Emotet

Inga Scheler (TU Kaiserslautern)

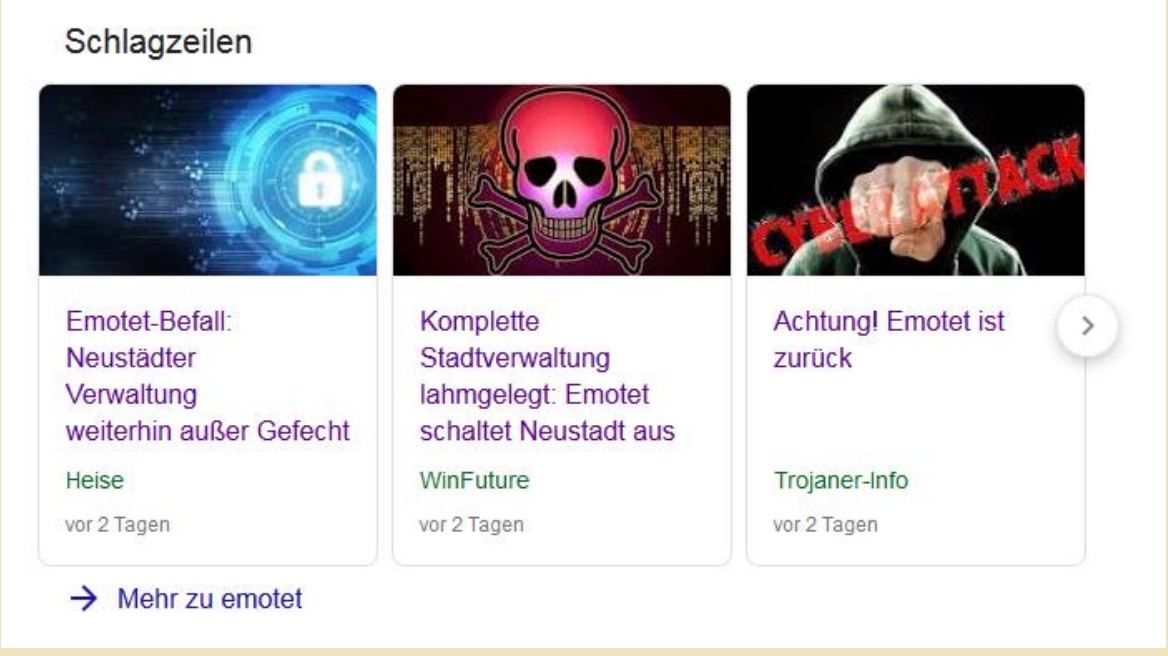
Andreas Bischoff (Uni Duisburg-Essen)

Marius Mertens (Uni Duisburg-Essen)

Inhalt

- **Was ist Emotet?**
  - Fähigkeiten und Verbreitung
  - Ablauf der Infektion
  - Erkennung und unmittelbare Reaktion
- **Nacharbeiten und weitere Maßnahmen**
  - Reparatur und Härtung der IT
  - Organisatorische Maßnahmen
- **Retrospektive**
  - Lessons learned
  - Empfehlungen

Was ist Emotet?



Google-Suche „Emotet“ vom 19.9.2019

Was ist Emotet?

- Bekannt seit 2014
- Eigentlich Banking-Trojaner
- Polymorph → Signaturbasierte V
- Sandboxerkennung
- Modularer Aufbau
  - Trickbot: Bankingtrojaner
  - Mimikatz: Stiehlt Kerberos-Tic
    Achtung: 2FA hilft dagegen nic
    (Neukompilierung für jeden mö
- Command & Control Server für
- Exfiltration von Kommunikations
- Distributions-Framework: Mail, F g, PW-Bruteforce, Schwachstellen (Ete
- Atombombe für die Hosentasch

Ablauf der Infektion an der UDE

TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

UNIVERSITÄT DUISBURG ESSEN
Offen im Denken

UDE

≤2018: Diverse Phishing-Wellen, immer wieder .doc-Dateien mit Malware, immer wieder Opfer trotz vielfältiger Aufklärung, mal Emotet (Phase 1), mal Anderes

November 2018: Sperrung der Legacy-Office-Formate geplant

23.11.2018: IT-Ausschuss

22.02.2019: IKM-Vorstand

11.03.2019: IKM-Fachkonferenz

22.03.2019: IKM-Kommission

14.05.2019, 15:43 Uhr: Emotet Phase 2!!!

TUK

Dezember 2018:

Warnung der Mitarbeiter vor der ersten Emotet-Welle, keine spürbaren Auswirkungen an der TUK

Dienstag 14.5.19:

Mitarbeiter meldet "diverse Phishing E-Mails“, Meldung deutet nicht auf einen besonderen Vorfall hin

Ablauf der Infektion an der UDE

TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

UNIVERSITÄT DUISBURG ESSEN
Offen im Denken

UDE

TUK

Dienstag 14.05.19:

15:55 Uhr: Erste Meldung weiterer Posteingänge durch Nutzer an CISO

15:55 Uhr: Aktivierung ZIM-CERT durch CISO

16:08 Uhr: Vorbereitung Warnmeldung (Sicherheits-RSS-Feed)

16:32 Uhr: Warnmeldung aktiv

17:15 Uhr: Weitere Spam-Meldungen, „Patient 0“ aus Phase 1 identifiziert

17:55 Uhr: Patient 0 wird unabhängig von weiterer Zielperson informiert

Ablauf der Infektion an der UDE

TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

UNIVERSITÄT DUISBURG ESSEN
Offen im Denken

UDE

Mittwoch 15.05.2019:

Einleitung der Überprüfung des PCs von Patient 0. Keine Infektion auffindbar, Rechner wird neu aufgesetzt

10:24 Uhr: Anfrage Datenschutz: Meldepflichtiger Vorfall?

TUK

Mittwoch 15.05.19:

13.48 Uhr: verstärkt treten Viren auf, die per E-Mail hereinkommen

15:05 Uhr: 5 Accounts nachweislich verseucht

15:10 Uhr: Es ist klar dass „Viren als E-Mail Anhang“ hereinkommen, Text der E-Mails = Kopien realer E-Mails, Aussehen der E-Mail wie reale E-Mail Antwort => Empfängern wird eine reale Antwort suggeriert

-> Vermutung Emotet

Ablauf der Infektion an der UDE

TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

UNIVERSITÄT DUISBURG ESSEN
Offen im Denken

UDE

TUK

Mittwoch 15.05.19:

15:25 Uhr: Versand einer Info-E-Mail an alle TUK-Angehörigen über eine Rundmail

-> Sensibilisierung zur Begrenzung des Befalls

15:43 Uhr: Kontaktaufnahme mit DFN-CERT

-> Problembeschreibung, Anfrage von Unterstützung hinsichtlich Virendefinition und Massnahmen

Ablauf der Infektion an der UDE

TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

UNIVERSITÄT DUISBURG ESSEN
Offen im Denken

UDE

TUK

Mittwoch 15.05.19:

16:30 Uhr: Terminalserver der Verwaltung werden heruntergefahren. Re-Boot am folgenden Tag mit einem sauberen Image

-> Eindämmung der Auswirkungen

16:58 Uhr: gesicherte Information: Es ist ein Emotet-Befall

-> Makros in den „.doc“ Dateien laden die Schadsoftware „Emotet“ nach

Ablauf der Infektion an der UDE

TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

UNIVERSITÄT DUISBURG ESSEN
Offen im Denken

UDE

TUK

Mittwoch 15.05.19:

21.26 Uhr: Erste Anweisungen an alle Mitarbeiter des Rechenzentrums zum Umgang mit infizierten Systemen / Accounts

-> keine Administrator-Passwörter auf Systemen eingeben, die unter Verdacht stehen infiziert zu sein: „Virus hört mit“

Ablauf der Infektion an der UDE

TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

UNIVERSITÄT DUISBURG ESSEN
Offen im Denken

UDE

16.05.2019, 13:25 Uhr: Auswertung und Entscheidung: Vorfall ist meldepflichtig

17.05.2019: Meldung des Vorfalls an das LDI durch den DSB

17.05.2019, 10:49 Uhr: Informationsmail des Personalrates an die Mitarbeiter

22.05.2019: Letzte Mails mit Charakteristiken von Phase 2 erreichen die UDE. 5 Rechner mit abgegriffenen Daten identifiziert und bereinigt

TUK

Ablauf der Infektion an der UDE

TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

UNIVERSITÄT DUISBURG ESSEN
Offen im Denken

UDE

19.06.2019: Rektoratsbeschluss: Legacy-Office-Sperre, Infomail, Schulungen

25.06.2019: (Signierte!) Informationsmail an alle Hochschulangehörigen

01.07.2019: Mails mit Legacy-Office-Dokumenten werden nicht mehr angenommen, der absendende wird Mail nicht los

10.09.2019: Bitte des LDI um aktuellen Stand zum Vorfall

16.09.2019: Phase 3 - Neue Mails mit alten Inhalten und ohne Schadcode erreichen einzelne Mitarbeiter der UDE

TUK

Wie wurde die Infektion bemerkt?

	UDE	TUK
Charakteristische E-Mails mit originalen Mailtexten und Schadcode	X	-
Verschlüsselungstrojaner	-	X
Beschwerde Externer über Spam von uns (auch bei Fake-Absendern)	X	-
Auffällige lokale Netzwerkzugriffe (SMB)	-	X
Verbindungen zu C&C-Servern	-	X

Wie wurde die Infektion behandelt?

	UDE	TUK
Warnung an die noch nicht Infizierten	X	X
Information der Patienten 0	X	-
Schnelle Isolation befallener Rechner	X	X
Befallene Rechner neu aufsetzen	X	X
Strafanzeige	-	X
Meldung LDI	X	X

Wie wurde die Infektion behandelt?

	UDE	TUK
Suche nach SMB-Scans im Kernnetz	-	X
Wechsel der Kommunikation auf Etherpad (Rechenzentrum intern)	-	X
Vorläufige Sperrung von E-Mails mit MIME-Type „application/ms-word“	-	X
Profile betroffener Mitarbeiter löschen	X	X
Alle Passworte „infizierter“ Nutzer zurücksetzen	X	X

Wer war beteiligt?

	UDE	TUK
Rechenzentrum – Mitarbeiter	X	X
Hochschulleitung	-	X
Datenschutzbeauftragter	X	X
Alle Administratoren in den dezentralen Bereichen	-	X
CISO	X	-
CERT-lokal	X	-
DFN-CERT	-	X
Rechenzentrum Goethe-Uni Frankfurt	-	X

Vorbeugende Maßnahmen

- Personaldezernentin mit S-MIME-Zertifikat ausgestattet
  - Vorbildfunktion
  - Stark verbreitete S-MIME-Signatur in der Hochschulverwaltung
- Crypto-Partys in den Abteilungen der Hochschulverwaltung
- **Infomail durch RZ-Leiter an alle Hochschulangehörigen**
  - **Sperrung der Legacy-Office-Formate**
  - **Phishing-Warnung**
  - **Information über meldepflichtigen Datenschutzvorfall**
- **Sperrung der Legacy-Office-Formate (allerdings nicht sofort, sondern erst nach erneutem Gremien-Lauf per Rektoratsbeschluss)**
- Verpflichtende Awareness-Schulung für alle Mitarbeiter
- Nicht vergessen: Auch von mittlerweile bereinigten Rechnern wird die abgegriffene Kommunikation weiterhin für Angriffe verwendet!

- **Mögliche Zustände „nach“ Emotet**
  - Wir haben unser AD neu aufgesetzt und alle alten Rechner entsorgt
  - Wir haben offensichtlich befallene PCs neu installiert und die Nutzer haben ihre Passwörter geändert
  - Ähhh, Lasagne?

Emotet – Fragen „Heute“

-> Gibt es eventuell noch „Schläfer“?

Es sind keine sicheren Kriterien bekannt, um herauszufinden, ob Emotet auf einem System aktiv ist oder nicht.

-> Haben „Dritte“ Zugriff auf IT-Systeme?

Es ist unklar ob Passwörter „abgegriffen“ wurden.

Lessons learned

- **Auswirkungen der Maßnahmen**
  - **Trotz intensiver Information sind nicht alle Nutzer informiert**
  - Mails werden nicht gelesen
  - RSS-Feed wird nicht gelesen
  - Ca. 1 Monat nach Scharfschaltung der Sperre:
    Wenige „Meckerer“, aber sehr intensiv mit teilweise persönlichen Angriffen
  - Begründungen:
    - **Alte Formate werden zwingend benötigt**
    - **Zusammenarbeit mit externen Wissenschaftlern sonst nicht möglich**
    - „Sicherheit“ sei nett, die Maßnahme aber völlig überzogen
    - „Mir ist noch nie etwas passiert“
    - Versuch, Sonderregelungen durchzusetzen

Lessons learned

- **Auswirkungen der Maßnahmen**
  - **Trotz intensiver Information sind … informiert**
  - Mails werden nicht gelesen
  - RSS-Fe… nicht gelese…
  - …
  - **Z… benöt… mö…**
  - „Sicherheit“ sei nett, die Maßnahm…
  - „Mir ist noch nie etwas passiert“
  - Versuch, Sonderregelungen durchzu…

Keiner wusste das. Als "Entsetzen" kann man die Reaktion der Kollegen bezeichen, vor allem auf die Tatsache, dass Sie mit niemanden in der geisteswissenschaftlichen Fakultät gesprochen haben

Ich beschreibe diese Situation deswegen in Detail, damit Sie wissen, welche negative Folgen Ihre Entscheidung hat. Ich wiederhole: eine Entscheidung, die Sie getroffen haben, ohne ein einziges Wort mit den Betroffenen zu wechseln.

Dass Sie und Ihre Gremien eine solche folgenschwere Entscheidung getroffen haben, ohne ein Wort mit den Betroffenen gewechselt zu haben, finden wir für Sie beschämend.

Empfehlungen – technisch

- ALLE Passwörter, die auf befallenen Rechnern jemals benutzt wurden, ändern (auch gespeicherte Passwörter im Browser)
- 3-Tier-Adminkonzept für AD
- Diversität in der IT hilft
- Datensicherung hilft immer
- Administratoren: Desaster Recovery vorbereiten und üben

KEIN BACKUP?
KEIN MITLEID!

Empfehlungen – organisatorisch

- **Lokales CERT**
- **Nutzer melden Spam und Phishing an spezielle E-Mail-Adresse**
- **Kommunikationskanal zu den Nutzern**
  - Mehrsprachig
  - Sicherheits-RSS-Feed (wird von dezentralen Admins sogar gelesen) mit u.a. regelmäßigen Spam-Warnungen
  - Website
  - (Massen-)E-Mail ist problematisch, wenn dann nur signiert
- **CISO**
- **Informationssicherheitsrichtlinie**
- **Dezentrale Informationssicherheitsbeauftragte**
- **Sensibilisierungsmaßnahmen – notfalls verpflichtend**

Empfehlungen – organisatorisch

- **Weg definieren einheitliche Maßnahmen durch Admins durchsetzen**

-> nicht alle Windows Systeme sind im zentralen AD, zum Teil Admins unbekannt bzw. nicht vorhanden, veraltete Informationen

- **Nutzer via eduroam oder in Studentenwohnheimen können nicht leicht erreicht werden**

-> Sperren der Accounts und Netzwerkdosen und warten, dass Nutzer sich melden.

- **DFN CERT in kritischen Situationen einschalten**
- **Das Ganze hat richtig (!!!) viel Arbeitszeit gekostet.**

Empfehlungen und Fazit

- **Meldewege vorbereiten, kommunizieren, üben**
  - Spamverdacht? Nutzer => IT
  - Bedrohungslage? IT => Nutzer
- **Technisches**
  - Security by Design
  - Diversität nutzen
- **Durchführung von Maßnahmen**
  - Rückhalt bei Leitung und Gremien suchen => Es gibt immer Widerstand
  - Befugnisse und Verantwortlichkeiten im Vorfeld regeln
- **Empfehlungen für Leiter**
  - Sicherheitsmaßnahmen mittragen und vertreten (auch gegen chronische Meckerer)
  - Auf das Sicherheitsteam hören, bevor es wehtut

Empfehlungen und Fazit

- **Sicherheitskultur**
  - Erkenne deinen Feind
  - Sei kein Teil des Problems
  - Organisationsstruktur vorhanden?
- **Mehr DFN-weite Kooperation**
  - Besseres Verständnis des Angreifers
  - Frühwarnsystem
  - Information zu übernommenen Accounts

Ausblick: Emotet war erst der Anfang, die Atombombe für die Hosentasche wird für jeden Angreifer verfügbar
Neue Anwendung für Passwortklau: Übernahme aller Nutzeraccounts (Mail, Cloud, soziale Medien) und Freigabe gegen Bitcoins
Weitere Angriffsvektoren: Übernahme von IoT und Smartphones