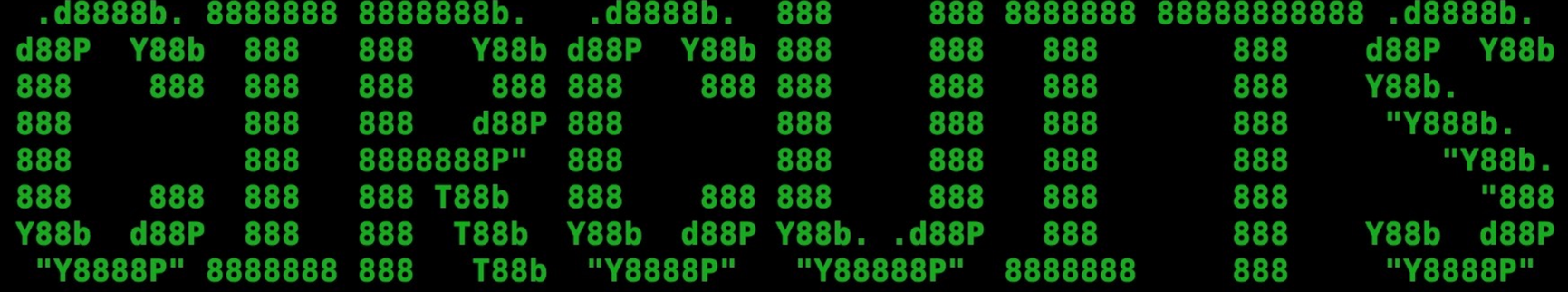


DATANET PROC RECORD: 2SNKY4U Transnet on/xc-3





******** Presented by Joe Grand (@joegrand // grandideastudio.com) ********

[ ] Press Any Key to Begin

GRAND IDEA STUDIO

Sneaky Circuits: An Overview of Hardware-Based Espionage

- Introduction to Hardware Hacking
- Supply Chain / Espionage Threats
- Selected Examples

GRAND IDEA STUDIO

Hardware Hacking Process

- Information Gathering
  - Obtaining information about the target
- Teardown
  - Product disassembly, component/subsystem ID
- Buses & Interfaces
  - Signal monitoring/analysis/emulation/fault injection
- Memory & Firmware
  - Extract/modify/analyze/reprogram code or data
- Chip-Level
  - Silicon die modification/data extraction

GRAND IDEA STUDIO

Approaches

- Attack the hardware directly
  - Find a vulnerability and exploit it for access to system/data
- Attack *with* hardware
  - Mount an attack from the subverted hardware
  - Use hardware as a stepping stone to further attacks
- Implant the hardware
  - Add malicious functionality into an otherwise operable system

GRAND IDEA STUDIO

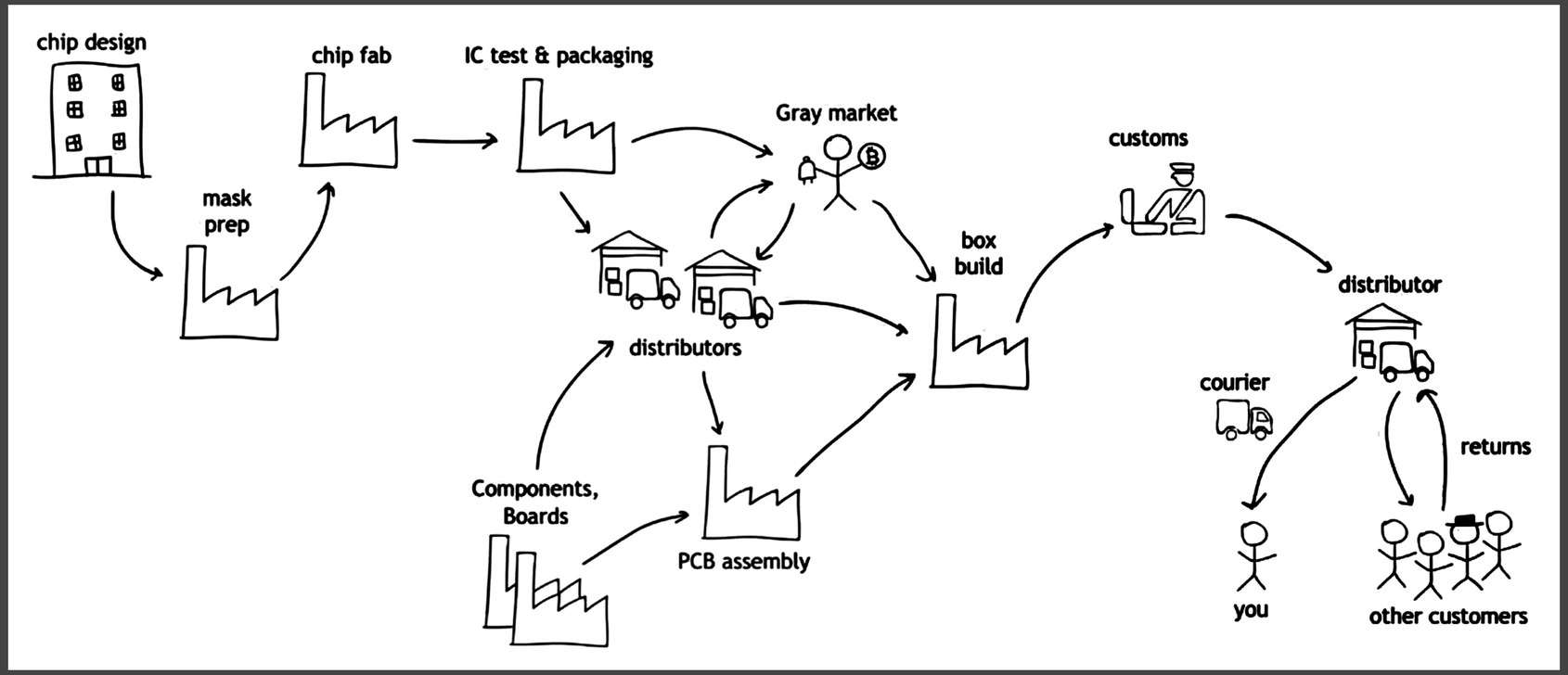
Supply Chain / Espionage

- Not all devices follow the rules
  - Adversary can insert unexpected/alternate behavior
  - Ex.: Create backdoor/remote access, capture/exfiltrate data, manipulate/patch memory, privilege escalation, feature unlocking
- Achieved at any layer of the product
  - Injection point dependent on product/attack goal
  - HW, FW, or SW modification
  - Corrupt/deceived insiders

GRAND IDEA STUDIO

Supply Chain / Espionage 2

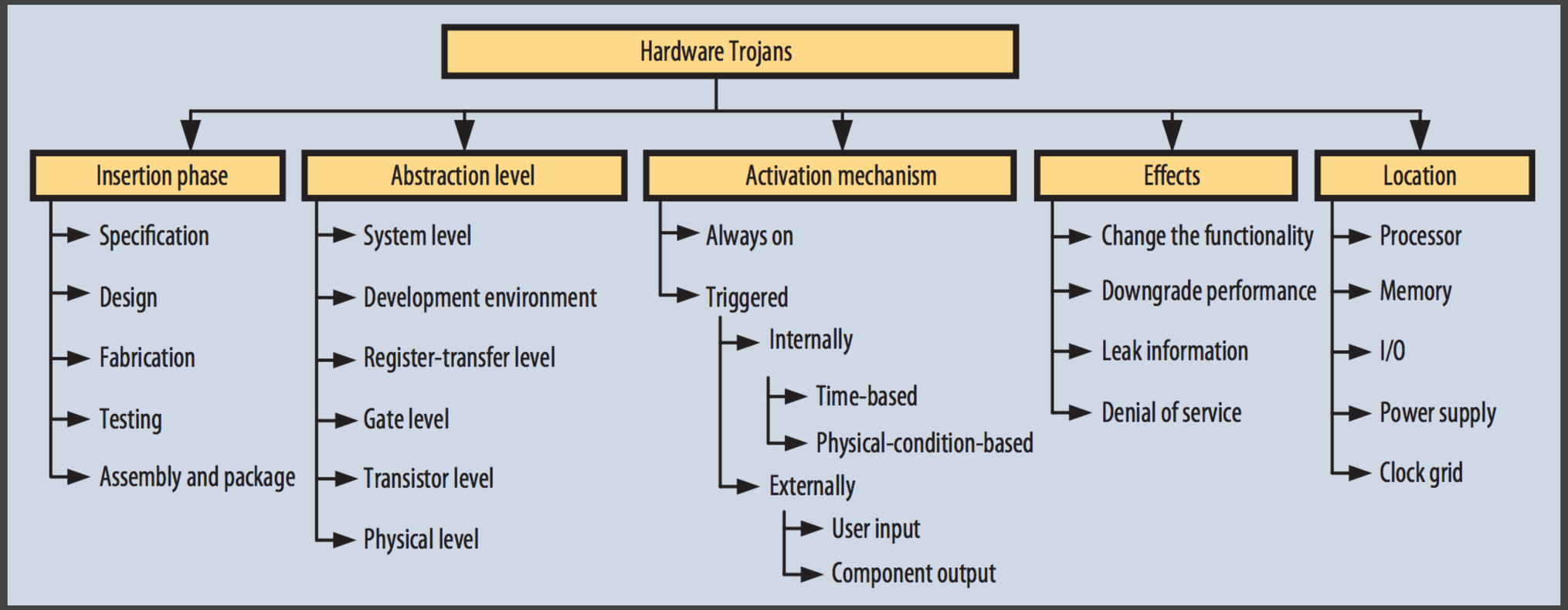
- Could be implemented at any part of the lifecycle
  - Design, fabrication, distribution, storage, integration, in-the-field



Supply Chain Security: If I were a Nation State, Huang, BlueHat IL 2019

GRAND IDEA STUDIO

Supply Chain / Espionage 3

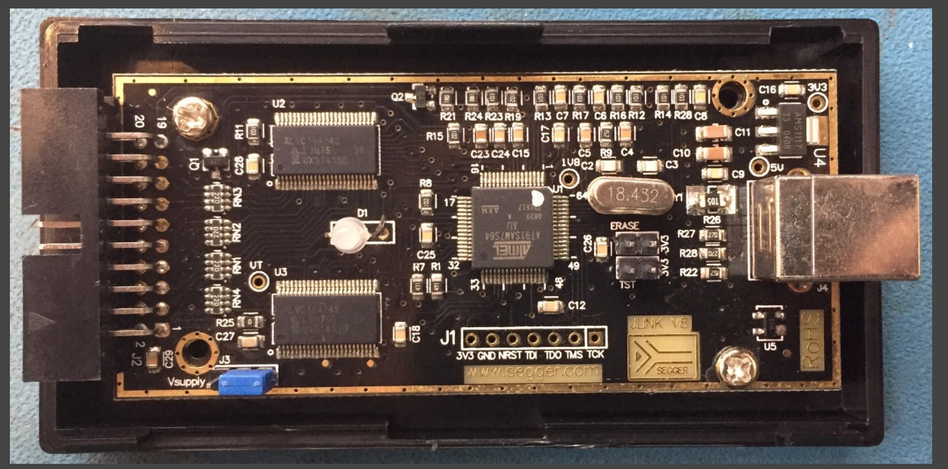


Trustworthy Hardware - Identifying and Classifying Hardware Trojans, R. Karri, et al., IEEE 2010

Development Tool Threats

- Engineering tools used during product development/manufacturing may be targeted
- Implant malicious code via compiler/programmer
  - Ex.: Infecting the Embedded Supply Chain, DEFCON 26, Miller & Kissinger
    - Arbitrary loading of code onto any devices connected to SEGGER J-Link
    - Load malicious firmware onto the J-Link itself

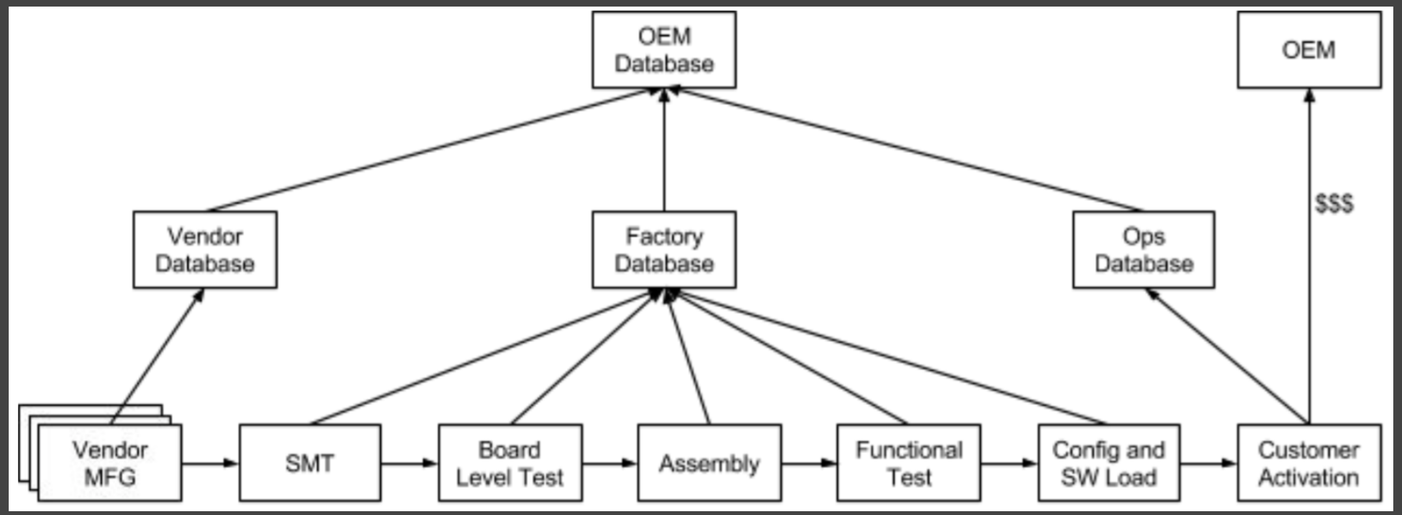




GRAND IDEA STUDIO

Factory Threats

- Shadow supply chain (grey market runs)
- Unauthorized component replacement/PCB changes
- Targeted network access via malware/rogue devices
- Firmware/data modification
- Leaked software/tools/schematics/data

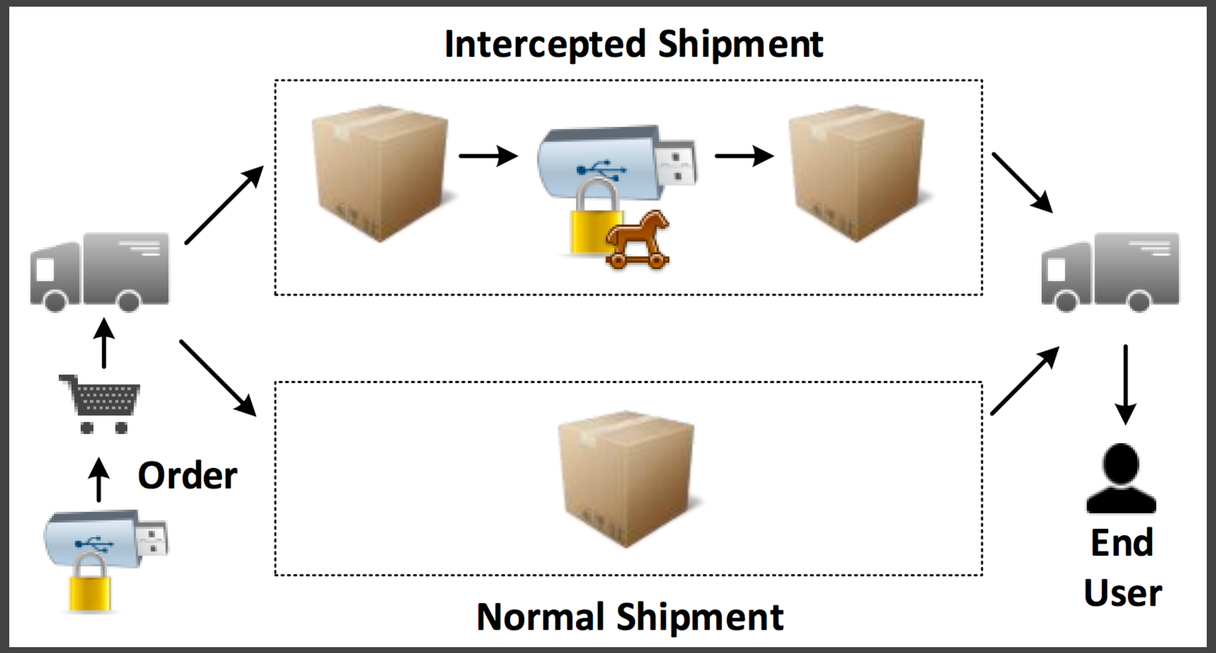


Secure Device Manufacturing: Supply Chain Security Resilience, NCC Group, 2015

GRAND IDEA STUDIO

Interdiction Threats

- Product intercepted between factory and intended customer/target
- Unauthorized field upgrades (modifications, implants)
- Repackaged and placed back into transit to original destination

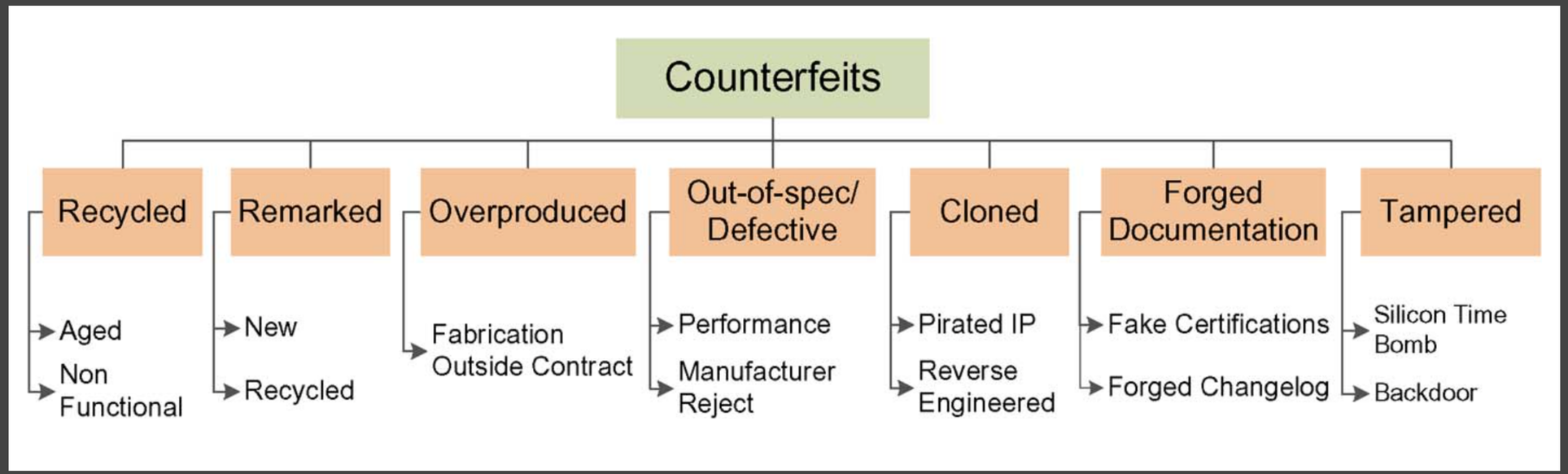


Interdiction in Practice - Hardware Trojan Against a High-Security USB Flash Drive, Swierczynski, et al., 2015

GRAND IDEA STUDIO

Silicon Threats

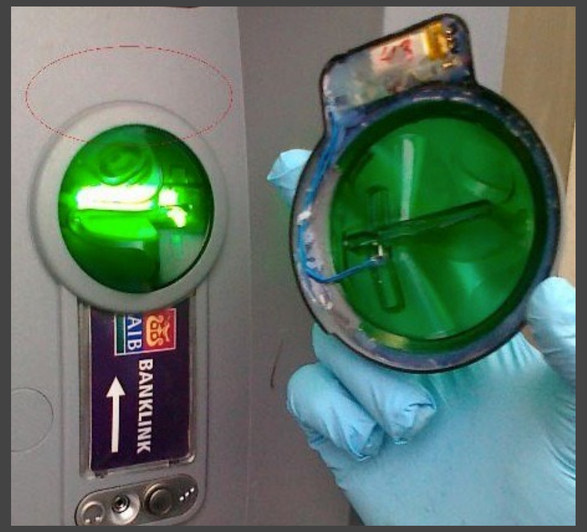
- Like dealing with circuitry, but at a microscopic level
- The semiconductor supply chain is ~~potentially~~ compromised
  - 15% of replacement semiconductors purchased by the Pentagon are estimated to be counterfeit (2013)



Counterfeit Integrated Circuits: A Rising Threat in the Global Semiconductor Supply Chain, Guin et al., IEEE 2014

GRAND IDEA STUDIO









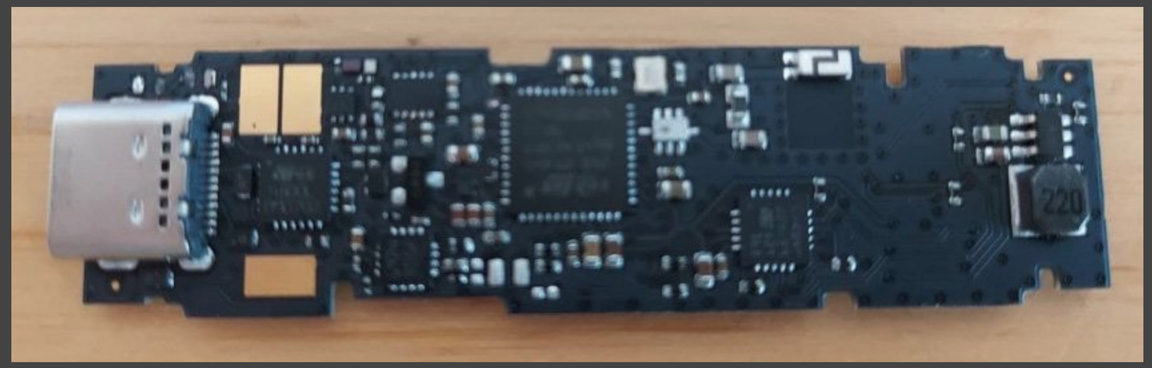


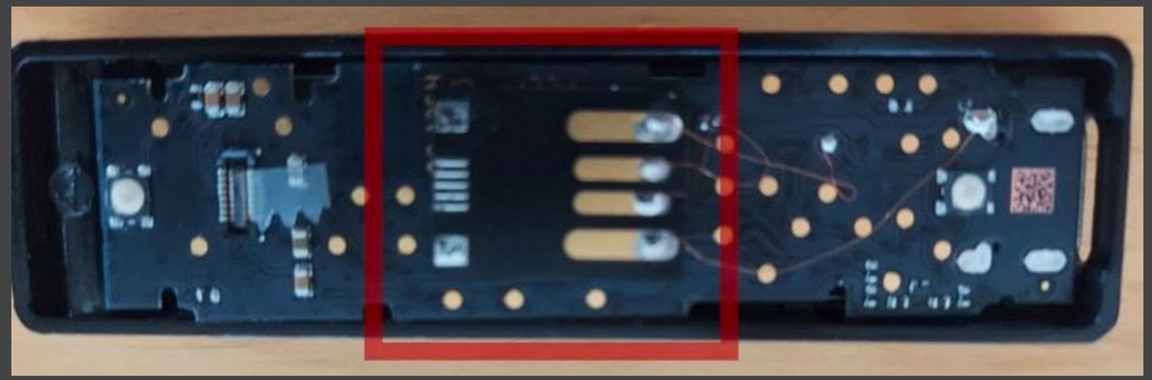
http://krebsonsecurity.com/tag/atm-skimmer/

GRAND IDEA STUDIO



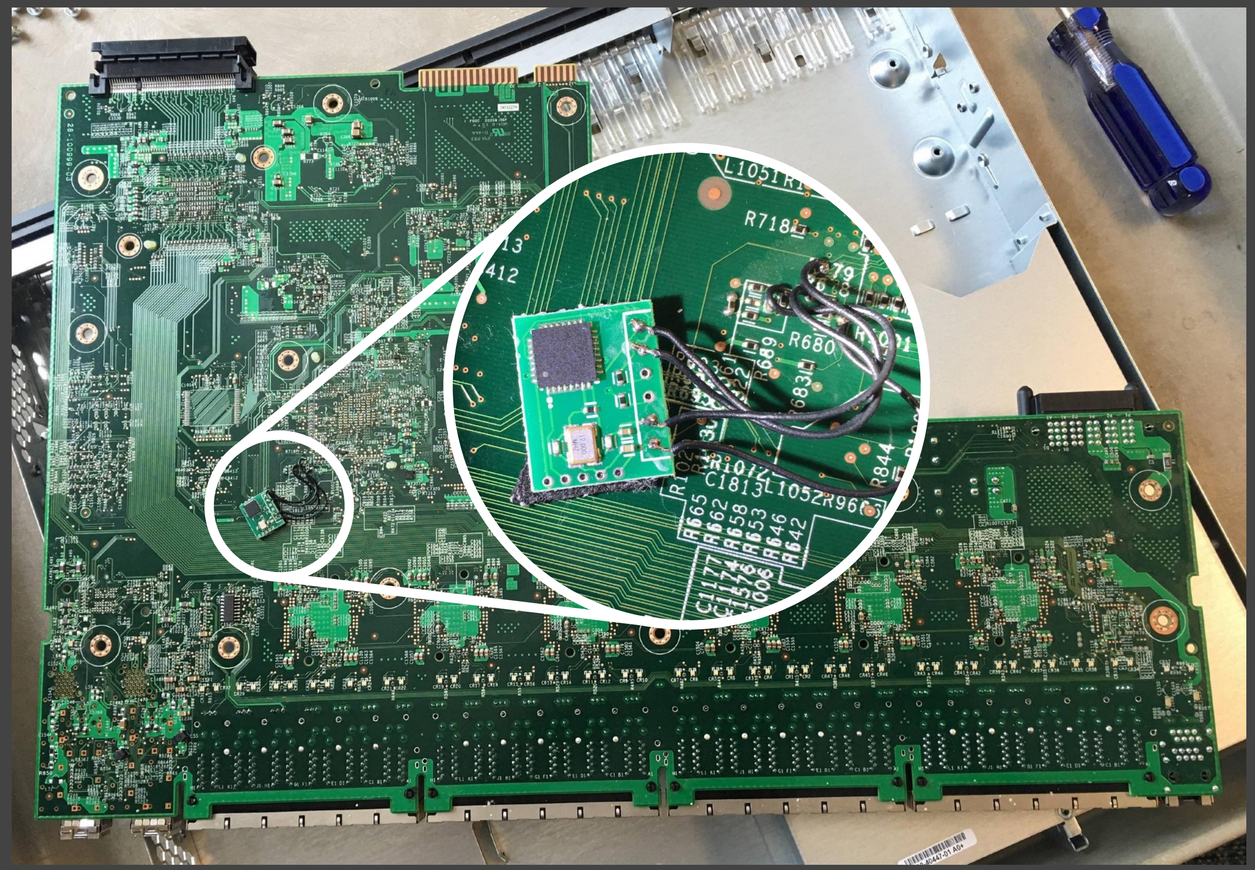
https://shop.hak5.org/products/omg-cable

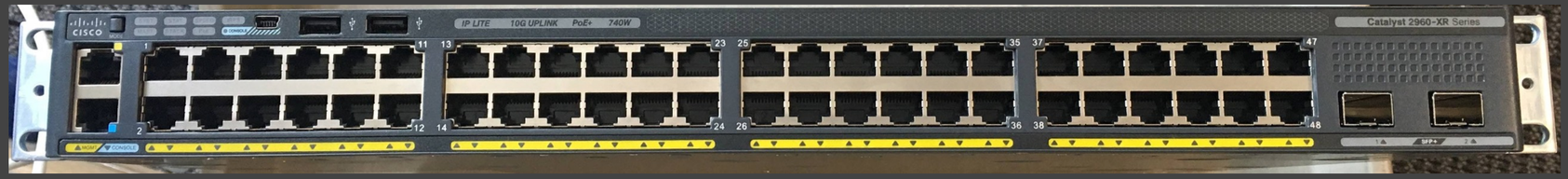




www.reddit.com/r/ledgerwallet/comments/o154gz/package_from_ledger_is_this_legit/

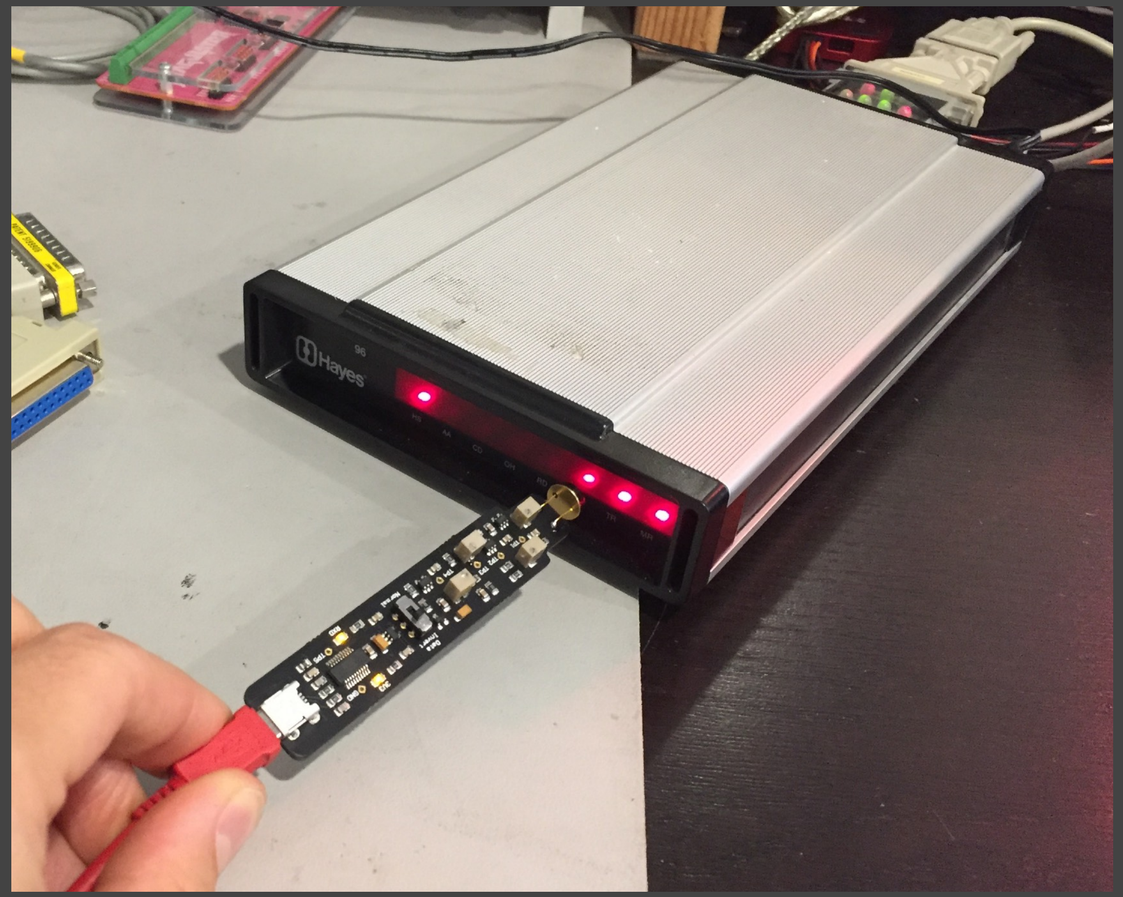
GRAND IDEA STUDIO





www.reddit.com/r/networking/comments/4iwa5f/possible_counterfeit_cisco_equipment_wphotos/

GRAND IDEA STUDIO





GRAND IDEA STUDIO

Final Thoughts

- HW should not be inherently trusted
  - Defined functionality can't always be guaranteed
- Easy to hide trickery when no one is looking
  - Adversaries will increase skill as needed to maintain advantage
- Supply chain security is an extremely complex problem
  - Identify and focus on areas most likely to be exploited
  - Operate under the assumption that you've been compromised

GRAND IDEA STUDIO

Additional Resources

- In Search of Lost Bytes Hardware Implants and the Trouble with Supply Chains (d'Antoine, Kernelcon 2020)
- Air-Gap Research Page, Cyber-Security Research Center, Ben-Gurion University of the Negev, Israel
- The Huawei and Snowden Questions: Can Electronic Equipment from Untrusted Vendors be Verified? Can an Untrusted Vendor Build Trust into Electronic Equipment? (Lysne, 2018)
- CIST: A Threat Modeling Approach for Hardware Supply Chain Security (Halak, 2021)
  - Counterfeiting
  - Information Leakage
  - Sabotage
  - Tampering




BLOCK
VOID