advact
advise & act

Ransomware

The «good», the bad and the ugly.

Alain Keller
Security Consultant, Penetrationtester
advact AG

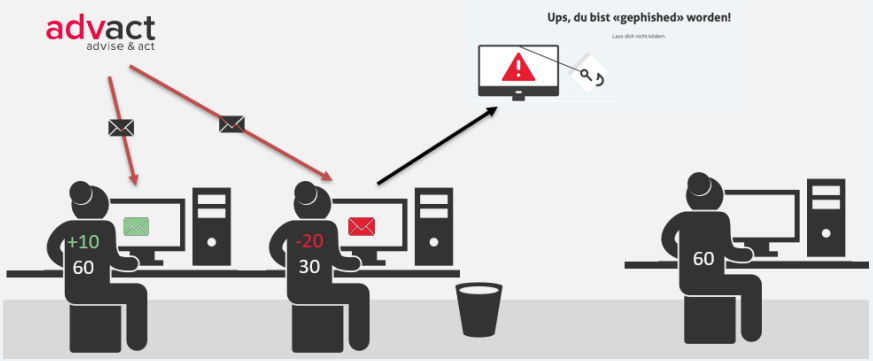
Who am I?

What is advact doing?

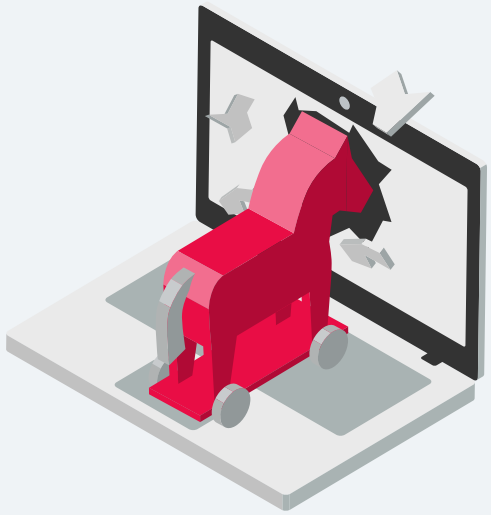
advact.ch
phishingservice.ch
phishingreporter.ch

advact AG

- Phishing Simulations
- Phishing Button
- Phishing Response Service



- Penetrationtests
  - Internal / External
  - Web-Applications
- Audits
- Ransomware Readiness



CLINT EASTWOOD

THE GOOD THE BAD and THE UGLY

Content

- Introduction / The Bad
  - Current situation Worldwide & Switzerland
  - “Facts and Figures“
- Attack Flow / Impact / The Ugly
  - Cyber Kill Chain ®
- Preparation / The Good
  - Technical
  - Organizational
  - Procedural
- Questions

INTRODUCTION

CURRENT SITUATION

THE BAD

Ransomware Example

Extortion - optional

- No encryption but exfiltration of data

- Important Company Secrets, Customer Data, User Data etc.

- Pay or release the information
- Ransom with Cryptocurrency

➔ First Ransomware & then Extortion?

advact
advise & act

Ransomware-Report: Schweizer Angriffe April 2021 bis Mai 2022

Von Philipp Anz,Thomas Schwendener, 23. Mai 2022 um 14:51

Mai 2022

Arztpraxis Appenzell: Hacker veröffentlichen erneut sensible Schweizer Gesundheitsdaten

M&R Spedag Group: Grosser Schweizer Logistiker gehackt

April 2022

Zürcher Kleinfirma: Darum kam es in Zürich trotz mehrfacher Warnung zum Ransomware-Vorfall

März 2022

Neuenburger Arztpraxen: Gehackte Arztpraxen – jetzt wird das Ausmass klar

Alterszentrum Dreilinden: Lockbit-Bande greift Innerschweizer Alterszentrum an

Migros: Migros-CIO bestätigt Ransomware-Angriff

Wimmog: Ransomware-Bande nennt gleich zwei neue Schweizer Opfer

Kitas EFAJE: Cyberkriminelle greifen Schweizer Kita-Verband an

Februar 2022

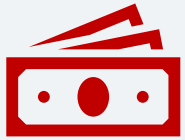
Universität Neuenburg: Nach Cyberangriff – Universität Neuenburg bestätigt Datenabfluss

Swissport: Swissport-Angreifer veröffentlichen Daten

Facts & Figures

advact
advise & act

- > 600M payed in Cryptocurrency 2021
- 180M only from Conti – RaaS
- Ransom range 10K – Millions
- ~ 45% Swiss Companys ever were Ransomwared
- On Average 1.4M CHF total costs (CH)
- 32% payed the ransom (Worldwide)

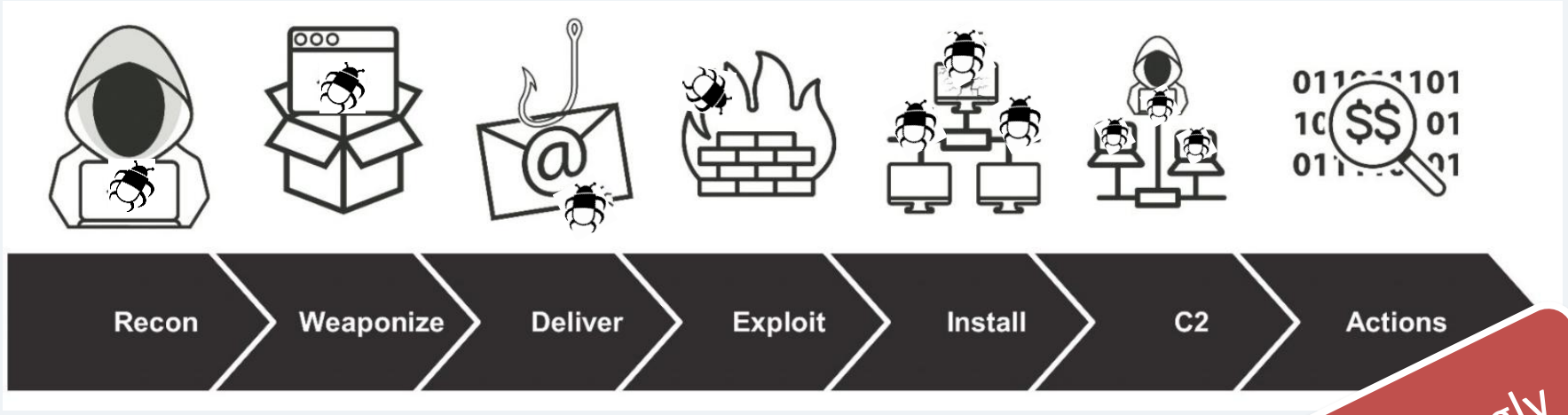


ATTACK FLOW

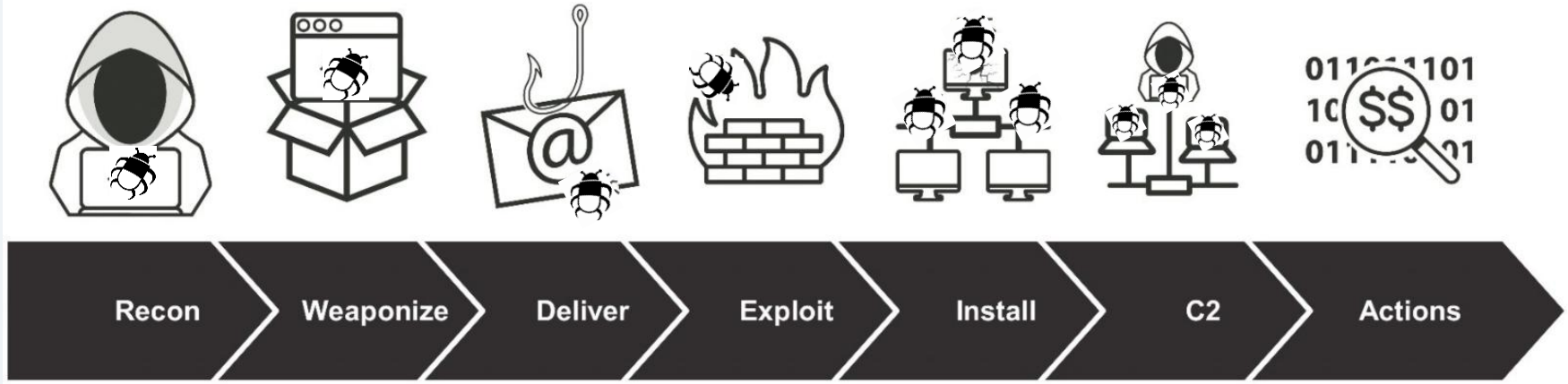
IMPACT

THE UGLY

Cyber Kill Chain®



Cyber Kill Chain®



HOW TO PREPARE?

HOW TO REACT?

THE «GOOD»

The «good»

- Nothing really «good» about Ransomware…
- Companies have to prepare for Cyber Security Incidents
- Preparation helps for general IT & IT-Security emergencies
- «Prepare for the worst, hope for the best…»

- Get help from external Security Professionals

  Hint: No, it is (usually) not your IT Provider 😉

- Cyber Security Industry

NIST – Cybersecurity Framework

Prepare – Identify & Protect

advact
advise & act

- Identify what to protect?
- All «classic» Security Controls like FW, AV, Proxy etc.
- Communication with
  - Management
  - Customers
  - Third-Party (Press? ☺)
- Digital Forensic & Incident Response (DFIR) Service
- Monitoring
- Crisis Management in General / Excercise

Prepare – Detect & Respond

advact
advise & act

- All «new» Security Controls like EDR, NDR, SIEM, SOC etc.
- Involve Police and National Cyber Security Center (NCSC)
- Involve Data Privacy Officer of your canton?
- Think about your Compliance
  - Data Privacy Law
  - GDPR
- Out-of-band communication
- Digital Forensic & Incident Response (DFIR) Service
- Monitoring

Prepare – Recover

- Recovery of Backup
  - What data/time/dependecy do we have?
  - Where to backup? Online/Offline/Cloud
    - Immutable Backups?
  - Protected if attacker has domain admin privileges
  - Testing

- Digital Forensic & Incident Response (DFIR) Service
- Regular exercise the restore

Prepare - Help

Additional Informaiton: Informationen für Private (admin.ch)

Report Incident: https://www.report.ncsc.admin.ch/de/chat

Your local Police

NoMoreRansom: https://www.nomoreransom.org/

SUMMARY & QUESTIONS

Summary

- Prepare on a technical, organizational and procedural level
- Regularly exercise the emergency
- Use a Security Professionals for Pentesting your Environment
  - Internal & External Penetrationtest
- Use Security Best Practices
- Awareness of Users
  - Especially **Mail (Attachements / Links / Phishing...)**
  - Communication on LinkedIn/XING etc.

Questions?

Alain Keller
Security Consultant
Penetrationtester

alain.keller@advact.ch

Sources

- https://www.inside-it.ch/ransomware-report-schweizer-angriffe-april-2021-bis-mai-2022-20220523
- https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf
- https://assets.sophos.com/X24WTUEQ/at/k4qjqs73jk9256hffhqsmf/sophos-state-of-ransomware-2021-wp.pdf?cmp=120469
- https://www.washingtonpost.com/politics/2022/03/18/11-big-takeaways-conti-ransomware-leaks/
- Pictures: https://www.techtag.de/it-und-hightech/it-security/cyber-kill-chain-it-infrastruktur/attachment/traditional-cyber-kill-chain/
  Pictures: https://www.nist.gov/cyberframework