Greater Manchester | Greater Security | Greater Business

Cyber Foundry

Counterfeit Products

Protecting your business from imitation hardware

Audience: General **Reading Time: 15 Mins**

As the costs of research and development rise, innovative hardware devices that reflect these increased expenses are being targeted by counterfeit criminals

Key Points

- It is a very profitable business to copy existing devices, replacing expensive manufacturing processes and parts with cheaper and less reliable alternatives.
- Cloned hardware can often appear almost identical to the real thing and only the reduced-price signals doubt.
- Devices are being created to bypass standard authentication checks created by the original equipment manufacturers.
- Counterfeit devices are already in the supply chain and retailers may be selling them without knowing that they are not the genuine article.
- Known counterfeit devices have failed during software upgrades leaving businesses networks down.
- Manufactures need to improve the level of certainty to consumers that a purchased product is genuine.

European Union
European Regional Development Fund
Manchester Metropolitan University
MANCHESTER 1824 The University of Manchester
University of Salford MANCHESTER
Lancaster University

Fake Devices

An unnamed company in Autumn 2018 contacted F-Secure regarding potentially fake Cisco Catalyst 2960X Switches. Dmitry Janushkevich, an F-Secure Consultant in the Hardware Security Team was tasked to discover whether these devices contained backdoors or malicious code. The switches were being used as part of the business's live network, but during a scheduled software upgrade, the devices failed to restart.

When the company contacted the vendor and attempted to acquire replacements, they were informed that these devices were likely counterfeit. This is when the CISO of the company shipped the hardware to F-Secure to review and determine whether the company had been a victim of cyber espionage.

Dmitry discovered that the devices did have suspicious code and additional hardware, but these were being used to trick the authenticity checks being made by Cisco. He did not find any evidence of backdoors or malicious code.

The only differences he could notice that distinguished the genuine article from the fakes were different label colours and alignment (Figure 1). Unless you had the original to compare to it would be impossible to determine that anything was amiss.

The only truly noticeable difference found was that the genuine device had a holographic Cisco sticker whereas the counterfeit products did not (Figure 2). The problem was, this sticker is on the board of the switch and would require you to open the device to check.

Figure 1 - Fake device on the left, Genuine device on the right

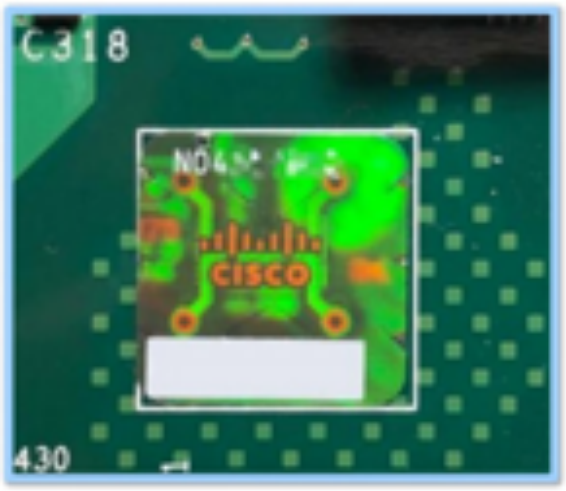

Figure 1 - A genuine CISCO hologram found internally within the device

The only other way to determine that these counterfeit devices are not the real thing is to run a software upgrade which stops them from working entirely. The sophistication displayed to produce these switches to such a standard that they were able to be installed into a business without any suspicion is extremely worrying.

Despite these devices not being produced for any other intent than to produce profit for the original counterfeit manufacturers, they could have easily been modified for malicious intent by external threat actors anywhere along the supply chain.

Cisco is not the only original equipment manufacturer facing hardware clones, for example, Honda has seen their after-market engine control units imitated and sold as authentic, world-wide and on a massive scale.

These counterfeit products were clearly poor imitations of the real thing, but the safety concerns are real as these devices are designed to connect directly to the engine of a vehicle. Hackers have previously shown that via engine control units it is possible to control the steering and brakes.

Counterfeit USBs

One of the most common counterfeited devices on the market today are USB Memory Sticks. Generally, these fake USB Sticks just pretend to much higher capacity than they really are.

There are two types of fake USB Storage though, ones that when they hit their real maximum capacity just stop writing and others that continue to write by cycling back and overwriting the original data placed on the stick.

Many consumers are unaware they have either of these devices until they start to have issues with their storage device not saving files, or worse, when the original data they put on the stick is no longer accessible.

Yet again the devices here that are not necessarily malicious beyond fooling the consumer into thinking they have purchased a much larger capacity device than the reality.

There is a potential for harm on both types of USB Stick when it comes to saving data beyond its real maximum capacity. One will pretend it has copied correctly but will actually save nothing and the other will overwrite the original data stored. This can lead to unrecoverable data loss if the owner doesn't have any backups or the originally transferred data.

USB Sticks can be used for malicious intent though and many such devices exist. USB related attacks are referred to as hotplug attacks as they can be initiated by simply plugging a device into a live machine.

Cyber security workers use a variety of these hotplug tools for penetration testing of computers and networks, for example: some can detect keystrokes and others can deploy automated payloads for reconnaissance.

There is a real possibility that these counterfeit USB storage devices could be used for nefarious reasons, beyond just fooling consumers.

Definitions

Switch - A switch is used in a wired network to connect to other devices using Ethernet cables. The switch allows each connected device to talk to the others.

Backdoor - Backdoor is an undocumented way of gaining access to a program, online service or an entire computer system. A backdoor will bypass normal authentication mechanisms.

Malicious code - This is the term used to describe any code in any part of a software system or script that is intended to cause undesired effects, security breaches or damage to a system.

Penetration Testers - Companies employ penetration testers to improve information security by detecting and correcting system weaknesses before criminal hackers can exploit these weaknesses

Payload - In the context of a cyber-attack, a payload is the component of the attack which causes harm to the victim. Attack vectors such as viruses, wurms, and malware can all contain one or more malicious payloads.

Reconnaissance - Network reconnaissance is a term for testing for potential vulnerabilities in a computer network. This may be a legitimate activity by the network owner/operator, seeking to protect it or to enforce its acceptable use policy. It also may be a precursor to external attacks on the network

Copycats & Clones

Another technology product area that has concerns regarding counterfeit products is in the Internet of Things (IoT) space. One of the most famous Internet of Things device makers is the Arduino Company. They produce opensource software and hardware used in many IoT projects globally, everything from development systems that hobbyists are testing up to deployment into the industry.

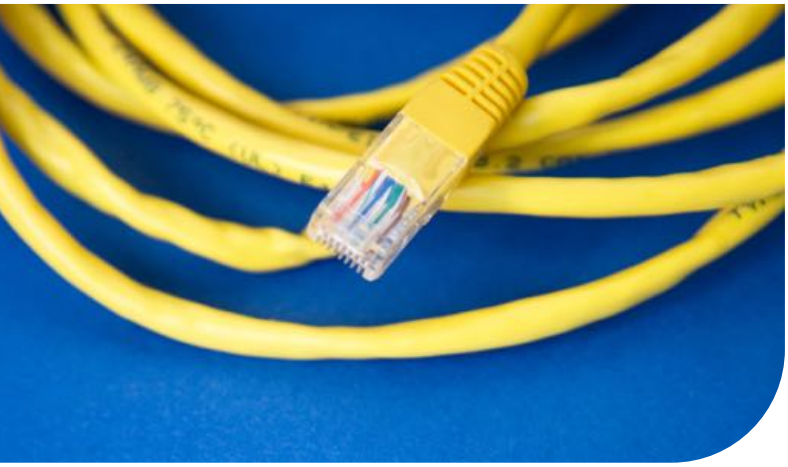

Image: Markus Spiske from Unsplash

Copycats have cloned the Arduino products quite extensively, devices that mimic the Arduino can often be purchased for up to 10 times less than the authentic product. Due to the opensource nature of the Arduino software and hardware it makes it very difficult for the Arduino Company to prevent these clones. Most of these clones are not in breach of any laws as they do not use the name "Arduino" but they also do not declare they aren't genuine in product listings.

The clones generally work fine but their quality is often far lower than the genuine device and they are not as easy to work with, but for most cases hobbyists do not notice a significant difference between the fake and the real thing. The concern is that these devices could be making their way into the industry where certain standards are expected. It is highly unlikely that these copycat Arduino boards are built to the standards required and there is always the possibility that they may introduce security risks due to this.

Research by BorderHawk and Senrio uncovered flaws in Remote Power Management devices, similar to smart plugs that many of us may have at home. These IoT devices allow remote control of power outlets in industries such as the Energy Sector.

The flaws included hidden features and commands specifically designed for malicious intent, such as retrieving a list of users and their passwords from the device.

The majority of these RPM devices are not accessible to remote attack as they are inside secured private networks, however, an IT Administrator from a large university in the United States did disclose that some of these devices have been deployed in a way that does make them vulnerable.

The idea that remote hackers could quite easily shut off power to critical equipment and that these devices are being designed for this is extremely unsettling. Unfortunately, there is no quick fix for these issues as there is no clear oversight in many of the factories that these devices are being made.

These computer parts are often produced in countries such as China, Indonesia, the Philippines and Taiwan. Products are then assembled from these parts in China before being sent exported to clients and customers via a complex arrangement of importers and distributors.

It is quite common to see counterfeit products tagged with "Made in the USA" and missing or outdated compliance certificates. Additional product information, such as user manuals or quick start guides, that are often included with the device may also have grammatical and spelling errors.

People in the industry who understand the complexity of these counterfeit devices have stated that the supply chain should be as rigorous for electronic devices as it is for food.

ARM often designs products referred to

as 'system on chip', this concept is better understood as just a very small computer. Whereas computers and laptop systems have multiple devices working together that are independent of one another, these System on Chip (SoC)'s are designed to have everything required manufactured on the same chip.

Many smartphone devices use these SoC designs as there just isn't the space for a more traditional computer system design where hardware is interchangeable. The problem is that these SoC's start life as diagrams and frameworks, they are designed to do some of the work that software does but not all of it.

Allwinner, a Chinese SoC company that makes the processor used in many low-cost Android tablets, set-top boxes, ARM-based PCs, and other devices has made multiple mistakes over the years relating to backdoors being left into their devices. These SoC manufacturers predominantly specialise in hardware, writing software to allow access to their SoC is a less important aspect of the business and this is where the flaws generally exist.

Software updates are principally the way by which SoC manufactures fix the errors they have made in the past in relation to security, but many SoC's may only be supported for six to twelve months as new designs are entering the market frequently. This means that a smartphone or tablet that is around four years old could have had a flaw for three of those years with no fix. The longer this device stays in use without a fix the more likely a malicious attack becomes prevalent towards it.

The best option that can be taken to protect our businesses is to visit the manufacturers' website for any equipment we want to buy. If it is possible to buy directly from the manufacturer then this is always the most advisable option.

In circumstances where the manufacturer does not sell its own products, they will generally have a page that lists their official resellers. Choose a reputable reseller that doesn't operate a marketplace and always ensure you are purchasing new and sealed products.

If you suspect tampering of a product purchased or have any reason for concern, contact the vendor first and then the manufacturer.

image: Michael Dziedzic Unsplash

Always make sure that any devices are kept up to date with the latest software patches or firmware updates. Many of these packages are designed to fix security holes that researchers have found since the initial products release.

The final piece of advice is to purchase devices that have longer warranties and support periods. For example, the Google Pixel smartphone is sold with update support for at least three years, Apple iPhones have up to four years of support.

Huawei has committed to offering support for up to two years on their devices but lesser-known Chinese brands such as Honor, Ulephone and Cubot do not clearly state their support periods or they vary depending on the device being purchased.

Consumers often overlook how products with a higher price offer longer support periods or warranties, however, this is generally why similar specification devices cost more. This additional support is not cheap and it generally allows a device to have a much longer and more secure lifespan.

Further Reading

About the Author

Robert Marsh is a published Internet of Things Forensics Researcher and an award-winning Artificial Intelligence Software Developer. He is currently working as a Cyber Security Analyst with the Greater Manchester Cyber Foundry technical team at The University of Salford.

University of Salford MANCHESTER

READ MORE

1. Are Ideas Getting Harder to Find?
   https://web.stanford.edu/~chadj/IdeaPF.pdf
2. Hunting for backdoors in Counterfeit Cisco devices
   https://labs.f-secure.com/assets/BlogFiles/2020-07-the-fake-cisco.pdf
3. Counterfeit S300 https://www.hondata.com/?_route_=counterfeit-s300
4. eBay Fake Capacity USB Sticks
   https://www.novatech.co.uk/blog/ebay-fake-capacity-usb-sticks/
5. Hak Penetration Testing Equipment
   https://shop.hak5.org/
6. How to spot a counterfeit Arduino
   https://www.arduino.cc/en/products/counterfeit
7. Copycats pose a serious security threat to the IoT
   https://iot.eetimes.com/copycats-pose-a-serious-security-threat-to-the-iot/
8. Flaws in networking devices highlight tech industry's quality control problem
   https://www.csmonitor.com/World/Passcode/2016/0518/Flaws-in-networking-devices-highlight-tech-industry-s-quality-control-problem
9. Software's Sausage Factory: The Supply Chain
   https://securityledger.com/2016/05/softwares-sausage-factory-the-supply-chain/
10. Qualcomm Snapdragon SoC vulnerability could compromise IoT security
    https://betanews.com/2016/03/15/internet-of-things-security/
11. Vulnerabilities on SoC-powered Android devices have implications for the IoT
    https://blog.trendmicro.com/vulnerabilities-on-soc-powered-android-devices-have-implications-for-the-iot/

For more info about GM Cyber Foundry: https://www.gmcyberfoundry.ac.uk

European Union
European Regional Development Fund
Manchester Metropolitan University
MANCHESTER 1824 The University of Manchester
University of Salford MANCHESTER
Lancaster University