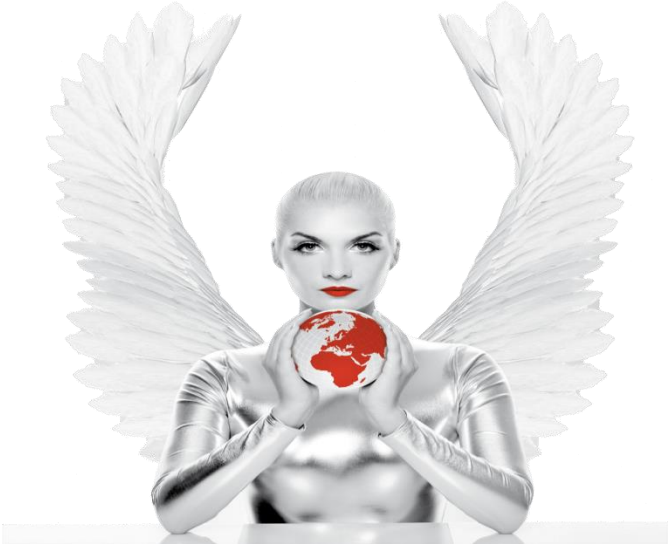
Access Denied – someone cryptowalled my network!



Basis Facts

- ✓ Ransomware =
- ✓ Durchschnittlicher Betrag USD 300

- ✓ Zahlungsmethode:
  - Locker Ransomware / Voucher Codes(ukash usw.)
  - Crypto Ransomware / Bitcoin (BTC)

- ✓ 2015 über 118.000 neue RansomBinaries / Monat
  - Locker 37%
  - Crypto 63%

Ziele:

- ✓ Windows, Linux, MacOS, Server & PCs, iOS (Jail Broken), AndroidOS
- ✓ der klassische „Home User“

  - kein Backup (90% der User verfügen über kein funktionelles/strukturiertes Backup)
  - Tonnen an wichtigen Dateien (Fotos, Diplomarbeiten usw.)

Prinzipiell jeder der bereit ist Lösegeld zu zahlen!

- ✓ Business

  - Backup und Desaster Recovery in vielen Firmen nach wie vor ein Fremdwort
  - Backup vorhanden! – auf Funktionalität getestet?

Lets get it Started

Ransom, what?

- ✓ Man unterscheidet zwischen 2 Gruppen:

  - Lockerware
    > sperrt Rechner

  - Cryptoware
    > verschlüsselt Rechner

BUNDESKRIMINALAMT

ABTEILUNG FÜR
COMPUTERKRIMINALITÄT

ACHTUNG !

IHR COMPUTER IST AUS EINEM ODER MEHREREN DER UNTEN AUFGEFÜHRTEN GRÜNDE GESPERRT

JAHR	TAG	MONAT	BEI	OFFENSE / KRIMINALITÄT
2012	21	06		CYBERCRIME

IP-ADRESSE	ISP	LAGE
		Austria

Die Seriennummer Ihrer Verletzung

ITC-BZXCCDD/FF

Sie haben gegen das Gesetz über «Urheberrecht und verwandte Schutzrechte» (Video, Musik, Software) verstoßen und unrechtmäßig urheberrechtliche Inhalte genutzt, bzw. verbreitet und somit gegen Art. 128 des Strafgesetzbuches der Bundesrepublik Deutschland verstoßen.
Art. 128 des Strafgesetzbuches zieht eine Strafe in Höhe von 2 bis 500 Mindestlöhnen oder eine Freiheitsstrafe von 2 bis 8 Jahren in Betracht.

Sie haben verbotene pornografische Inhalte eingesehen oder verbreitet (Child Porno/Zoofilia etc.) und damit gegen Art. 202 des Strafgesetzbuches der Bundesrepublik Deutschland verstoßen. Art. 202 des Strafgesetzbuches zieht eine Freiheitsstrafe von 4 bis 12 Jahren in Betracht.

Von ihrem Computer aus wurde ein rechtwidriger Zugang zu Computerdaten durchgeführt oder Sie.... Art. 208 des Strafgesetzbuches zieht eine Strafe in Höhe von 100.000€ und/oder Freiheitsstrafe von 4 bis 9 Jahren in Betracht.

Von ihrem Computer aus wurde ein rechtswidriger Zugang ohne ihre Kenntnis durchgeführt. Womöglich ist ihr Computer von schädlichen Programmen befallen, diesbezüglich verstoßen sie das Getz über die "Fahrlässige

PayPal
Geben Sie Ihre Kartennummer *
example: 4444 4444 4444 4444

ukash
Geben Sie Ihre Kartennummer *
example: 6334444444444444

paysafecard
Geben Sie Ihre Kartennummer *
example: 0004444444444444

Strafe zahlen

* Wählen Sie eine der Arten der Bezahlung

Norton by Symantec · VeriSign Secured · AVIA · Agip · Esso · OMV · Q1 · Westfalen · epay

Der Polizeipräsidentin Vienna Platz der Luftbrücke 6D-12101 Vienna

Cryptoware

- ✓ Verschlüsselt Daten / Files auf Computern, Servern und Netzlaufwerken
- ✓ Wird meist via SPAM-E-Mail versandt, z.B. als „www.badurl“ oder als „Rechnung.zip“
- ✓ Computer sind nach Infektion „eingeschränkt“ benutzbar
- ✓ Kosten: 350 – 5K USD, je nach „Projekt“
- ✓ Lösegeld Währung BTC neuere Generationen via TOR
- ✓ Verwendet symmetrische und asymmetrische Schlüssel

- ✓ Entschlüsselung nur unter massiven Aufwand möglich, bzw. nicht selten unmöglich

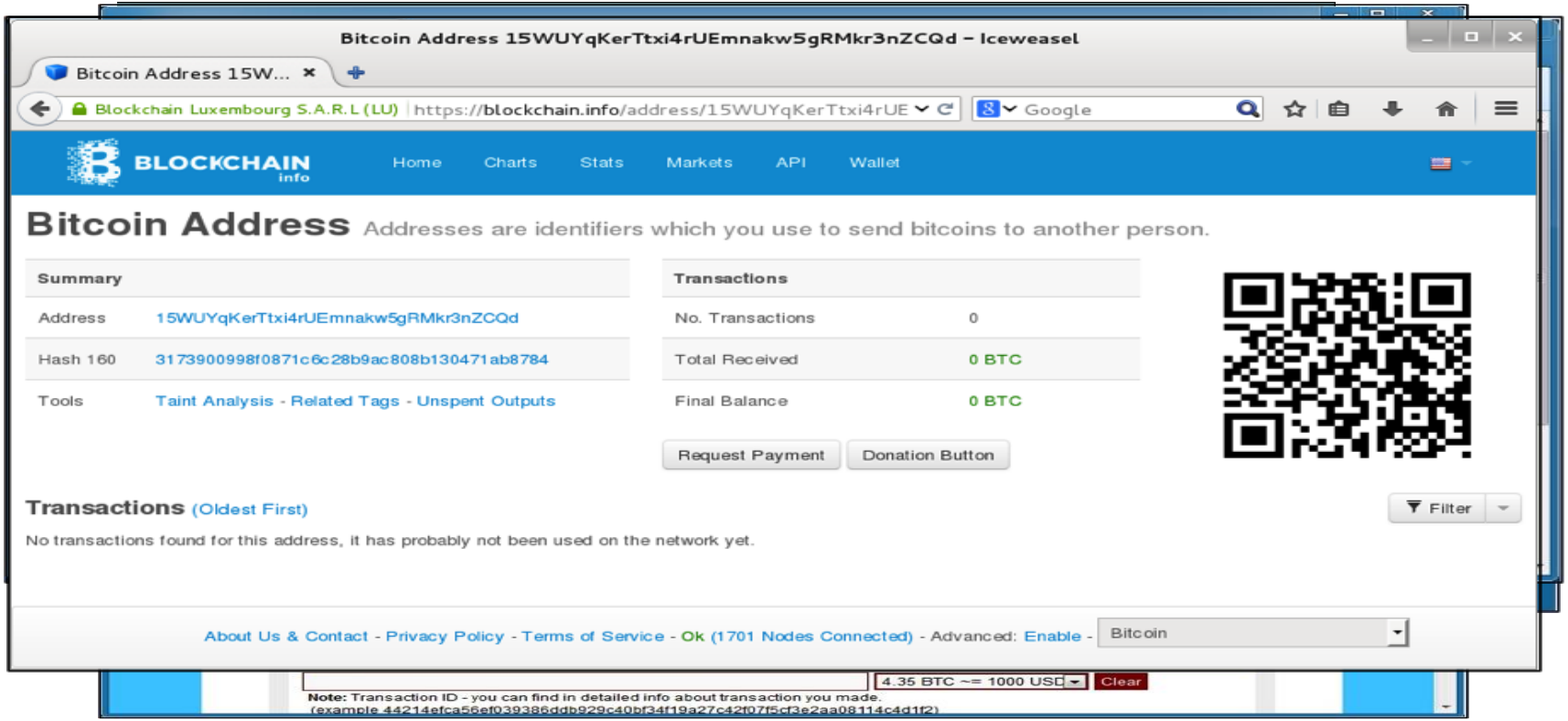
Symmetrisch vs. Asymmetrisch

- ✓ Symmetrisch
  - es wird ein Schlüssel verwendet, alle Dateien sind gleich verschlüsselt

- ✓ Asymmetrisch
  - verwendet 1 Schlüsselpaar (Private/Public-Key-Verfahren)

Cryptowall ab Vers.3.0 und TeslaCrypt verwenden beides!!

Infektionsablauf



„Zustellung“ CrytoWall 3.0

Verschickt jeweils viele E-Mails pro Bot – verhältnismäßig geringe Menge an Bots involviert (meist weniger als 250 pro Welle – dafür bis zu 500 Mails pro Bot)

hits: 472
ip's: 11
first seen: 11.12.2015 13:15:05
filename: Quittung.N2331X347.zip:Quittung.N2331X347.exe
scancenter: TA-Prof
filesize: 258548
last alert: 11.12.2015 15:11:41 hits = 133
md5: c2b18f218569f09e8be75d4594de364d
sample: http://mmwstat.isc.local/cgi-bin/genstatistic.pl?md5=c2b18f218569f09e8be75d4594de364d&module=download

Subject (count, subject)
5 *****POSSIBLE SPAM***** Ihre A1 Quittung N839598677-9 vom 12.12.2015
5 *****POSSIBLE SPAM***** Ihre A1 Quittung N839598677-9 vom 12.12.2015
5 *****POSSIBLE SPAM***** Ihre A1 Quittung N839598677-9 vom 12.12.2015
5 *****POSSIBLE SPAM***** Ihre A1 Quittung N839598677-9 vom 12.12.2015
5 *****POSSIBLE SPAM***** Ihre A1 Quittung N839598677-9 vom 12.12.2015
4 *****POSSIBLE SPAM***** Ihre A1 Quittung N839598677-9 vom 12.12.2015
4 *****POSSIBLE SPAM***** Ihre A1 Quittung N839598677-9 vom 12.12.2015
4 *****POSSIBLE SPAM***** Ihre A1 Quittung N839598677-9 vom 12.12.2015
4 *****POSSIBLE SPAM***** Ihre A1 Quittung N839598677-9 vom 12.12.2015
4 *****POSSIBLE SPAM***** Ihre A1 Quittung N839598677-9 vom 12.12.2015

Filename (count, filename)
464 Quittung.N2331X347.zip:Quittung.N2331X347.exe
5 rfc822-message:Quittung.N2331X347.zip:Quittung.N2331X347.exe
2 Quittung.N2331X347.exe
1 Ihre A1 Bestellung N3818257-6 vom 12.12.2015:Quittung.N2331X347.zip:Quittung.N2331X347.exe

Fromaddress (count, from)
152 admin <robot@a1.net>
11 admin <admin@a1.net>
7 robot <Admin@a1.net>
6 Admin <email@a1.net>
6 Admin <Office@a1.net>
6 manager <Admin@a1.net>
5 Buro <info@a1.net>
5 contact <a1@a1.net>
5 Hilfe <Office@a1.net>
5 info <admin@a1.net>

Sender (count, fqdn(ip))
306 194-17-250-10.customer.telia.com(194.17.250.10)
152 bsmtp8.bon.at(213.33.87.20)

„Zustellung“ TESLACrypt

hits: 123
ip's: 123
first seen: 14.12.2015 17:35:12
filename: invoice_90002995_scan.zip:invoice_copy_lIdT8p.js
scancenter: scancenter-ikarus
filesize: 49390
md5: 594a6d5ecbf499573e16766179ce68cd
sample: http://mmwstat.isc.local/cgi-bin/genstatistic.pl?md5=594a6d5ecbf499573e16766179ce68cd&module=download

Verschickt jeweils nur 1 E-Mail pro Bot – verhältnismäßig geringe Versandmenge (meist zwischen 100-500 E-Mails pro Welle – dafür bis zu 50 Wellen pro Stunde!!)

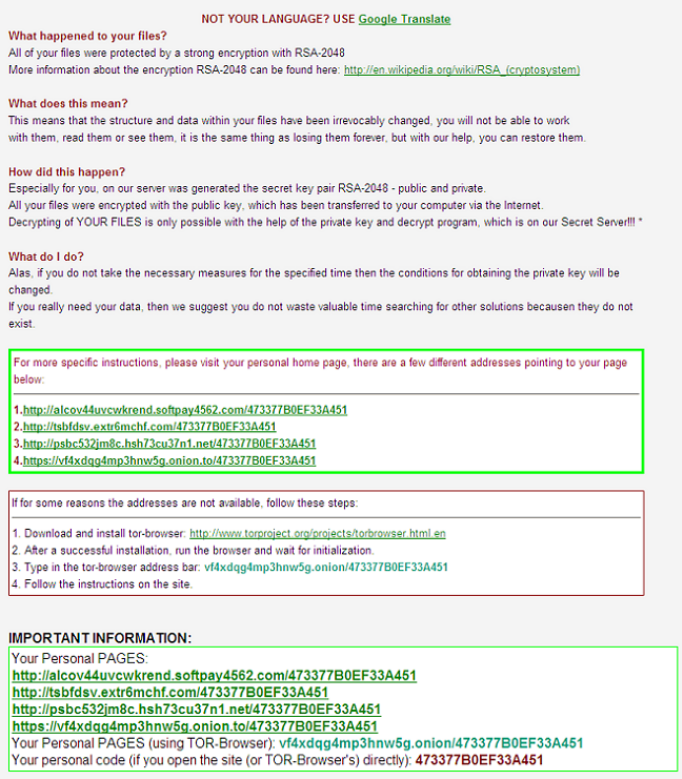
Subject (count, subject)
1 Your order #08626994
1 Your order #07043532
1 Your order #06666111
1 Your order #04603860
1 Your order #04217521
1 Your order #03481485
1 Your order #02651130
1 Your order #02346385
1 Your order #02174802
1 Your order #00788256

Filename (count, filename)
1 invoice_08626994_scan.zip:invoice_copy_lIdT8p.js
1 invoice_07043532_scan.zip:invoice_copy_lIdT8p.js
1 invoice_06666111_scan.zip:invoice_copy_lIdT8p.js
1 invoice_04603860_scan.zip:invoice_copy_lIdT8p.js
1 invoice_04217521_scan.zip:invoice_copy_lIdT8p.js
1 invoice_03481485_scan.zip:invoice_copy_lIdT8p.js
1 invoice_02651130_scan.zip:invoice_copy_lIdT8p.js
1 invoice_02346385_scan.zip:invoice_copy_lIdT8p.js
1 invoice_02174802_scan.zip:invoice_copy_lIdT8p.js
1 invoice_00788256_scan.zip:invoice_copy_lIdT8p.js

Keine EXE/ZIP-Files, sondern ein hoch – obfuscatetes JavaScript – als Erstinfektor – der die eigentliche Malware erst nachlädt

Fromaddress (count, from)
1 Angelita Kent <KentAngelita93109@gourmetfoodmixes.net>
1 Angelica Michael <MichaelAngelica6291@aumeilleurdelafrance.com>
1 Anastasia Osborne <OsborneAnastasia69@petitegrace.com.br>
1 Amanda Manning <ManningAmanda8531@hts.net.id>
1 Alta Ruiz <RuizAlta449@bestel.com.mx>
1 Alma Kramer <KramerAlma363@thepartnersource.com>
1 Alison Long <LongAlison2256@adpi-me.com>
1 Alfredo Rush <RushAlfredo90916@evnetics.com>
1 Alfreda Bush <BushAlfreda194@business.telecomitalia.it>

Ransom Trojan TESLA Crypt



NOT YOUR LANGUAGE? USE Google Translate

What happened to your files?
All of your files were protected by a strong encryption with RSA-2048
More information about the encryption RSA-2048 can be found here: http://en.wikipedia.org/wiki/RSA_(cryptosystem)

What does this mean?
This means that the structure and data within your files have been irrevocably changed, you will not be able to work with them, read them or see them, it is the same thing as losing them forever, but with our help, you can restore them.

How did this happen?
Especially for you, on our server was generated the secret key pair RSA-2048 - public and private.
All your files were encrypted with the public key, which has been transferred to your computer via the Internet.
Decrypting of YOUR FILES is only possible with the help of the private key and decrypt program, which is on our Secret Server!!! *

What do I do?
Alas, if you do not take the necessary measures for the specified time then the conditions for obtaining the private key will be changed.
If you really need your data, then we suggest you do not waste valuable time searching for other solutions becausen they do not exist.

For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:

1.http://alcov44uvcwkrend.softpay4562.com/473377B0EF33A451
2.http://tsbfdsv.extr6mchf.com/473377B0EF33A451
3.http://psbc532jm8c.hsh73cu37n1.net/473377B0EF33A451
4.https://vf4xdqg4mp3hnw5g.onion.to/473377B0EF33A451

If for some reasons the addresses are not available, follow these steps:

1. Download and install tor-browser: http://www.torproject.org/projects/torbrowser.html.en
2. After a successful installation, run the browser and wait for initialization.
3. Type in the tor-browser address bar: vf4xdqg4mp3hnw5g.onion/473377B0EF33A451
4. Follow the instructions on the site.

IMPORTANT INFORMATION:

Your Personal PAGES:
http://alcov44uvcwkrend.softpay4562.com/473377B0EF33A451
http://tsbfdsv.extr6mchf.com/473377B0EF33A451
http://psbc532jm8c.hsh73cu37n1.net/473377B0EF33A451
https://vf4xdqg4mp3hnw5g.onion.to/473377B0EF33A451
Your Personal PAGES (using TOR-Browser): vf4xdqg4mp3hnw5g.onion/473377B0EF33A451
Your personal code (if you open the site (or TOR-Browser's) directly): 473377B0EF33A451

Erzwingt vom Opfer auch die Installation eines TOR-Browsers um via TOR eine Website für weitere Informationen/Vorgehensweisen aufzusuchen.

Massive Erschwernis für Strafverfolgung und forensische Analysen.

Zwischenbilanz

- ✓ Der AIDS Trojaner anno 1989 „kostete“ 189 USD. Überraschenderweise ist der Preis für Ransomware über die Jahre nicht dramatisch angestiegen.

- ✓ Wenn man die Inflation zwischen 1989 und 2015 mit einbezieht entsprechen die 350 USD von heute den 189 USD von 1989!

- ✓ Conclusio: nicht alles wird teurer ;-)

Rechenbeispiel

rkennt das infizierte Binary

:h überall wo der User Zugriff

Teslacrypt next Generation

Für mobile Geräte

- ✓ Gibt es, allerdings wird es für Hacker/Cracker immer schwieriger da die Betriebssysteme immer mehr in Richtung Sicherheit getrimmt werden

- ✓ Schwachstellen sind die immer noch im Umlauf befindlichen alten unsicheren OS-Versionen, Rooting/JailBreaks und der User selbst (Rechtevergabe!)

- ✓ Hesperbot (Android Lockerware) Reversing

https://github.com/IKARUSSoftwareSecurity/hesperbot-cracker

Gemeinsamkeiten - Follow the Leader?

- ✓ Aids Trojan aka PC Cyborg
- ✓ Gpcode
- ✓ Archiveus
- ✓ Cryptowall 1.0 – xxx
- ✓ TeslaCrypt 1.0 –xxx
- ✓ Locky =

gleiches (Geschäfts)Modell mit „zeitgemäßer“ (Weiter)entwicklung

Wer sind die Drahtzieher?

WANTED
BY THE FBI

Conspiracy to Participate in Racketeering Activity; Bank Fraud; Conspiracy to Violate the Computer Fraud and Abuse Act; Conspiracy to Violate the Identity Theft and Assumption Deterrence Act; Aggravated Identity Theft; Conspiracy; Computer Fraud; Wire Fraud; Money Laundering; Conspiracy to Commit Bank Fraud

EVGENIY MIKHAILOVICH BOGACHEV

Aliases: Yevgeniy Bogachev, Evgeniy Mikhaylovich Bogachev, "lucky12345", "slavik", "Pollingsoon"

DESCRIPTION

Date(s) of Birth Used: October 28, 1983
Height: Approximately 5'9"
Weight: Approximately 180 pounds
NCIC: W890989955
Occupation: Bogachev works in the Information Technology field.

Hair: Brown (usually shaves his head)
Eyes: Brown
Sex: Male
Race: White

Remarks: Bogachev was last known to reside in Anapa, Russia. He is known to enjoy boating and may travel to locations along the Black Sea in his boat. He also owns property in Krasnodar, Russia.

Zukunft

- ✓ IoT – Vernetzung von TV, Kaffeemaschine, Kühlschrank
- ✓ NAS (Trojan.Synolocker für Synology)
- ✓ Linux basierende Systeme wie Raspberry Pi, Router, usw
- ✓ Gadgets (Smartwatch) durch infizierte APK-Installation am Smartphone automatischer Push auf die Uhr
- ✓ „smart“ Cars (diversester Hersteller)

Gegenmaßnahmen

- ✓ OS, Java und Browser immer am aktuellsten Stand halten (Patchen)
- ✓ Virenscanner
- ✓ SPAM-Filter
- ✓ Backups
- ✓ Network Protection, Firewall(s) & IPS
- ✓ %appdata% und %startup% via Grouppolicies am Ausführen von Executables hindern
- ✓ Makros Deaktivieren oder nur signierte Makros verwenden!
- ✓ **MERKE!** ERST die Malware entfernen und DANACH die Files entschlüsseln!!!
- ✓ https://www.fishnetsecurity.com/6labs/blog/cryptolocker-prevention-and-remediation-techniques


**** COMMODORE 64 BASIC V2 ****
64K RAM SYSTEM 38911 BASIC BYTES FREE
READY.
DANKE!
SIEGFRIED SCHAUER
IKARUS SECURITY SOFTWARE GMBH
BLECHTURMGASSE 11
1050 WIEN/AUSTRIA
SCHAUER.S(AT)IKARUS.AT
PGP FINGERPRINT 6DDC 1964 7EB9 9684 2686
363A EB6F 86C8 EBBD 31C0
WWW.IKARUSSECURITY.COM
LOAD
PRESS PLAY ON TAPE

Kontaktdetails / Sources

Siegfried Schauer
M.E.R.T.

IKARUS Security Software GmbH
Blechturmgasse 11 | 1050 Vienna | Austria
Tel: +43 1 589 95 – 235 | Fax: – 100 | E-Mail: Schauer.s@ikarus.at
PGP Fingerprint: 6DDC 1964 7EB9 9684 2686 363A EB6F 86C8 EBBD 31C0
FN 64708i ATU15191405
www.ikarussecurity.com

Sources:
https://www.virusbtn.com/pdf/magazine/1990/199002.pdf
http://vxheaven.org/lib/ajh00.html
http://www.anti-malware.info/old-visual-payloads/
http://blog.rackspace.com/exploit-kits-and-cryptowall-3-/
http://www.greenbookblog.org/2013/01/17/insights-the-needle-in-the-haystack/