# USB DROP
# & USB KILL ATTACK

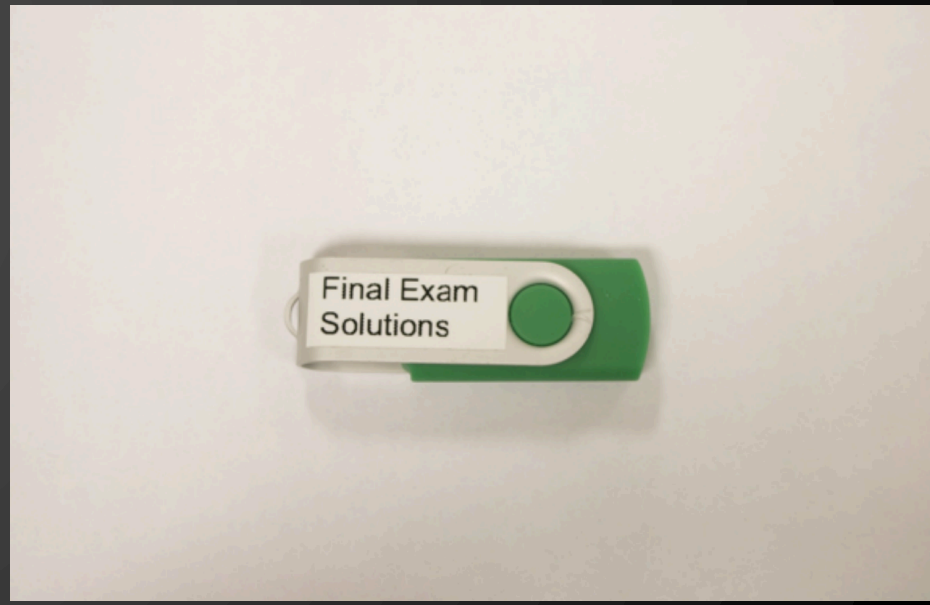
PRESENTED BY: (JASON) PAK YUNG NG

(CARY) JIA YING OU

(WENDY) WENYAN YAO

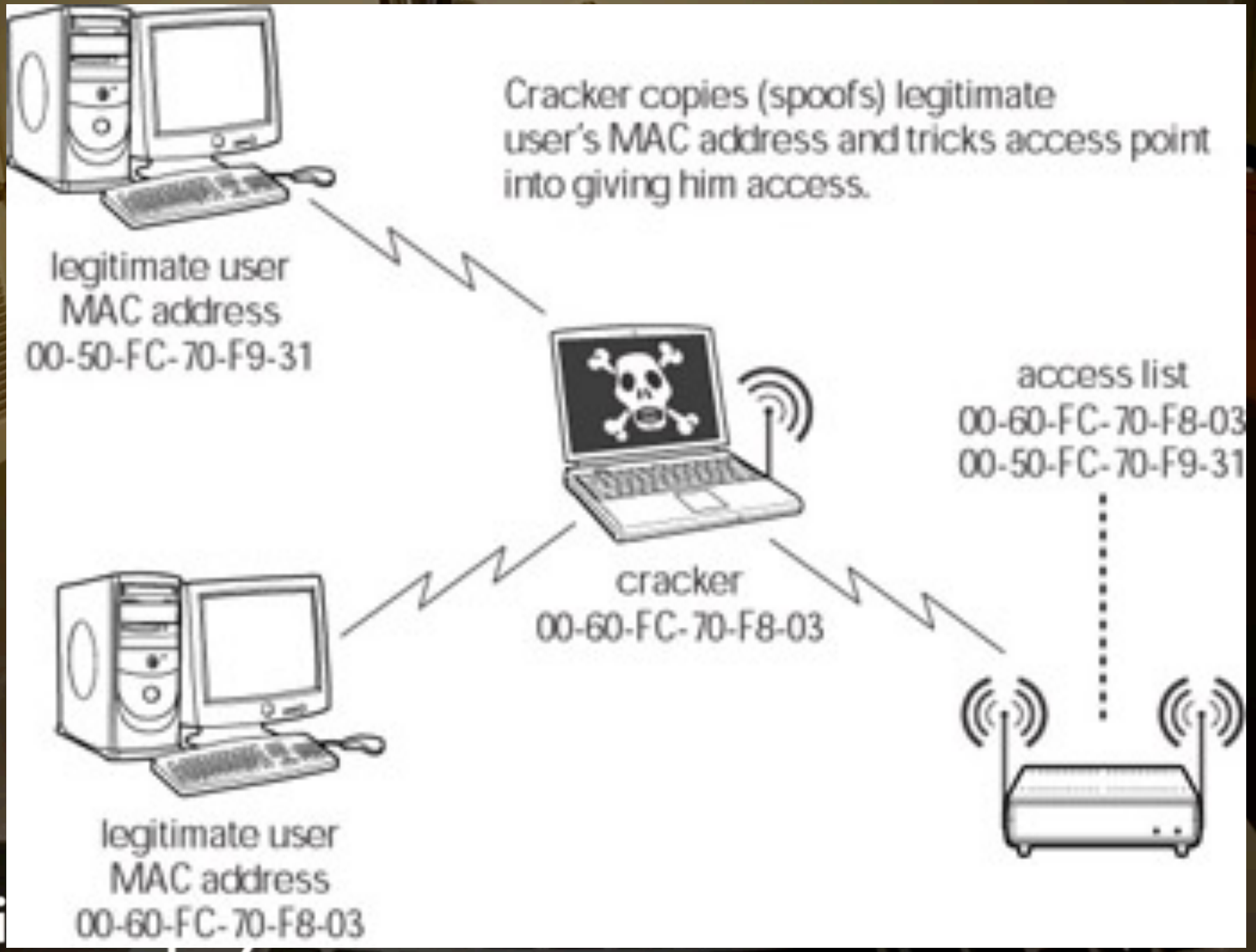
# USB DROP EXPERIMENT

- Experiment in University Illinois, Urbana-Champaign campus
- Dropped 300 USB drives with labels
- 98% picked up
- 45% detected files opened
- 45%-98% attack success rate
- 77 users provided detailed data



# THREAT

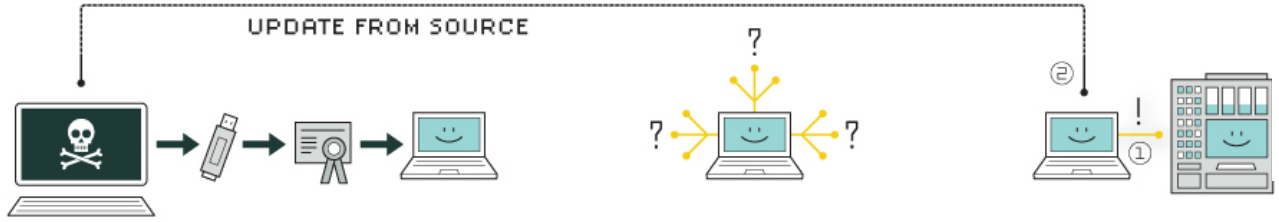
- Target
  - Any computer with USB port
- Agent
  - Hackers that are interested in sensitive information or damaging the computer
- Event
  - Plug the USB into a computer


Cracker copies (spoofs) legitimate user's MAC address and tricks access point into giving him access.
legitimate user
MAC address
00-50-FC-70-F9-31
cracker
00-60-FC-70-F8-03
access list
00-60-FC-70-F8-03
00-50-FC-70-F9-31
legitimate user
MAC address
00-60-FC-70-F8-03

Key mali

# Stuxnet

## HOW STUXNET WORKED




**1. infection**
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

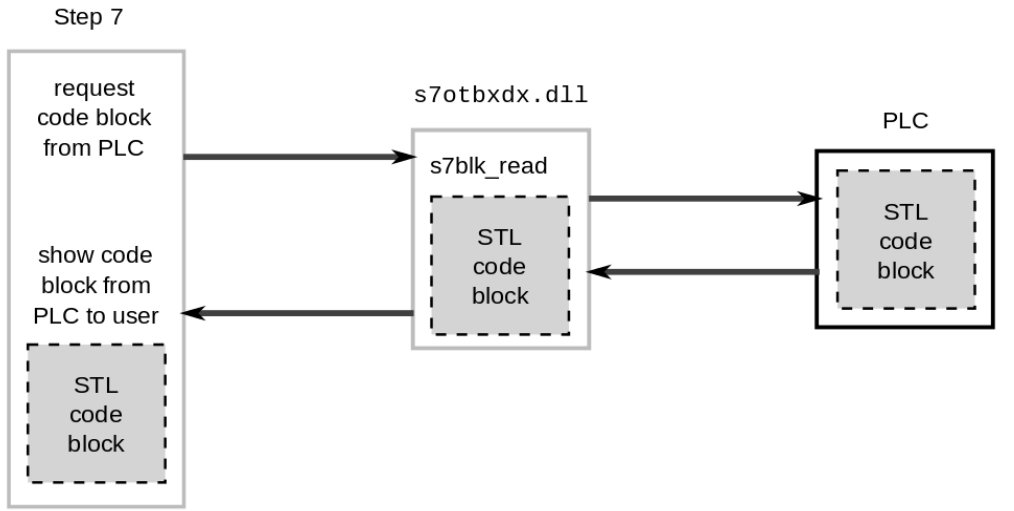
**2. search**
Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

**3. update**
If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

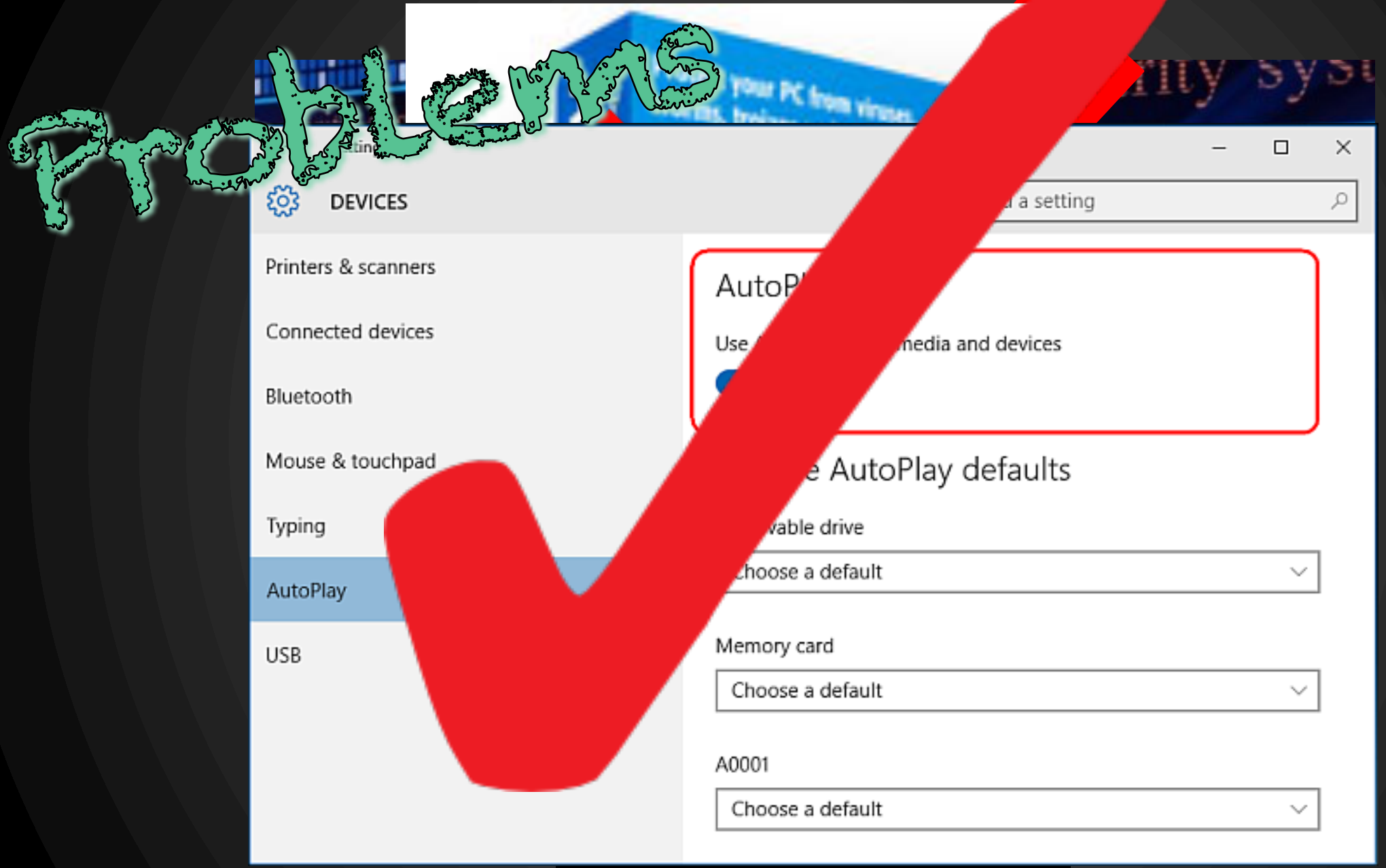
**4. compromise**
The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't been identified by security experts.

**5. control**
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

**6. deceive and destroy**
Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.




- 984 Uranium enriching centrifuges destroyed, which constituted a 30% decreased in enrichment efficiency.



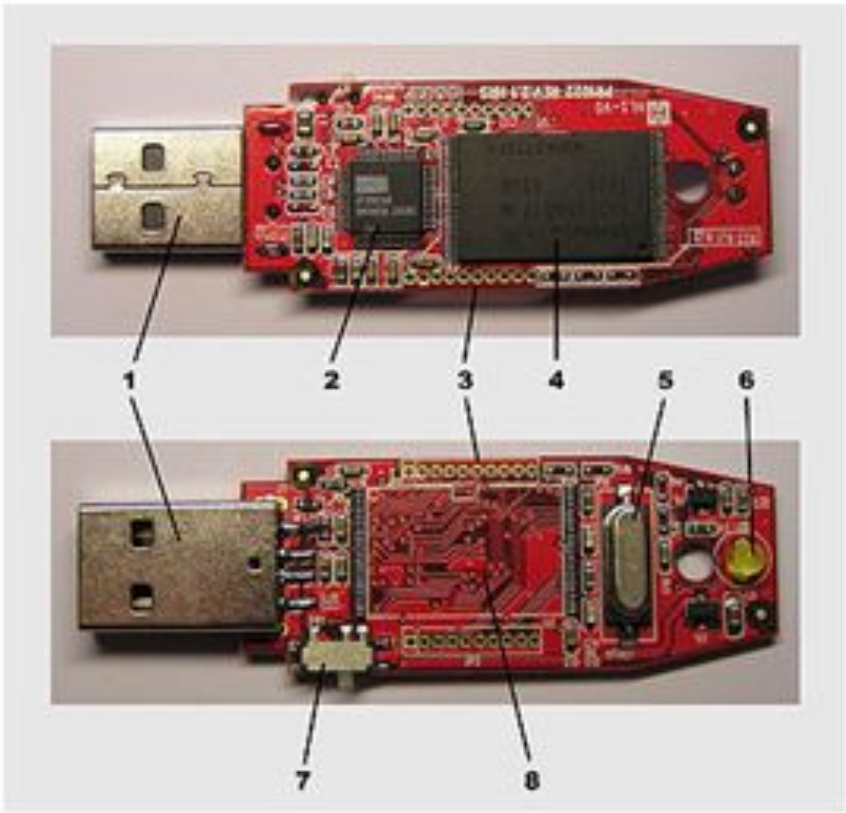

Disabling AutoPlay Feature

# Solution

- Disable Auto Run Functionality

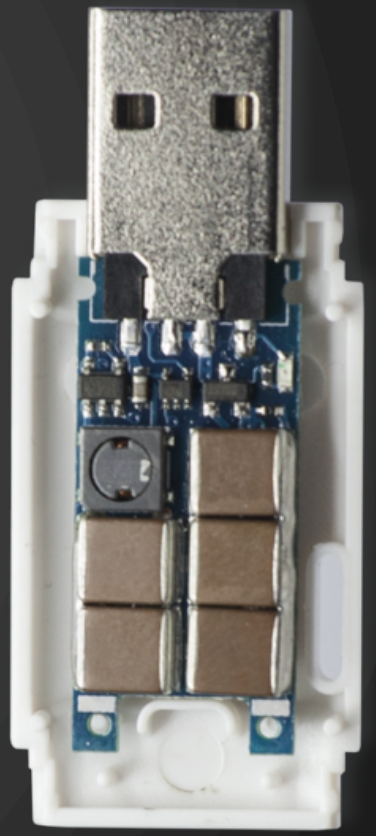
- Golden Rule: Do not Insert Any USB Devices That You Do Not Trust Into Your Computer.

# USB KILL ATTACK




**Internals of a typical USB flash drive**

1. USB Standard-A plug
2. USB mass storage controller
3. Test points
4. Flash memory chips
5. Crystal oscillators
6. LED
7. Write-protect switch (Optional)
8. Space for second flash chip



USBKILL.COM

# RUMORS

It appears that one of the only major manufacturers who won't see their devices affected by the USB Killer is Apple. Their MacBook line is reportedly immune to the device as it isolates the data lines on its USB ports.

Apparently, Apple is the only company not vulnerable to a USB attack, USB Killer told *Mashable*, with it voluntarily protecting its hardware.

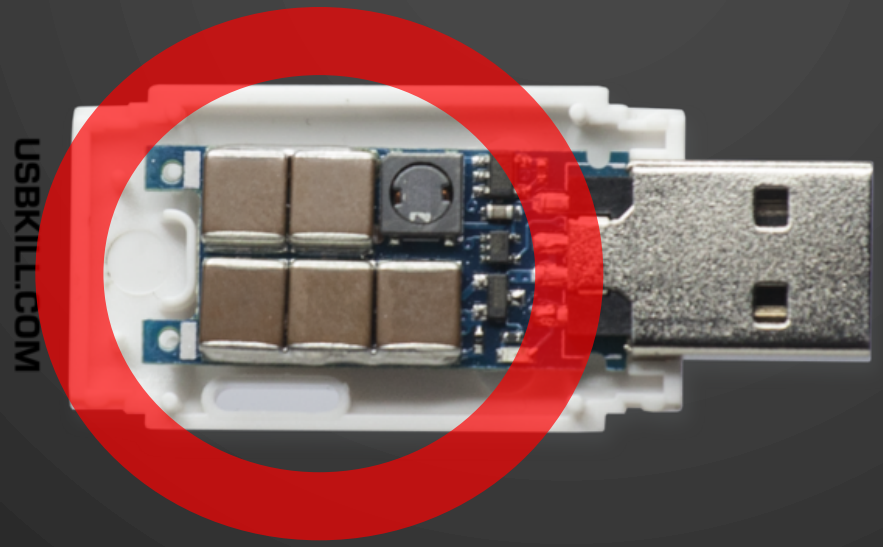

XBOX ONE
2 TB

# THE TRUTH

- Apple's Macbook is **ONLY** immune to USB KILLER from USBKILL.com

# HOW DOES IT WORK?

- Charges the power to capacitor
- Release circuit many time per second
- Electrostatic discharge (ESD)



# ACCESSIBILITY

- Can be purchased online
- Tutorial of how to make one

# USB KILL LATEST RELEASE

## USB KILLER V3

**$ 54.95**

**USB KILLLER V3:** 1.5x Power, 2x Faster Surges, 2x Stable

**Chose your edition:**
**Anonymous Edition**: No brand, no text, 100% discrete, or
**Standard Edition**: White Case, USB Kill Logo + Text

**GO PRO, SAVE BIG:** Get the **USB Kill Professional Kit** (USB Killer, Test Shield & Adaptor Kit) and get a **20% instant discount** and **free worldwide shipping!** *(Applied at checkout)*

QUANTITY 1 - + ADD TO CART

# PROTECTION AGAINST USB KILL ATTACK

- Never plug in untrusted USB
- USB Condom

## What is the event of a USB attack?

a) Pick up the USB
b) Plug in the USB
c) Drop the USB
d) None of the Above
e) All of the Above

# What is ESD?

a) Electronic Security Design
b) Electrostatic Discharge
c) Electricity Supply Discharge
d) Electronic Signal Detection
e) None of the Above

# WHICH OF THE FOLLOWING IS THE SOLUTION OF THE USB DROP ATTACK?

a) Use Anti- virus software
b) Never plug in untrusted USB
c) Discovering the security hole to fix it immediately.
d) None of the Above
e) All of the Above