Emotet

Wie moderne Trojaner unsere IT-Sicherheit bedrohen

Thomas Schwab

Ransomware

Viren und Würmer kennen wir bereits vor den 90er

- Seit 1985 sind Computerviren bekannt
- Sie treten immer mehr in den Hintergrund
- Eine E-Mail mit normalen Viren erkennt heute fast jeder Virenscanner

Von Ransomware geht mittlerweile eine sehr große Gefahr aus

- Insbesondere Verschlüsselungstrojaner bereiten uns Sorgen
- Emotet dient uns heute als Beispiel eines sehr komplexen Trojaner

… aber vorher ein kleiner Ausflug in die Historie der Malware

Entwicklung der Malware

- Theoretische Betrachtung seit späte 1940er
- Brain-Virus (1986) aus Pakistan – Bootsektor
- AIDS-Trojaner (1989) – erste nennenswerte Ransomware
- DOS-Viren (ab1990) – Tequillavirus, Michelangelo
- Würmer (ab 2000) – Loveletter (I-love-you-Virus)
- Trojaner – Stuxnet (2010 Angriff auf SCADA)
- … und nun ein Einblick in die Infektionswege von Ransomware

Wie infiziert sich mein Computer?

Trotz Virenscanner kann sich ein Computer infizieren

Die Ursachen hierfür sind heutzutage meistens:

- E-Mail – Anhang
  (vermeintliche Office-Dateien oder Updates)
- Malicious Links – Schädliche Links
- Exploit-Kits – Sammlung von Exploits
- Auto-Run bei Wechseldatenträger
  (eher unwahrscheinlich)

Emotet

True Story über den Verlauf eines Trojaner-Befalls

Wer oder Was ist Emotet?

- Emotet ist kein ägyptischer Pharao sondern ein fieser Trojaner
- Die Grundform wurde zuerst im Sommer 2014 in Deutschland, Österreich, Schweiz und USA gesichtet
  - Entstammt der Feodo Trojaner Familie
  - (Cridex/Dridex or Bugat) machten mit e-Banking Betrug Schlagzeilen
  - Stand 15.09.2018:
    Feodo botnet C&Cs tracked: 1736 C&C
    davon ca. 90 online, Rest offline

Wer oder Was ist Emotet?

- Emotet funktioniert über die Jahre – bis heute gleich
- Emotet ist ein sehr komplexer Trojaner
- Er verbreitet sich über bösartige Dokumente oder Links in einer E-Mail, z.B. als PDF-Rechnung getarnt
  - Typischerweise E-Mail Anhänge oder Malicious Links
  - Versuch, über Exploits den angegriffenen Rechner zu übernehmen

Wie komplex ist EMOTET?

- Er greift direkt in die Netzwerkkommunikation ein
  - Überwachung des Netzwerkverkehrs infizierter PCs
  - Ableitung sensibler Daten, z.B. Online-Banking
  - Zudem einnisten in Adressbüchern, um DOS-Angriffe gegenüber Dritten auszuführen
- Er ist modular aufgebaut und kann flexibel angepasst werden
- Er ist sehr raffiniert
- Er ist in erster Linie ein **Dropper**

Exkurs: Dropper

- Dropper sind Verbreitungs-Tools
- Sie dafür sorgen, dass Viren auf Computer gelangen
- Zuerst nistet sich der Dropper auf einem Computersystem ein
- Der Dropper ist der eigentliche Trojaner
- Der Dropper ist „nur“ Transportmittel für den Schadcode
- Eine Form, die keine Spuren hinterlässt und nur den Speicher manipuliert nennt sich Injector

Wie komplex ist EMOTET?

- Er hat ein eigenes Kommunikationsprotokoll (basierend auf Google Protobuf)
- Er bringt einen eigenen Webserver mit
  - Web-Server in Libevent geschrieben
- Er besitzt eine Verschlüsselung auf OpenSSL-Basis
- Er erkennt virtuelle Umgebungen

Emotet fliegt unter dem Radar

- Er lädt regelmäßig (alle 30 Minuten) Updates von sich selbst
- Nach dem Update ist er für die Meisten AV-Lösungen unsichtbar
- Selbst neueste AV-Techniken nach mathematisch-statistischen Erkennungsmuster tun sich schwer
- EMOTET verbreitet sich in einem Befallenen Netz über den WDUS „Windows Defender Update Service“
- EMOTET kann unterschiedliche Payload haben

Wer oder Was ist Emotet? – Hauptfunktion

- Emotet ist ein Dropper, der sich und die Module (Payload) aktuell hält
- Emotet aktualisiert sich selbst in hoher Frequenz
- Emotet sammelt Informationen über den Computer auf dem er läuft
- Emotet arbeitet mit IP-Adressen für die Kommunikation mit den C&C-Server
- Die Kommunikation ist mit zufälligen AES-Schlüssel gesichert
- Die Gefahr steckt letztlich in den geladenen Modulen
- Der Installationsumfang wird mit Hash-Werten abgeglichen

Muster eines Emotet-Angriffs – Teil 1

- Die Malware wird mit Spearfishing Techniken verteilt
  - Zielgerichtete Angriffe auf Behörden oder Unternehmen
  - E-Mails an ausgewählte Personen
  - Alternativ wären mit Exploit-Code präparierte Webseiten möglich
- Auf Basis von Office Dokumenten z.B. Word Dokument
  - Beim Öffnen wird ein Makro ausgeführt – Word ist nicht aktuell, bitte updaten …
- Beim Klick auf „Aktualisieren“
  - Natürliche kein Word-Update
  - Sondern laden eines Downloaders = Erstinfektion mit **TRICKBOT**

Exkurs: TRICKBOT 1/3

Entdeckt vom IBM X-Force-Security-Team

- Wahrscheinlich ab 2014 aktiv, wo es mehrere 10 Mio. USD ergaunert hat
- Modernste Techniken um den Browser zu manipulieren
- Seit Mitte 2016 umfangreiche Updates und Test der Entwickler
- Bis dahin primär auf australische, britische und kanadische Banken spezialisiert
- Agiert als man-in-the-middle attack zwischen der Kommunikation des Browsers des Opfers
- Primäres Ziels sind Unternehmen und Banken

Exkurs: TRICKBOT 2/3

Anwender austricksen

1. Phising E-Mails
2. Spam-E-Mails
3. Social Engineering
4. Malvertizing

Malware installieren

1. Öffnen des Office Dokuments (Word)
2. Makro verlang Office Update

Kontrolle des PCs

1. Client Zertifikate
2. MiTB Attacke (Men in The Browser)
3. Umleiten des Netzverkehrs über MiTM Server (Men in The Middle)

Exkurs: TRICKBOT 3/3

- Kommunikation mit C&C Servern (Command and Control)
- TRICKBOT wird verwendet für Download von Informationen über das infiltrierte Netzwerk
- TRICKBOT lädt weitere Hacking Tools auf die Systeme
- Die Vorbereitung eines solchen Angriffs dauert mehrere Monate
- EMOTET kann dann voll automatisiert alle PCs und Server einer Domäne übernehmen

Muster eines Emotet-Angriffs – Teil 2

- Der erste befallene Rechner richtet einen befallenen WDUS ein
  - Über den „Windows Defender Update Service“ werden weitere Systeme in der Domäne infiziert
- Ziel: Übernahme des Unternehmensnetzwerks
- Erbeutung der Domain-Admin-Accounts
- **Golden-Ticket-Angriff**
- Jetzt beginnt die Analysephase des Angreifer und dann die Vorbereitung auf den eigentlichen Anschlag

Exkurs: Golden Ticket Angriff 1/4

- Mit Golden Ticket hat man vollen Zugriff auf ALLE Ressourcen einer Windows Domäne
- Der Angreifer fungiert im Namen eine Benutzers – typischerweise als Domänenadministrator
- Sehr schwerer Angriff, erfordert äußerst viel Aufwand
- Kann nur am Domain Controller ausgelesen werden
- Um an das Golden Ticket zu kommen, benötigt man den NTLM Hash des Spezialusers KRBTGT (KeRBerusTicketGrantingTicket)

Exkurs: Golden Ticket Angriff 2/4

- Verwundbare Server sind:
  - Windows 2003 Server
  - Windows 2008 / 2008R2Server
    - Nicht angreifbar, wenn voll gepatcht
- Out-of-the-box sind NICHT angreifbar
  - Aktuelle Windows Server Versionen
    - z.B. 2012 oder 2016

Exkurs: Golden Ticket Angriff 3/4

Wie kann ich mich gegen Golden Ticket Angriff schützen?

- Regelmäßiges Ändern der Kennworts für den KRBTGT Benutzers der Domäne
  - Fertiges Script von Microsoft, aber Vorsicht bei 2003er Domäne
- Keine Domänen Admin Accounts verwenden!
  - Administratoren nutzen den eigenen Benutzeraccount
- Lokale Administration mit Lokalen Administrator Accounts

Exkurs: Golden Ticket Angriff 4/4

Wie kann ich Golden Ticket Angriff erkennen?

- Die Erkennung ist sehr schwierig oder teuer
- Microsoft Advanced Threat Analysis (ATA)
  - Hohe Lizenzkosten je Arbeitsplatz
- Einsatz von SIEM Systemen – Security Information and Event Management
  - Kibana
  - Logstash
  - Security Onion

Emotet – Jüngere Historie - 2017

- Prototyp ist Q2/2017 und Q3/2017 aufgefallen
- Hier wurde ein gesamtes Unternehmensnetzwerk mit über 1.000 Arbeitsplätzen und den Windows Servern infiziert
- Die bis dato unbekannte Malware wurde dabei auf den Rechnern verbreitet
- !!! Infizierte Rechner dienen als Sprungbrett für weiter Infektionen
- Bei dieser Variante war noch keine Payload vorhanden

Emotet – Sommer 2018

- Keine einfache Ransomware-Attacke
- Die Infizierung lief zunächst nach dem beschriebenem Muster
- Dann aber wurden alle Daten verschlüsselt, die Backups gezielt gelöscht oder unbrauchbar gemacht – mit **Bit Paymer**
- Es lagen KEINE Offline-Backup vor
- Unternehmensschaden mehrere Millionen USD
- KEINE Möglichkeit der Fremdentschlüsselung

Muster eines Emotet-Angriffs – Teil 3

Ziel des Angriffs:

- Ermitteln aller Backups und deren Vernichtung
  - Tape Libraries sowie NAS-Systeme betroffen
- Diebstahl des Domain Admin Accounts
  - Mit Hash und Passwort
- Wie kann das passieren?
  - Pass the Hash Angriff gegen das AD
  - Auslesen des Domain Admins auf Server-Anwendungen mit administrativen Rechten

PRAXIS: Angriff mit Trojaner

- Ein personalisierter Trojaner wurde auf ein Testsystem aufgebracht
- Wir schauen uns Live den Angriff an

...

Muster eines Emotet-Angriffs – Teil 4

Zustand nach dem Angriff

- Storage Devices und Virtual Tape Libraries wurden überschrieben oder gelöscht
- Ransomware wurde in der gesamten Domäne verbreitet

Super-GAU:

Unternehmen komplett verschlüsselt!

Keine Backups verfügbar!

Muster eines Emotet-Angriffs – Teil 5

Was kommt danach?
Nach Entschlüsseln und Wiederherstellen aller Systeme

- Dekontamination aller Unternehmensressourcen
- Analyse der Infektionswege und Beseitigung der Schwachstellen
    - Einsatz von Unterschiedliche Spezialisten
        - Computer Forensiker / Netzwerk Forensiker = Spezialisierte Forensiker = **Teuer**
    - Einrichtung eines Emergency Teams

Fazit: Die Wiederherstellung des Betriebs ist um ein vielfaches teurer als das gezahlte Lösegeld

Exkurs: Bit Paymer 2017

```
YOUR COMPANY HAS BEEN SUCCESSFULLY PENETRATED!
DO NOT RESET OR SHUTDOWN - files may be damaged. DO NOT TOUCH this file.
All files are encrypted. We accept only bitcoins to share the decryption software for your network.
Also, we have gathered all yout private sensitive date. So if you decide not to pay anytime soon, we would share it with media's.
It may harm your business reputation and the company capitalization fell shrply.

Do not try to do it with 3rd-party programsm files might be damaged then.

Decrypting of your files is only possible with the special decryption software.
To receive your private key and the decryption software please follow the link (using tor2web service):

        https://fjkfllkjl345789.onion.to/order/[redacted]

If this address is not available, follow these steps:
        1. Download and intall Tor Browser: https://torproject.org/projects/torbrowser.html.en
        2. After successful installation, run the browser and wait for initialiszation.
        3. Type in the address bar: http://fjkfllkjl345789.onion.to/order/[redacted]
        4. Follow the instructions on the site
        5. This link is valid for 72 hours only. After that period yout local data would be lost completely.
        6. Any question: 765ioiojfjkljflalkja@tutanota.com

KEY: [redacted]
```

Exkurs: Bit Paymer 2018

- Kein fester Betrag für den Entschlüsselungs-Key gefordert
- Kontaktaufnahme zu den Hacker über Anonyme E-Mail Services:
  - z.B. Protonmail, Counter Mail, Hushmail, Mailfence oder Tutanota
- Keine autom. Entschlüsselungstools
- Hohe Geldbeträge werden gefordert
- Bezahlung i.d.R. über Bitcoin durch spezialisierte Unternehmen (US)
  - Full-Service wird angeboten
  - Kommunikation mit Erpresser
  - Bezahlung an den Erpresser

Fazit

Emotet ist gefährlich weil …

- Er über die Dropper-Funktionalität leicht veränderbar ist und daher sehr flexibel eingesetzt werden kann
- Er eine hohe Update-Frequenz besitzt und daher sehr schwer von normaler Virensoftware zu erkennen ist
- Er verschlüsselt kommuniziert und daher nicht abgehört und sehr schwer entdeckt werden kann
- Künftig ist sicherlich mehr mit derartigen Trojanern zu rechnen

Wer sind die Angreifer?

… und …

wollen die überhaupt etwas von mir?

Kategorien von Hacker

Script Kiddies

Geringe Bedrohung

Geringes Know-How

Nutzt fertige Tools

Beispiel

Anonymous Angriffe (DDoS) gegen Amazon, VISA, MasterCard und co.

Hacker Alleine

Bedrohung vom Skill des Hackers abhängig

Hohes Know-How

Teilweise Fortgeschrittene Tools

Beispiel

Diebstahl von Kreditkartendaten bei US-Supermarkt Gruppe Target

Hackergruppe

Spezialisten für diverse Szenarien

Fortgeschrittene Tools

Finanzielle Ausrichtung

Beispiel

Diebstahl von Kreditkartendaten um diese auf Blanko-Karten zu brennen

Professionelle Hacker

Höchste Bedrohung

Hohes Budget (nachrichtendienstlich)

Hoher Spezialisierungsgrad

Uneingeschränkter Zugang zu Tools und Exploits

Motive von Hacker

Finanzielle Gründe

Diebstahl von Informationen

Unternehmenszahlen, Kundendaten oder technische Informationen

Erpressung

Emotionale Gründe

Diebstahl von Informationen

Sabotage

Defacement

Erpressung

Idealistische Gründe

Defacement

Aufklärung

Keine finanzielle Interessen

Politische Gründe

Informations-beschaffung

Manipulation von Infrastrukturen

Beispiele

Tipps für die schnelle Vorsorge …

- Sensibilisieren Sie Ihre Mitarbeiter
  - Social Engineering
    - Phishing Mails/Kurznachrichten oder Webseiten / Spear-Phishing
  - SEO Fraud
    - Ransomware
- Bereinigen Sie Ihre Websites und Internetauftritte
  - Entfernen Sie aus den Dokumenten die Metadaten
  - Am besten keine Office-Dokumente veröffentlichen, sondern nur PDF-Dateien

… kann ich mich gegen all das schützen?

Keine Angst, es muss nicht immer der teure Luxusdampfer sein

- Man kann mit OpenSource Werkzeugen Angriffe erkennen
  - Es können befallene Systeme erkannt und bereinigt werden
  - IDS-Systeme (auch kommerzielle) können Web-Angriffe nicht erkennen, hier werden WAF (WebAppilcationFirewall) benötigt
  - IDS-Beispiel ist Snort oder Suricata
  - Einsatz von Blocklisten an der Firewall
    - Möglich bei z.B. ‚Checkpoint‘ oder ‚Paolo Alto‘
    - nicht bei z.B. ‚Fortigate‘ oder ‚Watchguard‘
- Problem: Aufzeichnung von Mitarbeiterdaten! – Datenschutz!

Wie kann ich einen Angriff erkennen?

- Ziel: Früherkennung eines Angriffs
  - Noch während der Verbreitungsphase über die Kommunikationsmuster

- NSM Sensoren können Angriffe erkennen (**N**etwork **S**ecurity **M**onitoring)
  - z.B. mit Security Onion
    - TRICKBOT: Signaturen und Kommunikation mit den C&C
    - EMOTET: Verbindungsaufbau ins Feodo C&C

Wie funktionieren die IDS Systeme?

Statische oder dynamische Sensoren ?

- Statische Sensoren:
  - Vergleicht die Datenpakete aus dem Netzwerkstrom mit bekannten Angriffsmustern
  - Hier können False-Positives auftreten
  - Für Analyse wird ein sampling Sensor benötigt
- Dynamische Sensoren
  - Überwacht Netzwerk Protokolläufe (TCP / UDP)
  - i.d.R. „teure“ Lösungen - mehrere 100.000 €
  - Günstiger Lösungen sind auch möglich

PRAXIS: IDS-Systeme (Security Onion)

- Wir werden von Snort nicht viel sehen – läuft im Hintergrund
- Wenn von Sensoren bereits Datenströme als PCAP-Files aufgezeichnet wurden können diese zur weiteren Analyse verwendet werden
- Beispiel:
    - PCAP-Files werden wiedergegeben
    - von Snort aufgezeichnet
    - mit Squil und squert visualisiert

...

Vielen Dank für Ihre Aufmerksamkeit