



Introduction to Digital Forensics

COMP 8920 - Computer and
Network Forensics

Lesson 01



Outlines

- Forensics Science
- Digital Forensics
- Cybercrime Case Study
- Digital Forensics Research



Forensics Science



What is Forensics Science?

- Forensic science is a **branch of science**.
- Forensic science is the application of science to law.
- The application of **scientific methods** to establish factual answers to legal problems.
- The use of science and technology to investigate and establish facts in criminal or civil courts.

What does it mean?

History of Forensics Science (1)

Forensic science was established as a separate scientific domain during the 1800s and early 1900s.

1. **Mathieu Orfila (1787–1853)**, considered the father of forensic toxicology, published the first scientific text on forensic toxicology in 1814.
2. **Alphonse Bertillon (1853–1914)** developed a method for identification through body measurements and published a system on personal identification in 1879.

History of Forensics Science (2)

3. **Francis Galton (1822–1911)** studied fingerprints as a means of identification and published the book [Finger Prints](#) in 1892.
4. **Hans Gross (1847–1915)** established the principles for the application of science in investigations in several publications, the first one in 1893.
5. **Alberts S. Osborn (1858–1946)** established scientific principles for [document examination](#) and published the book *Questioned Documents* in 1910.

History of Forensics Science (3)

6. **Leone Lattes (1887–1954)** studied characteristics of **blood types** for identification and created a method for the analysis of blood groups in blood stains in 1915.
7. **Edmond Locard (1877–1966)**, recognized worldwide for promoting the **scientific method in criminal investigation**, established a police laboratory in Lyon in 1910.

Locard's Exchange Principle

- Edmond Locard formulated the famous Locard's exchange principle, which has served as an important principle for subsequent research within forensic science.
- The principle states that *"when a person or object comes in contact with another person or object, a cross-transfer of materials occurs"* (Saferstein, 2007).
- This means every criminal can be connected to a crime through trace evidence.

Locard's Exchange Principle

“Whenever two objects come into contact with one another, there is an exchange of materials between them.”

Does that principle hold for digital forensics?

NO the principle cannot necessarily be directly applied to digital forensics, as the dynamics of digital evidence is different from that of physical evidence.

Crime Reconstruction

- Crime reconstruction (or [crime scene reconstruction](#)) is the process of [determining the most likely hypothesis, or sequence of events, through the application of the scientific method.](#)
- Crime reconstruction is the determination of the actions and events surrounding the commission of a crime. [Crime Reconstruction by Chisum and Turvey (2008)]
- A crime reconstruction can leverage a wide range of [forensic methods](#), for example firearm ballistics tests, statistical simulations, and biological experiments.

Investigations

- An investigation is a **systematic examination**, typically with the purpose of identifying or verifying facts.
- A key objective during investigations is to identify key facts related to a crime or incident.
- There are many methodologies to conduct a forensics investigation.
- A common methodology is the **5W+H methodology**

5W+H Forensics Investigation Methodology

5W+H defines the objectives of an investigation as who, where, what, when, why, and how.

1. **Who:** Persons involved in the investigation, including suspects, witnesses, and victims
2. **Where:** The location of the crime and other relevant locations
3. **What:** Description of the facts of the crime in question
4. **When:** The time of the crime and other related events
5. **Why:** The motivation for the crime and why it happened at a given time
6. **How:** How the crime was committed

Evidence Dynamics

- Evidence dynamics refers to any influence that adds, changes, relocates, obscures, contaminates, or obliterates evidence, regardless of intent.
- The concept is useful in understanding the actual behavior of evidence and plays an important role in crime scene reconstructions.
- **Example:** evidence dynamics can describe the mechanisms for writing to a sector on a hard drive, or the operations for creating, changing, or deleting a file in a file system.



Digital Forensics



Digital Forensics

- The collection, preservation and analysis, of digital evidence derived from digital sources for the purpose of enabling the reconstruction of events found to be criminal.
- It is the application of forensics science in the digital domain
- It is the examination of digital storage and environments in order to determine what has happened.
- It is important to understand that digital forensics is not limited to investigating cybercrimes | digital crimes.

Digital Forensics

A more comprehensive definition

The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations

Cybercrimes

- Is any crime that involves a **computing device** (PC, Mobile, Smart Vehicle) and a **communication network**.
- Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense. [Techopedia]
- **Examples:** Ransomware attacks, RAT attacks (remote access trojan), etc.

Why Digital Forensics?

Digital forensics generally has two uses:

1. Understanding how the crime/incident was conducted helps in preventing similar crimes in the future, improve security and safety measure, identify weakness and vulnerabilities.
2. Collect digital evidences and establish evidence integrity for the the use in the court of law.

Digital Forensics Mode of Operations

In general, there are two mode of operations in digital forensics

1. After-the fact forensic analysis (often referred to as post mortem).
2. Real-time detection of cybersecurity incidents (e.g., intrusion detection) or as part of security incident handling processes.

Does that also apply in forensics analysis in general?

Digital Devices, Media, and Objects

Digital Device is a physical object, such as a laptop, a smartphone, usb stick, or a car (smart car).

Digital Media is part of a digital device that store digital or binary data, such as a hard drive, main memory (RAM), or any other media storage.

Digital Object is any collection and representation of digital data stored on a digital media (e.g. email messages, audio files, images, word files, etc).

Forensic Soundness and Evidence Integrity

An investigation is forensically sound if it adheres to established digital forensics principles, standards, and processes.

Evidence integrity refers to the preservation of evidence in its original form.

Chain of custody refers to the documentation of acquisition, control, analysis, and disposition of physical and electronic evidence.

Digital Evidence

Digital evidence is defined as any digital data that contains reliable information that can support or refute a hypothesis of an incident or crime.

In digital forensics, we aim to process and store digital evidence in a way that is consistent with the principles of evidence integrity and chain of custody



Cybercrime Case Study



Online Bank Fraud – A Real-World Example

- Online bank fraud is a well-known crime pattern in which a large number of computers are compromised and infected with Trojan [malware](#), allowing their computers to be monitored and remote controlled.
- The computers are part of a network of infected computers – a [botnet](#) – and typically controlled by one or more [command-and-control](#) centers.

Online Bank Fraud – A Real-World Example

Once established, the botnet is continuously monitored to gather personal information and credentials, and to establish an overview of the online bank accounts accessed by the victims through the compromised computers.

At some point during a regular online bank session, when a victim is active, the command-and-control center issues an instruction to initiate a transaction of a specific amount of money from a victim's account.

Online Bank Fraud – A Real-World Example

The Trojan malware, having circumvented the security of the online banking session, fools the unsuspecting victim to authenticate and authorize the transaction.

When such an illegitimate transaction is completed, an amount of money is transferred to a complicit third party – **a money mule** – whose primary task is typically to withdraw the money and transfer it to a (possibly foreign) account in a jurisdiction that is more forgiving to financial fraud and cybercrime

Operation Emmental: Online Bank Fraud

Finding holes in online banking systems.

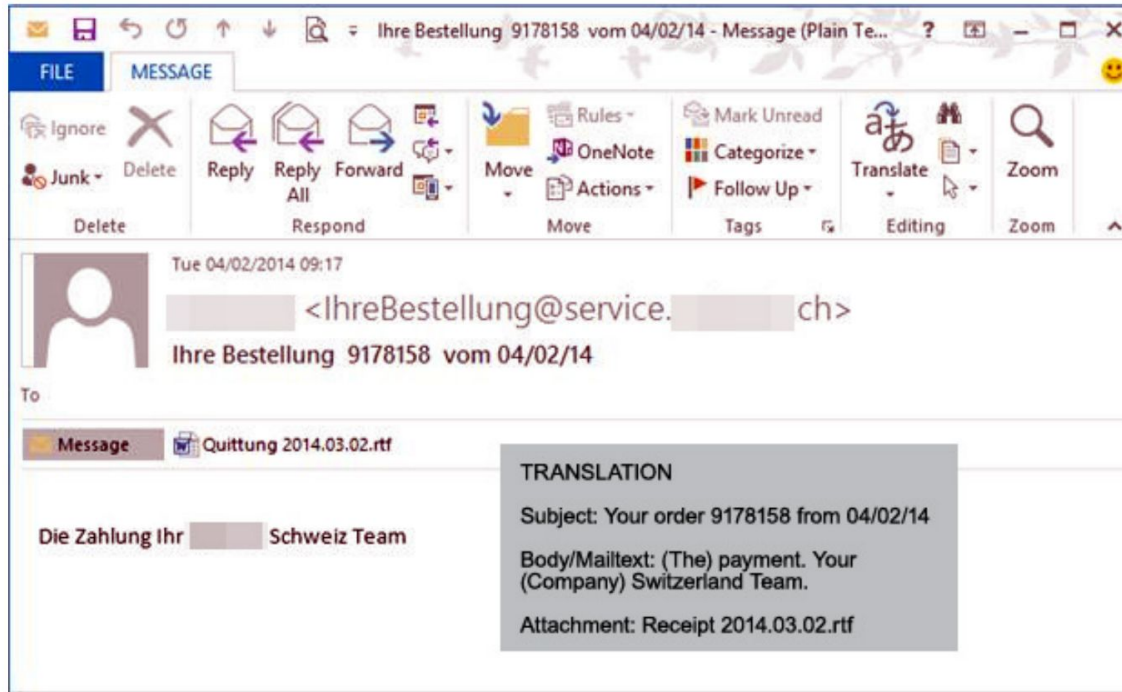


Operation Emmental: Online Bank Fraud

- A group of cyber criminals design and execute an attack against online banking customers.
- The attack uses several malware binaries, spoofing and phishing techniques.
- The attack bypass a two-factor authentication scheme that uses separate channels.
- The victims were customers to banks in Austria, Switzerland, Sweden, and Japan.

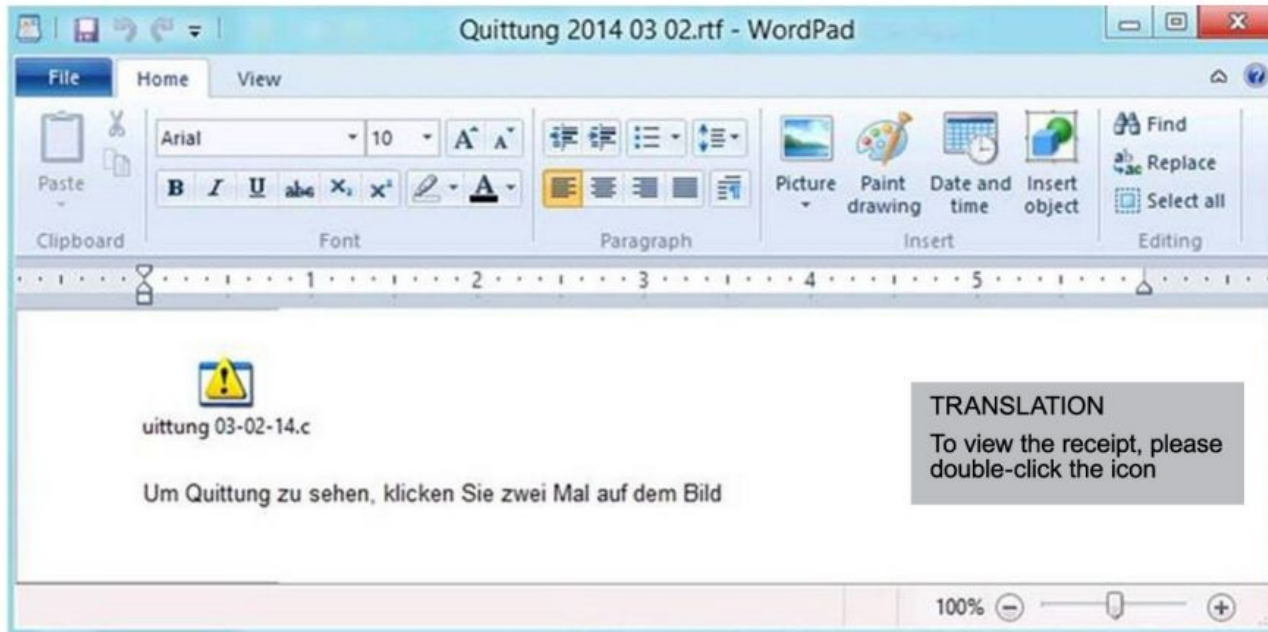
Operation Emmental: Stage One

Compromise the target user machine, using a phishing email message



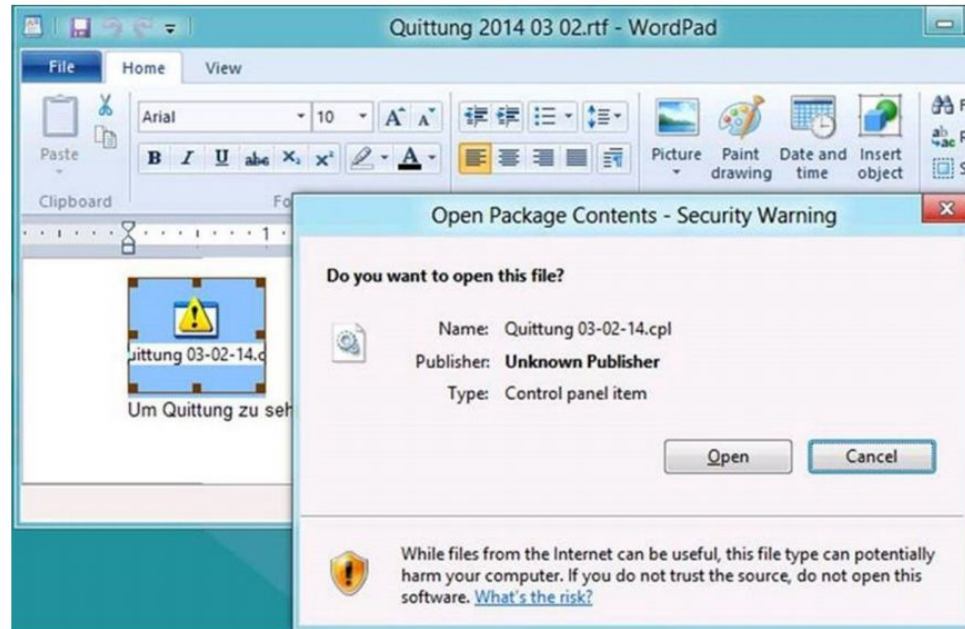
Operation Emmmental: Stage One

Malicious payload in the attached word file.



Operation Emmmental: Stage One

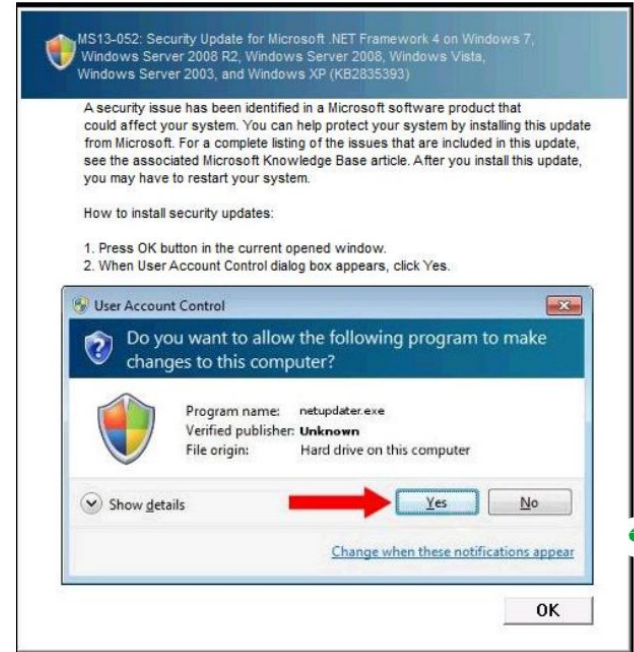
Why the users ignored the warning?



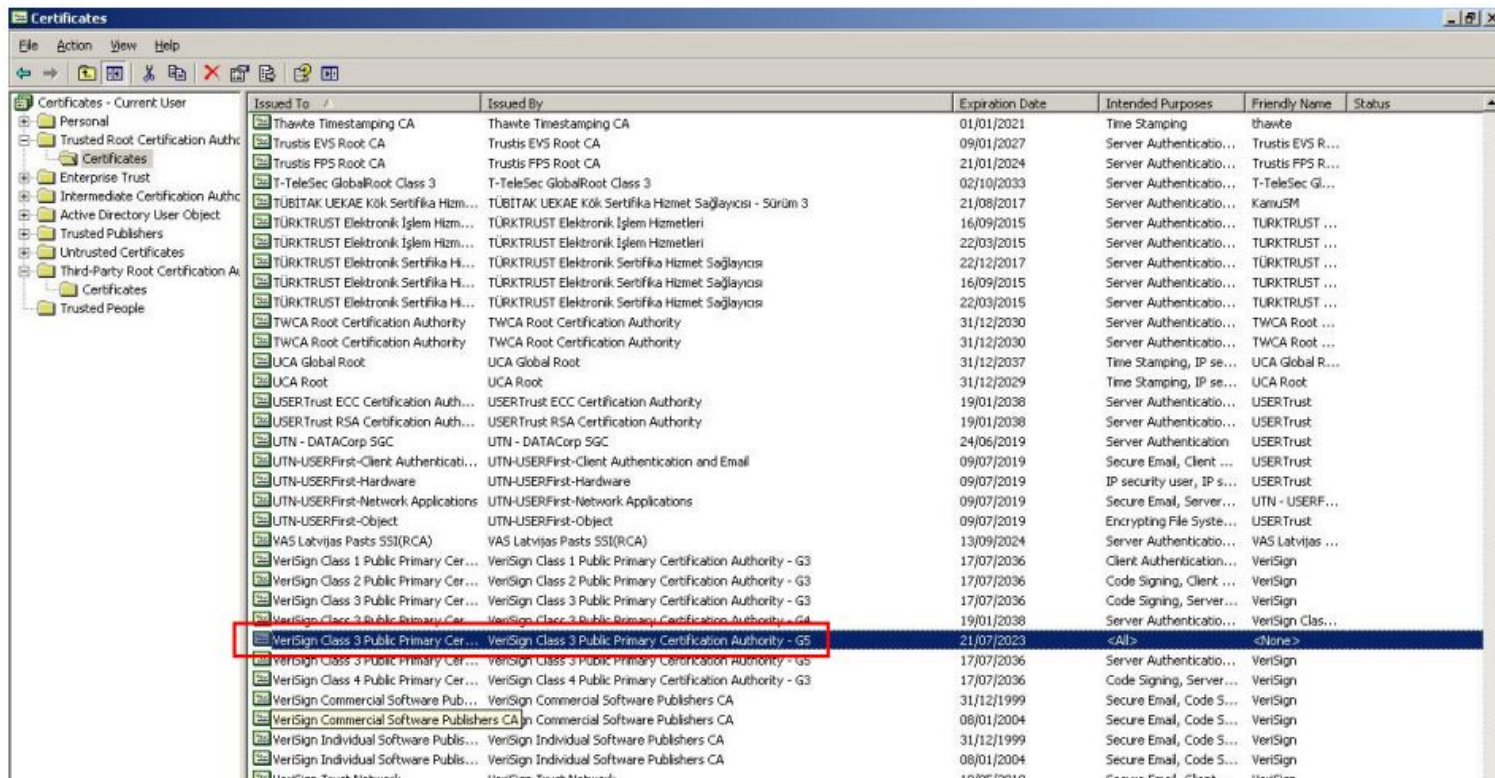
Operation Emmmental: Stage One

The exe file is a malware that will:

1. Changes the system's **Domain Name System (DNS) server** settings to point to one that is under the attackers' control.
2. Installs a new **root Secure Sockets Layer (SSL) certificate** in the infected system.
3. The **malware deletes itself without leaving any trace**, which makes it difficult for users to detect infection after installation.



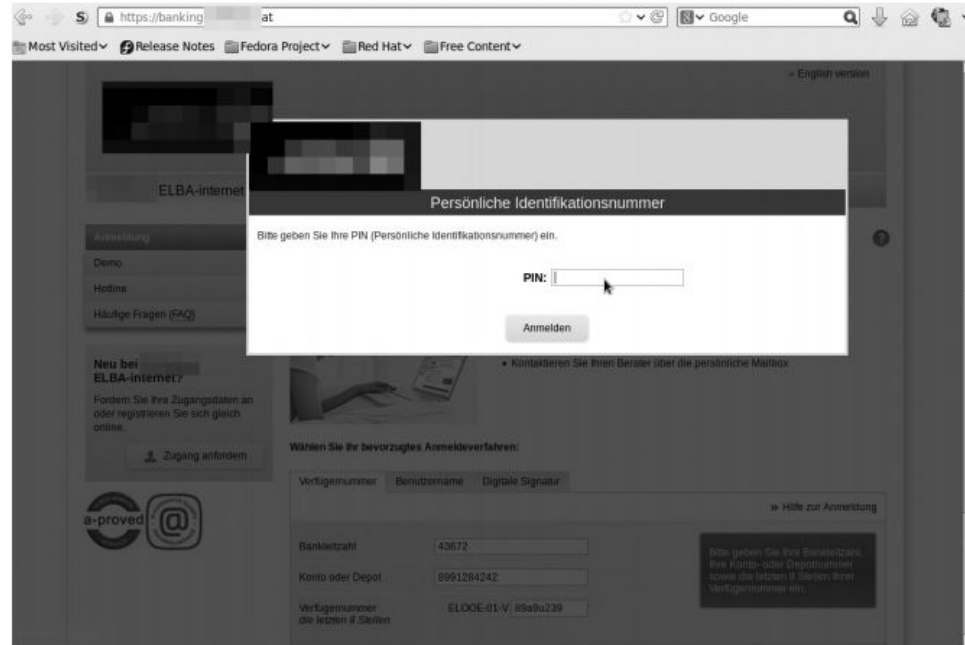
Operation Emmental: Stage One



	Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status
Personal	Thawte Timestamping CA	Thawte Timestamping CA	01/01/2021	Time Stamping	thawte	
Trusted Root Certification Authorities	Trustis EVS Root CA	Trustis EVS Root CA	09/01/2027	Server Authentication...	Trustis EVS R...	
Trusted Root Certification Authorities	Trustis FPS Root CA	Trustis FPS Root CA	21/01/2024	Server Authentication...	Trustis FPS R...	
Enterprise Trust	T-TeleSec GlobalRoot Class 3	T-TeleSec GlobalRoot Class 3	02/10/2033	Server Authentication...	T-TeleSec Gl...	
Intermediate Certification Authorities	TÜBİTAK UEKAE Kök Sertifika Hizmet Sağ...	TÜBİTAK UEKAE Kök Sertifika Hizmet Sağlayıcısı - Sürüm 3	21/08/2017	Server Authentication...	KamuSM	
Active Directory User Objects	TÜRKTRUST Elektronik İşlem Hizmetleri	TÜRKTRUST Elektronik İşlem Hizmetleri	16/09/2015	Server Authentication...	TURKTRUST ...	
Trusted Publishers	TÜRKTRUST Elektronik İşlem Hizmetleri	TÜRKTRUST Elektronik İşlem Hizmetleri	22/03/2015	Server Authentication...	TURKTRUST ...	
Untrusted Certificates	TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı	TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı	22/12/2017	Server Authentication...	TÜRKTRUST ...	
Third-Party Root Certification Authorities	TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı	TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı	16/09/2015	Server Authentication...	TURKTRUST ...	
Trusted People	TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı	TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı	22/03/2015	Server Authentication...	TURKTRUST ...	
	TWCA Root Certification Authority	TWCA Root Certification Authority	31/12/2030	Server Authentication...	TWCA Root ...	
	TWCA Root Certification Authority	TWCA Root Certification Authority	31/12/2030	Server Authentication...	TWCA Root ...	
	UCA Global Root	UCA Global Root	31/12/2037	Time Stamping, IP se...	UCA Global R...	
	UCA Root	UCA Root	31/12/2029	Time Stamping, IP se...	UCA Root	
	USERTrust ECC Certification Authority	USERTrust ECC Certification Authority	19/01/2038	Server Authentication...	USERTrust	
	USERTrust RSA Certification Authority	USERTrust RSA Certification Authority	19/01/2038	Server Authentication...	USERTrust	
	UTN - DATACorp SGC	UTN - DATACorp SGC	24/06/2019	Server Authentication...	USERTrust	
	UTN-USERFirst-Client Authentication and Email	UTN-USERFirst-Client Authentication and Email	09/07/2019	Secure Email, Client ...	USERTrust	
	UTN-USERFirst-Hardware	UTN-USERFirst-Hardware	09/07/2019	IP security user, IP s...	USERTrust	
	UTN-USERFirst-Network Applications	UTN-USERFirst-Network Applications	09/07/2019	Secure Email, Server...	UTN - USERF...	
	UTN-USERFirst-Object	UTN-USERFirst-Object	09/07/2019	Encrypting File Syste...	USERTrust	
	VAS Latvijas Pasts SSI(RCA)	VAS Latvijas Pasts SSI(RCA)	13/09/2024	Server Authentication...	VAS Latvijas ...	
	VeriSign Class 1 Public Primary Certification Authority - G3	VeriSign Class 1 Public Primary Certification Authority - G3	17/07/2036	Client Authentication...	VeriSign	
	VeriSign Class 2 Public Primary Certification Authority - G3	VeriSign Class 2 Public Primary Certification Authority - G3	17/07/2036	Code Signing, Client ...	VeriSign	
	VeriSign Class 3 Public Primary Certification Authority - G3	VeriSign Class 3 Public Primary Certification Authority - G3	17/07/2036	Code Signing, Server...	VeriSign	
	VeriSign Class 3 Public Primary Certification Authority - G4	VeriSign Class 3 Public Primary Certification Authority - G4	19/01/2038	Server Authentication...	VeriSign Clas...	
	VeriSign Class 3 Public Primary Certification Authority - G5	VeriSign Class 3 Public Primary Certification Authority - G5	21/07/2023	<All>	<None>	
	VeriSign Class 3 Public Primary Certification Authority - G5	VeriSign Class 3 Public Primary Certification Authority - G5	17/07/2036	Server Authentication...	VeriSign	
	VeriSign Class 4 Public Primary Certification Authority - G3	VeriSign Class 4 Public Primary Certification Authority - G3	17/07/2036	Code Signing, Server...	VeriSign	
	VeriSign Commercial Software Publishers CA	VeriSign Commercial Software Publishers CA	31/12/1999	Secure Email, Code S...	VeriSign	
	VeriSign Commercial Software Publishers CA	VeriSign Commercial Software Publishers CA	08/01/2004	Secure Email, Code S...	VeriSign	
	VeriSign Individual Software Publishers CA	VeriSign Individual Software Publishers CA	31/12/1999	Secure Email, Code S...	VeriSign	
	VeriSign Individual Software Publishers CA	VeriSign Individual Software Publishers CA	08/01/2004	Secure Email, Code S...	VeriSign	
	VeriSign Trust Network	VeriSign Trust Network	10/02/2010	Secure Email, Code S...	VeriSign	

Operation Emmmental: Stage Two

Phishing Online Banking System



Operation Emmmental: Stage Two

Attacking the second factor authentication

https://banking.at/#

Most Visited Release Notes Fedora Project Red Hat Free Content

English version

Installierung der Mobileapplikation. Schritte 2.

1. Installieren Sie die mobile Applikation aus der SMS auf Ihrem Telefon und starten Sie es.
2. Dann werden Sie die Möglichkeit bekommen das Einmalpasswort für den Zugang zu Ihrem Konto zu generieren. Klicken Sie „Passwort generieren“ für die Generierung des Passwortes.
3. Geben Sie das erhaltene Passwort auf dieser Seite ein und klicken Sie auf 'Weiter'.

[Ich habe keine SMS mit dem Link auf Mobilanfrage erhalten.](#)

Einmaliges Passwort, das von der mobilen Applikation generiert ist:

Weiter

Digitale Signatur

Hilfe zur Anwendung

Bitte geben Sie Ihre Bankleitzahl, Ihre Konto- oder Depotnummer sowie die letzten 8 Stellen Ihrer Wohnortnummer ein.

V: 89a9u239

TRANSLATION

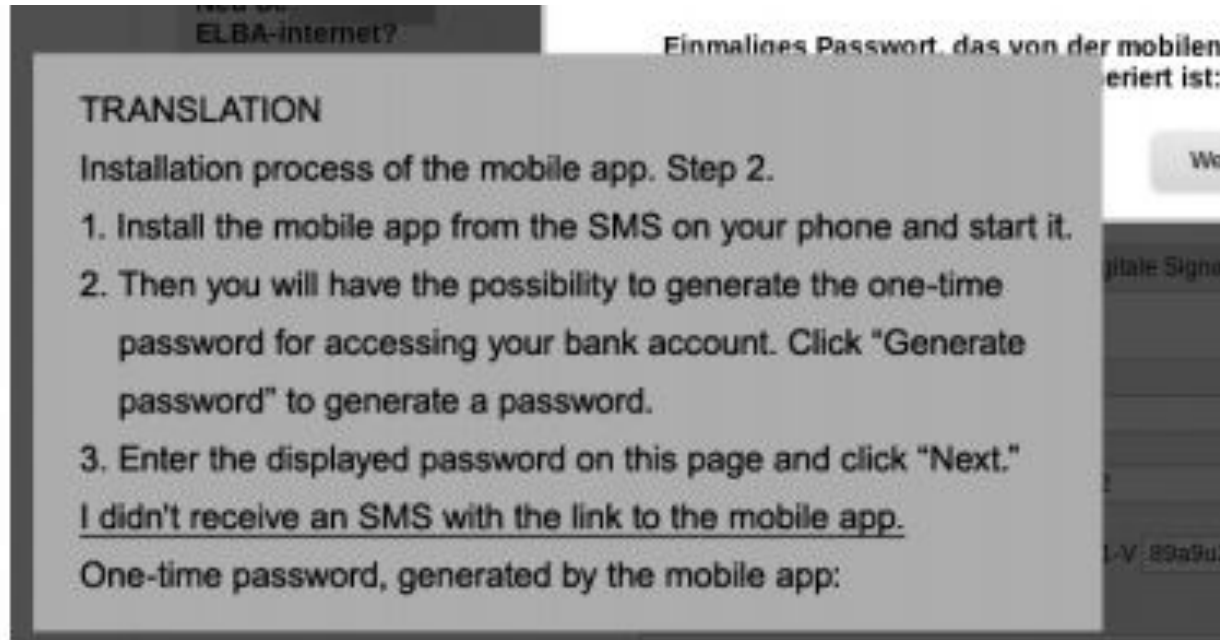
Installation process of the mobile app. Step 2.

1. Install the mobile app from the SMS on your phone and start it.
2. Then you will have the possibility to generate the one-time password for accessing your bank account. Click "Generate password" to generate a password.
3. Enter the displayed password on this page and click "Next."

[I didn't receive an SMS with the link to the mobile app.](#)

One-time password, generated by the mobile app:

Operation Emmental: Stage Two



The screenshot shows a mobile application interface. At the top, there is a header with the text "ELBA-internet?" on the left and "Einmaliges Passwort, das von der mobilen" on the right. Below the header, there is a large grey rectangular overlay containing the following text:

TRANSLATION

Installation process of the mobile app. Step 2.

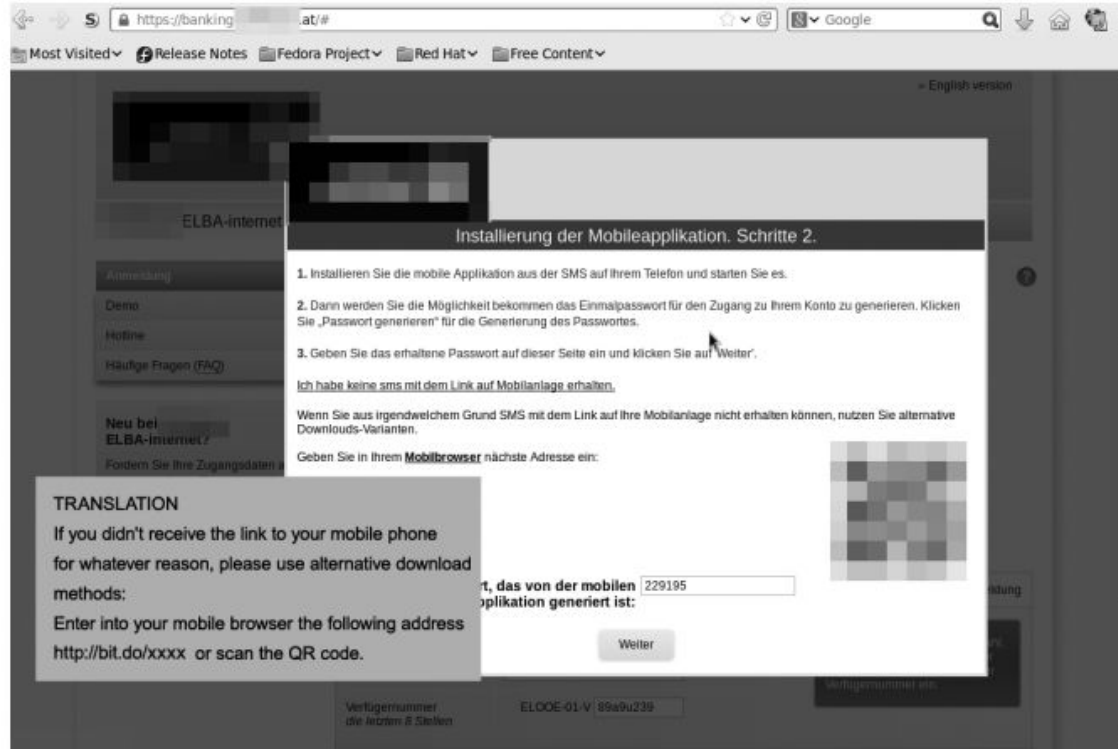
1. Install the mobile app from the SMS on your phone and start it.
2. Then you will have the possibility to generate the one-time password for accessing your bank account. Click "Generate password" to generate a password.
3. Enter the displayed password on this page and click "Next."

I didn't receive an SMS with the link to the mobile app.

One-time password, generated by the mobile app:

On the right side of the screen, partially obscured by the overlay, there is a button labeled "We" and some text including "gitale Sign" and "I-V 89a9u".

Operation Emmmental: Stage Two



https://banking.at/#

Most Visited Release Notes Fedora Project Red Hat Free Content

English version

Installierung der Mobileapplikation. Schritte 2.

1. Installieren Sie die mobile Applikation aus der SMS auf Ihrem Telefon und starten Sie es.
2. Dann werden Sie die Möglichkeit bekommen das Einmalpasswort für den Zugang zu Ihrem Konto zu generieren. Klicken Sie „Passwort generieren“ für die Generierung des Passwortes.
3. Geben Sie das erhaltene Passwort auf dieser Seite ein und klicken Sie auf „Weiter“.

[Ich habe keine sms mit dem Link auf Mobilanlage erhalten.](#)

Wenn Sie aus irgendwelchem Grund SMS mit dem Link auf Ihre Mobilanlage nicht erhalten können, nutzen Sie alternative Downloads-Varianten.

Geben Sie in Ihrem **Mobilbrowser** nächste Adresse ein:

229195

Weiter

TRANSLATION

If you didn't receive the link to your mobile phone for whatever reason, please use alternative download methods:

Enter into your mobile browser the following address

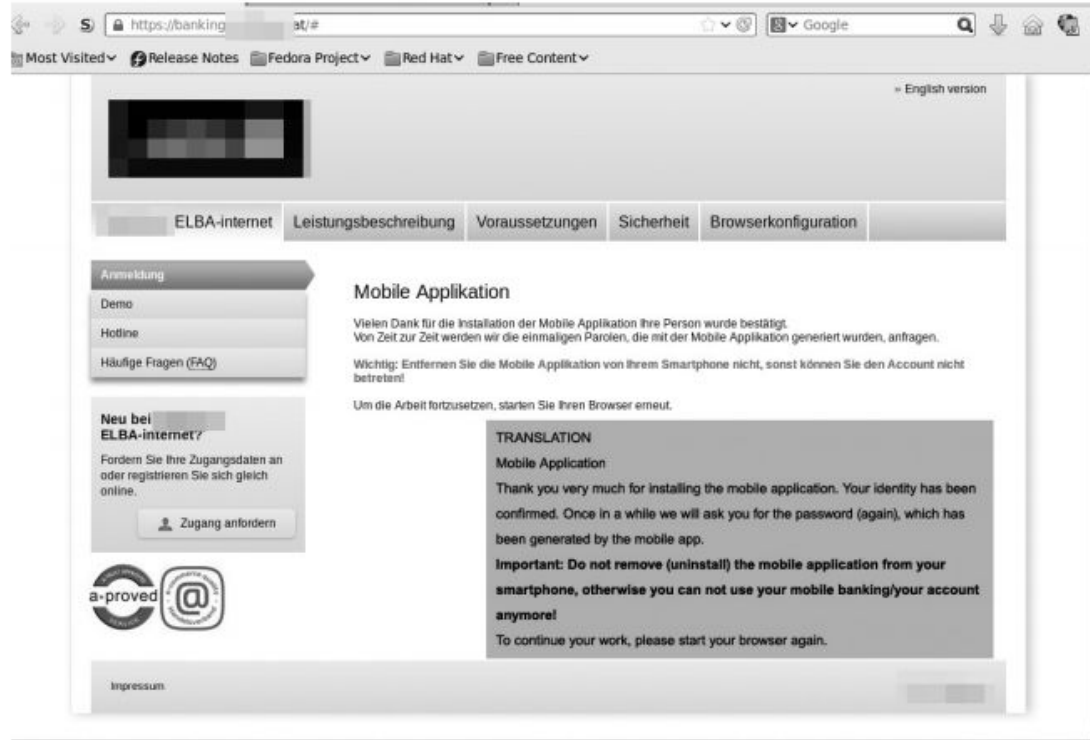
http://bit.do/xxxx or scan the QR code.

Verfügungnummer der Anzeigen 8 Stellen

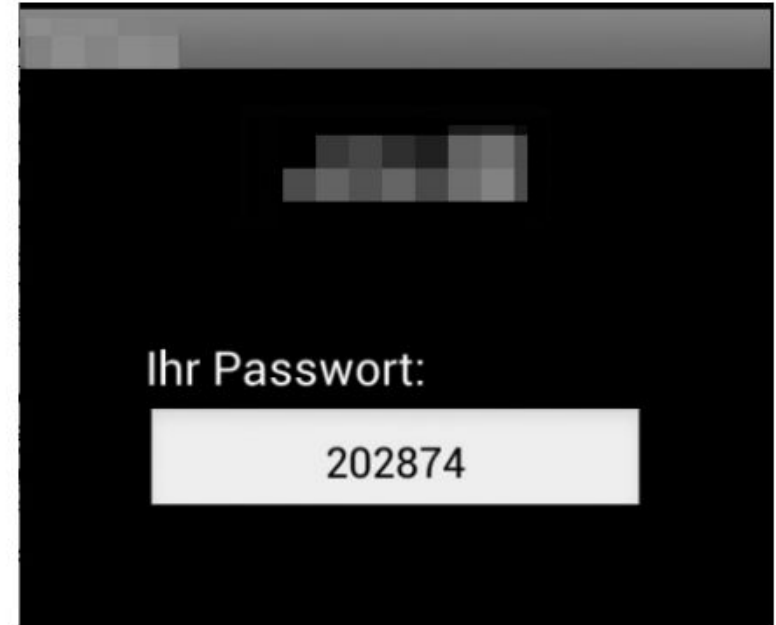
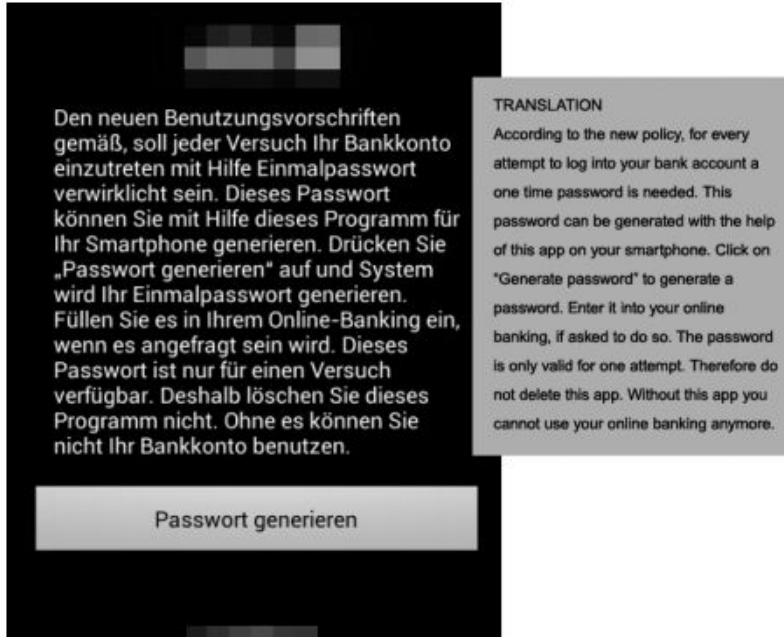
ELOOE-01-V 89a9u239

Verfügungnummer ein.

Operation Emmmental: Stage Two



Operation Emmmental: Stage Three



Operation Emmental: Stage Three

1. Every time the victim tries to access his online banking. He is directed to the fake online bank website.
2. The attacker send a login request to the victim online bank website. The bank send the PIN code to the victim mobile device via SMS message.
3. The malware (mobile app) intercept the SMS and send the PIN code to the attacker and delete the SMS.
4. The attacker gains access to the victim online bank account, preform money transfer to other accounts.
5. The attacker redirect the victim to the actual online banking account.



Research Directions



Research Directions

1. Volume and Scalability
2. Intelligent Analytical Approaches
3. Non-Standard Computing Environments
4. Forensic Tool Development.
5. Forensics Ready Digital Systems.
6. Anti-Digital Forensics Approaches

Summary

In this class we covered:

- Forensics Science
- Digital Forensics
- Cybercrime Investigation Example
- Research Directions

Note: Make sure to read the reading materials posted on the course website.

What is Next?

In our next Class we will focus on the Digital Forensics Process and the research challenges related to it

References

1. Notes by André Årnes from the Testimon Forensic Laboratory, Norwegian University of Science and Technology (NTNU), Gjøvik, Norway; and Telenor Group, Oslo, Norway
2. David Sancho, Feike Hacquebord, and Rainer Link Forward-Looking Threat Research Team, Trend Micro.
3. Nicole Beebe, DIGITAL FORENSIC RESEARCH: THE GOOD, THE BAD AND THE UNADDRESSED