Carsten Eilers | www.ceilers-it.de

Der erste Cyberwar hat begonnen

Stuxnet

Juni 2010

USB-Wurm verbreitet sich über 0-Day-Schwachstelle in Windows: Stuxnet

("Shortcut-Lücke")

Ziel der Angriffe:

SCADA-Systeme von Siemens

Stuxnet

2. August 2010:

Microsoft veröffentlicht Patch

5 Schädlingsfamilien nutzen die Shortcut-Lücke aus

Stuxnet

August 2010:

In SCADA-Systeme wird ein Rootkit eingeschleust

Es werden ganz bestimmte SCADA-Systeme angegriffen

Stuxnet

Außer Shortcut-Lücke 3 weitere 0-Days:

- im Printspooler zur Verbreitung im LAN

- beim Verarbeiten von Tastaturlayouts und
- im Task-Scheduler zur Privilegieneskalation

Stuxnet

November 2010

Stuxnet greift bestimmte Frequenzwandler zweier Hersteller an – einer sitzt in Finnland, der andere im Iran

Änderung der Ausgangsfrequenz ändert Drehzahl der Motoren, für kurze Intervalle und über Monate

Stuxnet

Diese Frequenzwandler werden in Zentrifugen zur Urananreicherung eingesetzt

Vermutliches Ziel:
Irans Urananreicherungsanlage

Stuxnet

15. Januar 2011, New York Times: Stuxnet von USA und Israel entwickelt, um iranische Urananreicherung zu sabotieren

Zwei Schadfunktionen:

- Zerstörung der Zentrifugen
- Täuschung der Überwachung

Stuxnet

Wie kam der Wurm in die Anlage?

Ausgehend von 5 zuerst angegriffenen Organisationen (laut Symantec)

oder

Eingeschleust von einem Mitarbeiter (laut ISSSource und NY Times)

Stuxnet

Stuxnet war erfolgreich:

IAEA-Inspekteure haben Anfang 2010 zerstörte Zentrifugen festgestellt

Stuxnet

1. Juni 2012, New York Times

Angriff 2006 von George W. Bush angeordnet, von Barak Obama fortgeführt

Stuxnet sollte Anlage nie verlassen (Programmierfehler, Änderungen durch Israel)

Duqu

Oktober 2011:

Schädling "Duqu" entdeckt

Wird von F-Secures Backend-System für Stuxnet-Variante gehalten

Duqu

Remote Administration Toolkit (RAT) ohne Verbreitungsroutine

Verbreitung durch gezielte Angriffe

Besitzt wie Stuxnet korrekte Signaturen

Duqu

2. November 2010

Duqu nutzt 0-Day-Schwachstelle im Windows-Kernel zum Eindringen

Wird als Word-Datei per E-Mail verbreitet

Duqu

Weltweit weniger als 50 Ziele,
die meisten im Iran

Darunter u.a. Zertifizierungsstellen

Flame

28. Mai 2012

Iran National CERT (MAHER) meldet
Angriffe über Wurm "Flame"

Gierige digitale eierlegende Wollmilchsau:
Kann alles, sammelt alles

Flame

Flame ist Backdoor, Trojaner, Wurm,

lässt sich über Plugins erweitern

Flame ist gross: 20 MB
AV-Hersteller haben ihn trotzdem lange übersehen

Flame

"Flame is lame"

- nutzt alte Schwachstellen zur Verbreitung
- besteht aus Open Source Software
- kann nichts, was andere nicht auch schon konnten

Flame

Juni 2012

Flame nutzt 0-Day-Schwachstelle in Windows Update zur Verbreitung im LAN

Flame

Der Super-GAU

Schwachstelle erlaubt Schadsoftware, sich durch gefälschte Zertifikate als Microsoft-Update auszugeben

Sehr komplizierte und teure Entwicklung!

Flame

Verbindungen zwischen Stuxnet, Duqu und Flame weisen auf gemeinsamen Urheber hin.

Laut Washington Post wurde Flame von den USA und Israel entwickelt, um Cyber-Angriffe vorzubereiten

Gauss

August 2012

Gauss wird entdeckt – ein staatlicher Onlinebanking-Trojaner

Basiert auf Flame-Plattform

Gauss

Sammelt Daten

Enthält verschlüsselten Schadcode für ganz bestimmte Systeme

Installiert Font "Palida Narrow"

Grund: Unbekannt

Was haben wir damit zu tun?

Bilanz

- Stuxnet: 4 0-Day-Schwachstellen
- Duqu: 1 0-Day-Schwachstelle
- Flame: 1 0-Day-Schwachstelle

Bisher!

Wie Flame und Gauss eingeschleust wurden, ist noch nicht bekannt

Was haben wir damit zu tun?

Es gibt keine "gute Schadsoftware"

0-Day-Schwachstellen werden von Cyberkriminellen genutzt

Schwachstellen können mehrmals entdeckt werden

Was haben wir damit zu tun?

Dazu kommt, dass manche Politiker mal wieder Amok laufen

Bomben gegen Cyberangriffe?

Wer ist der Angreifer?