Ransomware: Past, present, future

Ralf Benzmüller, G DATA CyberDefense AG

Mindshare 2023
September 19th/20th

G DATA CyberDefense
EVIDEN an atos business

Agenda

1 History and evolution of ransomware

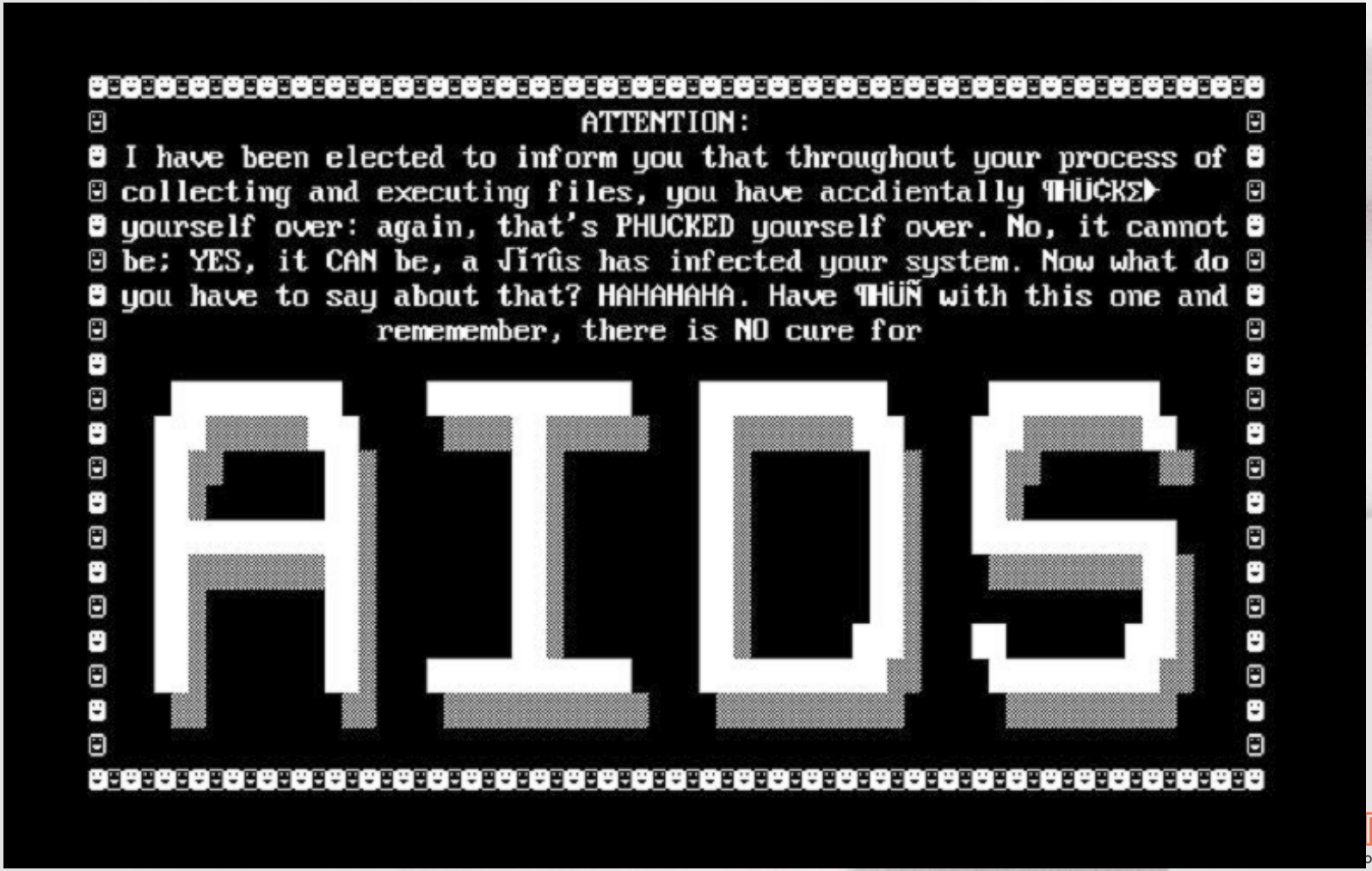
2 Ransomware today

3 Decryption tools: Crypto fails and failures

4 What the future brings

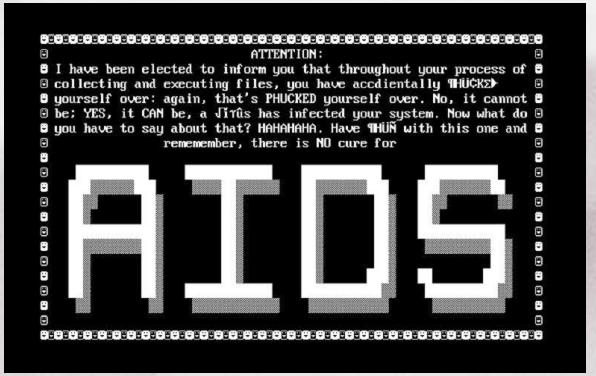
History and evolution of ransomware


Ransomware
$
Shift



AIDS Trojan

First Ransomware 1989



- 1989 PC Cyborg Corporation, Joseph L. Popp
- Disk with AIDS information distributed 20.000 copies on WHO conference.
- Starts encrypting all files on disk after 90 reboots
- Asks $189 ransom
  Send to a postbox in Panama
- Displays a EULA

Ransomware GPCoder

2005: First modern crypto malware

- Encrypts files with certain file extensions
- Makes itself persistent
- Deletes itself after work is done
- Ransom note as text file („ATTENTION!!!.txt“)
- Payment details negotiated per email
- Encryption improves over time

.asc
.db
.db1
.db2
.dbf
.doc
.htm
.html
.jpg
.pgp
.rar
.rtf
.txt
.xls
.zip

Ransomware: GPCoder evolution

Learning curve crypto implementation

2006

- 4-bit key
- Safed in Registry
- One key for all

2007

- Applies symmetric standard procedures like 3DES and AES

2008

- Encryption of files with RC4
- RC4-keys are encrypted with RSA-1024 Public Key
- Original keys are deleted

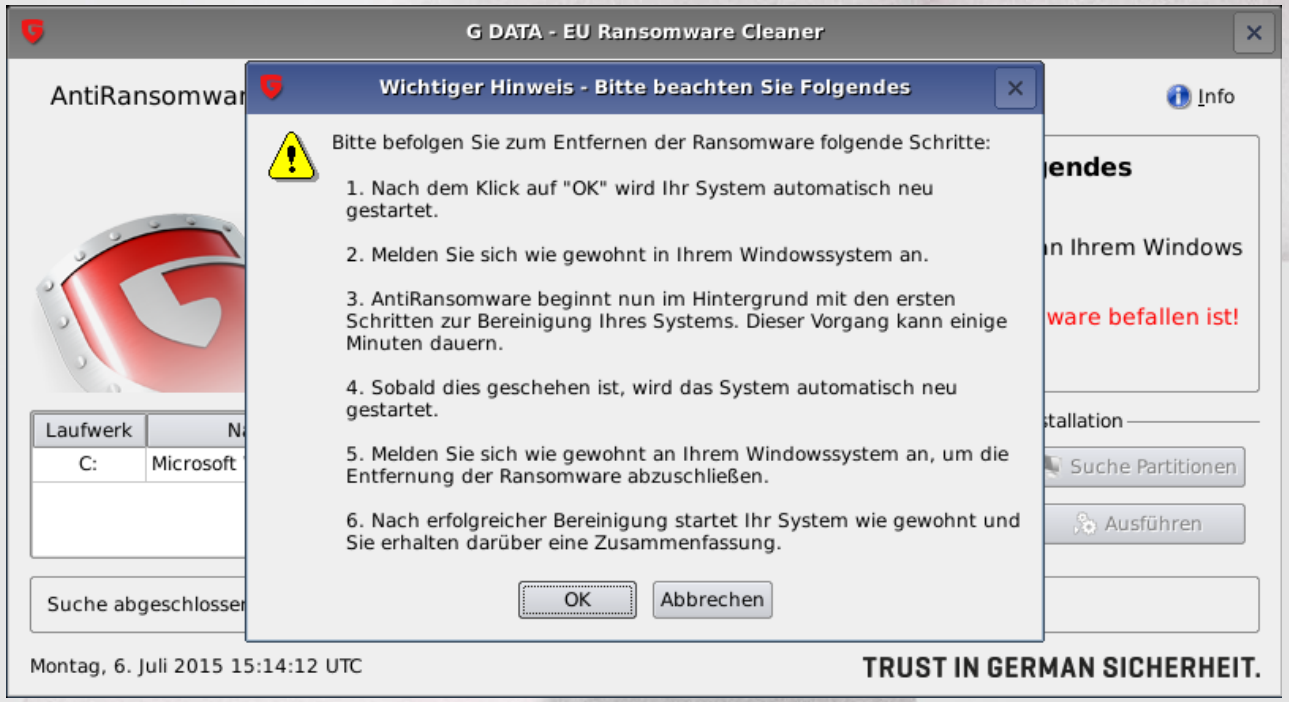
Ransomware: System locker

G DATA CyberDefense

EVIDEN an atos business

Circumventing System blockers

- Sometimes: Safe Mode
- Clean Boot

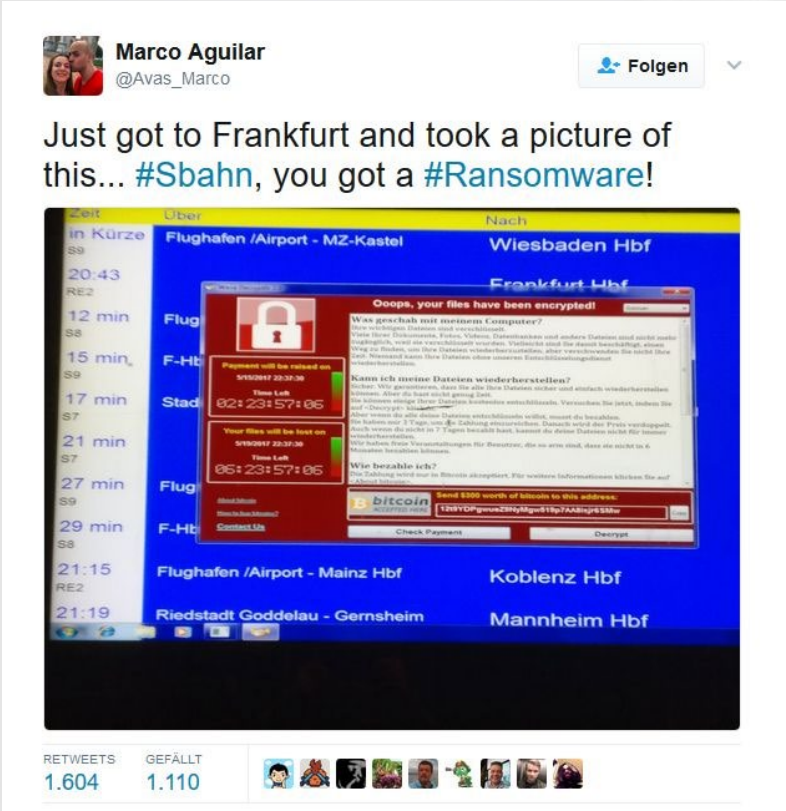


Ransomware: Cryptolocker

G DATA CyberDefense

EVIDEN an atos business

Ransomware: WannaCry May, 12th 2017



G DATA CyberDefense

EVIDEN an atos business

Ransomware WannaCry is a wiper

- Ca. 500K infections worldwide, mostly organizations
- Mass distribution (worm) based on „EternalBlue“
- Exploiting SMB interface on Windows
- Originally in use by „Equation Group“ (USA)
- Leaked by „Shadow Brokers“ (Hacktivists) 04/2017
- Cashout „error“: No victim-specific Bitcoin addresses
- Victims cannot be decrypted individually
- „Kill switch“ domain stops spreading

Chimera threatens to publish data if you don‘t pay

Ransomware evolution in the early years

< 2014	2014	2015		2016	
AIDS Trojan	Linkup	ThreatFinder	Encryptor RaaS	Ransom32	Manamecrypt
Saddam Hussein	Cryptowall	*TeslaCrypt*	CryptoApp	Locky	Jigsaw
…	CryptoDefense	Cryptolocker2015	*HiddenTear*	CryptoJoker	AutoLocky
Gpcoder	*CTB-Locker/ Citroni*	CryptVault	ORX-Locker	Magic	8lock8
CryZip	TorrentLocker	Pacman	Fonco	Cerber	Brazilian
Archiveus	*Synolocker*	Pclock	CryptInfinite	UmbreCrypt	Bucbi
Reveton	ZeroLocker	VaultCrypt	Unix.Ransomcrypt	NanoLocker	Crybola
Urausy	CoinVault	CryptoFortress	Linux.Encoder	Vipasana	Crypren
Kovter	CryptoGraphicLocker	ToxCrypt	Mabouia	Virus Encoder	CryptoHost
Nymaim	Cryakl	Crypt0L0cker	Ungluk	Xorist	CryptoMix
Harasom	BandarChor	Locker	Power Worm	LeChiffre	CryptXXX
CryptoLocker	Isda	Troldesh	Radamant	7ev3n	Fury
Browlock	KeyBTC	BitCryptor	DMA-Locker	Hi Buddy	GhostCrypt
	KeyHolder		Gomasom	Samsam	GNL Locker
	VirLock		XRTN	PayCrypt	iLock
			Chimera	JobCryptor	KryptoLocker
				Magic	Lortok
				PadCrypt	Mischa
				Petya	Rector
				Coverton	Scraper
				KimcilWare	Shujin
				Nemucod	Skidlocker
				Maktub	BadBlock
				Rokku	Zcryptor
				CryptoHasYou	BlackShades
				Ginx	ODCODC
				KeRanger	…uvm

Ransomware evolution 2016

2016

777
7ev3n
7h9r
8lock8
ACCDFISA
Alcatraz
Alpha
Alma
AMBA
AngryDuck
Apocalypse
ApocalypseVM
ASN1
AutoLocky
AxCrypter
BadBlock
BaksoCrypt
Bandarchor
Bart
BitCrypt
BitCryptor
BitMessage
BitStak
Black Shades
Blocatto
Booyah
Brazilian
Bucbi
Cerber
CoinLocker
Coverton
Crybola
CryFile
CrypMic
Crypren
Crypt38
Cryptear
CryptFile2
CryptoBit
CryptoDefense
CryptoFinancial
CryptoHasYou
CryptoHitman
CryptoHost
CryptoJoker
CryptoMix
CryptorBit
CryptoRoger
CryptoShocker
CryptoWire
CryptXXX
CryPy
CrySiS
CTB-Faker
Cute
Deadly
DEDCryptor
DirtyDecrypt
DetoxCrypto
DMALocker
Domino
ECLR
EduCrypt
El-PoLocker
Enigma
Exotic
Fairware
Fantom
Fonco
FSociety
Fury
GhostCrypt
Ginx
Globe
GNL Locker
HDDCrypter
Herbst
Hi Buddy
Hitler
HolyCrypt
Hucky
HydraCrypt
iLock
iLockLight
Jager
Jeiphoos
Jigsaw
JobCryptor
JuicyLemon
KeRanger
KillerLocker
KimcilWare
Kostya
Kozy.Jozy
KratosCrypt
Kriptovor
KryptoLocker
LeChiffre
Locky
Lortok
Magic
Maktub
Manamecrypt
MasterBuster
MirCop
Mischa
MM Locker
Mobef
n1n1n1
NanoLocker
NegozI
Nemucod
NoobCrypt
ODCODC
Offline
OMG!Ransomcrypt
Onyx
PadCrypt
PayCrypt
PayForNature
Petya
Philadelphia
PizzaCrypts
Powerware
PowerLocky
PRISM
R980
RAA Encryptor
Razy
Rector
RektLocker
RemindMe
Rokku
Samsam
Sanction
Satana
Scraper
SecureCryptor
Shujin
Simple_Encoder
Skidlocker
Smrss32
SNSLocker
Sport
Stampado
Strictor
SuperCrypt
Surprise
Survey
SZFLocker
TowerWeb
ToxCrypt
TrueCrypter
UCCU
UmbreCrypt
Unlock92
Uyari
VaultCrypt
Venis
VenusLocker
Vipasana
Virus Encoder
WildFire Locker
Winnix Cryptor
WinRarer
WonderCrypter
Xorist
Xort
zCrypt
Zcryptor
ZimbraCryptor
Zyklon

2016> 200
Total: 491

Some serious ransomware threat actors

- Maze
- SamSam (Atlanta)
- Robin Hood (Baltimore)
- Darkside (Colonial Pipeline, ceased business)
  => Darkside 2 => BlackMatter (stopped Nov 21) => BlackCat
- GandCrab => REvil / Sodinokibi (stopped business)
- Conti (Conti leaks show connections to FSB)
- Lockbit
- Clop (arrested)
- Egregor (arrested in Feb 2021, former Maze?)
- Emotet /Ryuk (Shutdown Oct 2020)
- Doppelpaymer => Grief

5 types of ransomware

- Lockers: block system access
- Scareware force users to install (fake) software
- Crypter encrypts data
- Wiper destroys data
- Leakware steals data and threatens to publish it

Ransomware today

Ransomware is here to stay

- It‘s in the news – daily
- Big game hunting
- Sophisticated attacks (supply chain, zero-day exploits)
- High damages
  - Ransom
  - Production outage for weeks or months
  - Reputation
- Amount of ransom adapted to victim
- Vivid cybercrime ecosystem

Ransomware as a Service – payment models

- RaaS = extortion services for beginners
- Share of the ransom
- Rent the infrastructure
- Sell the infrastructure

- Crypto currencies: Bitcoin, Monero
- Service orientation

Decryption tools: Crypto fails and failures

How to get your data back without a backup?

Decryption tools

- Which family
  - ID Ransomware identifies 1118 ransomware families (https://id-ransomware.malwarehunterteam.com/)

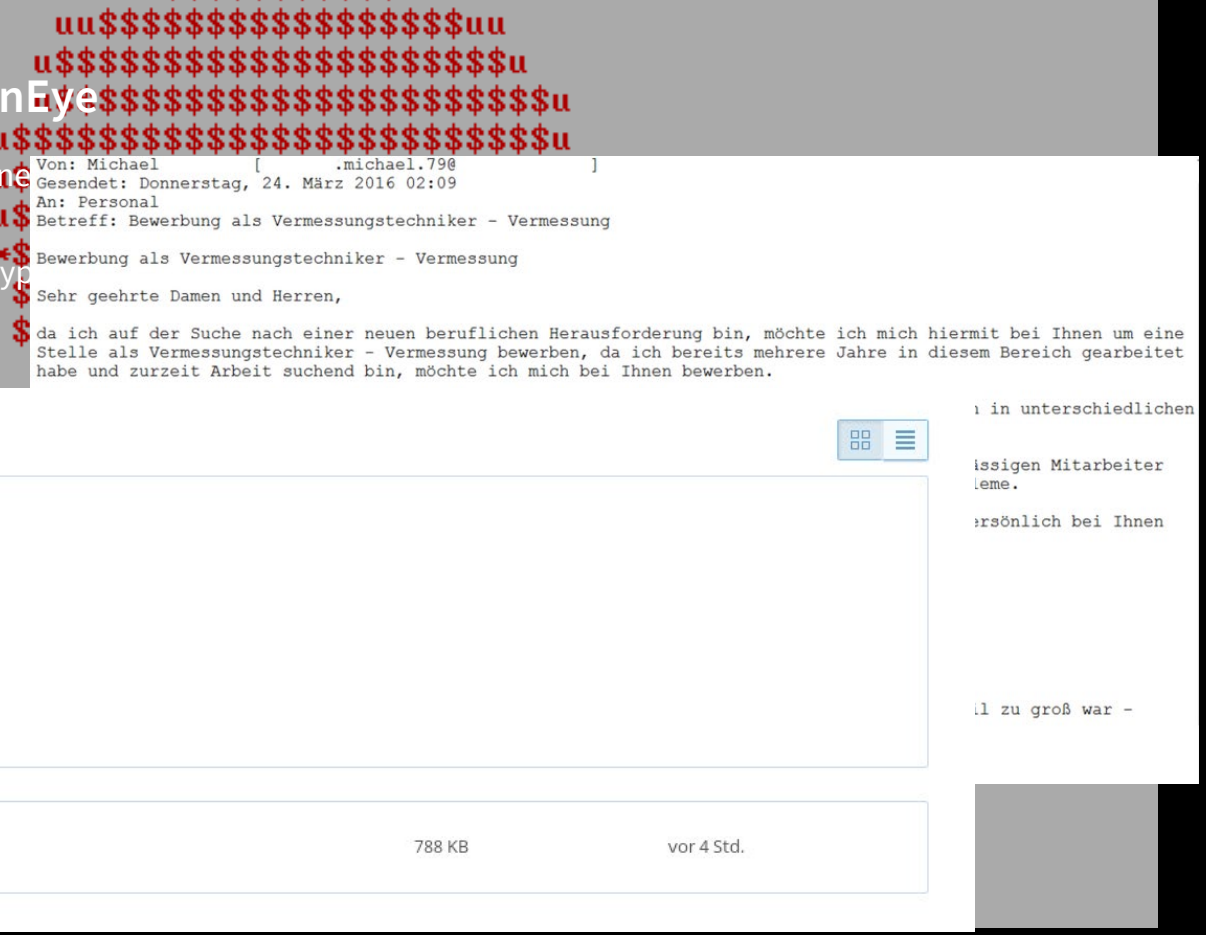
- Decryption tools
  - **No more ransom** has 173 decryptors (https://www.nomoreransom.org/)
  - Heimdal (https://heimdalsecurity.com/blog/ransomware-decryption-tools/)
  - Emsisoft
  - AV vendors

Unlocking data: Find the key and more

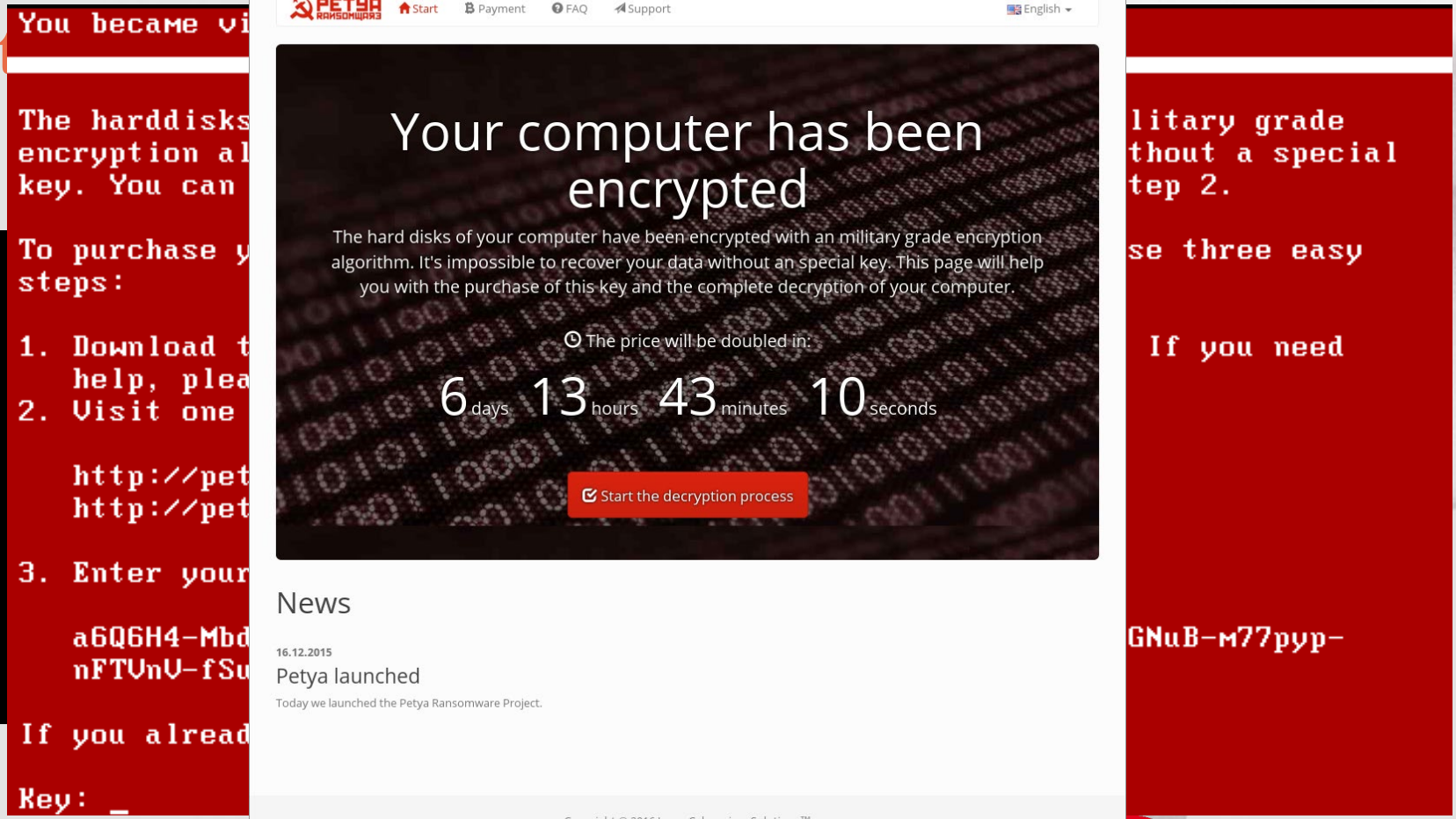
- Password in binary. Same password for all victims (Harasom)
- Static password somewhere in system or based on system info
  - E.g. ManameCrypt:
    SHA1Hash(Win32_processor.processorID + VolumeSerialNumber_Laufwerk_C
- Weak implementation in open source (e.g. Hidden Tear)
- Brute force (known file headers, AI, timestamps)
- Key is not deleted from memory (it‘s gone when you switch off)
- Key is transferred unencrypted => Logfiles, browser history
- Restore data from shadow copies or try data recovery tools
- Get decryptor tool from ransomware site without paying

Petya + Mischa = GoldenEye

- Distribution per spam campagne
- Target: Enterprises
- New: Overwrites MBR and encryp



Pe

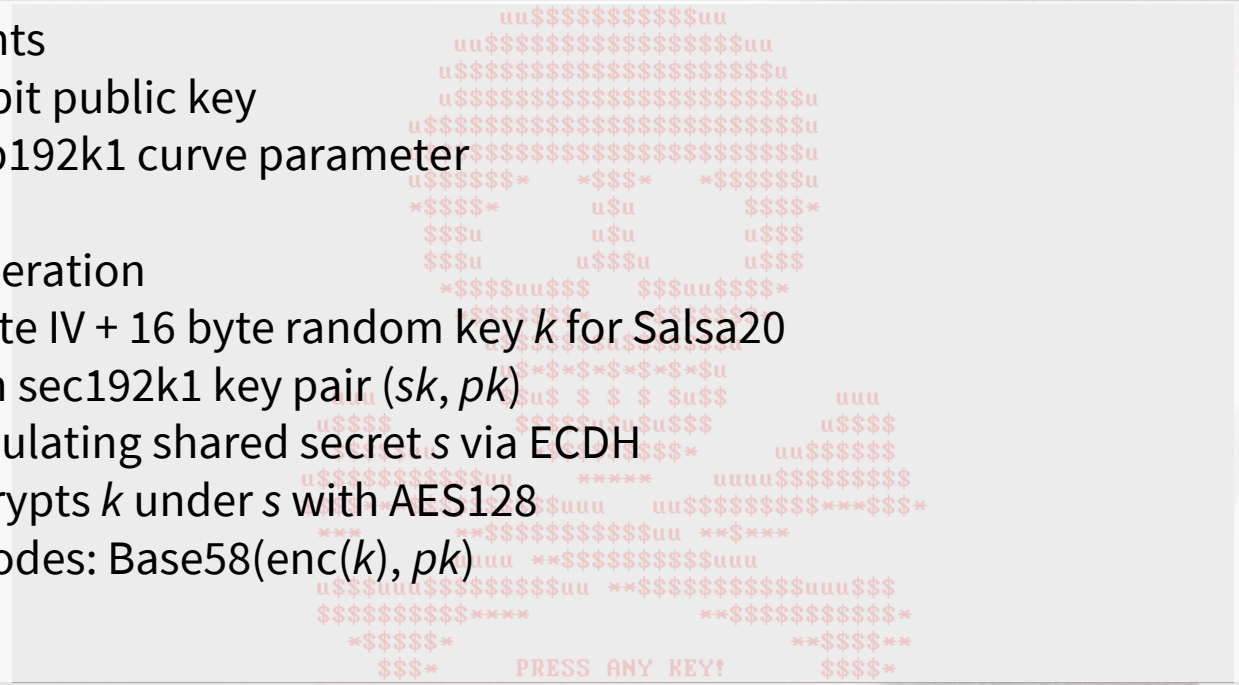


G DATA CyberDefense

EVIDEN an atos business

Petya encryption: Stage 1

- Constants
  - 192bit public key
  - secp192k1 curve parameter
- Key generation
  - 8 byte IV + 16 byte random key *k* for Salsa20
  - Own sec192k1 key pair (*sk*, *pk*)
  - Calculating shared secret *s* via ECDH
  - Encrypts *k* under *s* with AES128
  - Encodes: Base58(enc(*k*), *pk*)



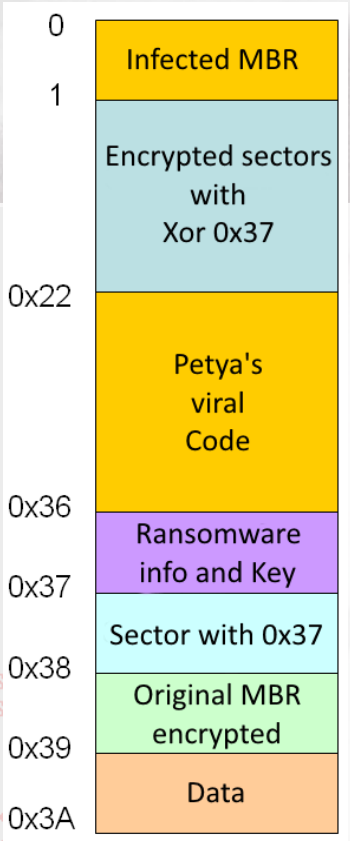
G DATA CyberDefense

EVIDEN an atos business

Petya encryption: Stage 1

- Manipulating the hard drive
  - MBR XOR 0x37
  - Sector(1..34) XOR 0x37
  - Writes own Bootloader
  - Writes Stage 2

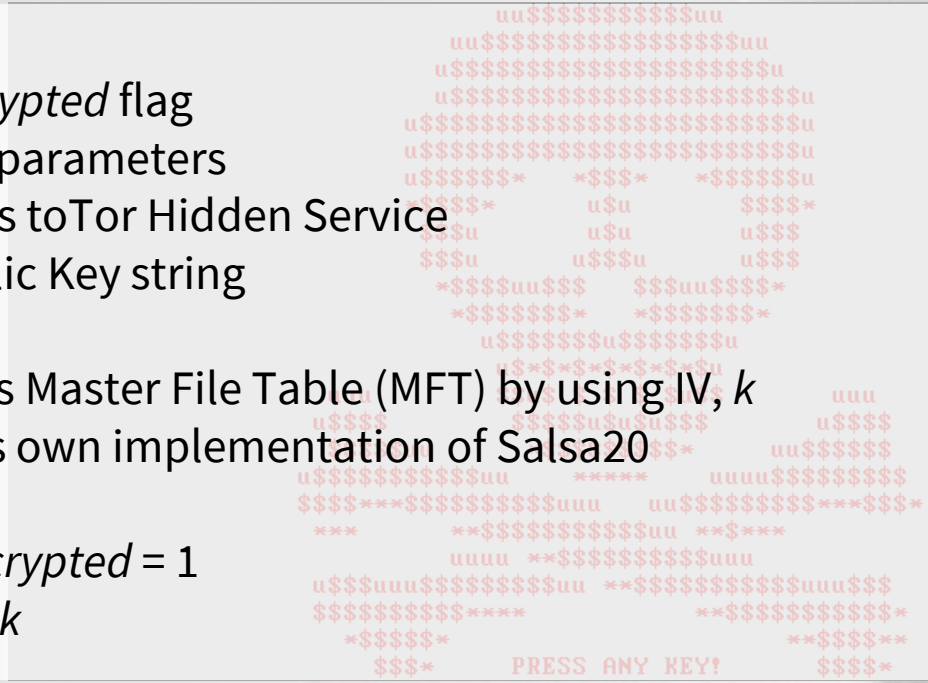
- Core data in Sector 54
  - *encrypted* flag (0|1|2)
  - Salsa20 IV + *k*
  - Links to Tor Hidden Serice
  - Public key string



Quelle: tgsoft.it

Petya encryption: Stage 2

- Reads
  - *encrypted* flag
  - Key parameters
  - Links toTor Hidden Service
  - Public Key string
- Encrypts Master File Table (MFT) by using IV, *k*
  - Uses own implementation of Salsa20
- Sets *encrypted* = 1
- Deletes *k*



Petya encryption: kinda Salsa20 16bit

Salsa20

- Stream index: uint64_t
- Function *rotate left*: uint32_t
  return (value << shift) | (value >>(32-shift));
- Hash function f. keystream output:
  split 64bit input in 2*32bit output

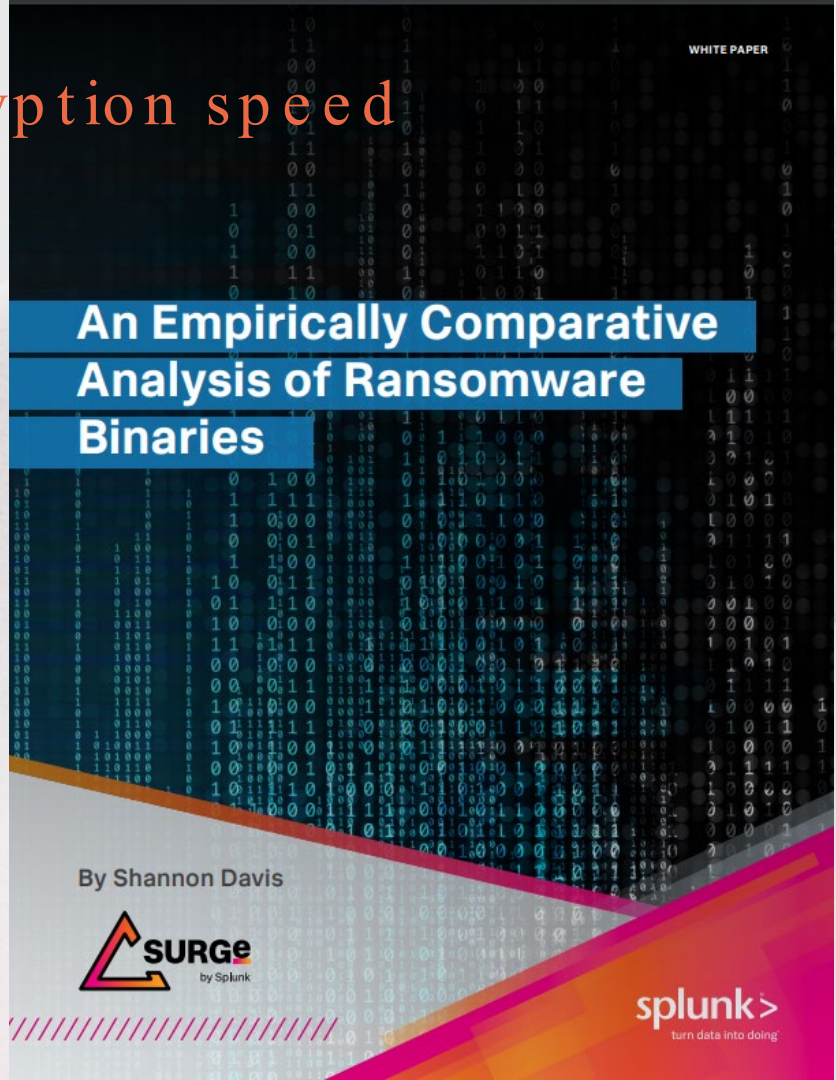
Petya

- Stream index: uint32_t
- Function *rotate left*: uint16_t
  return (value << shift) | (value >>(32-shift));
- Hash function f. keystream output:
  split 64bit input in 2*16bit output
- Effectively used key bytes:
  b0, b2, b4, b6, b8, b10, b12, b14

Brute-forcing is possible

Time matters: Measuring encryption speed

- Splunk March 2022
- 10 families
- 98.58k files



Encrypting swiftly with intermittent encryption

Family	Median duration files
LockBit	00:05:50
Babuk	00:06:34
Avaddon	00:13:15
Ryuk	00:14:30
Revil	00:24:16
BlackMatter	00:43:03
Darkside	00:44:52
Conti	00:59:34
Maze	01:54:33
Mespinoza (PYSA)	01:54:54

Top speed: Rorschach

- Appeared in March 2023
- Blend of curve25519 and eSTREAM cipher hc-128
- Intermittent encryption
- highly effective thread scheduling

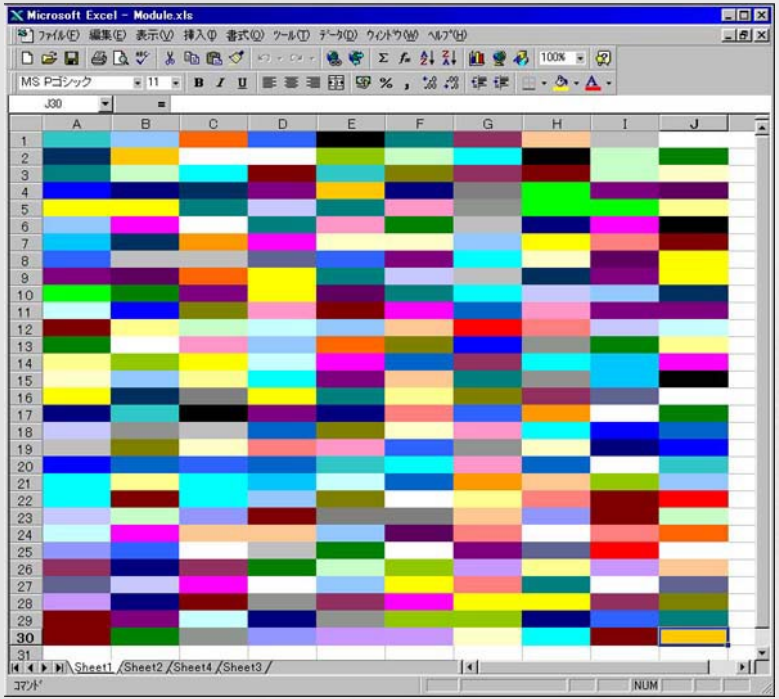
- Encrypts 220k files in 4.5 mins. Lockbit 3.0 needs 7 mins

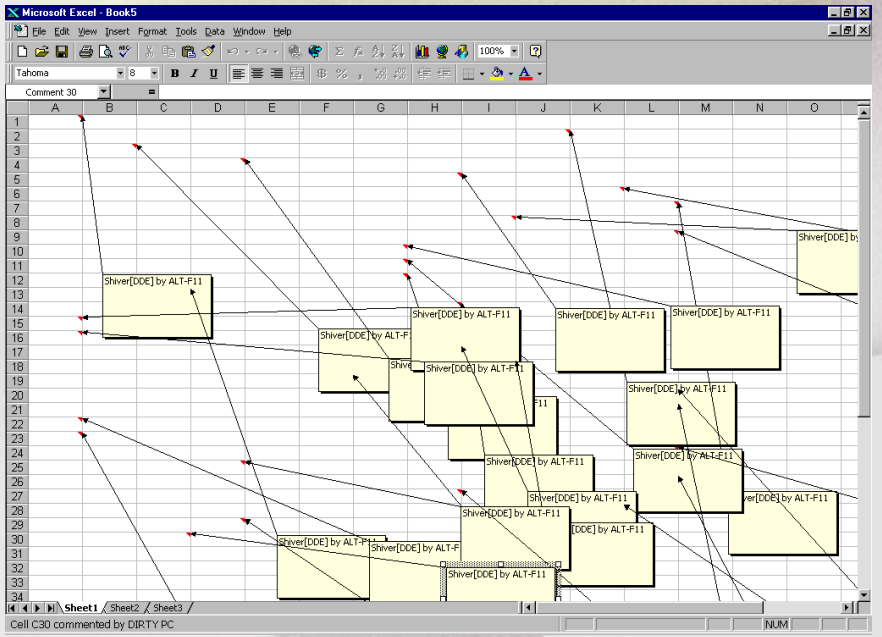
The future of ransomware

Evolution of the ransom business model

- Top => down: Big game hunting => SMEs
- RaaS => more specialisation
- Follow the money

Attacking integrity





G DATA CyberDefense

EVIDEN an atos business

Future of ransomware: research

More and better defense

- Ransomware prevention
- Ransomware mitigation
- Honeytraps
- Ransomware prediction
- Legal requirements
- Automation with AI, ML, DM, DS

c.f. https://ieeexplore.ieee.org/document/10105244

New fields

Extortion based on established infrastructure

- Smart Home, Smart TV
- Smart Factory, IoT, IIoT
- Connected cars, eMobility
- Smart City, Smart Meter, ...
- Access to Internet, LAN, Cloud services, Web applications
- Virtual & Augmented Reality
- Metaverse

Depends on profitability

Key takeaways

- Ransomware is here to stay
- Take cyber security seriously
- Be prepared: cyber resilience and business continuity
- Consider blackmailing in your threat models

Questions