INSIGHTS AUS REALEN SICHERHEITSVORFÄLLEN

30. Juni 2023 – EDI Podium

InfoGuard
SWISS CYBER SECURITY

MEIN NAME IST STEFAN ROTHENBÜHLER UND ICH JAGE HACKER

BSc. Hochschule Luzern/FHZ

MAS in Information Security

Offensive Security Certified Professional

- since 2018 Principal Cyber Security Analyst Intelligence & Investigations (CSIRT)
- 2016 – 2018 Penetration Tester at InfoGuard AG Red Team
- 2009 – 2016 Systems Engineer Swisscom AG (@bluewin.ch)
- 2007 – 2009 SUN Campus Ambassador Hochschule Luzern

INFOGUARD –
IHR SCHWEIZER CYBER SECURITY EXPERTE

InfoGuard
SWISS CYBER SECURITY

200
SICHERHEITSEXPERT*INNEN

52 MIO. CHF
UMSATZ 2022

100%
IM BESITZ DES SCHWEIZER MANAGEMENTS

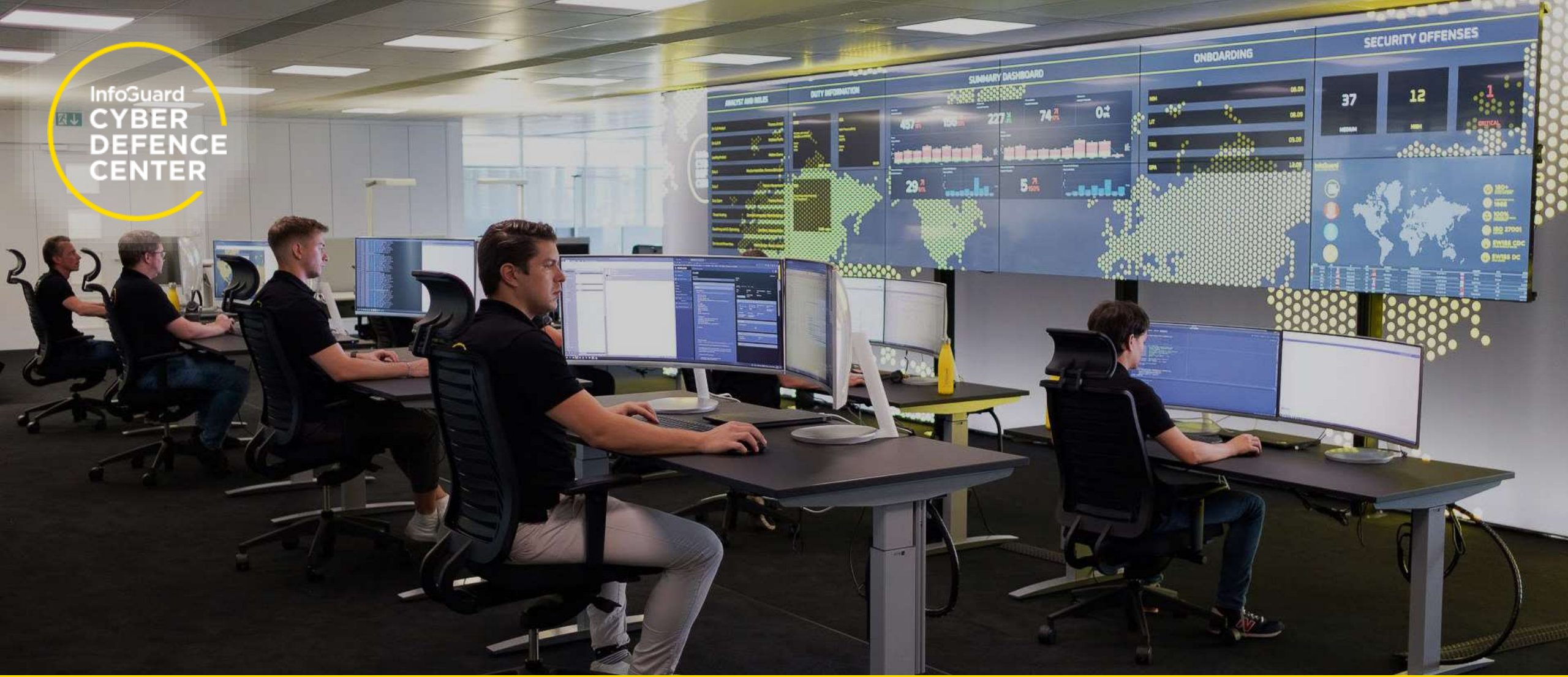
KOMPETENZ SEIT
2001

NIEDERLASSUNGEN
BAAR, BERN, MÜNCHEN & WIEN

SWISS CDC
CYBER DEFENCE CENTER

APT-RESPONDER BSI qualifiziert
FIRST
Forum of Incident Response & Security Teams

ISO 27001
ISAE 3000 TYP 2
ISO 14001



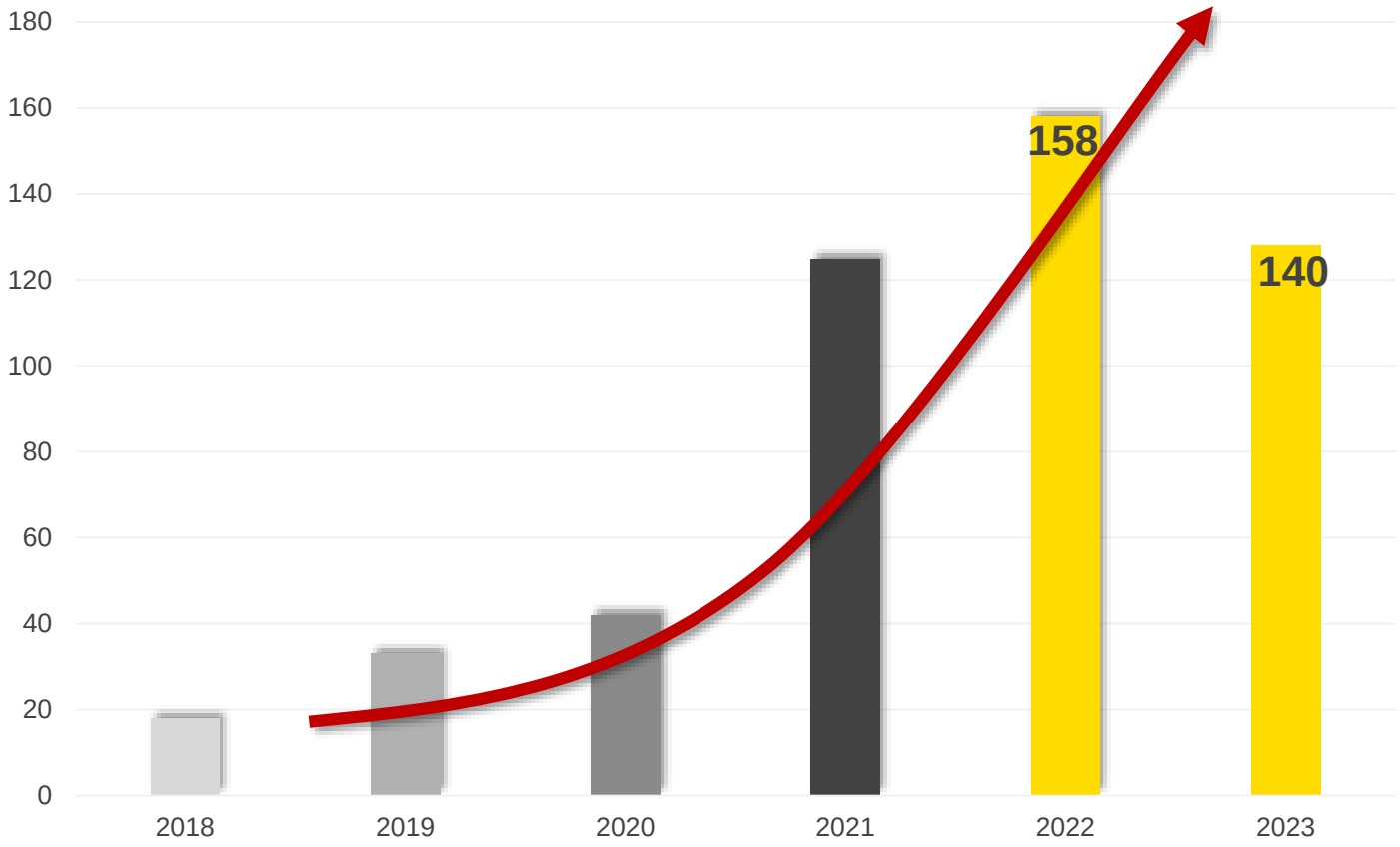
SWISS CDC
CYBER DEFENCE CENTER

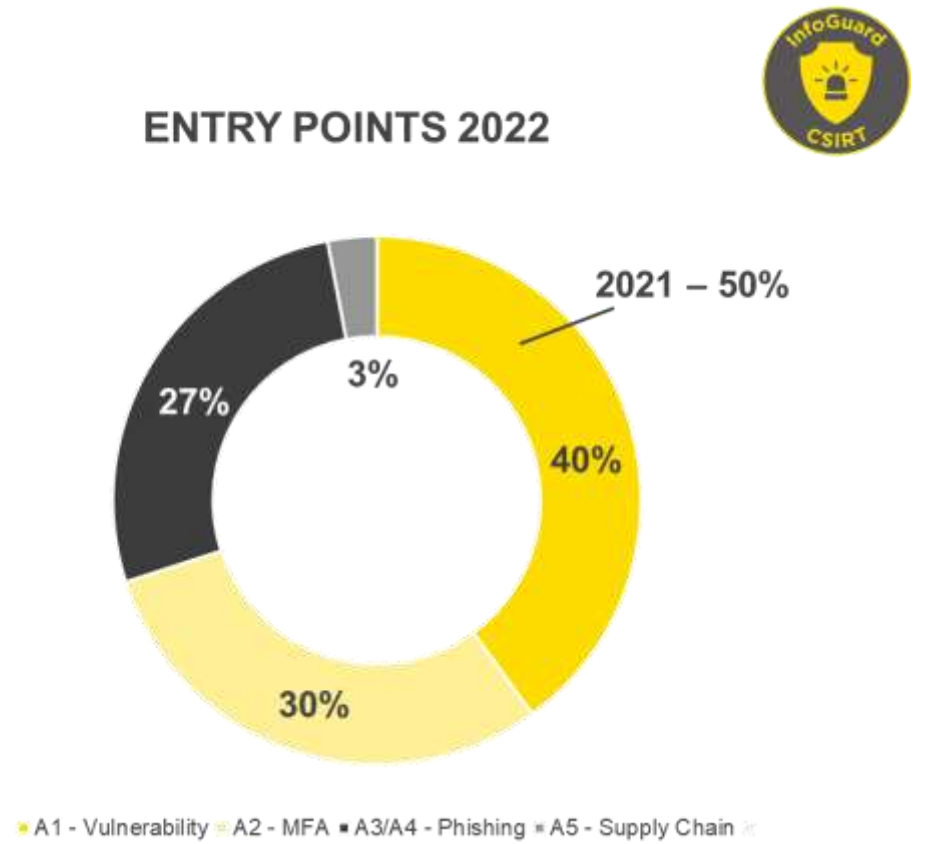
70+
EXPERT*INNEN

550m²
OFFICEFLÄCHE

ISO 27001
ISAE 3000 TYP 2

INFOGUARD CSIRT – FALLSTATISTIK





Quelle: InfoGuard CSIRT

PROFESSIONELLE UNTERSTÜTZUNG BEI EINEM SICHERHEITSVORFALL

Übernahme / Coaching Krisenstab

Forensische Untersuchung

Verhandlung mit Erpressern

Behörden

Rechtliche Unterstützung

Krisen-kommunikation

Unterstützung bei Bezahlung

Learnings & Verbesserung

Gesicherter Wiederanlauf / Aufbau

SICHERHEITSVORFÄLLE IM HEALTHCARE-UMFELD

InfoGuard
SWISS CYBER SECURITY

Phishing Attack Breaches Data of 30,000 Memorial Hospital Patients

An employee of Memorial Hospital at Gulfport, Mississippi responded to a phishing email 11 days before it was discovered; an extortion attempt, compromised server, and malware complete this week's breach roundup.

By Jessica Davis

CANADA

eHealth files stolen in ransomware attack

Another 2.2 million patients affected by AMCA data breach

Arztpraxis stellt Patientendossiers als Altpapier an Strasse

Vor einer Zürcher Arztpraxis lagen grosse Stapel vertraulicher Patientenakten – als Altpapier gebündelt. Laut dem Praxisleiter handelt es sich um ein Versehen.

Daniel Graf

World Health Organization

Health Topics | Countries | Newsroom | Emergencies

Home / Newsroom / Detail / WHO reports fivefold increase in cyber attacks, urges vigilance

WHO reports fivefold increase in cyber attacks, urges vigilance

23 April 2020 | News release | Geneva

Since the start of the COVID-19 pandemic, WHO has seen a dramatic increase in the number of cyber attacks directed at its staff, and email scams targeting the public at large.

This week, some 450 active WHO email addresses and passwords were leaked online along with thousands belonging to others working on the novel coronavirus response.

The leaked credentials did not put WHO systems at risk because the data was not recent. However, the attack did impact an older extranet system, used by current and retired staff as well as partners.

WHO is now migrating affected systems to a more secure authentication system.

Scammers impersonating WHO in emails have also increasingly targeted the general public in order to channel donations to a fictitious fund and not the authentic COVID-19 Solidarity Response Fund. The number of cyber attacks is now more than five times the number directed at the Organization in the same period last year.

"Ensuring the security of health information for Member States and the privacy of users interacting with us a priority for WHO at all times, but also particularly during the COVID-19 pandemic. We are grateful for the alerts we receive from Member States and the private sector. We are all in this fight together," said Bernardo Mariano, WHO's Chief Information Officer.

WHO is working with the private sector to establish more robust internal systems and to strengthen security measures and is educating staff on cybersecurity risks.

WHO asks the public to remain vigilant against fraudulent emails and recommends the use of reliable sources to obtain factual information about COVID-19 and other health issues.

For more information, please visit www.who.int/covid-19

HIGHTECH VERBREITET MALWARE

HIGHTECH VERBREITET MALWARE

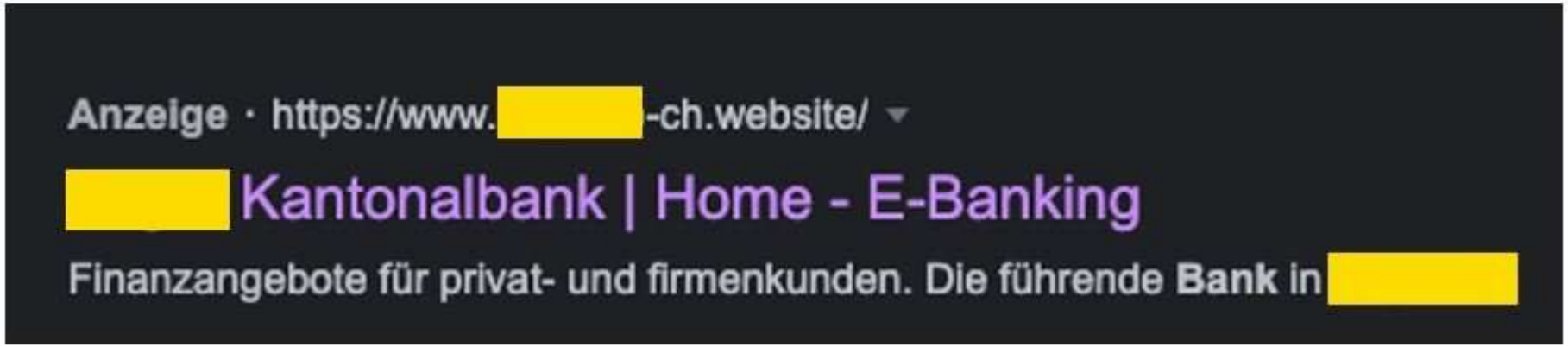
- Medizintech für mehrere Mio $
- Gerät wurde mit NotPetya (06.2017) ausgeliefert
- ~150 Systeme infiziert, bevor die Ausbreitung gestoppt wurde

FALLBEISPIEL 1: E-BANKING

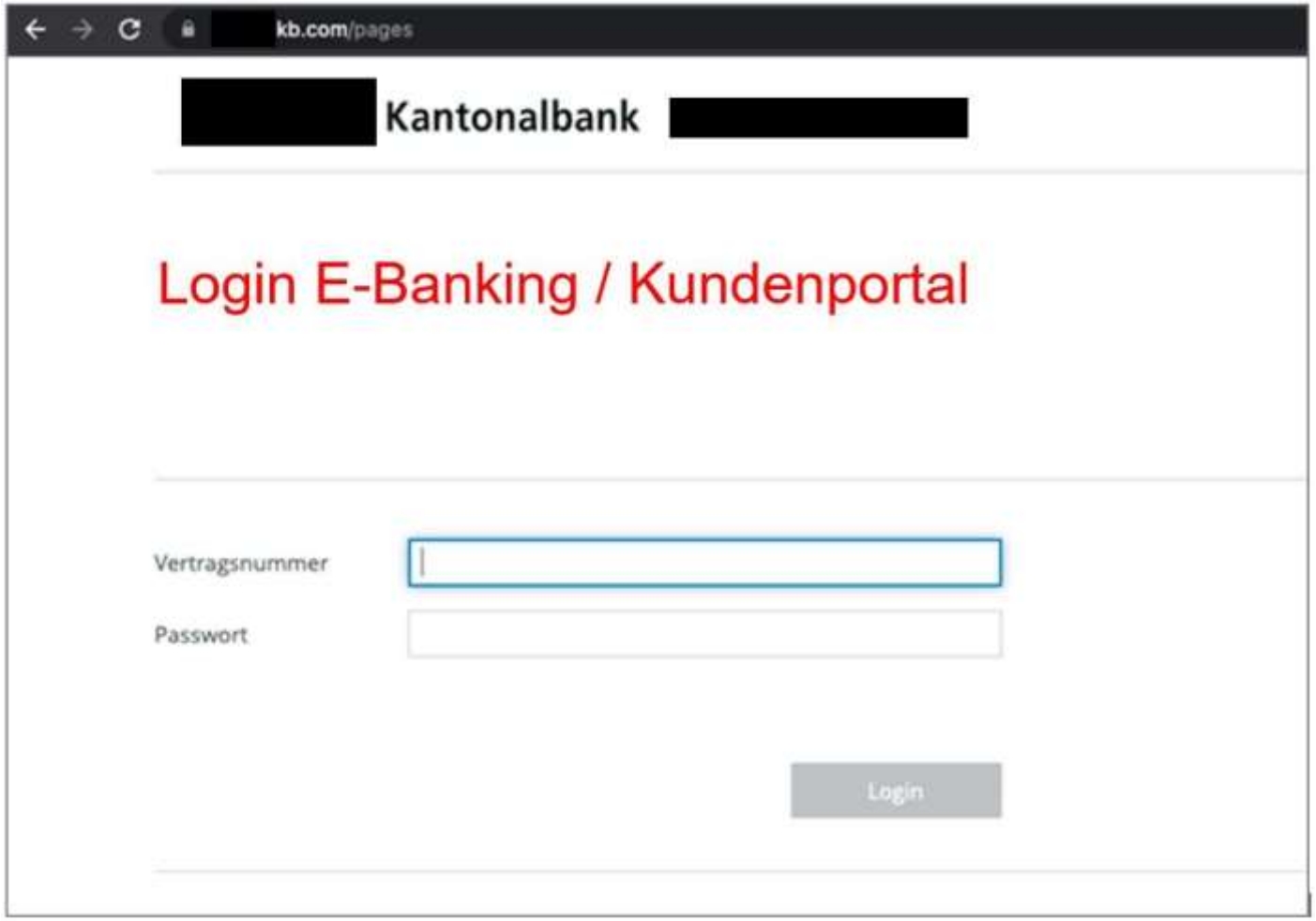
AUS AKTUELLEM ANLASS: INFOGUARD CSIRT WARNT VOR E-BANKING-BETRUGSFÄLLEN

Veröffentlicht am 23. Aug 2022 | von Stefan Rothenbühler | Breach Detection | Cyberrisiken

FALLBEISPIEL 1: E-BANKING



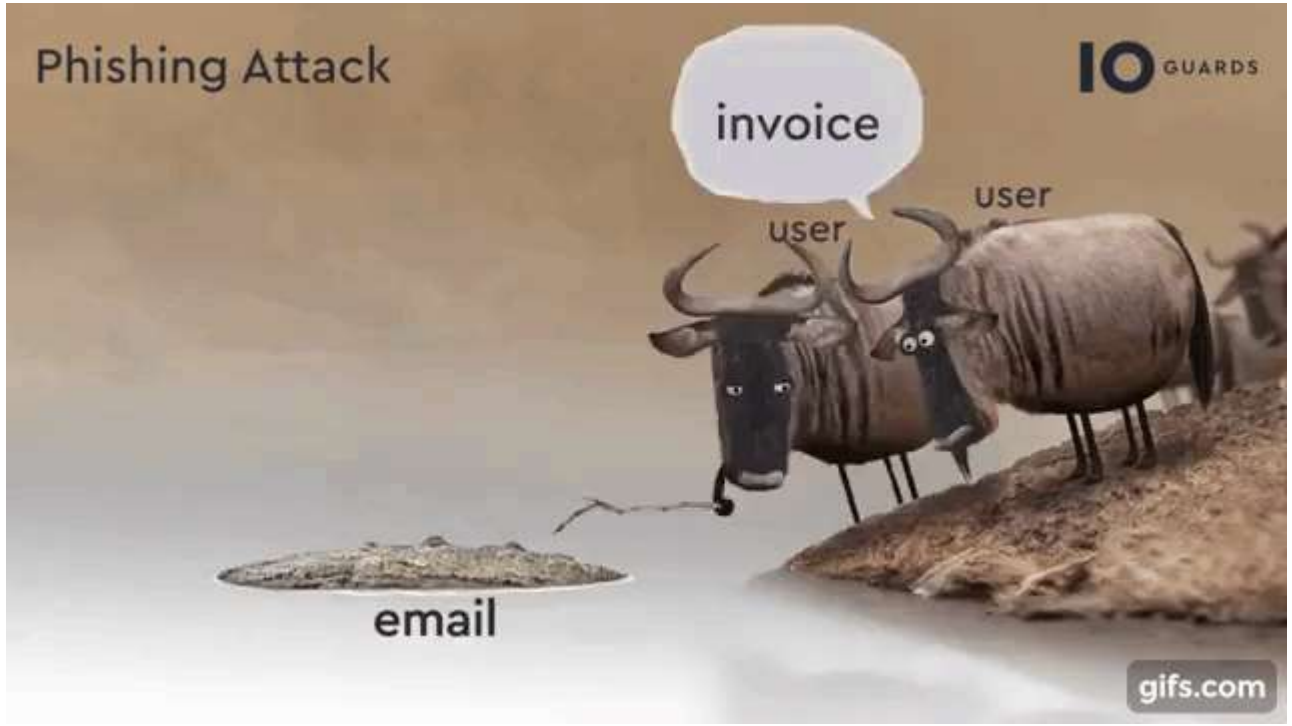
FALLBEISPIEL 1: E-BANKING



FALLBEISPIEL 1: E-BANKING

Schutz für Endkunden

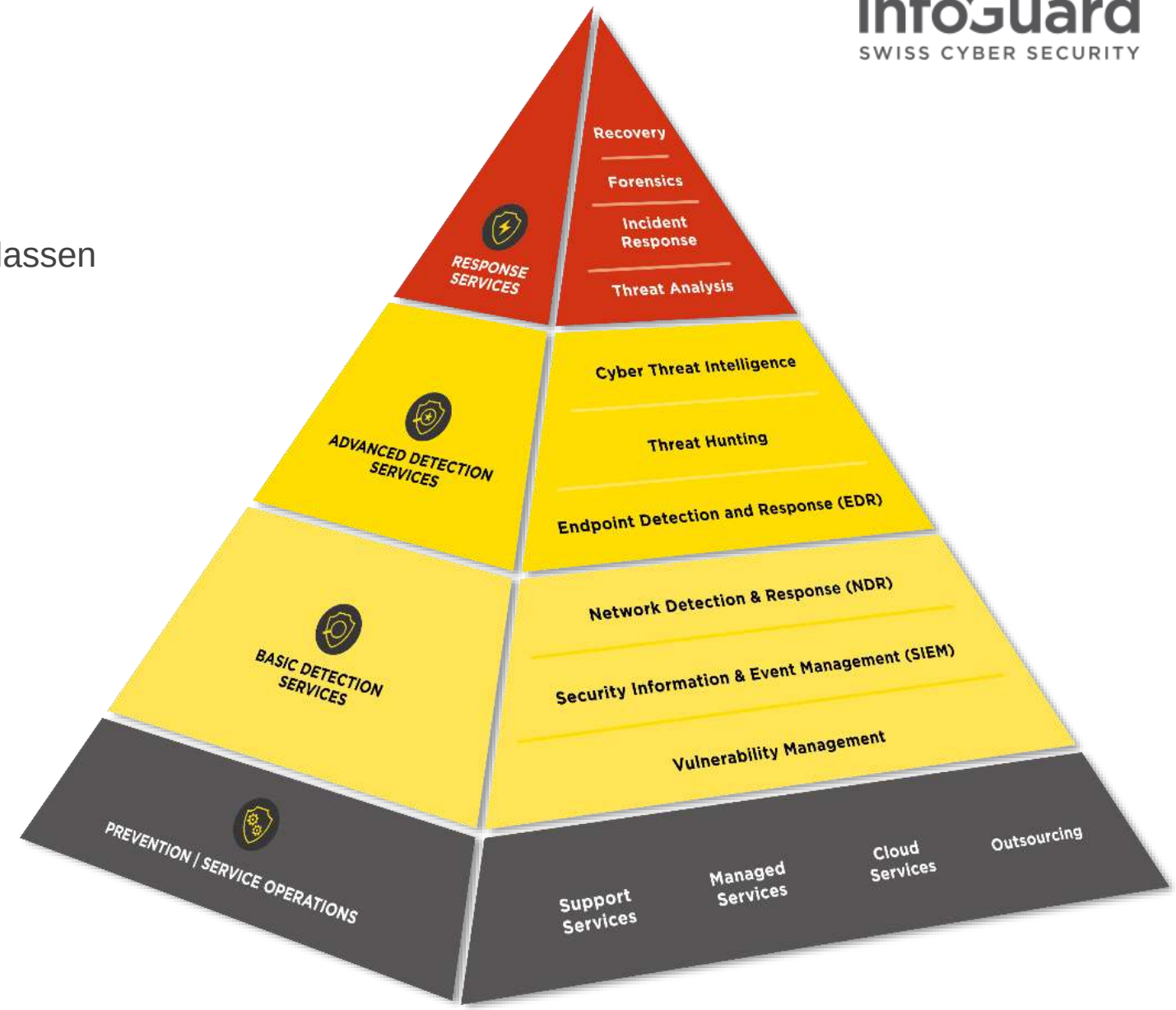
- Don’t google
- Als Favoriten hinzufügen
- Separates Benutzerprofil
- Lang dauernde Sessions abbrechen
- Don’t click that link



FALLBEISPIEL 1: E-BANKING

Schutz für Anbieter von E-Banking-Services

- PhotoTAN Geräte nur via Briefpost authentifizieren lassen
- Ungewöhnliche Referrals
- Lange Session Durations
- Neu hinzugefügte Photo-Tan Geräte?
- TypoSquatting Monitoring - CTI Service ->



FALLBEISPIEL 2: BUSINESS E-MAIL COMPROMISE

DUNKLE WOLKEN AM SECURITY-HIMMEL – KOMPROMITTIERUNG VON AZURE-ACCOUNTS

Veröffentlicht am 05. Okt 2021 | von Stephan Berger | Breach Detection | Cyberrisiken

Das CSIRT der InfoGuard hat in den letzten Monaten verschiedene Cybervorfälle im Azure Umfeld bearbeitet, primär im Umfeld der sogenannten «Business E-Mail Compromise». Mehr dazu im aktuellen Blogartikel von Stephan Berger, Senior Cyber Security Analyst bei InfoGuard.

Was ist Business E-Mail Compromise?

FALLBEISPIEL 2: BUSINESS E-MAIL COMPROMISE – ORIGINAL

[redacted]

Payment for ARA

To Sarah[redacted]

Cc [redacted]

I150773 [redacted].pdf
468 KB

Dear Sarah,

Please organize the payment for ARA invoice as attached.

Best Regards!

Victor [redacted]

ARA ELECTRICAL

ARA Electrical Engineering Services Pty Ltd
ABN: 37 002 436 384

Tax Invoice

To: [redacted]

From: Administration/Accounts Receivable
ARA Electrical Engineering Services Pty Ltd
PO Box 356
UNANDERRA NSW 2526
ABN 37 002 436 384

Invoice No.	Invoice Date	PO No.	Job No.	Payment Terms
150773	26/04/2021	CONTRACT	110740	NET 30 DAYS

JOB DESCRIPTION: [redacted]-Chullora Test F

Attention: Accounts Payable

Works complete at Chullora Test Facility - [redacted]

Subtotal	$39,390.00
GST	$3,939.00
Total	$43,329.00

Payment via EFT: WESTPAC BSB 032-26[redacted]
Payment via credit card: Please call for more details
Remittance to: accounts.receivable@araelect.com.au

FALLBEISPIEL 2: BUSINESS E-MAIL COMPROMISE – FÄLSCHUNG

Subject: Re: Payment for ARA
To: Sarah [redacted]
Cc: [redacted]

Dear Sarah,

Please kindly disregard the invoice i sent in my previous mail for ARA and use the attached invoice for they updated their bank account information. Kindly organize payment in this attached invoice with New updated bank account information and send me mail once paid.

Best Regards!

Victor [redacted]

ARA ELECTRICAL

ARA Electrical Engineering Services Pty Ltd
ABN: 37 002 436 384

Tax Invoice

To: [redacted]

From: Administration/Accounts Receivable
ARA Electrical Engineering Services Pty Ltd
PO Box 356
UNANDERRA NSW 2526
ABN 37 002 436 384

Invoice No.	Invoice Date	PO No.	Job No.	Payment Terms
150773	26/04/2021	CONTRACT	110740	NET 30 DAYS

JOB DESCRIPTION: [redacted] -Chullora Test F

Attention: Accounts Payable

Works complete at Chullora Test Facility - [redacted]

Subtotal	$39,390.00
GST	$3,939.00
Total	$43,329.00

Payment via EFT: COMMONWEALTH BSB 0626 [redacted]
Payment via credit card: Please call for more details

SCHUTZ VOR BUSINESS E-MAIL COMPROMISE

- Mitarbeitenden Awareness
- Überwachen der Risk-Sign-Ins
- MFA (Multi-Factor-Authentication)
- Typosquatting-Überwachung (CTI Service)

Date	User	IP address	Location	Risk state
8/18/2021, 10:14:30 PM	Ines Persico	78.110.164.54	Rugby, Warwickshire, GB	At risk
8/18/2021, 10:14:28 PM	Ines Persico	78.110.164.54	Rugby, Warwickshire, GB	At risk
8/18/2021, 2:25:13 PM	Ines Persico	193.32.210.67	Tockington, South Gloucestershire, GB	At risk

FALLBEISPIEL 3: RANSOMWARE

FALLBEISPIEL 3: RANSOMWARE

Bug Bounty Program

We invite all security researchers, ethical and unethical hackers on the planet to participate in our bug bounty program.
The amount of remuneration varies from $1000 to $1 million.

Web Site Bugs

XSS vulnerabilities, mysql injections, getting a shell to the site and more, will be paid depending on the severity of the bug, the main direction is to get a decryptor through bugs web site, as well as access to the history of correspondence with encrypted companies.

Locker Bugs

Any errors during encryption by lockers that lead to corrupted files or to the possibility of decrypting files without getting a decryptor.

Brilliant ideas

We pay for ideas, please write us how to improve our site and our software, the best ideas will be paid. What is so interesting

Doxing

We pay exactly one million dollars, no more and no less, for doxing the affiliate program boss. Whether you're an FBI agent or a very clever hacker who knows how to find anyone, you can write us a TOX messenger, give us your boss's name, and get $1 million in bitcoin or monero for it.

TOX messenger

Vulnerabilities of TOX messenger that allow you to intercept correspondence, run malware, determine the IP address of the interlocutorand other interesting vulnerabilities.

Tor network

Any vulnerabilities which help to get the IP address of the server where the site is

FALLBEISPIEL 3: RANSOMWARE

- Unsicherer Fernzugang

CITRIX

VPN

- Phishing/Malspam

- Sicherheitslücken

Exchange

VMware Horizon

Confluence

- Supply Chain Attacken

WAS KÖNNEN WIR BESSER MACHEN?

- Patch/Vulnerability Management
- MFA (Multi Factor Authentication)
- AV Alerts
- AD Sanity (PingCastle/Compromise Assessment)
- Keine vertiefte Analyse nach Incident (da war doch schon mal was im 2019?)
- Direkter Internetzugang
- Security Monitoring (EDR/SOC)

SECURITY MONITORING

- Rollout EDR bei Fällen
- 7/24 Security Monitoring

WIR SIND FÜR SIE DA!

InfoGuard
SWISS CYBER SECURITY

CSIRT

7x24 Hotline: +41 41 749 19 99
E-Mail: investigations@infoguard.ch

Please note, that in urgent cases and out of office hours the hotline has to be called.


InfoGuard
SWISS CYBER SECURITY
VIELEN DANK
Stefan Rothenbühler
Principal Cyber Security Analyst
Stefan.Rothenbuehler@infoguard.ch
@rothi83

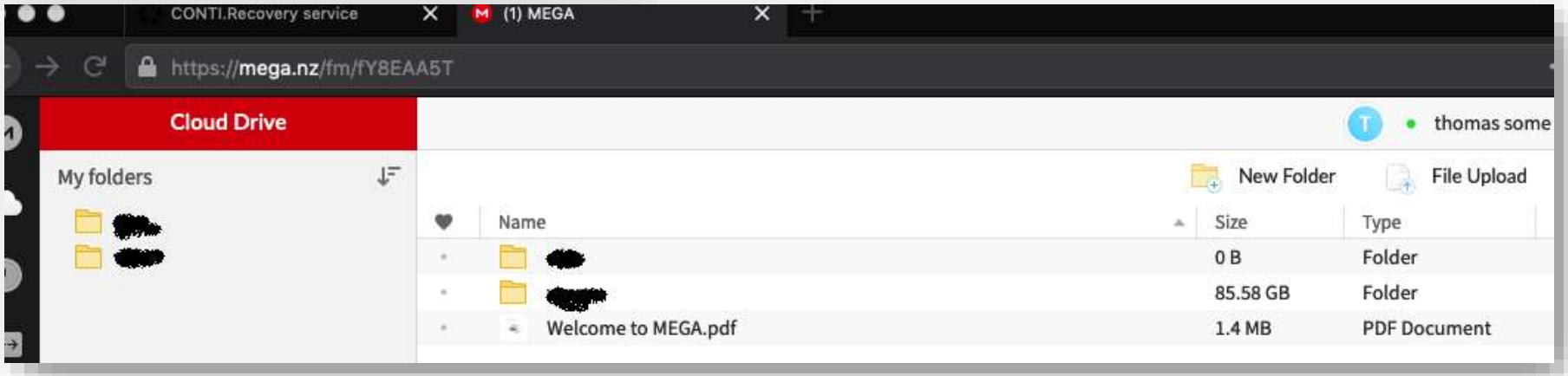
HACKERS HICKUPS

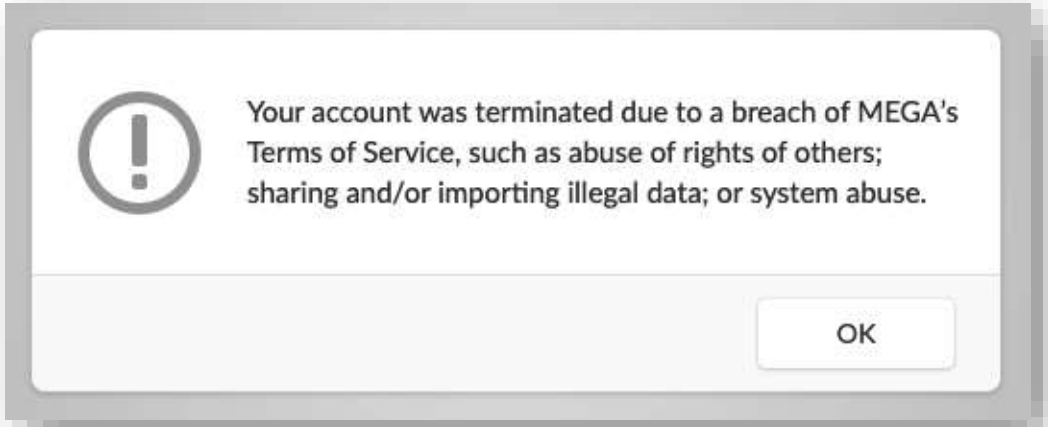
What initial actions were peformed after the incident?

Turned off both notebooks and wrapped them in tinfoil…

YOU LOST YOUR KEYS!

```
type = mega
user = cold_          @protonmail.com
pass = _DG
```





NEGOTIATING…

Bandit

Hi, yes of course. To decrypt your data, you need to pay $ 60,000 in bitcoin

2021-[redacted]6:51:21

we would go as far as 15k

2021-[redacted]18:22:42

We already offered you a 50% discount. 25,000 is the last price.

2021-[redacted]18:23:19

Understand, this is the most we can help you with. We are ready to go as much as $20,000 if paid in XMR

2021-[redacted]18:24:22

… OR NOT

Again I emphasize that your files will not corrupt after decryption.

If you ask for more discount we won't respond to your email anymore.

I told you 0.32048592 BTC is the only accepted price

You have 72 hours to pay and get the decryptor
or the price will be doubled.

Before	Time to end	Now
$ ~~500,000~~	Time is over	100,000 $
~~13.22 (with 25% fee)~~	Price was increased	(with 25% fee) 2.38
~~1664.5~~		317.89