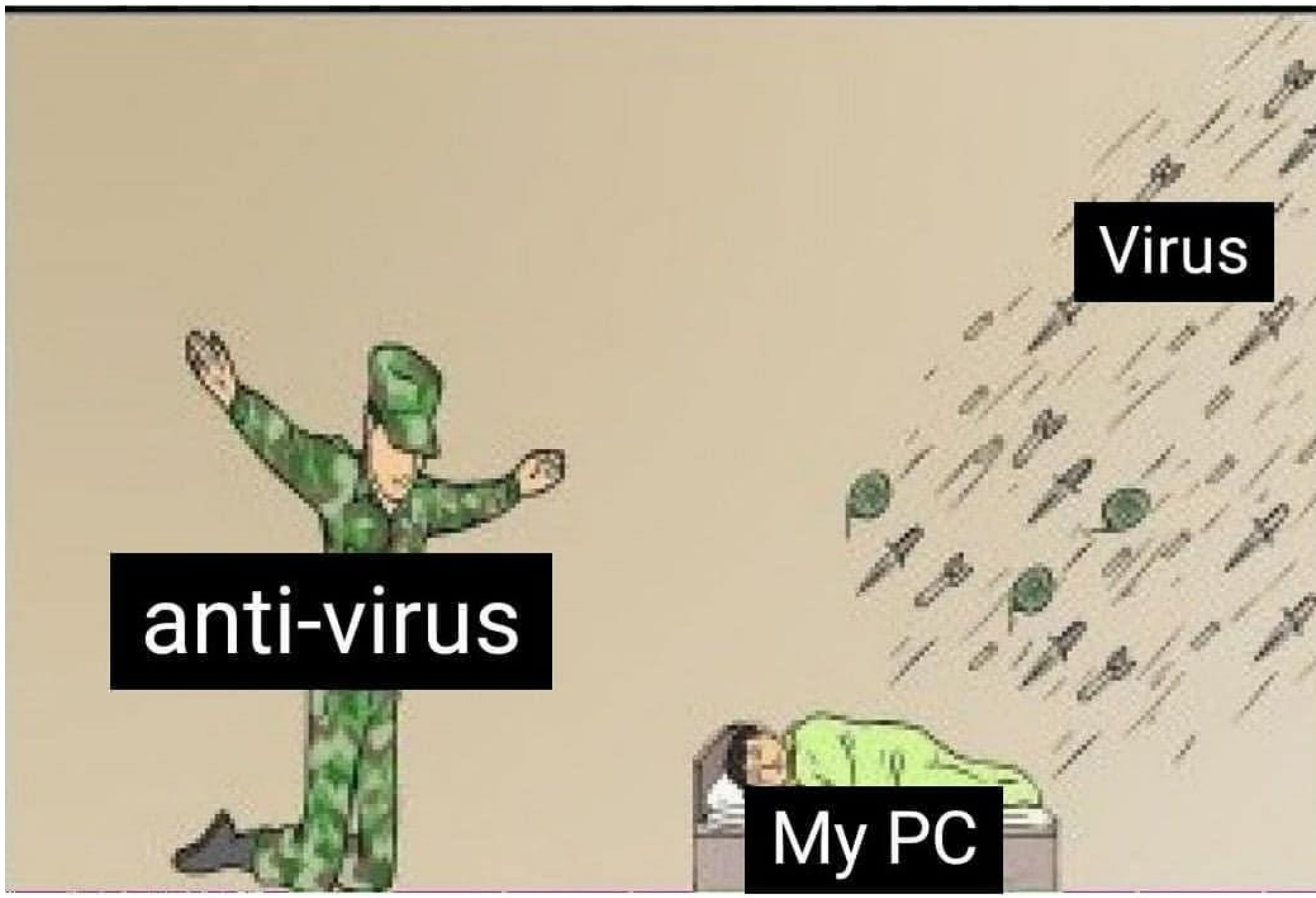
Ransomware.

Auditoria e segurança.

Contexto.

O temo “ransoware” surgiu da junção da palavra ransom, que significa resgate com malware.

Tornou-se umas das principais ameaças cibernéticas atualmente, impactando milhões de empresas e pessoas.



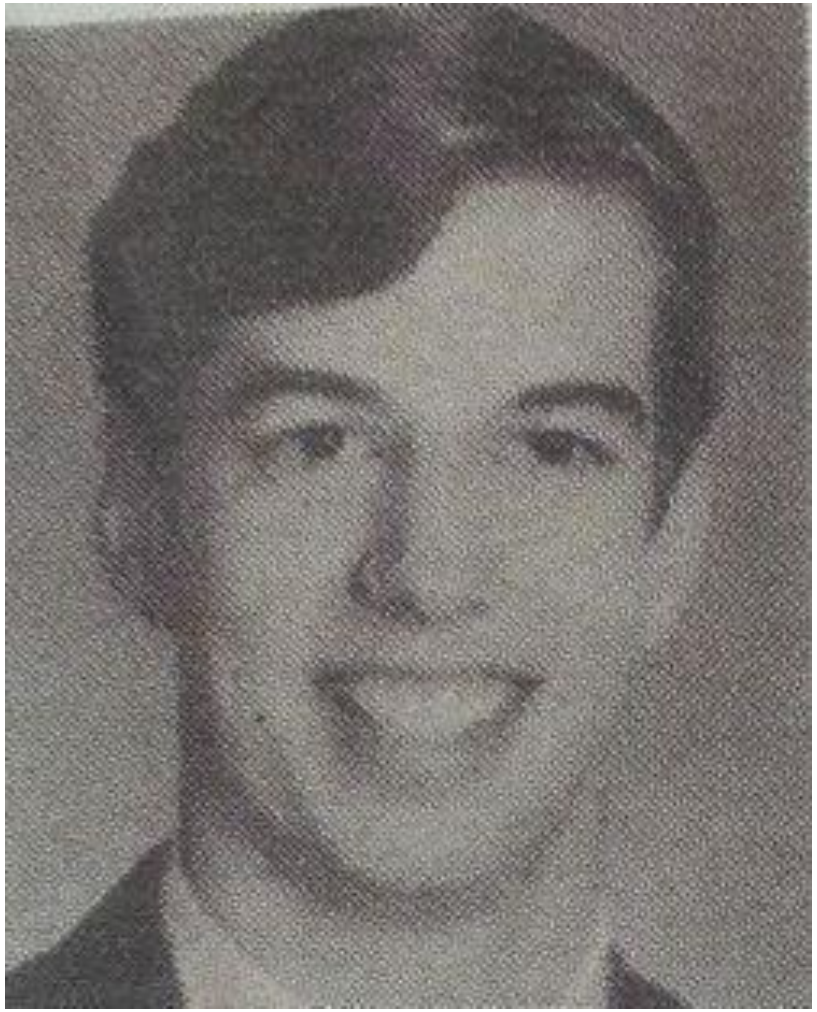
Tipos de ransomware.

Ransomware Locker: impede que você acesse o equipamento infectado.

Tipos de ransomware.

Ransomware Crypto: impede que você acesse aos dados armazenados no equipamento infectado, geralmente usando criptografia.

Ransomware quando não exisitia ransomware.



Joseph L Popp Jr, que futuramente viria a ser considerado o “Pai do Ransomware”

O “Pai do Ransomware” não era um hacker, profissional de TI, ou outra coisa do tipo, e sim um biologista.

Joseph se tornou o antecessor daquilo que anos depois se tornaria a ser um dos crimes cibernéticos mais lucrativos de todos os tempos.

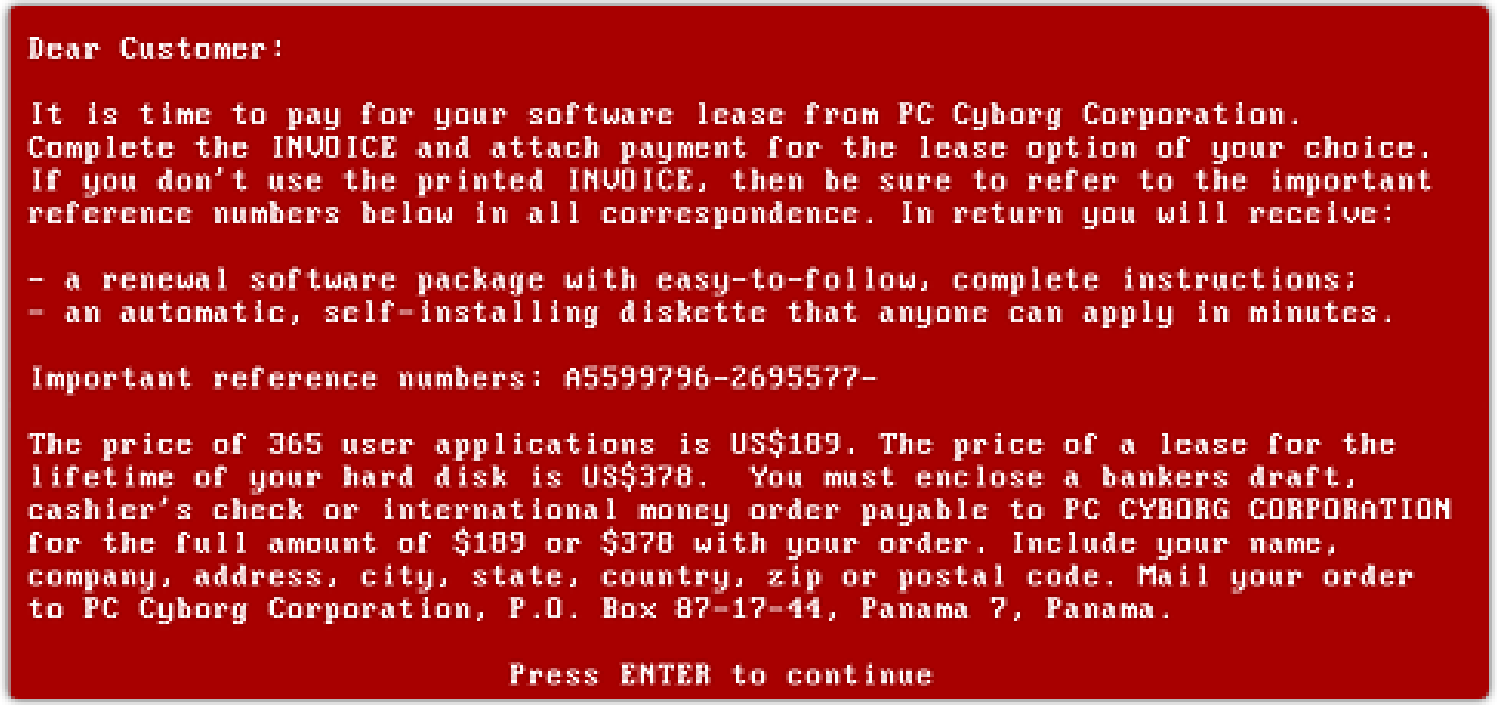
Rejeição em uma vaga de emprego e o crime.

Após ser rejeitado para trabalhar na OMS, Joseph enviou cerca de 20.000 disquetes pelo correio aos participantes da conferência de AIDS da Organização Mundial da Saúde em Estocolmo.

O incidente criou muitos problemas danos naquela época, com empresas perdendo anos de pesquisa.

Após alguns dias da infecção ele pedia para enviar $ 189 para uma caixa postal no Panamá para liberar os dados.

Rejeição em uma vaga de emprego e o crime.



Os diretórios ainda estavam lá, mas estavam ocultos e os nomes dos arquivos foram alterados para strings de caracteres aleatórios. O conteúdo de seus arquivos permaneceu inalterado.

AIDS Information - Introductory Diskette

Please find enclosed a computer diskette containing health information on the disease AIDS. The information is provided in the form of an interactive computer program. It is easy to use. Here is how it works:

- The program provides you with information about AIDS and asks you questions
- You reply by choosing the most appropriate answer shown on the screen
- The program then provides you with a confidential report on your risk of exposure to AIDS
- The program provides recommendations to you, based on the life history information that you have provided, about practical steps that you can take to reduce your risk of getting AIDS
- The program gives you the opportunity to make comments and ask questions that you may have about AIDS
- This program is designed specially to help: members of the public who are concerned about AIDS and medical professionals.

Instructions

This software is designed for use with IBM® PC/XT™ microcomputers and with all other truly compatible microcomputers. Your computer must have a hard disk drive C, MS-DOS® version 2.0 or higher, and a minimum of 256K RAM. First read and assent to the limited warranty and to the license agreement on the reverse. [If you use this diskette, you will have to pay the mandatory software leasing fee(s).] Then do the following:

Step 1: Start your computer (with diskette drive A empty).

Step 2: Once the computer is running, insert the Introductory Diskette into drive A.

Step 3: At the C> prompt of your root directory type: A:INSTALL and then press ENTER. Installation proceeds automatically from that point. It takes only a few minutes.

Step 4: When the installation is completed, you will be given easy-to-follow messages by the computer. Respond accordingly.

Step 5: When you want to use the program, type the word AIDS at the C> prompt in the root directory and press ENTER.

Hacker, hackeia?

O WannaCry foi o marco na indústria do crime cibernético, onde percebeu-se a possibilidade de lucrar com os ataques.... E talvez com uma ajudinha estatal.

O WannaCry foi possível graças falha revelada num vazamento de dados da NSA (agência de segurança digital dos EUA) feito pelo grupo de hackers conhecido como Shadow Brokers.

De volta para você, amigo.

Em meio a esse vazamento existia até o momento uma falha desconhecida até mesmo da própria Microsoft. Foi publicada uma atualização para essa falha, mas muitos computadores não foram atualizados, o que ajuda a explicar o sucesso do ataque.

A falha ficou conhecida como conhecida como "EternalBlue"

De herói a vilão.

Marcus Hutchins foi o responsável por parar o ataque do WannaCry ao registrar um domínio aleatório que servia como uma espécie de freio.

Tempos depois foi preso nos EUA na DEFCON. Ironicamente ele era responsável pelo o desenvolvimento de uma malware bancário.

Acabou confessando seus crimes e sendo inocentado devido ao seu trabalho.

200,000+ Systems Affected by WannaCry Ransom Attack

The WannaCry ransomware attack in numbers

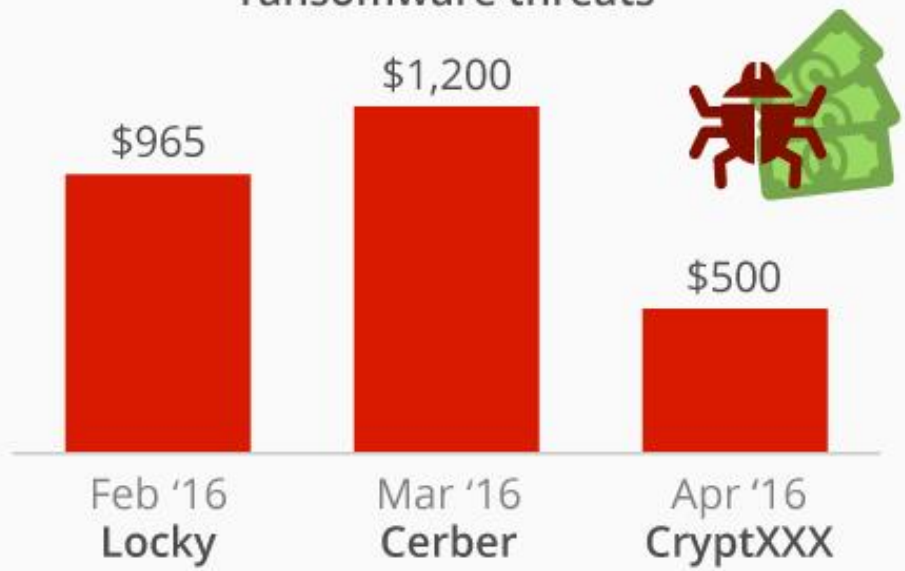
Affected systems
>220,000

Affected countries
150

Ransom per system
$300

Average ransom in past ransomware attacks

Approx. ransom in major ransomware threats



Sources: Media reports, Symantec

Ataques virtuais, consequências no mundo real.

Criança de 3 anos sofre overdose de medicamentos depois de sistema de hospital ser atacado por hackers

BBC NEWS BRASIL

Notícias Brasil Internacional Economia Saúde Ciência Tecnologia Vídeos

O ataque de hackers a maior oleoduto dos EUA que fez governo declarar estado de emergência

OLHAR DIGITAL

NOTÍCIAS VÍDEOS EDITORIAS SUPORTE OD SEGURANÇA OFERTA

Olhar Digital > Notícias > Ataque de ransomware em hospital leva paciente à morte na Alemanha

NOTÍCIAS SEGURANÇA E PRIVACIDADE

Ataque de ransomware em hospital leva paciente à morte na Alemanha

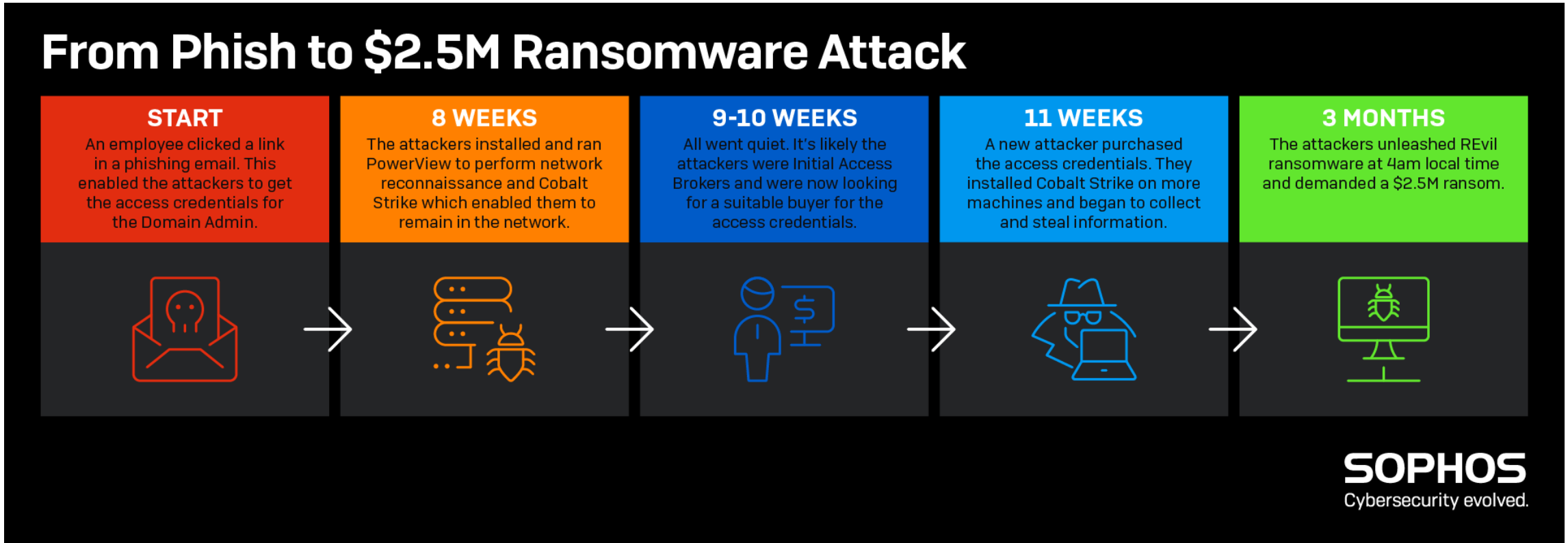
Devido a inoperabilidade do local em questão, a vítima teve de procurar atendimento para sua condição crítica em uma unidade mais distante, não resistindo à espera

Como a infecção ocorre?

1. Phishing;
2. Mídias infectadas;
3. Insiders.

Phishing

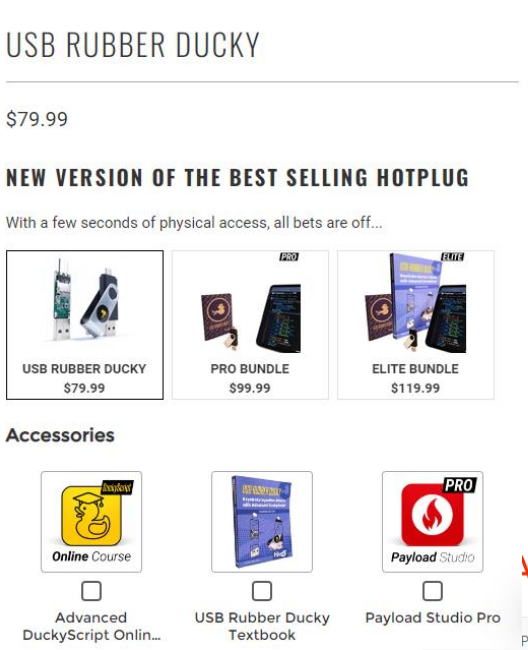
Ataques de phishing são os principais vetores de ataque para ocasionar um ataque de ransomware. Phishing consistem em e-mails falsos com propósito de roubar dados. Abaixo o esquema de uma campanha bem sucedida:

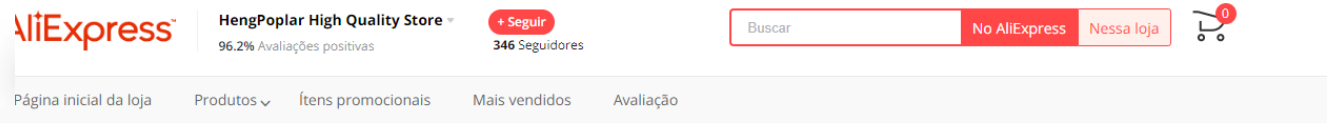


Mídias infectadas.

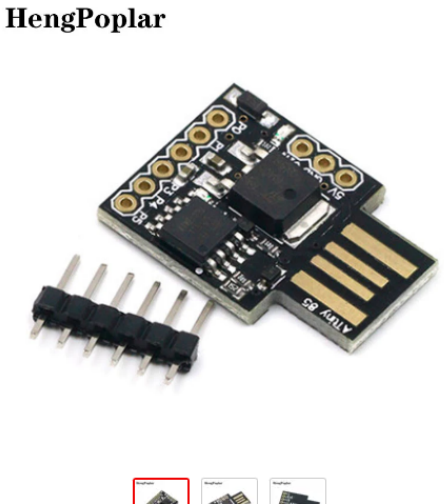
Ao conectar o dispositivo sem realizar checagens de segurança a máquina pode ser infectada abrindo portas para futuros ataques. Dados do FBI indicam que a campanha de ataque começou em 2021.

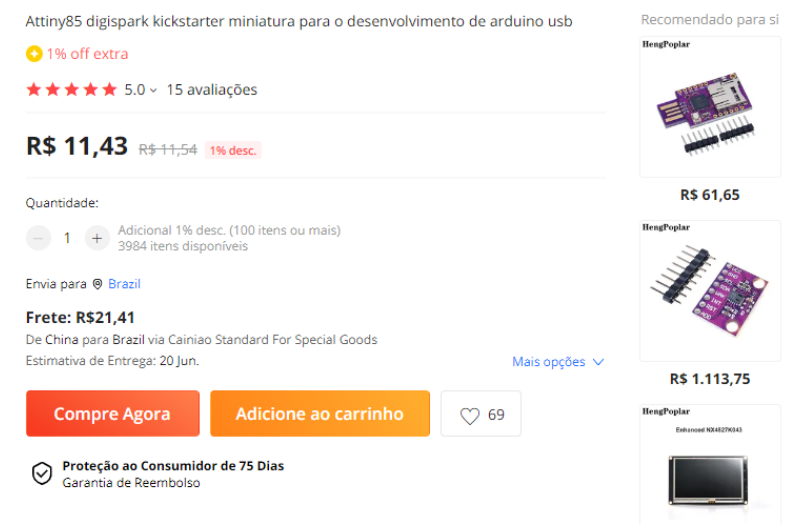
Mídias infectadas.





USB Rubber Ducky x Digispark





Insiders.

O que estamos vendo agora é que alguns grupos de ransomware preferindo fazer parceria diretamente com um funcionário interno. O LockBit 2.0 foi pioneiro nessa abordagem.

Por Altieres Rohr
É fundador de um site especializado na defesa contra ataques cibernéticos

FBI prende russo acusado de oferecer US$ 1 milhão para funcionário da Tesla instalar vírus de resgate em fábrica

Como Funciona um Ataque?

A vítima clica ou baixa um arquivo contendo o código malicioso enviado por email ou baixado de um site.

O Ransomware se instala e se conecta com o criminoso que originou o ataque.

O malware inicia o ataque criptografando os arquivos da vítima.

O malware utiliza falhas do sistema para infectar outras máquinas da rede.

A vítima paga o resgate ou perde os seus arquivos para sempre.

Um planejamento adequado de backup e recuperação evitaria o problema.

Infobusiness

Nova fase: Roubo de dados e extorsão.

A tecnologia evolui, assim como o crime também, com isso as gangues arranjaram novas maneiras de ganhar dinheiro além da criptografia dos dados por meio da extorsão através de:

1. DDOS
2. Vazamento dos dados
3. Denuncia a autoridades

Nova fase: Roubo de dados e extorsão.

Happy Blog

Blog search

Search

[redacted]

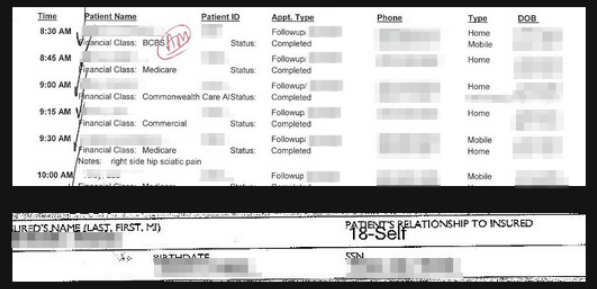
Hello [redacted] - some of your files containing **confidential** information have been **downloaded** and are located on our servers. If you refuse to negotiate with us, **all documents** will be **published** on the **blog** and published by the **media**. If an agreement is reached, the data will be permanently deleted. We advise you to quickly contact us through the **support chat**.

Name	Type	Compressed size	Password ...	Size	Ratio
[redacted]	Microsoft Excel Worksheet	14 KB	No	17 KB	19%
	Microsoft Excel Worksheet	13 KB	No	15 KB	20%
	Microsoft Excel Worksheet	12 KB	No	15 KB	20%
	Microsoft Excel Worksheet	24 KB	No	87 KB	74%
	Microsoft Excel Worksheet	44 KB	No	49 KB	10%
	Microsoft Excel Worksheet	1 KB	No	1 KB	87%
	Microsoft Excel Worksheet	1 KB	No	1 KB	87%
	Microsoft Excel Worksheet	22 KB	No	25 KB	12%
	Microsoft Excel Worksheet	176 KB	No	179 KB	2%
	Microsoft Excel Worksheet	54 KB	No	57 KB	7%
	Microsoft Excel Worksheet	17 KB	No	20 KB	16%
	Microsoft Excel Worksheet	334 KB	No	338 KB	2%
	Microsoft Excel Worksheet	141 KB	No	152 KB	8%
	Microsoft Excel Worksheet	242 KB	No	249 KB	4%
	Microsoft Excel Worksheet	322 KB	No	338 KB	5%
	Microsoft Excel Worksheet	375 KB	No	379 KB	2%
	Microsoft Excel Worksheet	63 KB	No	66 KB	4%

Data Leak **Blog**

[redacted]

Patients, employees information.



Site: https://[redacted].com
Stolen files: mega.nz

[redacted]

The first dump, if the company continues to be silent, we will continue to publish other parts.

Site: https://[redacted]
Stolen files #1: mega.nz

DD4BC
Newbie

Online

Activity: 7

Trust: -4: -1 / +0(0)
Warning: Trade with extreme caution!

What do you prefer?

What would you like more?

1. I ddos your site.

2. I report you [redacted] for running illegal gambling site.

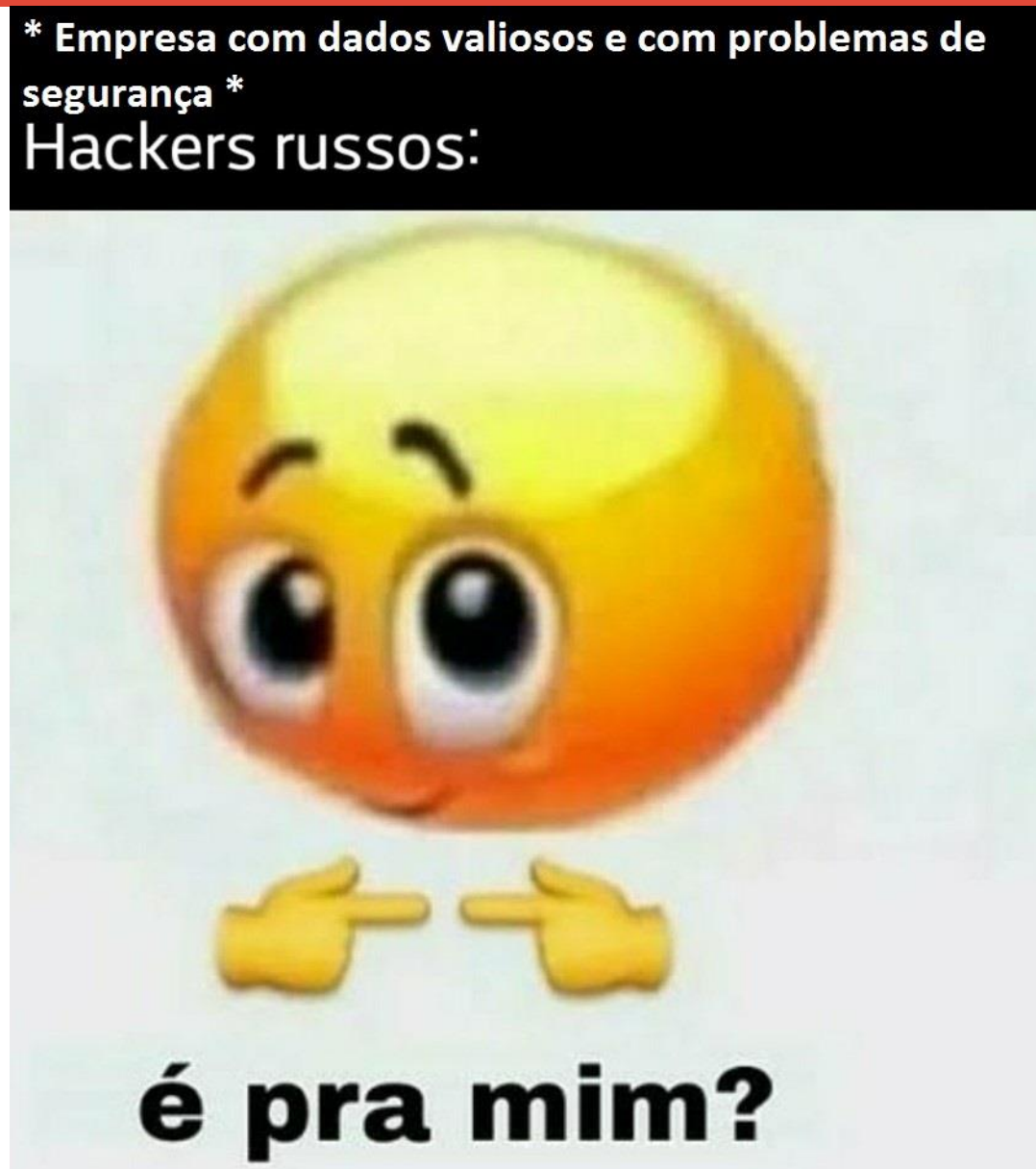
3. You pay me 2 BTC to 17WQov8BTXJAemWmqn5XJ8ibiq13SNoaqs

Chose one option!

btw. Do you know why you are down while competition is up? Because they pay.

Inimigo do meu inimigo é meu amigo.

Uma das razões pelas quais tantos hackers parecem vir da Rússia e de partes da antiga União Soviética é que esses países colocam uma ênfase muito maior do que as instituições educacionais no Ocidente no ensino de tecnologia nas escolas de ensino fundamental e médio. Aliado a isso há questões em que tecnicamente o crime cibernético é liberado, desde que não seja direcionado a empresas ou cidadãos russos.



Projeto “No More Ransom”

É uma iniciativa da Unidade de Crime de Alta Tecnologia da Polícia Holandesa, do European Cybercrime Centre (EC3) da Europol, Kaspersky e McAfee com o objetivo de ajudar as vítimas de ransomware a recuperar os seus dados cifrados sem terem que pagar a criminosos.

Agências Policiais:

INTERPOL

GCC POL

Bundeskriminalamt

Alemanha

AFP
AUSTRALIAN FEDERAL POLICE

Austrália

POLICIA
FEDERAL

Brazil

Bulgária

POLICIJA
ПОЛИЦИЈА
BRČKO DISTRIKT BIH
БРЧКО ДИСТРИКТ БИХ

Bósnia e Herzegovina

Canadá

Como se proteger?

1. Nunca clique em links inseguros;
2. Mantenha uma rotina de backup desconectado da rede e separado;
3. Evite divulgar informações pessoais;
4. Não abra anexos de e-mail suspeitos;
5. Nunca use USB’s desconhecidos;
6. Mantenha seus programas e sistema operacional atualizados;
7. Use apenas fontes de download conhecidas;
8. Use serviços VPN em redes Wi-Fi públicas.

PatrikH0lop / malware_showcase Public

Watch 33 | Fork 264 | Star 1.4k

Code | Issues | Pull requests 1 | Actions | Projects | Security | Insights

master | 2 branches | 0 tags | Go to file | Add file | Code

PatrikH0lop Add simple dropper in Python. ... 452312c on May 8, 2020 18 commits

adware	Add simple adware in Python.	4 years ago
dropper	Add simple dropper in Python.	3 years ago
file_infection	Add simple file infector in Python.	4 years ago
ransomware	Add simple ransomware in Python.	4 years ago
spyware	Add simple spyware in Python.	4 years ago
trojan	Add simple trojan in Python.	4 years ago
worm	Add simple SSH worm in Python.	4 years ago
LICENSE	Add official license.	4 years ago
README.md	Add simple dropper in Python.	3 years ago
logo.svg	Add a repository logo to README	4 years ago

About

Understand the nature of malicious software with practical examples in Python.

Readme

MIT license

1.4k stars

33 watching

264 forks

Report repository

Releases

No releases published

CRIAÇÃO DE RANSOMWARE MULTI-PLATAFORMA COM JAVASCRIPT ES6

POR THAU0x01

HACKA FLAG ACADEMY

Parte prática.

Demonstração