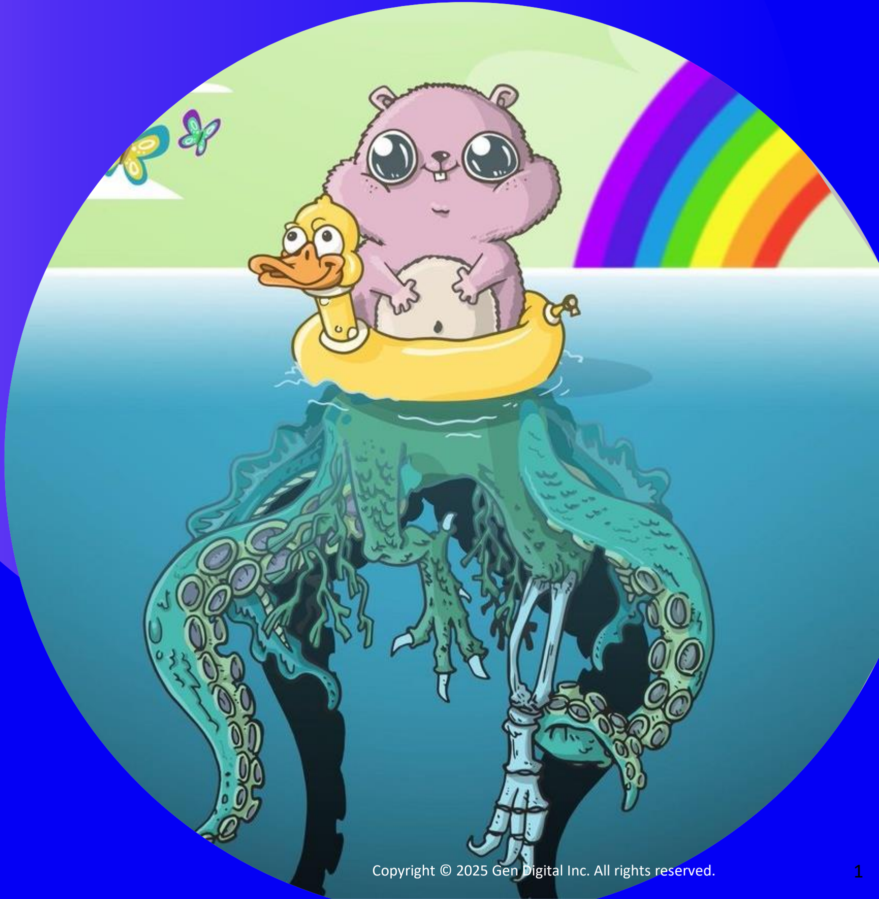
Demystifying Malware and Ransomware

2027-03-17

Ladislav Zezula, Jakub Křoustek



About Me

- Senior Malware Researcher at Grisoft → AVG → Avast → Norton → Gen
  - Malware analysis
  - Writing detection rules in YARA
  - Co-author of Win64/Win32 emulator
  - Ransomware decryption tools
  - File infector cleaning tools (read: an obsolete stuff)
- ladislav.zezula[at]gendigital.com
- X: @LadislavZezula

Agenda

1. Malware types
2. Malware detection crash course
3. Ransomware dissection
4. Conclusion

What is Malware?

- Malware = **Mal**icious Soft**ware**
- Started about in 1970s - demonstrate technical skills, ego… (Creeper 1971)
- File infectors in 1990s - mass spreading (OneHalf, Tremor, Helloween, …)
- Shifted to financial gain in 2000s (Zeus 2007)
- Evolved into espionage, government-sponsored hacking, cyberwar (up to today)
- Billion-dollar business for cyber-threat authors
- Trillion-dollar problem to solve

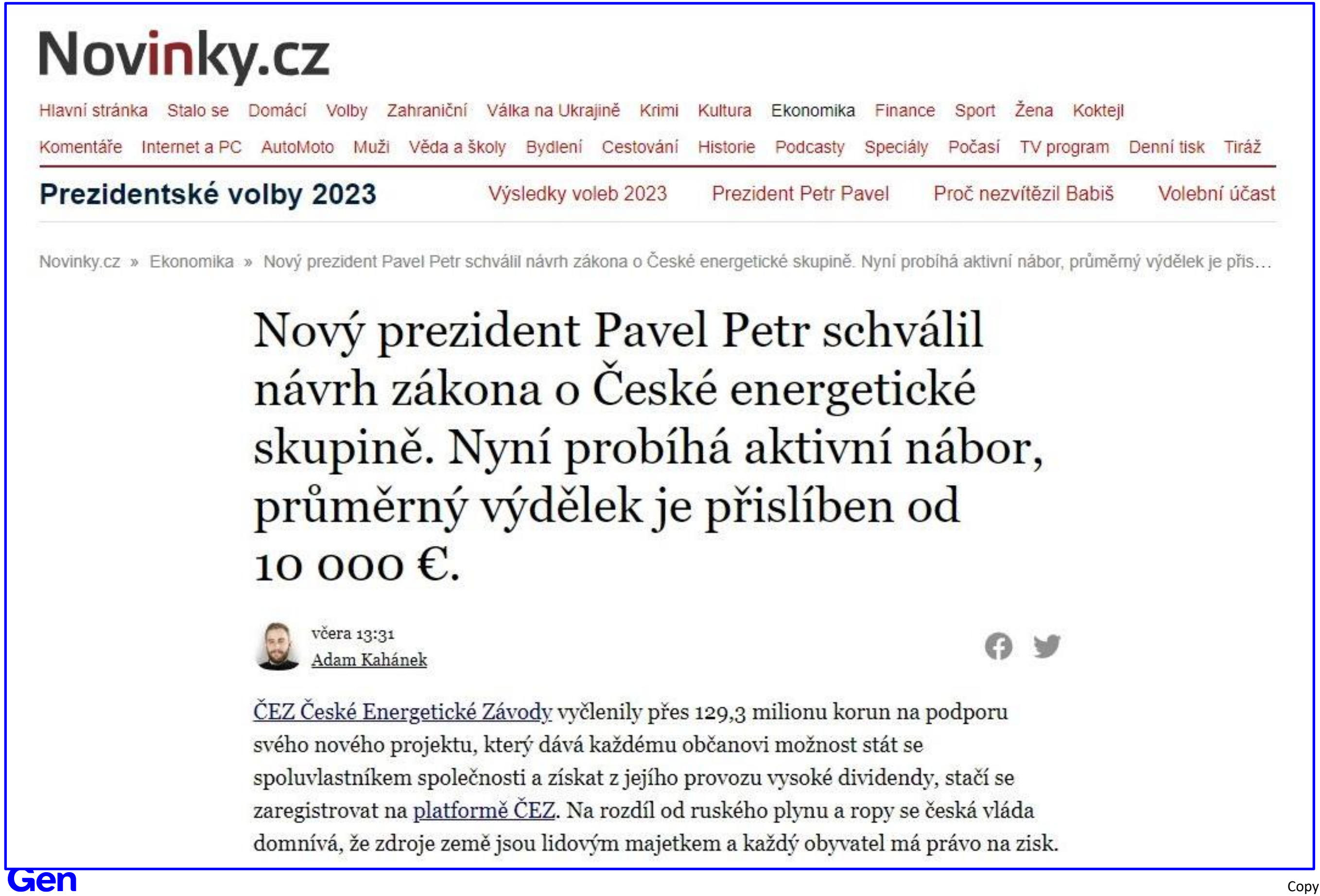
Malware Taxonomy

- **Information stealer**
  - Steals passwords, banking credentials, crypto wallet keys, etc.
  - Many subtypes: Banking trojan, Keylogger, Password stealer, Spyware, Stalkerware…
- **Malicious remote access**
  - Secures long-term access to the infected computer to utilize its resources
  - Many subtypes: Bot, Backdoor, Remote access trojan (RAT)…
- **Scam**
  - Trick you into giving an attacker your personal information or money
  - Many subtypes: Phishing, Spear-phishing, Dating scam, Financial scam, E-shop scam…
- **Other**
  - Adware, ATM, Bootkit, Rootkit, Coin miner, Cryptic, Dialer, Dropper, Exploit, File infector, Hack tool, Injector, Ransomware, Screenlocker, Trojan, Wiper, Worm, and many more

Threat Example: Wiper

- Destructive type of malware
- Goal: loss of control and data
- HermeticWiper (used by Russia in Ukraine 23-Feb-2022)
  - https://x.com/ESETresearch/status/1496581903205511181
- BlackEnergy (23-Dec-2015 in Ukraine)
  - https://en.wikipedia.org/wiki/2015_Ukraine_power_grid_hack

Threat Example: Scam and Phishing


Novinky.cz
Hlavní stránka Stalo se Domácí Volby Zahraniční Válka na Ukrajině Krimi Kultura Ekonomika Finance Sport Žena Koktejl
Komentáře Internet a PC AutoMoto Muži Věda a školy Bydlení Cestování Historie Podcasty Speciály Počasí TV program Denní tisk Tiráž
Prezidentské volby 2023
Výsledky voleb 2023 Prezident Petr Pavel Proč nezvítězil Babiš Volební účast
Novinky.cz » Ekonomika » Nový prezident Pavel Petr schválil návrh zákona o České energetické skupině. Nyní probíhá aktivní nábor, průměrný výdělek je přis…

Nový prezident Pavel Petr schválil návrh zákona o České energetické skupině. Nyní probíhá aktivní nábor, průměrný výdělek je přislíben od 10 000 €.

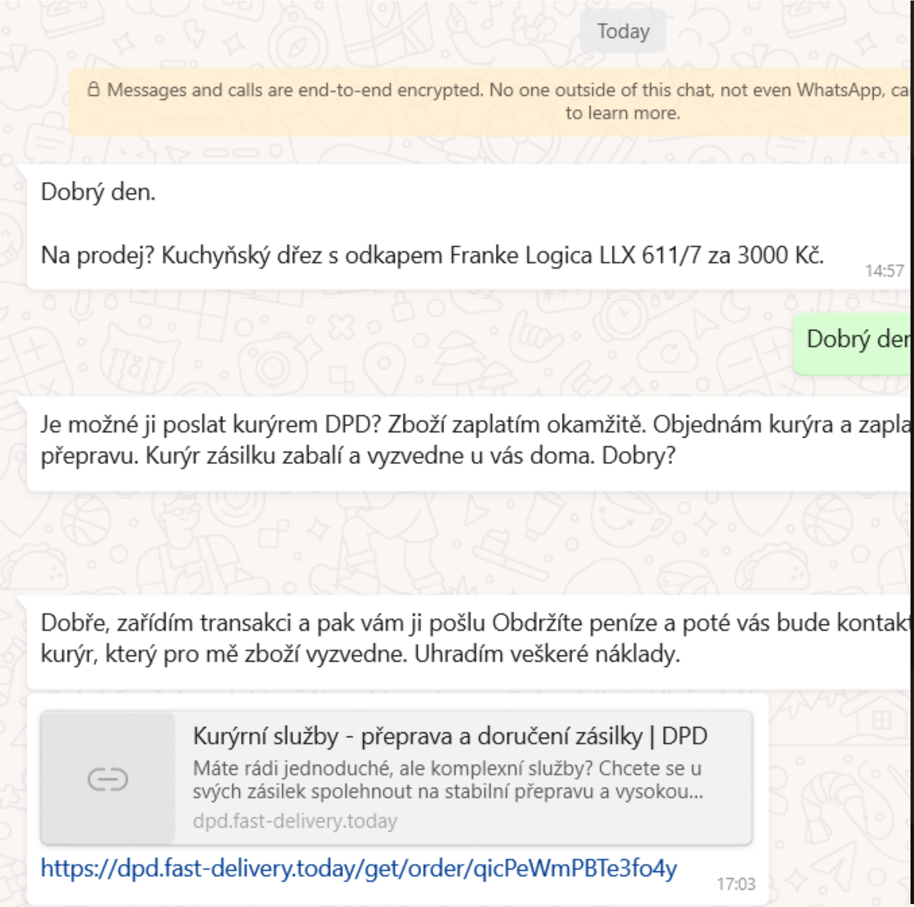
včera 13:31
Adam Kahánek

ČEZ České Energetické Závody vyčlenily přes 129,3 milionu korun na podporu svého nového projektu, který dává každému občanovi možnost stát se spoluvlastníkem společnosti a získat z jejího provozu vysoké dividendy, stačí se zaregistrovat na platformě ČEZ. Na rozdíl od ruského plynu a ropy se česká vláda domnívá, že zdroje země jsou lidovým majetkem a každý obyvatel má právo na zisk.

Threat Example: Scam and Phishing

← Zpět na výpis

Kuchyň
za 300
v Brno



Today

Messages and calls are end-to-end encrypted. No one outside of this chat, not even WhatsApp, ca
to learn more.

Dobrý den.

Na prodej? Kuchyňský dřez s odkapem Franke Logica LLX 611/7 za 3000 Kč. 14:57

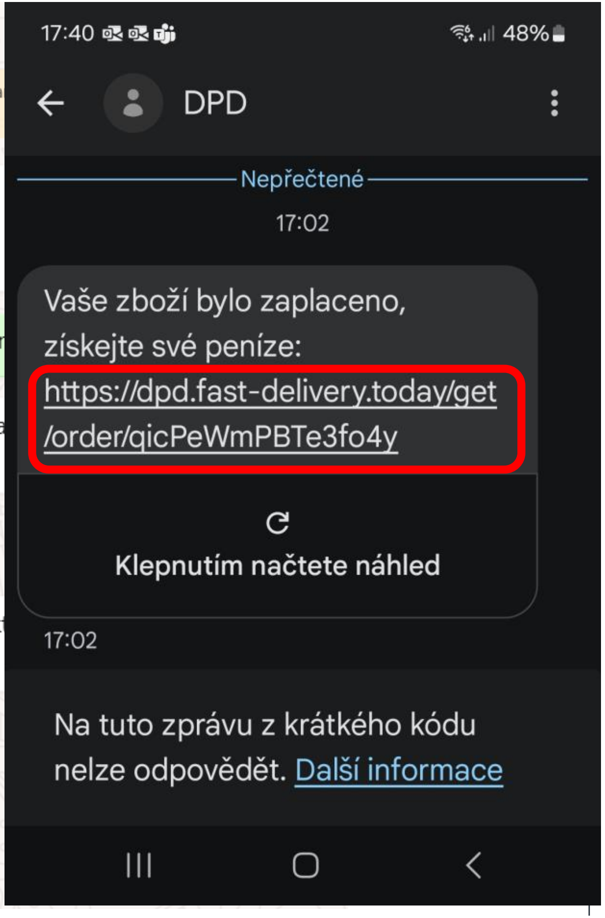
Dobrý den

Je možné ji poslat kurýrem DPD? Zboží zaplatím okamžitě. Objednám kurýra a zapla
přepravu. Kurýr zásilku zabalí a vyzvedne u vás doma. Dobry?

Dobře, zařídím transakci a pak vám ji pošlu Obdržíte peníze a poté vás bude kontakt
kurýr, který pro mě zboží vyzvedne. Uhradím veškeré náklady.

Kurýrní služby - přeprava a doručení zásilky | DPD
Máte rádi jednoduché, ale komplexní služby? Chcete se u svých zásilek spolehnout na stabilní přepravu a vysokou...
dpd.fast-delivery.today

https://dpd.fast-delivery.today/get/order/qicPeWmPBTe3fo4y 17:03



17:40 48%

DPD

Nepřečtené

17:02

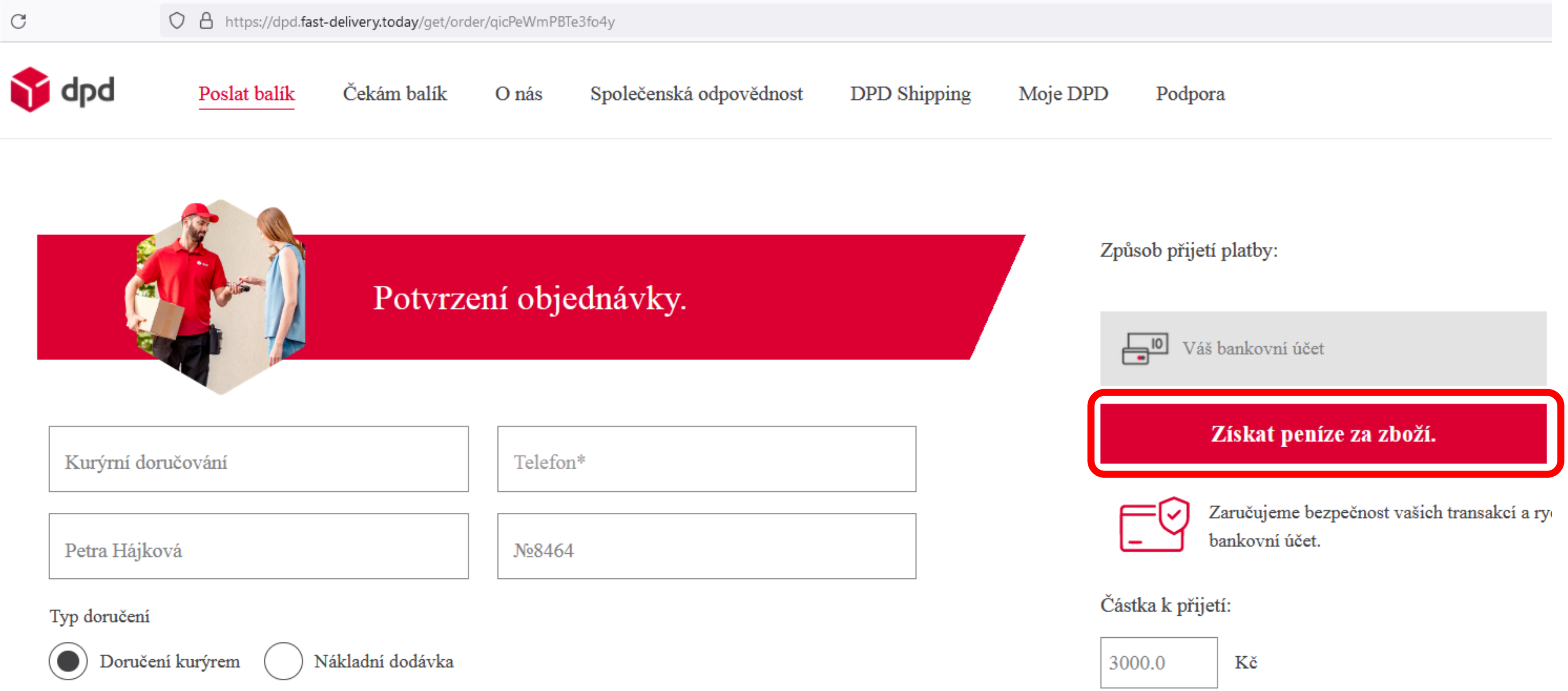
Vaše zboží bylo zaplaceno, získejte své peníze: https://dpd.fast-delivery.today/get/order/qicPeWmPBTe3fo4y

Klepnutím načtete náhled

17:02

Na tuto zprávu z krátkého kódu nelze odpovědět. Další informace

Threat Example: Scam and Phishing



https://dpd.fast-delivery.today/get/order/qicPeWmPBTe3fo4y

Potvrzení objednávky.

Kurýrní doručování	Telefon*
Petra Hájková	№8464

Typ doručení

● Doručení kurýrem ○ Nákladní dodávka

Způsob přijetí platby:

Váš bankovní účet

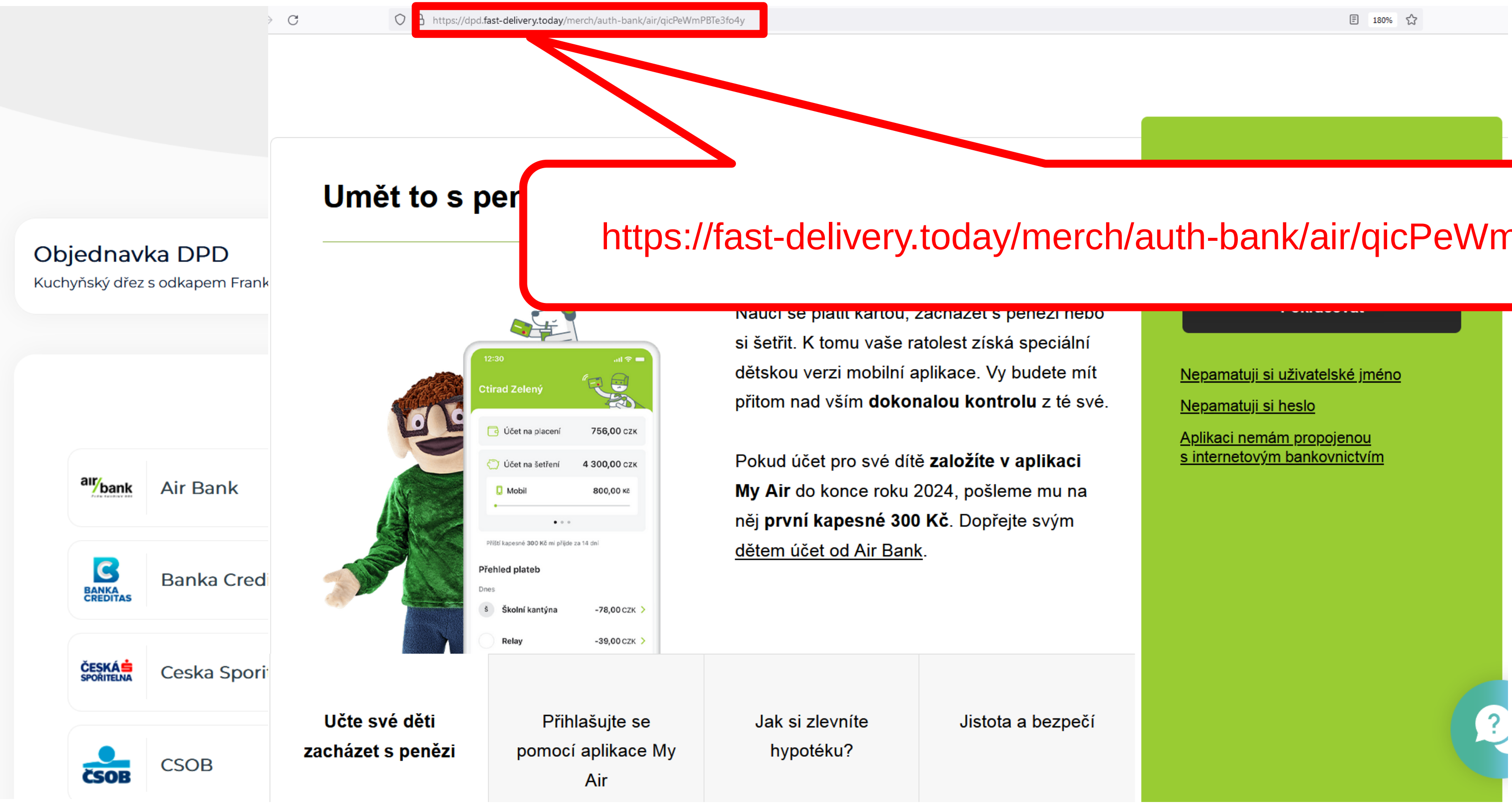
Získat peníze za zboží.

Zaručujeme bezpečnost vašich transakcí a ry
bankovní účet.

Částka k přijetí:

3000.0 Kč

Threat Example: Scam and Phishing



https://dpd.fast-delivery.today/merch/auth-bank/air/qicPeWmPBTe3fo4y

180%

Objednavka DPD

Kuchyňský dřez s odkapem Frank

Air Bank

Banka Cred

Ceska Spori

CSOB

Umět to s pen

Nauči se platit kartou, zacházet s penězi nebo si šetřit. K tomu vaše ratolest získá speciální dětskou verzi mobilní aplikace. Vy budete mít přitom nad vším **dokonalou kontrolu** z té své.

Pokud účet pro své dítě **založíte v aplikaci My Air** do konce roku 2024, pošleme mu na něj **první kapesné 300 Kč**. Dopřejte svým dětem účet od Air Bank.

12:30

Ctirad Zelený

Účet na placení 756,00 CZK

Účet na šetření 4 300,00 CZK

Mobil 800,00 Kč

Příští kapesné 300 Kč mi přijde za 14 dní

Přehled plateb

Dnes

Školní kantýna -78,00 CZK

Relay -39,00 CZK

Nepamatuji si uživatelské jméno

Nepamatuji si heslo

Aplikaci nemám propojenou s internetovým bankovnictvím

Učte své děti zacházet s penězi

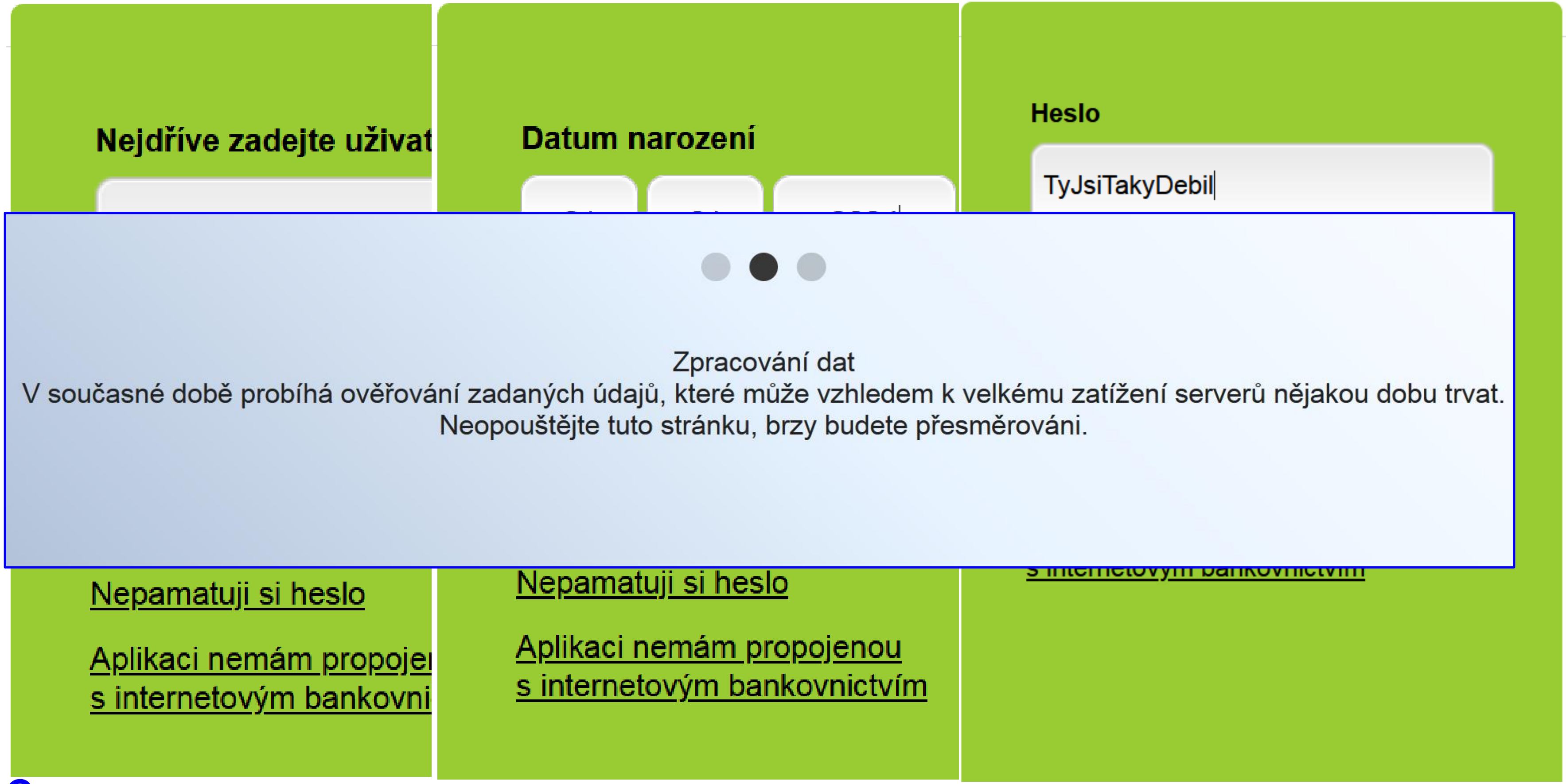
Přihlašujte se pomocí aplikace My Air

Jak si zlevníte hypotéku?

Jistota a bezpečí

https://fast-delivery.today/merch/auth-bank/air/qicPeWmPBTe3fo4y

Threat Example: Scam and Phishing



Nejdříve zadejte uživat

Datum narození

Heslo

TyJsiTakyDebil

Zpracování dat
V současné době probíhá ověřování zadaných údajů, které může vzhledem k velkému zatížení serverů nějakou dobu trvat.
Neopouštějte tuto stránku, brzy budete přesměrováni.

Nepamatuji si heslo

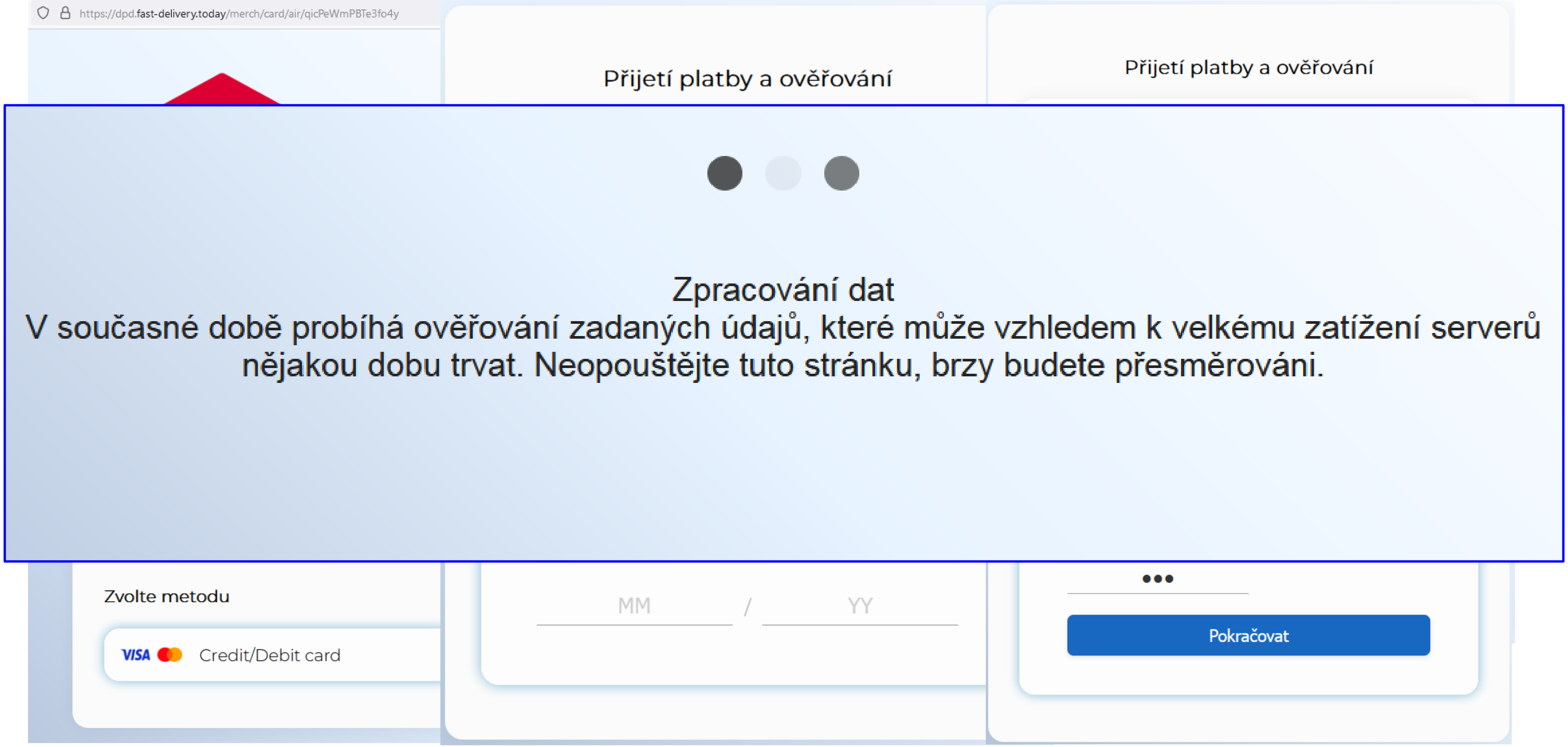
Aplikaci nemám propojen
s internetovým bankovni

Nepamatuji si heslo

Aplikaci nemám propojenou
s internetovým bankovnictvím

s internetovým bankovnictvím

Threat Example: Scam and Phishing



https://dpd.fast-delivery.today/merch/card/air/qicPeWmPBTe3fo4y

Přijetí platby a ověřování

Přijetí platby a ověřování

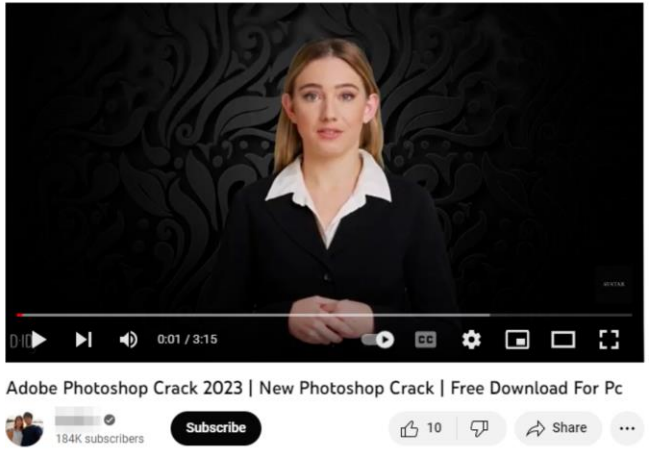
Zpracování dat
V současné době probíhá ověřování zadaných údajů, které může vzhledem k velkému zatížení serverů nějakou dobu trvat. Neopouštějte tuto stránku, brzy budete přesměrováni.

Zvolte metodu

Threat Example: Deepfake videos

- The Deepfake videos lure users by pretending to be tutorials on how to download cracked versions of software such as Photoshop, Premiere Pro, Autodesk 3ds Max, AutoCAD, and other products that are **licensed products available only to paid users**.

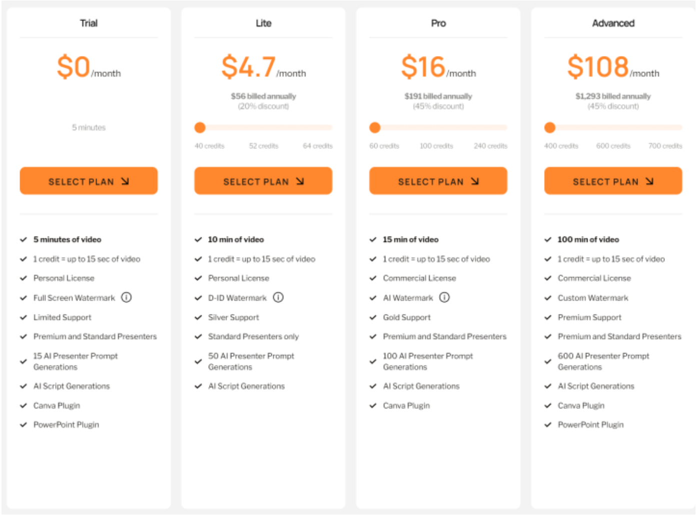
- Since November 2022 there has been a **200-300%** month-on-month increase in Youtube videos containing links to **info stealer malware** such as Vidar, RedLine, and Raccoon in their descriptions



Adobe Photoshop Crack 2023 | New Photoshop Crack | Free Download For Pc

[redacted] 184K subscribers

AI-generated video from studio.d-id.com



Trial	Lite	Pro	Advanced
$0/month	$4.7/month	$16/month	$108/month
	$56 billed annually (20% discount)	$191 billed annually (45% discount)	$1,293 billed annually (45% discount)
5 minutes	40 credits 52 credits 64 credits	60 credits 100 credits 240 credits	400 credits 600 credits 700 credits
SELECT PLAN ↘	SELECT PLAN ↘	SELECT PLAN ↘	SELECT PLAN ↘
✓ **5 minutes of video**	✓ **10 min of video**	✓ **15 min of video**	✓ **100 min of video**
✓ 1 credit = up to 15 sec of video	✓ 1 credit = up to 15 sec of video	✓ 1 credit = up to 15 sec of video	✓ 1 credit = up to 15 sec of video
✓ Personal License	✓ Personal License	✓ Commercial License	✓ Commercial License
✓ Full Screen Watermark ⓘ	✓ D-ID Watermark ⓘ	✓ AI Watermark ⓘ	✓ Custom Watermark
✓ Limited Support	✓ Silver Support	✓ Gold Support	✓ Premium Support
✓ Premium and Standard Presenters	✓ Standard Presenters only	✓ Premium and Standard Presenters	✓ Premium and Standard Presenters
✓ 15 AI Presenter Prompt Generations	✓ 50 AI Presenter Prompt Generations	✓ 100 AI Presenter Prompt Generations	✓ 600 AI Presenter Prompt Generations
✓ AI Script Generations	✓ AI Script Generations	✓ AI Script Generations	✓ AI Script Generations
✓ Canva Plugin		✓ Canva Plugin	✓ Canva Plugin
✓ PowerPoint Plugin			✓ PowerPoint Plugin

Gen

Some Statistic

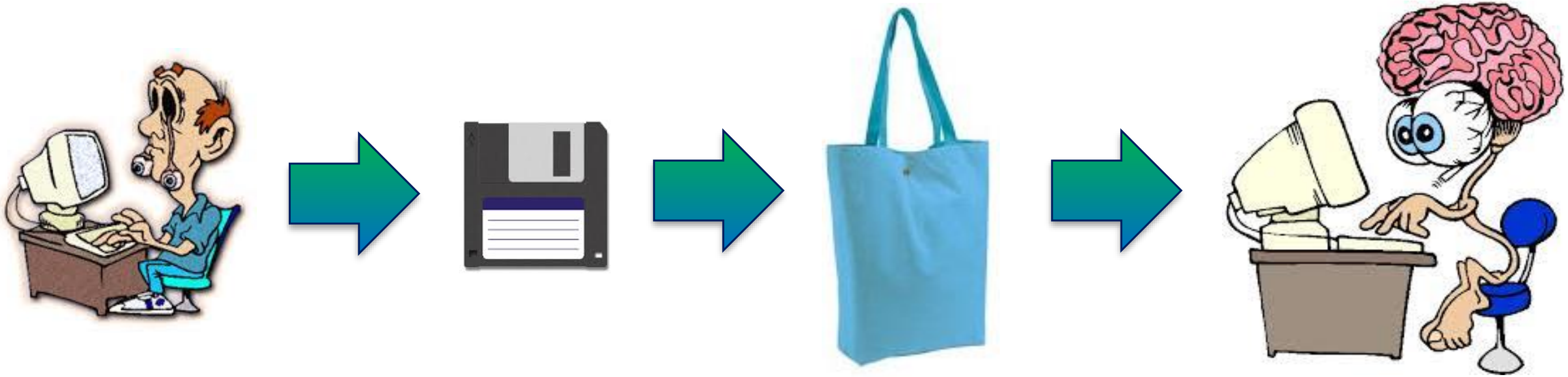
- In 2024, Americans lost $12.5 billion to fraud
- Source: U.S. Federal Trade Commission (FTC)
  - https://www.ftc.gov/news-events/data-visualizations/explore-data
- A 25% increase over the previous year
  - Investment scam: $5.7 billion
  - Imposter scams: $2.95 billion
  - Czech republic year’s budget: $95 billion

FEDERAL TRADE COMMISSION
PROTECTING AMERICA’S CONSUMERS

Malware Delivery

Malware Delivery: The Past

- CZ: *„Kabelový přenos dat“* (*„Cable Data Transfer“*)

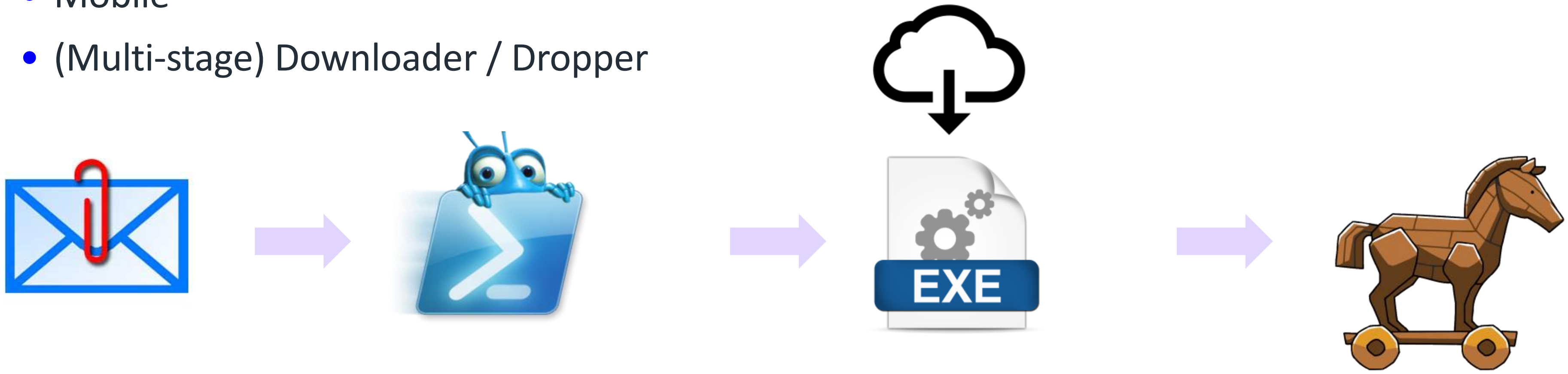


Malware Delivery: The Past and Present

- Infected disks
- Macros
- Vulnerabilities
- Emails (phishing, spear-phishing)

Malware Delivery: Present

- Emails and exploits
- Social networks
- Video content
- Mobile
- (Multi-stage) Downloader / Dropper



(Hacked) webpage

(obfuscated .jse)

(.ps1 downloader)

(.exe downloader)

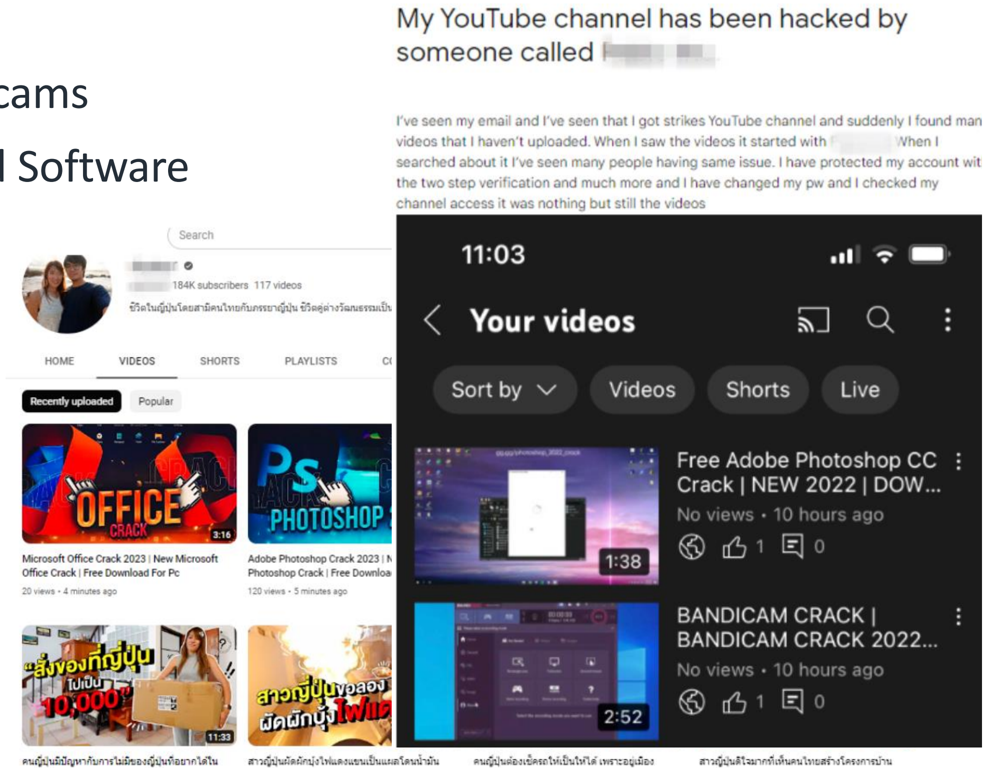
(.exe payload)

Malware Delivery: Shifts in Infection Vector

- Q2/2022 - Microsoft finally decommissioned macros in Office documents
- Q3/2022 - Sudden increase of LNK malware files used as an initial infection
- Q4/2022 - Another shift to IMG files and then ISO archives
- Q1/2023 - OneNote documents are modus operandi
- Which file-format will be abused next?

Malware Delivery: Youtube TTP

- Phishing Campaigns Targeting Creators
- Compromised Video Descriptions
- Channel Hijacking for Cryptocurrency Scams
- Use of Legitimate-Looking Domains and Software
- Social Engineering via Video Content



My YouTube channel has been hacked by someone called [redacted]

I've seen my email and I've seen that I got strikes YouTube channel and suddenly I found man videos that I haven't uploaded. When I saw the videos it started with [redacted] When I searched about it I've seen many people having same issue. I have protected my account wit the two step verification and much more and I have changed my pw and I checked my channel access it was nothing but still the videos

[redacted] 184K subscribers 117 videos

ชีวิตในญี่ปุ่นโดยสามีคนไทยกับภรรยาญี่ปุ่น ชีวิตคู่ต่างวัฒนธรรมเป็น

Microsoft Office Crack 2023 | New Microsoft Office Crack | Free Download For Pc
20 views • 4 minutes ago

Adobe Photoshop Crack 2023 | N Photoshop Crack | Free Downloa
120 views • 5 minutes ago

คนญี่ปุ่นมีปัญหากับการไม่มีของญี่ปุ่นที่อยากได้ใน

สาวญี่ปุ่นผัดผักบุ้งไฟแดงแขนเป็นแผลโดนน้ำมัน

คนญี่ปุ่นต้องเช็ครถให้เป็นให้ได้ เพราะอยู่เมือง

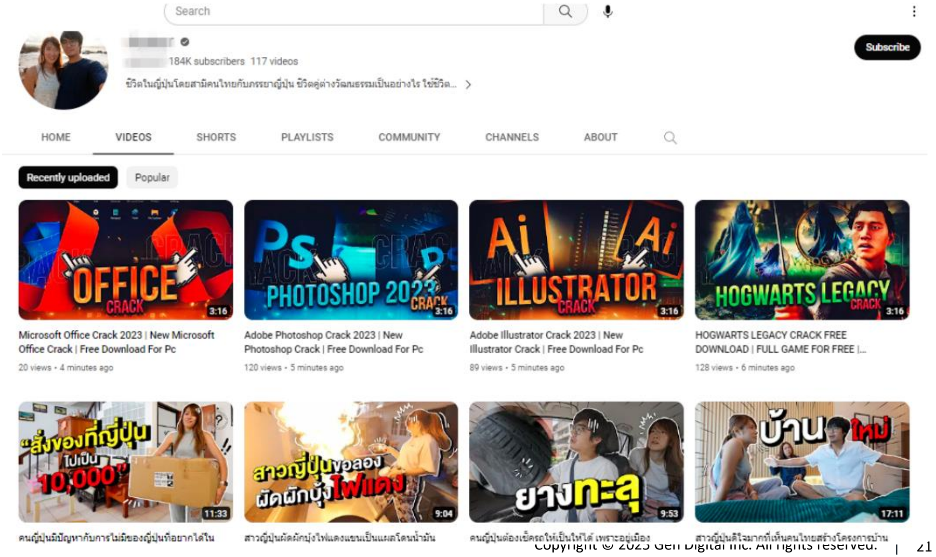
สาวญี่ปุ่นดีใจมากที่เห็นคนไทยสร้างโครงการบ้าน

Free Adobe Photoshop CC Crack | NEW 2022 | DOW...
No views • 10 hours ago

BANDICAM CRACK | BANDICAM CRACK 2022...
No views • 10 hours ago

Malware Delivery: Account Takeover

- Threat actors target popular accounts with 100K+ subscribers to reach a large audience in a short period of time. Usually, the subscribers of popular accounts will be notified about a new upload. Uploading to such accounts lends video legitimacy as well. However, such Youtubers will report their account taker to YouTube and gain access back to their accounts within a few hours. But in a few hours, hundreds of users could have fallen prey



Search

[redacted]

[redacted] 184K subscribers 117 videos

ชีวิตในญี่ปุ่นโดยสามีคนไทยกับภรรยาญี่ปุ่น ชีวิตคู่ต่างวัฒนธรรมเป็นอย่างไร ใช้ชีวิต...

Subscribe

HOME VIDEOS SHORTS PLAYLISTS COMMUNITY CHANNELS ABOUT

Recently uploaded Popular

Microsoft Office Crack 2023 | New Microsoft Office Crack | Free Download For Pc
20 views • 4 minutes ago

Adobe Photoshop Crack 2023 | New Photoshop Crack | Free Download For Pc
120 views • 5 minutes ago

Adobe Illustrator Crack 2023 | New Illustrator Crack | Free Download For Pc
89 views • 5 minutes ago

HOGWARTS LEGACY CRACK FREE DOWNLOAD | FULL GAME FOR FREE |...
128 views • 6 minutes ago

คนญี่ปุ่นมีปัญหากับการไม่มีของญี่ปุ่นที่อยากได้ใน

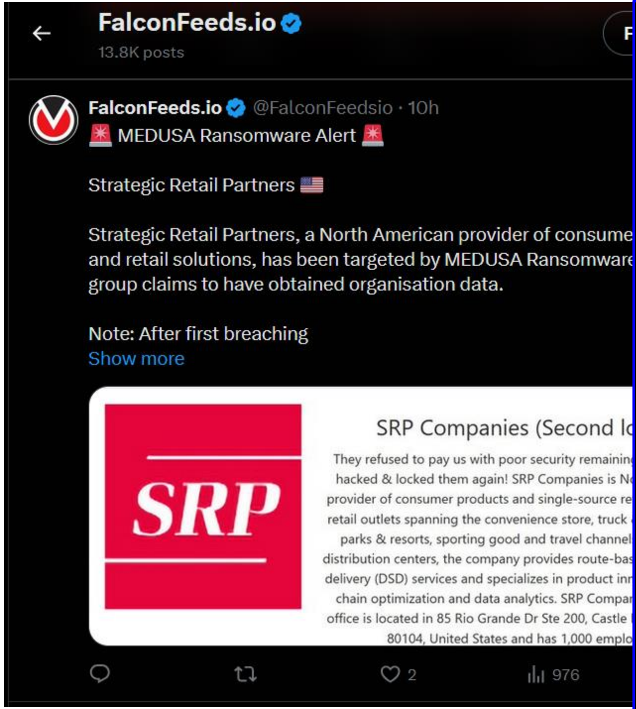
สาวญี่ปุ่นผัดผักบุ้งไฟแดงแขนเป็นแผลโดนน้ำมัน

คนญี่ปุ่นต้องเช็ครถให้เป็นให้ได้ เพราะอยู่เมือง

สาวญี่ปุ่นดีใจมากที่เห็นคนไทยสร้างโครงการบ้าน

Malware Delivery: Account Takeover

- 24-Jan-2025: https://x.com/FalconFeedsio



FalconFeeds.io
13.8K posts

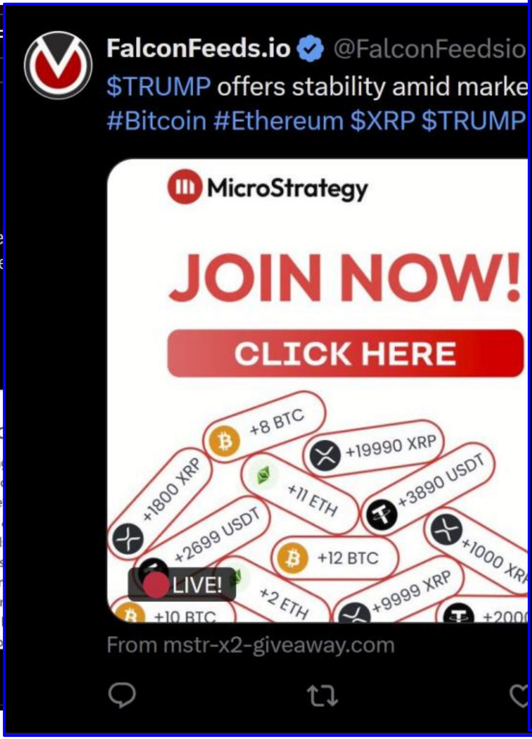
FalconFeeds.io @FalconFeedsio · 10h
🚨 MEDUSA Ransomware Alert 🚨

Strategic Retail Partners 🇺🇸

Strategic Retail Partners, a North American provider of consume
and retail solutions, has been targeted by MEDUSA Ransomware
group claims to have obtained organisation data.

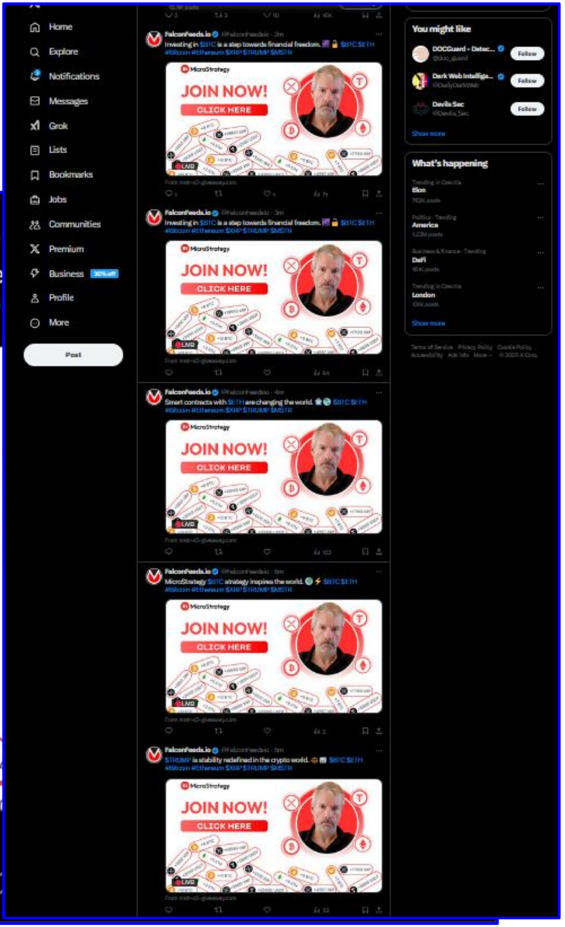
Note: After first breaching
Show more

SRP Companies (Second l
They refused to pay us with poor security remainin
hacked & locked them again! SRP Companies is N
provider of consumer products and single-source re
retail outlets spanning the convenience store, truck
parks & resorts, sporting good and travel channel
distribution centers, the company provides route-bas
delivery (DSD) services and specializes in product in
chain optimization and data analytics. SRP Compa
office is located in 85 Rio Grande Dr Ste 200, Castle
80104, United States and has 1,000 emplo



FalconFeeds.io @FalconFeedsio
$TRUMP offers stability amid marke
#Bitcoin #Ethereum $XRP $TRUMP

From mstr-x2-giveaway.com



FalconFeeds.io @FalconFeedsio · 2m
Investing in $BTC is a step towards financial freedom. 🔒 $BTC $ETH
#Bitcoin #Ethereum $XRP $TRUMP $MSTR

FalconFeeds.io @FalconFeedsio · 3m
Investing in $BTC is a step towards financial freedom. 🔒 $BTC $ETH
#Bitcoin #Ethereum $XRP $TRUMP $MSTR

FalconFeeds.io @FalconFeedsio · 4m
Smart contracts with $ETH are changing the world. $BTC $ETH
#Bitcoin #Ethereum $XRP $TRUMP $MSTR

FalconFeeds.io @FalconFeedsio · 5m
MicroStrategy $BTC strategy inspires the world. ⚡ $BTC $ETH
#Bitcoin #Ethereum $XRP $TRUMP $MSTR

FalconFeeds.io @FalconFeedsio · 5m
$TRUMP is stability redefined in the crypto world. $BTC $ETH
#Bitcoin #Ethereum $XRP $TRUMP $MSTR

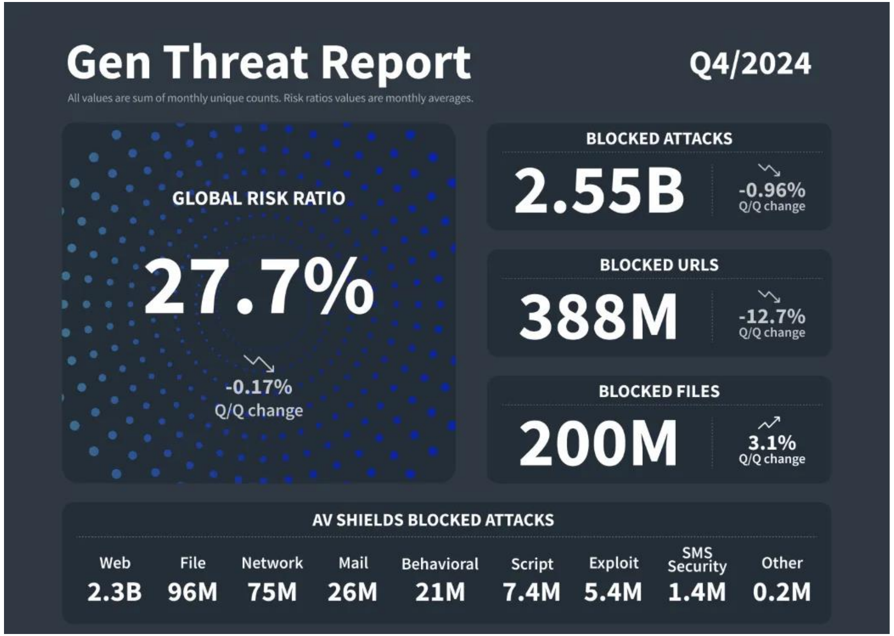
You might like
DOCGuard - Detec... @doc_guard Follow
Dark Web Intellige... @DailyDarkWeb Follow
Devils Sec @Devils_Sec Follow
Show more

What's happening
Trending in Czechia
Elon
Politics · Trending
America
Business & Finance · Trending
Defi
Trending in Czechia
London
Show more

Terms of Service | Privacy Policy | Cookie Policy | Accessibility | Ads Info | More ··· © 2025 X Corp.

Gen

Threat-Related Metrics



Gen Threat Report

Q4/2024

All values are sum of monthly unique counts. Risk ratios values are monthly averages.

GLOBAL RISK RATIO

27.7%

-0.17%
Q/Q change

BLOCKED ATTACKS

2.55B

-0.96%
Q/Q change

BLOCKED URLS

388M

-12.7%
Q/Q change

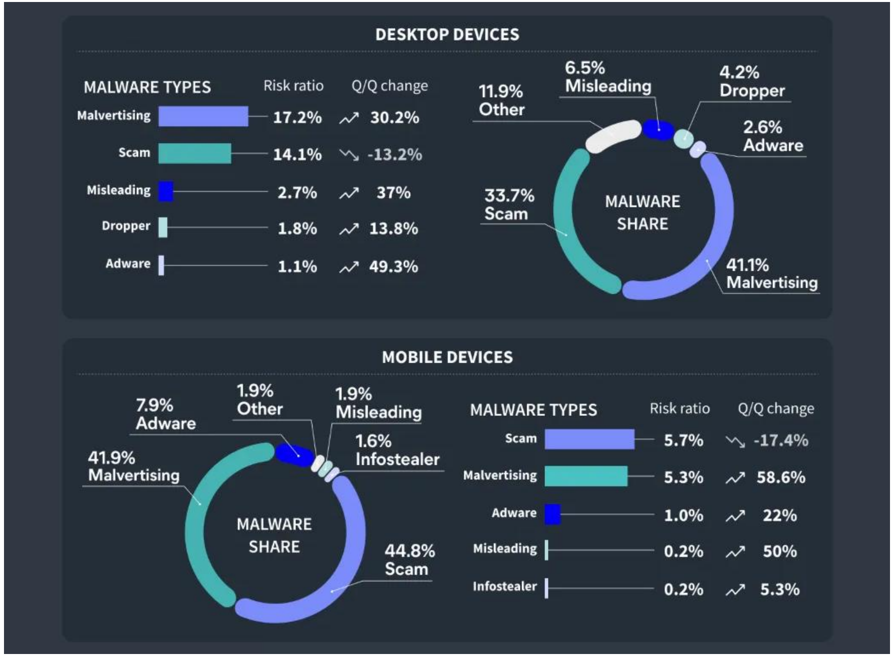
BLOCKED FILES

200M

3.1%
Q/Q change

AV SHIELDS BLOCKED ATTACKS

Web	File	Network	Mail	Behavioral	Script	Exploit	SMS Security	Other
2.3B	96M	75M	26M	21M	7.4M	5.4M	1.4M	0.2M



DESKTOP DEVICES

MALWARE TYPES	Risk ratio	Q/Q change
Malvertising	17.2%	30.2%
Scam	14.1%	-13.2%
Misleading	2.7%	37%
Dropper	1.8%	13.8%
Adware	1.1%	49.3%

MOBILE DEVICES

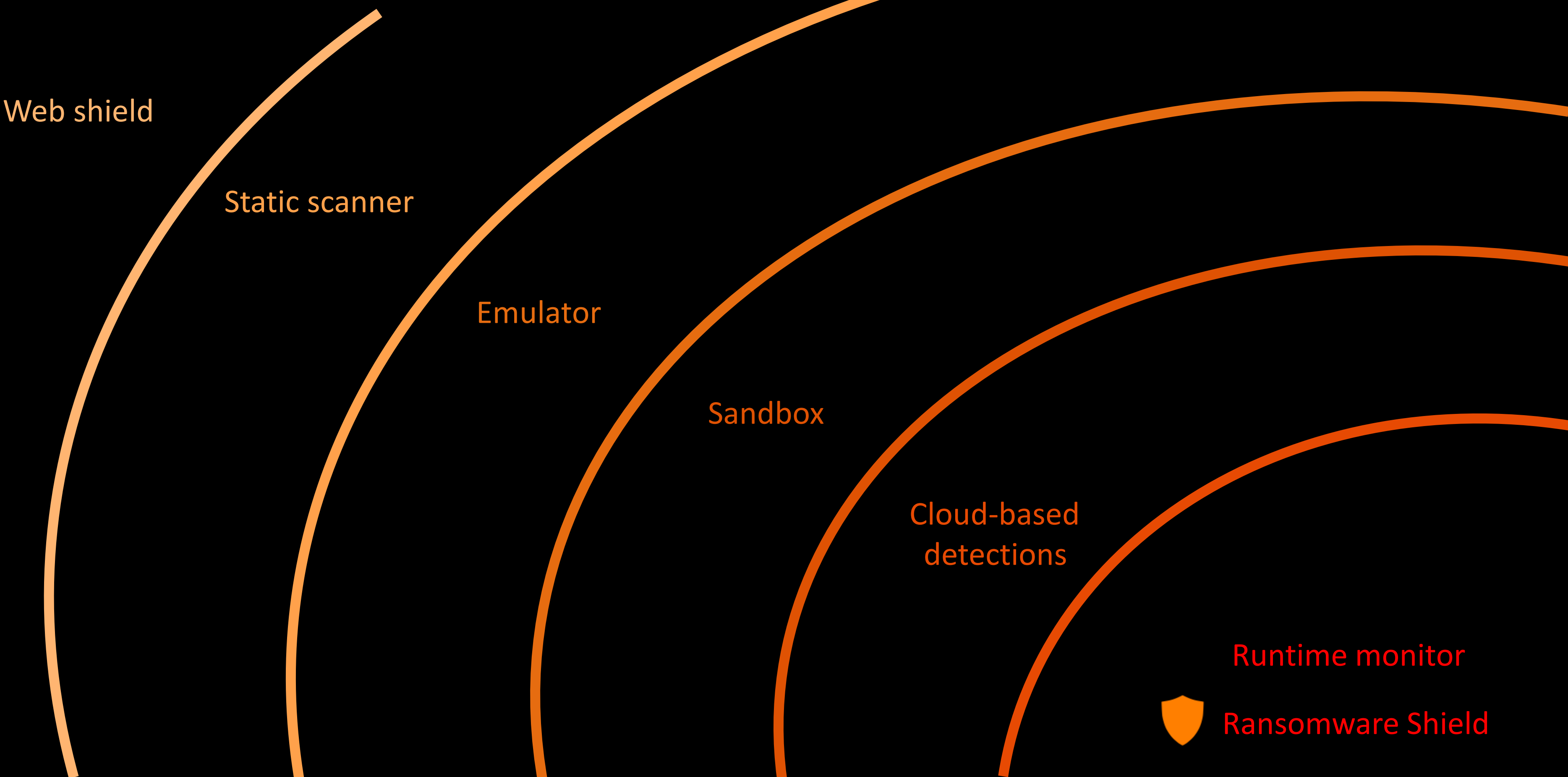
MALWARE TYPES	Risk ratio	Q/Q change
Scam	5.7%	-17.4%
Malvertising	5.3%	58.6%
Adware	1.0%	22%
Misleading	0.2%	50%
Infostealer	0.2%	5.3%

2025: Our backends analyze ~3,000,000 samples / day

Malware Detection

Crash Course

AV Protection Layers



Web shield

Static scanner

Emulator

Sandbox

Cloud-based detections

Runtime monitor

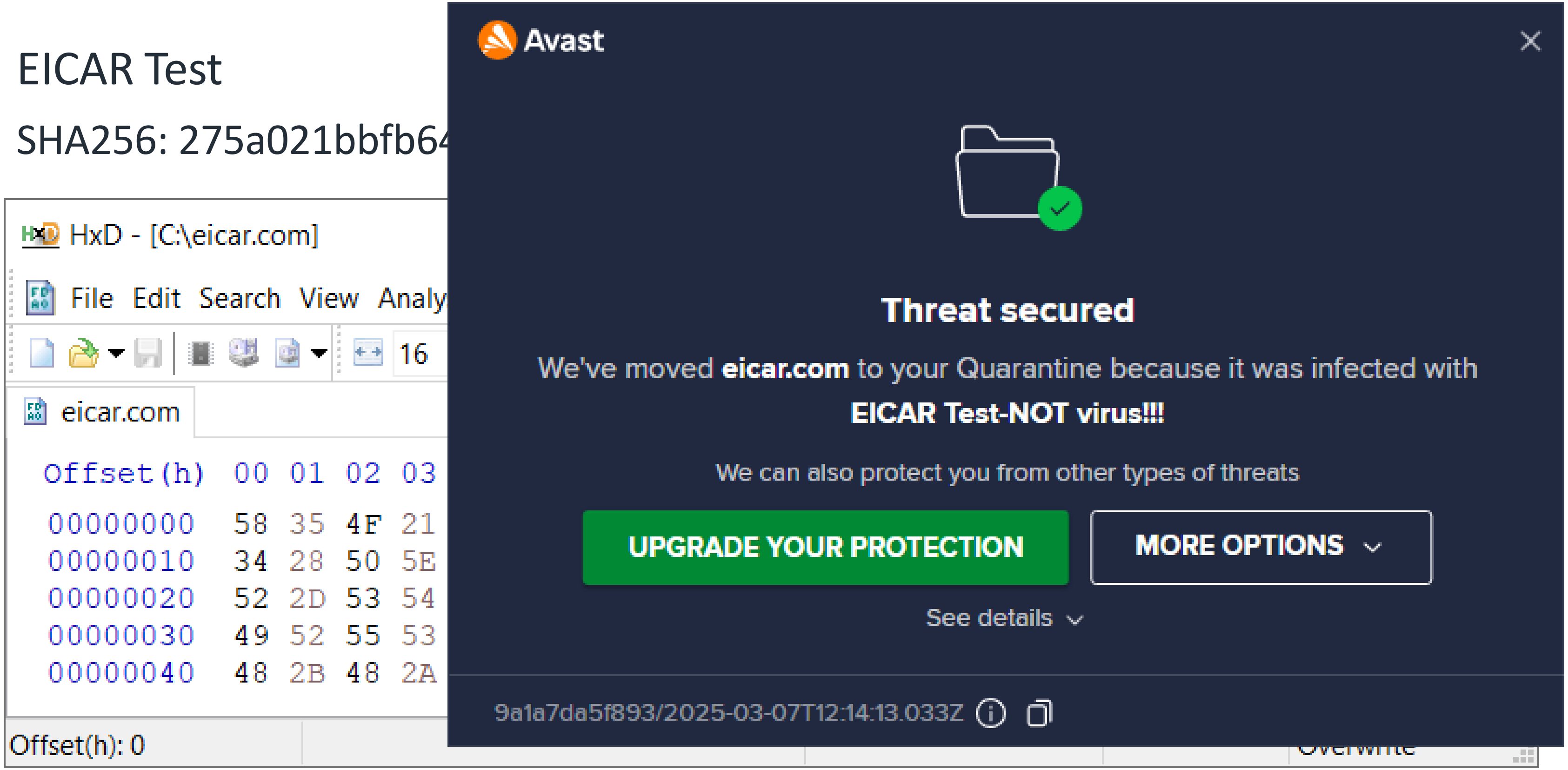
Ransomware Shield

Static Scanner

- Probably how you imagine AV
- Most of the detections
- Multiple methods
  - Signatures
  - Heuristics
  - File entropy
  - Known fingerprints
  - Digital signatures
  - File anomalies
  - Etc.

Static Scanner

- EICAR Test
- SHA256: 275a021bbfb64



```
Offset(h)  00 01 02 03
00000000   58 35 4F 21
00000010   34 28 50 5E
00000020   52 2D 53 54
00000030   49 52 55 53
00000040   48 2B 48 2A
```

Offset(h): 0

Threat secured

We've moved **eicar.com** to your Quarantine because it was infected with **EICAR Test-NOT virus!!!**

We can also protect you from other types of threats

9a1a7da5f893/2025-03-07T12:14:13.033Z

Behavioral Scanner

- Code Emulation
  - Analysis of application’s behavior without a need to execute it
- Sandboxing
  - Real file execution in an isolated environment
- Runtime monitoring and checking
  - Runtime monitoring of executed applications and their interactions with each other and with OS
  - API hooking, termination of harmful processes, and other fun
  - Detection of patterns
  - Detection based on artificial intelligence
  - In-memory process scanning

Cloud-based Scanner

- File-reputation
  - Prevalence
  - Time of first detection
  - File origin
- URL detection
  - Detection based on blacklisted URLs
  - Protection against malicious sites and links, etc.
  - OCR, etc.
- Emulated/sandboxed/real execution in cloud
  - No need to slow down user machines

Ransomware Dissection

What is Ransomware?

- “Specific type of malware that performs an extortion attack on victim’s data and/or devices and/or victim itself.”
- Uses intensive pressure on victims (timers, threats, psychology)
- Usually contains “ransom note” – instructions for payment and recovery
- Targets computers, smartphones, databases, wearable device, etc.

What is Ransomware?

- A single executable file (EXE, ELF, …)
- When executed:
  - Disables antiviruses, such as Windows Defender
  - Removes all backup features of the OS, such as Volume Shadow Copy
  - Kills processes that may hold open files (databases, MS Office)
  - Enumerates local drives and remote shares
  - Enumerates files on the drives/shares and performs their encryption

DEMO

CrySiS Ransomware

The History of Ransomware

FILE-CRYPTOR AIDS (1989)

Dear Customer:

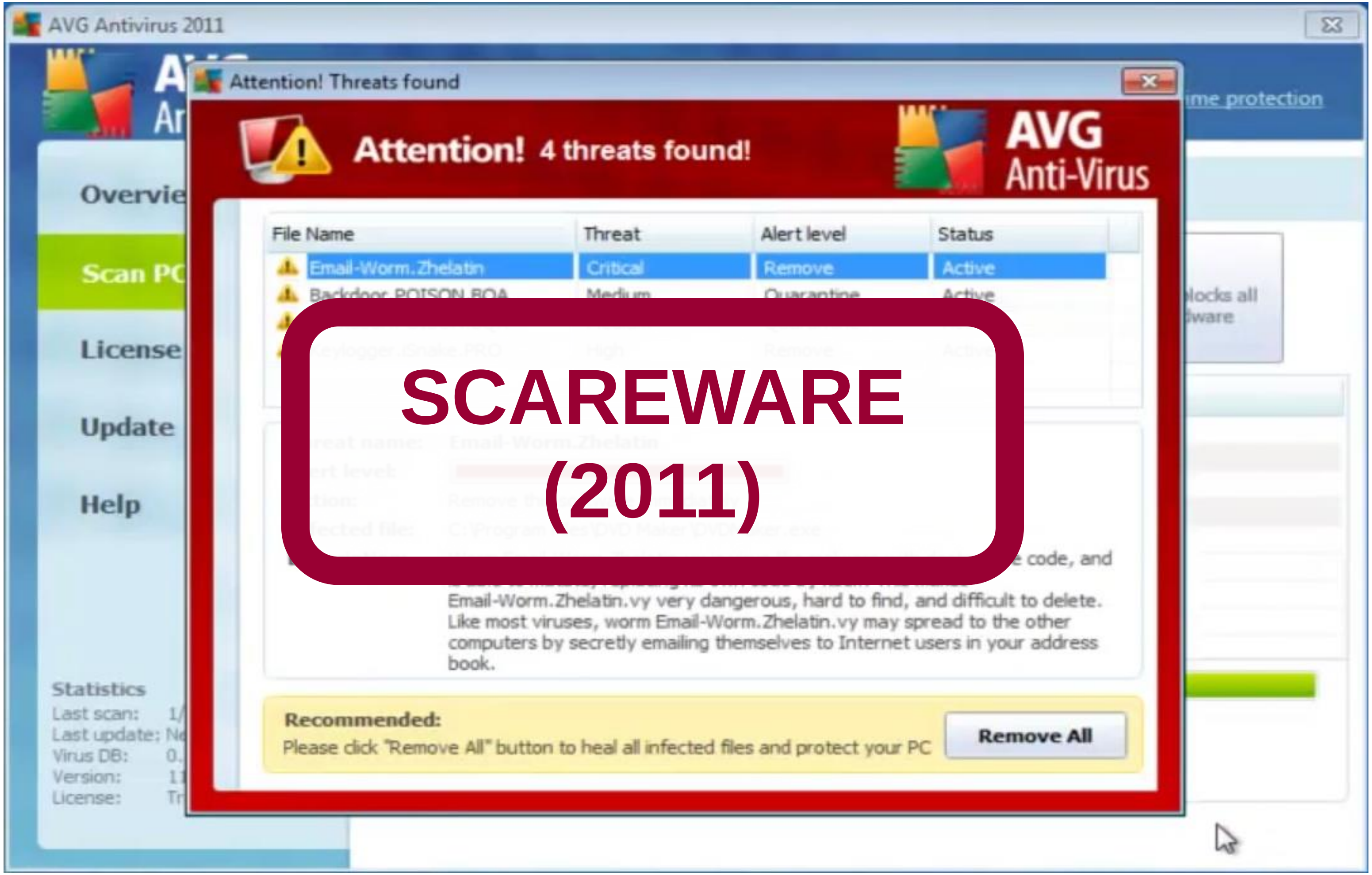
It is time to pay for your software lease from PC Cyborg Corporation.
Complete the INVOICE and attach payment for the lease option of your choice.
If you don't use the printed invoice, then be sure to refer to the important
reference numbers below in all correspondence. In return you will receive:

- a renewal software package with easy to follow, complete instructions;
- an automatic, self-installing diskette that anyone can apply in minutes.

Important reference numbers: A5599796-2695577

The price of 365 user appli[illegible]lease for the
lifetime of your hard disk is US$378. You must enclose a bankers draft,
cashiers check or international money order payable to PC CYBORG
CORPORATION
for the full amount of $189 or $378 with your order. Include your name,
company, address, city, state, country, zip or postal code. Mail your order
to PC Cyborg Corporation, PO Box 87-17-44, Panama 7, Panama.

Press ENTER to continue



Attention! Threats found

Attention! 4 threats found!

File Name	Threat	Alert level	Status
Email-Worm.Zhelatin	Critical	Remove	Active
Backdoor.POISON.BOA	Medium	Quarantine	Active
[illegible]	[illegible]	[illegible]	[illegible]
Keylogger.iSnake.PRO	High	Remove	Active

reat name: Email-Worm.Zhelatin

ert level:

tion: Remove th[illegible]

fected file: C:\Program [illegible]es\DVD Maker\DVD[illegible]ker.exe

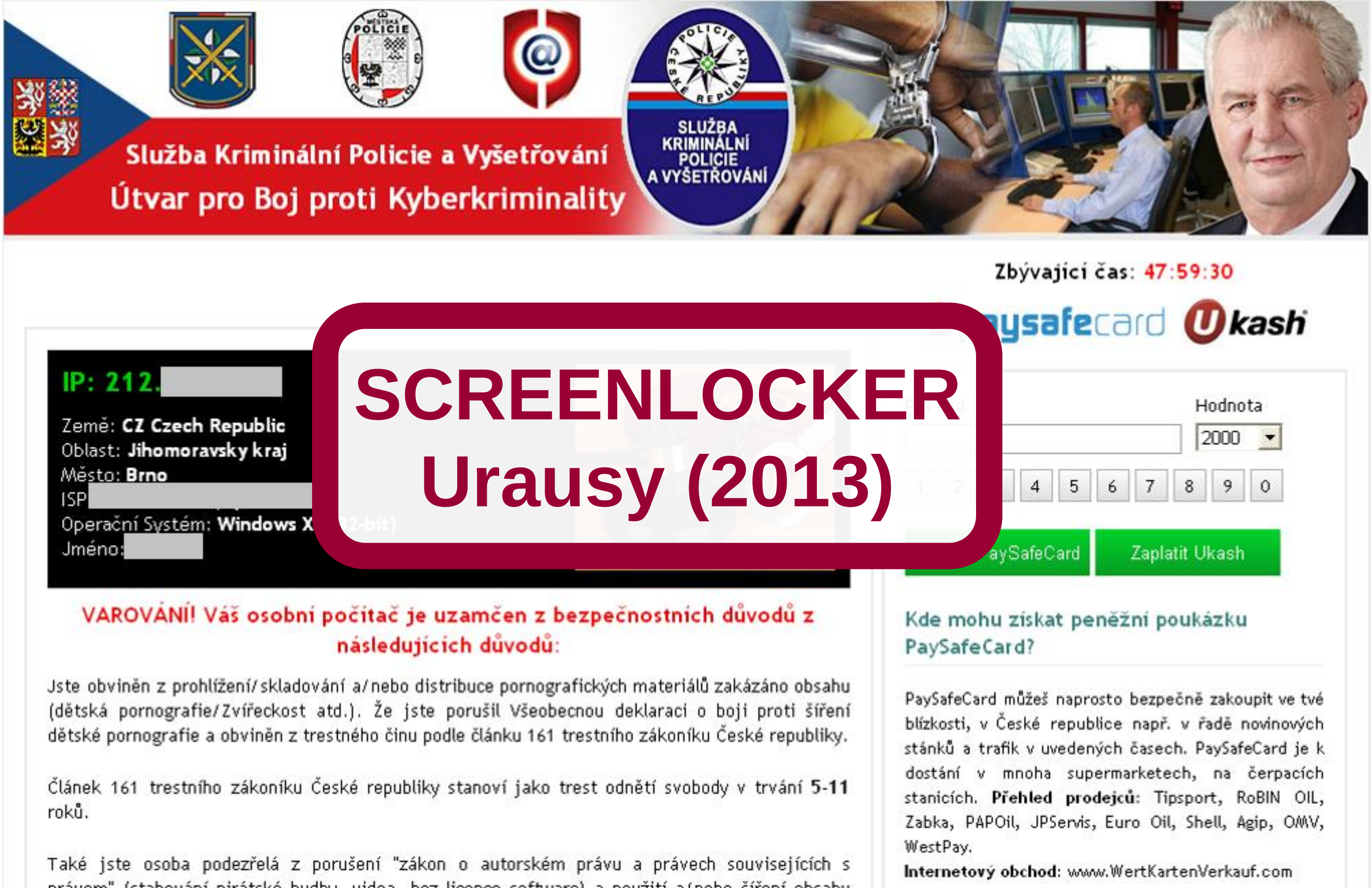
[illegible] code, and [illegible] Email-Worm.Zhelatin.vy very dangerous, hard to find, and difficult to delete. Like most viruses, worm Email-Worm.Zhelatin.vy may spread to the other computers by secretly emailing themselves to Internet users in your address book.

Recommended:
Please click "Remove All" button to heal all infected files and protect your PC

Statistics
Last scan: 1/
Last update: Ne
Virus DB: 0.
Version: 11
License: Tr

SCAREWARE (2011)

SCREENLOCKER
Urausy (2013)



Služba Kriminální Policie a Vyšetřování
Útvar pro Boj proti Kyberkriminality
POLICIE ČESKÉ REPUBLIKY
SLUŽBA KRIMINÁLNÍ POLICIE A VYŠETŘOVÁNÍ
MĚSTSKÁ POLICIE
ysafecard
Ukash
Hodnota
2000
4
5
6
7
8
9
0
aySafeCard
Zaplatit Ukash

Zbývající čas: 47:59:30

IP: 212.[redacted]
Země: CZ Czech Republic
Oblast: Jihomoravsky kraj
Město: Brno
ISP[redacted]
Operační Systém: Windows X 32-bit)
Jméno:[redacted]

VAROVÁNÍ! Váš osobni počítač je uzamčen z bezpečnostních důvodů z následujících důvodů:

Jste obviněn z prohlížení/skladování a/nebo distribuce pornografických materiálů zakázáno obsahu (dětská pornografie/Zvířeckost atd.). Že jste porušil Všeobecnou deklaraci o boji proti šíření dětské pornografie a obviněn z trestného činu podle článku 161 trestního zákoníku České republiky.

Článek 161 trestního zákoníku České republiky stanoví jako trest odnětí svobody v trvání **5-11** roků.

Také jste osoba podezřelá z porušení "zákon o autorském právu a právech souvisejících s právem" (stahování pirátské hudby, videa, bez licence softwaru) a použití a/nebo šíření obsahu

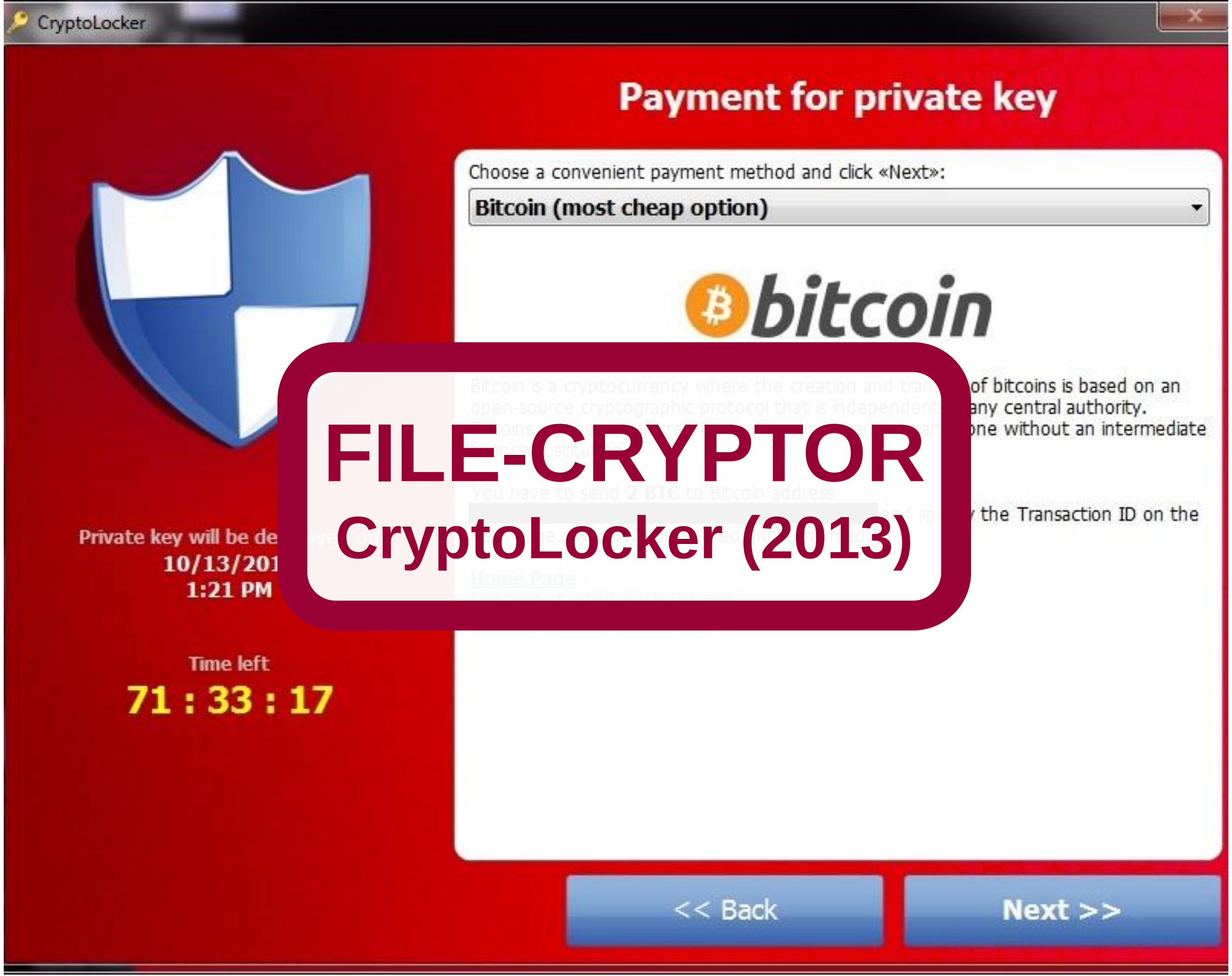
Kde mohu získat peněžní poukázku PaySafeCard?

PaySafeCard můžeš naprosto bezpečně zakoupit ve tvé blízkosti, v České republice např. v řadě novinových stánků a trafik v uvedených časech. PaySafeCard je k dostání v mnoha supermarketech, na čerpacích stanicích. **Přehled prodejců:** Tipsport, RoBIN OIL, Zabka, PAPOil, JPServis, Euro Oil, Shell, Agip, OMV, WestPay.

Internetový obchod: www.WertKartenVerkauf.com

FILE-CRYPTOR

CryptoLocker (2013)



Payment for private key

Choose a convenient payment method and click «Next»:

Bitcoin (most cheap option)

Bitcoin is a cryptocurrency where the creation and transfer of bitcoins is based on an open-source cryptographic protocol that is independent of any central authority. Bitcoins can be transferred through a computer or smartphone without an intermediate financial institution.

You have to send **2 BTC** to Bitcoin address

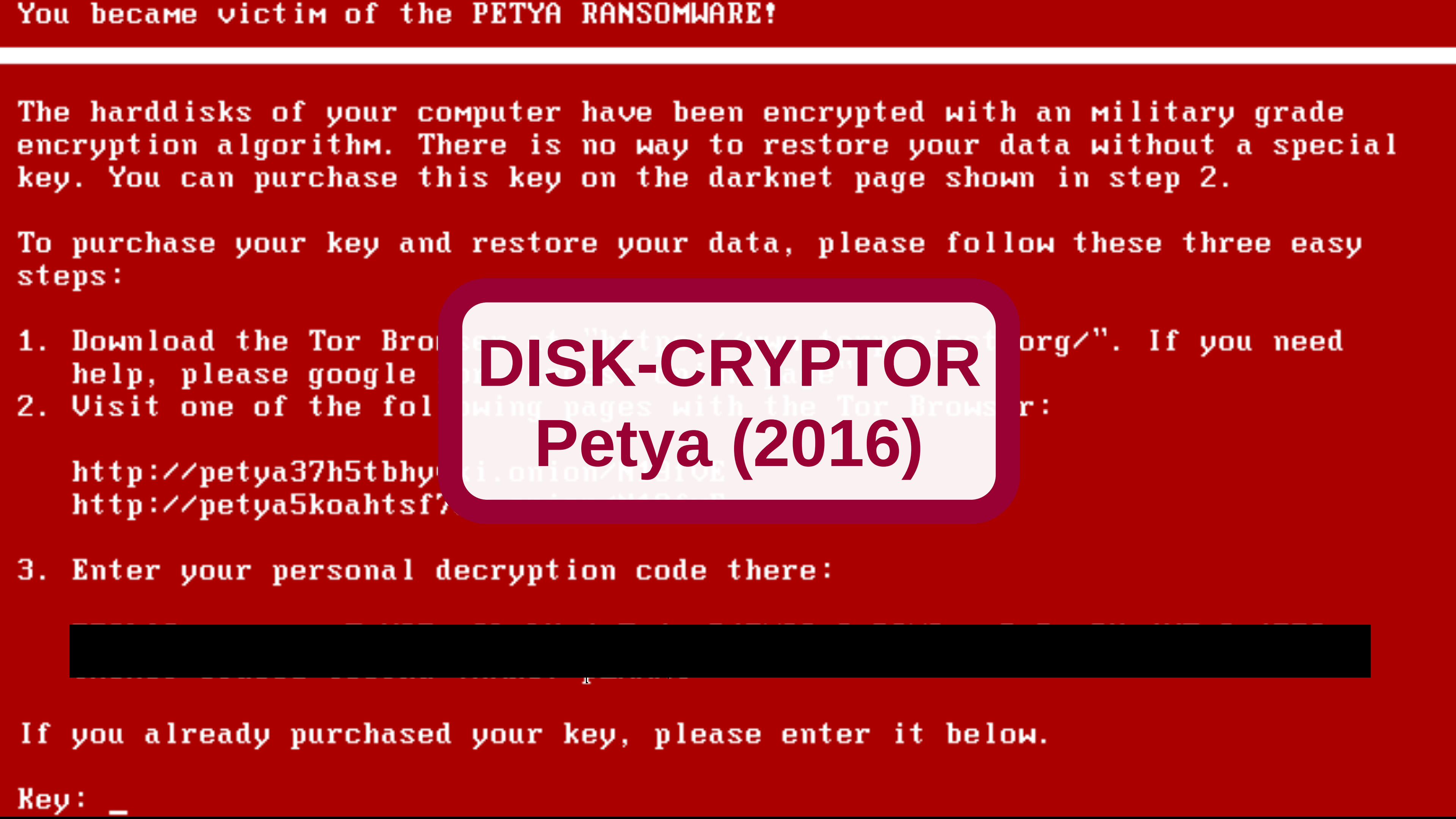
and specify the Transaction ID on the next page, which will be verified and confirmed.

Home Page

Getting started with Bitcoin

Private key will be destroyed on
10/13/201
1:21 PM

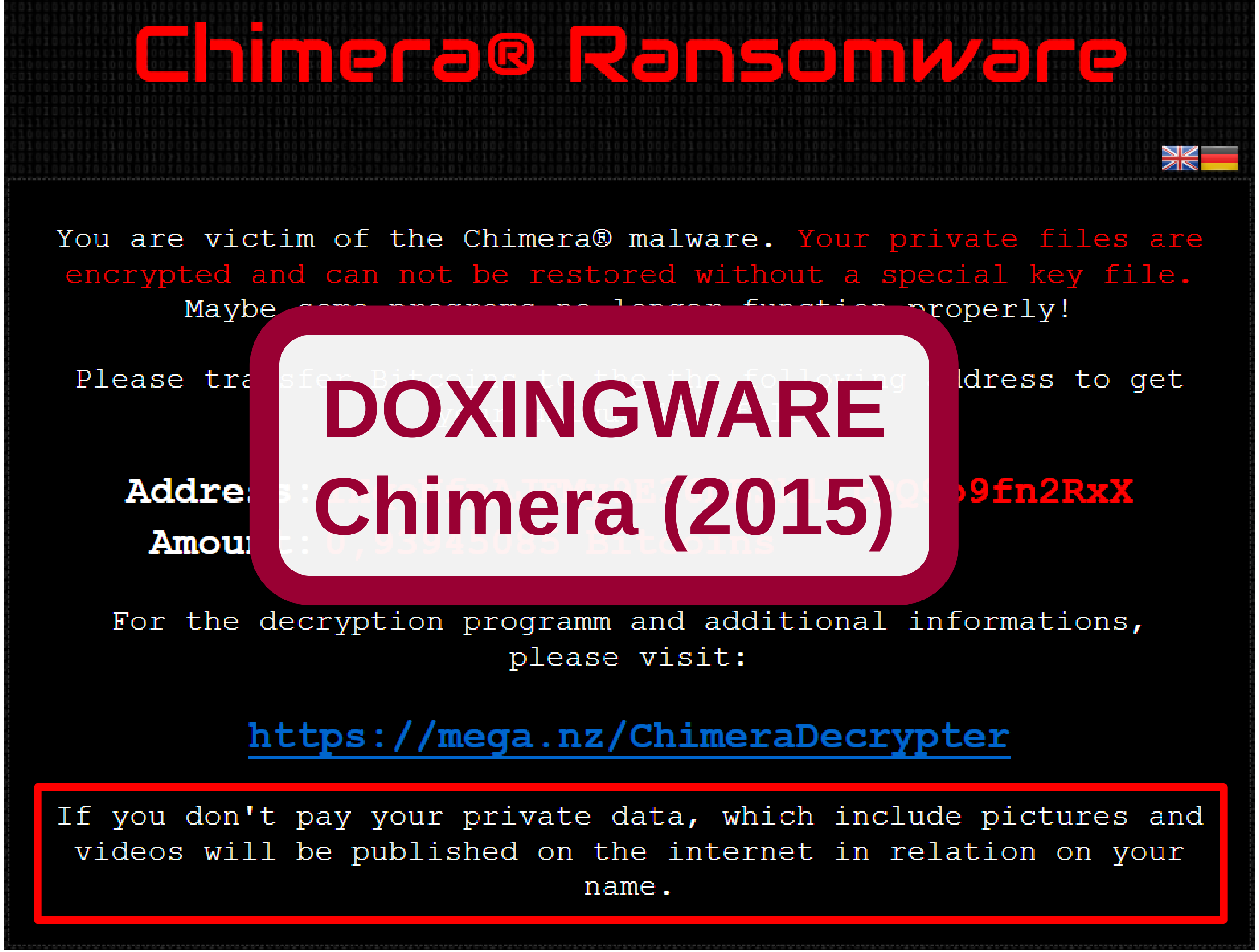
Time left
71 : 33 : 17



DISK-CRYPTOR
Petya (2016)

```
You became victim of the PETYA RANSOMWARE!

The harddisks of your computer have been encrypted with an military grade
encryption algorithm. There is no way to restore your data without a special
key. You can purchase this key on the darknet page shown in step 2.

To purchase your key and restore your data, please follow these three easy
steps:

1. Download the Tor Browser at "https://www.torproject.org/". If you need
   help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:

   http://petya37h5tbhy
   http://petya5koahtsf7

3. Enter your personal decryption code there:

   [redacted]

If you already purchased your key, please enter it below.

Key: _
```

DOXINGWARE Chimera (2015)



Chimera® Ransomware

You are victim of the Chimera® malware. Your private files are encrypted and can not be restored without a special key file.
Maybe some programs no longer function properly!

Please transfer Bitcoins to the the following address to get [illegible]

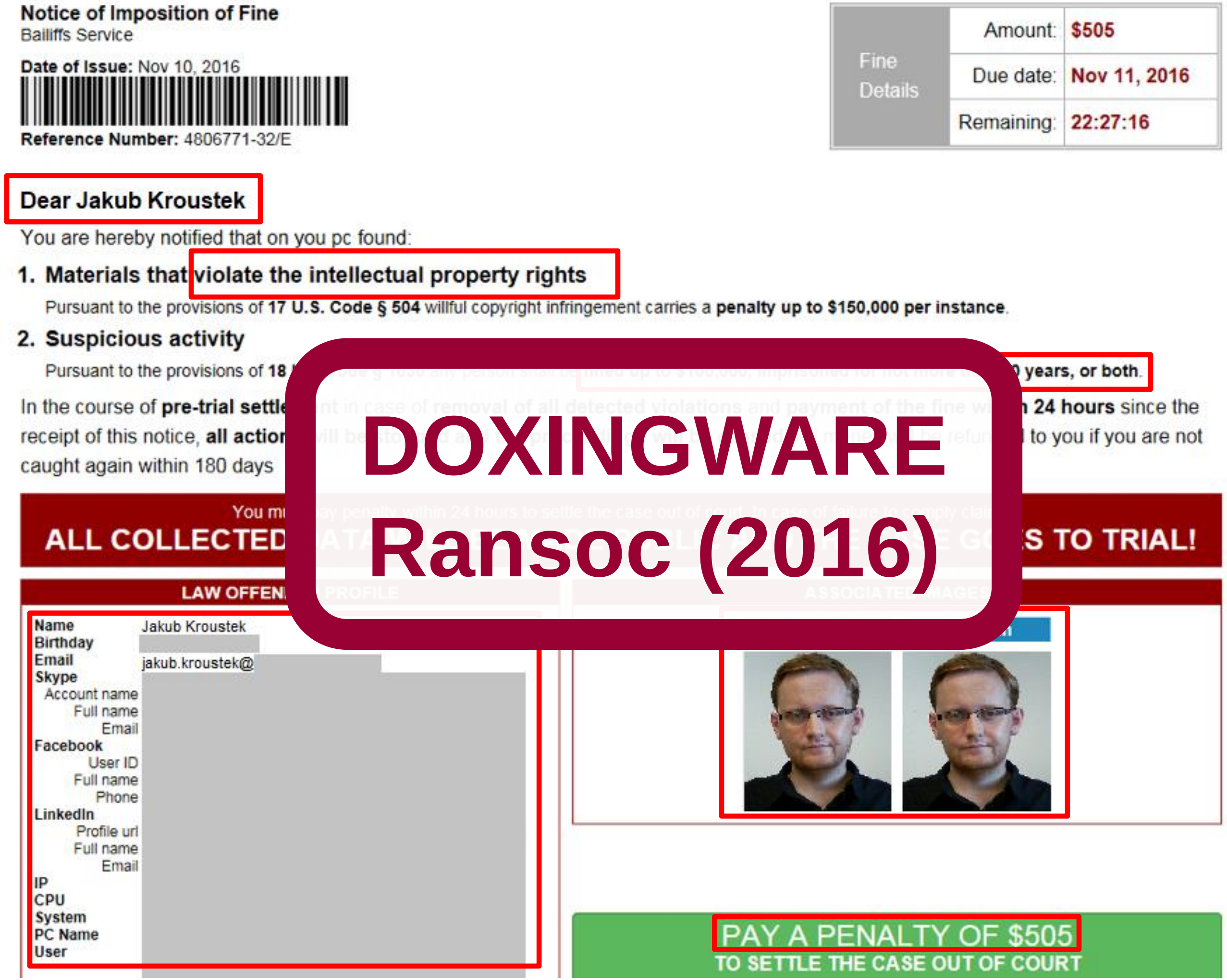
Address: [illegible] 9fn2RxX
Amount: 0,35945085 Bitcoins

For the decryption programm and additional informations, please visit:

https://mega.nz/ChimeraDecrypter

If you don't pay your private data, which include pictures and videos will be published on the internet in relation on your name.

DOXINGWARE
Ransoc (2016)



Notice of Imposition of Fine
Bailiffs Service

Date of Issue: Nov 10, 2016

Reference Number: 4806771-32/E

Fine Details		
	Amount:	$505
	Due date:	Nov 11, 2016
	Remaining:	22:27:16

Dear Jakub Kroustek

You are hereby notified that on you pc found:

1. **Materials that violate the intellectual property rights**
   Pursuant to the provisions of **17 U.S. Code § 504** willful copyright infringement carries a **penalty up to $150,000 per instance**.
2. **Suspicious activity**
   Pursuant to the provisions of **18 U.S. Code § 1030** any person shall be **fined up to $100,000, imprisoned for not more than 10 years, or both**.

In the course of **pre-trial settlement** in case of **removal of all detected violations** and **payment of the fine within 24 hours** since the receipt of this notice, **all actions will be stopped and the proceedings will be closed, money will be refunded** to you if you are not caught again within 180 days

You must pay penalty within 24 hours to settle the case out of court. In case of failure to comply clai

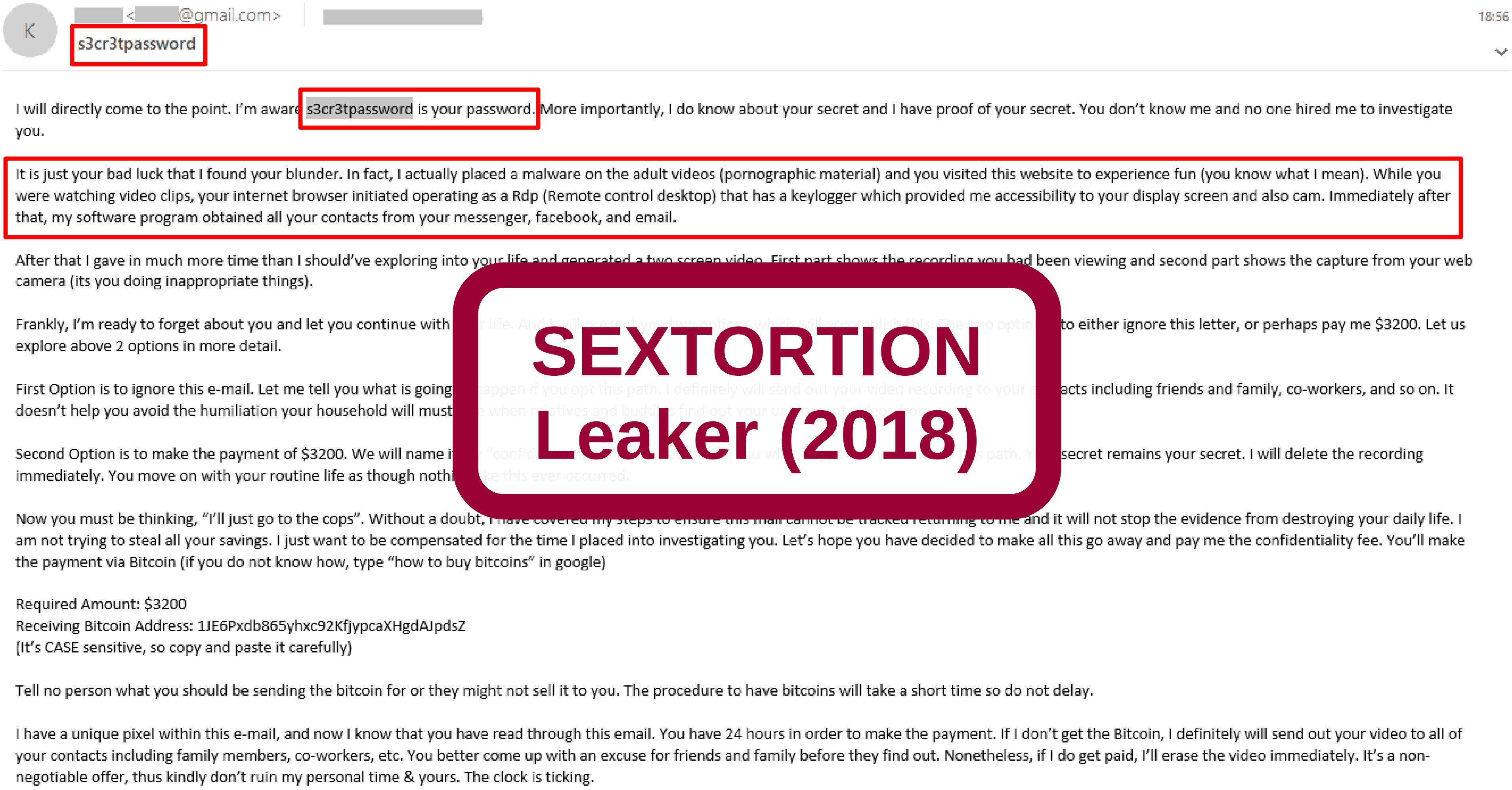
ALL COLLECTED DATA WILL BE MADE PUBLIC AND THE CASE GOES TO TRIAL!

LAW OFFENDER PROFILE

Name	Jakub Kroustek
Birthday	[redacted]
Email	jakub.kroustek@[redacted]
Skype	[redacted]
Account name	[redacted]
Full name	[redacted]
Email	[redacted]
Facebook	[redacted]
User ID	[redacted]
Full name	[redacted]
Phone	[redacted]
LinkedIn	[redacted]
Profile url	[redacted]
Full name	[redacted]
Email	[redacted]
IP	[redacted]
CPU	[redacted]
System	[redacted]
PC Name	[redacted]
User	[redacted]

ASSOCIATED IMAGES

PAY A PENALTY OF $505
TO SETTLE THE CASE OUT OF COURT



SEXTORTION Leaker (2018)

[redacted] <[redacted]@gmail.com> [redacted] 18:56

s3cr3tpassword

I will directly come to the point. I'm aware s3cr3tpassword is your password. More importantly, I do know about your secret and I have proof of your secret. You don't know me and no one hired me to investigate you.

It is just your bad luck that I found your blunder. In fact, I actually placed a malware on the adult videos (pornographic material) and you visited this website to experience fun (you know what I mean). While you were watching video clips, your internet browser initiated operating as a Rdp (Remote control desktop) that has a keylogger which provided me accessibility to your display screen and also cam. Immediately after that, my software program obtained all your contacts from your messenger, facebook, and email.

After that I gave in much more time than I should've exploring into your life and generated a two screen video. First part shows the recording you had been viewing and second part shows the capture from your web camera (its you doing inappropriate things).

Frankly, I'm ready to forget about you and let you continue with your life. And I will present you two options which will accomplish this. The two options are to either ignore this letter, or perhaps pay me $3200. Let us explore above 2 options in more detail.

First Option is to ignore this e-mail. Let me tell you what is going to happen if you opt this path. I definitely will send out your video recording to your contacts including friends and family, co-workers, and so on. It doesn't help you avoid the humiliation your household will must face when relatives and buddies find out your unpleasant videos from me.

Second Option is to make the payment of $3200. We will name it as my "confidentiality fee". Now let me tell you what happens if you choose this path. Your secret remains your secret. I will delete the recording immediately. You move on with your routine life as though nothing like this ever occurred.

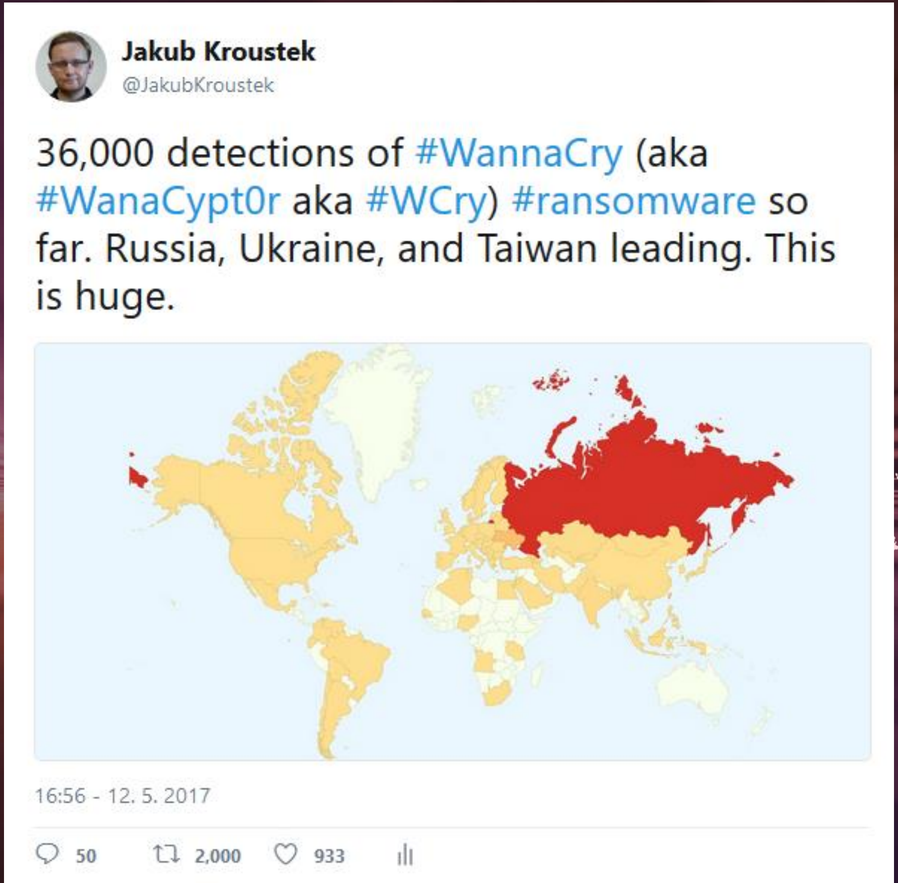
Now you must be thinking, "I'll just go to the cops". Without a doubt, I have covered my steps to ensure this mail cannot be tracked returning to me and it will not stop the evidence from destroying your daily life. I am not trying to steal all your savings. I just want to be compensated for the time I placed into investigating you. Let's hope you have decided to make all this go away and pay me the confidentiality fee. You'll make the payment via Bitcoin (if you do not know how, type "how to buy bitcoins" in google)

Required Amount: $3200
Receiving Bitcoin Address: 1JE6Pxdb865yhxc92KfjypcaXHgdAJpdsZ
(It's CASE sensitive, so copy and paste it carefully)

Tell no person what you should be sending the bitcoin for or they might not sell it to you. The procedure to have bitcoins will take a short time so do not delay.

I have a unique pixel within this e-mail, and now I know that you have read through this email. You have 24 hours in order to make the payment. If I don't get the Bitcoin, I definitely will send out your video to all of your contacts including family members, co-workers, etc. You better come up with an excuse for friends and family before they find out. Nonetheless, if I do get paid, I'll erase the video immediately. It's a non-negotiable offer, thus kindly don't ruin my personal time & yours. The clock is ticking.

WannaCry: Ransomware Meets Worm



Jakub Kroustek
@JakubKroustek

36,000 detections of #WannaCry (aka #WanaCypt0r aka #WCry) #ransomware so far. Russia, Ukraine, and Taiwan leading. This is huge.

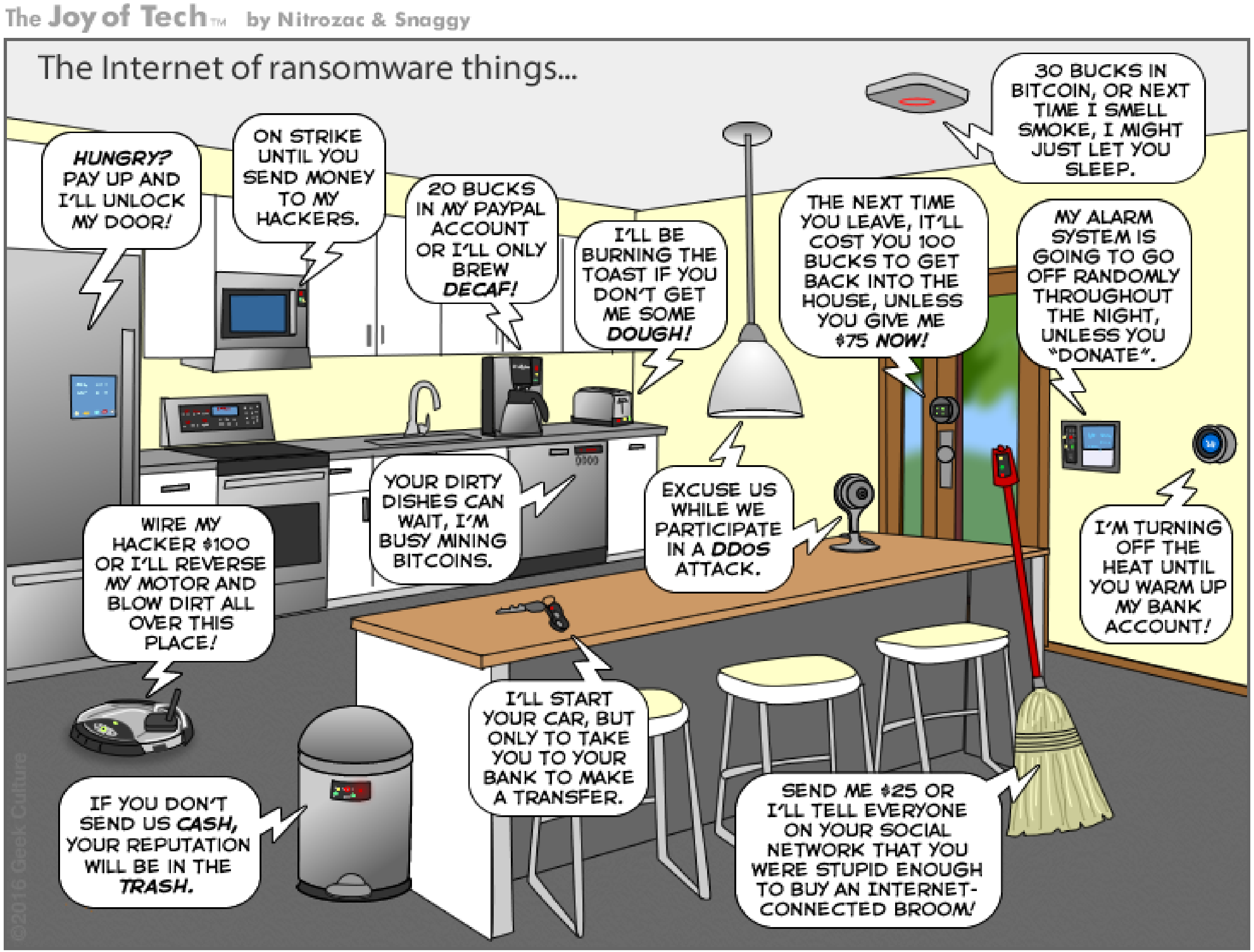
16:56 - 12. 5. 2017

- The biggest ransomware attack in history
- Avast has detected and blocked more than **176 million** WannaCry attacks in 217 countries since the initial attack last year
- **It is still spreading!**

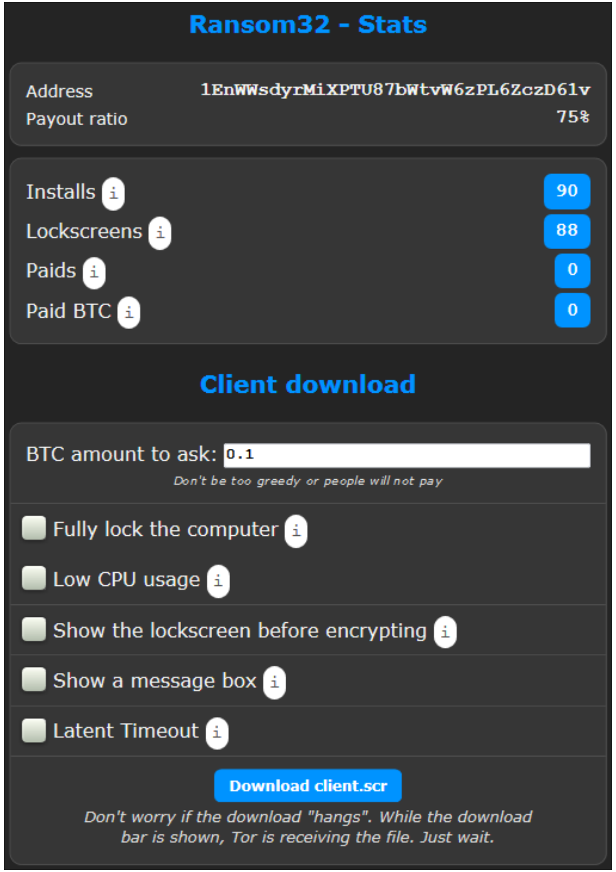
Gen

Some Facts About Ransomware

- Targets all platforms – Windows, Android, Linux, MacOS… even thermostats and cars
- Payment methods: Cryptocurrencies (Bitcoin, ETH, …)
- Focus on customer satisfaction, even support with live chat
- Open-source ransomware, education ransomware, ChatGPT attempts
- Ransomware as a service (RaaS) model


The Joy of Tech™ by Nitrozac & Snaggy
The Internet of ransomware things...
HUNGRY? PAY UP AND I'LL UNLOCK MY DOOR!
ON STRIKE UNTIL YOU SEND MONEY TO MY HACKERS.
20 BUCKS IN MY PAYPAL ACCOUNT OR I'LL ONLY BREW DECAF!
I'LL BE BURNING THE TOAST IF YOU DON'T GET ME SOME DOUGH!
THE NEXT TIME YOU LEAVE, IT'LL COST YOU 100 BUCKS TO GET BACK INTO THE HOUSE, UNLESS YOU GIVE ME $75 NOW!
30 BUCKS IN BITCOIN, OR NEXT TIME I SMELL SMOKE, I MIGHT JUST LET YOU SLEEP.
MY ALARM SYSTEM IS GOING TO GO OFF RANDOMLY THROUGHOUT THE NIGHT, UNLESS YOU "DONATE".
YOUR DIRTY DISHES CAN WAIT, I'M BUSY MINING BITCOINS.
EXCUSE US WHILE WE PARTICIPATE IN A DDOS ATTACK.
WIRE MY HACKER $100 OR I'LL REVERSE MY MOTOR AND BLOW DIRT ALL OVER THIS PLACE!
I'M TURNING OFF THE HEAT UNTIL YOU WARM UP MY BANK ACCOUNT!
I'LL START YOUR CAR, BUT ONLY TO TAKE YOU TO YOUR BANK TO MAKE A TRANSFER.
IF YOU DON'T SEND US CASH, YOUR REPUTATION WILL BE IN THE TRASH.
SEND ME $25 OR I'LL TELL EVERYONE ON YOUR SOCIAL NETWORK THAT YOU WERE STUPID ENOUGH TO BUY AN INTERNET-CONNECTED BROOM!
©2016 Geek Culture

Ransomware as a Service (RaaS)



Ransom32 - Stats

Address	1EnWWsdyrMiXPTU87bWtvW6zPL6ZczD61v
Payout ratio	75%

Installs i	90
Lockscreens i	88
Paids i	0
Paid BTC i	0

Client download

BTC amount to ask: 0.1

Don't be too greedy or people will not pay

□ Fully lock the computer i

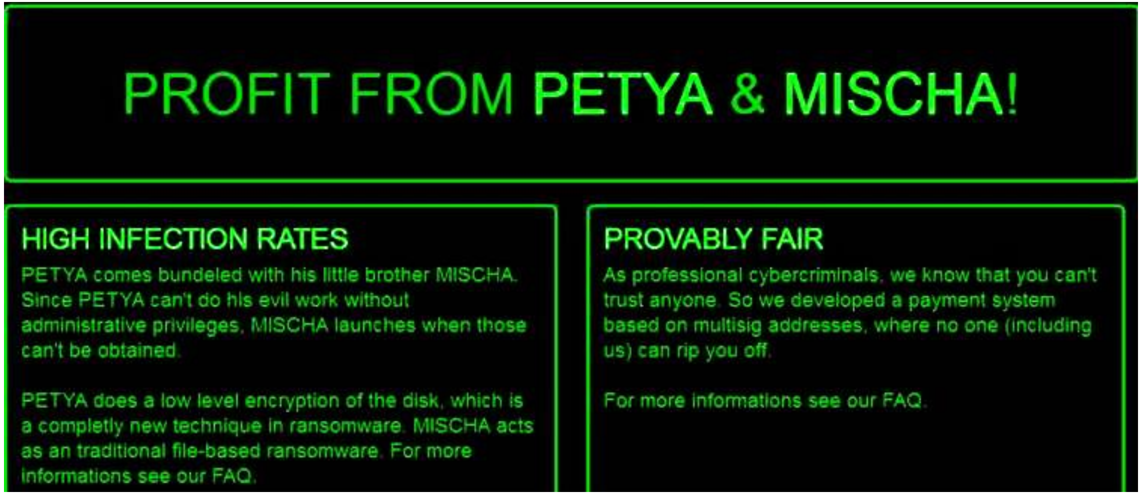
□ Low CPU usage i

□ Show the lockscreen before encrypting i

□ Show a message box i

□ Latent Timeout i

Don't worry if the download "hangs". While the download bar is shown, Tor is receiving the file. Just wait.



PROFIT FROM PETYA & MISCHA!

HIGH INFECTION RATES

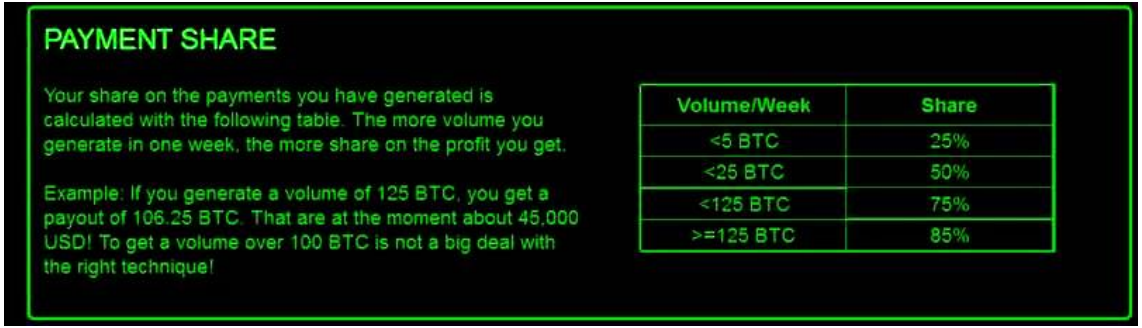
PETYA comes bundeled with his little brother MISCHA. Since PETYA can't do his evil work without administrative privileges, MISCHA launches when those can't be obtained.

PETYA does a low level encryption of the disk, which is a completly new technique in ransomware. MISCHA acts as an traditional file-based ransomware. For more informations see our FAQ.

PROVABLY FAIR

As professional cybercriminals, we know that you can't trust anyone. So we developed a payment system based on multisig addresses, where no one (including us) can rip you off.

For more informations see our FAQ.



PAYMENT SHARE

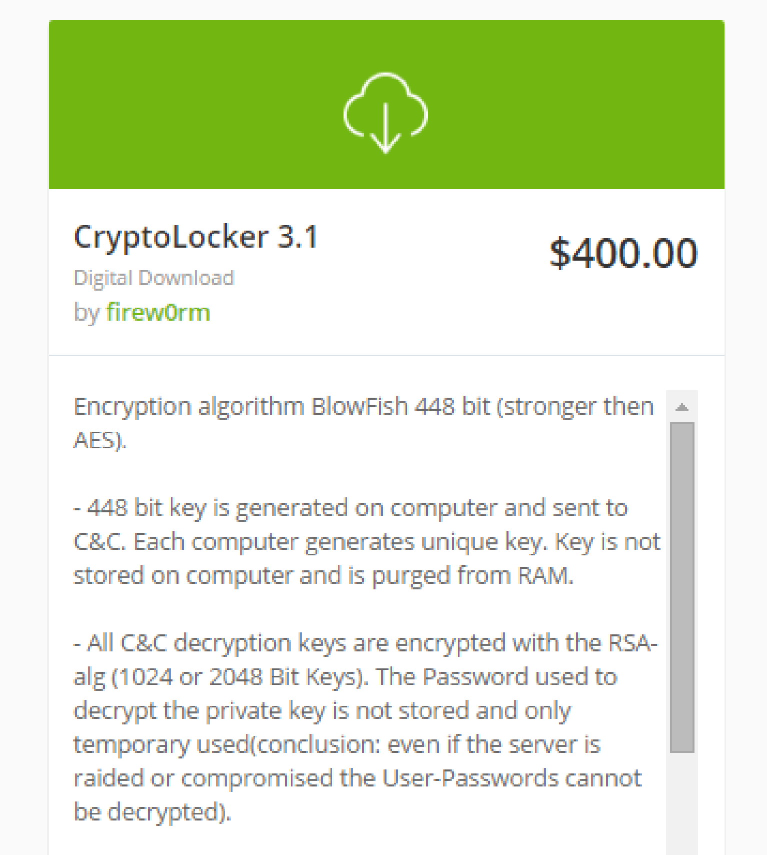
Your share on the payments you have generated is calculated with the following table. The more volume you generate in one week, the more share on the profit you get.

Example: If you generate a volume of 125 BTC, you get a payout of 106.25 BTC. That are at the moment about 45.000 USD! To get a volume over 100 BTC is not a big deal with the right technique!

Volume/Week	Share
<5 BTC	25%
<25 BTC	50%
<125 BTC	75%
>=125 BTC	85%

Gen

Ransomware as a Service (RaaS)



CryptoLocker 3.1

Digital Download

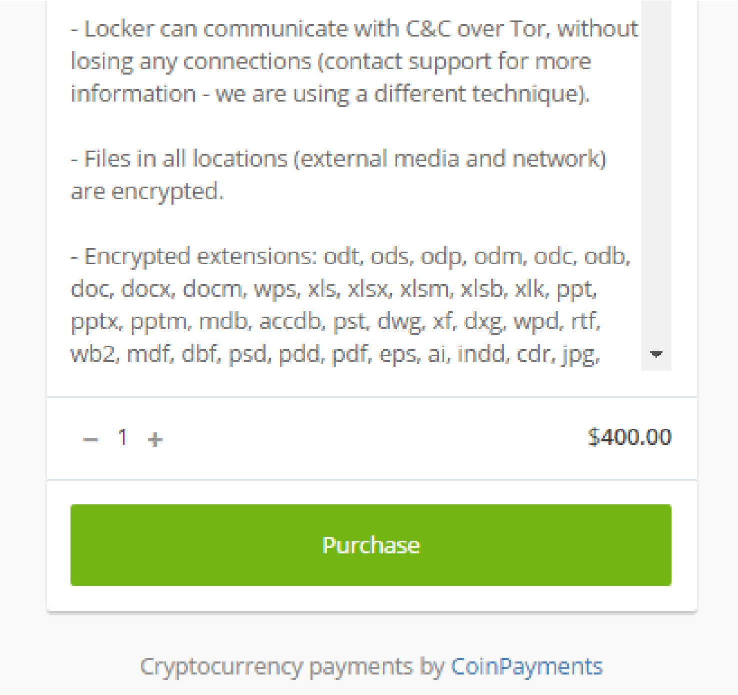
by firew0rm

$400.00

Encryption algorithm BlowFish 448 bit (stronger then AES).

- 448 bit key is generated on computer and sent to C&C. Each computer generates unique key. Key is not stored on computer and is purged from RAM.

- All C&C decryption keys are encrypted with the RSA-alg (1024 or 2048 Bit Keys). The Password used to decrypt the private key is not stored and only temporary used(conclusion: even if the server is raided or compromised the User-Passwords cannot be decrypted).



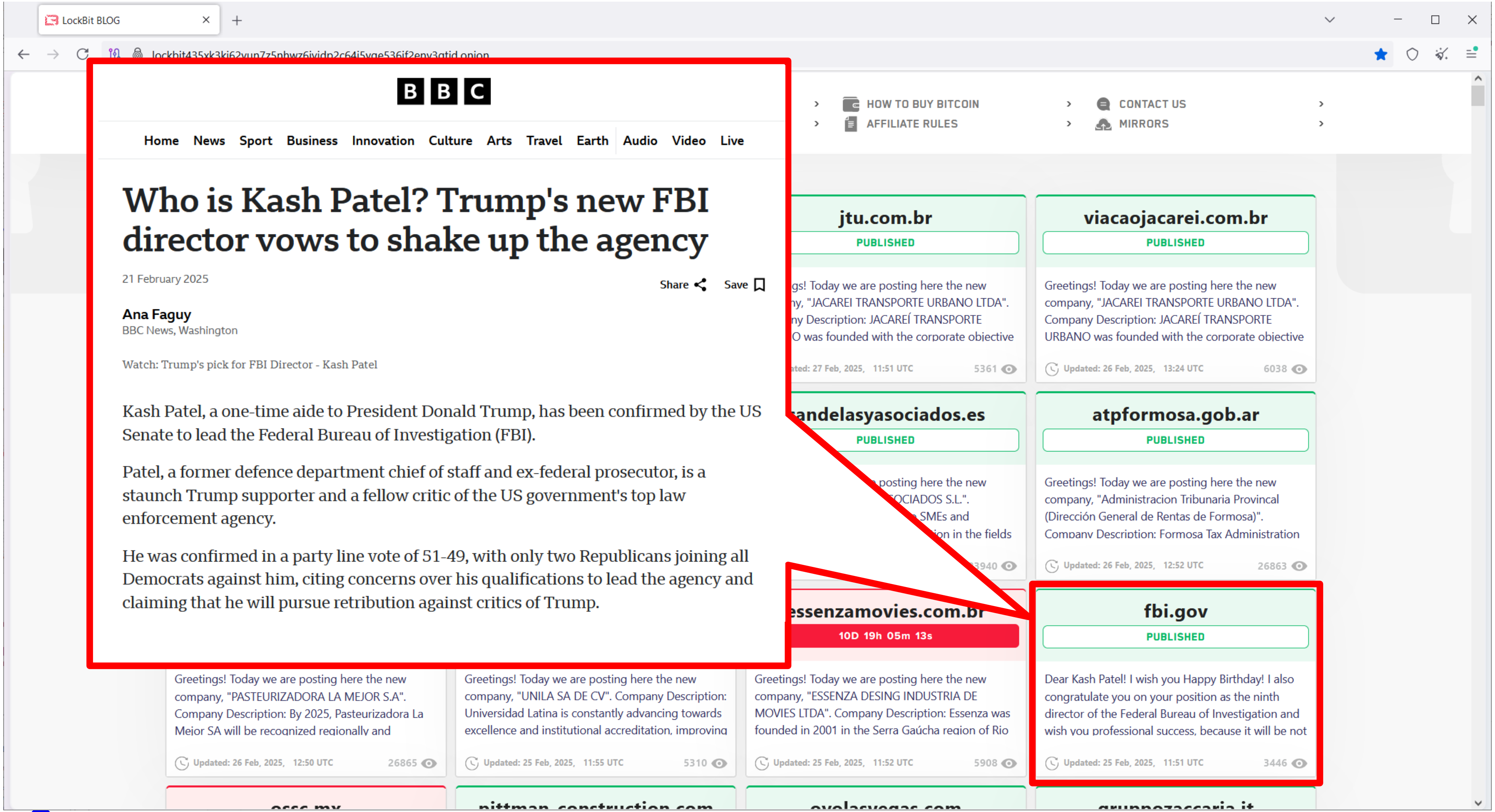
- Locker can communicate with C&C over Tor, without losing any connections (contact support for more information - we are using a different technique).

- Files in all locations (external media and network) are encrypted.

- Encrypted extensions: odt, ods, odp, odm, odc, odb, doc, docx, docm, wps, xls, xlsx, xlsm, xlsb, xlk, ppt, pptx, pptm, mdb, accdb, pst, dwg, xf, dxg, wpd, rtf, wb2, mdf, dbf, psd, pdd, pdf, eps, ai, indd, cdr, jpg,

$400.00

Cryptocurrency payments by CoinPayments



LockBit BLOG
lockbit435xk3ki62yun7z5nhwz6jyjdp2c64j5vge536if2eny3gtid.onion
HOW TO BUY BITCOIN
AFFILIATE RULES
CONTACT US
MIRRORS

BBC

Who is Kash Patel? Trump's new FBI director vows to shake up the agency

21 February 2025

Ana Faguy
BBC News, Washington

Watch: Trump's pick for FBI Director - Kash Patel

Kash Patel, a one-time aide to President Donald Trump, has been confirmed by the US Senate to lead the Federal Bureau of Investigation (FBI).

Patel, a former defence department chief of staff and ex-federal prosecutor, is a staunch Trump supporter and a fellow critic of the US government's top law enforcement agency.

He was confirmed in a party line vote of 51-49, with only two Republicans joining all Democrats against him, citing concerns over his qualifications to lead the agency and claiming that he will pursue retribution against critics of Trump.

jtu.com.br
PUBLISHED
gs! Today we are posting here the new
ny, "JACAREI TRANSPORTE URBANO LTDA".
ny Description: JACAREÍ TRANSPORTE
O was founded with the corporate objective
ated: 27 Feb, 2025, 11:51 UTC 5361

viacaojacarei.com.br
PUBLISHED
Greetings! Today we are posting here the new company, "JACAREI TRANSPORTE URBANO LTDA". Company Description: JACAREÍ TRANSPORTE URBANO was founded with the corporate objective
Updated: 26 Feb, 2025, 13:24 UTC 6038

andelasyasociados.es
PUBLISHED
posting here the new
OCIADOS S.L.".
SMEs and
ion in the fields
3940

atpformosa.gob.ar
PUBLISHED
Greetings! Today we are posting here the new company, "Administracion Tribunaria Provincal (Dirección General de Rentas de Formosa)". Company Description: Formosa Tax Administration
Updated: 26 Feb, 2025, 12:52 UTC 26863

Greetings! Today we are posting here the new company, "PASTEURIZADORA LA MEJOR S.A". Company Description: By 2025, Pasteurizadora La Mejor SA will be recognized regionally and
Updated: 26 Feb, 2025, 12:50 UTC 26865

Greetings! Today we are posting here the new company, "UNILA SA DE CV". Company Description: Universidad Latina is constantly advancing towards excellence and institutional accreditation, improving
Updated: 25 Feb, 2025, 11:55 UTC 5310

essenzamovies.com.br
10D 19h 05m 13s
Greetings! Today we are posting here the new company, "ESSENZA DESING INDUSTRIA DE MOVIES LTDA". Company Description: Essenza was founded in 2001 in the Serra Gaúcha region of Rio
Updated: 25 Feb, 2025, 11:52 UTC 5908

fbi.gov
PUBLISHED
Dear Kash Patel! I wish you Happy Birthday! I also congratulate you on your position as the ninth director of the Federal Bureau of Investigation and wish you professional success, because it will be not
Updated: 25 Feb, 2025, 11:51 UTC 3446

ossc.mx
pittman-construction.com
evolasvegas.com
gruppozaccaria.it

Gen

DEMO

LockBit Ransomware Dark Web Site

What’s the Design of a (Perfect) Ransomware?

Building Ransomware 101

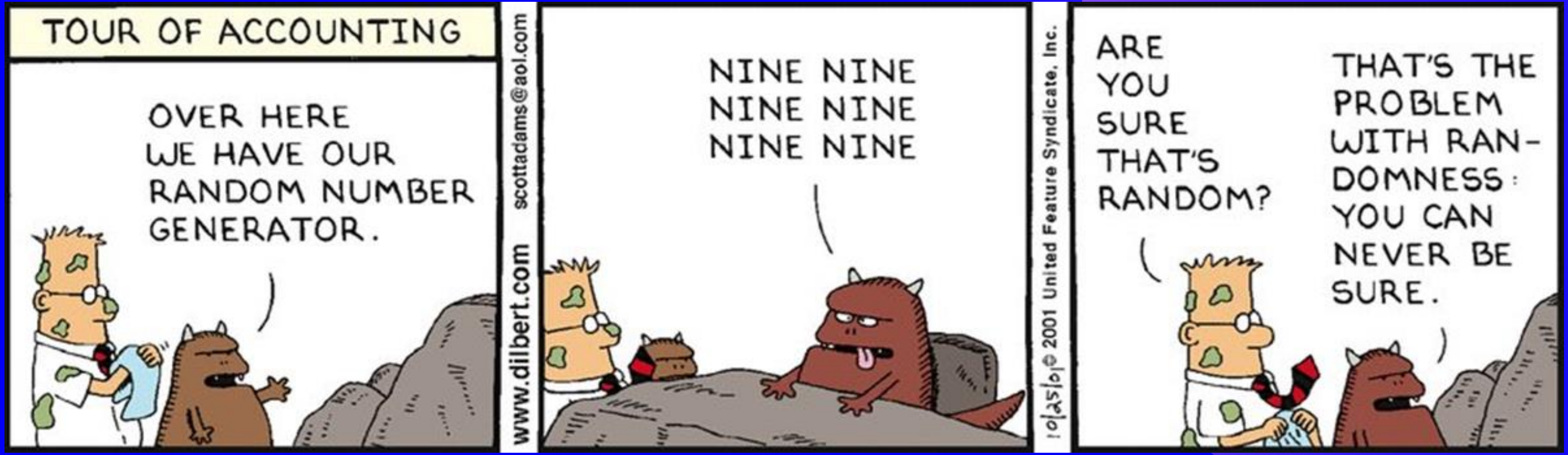
Tasks to solve by ransomware authors:

1. How to generate encryption key?
2. How/where to store key?
3. How to encrypt files?
4. How to secure backend infrastructure?
5. How to decrypt after payment?

Fail at any point:

- Free decryption ☺
- … or no chance to recover files ☹

#1
Key Generation

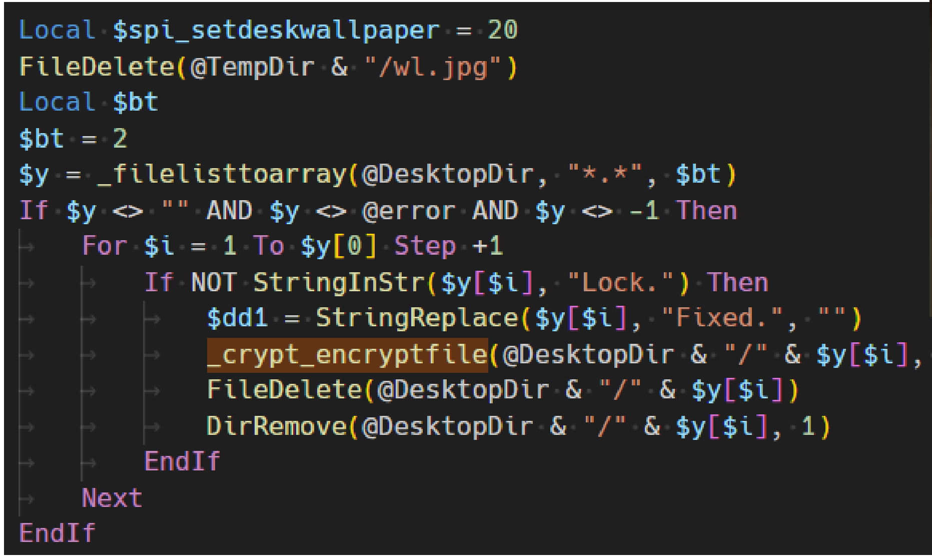

TOUR OF ACCOUNTING
OVER HERE WE HAVE OUR RANDOM NUMBER GENERATOR.
scottadams@aol.com
www.dilbert.com
NINE NINE NINE NINE NINE NINE
© 2001 United Feature Syndicate, Inc.
10/25/01
ARE YOU SURE THAT'S RANDOM?
THAT'S THE PROBLEM WITH RANDOMNESS: YOU CAN NEVER BE SURE.

Key Generation

- There are rules that need to be obeyed
  - The key must be generated with a good random number generator (RNG)
  - The key must be generated new for each file

Key Generation: The Wrong Way #1

- Crypt888 ransomware
- The authors considered the password „888“ goo



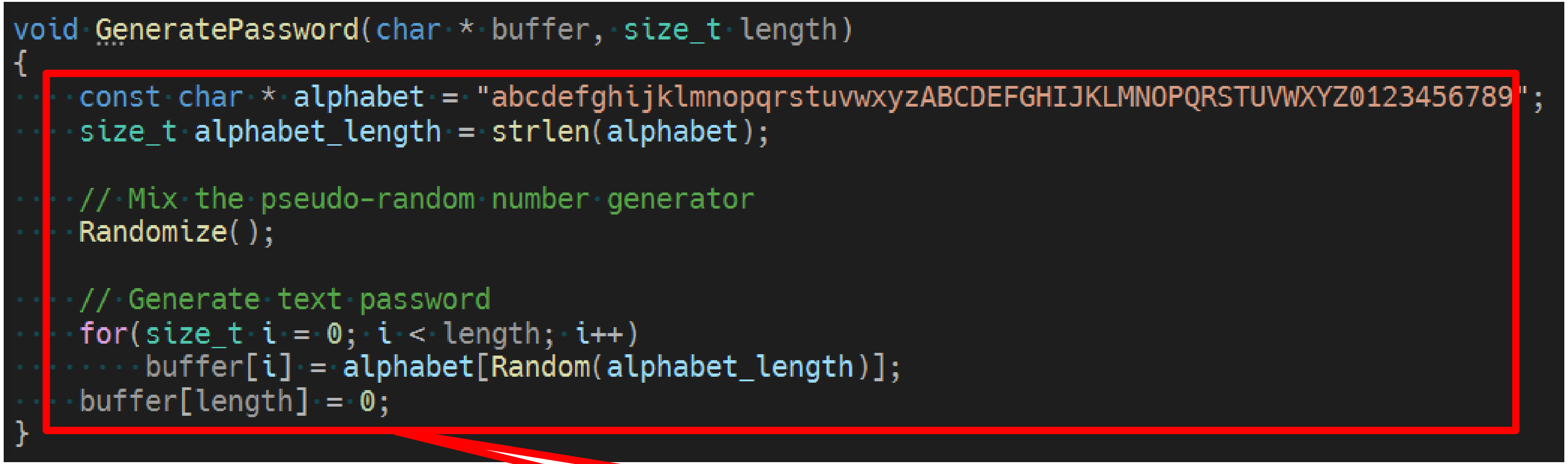
```
Local $spi_setdeskwallpaper = 20
FileDelete(@TempDir & "/wl.jpg")
Local $bt
$bt = 2
$y = _filelisttoarray(@DesktopDir, "*.*", $bt)
If $y <> "" AND $y <> @error AND $y <> -1 Then
    For $i = 1 To $y[0] Step +1
        If NOT StringInStr($y[$i], "Lock.") Then
            $dd1 = StringReplace($y[$i], "Fixed.", "")
            _crypt_encryptfile(@DesktopDir & "/" & $y[$i], @DesktopDir & "/Lock." & $dd1, "888"  $calg_des)
            FileDelete(@DesktopDir & "/" & $y[$i])
            DirRemove(@DesktopDir & "/" & $y[$i], 1)
        EndIf
    Next
EndIf
```

Key Generation: The Wrong Way #2

- Generated key
  - Based on system configuration (key: USER_userpc_00:14:22:01:23:45) ☺
  - The rand() function provided by framework libraries - PRNG
  - GetTickCount()
- Example: BadBlock ransomware

Key Generation: The Wrong Way #2

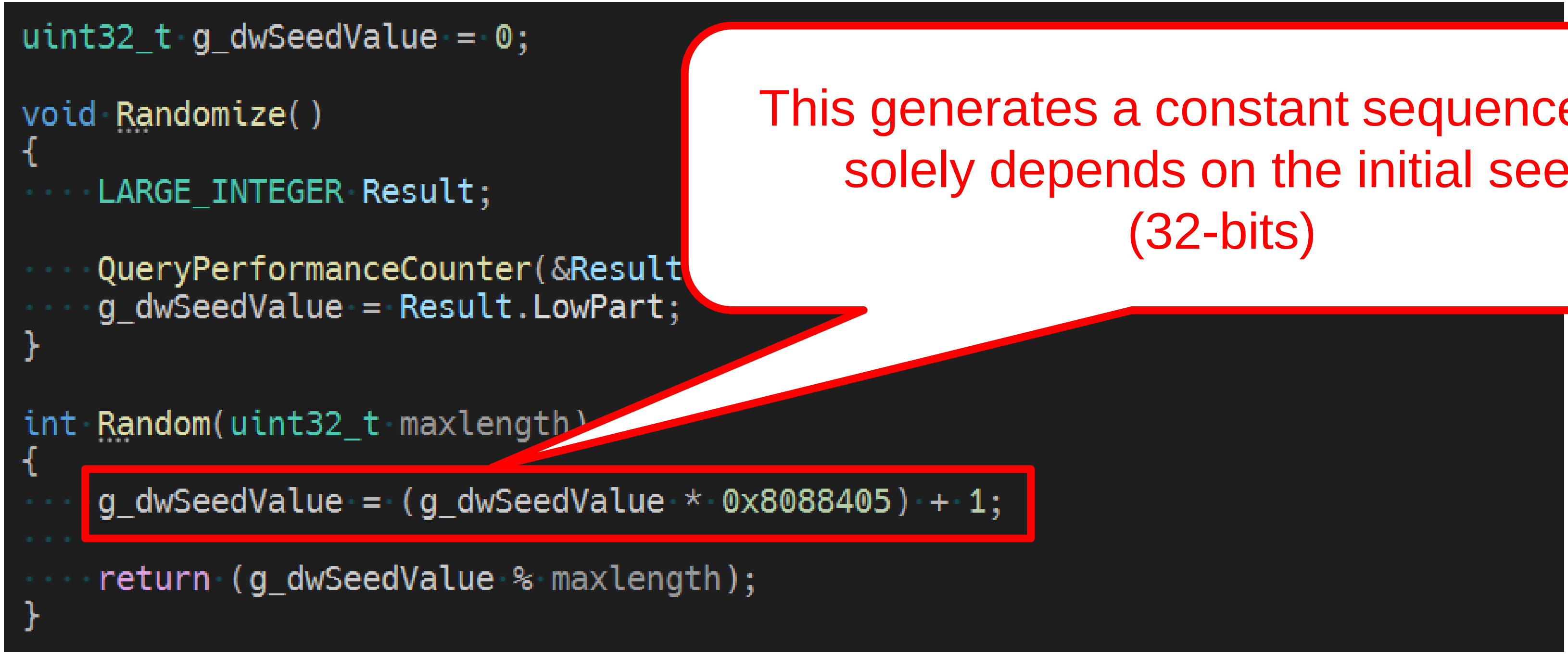
- BadBlock Ransomware's key generation algorithm



```
void GeneratePassword(char * buffer, size_t length)
{
    const char * alphabet = "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789";
    size_t alphabet_length = strlen(alphabet);

    // Mix the pseudo-random number generator
    Randomize();

    // Generate text password
    for(size_t i = 0; i < length; i++)
        buffer[i] = alphabet[Random(alphabet_length)];
    buffer[length] = 0;
}
```

Can you find the weak spot?

Key Generation: The Wrong Way #2



```
uint32_t g_dwSeedValue = 0;

void Randomize()
{
    LARGE_INTEGER Result;

    QueryPerformanceCounter(&Result
    g_dwSeedValue = Result.LowPart;
}

int Random(uint32_t maxlength)
{
    g_dwSeedValue = (g_dwSeedValue * 0x8088405) + 1;

    return (g_dwSeedValue % maxlength);
}
```

This generates a constant sequence that solely depends on the initial seed (32-bits)

Key Generation: The Wrong Way #2

- Regardless the length of the password, its strength is 32 bits
- Brute-forceable at speed of ~7.5 M passwords per second
    - Intel Xeon E5-1620 v3 @ 3.5 GHz (Windows 10 64-bit, 8 threads)

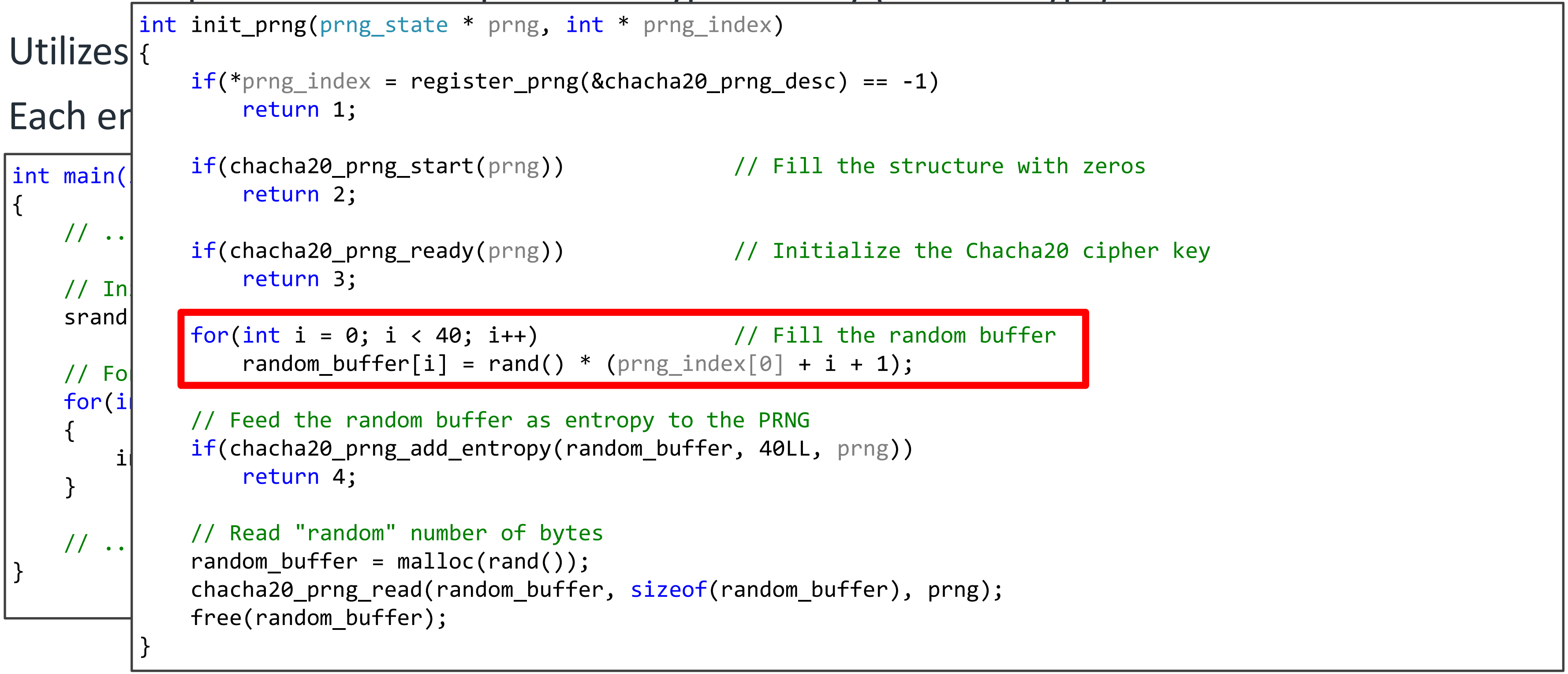
Rhysida Ransomware (2023)

- Written in pure C with multiplatform crypto-library (LibTomCrypt)
- Utilizes multiple encryptor threads
- Each encryptor thread has its own PRNG for generating keys

```c
int main(int argc, char * argv[])
{
    // ...

    // Init the CRT pseudo-random number generator (PRNG)
    srand(time(NULL));

    // For every encryptor thread, create its own Chacha20 PRNG
    for(int i = 0; i < g_encryptor_threads; i++)
    {
        init_prng(&g_thread_prngs[i], &g_perthread_prng_indexes[i]);
    }

    // ...
}
```

Rhysida Ransomware (2023)

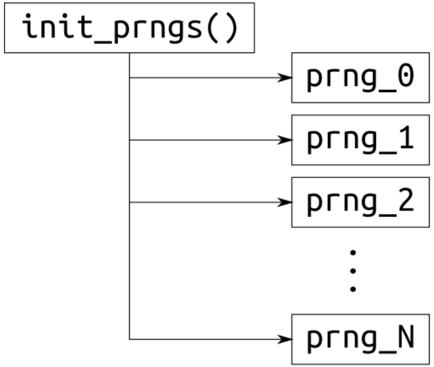
- Written in pure C with multiplatform crypto-library (LibTomCrypt)
- Utilizes
- Each er



```
int main(
{
    // ..

    // In
    srand

    // Fo
    for(i
    {
        i
    }

    // ..
}
```

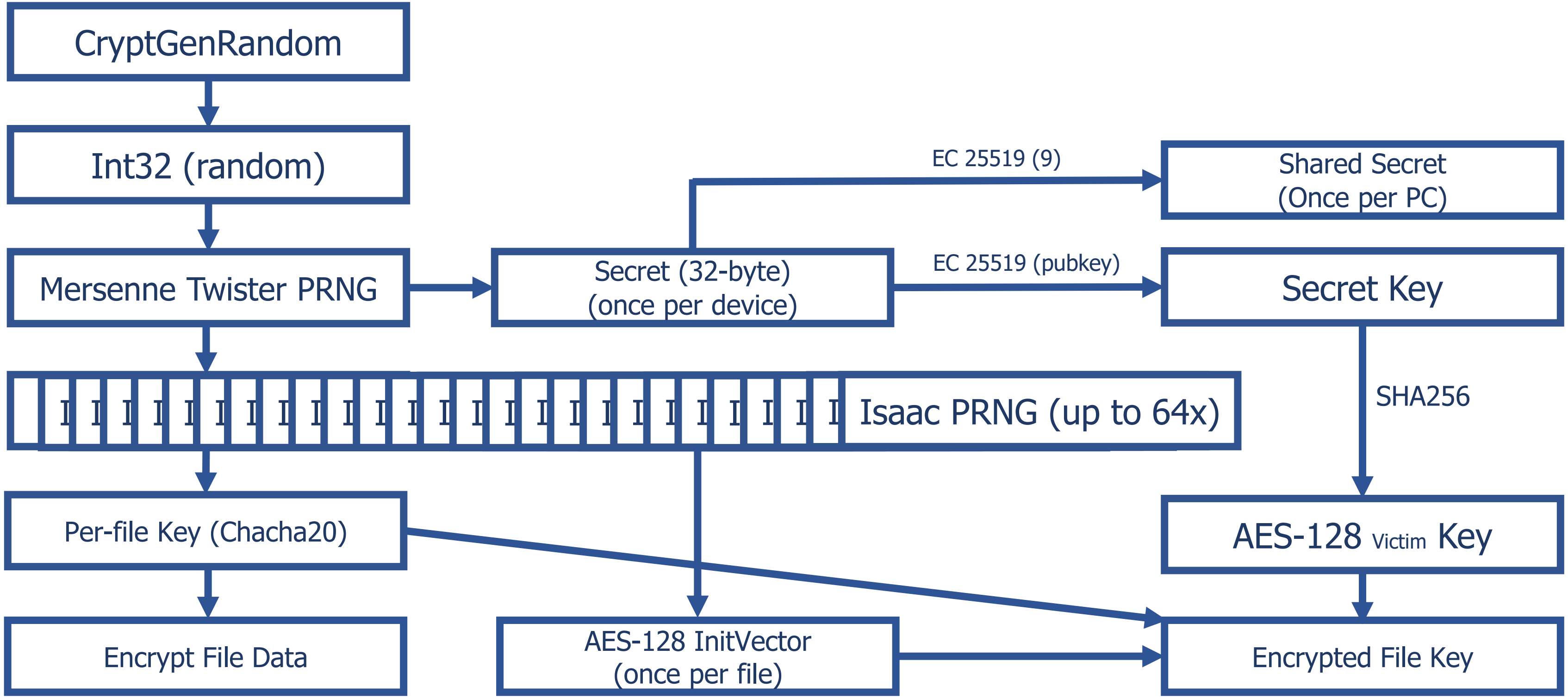
```
int init_prng(prng_state * prng, int * prng_index)
{
    if(*prng_index = register_prng(&chacha20_prng_desc) == -1)
        return 1;

    if(chacha20_prng_start(prng))               // Fill the structure with zeros
        return 2;

    if(chacha20_prng_ready(prng))               // Initialize the Chacha20 cipher key
        return 3;

    for(int i = 0; i < 40; i++)                 // Fill the random buffer
        random_buffer[i] = rand() * (prng_index[0] + i + 1);

    // Feed the random buffer as entropy to the PRNG
    if(chacha20_prng_add_entropy(random_buffer, 40LL, prng))
        return 4;

    // Read "random" number of bytes
    random_buffer = malloc(rand());
    chacha20_prng_read(random_buffer, sizeof(random_buffer), prng);
    free(random_buffer);
}
```

Rhysida Ransomware (2023)



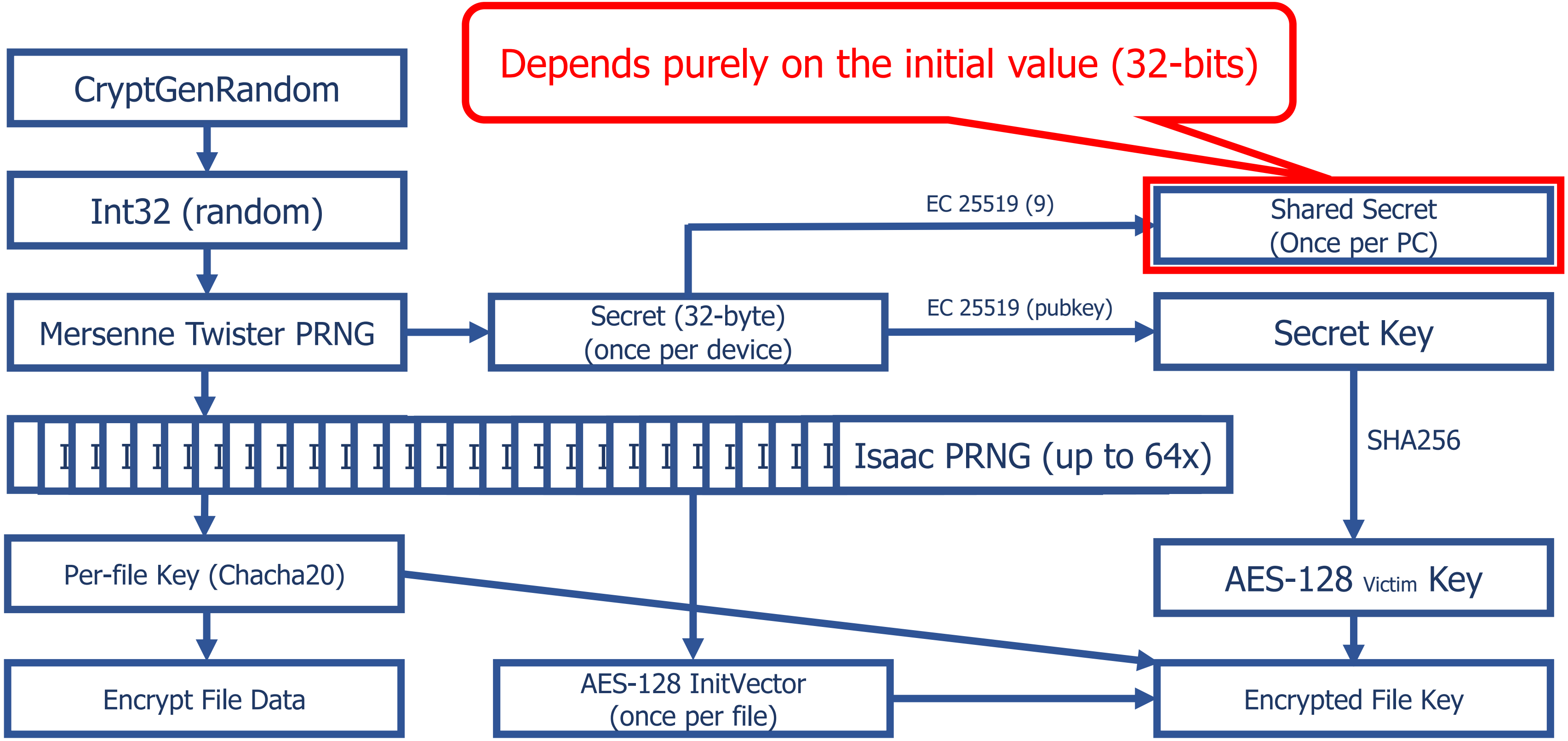
```
...
filename = get_filename(file_queue);
while (filename! = NULL) {
  key = gen_random_bytes(&prng[thread_id], 0x20);
  iv  = gen_random_bytes(&prng[thread_id], 0x10);

  encrypt_file_AES(filename, key, iv);

  encrypt_RSA(enc_key, key, 0x20, master_key);
  encrypt_RSA( enc_iv,  iv, 0x10, master_key);

  append2file(filename, enc_key, RSA_BLOCK_SIZE);
  append2file(filename,  enc_iv, RSA_BLOCK_SIZE);

  filename = get_filename(file_queue);
}
```

TargetCompany Ransomware (2022)



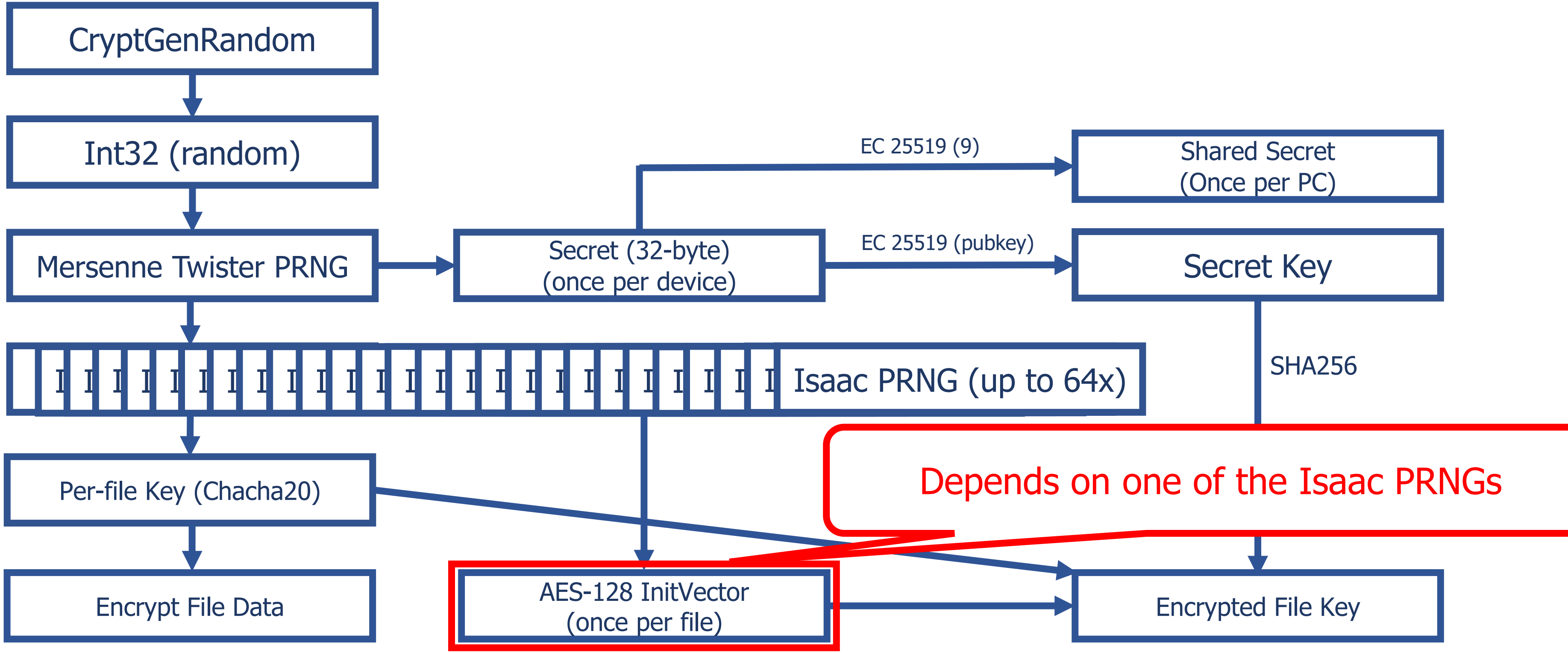
Gen

TargetCompany Ransomware (2022)



Gen

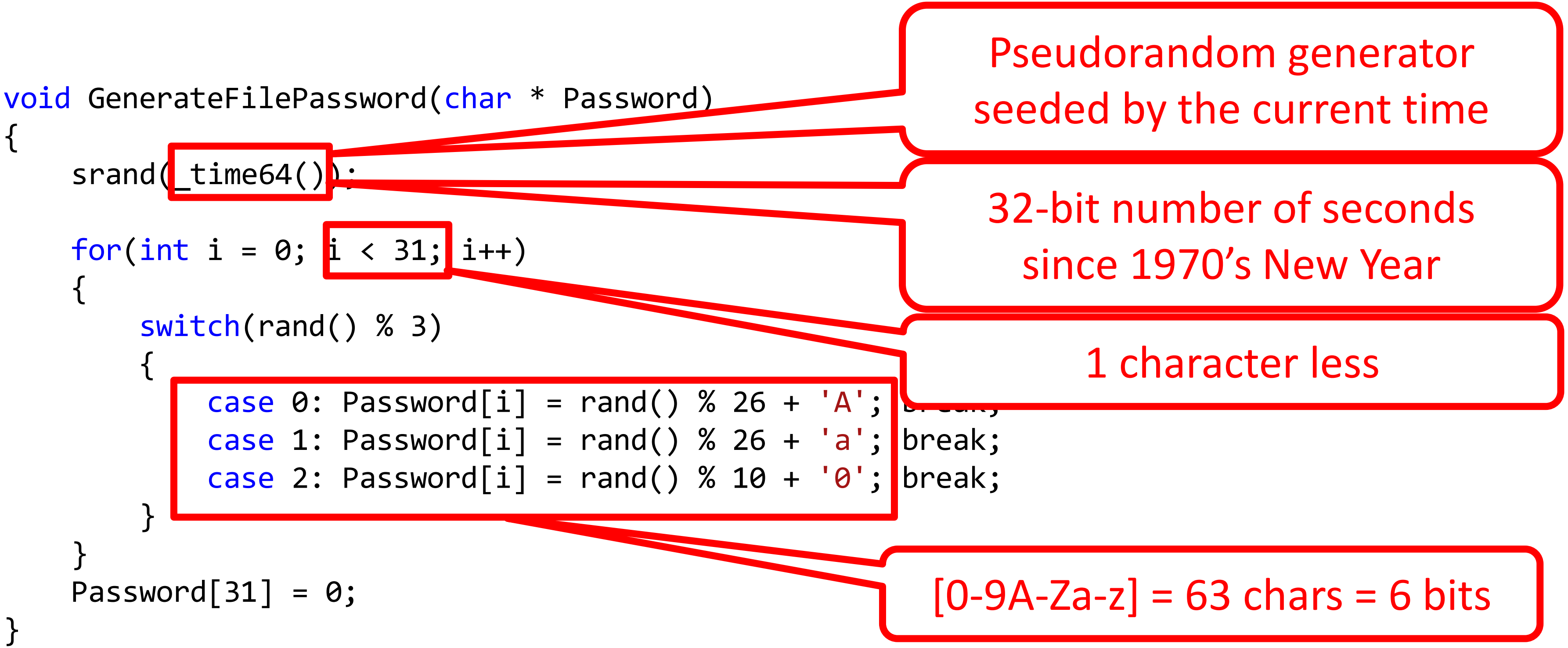
TargetCompany Ransomware (2022)



Depends on one of the Isaac PRNGs

Gen

AtomSilo Ransomware (2021)



```
void GenerateFilePassword(char * Password)
{
    srand(_time64());

    for(int i = 0; i < 31; i++)
    {
        switch(rand() % 3)
        {
            case 0: Password[i] = rand() % 26 + 'A'; break;
            case 1: Password[i] = rand() % 26 + 'a'; break;
            case 2: Password[i] = rand() % 10 + '0'; break;
        }
    }
    Password[31] = 0;
}
```

Pseudorandom generator seeded by the current time

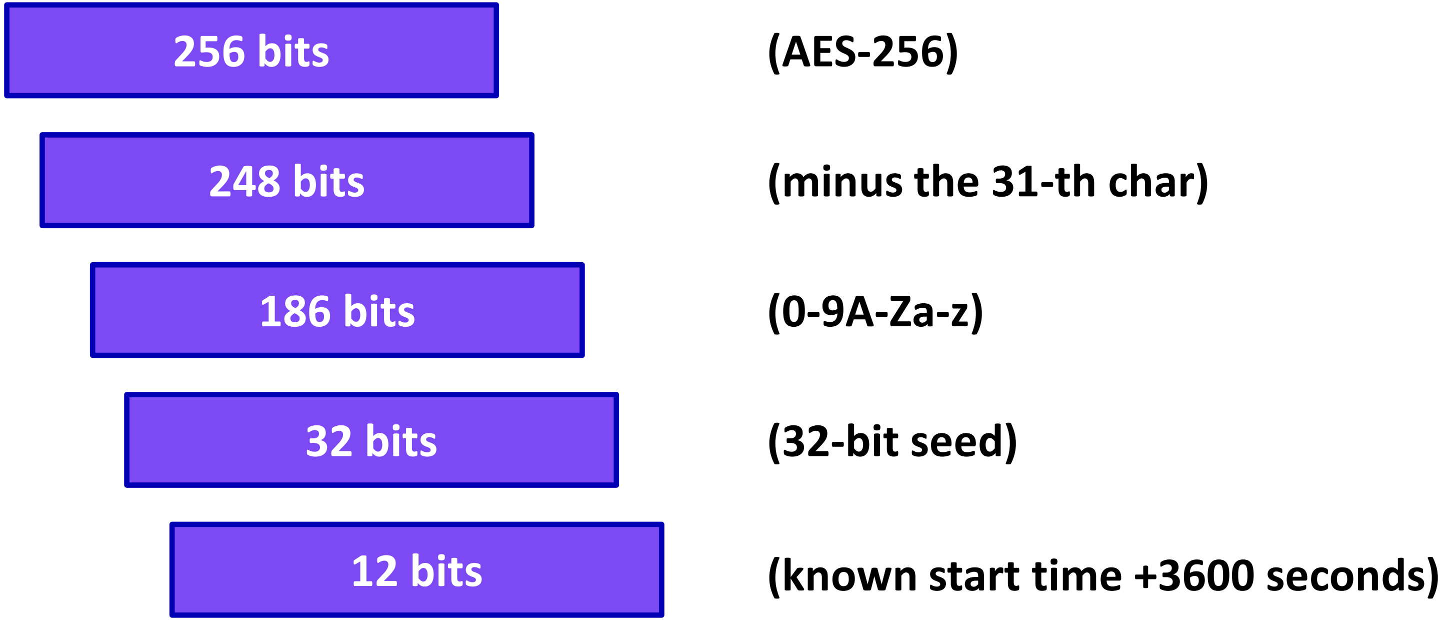
32-bit number of seconds since 1970's New Year

1 character less

[0-9A-Za-z] = 63 chars = 6 bits

AtomSilo (2021)

- Key strength degradation:

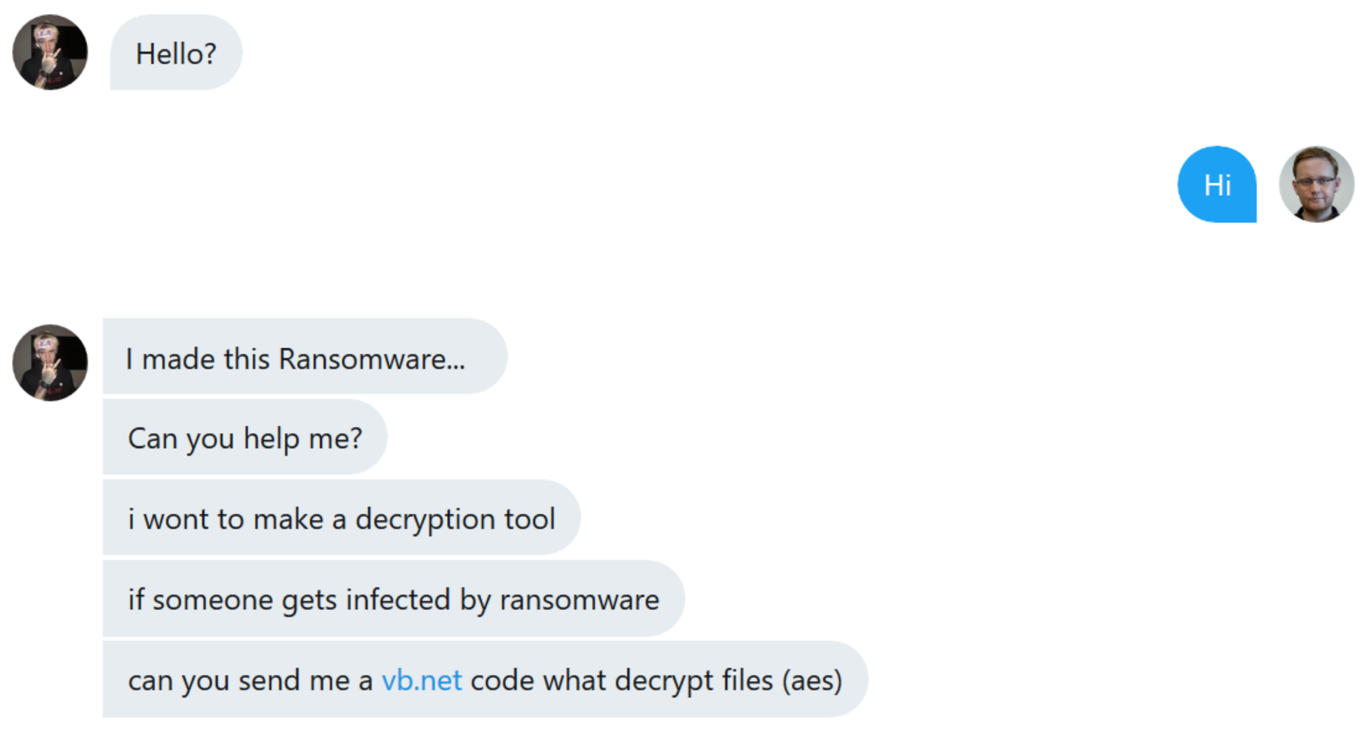


256 bits	(AES-256)
248 bits	(minus the 31-th char)
186 bits	(0-9A-Za-z)
32 bits	(32-bit seed)
12 bits	(known start time +3600 seconds)

BitCrypt Ransomware (2014)

- Uses RSA key: 312988471966254006395069386371619301627890114642959526005441458293358 49533528834917800088971765784757175491347320005860302574523
- Quiz: good / bad?
- 128 digits != 128 bytes (RSA-426 != RSA-1024)
- Crackable within a few hours on a regular PC
- $ ./factor.sh <key> -s 4 -t 6
- Total cpu/real time for cracking: 751058/51141
- https://www.infosecurity-magazine.com/news/bitcrypt-ransomware-easily-broken/

#2 Failures in Encryption Algorithm



Hello?

Hi

I made this Ransomware...

Can you help me?

i wont to make a decryption tool

if someone gets infected by ransomware

can you send me a vb.net code what decrypt files (aes)

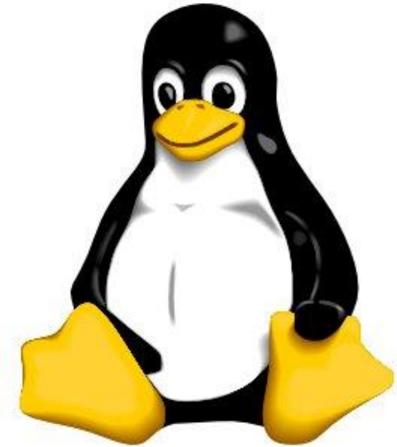
Encryption Algorithm

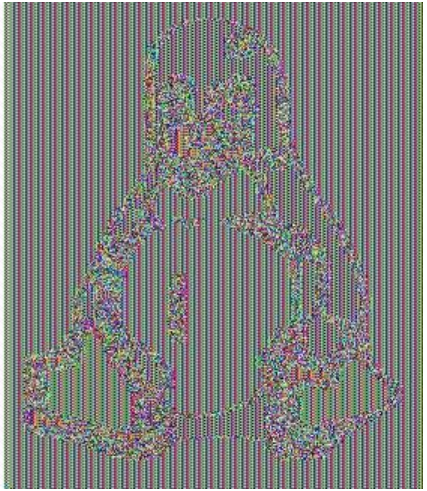
- Symmetric cryptography vs asymmetric cryptography

	Symmetric	Asymmetric
Number of keys	One	Two (public and private)
Speed	Fast	Slow
Block size	Small	Large
Code complexity	Small to medium	Medium to high
Decryption without a key	Trivial to impossible	Damn-hard to impossible

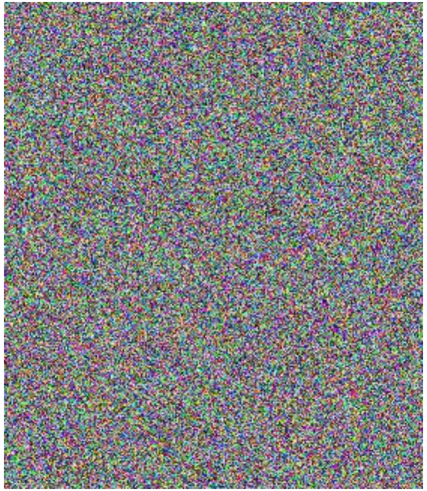
- The most used algorithms: XOR (!), RC4, ChaCha20, AES, Blowfish, RSA, ECDH

Block Cipher Modes of Operation

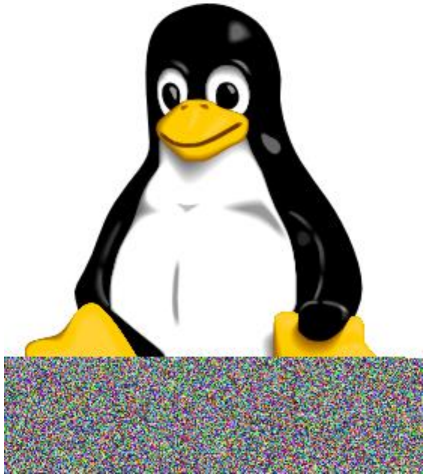




Bandarchor
(AES-ECB)



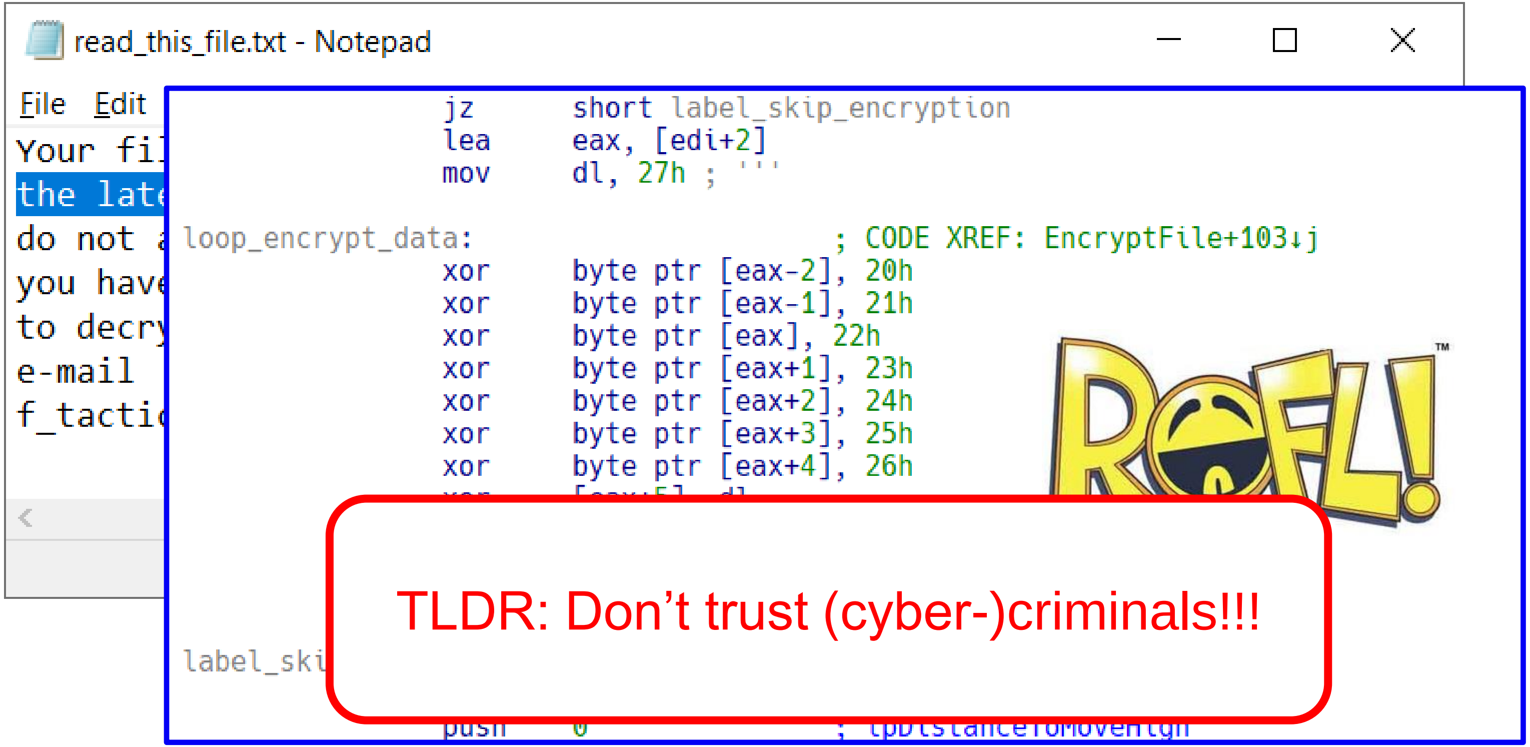
TeslaCrypt
(AES-CBC)



Globe
(AES-CBC)

Legion Ransomware

- Claims to be using “the latest encryption algorithm RSA 2048”

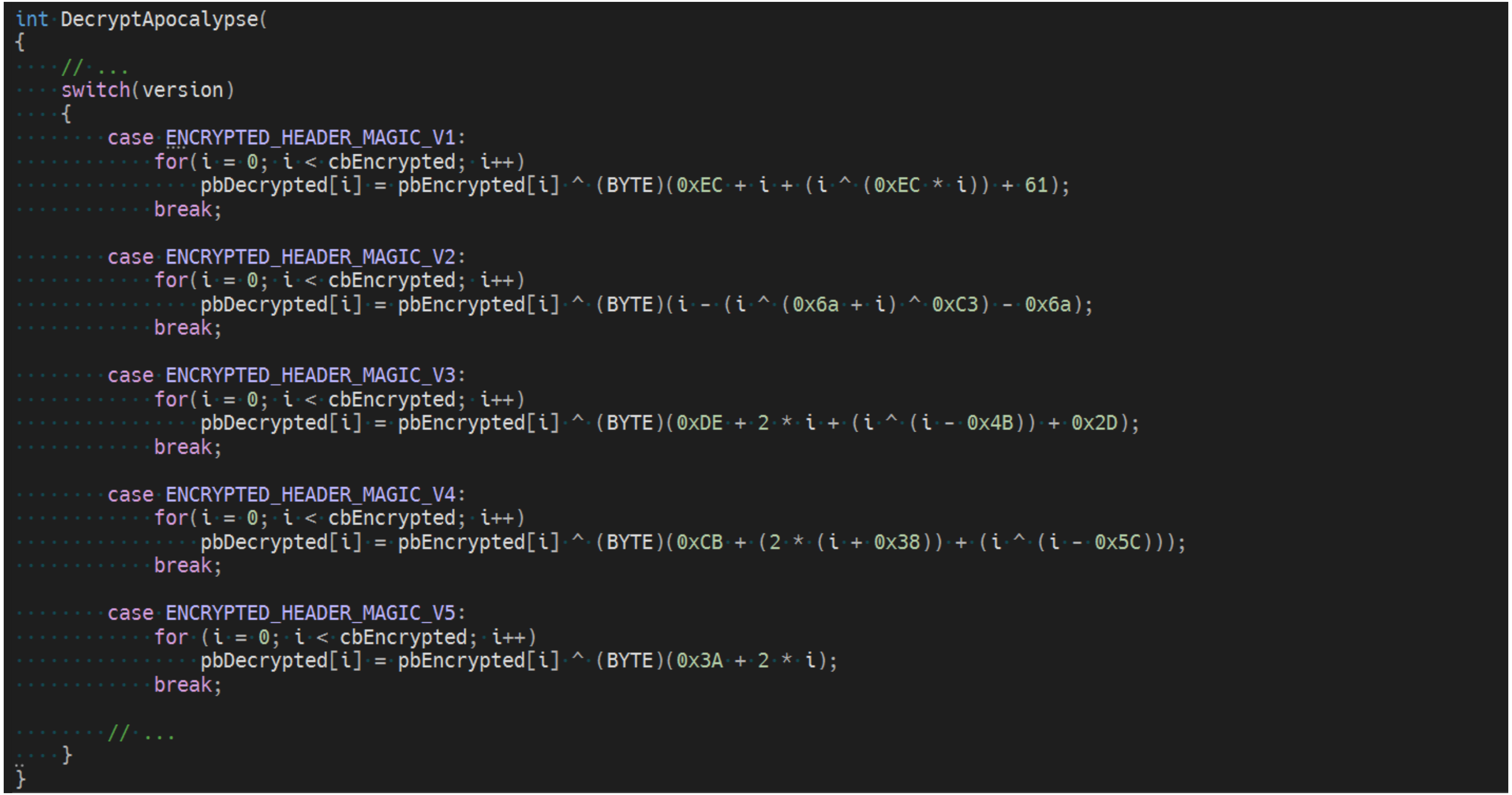


```
Your fi
the late
do not a
you have
to decry
e-mail
f_tactic
```

```
                jz      short label_skip_encryption
                lea     eax, [edi+2]
                mov     dl, 27h ; '''

loop_encrypt_data:                      ; CODE XREF: EncryptFile+103↓j
                xor     byte ptr [eax-2], 20h
                xor     byte ptr [eax-1], 21h
                xor     byte ptr [eax], 22h
                xor     byte ptr [eax+1], 23h
                xor     byte ptr [eax+2], 24h
                xor     byte ptr [eax+3], 25h
                xor     byte ptr [eax+4], 26h
                xor     [eax+5], dl

label_ski

                push    0               ; lpDistanceToMoveHigh
```

TLDR: Don’t trust (cyber-)criminals!!!

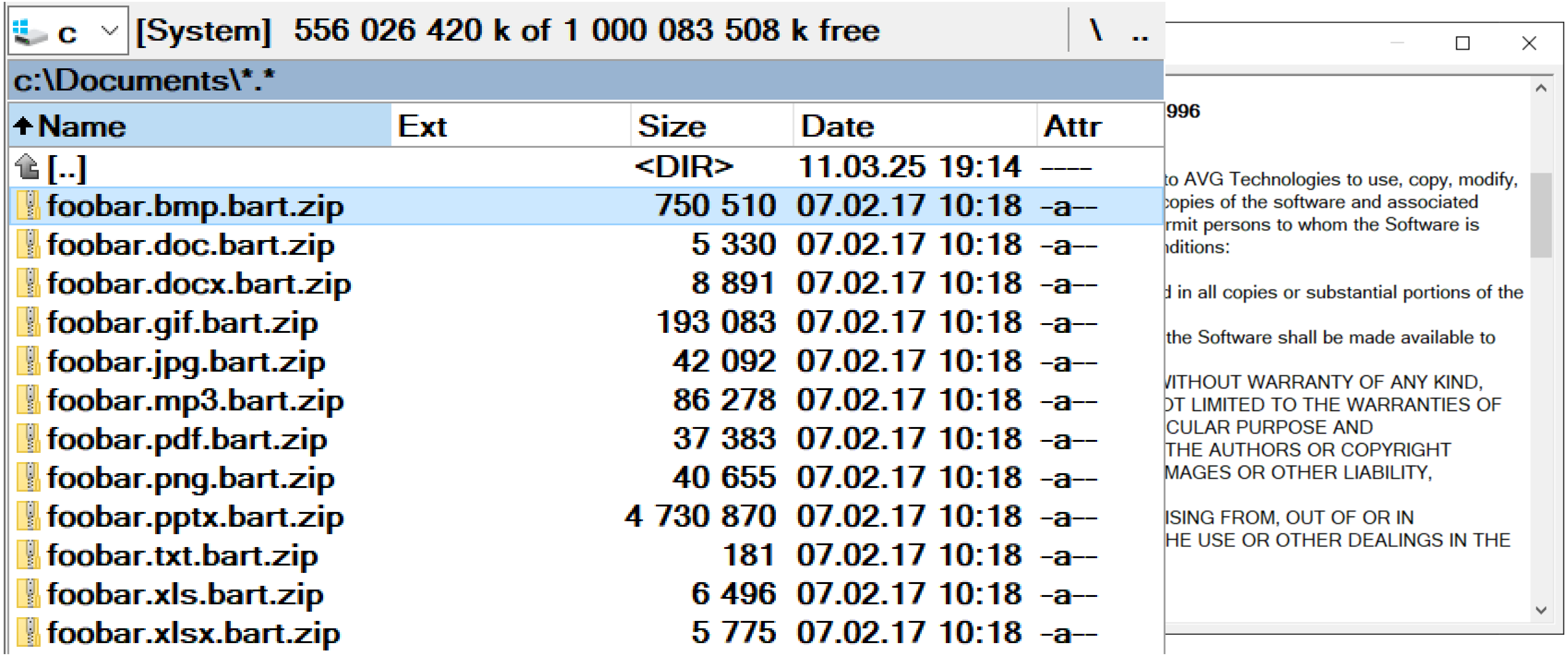
Apocalypse Ransomware



```
int DecryptApocalypse(
{
    // ...
    switch(version)
    {
        case ENCRYPTED_HEADER_MAGIC_V1:
            for(i = 0; i < cbEncrypted; i++)
                pbDecrypted[i] = pbEncrypted[i] ^ (BYTE)(0xEC + i + (i ^ (0xEC * i)) + 61);
            break;

        case ENCRYPTED_HEADER_MAGIC_V2:
            for(i = 0; i < cbEncrypted; i++)
                pbDecrypted[i] = pbEncrypted[i] ^ (BYTE)(i - (i ^ (0x6a + i) ^ 0xC3) - 0x6a);
            break;

        case ENCRYPTED_HEADER_MAGIC_V3:
            for(i = 0; i < cbEncrypted; i++)
                pbDecrypted[i] = pbEncrypted[i] ^ (BYTE)(0xDE + 2 * i + (i ^ (i - 0x4B)) + 0x2D);
            break;

        case ENCRYPTED_HEADER_MAGIC_V4:
            for(i = 0; i < cbEncrypted; i++)
                pbDecrypted[i] = pbEncrypted[i] ^ (BYTE)(0xCB + (2 * (i + 0x38)) + (i ^ (i - 0x5C)));
            break;

        case ENCRYPTED_HEADER_MAGIC_V5:
            for (i = 0; i < cbEncrypted; i++)
                pbDecrypted[i] = pbEncrypted[i] ^ (BYTE)(0x3A + 2 * i);
            break;

        // ...
    }
}
```

Bart Ransomware

- Stored original files into ZIP archives, protected with password



c [System] 556 026 420 k of 1 000 083 508 k free \ ..

c:\Documents*.*

Name	Ext	Size	Date	Attr
[..]		<DIR>	11.03.25 19:14	----
foobar.bmp.bart.zip		750 510	07.02.17 10:18	-a--
foobar.doc.bart.zip		5 330	07.02.17 10:18	-a--
foobar.docx.bart.zip		8 891	07.02.17 10:18	-a--
foobar.gif.bart.zip		193 083	07.02.17 10:18	-a--
foobar.jpg.bart.zip		42 092	07.02.17 10:18	-a--
foobar.mp3.bart.zip		86 278	07.02.17 10:18	-a--
foobar.pdf.bart.zip		37 383	07.02.17 10:18	-a--
foobar.png.bart.zip		40 655	07.02.17 10:18	-a--
foobar.pptx.bart.zip		4 730 870	07.02.17 10:18	-a--
foobar.txt.bart.zip		181	07.02.17 10:18	-a--
foobar.xls.bart.zip		6 496	07.02.17 10:18	-a--
foobar.xlsx.bart.zip		5 775	07.02.17 10:18	-a--

996

to AVG Technologies to use, copy, modify,
copies of the software and associated
rmit persons to whom the Software is
nditions:

d in all copies or substantial portions of the

the Software shall be made available to

WITHOUT WARRANTY OF ANY KIND,
OT LIMITED TO THE WARRANTIES OF
CULAR PURPOSE AND
THE AUTHORS OR COPYRIGHT
MAGES OR OTHER LIABILITY,

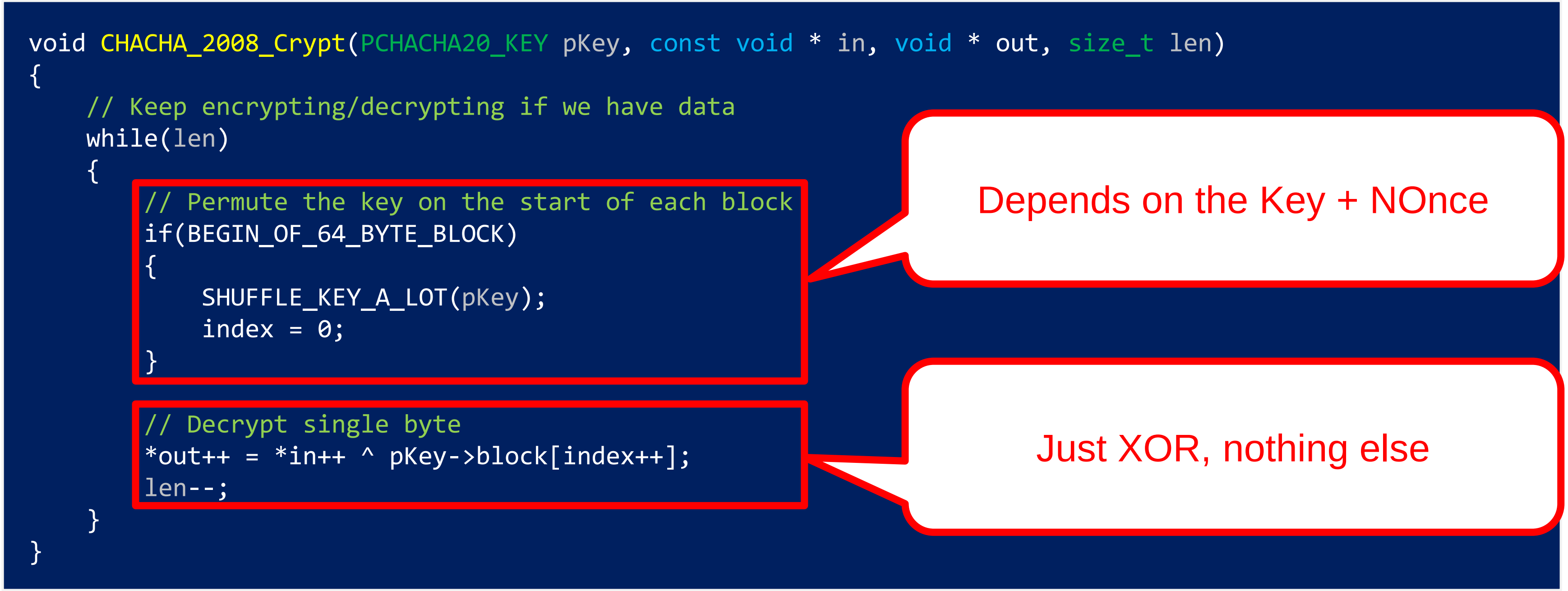
ISING FROM, OUT OF OR IN
HE USE OR OTHER DEALINGS IN THE

Akira Ransomware (2023)

- Encrypts files using Chacha20 algorithm
- Key and n-once are generated by a secure RNG (CryptGenRandom)
- However, only one key&n-once is generated per machine ☹

Can this fact be used for decryption?

Akira Ransomware (2023)

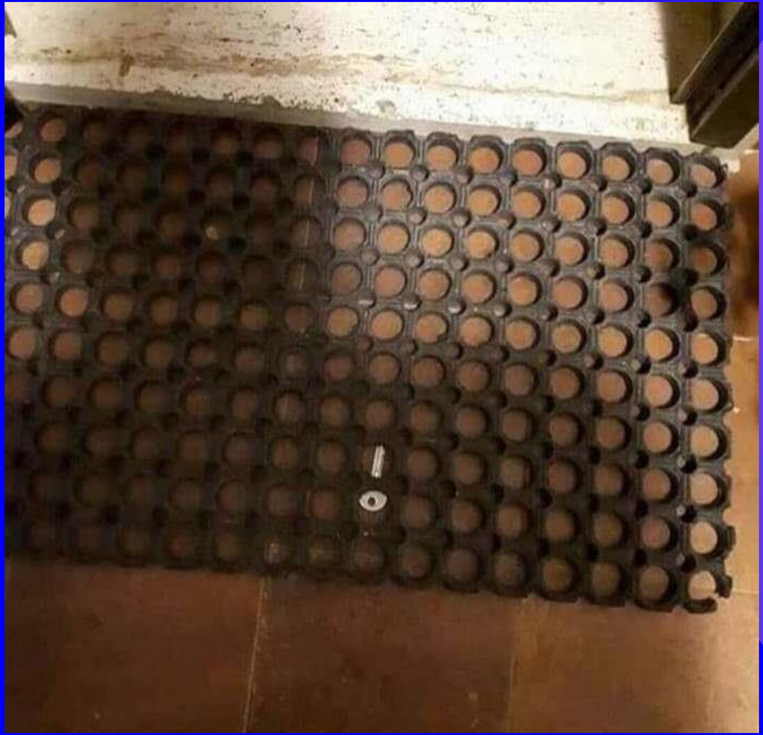


```
void CHACHA_2008_Crypt(PCHACHA20_KEY pKey, const void * in, void * out, size_t len)
{
    // Keep encrypting/decrypting if we have data
    while(len)
    {
        // Permute the key on the start of each block
        if(BEGIN_OF_64_BYTE_BLOCK)
        {
            SHUFFLE_KEY_A_LOT(pKey);
            index = 0;
        }

        // Decrypt single byte
        *out++ = *in++ ^ pKey->block[index++];
        len--;
    }
}
```

Depends on the Key + NOnce

Just XOR, nothing else

#3
Key Storage

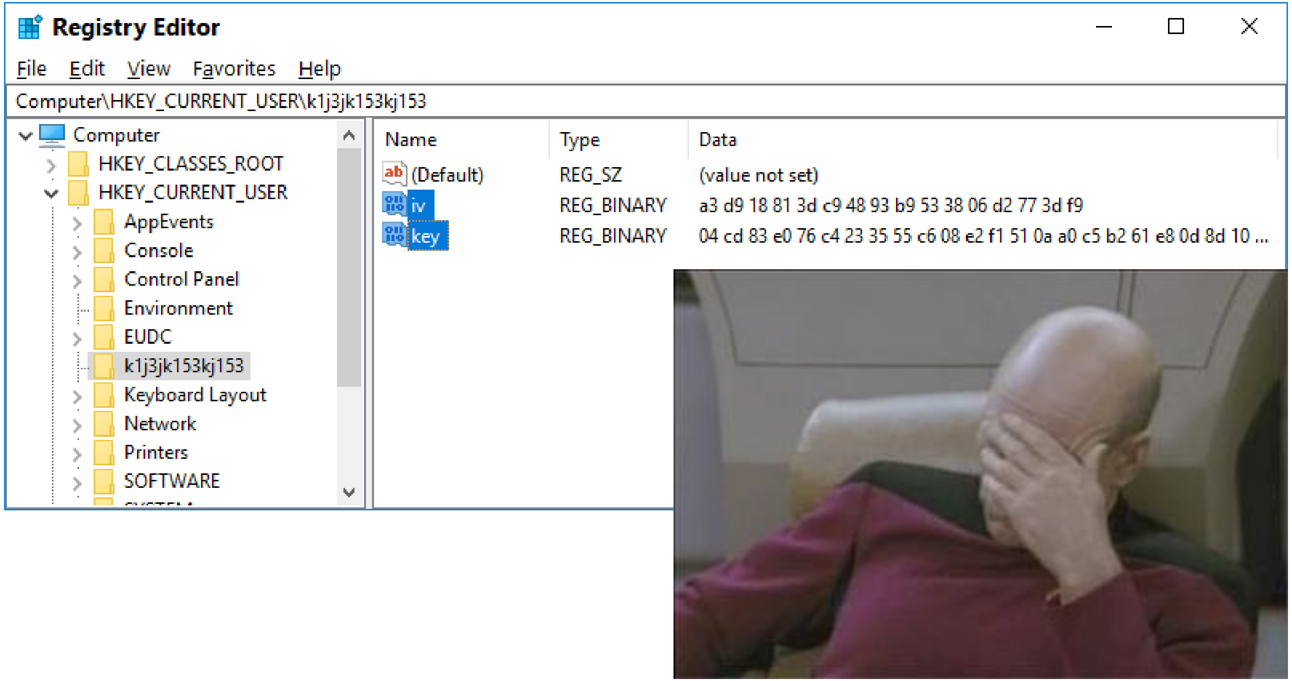


Key Storage

- To allow decryption, keys must be stored somewhere / somehow
- Not as easy as you would think
- Store the key somewhere in the system?
  - How?
- Send the key to the cloud?
  - What if the cloud server is down?
  - What if the cloud server is taken down by the law-enforcement?
- Generate the key in the cloud?
  - Again: What if the cloud server is taken down by the law-enforcement?
- Encrypt files with asymmetric cryptography?

Key Storage: The Wrong Way #1

- Example: NoobCrypt ransomware
- Keeps the key on the infected system. In plaintext



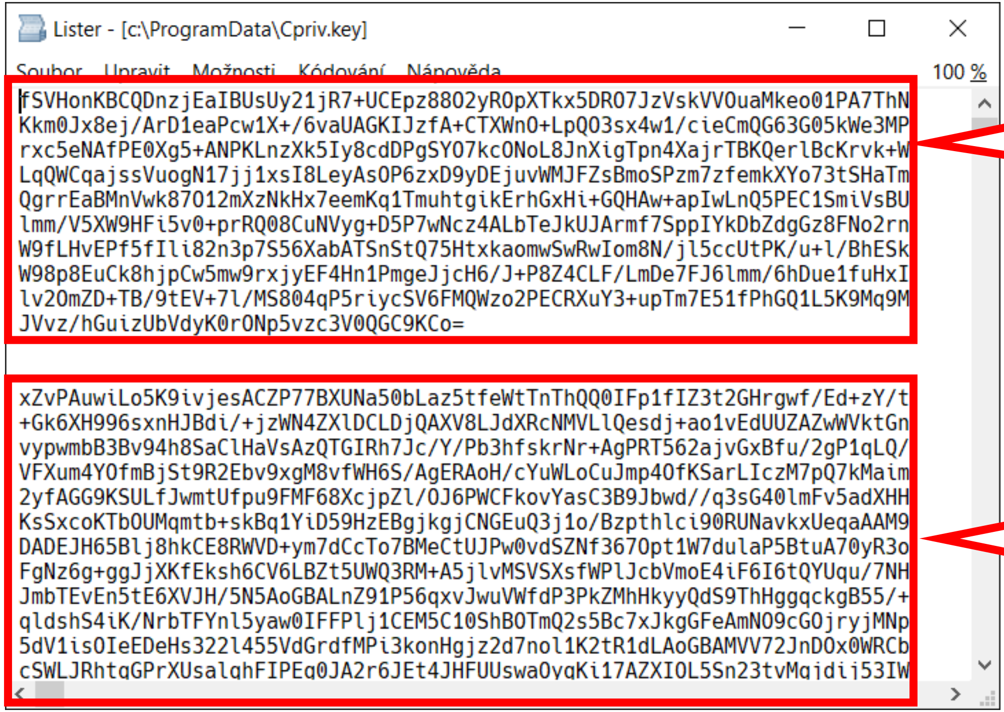
Computer\HKEY_CURRENT_USER\k1j3jk153kj153

Name	Type	Data
(Default)	REG_SZ	(value not set)
iv	REG_BINARY	a3 d9 18 81 3d c9 48 93 b9 53 38 06 d2 77 3d f9
key	REG_BINARY	04 cd 83 e0 76 c4 23 35 55 c6 08 e2 f1 51 0a a0 c5 b2 61 e8 0d 8d 10 ...

Key Storage: The Wrong Way #2

- Fonix Ransomware
- File Key (Salsa/Chacha20)
    - … is encrypted by “Session Key” (RSA-2048)
    - … which is encrypted by “Master Key” (RSA-4096)
- The session RSA key is stored in two files:
    - C:\ProgramData\Cpub.key (public key)
    - C:\ProgramData\Cpriv.key (private key)

Key Storage: The Wrong Way #2



```
fSVHonKBCQDnzjEaIBUsUy21jR7+UCEpz8802yROpXTkx5DRO7JzVskVVOuaMkeo01PA7ThN
Kkm0Jx8ej/ArD1eaPcw1X+/6vaUAGKIJzfA+CTXWnO+LpQO3sx4w1/cieCmQG63G05kWe3MP
rxc5eNAfPE0Xg5+ANPKLnzXk5Iy8cdDPgSYO7kcONoL8JnXigTpn4XajrTBKQerlBcKrvk+W
LqQWCqajssVuogN17jj1xsI8LeyAsOP6zxD9yDEjuvWMJFZsBmoSPzm7zfemkXYo73tSHaTm
QgrrEaBMnVwk87O12mXzNkHx7eemKq1TmuhtgikErhGxHi+GQHAw+apIwLnQ5PEC1SmiVsBU
lmm/V5XW9HFi5v0+prRQ08CuNVyg+D5P7wNcz4ALbTeJkUJArmf7SppIYkDbZdgGz8FNo2rn
W9fLHvEPf5fIli82n3p7S56XabATSnStQ75HtxkaomwSwRwIom8N/jl5ccUtPK/u+l/BhESk
W98p8EuCk8hjpCw5mw9rxjyEF4Hn1PmgeJjcH6/J+P8Z4CLF/LmDe7FJ6lmm/6hDue1fuHxI
lv2OmZD+TB/9tEV+7l/MS804qP5riycSV6FMQWzo2PECRXuY3+upTm7E51fPhGQ1L5K9Mq9M
JVvz/hGuizUbVdyK0rONp5vzc3V0QGC9KCo=


xZvPAuwiLo5K9ivjesACZP77BXUNa50bLaz5tfeWtTnThQQ0IFp1fIZ3t2GHrgwf/Ed+zY/t
+Gk6XH996sxnHJBdi/+jzWN4ZXlDCLDjQAXV8LJdXRcNMVLlQesdj+ao1vEdUUZAZwWVktGn
vypwmbB3Bv94h8SaClHaVsAzQTGIRh7Jc/Y/Pb3hfskrNr+AgPRT562ajvGxBfu/2gP1qLQ/
VFXum4YOfmBjSt9R2Ebv9xgM8vfWH6S/AgERAoH/cYuWLoCuJmp4OfKSarLIczM7pQ7kMaim
2yfAGG9KSULfJwmtUfpu9FMF68XcjpZl/OJ6PWCFkovYasC3B9Jbwd//q3sG40lmFv5adXHH
KsSxcoKTbOUMqmtb+skBq1YiD59HzEBgjkgjCNGEuQ3j1o/Bzpthlci90RUNavkxUeqaAAM9
DADEJH65Blj8hkCE8RWVD+ym7dCcTo7BMeCtUJPw0vdSZNf367Opt1W7dulaP5BtuA70yR3o
FgNz6g+ggJjXKfEksh6CV6LBZt5UWQ3RM+A5jlvMSVSXsfWPlJcbVmoE4iF6I6tQYUqu/7NH
JmbTEvEn5tE6XVJH/5N5AoGBALnZ91P56qxvJwuVWfdP3PkZMhHkyyQdS9ThHggqckgB55/+
qldshS4iK/NrbTFYnl5yaw0IFFPlj1CEM5C10ShBOTmQ2s5Bc7xJkgGFeAmNO9cGOjryjMNp
5dV1isOIeEDeHs322l455VdGrdfMPi3konHgjz2d7nol1K2tR1dLAoGBAMVV72JnDOx0WRCb
cSWLJRhtqGPrXUsalqhFIPEq0JA2r6JEt4JHFUUswaOvqKi17AZXIOL5Sn23tvMqjdij53IW
```

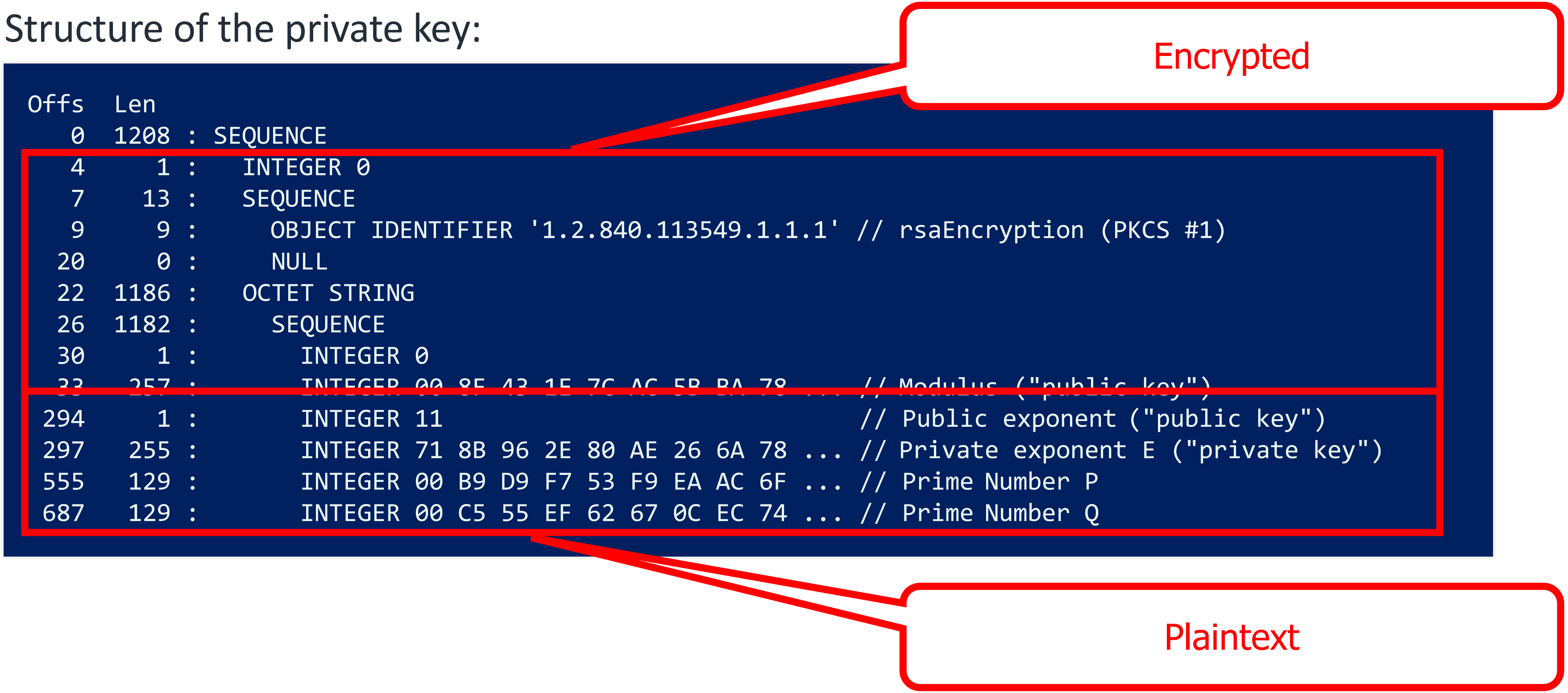
The first part is encrypted (512 bytes)

The second part is in plaintext

Gen

Key Storage: The Wrong Way #2

- Structure of the private key:

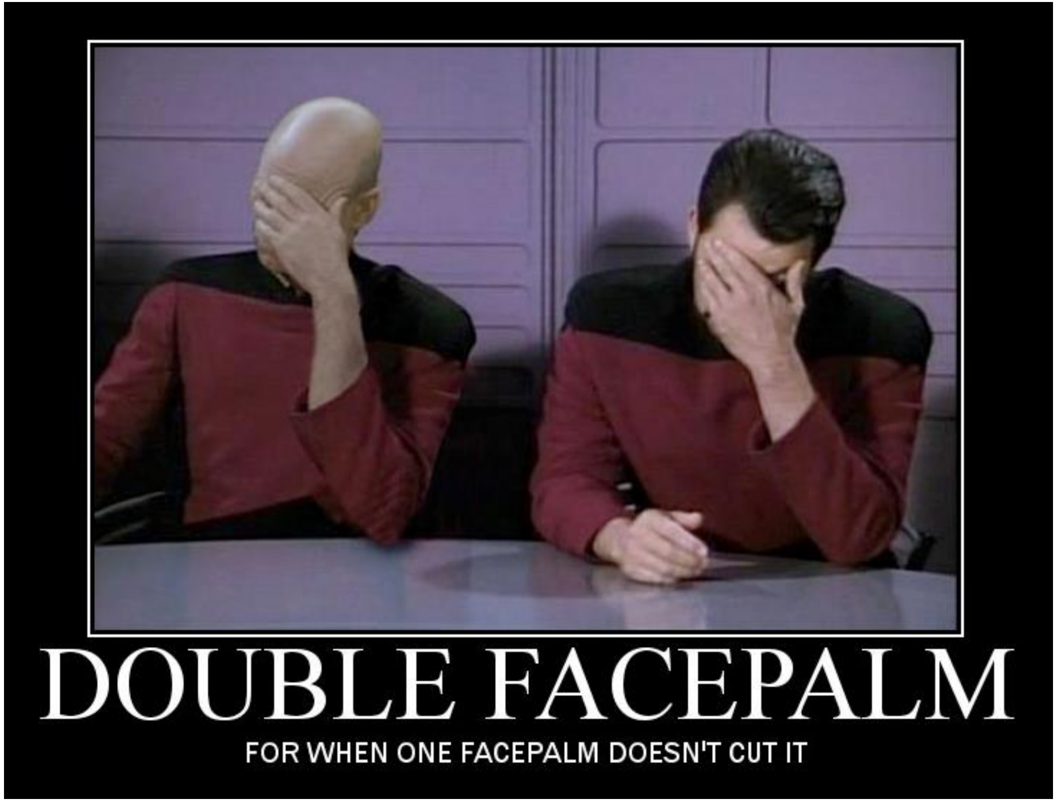


```
Offs  Len
   0  1208 : SEQUENCE
   4     1 :   INTEGER 0
   7    13 :   SEQUENCE
   9     9 :     OBJECT IDENTIFIER '1.2.840.113549.1.1.1' // rsaEncryption (PKCS #1)
  20     0 :     NULL
  22  1186 :   OCTET STRING
  26  1182 :     SEQUENCE
  30     1 :       INTEGER 0
  33   257 :       INTEGER 00 8F 43 1E 7C AC 5B BA 78 ... // Modulus ("public key")
 294     1 :       INTEGER 11                            // Public exponent ("public key")
 297   255 :       INTEGER 71 8B 96 2E 80 AE 26 6A 78 ... // Private exponent E ("private key")
 555   129 :       INTEGER 00 B9 D9 F7 53 F9 EA AC 6F ... // Prime Number P
 687   129 :       INTEGER 00 C5 55 EF 62 67 0C EC 74 ... // Prime Number Q
```

Encrypted

Plaintext

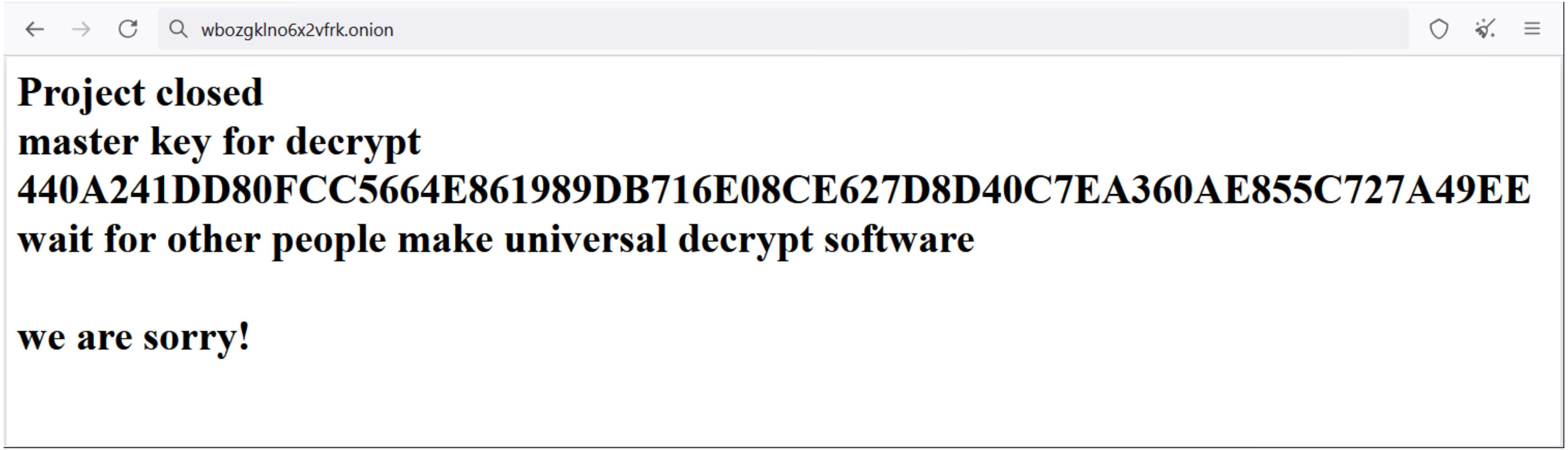
Key Storage: The Wrong Way #2



#4
Protect Backend Infrastructure

Protect Backend Infrastructure

- Published / leaked encryption keys
- Example: Shutdown of the TeslaCrypt ransomware (May 2016)

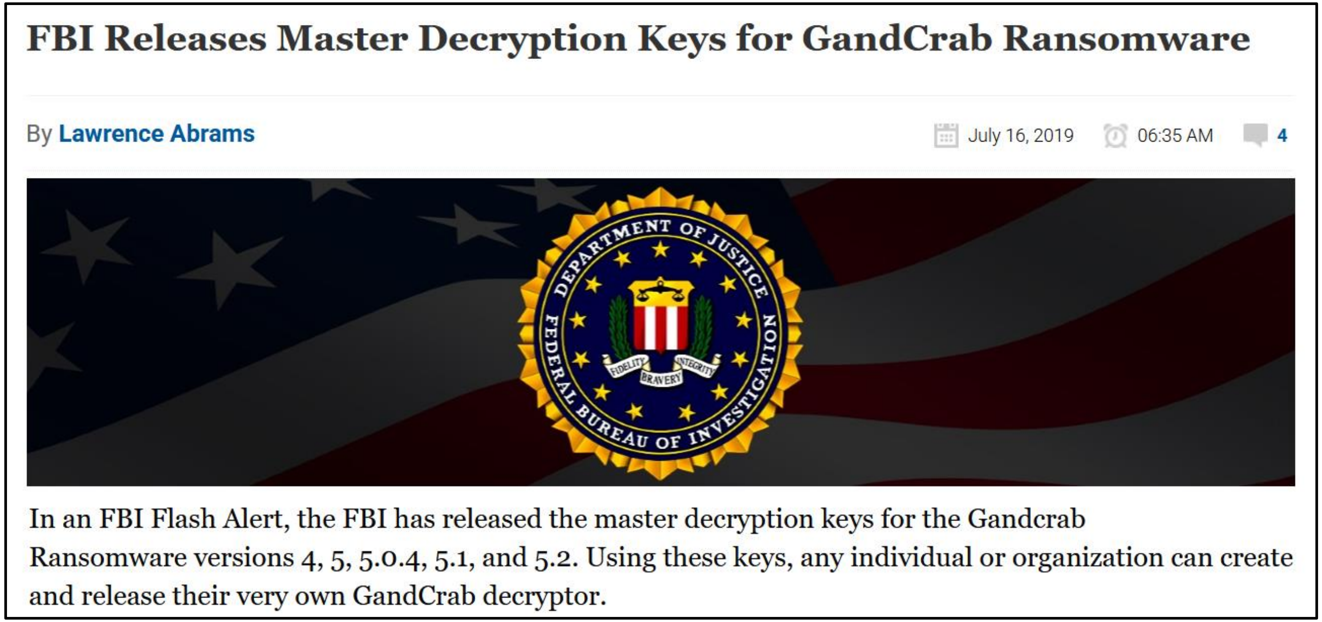


Project closed
master key for decrypt
440A241DD80FCC5664E861989DB716E08CE627D8D40C7EA360AE855C727A49EE
wait for other people make universal decrypt software

we are sorry!

Protect Backend Infrastructure

- Example: Bitdefender’s breach of the GandCrab servers (2019)



FBI Releases Master Decryption Keys for GandCrab Ransomware

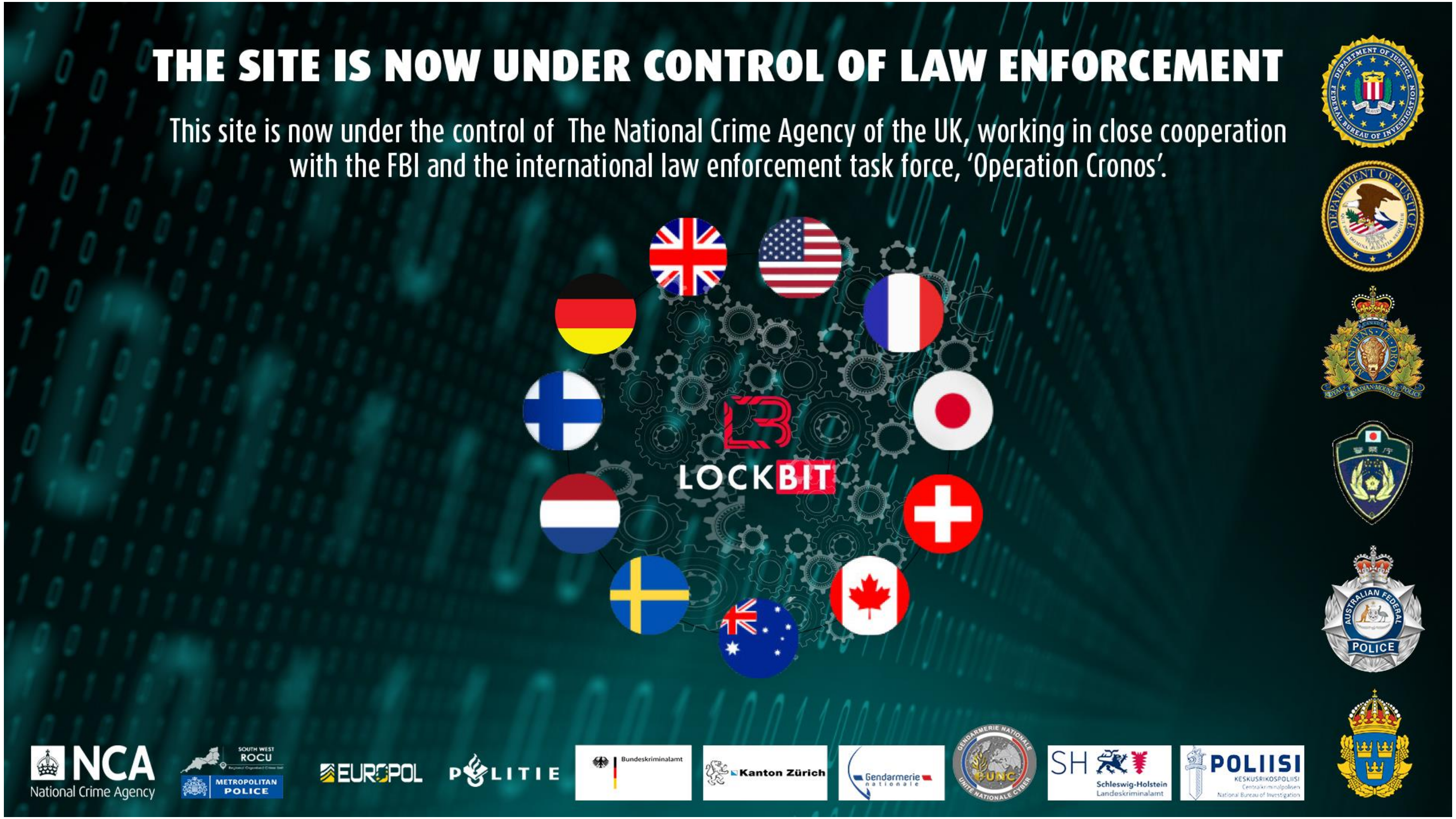
By **Lawrence Abrams** July 16, 2019 06:35 AM 4

In an FBI Flash Alert, the FBI has released the master decryption keys for the Gandcrab Ransomware versions 4, 5, 5.0.4, 5.1, and 5.2. Using these keys, any individual or organization can create and release their very own GandCrab decryptor.

Protect Backend Infrastructure

- Example: LockBit’s leak site hacked by joint operation of LE from 11 countries
- Exploited a PHP vulnerability (CVE-2023-3824)

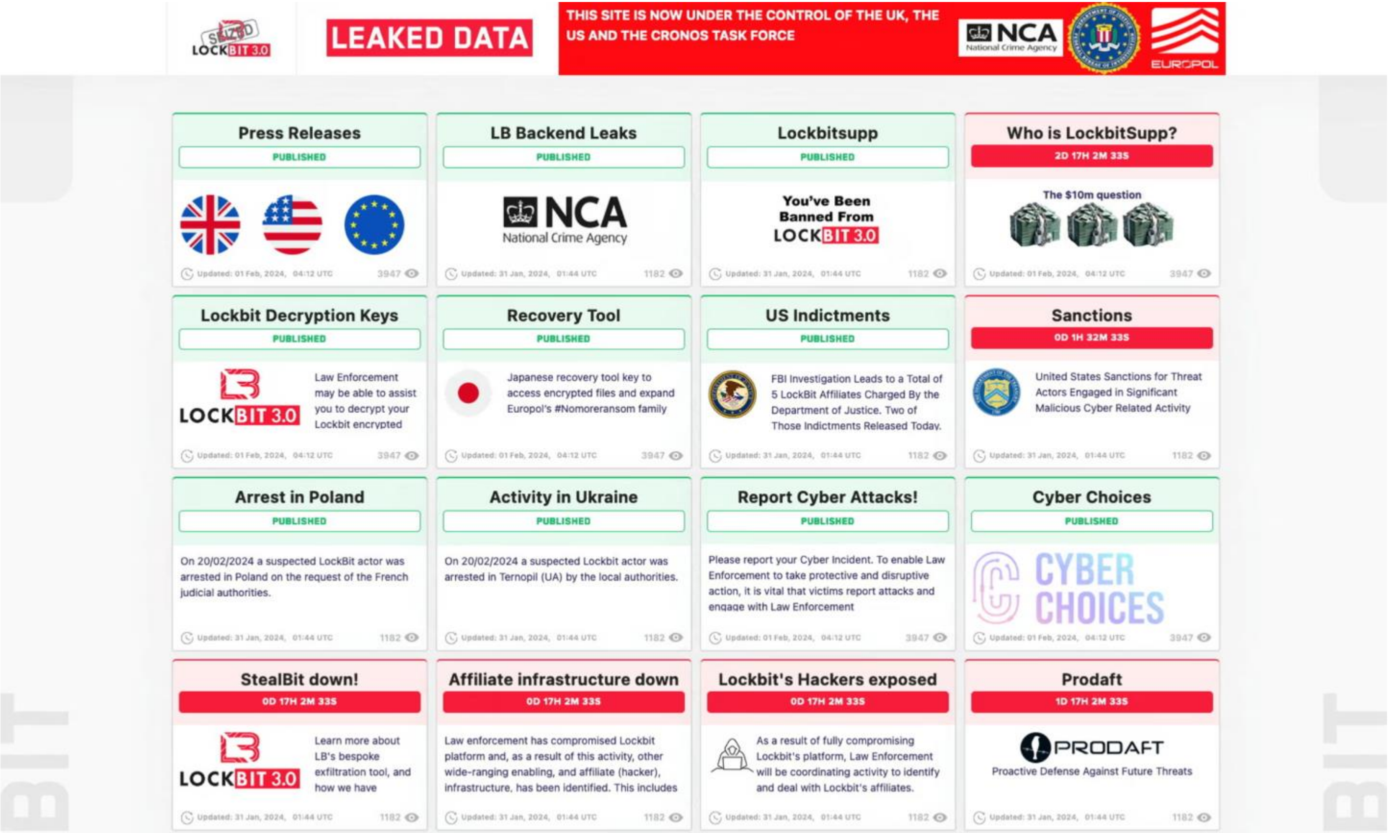
Protect Backend Infrastructure



THE SITE IS NOW UNDER CONTROL OF LAW ENFORCEMENT

This site is now under the control of The National Crime Agency of the UK, working in close cooperation with the FBI and the international law enforcement task force, 'Operation Cronos'.

Protect Backend Infrastructure



SEIZED LOCKBIT 3.0

LEAKED DATA

THIS SITE IS NOW UNDER THE CONTROL OF THE UK, THE US AND THE CRONOS TASK FORCE

NCA National Crime Agency

EUROPOL

Press Releases
PUBLISHED
Updated: 01 Feb, 2024, 04:12 UTC 3947

LB Backend Leaks
PUBLISHED
NCA National Crime Agency
Updated: 31 Jan, 2024, 01:44 UTC 1182

Lockbitsupp
PUBLISHED
You've Been Banned From LOCKBIT 3.0
Updated: 31 Jan, 2024, 01:44 UTC 1182

Who is LockbitSupp?
2D 17H 2M 33S
The $10m question
Updated: 01 Feb, 2024, 04:12 UTC 3947

Lockbit Decryption Keys
PUBLISHED
LOCKBIT 3.0
Law Enforcement may be able to assist you to decrypt your Lockbit encrypted
Updated: 01 Feb, 2024, 04:12 UTC 3947

Recovery Tool
PUBLISHED
Japanese recovery tool key to access encrypted files and expand Europol's #Nomoreransom family
Updated: 01 Feb, 2024, 04:12 UTC 3947

US Indictments
PUBLISHED
FBI Investigation Leads to a Total of 5 LockBit Affiliates Charged By the Department of Justice. Two of Those Indictments Released Today.
Updated: 31 Jan, 2024, 01:44 UTC 1182

Sanctions
0D 1H 32M 33S
United States Sanctions for Threat Actors Engaged in Significant Malicious Cyber Related Activity
Updated: 31 Jan, 2024, 01:44 UTC 1182

Arrest in Poland
PUBLISHED
On 20/02/2024 a suspected LockBit actor was arrested in Poland on the request of the French judicial authorities.
Updated: 31 Jan, 2024, 01:44 UTC 1182

Activity in Ukraine
PUBLISHED
On 20/02/2024 a suspected Lockbit actor was arrested in Ternopil (UA) by the local authorities.
Updated: 31 Jan, 2024, 01:44 UTC 1182

Report Cyber Attacks!
PUBLISHED
Please report your Cyber Incident. To enable Law Enforcement to take protective and disruptive action, it is vital that victims report attacks and engage with Law Enforcement
Updated: 01 Feb, 2024, 04:12 UTC 3947

Cyber Choices
PUBLISHED
CYBER CHOICES
Updated: 01 Feb, 2024, 04:12 UTC 3947

StealBit down!
0D 17H 2M 33S
LOCKBIT 3.0
Learn more about LB's bespoke exfiltration tool, and how we have
Updated: 31 Jan, 2024, 01:44 UTC 1182

Affiliate infrastructure down
0D 17H 2M 33S
Law enforcement has compromised Lockbit platform and, as a result of this activity, other wide-ranging enabling, and affiliate (hacker), infrastructure, has been identified. This includes
Updated: 31 Jan, 2024, 01:44 UTC 1182

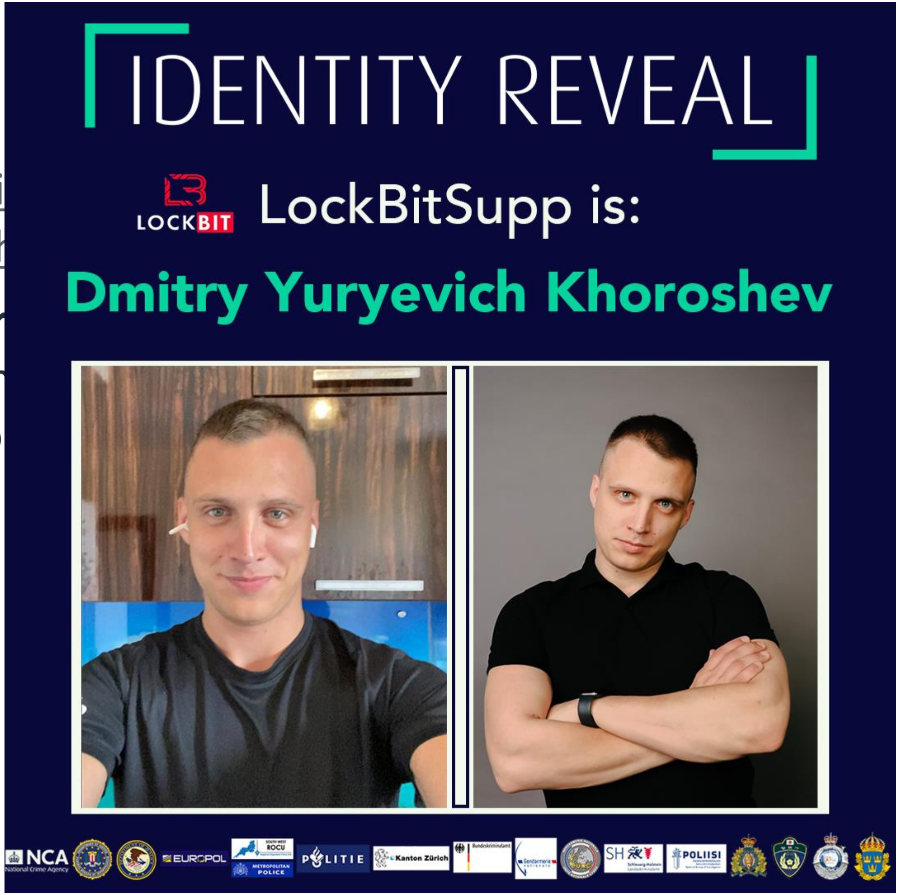
Lockbit's Hackers exposed
0D 17H 2M 33S
As a result of fully compromising Lockbit's platform, Law Enforcement will be coordinating activity to identify and deal with Lockbit's affiliates.
Updated: 31 Jan, 2024, 01:44 UTC 1182

Prodaft
1D 17H 2M 33S
PRODAFT
Proactive Defense Against Future Threats
Updated: 31 Jan, 2024, 01:44 UTC 1182

Gen

Protect Backend Infrastructure

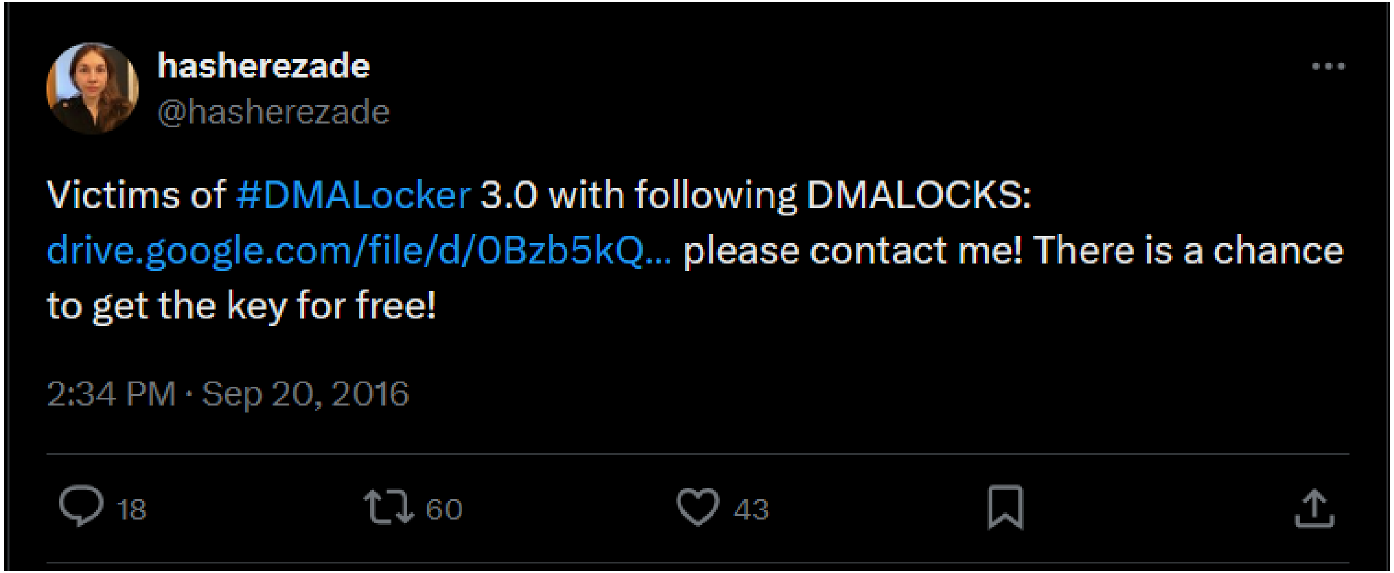
- LockBit’s main administrator deanonymized
- https://www.state.gov/transnational-organi
ransomware-administrator-dmitry-yuryevich
- “The U.S. Department of State is offering a r
information leading to the arrest and/or con
Khoroshev for participating in, conspiring to
in LockBit ransomware activities.”



#5
Decrypt After Payment

Decrypt After Payment

- Threat actors provide decryptors for victims who paid the ransom
- Incorrect encryption schema may make a decryptor work for every victim
- Example: DMALocker ransomware



hasherezade
@hasherezade

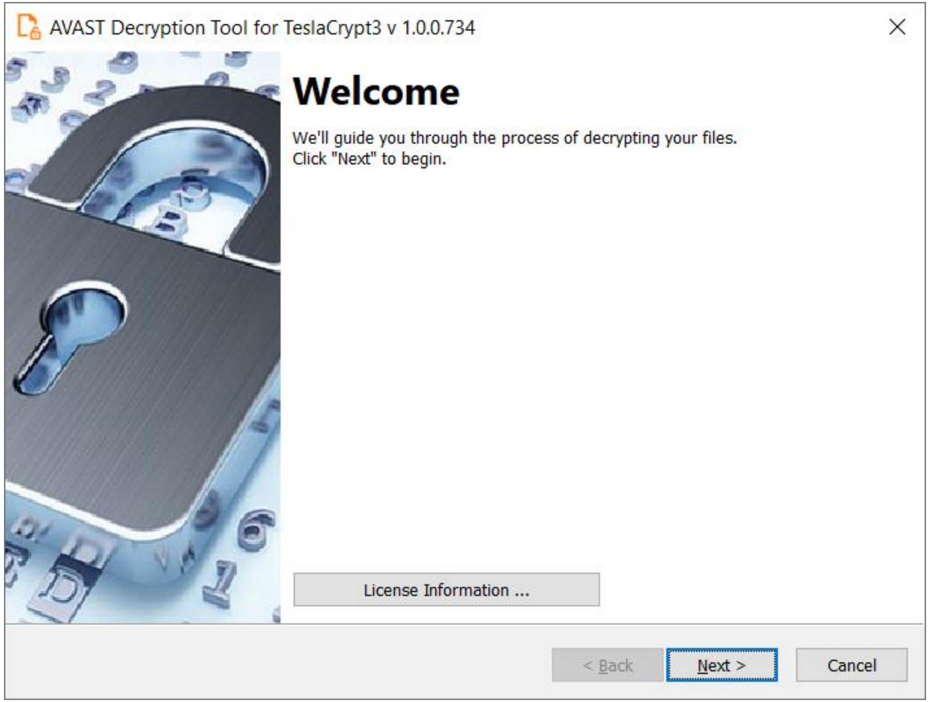
Victims of #DMALocker 3.0 with following DMALOCKS: drive.google.com/file/d/0Bzb5kQ... please contact me! There is a chance to get the key for free!

2:34 PM · Sep 20, 2016

They Failed! What’s next?

Avast Free Ransomware Decryptors

- The last resort of ransomware protection
- Free recovery of already encrypted files
- We're an associate partner of NO MORE RANSOM!
- https://www.nomoreransom.org



AVAST Decryption Tool for TeslaCrypt3 v 1.0.0.734

Welcome

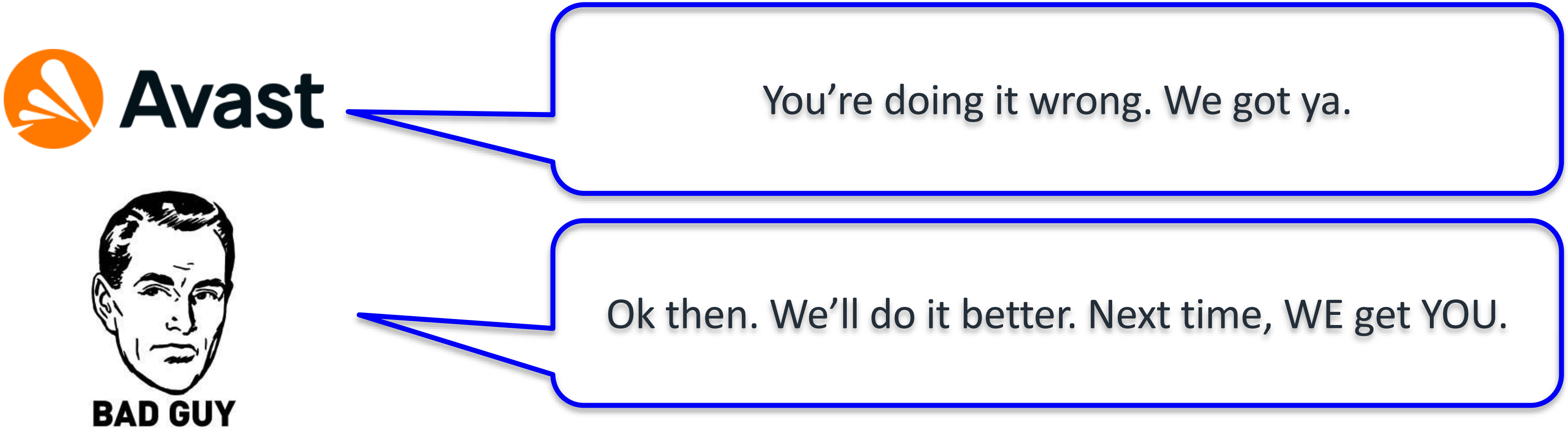
We'll guide you through the process of decrypting your files.
Click "Next" to begin.

The (Not So Good) News

NO
BR ING NEWS
ANSOMWAR DEAD
13:27
AVG TECHNOLOGIES CAN DECRYPT 6 MOST PREVALENT RANSOMWARE FAMILIES

The (Not So Good) News

- It would be cool if it was always possible. But it isn't. Often.
- Moreover, by releasing a decryptor, we also deliver a message to the bad guys

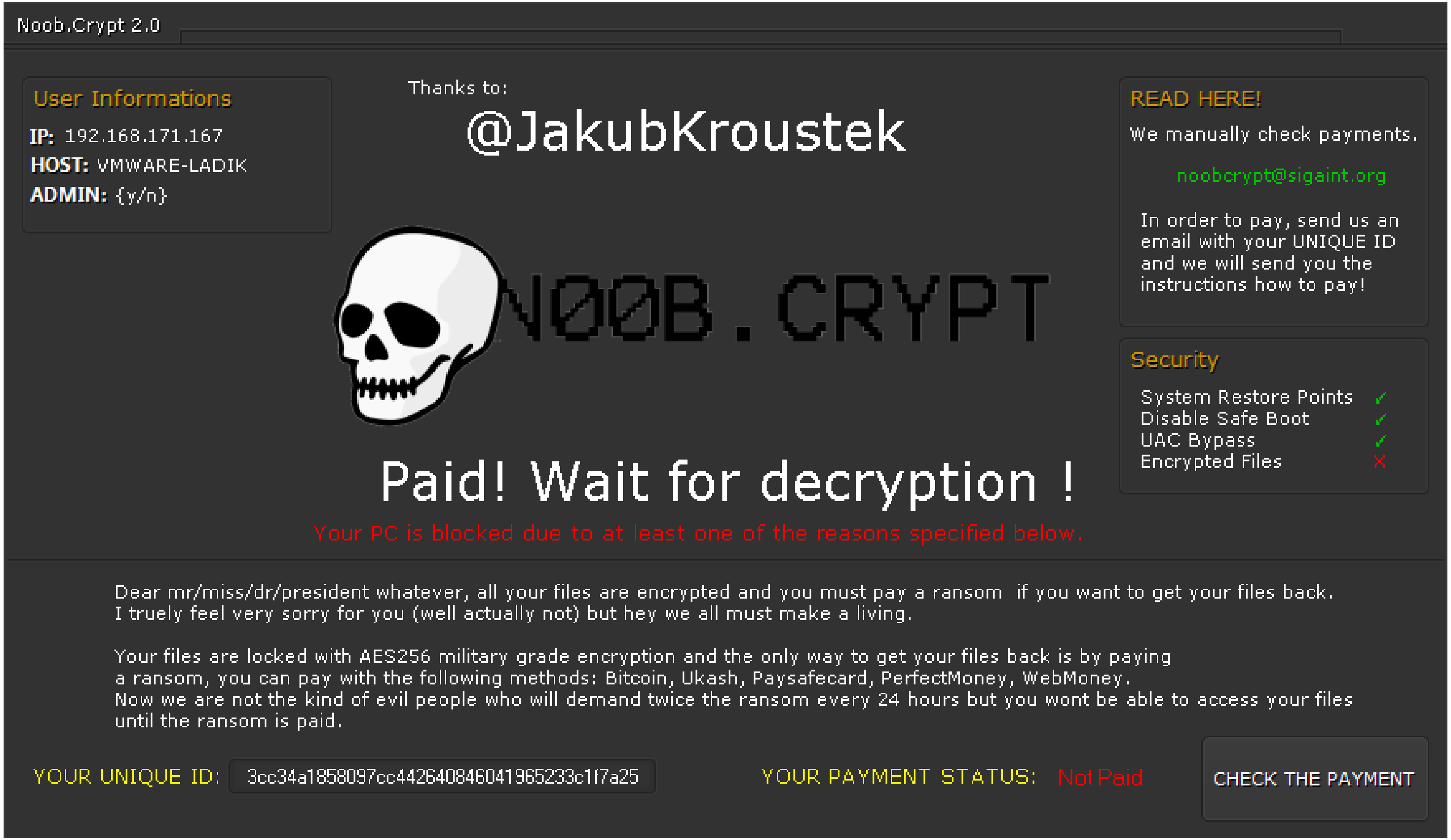


You're doing it wrong. We got ya.

Ok then. We'll do it better. Next time, WE get YOU.

The Happy ~~Sad~~ ~~Funny~~ Story of the Bart Ransomware

- Jun 21, 2016: Discovered
- Jul 19, 2016: “Bart’s Shenanigans Are No Match for AVG“
  - http://now.avg.com/barts-shenanigans-are-no-match-for-avg/
- Aug 22, 2016: A new version of Bart emerged, based on Diffie-Hellman encryption
- Apr 4, 2017: Bitdefender creates decryption tool for Bart ransomware



User Informations

IP: 192.168.171.167
HOST: VMWARE-LADIK
ADMIN: {y/n}

Thanks to:
@JakubKroustek

Paid! Wait for decryption !

Your PC is blocked due to at least one of the reasons specified below.

READ HERE!

We manually check payments.

noobcrypt@sigaint.org

In order to pay, send us an email with your UNIQUE ID and we will send you the instructions how to pay!

Security

System Restore Points ✓
Disable Safe Boot ✓
UAC Bypass ✓
Encrypted Files ✗

Dear mr/miss/dr/president whatever, all your files are encrypted and you must pay a ransom if you want to get your files back.
I truely feel very sorry for you (well actually not) but hey we all must make a living.

Your files are locked with AES256 military grade encryption and the only way to get your files back is by paying a ransom, you can pay with the following methods: Bitcoin, Ukash, Paysafecard, PerfectMoney, WebMoney.
Now we are not the kind of evil people who will demand twice the ransom every 24 hours but you wont be able to access your files until the ransom is paid.

YOUR UNIQUE ID: 3cc34a1858097cc442640846041965233c1f7a25

YOUR PAYMENT STATUS: Not Paid

2024 Ransomware Trends

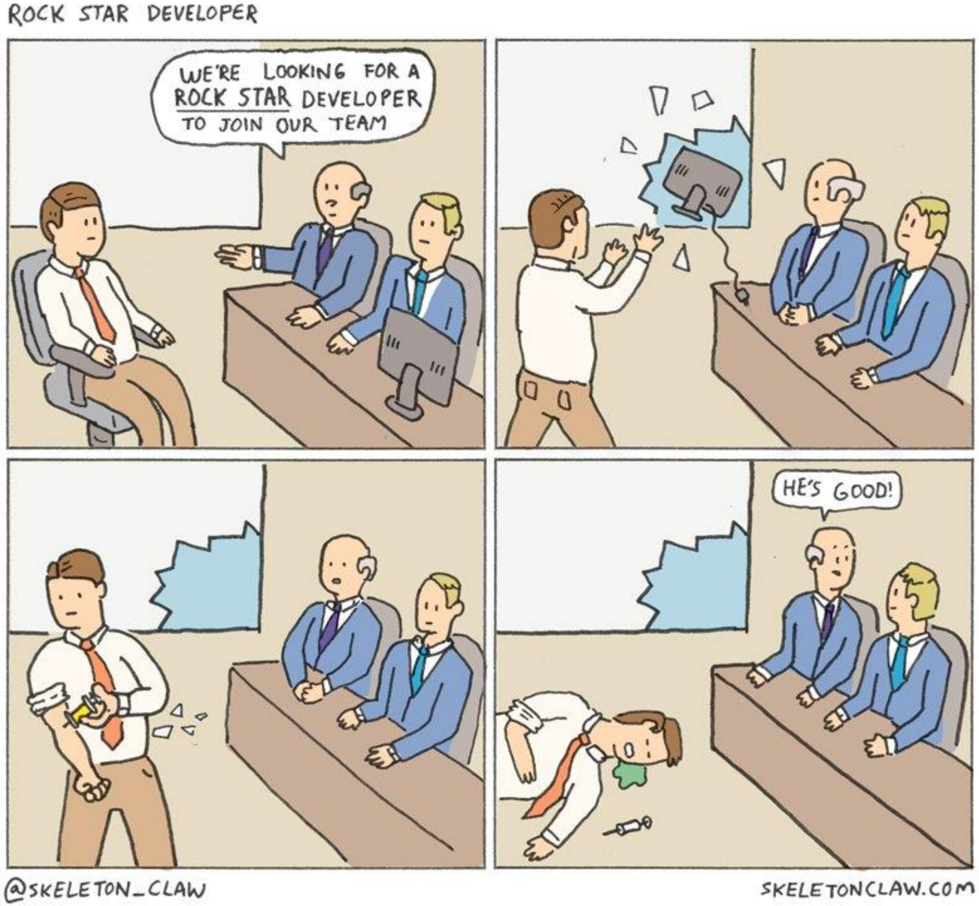
- Different attacks based on the target
  - Warez/Discord for consumer
  - RDP/Samba/phishing for SMB
  - **Targeted attacks for Enterprise**
- Multi-extorsion schema (decryption, doxing, network access, etc.)
- File corruption instead of encryption or partial encryption
- Encryption of ESXI servers (Linux)
- Malware-less attacks

Conclusions

- Malware is a regular business now
- Don’t trust the criminals
- Don’t pay the ransom
- Malware analysis is fun but challenging
- Creating a solid encryption system is not that easy

Student Theses at GEN

- Long history of cooperation
- So far, so good ☺



Gen

Student Theses at GEN

- Developing systems for malware classification (internal and open-source tools)
- Detection of anomalies, threats and campaigns
- Reverse engineering (an existing experience is required)
- Malware analysis of novel threats (HTML/JS, browser-specific, etc.)
- … and more
- Programming languages: C/C++, Python, Rust
- For more information, follow VUT IS or contact us
  - E-Mail: iregeciova@fit.vutbr.cz
  - Discord: iregeciova

Further reading:

- P. Szor: The Art of Computer Virus Research and Defense, 2005
- M. Sikorski, A. Honig: Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software, 2012
- J. P. Aumasson: Serious Cryptography: A Practical Introduction to Modern Encryption, 2017

jakub.kroustek[at]gen.com
https://twitter.com/JakubKroustek

ladislav.zezula[at]gen.com
https://twitter.com/LadislavZezula