed 76  1f c0 64 2c 43 ff ed 39  ||...P<.v..d,C..9|
00000110  bf bd 76 ac 39 a3 40 4a  a0 8b 2f 3c 0c 19 4d fb  |..v.9.@J../<..M.|
00000120  ee 70 a7 c8 06 9a 91 66  df f6 ca 0f 13 46 18 ec  |.p.....f.....F..|
00000130  70 b9 40 84 9d 76 13 af  bb f9 df 99 bd 10 1b 6f  |p.@..v.........o|
00000140  62 3e 13 9c 38 9a 18 9b  e4 a2 fd f7 71 09 e6 b7  |b>..8.......q...|
00000150  1f c2 63 4c a2 e4 99 2d  db 59 a0 27 0d e7 c3 3d  |..cL...-.Y.'...=|
00000160  d6 74 c1 93 9b e9 6e a4  7b d8 d9 e5 88 6d f2 2d  |.t....n.{....m.-|
00000170  2a dd eb fe 2f 86 2c 02  11 79 4b 5a 3d 42 3d d5  |*.../.,..yKZ=B=.|
00000180  30 66 01 c2 29 a0 5f 11  4d 91 8b ab c4 b5 97 d5  |0f..)._.M.......|
00000190  dc fd be a6 e0 61 fa 21  f8 50 06 35 e3 7a d3 c4  |.....a.!.P.5.z..|
000001a0  65 fd b0 82 76 5a 13 5d  ea 04 98 12 33 81 25 d6  |e...vZ.]....3.%.|
000001b0  c1 2b 81 ec ea 0b 6d d2  e3 44 78 ec 39 b5 ea 44  |.+....m..Dx.9..D|
000001c0  8c d8 9b 28 ad 0a 8a a0  15 c9 b2 a1 dd 8d fd 4c  |...(...........L|
000001d0  84 5d a4 20 6d 70 18 90  0e 09 78 d8 8f b8 18 61  |.]. mp....x....a|
000001e0  8e ac 6d a8 04 5c ce 1a  4b d9 dd c6 84 73 4c 2a  |..m..\..K....sL*|
000001f0  49 6a 2d 72 f0 3f 40 e2  fa a0 a9 f3 95 69 7c 48  |Ij-r.?@......i|H|
00000200  d5 8d fb 5b 1d ec 9f 10  59 79 ae 65 83 54 d2 9e  |...[....Yy.e.T..|
```

```
ubuntu@ubuntu-VirtualBox:~/Documentos$ hexdump -C honeyfile.txt.31gs1-7c4f31ff
00000000  a7 c2 f3 d2 68 1b 9b 4c  a0 ee 30 e5 13 e1 a1 5c  |....h..L..0....\|
00000010  69 6c 65 0a 3d 46 5a 07  6b ed e1 0e d1 82 3a 87  |ile.=FZ.k.....:.|
00000020  2f 31 19 13 94 99 7d 97  2b 42 d7 72 3a 4a 5f e7  |/1....}.+B.r:J_.|
00000030  df 86 a4 d5 0e 5f fa e1  e1 03 64 61 2a c1 99 b2  |....._....da*...|
00000040  97 56 90 09 ba 71 4e 0e  db 1b 34 34 4f aa 47 ff  |.V...qN...44O.G.|
00000050  25 c6 5c c7 24 fd e9 37  b2 66 01 64 1f c4 dd e7  |%.\.$..7.f.d....|
00000060  1f 7a 1c b0 5e f8 a6 9f  85 9b 6b c7 9d f3 c6 f7  |.z..^.....k.....|
00000070  52 88 73 f3 20 b5 c0 75  00 02 92 b1 d4 5f c2 67  |R.s. ..u....._.g|
00000080  c4 33 f7 cc ec 42 f6 f6  79 08 6d f4 c0 a4 ac df  |.3...B..y.m.....|
00000090  62 fd 46 a2 e1 62 19 1b  d3 b7 2e e5 b4 74 2f c4  |b.F..b.......t/.|
000000a0  93 a4 26 60 16 e4 e8 8e  61 02 35 c4 55 25 b8 62  |..&`....a.5.U%.b|
000000b0  57 7f ac f2 c0 93 4c f1  3d 3f 65 4d cb 00 fb 5f  |W.....L.=?eM..._|
000000c0  7b 84 82 94 02 66 ef 53  69 0f a3 ed cb ee 26 8f  |{....f.Si.....&.|
000000d0  b3 53 3a c4 32 bf c8 3b  81 c2 e6 82 70 72 fd 9a  |.S:.2..;....pr..|
000000e0  0b 88 8e e0 c2 c9 94 f6  78 a0 ac ce 82 fc dd 46  |........x......F|
000000f0  7d 76 be cf 4f c4 ca 41  41 07 09 5f 93 0d 86 eb  |}v..O..AA._....|
00000100  8a 43 a0 84 48 cf d9 e6  65 3f f0 f5 ab 0b 6e 4e  |.C..H...e?....nN|
00000110  6a 25 f8 b5 ec 3c d9 f4  69 e5 db 6a a7 1e 50 0e  |j%...<..i..j..P.|
00000120  b2 0b 6a 9d 5d 90 b9 39  56 f3 35 8d f9 1d 40 fd  |..j.]..9V.5...@.|
00000130  6b 2f 35 35 78 67 4b f5  12 e2 5f c4 18 cd 89 63  |k/55xgK..._....c|
00000140  f0 b4 fc 0b 25 86 f9 17  8f c5 ea fc a8 3e e0 36  |....%........>.6|
00000150  f8 05 9f d6 7f 52 ea 83  7f fb 29 bb 76 47 7e cd  |.....R....).vG~.|
00000160  ab 10 28 78 db 7a f7 ae  73 c1 a4 fb b7 f9 41 f0  |..(x.z..s.....A.|
00000170  92 7f 57 1d f7 af 37 96  77 1b ba 3c 3e 94 31 c9  |..W...7.w..<>.1.|
00000180  b4 b6 fb ce 87 12 e8 4e  d6 83 48 1e 39 0d 4f 1e  |.......N..H.9.O.|
00000190  4d 3d 01 dc 3c e0 81 92  de 85 e1 f3 d5 91 8b 3c  |M=..<..........<|
000001a0  f5 9c d0 ef 96 36 6c de  95 d4 e3 56 be 7b cc 45  |.....6l....V.{.E|
000001b0  d5 a4 75 fc b9 f2 50 44  7c 46 aa 6b d9 7b e7 43  |..u...PD|F.k.{.C|
000001c0  bc fa b8 fa 84 ee 65 fc  5c 66 c3 d6 8f 6d 68 52  |......e.\f...mhR|
000001d0  4b 2a 15 73 b2 9c 6a f2  fd e3 3e 6f e9 91 41 f8  |K*.s..j...>o..A.|
000001e0  2e b0 c1 71 50 34 30 c6  25 f0 e4 3c 7f 4c 65 20  |...qP40.%..<.Le |
000001f0  b5 2b 30 48 13 33 6b fc  13 e8 a8 86 8d 6a 84 09  |.+0H.3k......j..|
00000200  4b f5 f7 1e 85 0a 9f 5b  13 d5 52 7a 53 d7 f8 d6  |K......[..RzS...|
```

RansomExx

```
(gdb) set $eax = 0x5fa6d4d6
(gdb) set $edi = 0x5fa6d4d6
(gdb) c
Continuando.

Breakpoint 4, 0x00005555555576da in GeneratePreData ()
(gdb) info registers rax
rax            0x356eb83d7876829f       3850217305601901215
(gdb)
```

RansomExx

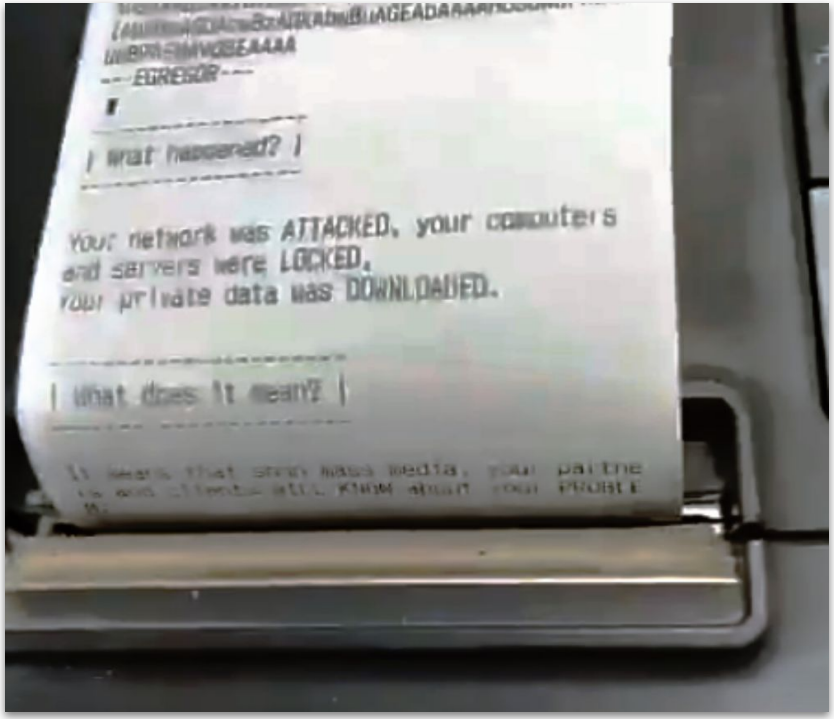


```
lea     rax, [rbp+var_1190]
add     rax, 10h
mov     rdi, rax
call    mbedtls_mpi_bitlen
add     rax, 7
shr     rax, 3
mov     [rbp+var_1188], rax
lea     rsi, [rbp+var_1720]
lea     rdx, [rbp+var_1700]
lea     rax, [rbp+var_1190]
sub     rsp, 8
lea     rcx, [rbp+var_1040]
push    rcx
mov     r9, rsi
mov     r8d, 20h ; ' '
mov     ecx, 0
lea     rsi, mbedtls_ctr_drbg_random
mov     rdi, rax
call    mbedtls_rsa_pkcs1_encrypt
add     rsp, 10h
mov     [rbp+var_34], eax
cmp     [rbp+var_34], 0
jnz     loc_3776
```

Para Onde Vamos?

Educação ainda é a chave...

PoS Ransomware



Como se proteger

- Não negligencie seu **BACKUP!**

https://cartilha.cert.br/ransomware/ransomware-folheto.pdf

Como se proteger

- Não negligencie seu **BACKUP!**
- Além disso:
  - **Evite acesso** desmedido a links e anexos em e-mails
  - Preste atenção em *malvertising* e use um **bloqueador de *ads***
  - **Desabilite funcionalidades desnecessárias**/extras em leitores de PDF, como execução de JavaScript
  - Mantenha SO, *browsers*, aplicativos, *plug-ins*, serviços e mecanismos de segurança **atualizados**
  - Desenvolva políticas de segurança e as **implemente** na prática
  - **Verifique** o uso das políticas e o nível de alerta de seus usuários

Considerações Finais

Backups everywhere

Como se proteger

- Faça **BACKUP!**
- Certifique-se de que seu **BACKUP** restaure
- Proteja seu **BACKUP** que está na rede
- Tenha um **BACKUP** offline das coisas mais importantes do seu **BACKUP...**

https://cartilha.cert.br/fasciculos/backup/fasciculo-backup.pdf

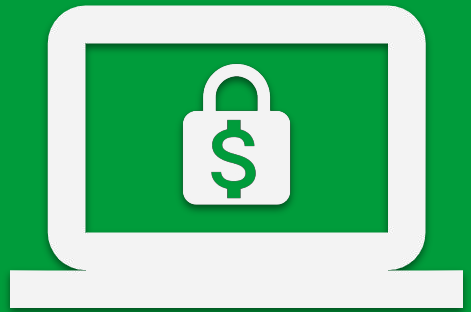
Lembrem-se:

https://www.trinustech.com/wp-content/uploads/2019/03/In-case-of-cyber-attack-please-break-glass-and-pull-cables.jpg

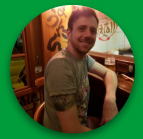
Conclusion

- Leituras
  - “The other guys: automated analysis of marginalized malware”: https://secret.inf.ufpr.br/papers/behemot.pdf
  - “A Ransomware in a Brazilian Justice Court”: https://secret.inf.ufpr.br/2020/11/06/a-ransomware-in-a-brazilian-justice-court/
  - “Brazilian Justice Court Ransomware: Another piece in the Puzzle”: https://secret.inf.ufpr.br/2020/11/17/brazilian-justice-court-ransomware-another-piece-in-the-puzzle/
  - “An Obfuscation Tour”: https://secret.inf.ufpr.br/2020/05/08/an-obfuscation-tour/
  - “Ransomware in Times of Coronavirus”: https://secret.inf.ufpr.br/2020/05/08/ransomware-in-times-of-coronavirus/

Integridade, confidencialidade, disponibilidade, ransomware



Contato: {gregio, mfbotacin}@inf.ufpr.br
Website: secret.inf.ufpr.br



André Grégio
Federal University of Paraná, BR
@abedgregio

Marcus Botacin
Federal University of Paraná, BR
@MarcusBotacin

GTER 49 | GTS 35
30 DE NOVEMBRO A 1º DE DEZEMBRO DE 2020
EDIÇÃO ON-LINE