

Ransomware: Past, present, future

Ralf Benz Müller, G DATA CyberDefense AG

Mindshare 2023
September 19th/20th

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

=====

ATTENTION:

I have been elected to inform you that throughout your process of collecting and executing files, you have accidentally PHUCKED yourself over: again, that's PHUCKED yourself over. No, it cannot be; YES, it CAN be, a Virus has infected your system. Now what do you have to say about that? HAHahaha. Have FUN with this one and remember, there is NO cure for

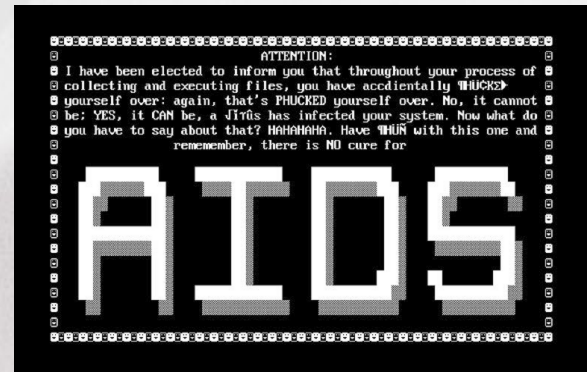
A I O S

=====

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



Ransom ware GP Coder

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

Ransom ware: System locker

BUNDESPOLIZEI
NATIONAL CYBER CRIMES UNIT
ACHTUNG!!!

Das Betriebssystem wurde im Zusammenhang mit
Es wurde folgender Verstoß festgestellt: Ihre IP Adresse lautet [REDACTED] mit dieser IP
Ihrem Computer wurden ebenfalls Videodateien mit porn
Es wurden auch Emails in Form von Spam, mit terroristischen Hintergründe

**Um die Sperre des Computers aufzuheben, sind Sie dazu verpflichtet
von 100 Euro zu zahlen. Sie haben zwei Möglichkeiten die Zahlung v
Euro zu leisten.**

1) Die Zahlung per Ukash begleichen:
Dazu geben Sie bitte den erworbenen Code in das Zahlungsfeld ein und drücken Sie aus
OK (haben Sie mehrere Codes,so geben Sie Diese einfach nacheinander ein und drücken
anschliessend auf OK).

Sollte das System Fehler melden, so müssen Sie den Code per Email
einzahlung@inter-bundeskriminalamt.eu versenden.

2) Die Zahlung per Paysafecard begleichen:
Dazu geben Sie bitte den erworbenen Code (gegebenfalls inkl. Passwort) in das Zahlung
drücken Sie anschliessend auf OK (haben Sie mehrere Codes,so geben Sie Diese einfach
ein und drücken Sie anschliessend auf OK).

Sollte das System Fehler melden, so müssen Sie den Code per Email
einzahlung@inter-bundeskriminalamt.eu versenden.

POLIZEI
Cyber Crime Investigation Department
Politie
Federal Computer Crime Unit
BUNDESPOLIZEI
ACHTUNG! AUFGEZEICHNET VERBRECHEN

**Office Central de lutte contre la
Criminalité liée aux Technologies de
l'Information et de la Communication**

POLIZIA DI STATO
UNITÀ DI ANALISI SUL CRIMINE INFORMATICO

POLITIE
POLITIE NEDERLAND
AFTDELING OM CRIMINALITEIT EN SURVEILLANTIE
Specialist Crime Directorate
Police Central e-crime Unit

COMANDO DE ESPAÑA
CORPO NACIONAL DE POLICIA
**BRIGADA DE INVESTIGACION
TECNOLÓGICA**
Atención!

PCeU
POLICE CENTRAL E-CRIME UNIT

Ukash
Vous pouvez acheter un voucher Ukash

Paysafecard
Vous pouvez acheter un voucher Paysafecard

IP: 16[REDACTED].67
Country: United States
Region:
City:

ATTENTION!
Your phone has been blocked up
for safety reasons listed below.
All the actions performed on this
phone are fixed.
All your files are encrypted.
CONDUCTED AUDIO AND VIDEO.

You are accused of viewing/storage and/or
dissemination of banned pornography (child
pornography/zoophilia/rape etc). You have
violated World Declaration on non-proliferation of
child pornography. You are accused of
committing the crime envisaged by Article 161 of
United States of America criminal law.

Article 161 of United States of America criminal

Circumventing System blockers

- ▶ Sometimes: Safe Mode
- ▶ Clean Boot

The screenshot shows the 'G DATA - EU Ransomware Cleaner' application window. A prominent warning dialog box is overlaid on top, titled 'Wichtiger Hinweis - Bitte beachten Sie Folgendes'. The dialog contains a yellow warning icon and a list of six steps for removing ransomware. The background application window shows a search progress bar at the bottom with the text 'Suche abgeschlossen' and a table of detected files.

G DATA - EU Ransomware Cleaner

Wichtiger Hinweis - Bitte beachten Sie Folgendes

Bitte befolgen Sie zum Entfernen der Ransomware folgende Schritte:

1. Nach dem Klick auf "OK" wird Ihr System automatisch neu gestartet.
2. Melden Sie sich wie gewohnt in Ihrem Windowssystem an.
3. AntiRansomware beginnt nun im Hintergrund mit den ersten Schritten zur Bereinigung Ihres Systems. Dieser Vorgang kann einige Minuten dauern.
4. Sobald dies geschehen ist, wird das System automatisch neu gestartet.
5. Melden Sie sich wie gewohnt an Ihrem Windowssystem an, um die Entfernung der Ransomware abzuschließen.
6. Nach erfolgreicher Bereinigung startet Ihr System wie gewohnt und Sie erhalten darüber eine Zusammenfassung.

OK Abbrechen

Montag, 6. Juli 2015 15:14:12 UTC

TRUST IN GERMAN SICHERHEIT.

Laufwerk	Name
C:	Microsoft

Suche abgeschlossen

Ransom ware: Cryptolocker

Cryptolocker 2.0

Your personal files are encrypted



Your files will be lost
without payment on:

11/24/2013 3:16:34 PM

Info

Your **important files were encrypted** on this computer: photos, videos, documents , etc. You can verify this by click on see files and try to open them.

Encryption was produced using **unique** public key **RSA-4096** generated for this computer. To decrypt files, you need to obtain **private** key.

The single copy of the private key, which will allow you to decrypt the files, is located on a secret server on the Internet; **the server will destroy the key within 72 hours after encryption completed.** After that, nobody and never will be able to restore files.]

To retrieve the private key, you need to pay 0.5 bitcoins.

Click **proceed to payment** to obtain private key.

Any attempt to remove or damage this software will lead to immediate private key destruction by server.

See files

<< Back

Proceed to payment >>

Cryptolocker 2.0

Payment for private key



Your files will be lost
without payment on:

11/24/2013 3:16:34 PM

Info

We only accept **Bitcoin** as payment solution for private key. To obtain it, you have to pay **0.5 BTC**.

Send 0.5 bitcoins to:

148m2eWmEJAi2b5TQ1CnzAY8YiZ0B9rpJJ

For more info about bitcoin visit <http://bitcoin.org/en/>

Once you done the payment, it will take some time, till we validate it and release the private key. Click on **'Validate payment >>'** to verify your payment and decrypt your files.

See files

<< Back

Validate payment >>

Ransomware: WannaCry May, 12th 2017

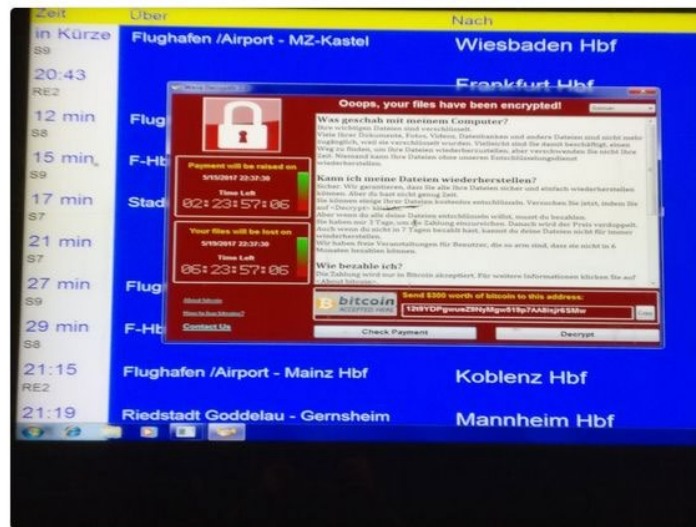


Marco Aguilar

@Avas_Marco

Folgen

Just got to Frankfurt and took a picture of this... #Sbahn, you got a #Ransomware!



RETWEETS
1.604

GEFÄLLT
1.110



Ransom ware 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

Chimera® Ransomware



Sie wurden Opfer der Chimera® Malware. Ihre privaten Dateien wurden verschlüsselt und sind ohne eine spezielle Schlüsseldatei nicht wiederherstellbar. Möglicherweise funktionieren einige Programme nicht mehr ordnungsgemäß!

Hiermit werden Sie aufgefordert Bitcoins an die unten stehende Adresse zu transferieren, um Ihre persönliche Schlüsseldatei zu erhalten.

Adresse: **1FcFozFbBEpLrBZhjkCTt3rvgxQfHNBW6v**
Forderung: **1,03424891 Bitcoins**

Das Entschlüsselungsprogramm und weitere Informationen, die Sie zur Wiederherstellung Ihrer Dateien benötigen, werden auf der folgenden Webseite zur Verfügung gestellt:

Wenn Sie der Forderung nicht nachgehen, werden wir Ihre persönlichen Daten, Fotos und Videos in Verbindung mit Ihrem Namen im Internet veröffentlichen.

bestätigen kann, dass diese Forderung echt ist.

Profitieren Sie von unserem Affiliate-Programm!
Weitere Informationen im Quelltext dieser Datei.

Ransomware evolution in the early years

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

Ransomware evolution 2016

2016

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

2016: 7200
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 campaign
- Target: Enterprises
- New: Overwrites MBR and encrypts

Von: Michael [redacted] <.michael.79@redacted>
Gesendet: Donnerstag, 24. März 2016 02:09
An: Personal
Betreff: Bewerbung als Vermessungstechniker - Vermessung

Bewerbung als Vermessungstechniker - Vermessung

Sehr geehrte Damen und Herren,

da ich auf der Suche nach einer neuen beruflichen Herausforderung bin, möchte ich mich hiermit bei Ihnen um eine Stelle als Vermessungstechniker - Vermessung bewerben, da ich bereits mehrere Jahre in diesem Bereich gearbeitet habe und zurzeit Arbeit suchend bin, möchte ich mich bei Ihnen bewerben.

Bewerbungsunterlagen



BewerbungsmappePDF.exe

788 KB

vor 4 Std.

in unterschiedlichen

issigen Mitarbeiter
leme.

rsönlich bei Ihnen

l zu groß war -

Petya

You became victim of Petya ransomware. The harddisks on your computer are encrypted with a military grade encryption algorithm. You can't access your data without a special key. To purchase your data back, please follow these steps:

1. Download the decryption key from our website. <http://petya-ransomware.com>
2. Visit one of our payment pages. <http://petya-ransomware.com>
3. Enter your payment details and purchase the key. If you already have a key, please enter it here. Key: _____

News

16.12.2015

Petya launched

Today we launched the Petya Ransomware Project.

lilitary grade encryption without a special key. Step 2.

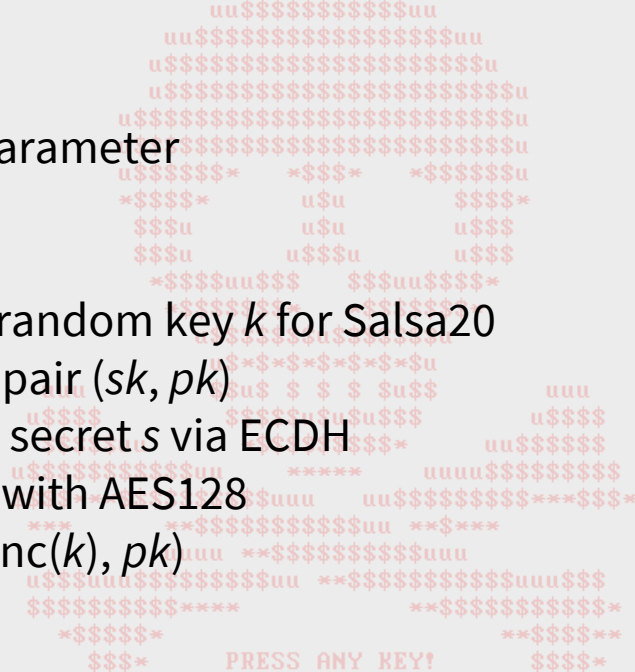
se three easy steps:

If you need a key, please purchase it from our website. <http://petya-ransomware.com>

GNuB-m77pyp-

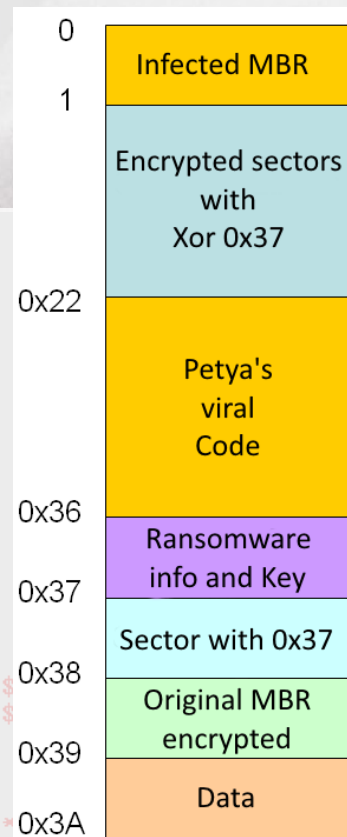
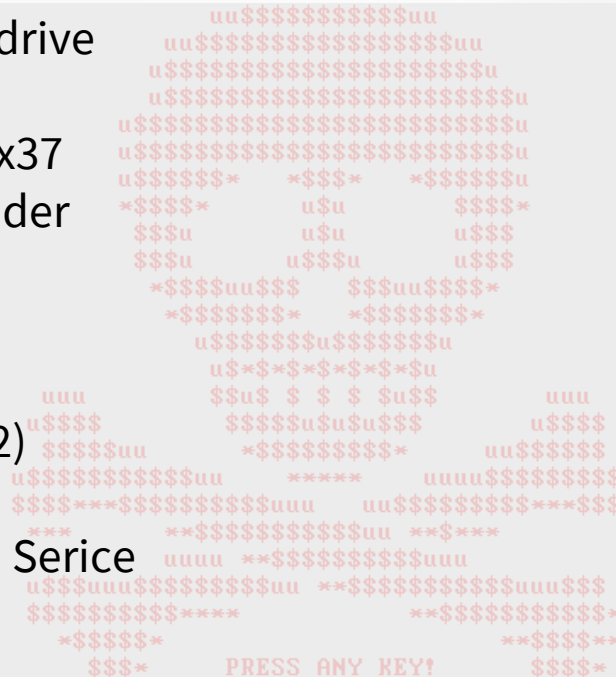
Petya encryption: Stage 1

- 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)



Petya encryption: Stage 1

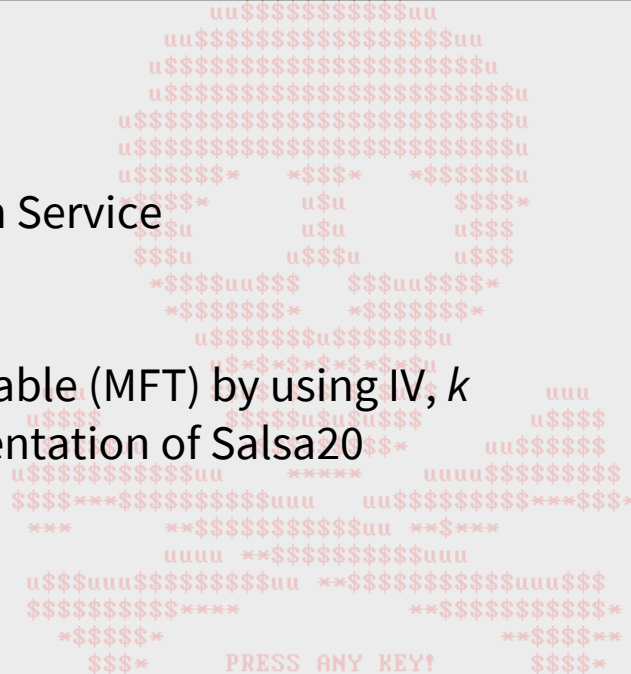
- Manipulating the hard drive
 - MBR XOR 0x37
 - Sector(1..34) XOR 0x37
 - Writes own Bootloader
 - Writes Stage 2
- Core data in Sector 54
 - *encrypted* flag (0|1|2)
 - Salsa20 IV + k
 - Links to Tor Hidden Service
 - Public key string



Quelle: tgsoft.it

Petya encryption: Stage 2

- Reads
 - *encrypted* flag
 - Key parameters
 - Links to Tor 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

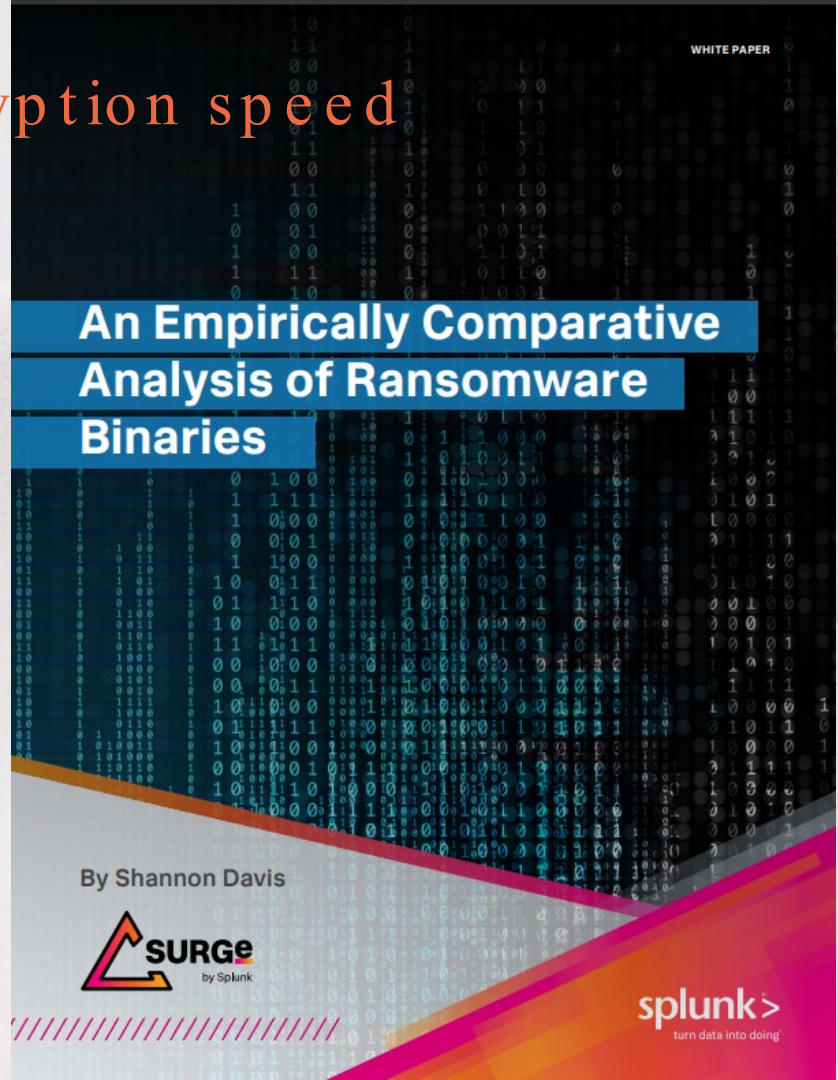
Petya

- 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



An Empirically Comparative Analysis of Ransomware Binaries

By Shannon Davis



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

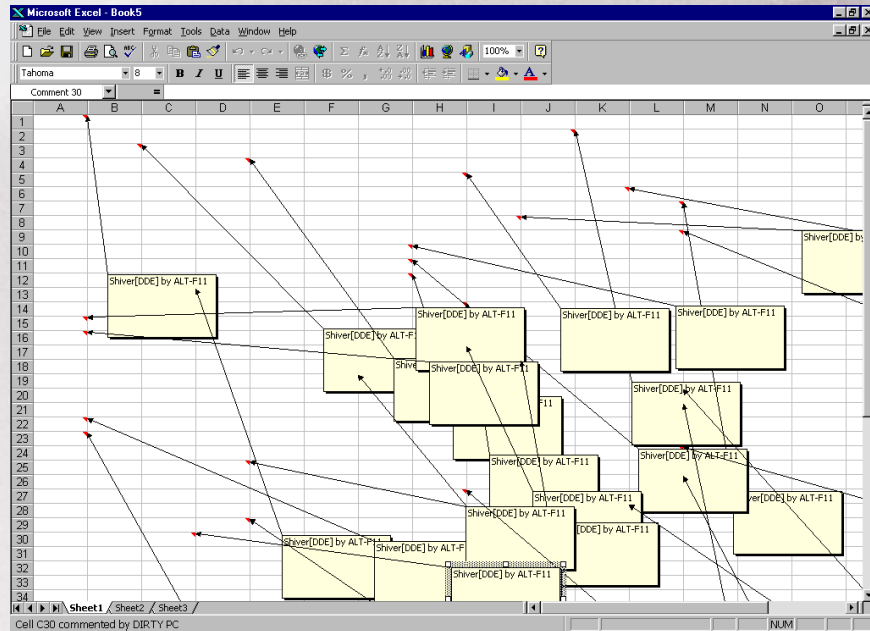
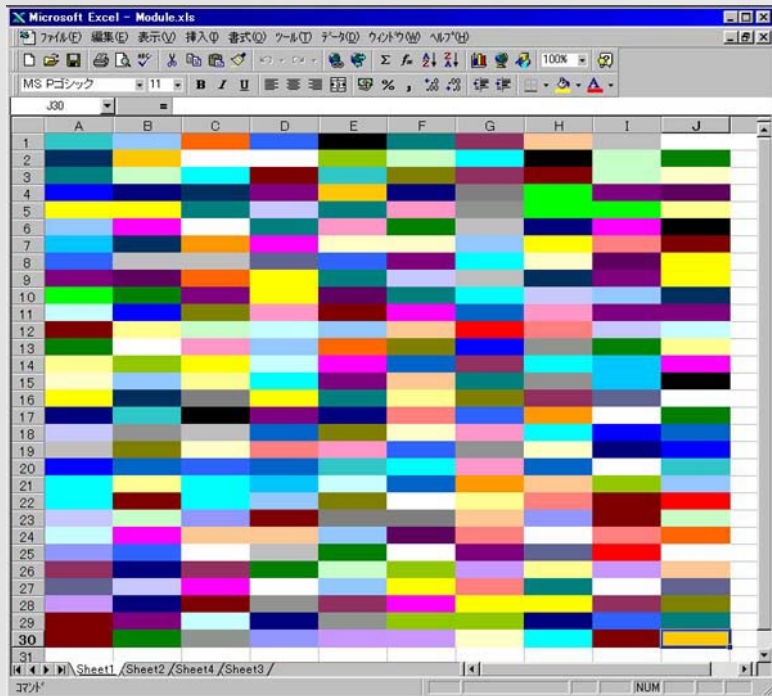
- ▶ Appeared in March 2023
- ▶ Blend of curve25519 and eSTREAM cipher hc-128
- ▶ Intermittent encryption
- ▶ highly effective thread scheduling
- ▶ Encrypts 220k files in 4.5 mins. Lockbit 3.0 needs 7 mins

The future of ransomware

Evolution of the ransom business model

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

Attacking integrity



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

