Universitätsklinikum Tübingen

EK UNICO

IT Security im Gesundheitswesen: Live Hacking – So brechen digitale Angreifer in Ihre Systeme ein

Sebastian Schreiber

Dipl.-Inform. Sebastian Schreiber
Managing Director
+49 7071 - 407856-0
sebastian.schreiber@syss.de

THE PENTEST EXPERTS.

LIVE HACKING

27 Jahre SySS 1998-2025

ZUM UNTERNEHMEN

- 1998: Gründung der SySS GmbH durch S. Schreiber
- Heute: 175 Mitarbeiter
- Sitz in Frankfurt/M., Tübingen, München und Wien, weltweit tätig
- Dienstleistungen:
  - Penetration Testing
  - Incident Response/Forensik/TC/ Schulungen/Auftritte

AGENDA LIVE HACKING

1. Smarte Thermostate knacken
2. Krypto-USB-Drives: Code-Sperre
3. Krypto-USB-Drives: Fingerabdruck-Scanner
4. SMS fälschen
5. Virenscanner überlisten
6. WebShop knacken
7. Angriff auf Alarmanlage
8. Fake-Anrufe
9. Angriff auf Funktastatur
10. Fotos von Android Smartphone stehlen

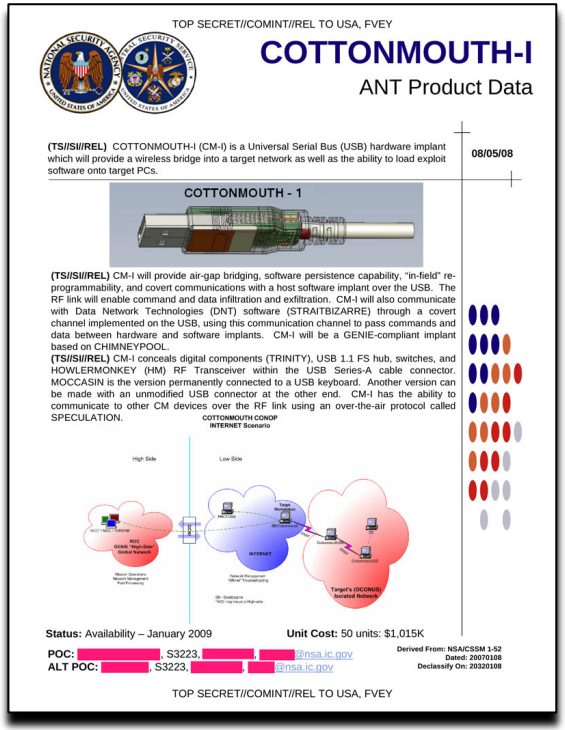
Falls Zeit

1. USB-Tools
2. Trojaner-Angriff gegen Smartphone
3. Übung: QR-Code

WHY TO HACK A THERMOSTATE?

Frühe iOS-Hacks bei SySS

Zeitgleich bei der NSA....



TOP SECRET//COMINT//REL TO USA, FVEY

COTTONMOUTH-I

ANT Product Data

(TS//SI//REL) COTTONMOUTH-I (CM-I) is a Universal Serial Bus (USB) hardware implant which will provide a wireless bridge into a target network as well as the ability to load exploit software onto target PCs.

08/05/08

COTTONMOUTH - 1

(TS//SI//REL) CM-I will provide air-gap bridging, software persistence capability, "in-field" re-programmability, and covert communications with a host software implant over the USB. The RF link will enable command and data infiltration and exfiltration. CM-I will also communicate with Data Network Technologies (DNT) software (STRAITBIZARRE) through a covert channel implemented on the USB, using this communication channel to pass commands and data between hardware and software implants. CM-I will be a GENIE-compliant implant based on CHIMNEYPOOL.

(TS//SI//REL) CM-I conceals digital components (TRINITY), USB 1.1 FS hub, switches, and HOWLERMONKEY (HM) RF Transceiver within the USB Series-A cable connector. MOCCASIN is the version permanently connected to a USB keyboard. Another version can be made with an unmodified USB connector at the other end. CM-I has the ability to communicate to other CM devices over the RF link using an over-the-air protocol called SPECULATION.

COTTONMOUTH CONOP
INTERNET Scenario

High Side | Low Side

INTERNET

Status: Availability – January 2009 **Unit Cost:** 50 units: $1,015K

POC: [redacted], S3223, [redacted], [redacted]@nsa.ic.gov
ALT POC: [redacted], S3223, [redacted], [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

TOP SECRET//COMINT//REL TO USA, FVEY

Unit Cost: 50 Units: $1,015K
Das sind 20.000$ pro Kabel

THE PENTEST EXPERTS

WWW.SYSS.DE