IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Hardware Hacking: An Approach to Evaluate the Importance of Hardware Hacking and its Associated Risks

Mr. Hitendra Swami[1] *NLIU, Bhopal, M.P.*
Dr. Satya Prakash[2] *NLIU, Bhopal, M.P.*
Dr. Shrish Kumar Tiwari[3] *CUG, Gandhinagar, Gujrat*

Abstract

Hacking is not just limited to the software aspect of the cyberspace; hardware aspect of hacking has the same relevance and importance. as we saw a lot of hardware hacking attacks in past, like Stuxnet attack, we should not neglect the presence of these cyber-attacks which involve hardware hacking as they include a wide variety of targeted system such as, computer systems, IOTs servers, networks, automobiles, as well as medical implants too. In this research paper, Researchers tried to explore the hardware hacking tools and its associated risk and its avoided side of cyber security.

Keywords: hardware hacking, hardware hacking tools, hardware hacking attacks,

Introduction

Hardware hacking involves modifying or repurposing electronic devices to access restricted features or functionality using software or hardware tools. It has a rich history that can be traced back to the 1970s and 1980s when personal computing became more widespread and accessible. Today, hardware hacking has become a more specialised and sophisticated field, requiring a deep understanding of electronics and computer systems. Hardware hackers can be found in a variety of settings, including research and development, security, and hacking communities. While hardware hacking can have a wide range of applications, it is also used by some threat actors to perform some negative tasks. This paper aims to provide a comprehensive overview of hardware hacking and associated tools, including its applications, techniques, and risks, to raise awareness among users and promote responsible hardware hacking practices for the sake of human evolution towards a better future.

Types of Hardware Hacking Techniques

- **Reverse Engineering:** This technique involves analysing the hardware or software of a device to understand its functions, interactions and protocols. It helps identify vulnerabilities, hidden features, or backdoors that can be exploited for malicious purposes. It can also be used to modify or repurpose a device for different uses.
- **Retrofitting:** This type of hacking involves modifying or repurposing existing hardware to perform functions beyond their original design. One example of this is converting an ICE vehicle into an EV. While this type of hacking is generally not considered malicious, it involves modifying a system to perform functions beyond its original design.

[1] Mr. Hitendra Swami is a student of MCLIS program at NLIU, Bhopal
[2] Dr. Satya Prakash is an Assistant Professor, Department of Cyber Law and Information Security at NLIU, Bhopal
[3] Dr. Shrish Kumar Tiwari is an Assistant Professor, Centre for Strategic Technologies, School of National Security Studies (SNSS)

- **Hardware Merging:** This technique involves taking components from multiple devices and combining them to create a new device that performs a specific function. It requires a good understanding of the components and their interactions, as well as hardware and software skills. It can be used to create custom devices or modify existing devices.
- **Zombie Device:** This involves modifying a device's hardware or firmware to take control of it and turn it into a "zombie" that can be used for malicious purposes, such as a botnet. It can be accomplished through firmware malware or hardware implants.
- **Parasitic Hardware Hacking:** This technique involves using malicious hardware devices or components that are physically implanted or attached to a computer. It can be used to intercept or modify data, provide remote access or control, or launch other types of attacks. To protect against this type of hacking, it is important to use trusted sources for hardware and inspect devices for signs of physical tampering or modification regularly.

Literature review

This guide provides an introduction to the world of hardware hacking, covering various tools and techniques used for analysing and exploiting hardware vulnerabilities. The guide offers a clear and concise overview of hardware hacking and is a great starting point for those interested in this field[4].

This article provides an introduction to hardware hacking and explains various methods used to exploit hardware vulnerabilities. The article is well-written and provides valuable insights into the world of hardware hacking[5].

This article explains how Kali Linux can be used for hardware hacking and social engineering. The article covers various tools and techniques used for hardware hacking and provides step-by-step instructions on how to use them[6].

This article provides an overview of Flipper Zero, a wireless hacking gadget that can be used for various tasks such as pen-testing, signal analysis, and more. The article is well-written and provides valuable information about this interesting device[7].

Statement of Problem

Hardware hacking is getting prevalent these days and as we know that hardware hacking tools are rightly available in just some clicks, how they can change our future.

Hypothesis

Hardware hacking can have both malicious and beneficial purposes, including improving functionality, security research, innovation, cost savings, and defense. It can lead to new technologies and advancements in computer science and electronics. Awareness is crucial to protect ourselves from being targeted.

Research Objective

The objective of this research is to explore and examine the various hardware hacking tools available in the market and their positive and negative capabilities and also examine the various purposes of hardware hacking that can be used in different industries.

---

[4] Steve Worsley, "A Fundamental Guide to Hardware Hacking" (EXPLIoT) <https://store.expliot.io/blogs/iot/a-fundamental-guide-to-hardware-hacking> accessed January 30, 2023.

[5] "An Introduction to Hardware Hacking" (*An Introduction to Hardware Hacking*, September 14, 2020) <https://www.cyberark.com/resources/threat-research-blog/an-introduction-to-hardware-hacking> accessed January 30, 2023..

[6] Anurag Dubey, "Hardware Hacking and Social Engineering Tools in Kali Linux - GeeksforGeeks" (*GeeksforGeeks*, December 27, 2022) <https://www.geeksforgeeks.org/hardware-hacking-and-social-engineering-tools-in-kali-linux/> accessed January 30, 2023.

[7] Stan Schroeder, "The Flipper Zero Is a Swiss Army Knife of Antennas" *The Flipper Zero is a Swiss Army knife of antennas - The Verge* (November 2, 2022) <https://www.theverge.com/23433594/flipper-zero-hacking-gadget-wireless-pentesting-open-source-antenna> accessed January 30, 2023.

Research Questions

1. What are the different types of hardware hacking tools available in the market and how do they work?
2. How hardware hacking can be beneficial for industries and researchers?
3. Are there any existing countermeasures and detection methods used to prevent hardware hacking attacks, and how effective are they?
4. Can we formulate some concept or ideas as countermeasures for future devices?

Research Methodology

The researcher's approach for this research is based on the secondary data. The researcher explores various hardware hacking technique and associated tools used, relevant events and the risk associated with them.

Limitations and Scope of Research

The researcher proposes to perform an overall security analysis of different types of Hardware hacking tools. Due to the lack of time and resources, the research will be confined to the different types of tools associated to hardware hacking and possible risks proposed by them, researcher will be exploring them on the basis of the researcher's findings and previous educational knowledge in this domain.

How hardware hacking can help us in various ways?

Hardware hacking, the art of modifying and manipulating the physical components of electronic devices, can be beneficial when used for ethical purposes. It has various benefits in different industries, such as the automotive industry, healthcare industry, and cybersecurity industry.

Automotive Industry

Cars have become more susceptible to hacking, and malicious actors can exploit vulnerabilities in these systems to gain control of the car and cause accidents. Ethical hardware hacking can be used to identify and patch these vulnerabilities. By finding and addressing these vulnerabilities before malicious actors can exploit them, hardware hacking can make cars safer for drivers and passengers. Additionally, hardware hacking can be used to analyse a car's communication protocols and identify potential attack vectors.

Healthcare Industry

Medical devices such as pacemakers, insulin pumps, and defibrillators, are vital for patients with serious health conditions. However, these devices are also vulnerable to hacking, which can lead to life-threatening situations. Hardware hacking can be used to identify and patch vulnerabilities in medical devices. By modifying the device's firmware or hardware, researchers can add new security features that prevent unauthorised access.

Cybersecurity Industry

Hardware hacking can also be used to improve cybersecurity in various industries. By using hardware hacking, cybersecurity researchers can identify and patch vulnerabilities in hardware components, making it more difficult for attackers to exploit them. Furthermore, hardware hacking can be used to test the security of devices and systems, and identify potential weaknesses. By doing so, researchers can develop more robust and effective security measures that can protect against a wide range of threats.

In conclusion, hardware hacking can help to improve the security and safety of various industries. By using hardware hacking for ethical purposes, we can identify and patch vulnerabilities, develop new security technologies, and ultimately create a safer world for everyone.

Master tools for hardware hacking in present time

1. **Flipper Zero:** Flipper Zero is a handheld device that can be used for hardware hacking. Hardware hacking is the manipulation or modification of electronic devices to gain access to their hardware, software, or firmware and manipulate it in such a way that it performs functions beyond what it was initially designed for. Flipper Zero can be used for different tasks in hardware hacking, including sniffing and analysing communication protocols, emulating electronic devices, reverse engineering electronic devices, controlling electronic devices, and debugging electronic devices.

   However, the use of Flipper Zero can also pose risks such as unauthorised access, reverse engineering, data theft, network vulnerabilities, and privacy concerns. Nevertheless, Flipper Zero can make life easier in terms of security testing, debugging, emulation, reverse engineering, and as a learning tool for hardware hacking and electronic device development.

2. **Rubber Ducky:** Rubber Ducky is a small USB device that can perform automated keystroke injections and is used in hardware hacking to exploit vulnerabilities in computer systems. It can automate a wide range of tasks, including password cracking, network penetration testing, social engineering attacks, and malware injection. Despite its usefulness, it also poses significant risks, including the theft of sensitive information, manipulation of individuals, unauthorised access, and legal consequences. To reduce these risks, Rubber Ducky should be used responsibly and within the bounds of the law. Ethical hackers can use Rubber Ducky to test the security of computer systems, perform social engineering testing, penetration testing, and automate repetitive tasks. It can help identify vulnerabilities that can be patched before they are exploited by malicious actors, develop better training and awareness programs to prevent social engineering attacks, and improve overall system security.

3. **Raspberry Pi:** Raspberry Pi is a small computer based on a Broadcom system-on-a-chip (SoC) that runs on Linux distributions like Raspbian OS, Ubuntu, and Debian. It is ideal for embedded and IoT applications due to its small size, which fits in the palm of your hand. Raspberry Pi has GPIO pins, USB ports, HDMI output, Ethernet port, Wi-Fi, and Bluetooth, and is available in different models with varying specifications. It can be used for a wide range of applications such as media center, gaming console, web server, home automation, and robotics. Raspberry Pi is affordable, open-source, and has become a valuable tool for education, especially in computer science, science, engineering, and mathematics.

   Raspberry Pi's versatility and accessibility have made it popular in the world of hardware hacking. Its low cost and availability make it an excellent option for those who want to experiment with different projects. Raspberry Pi's flexibility allows it to be programmed to perform a wide range of tasks and used in many different applications. Its use in hardware hacking has become increasingly popular, from controlling robotic arms to building complex security systems.

4. **Arduino :** Arduino is a versatile microcontroller board that is programmed with a simplified version of C++. It is popular for hardware hacking, enabling users to create custom hardware solutions for various applications such as robotics, home automation, security systems, and wearable technology. However, it's important to be aware of the potential security risks and ethical concerns associated with the use of Arduino. While Arduino can be a powerful tool in the hands of skilled users, it can also be used for malicious purposes by threat actors. Therefore, it's crucial to follow proper security practices, including implementing access controls and using secure communication protocols, to mitigate the risk of security vulnerabilities. Additionally, developers must be mindful of the potential for misuse of their projects and take steps to ensure that their projects are not being used for unethical purposes.

5. **HackRF One:** HackRF One is a software-defined radio (SDR) platform that can be used for a wide range of hardware hacking applications. It is designed to be an affordable, open-source alternative to expensive radio equipment and offers a range of capabilities for exploring, experimenting, and hacking wireless communication systems.

With HackRF One, users can receive and transmit a wide range of radio signals, including WiFi, Bluetooth, cellular, and GPS. It allows users to capture, record, and replay signals, making it a powerful tool for reverse engineering and analysing wireless protocols. The platform can also be used for testing and experimenting with new wireless technologies and developing custom radio applications.

6. **LAN Turtle:** A pocket-sized Ethernet Turtle that allows for covert remote access to a network. The device can be plugged into an Ethernet port and can be remotely accessed via SSH or VPN, enabling users to remotely control and monitor target systems.
7. **Packet Squirrel:** A tiny Ethernet multi-tool that enables network monitoring, packet capture and injection, as well as VPN and tunnelling capabilities. The device is easily configurable and can be used for network security, testing and analysis.
8. **Shark Jack:** A versatile Ethernet adapter that can be used to perform a range of hacking activities, including network sniffing, port scanning, and payload injection. The device is highly portable and easy to use, making it ideal for on-the-go hacking.
9. **O.MG Cable:** A USB cable that contains a hidden Wi-Fi hotspot, allowing attackers to remotely connect to target systems. The cable is difficult to detect and can be used to exfiltrate data or execute remote commands on target systems.
10. **Signal Owl:** A wireless security testing device that can perform network reconnaissance, Wi-Fi hacking, and Bluetooth scanning. The device is highly portable and can be used for a range of security testing activities, including penetration testing and vulnerability assessment.
11. **Plunder Bug:** A compact Ethernet sniffer that can be used to monitor network traffic and capture packets. The device is easy to use and highly portable, making it ideal for network security testing and troubleshooting.
12. **Bash Bunny:** A collection of pre-configured payloads that can be used with the Bash Bunny to perform a range of hacking activities, including credential harvesting, network scanning, and payload delivery.
13. **Key Croc:** A keystroke injection tool that can be used to simulate keyboard inputs and execute scripts on target systems. The device is highly configurable and can be programmed to perform a range of tasks, including password cracking, data exfiltration, and privilege escalation.

Comparison sheet

Hardware Hacking Tool	Specifications	Capabilities	Purpose
Flipper Zero	32-bit MCU, 1.3" OLED display, BLE, IR, NFC, GPIO pins	Open-source hardware tool for hardware security research and hacking	Reverse engineering, debugging, emulating, sniffing, and tampering with various wireless communications
Rubber Duck	Microcontroller, USB connector	Emulates a USB keyboard to inject keystrokes and commands	Social engineering, password recovery, and privilege escalation
Raspberry Pi	Single-board computer, GPIO pins, Wi-Fi, Bluetooth, Ethernet, USB ports	General-purpose computing, programming, and automation	Network monitoring, penetration testing, and hacking

Hardware Hacking Tool	Specifications	Capabilities	Purpose
Arduino	Microcontroller, GPIO pins, USB connector	DIY electronics prototyping and automation	Robotics, sensors, and home automation
HackRF One	Software-defined radio, USB connector, antenna	Receives, decodes, and transmits radio signals	Wireless protocol analysis, jamming, and spoofing
LAN Turtle	Microcontroller, Ethernet connector, USB connector	Emulates a network device to perform automated attacks	Network reconnaissance, penetration testing, and hacking
Packet Squirrel	Microcontroller, Ethernet connector, USB connector	Man-in-the-middle attacks and network interception	Network monitoring, data exfiltration, and hacking
Shark Jack	Microcontroller, Ethernet connector, USB connector	Emulates a network device to perform automated attacks	Network reconnaissance, penetration testing, and hacking
O.MG Cable	Microcontroller, USB connector	Emulates a USB device to perform automated attacks	Social engineering, password recovery, and privilege escalation
Signal Owl	Microcontroller, Wi-Fi, Ethernet connector, USB connector	Wireless network reconnaissance, penetration testing, and hacking	Wireless network monitoring, data exfiltration, and hacking
Plunder Bug	Microcontroller, Ethernet connector, USB connector	Network monitoring and interception	Network reconnaissance, data exfiltration, and hacking
Bash Bunny	Microcontroller, USB connector	Emulates a USB device to perform automated attacks	Password recovery, privilege escalation, and network penetration testing
Key Croc	Microcontroller, Ethernet connector, USB connector	Emulates a USB keyboard to perform automated attacks	Social engineering, password recovery, and privilege escalation

Cyber-attacks in past (Hardware hacking attacks)

- **Stuxnet attack:** Stuxnet is a computer worm that targeted Iran's nuclear program by attacking industrial control systems (ICS). It spread through USB drives, exploited zero-day vulnerabilities in Windows, and manipulated the equipment it controlled. Stuxnet used advanced techniques to evade detection and was a notable example of hardware hacking on critical infrastructure.

- **Operation Cloud Hopper:** Operation Cloud Hopper was a cyber espionage campaign by Chinese hacking group APT10. They used a "supply-chain attack" to target technology, service providers, and telecommunications firms worldwide, stealing commercial secrets and intellectual property. What's notable is the use of hardware hacking

techniques like "BIOS implant" to infect the firmware of a computer's BIOS, gaining persistence and evading detection. This attack highlights the need for comprehensive security measures to protect against cyber-attacks.

- **The Equation Group:** A highly sophisticated hacking group believed to be affiliated with the NSA, the Equation Group developed and used a series of hardware hacking tools called "IronChef" to implant malicious firmware onto hard drives. This allowed them to gain persistent access to the targeted systems, even after reformatting or replacing the hard drives.

- **The Shadow Brokers:** A group that leaked a series of hacking tools developed by the NSA, including hardware hacking tools that could be used to exploit vulnerabilities in network hardware such as routers and firewalls.

- **Dragonfly:** A hacking group believed to be associated with the Russian government, Dragonfly launched a series of attacks on energy companies, targeting industrial control systems. They used a combination of phishing emails and hardware hacking techniques to gain access to these systems and manipulate their operations.

To protect the progress of humanity, we strictly need to address these kinds of attacks, and should train our IT professional to counter such hardware hacking attacks.

Precautionary Measures & Countermeasure Solutions

Hardware hacking attacks are becoming increasingly common and pose a significant threat to the security and privacy of hardware devices. In order to protect against these attacks, it is important to understand the methods used by attackers and to implement preventive and countermeasure solutions. This paper will provide an overview of the different measures that can be taken to protect against hardware hacking attacks.

1) Ensuring supply chain security can prevent the introduction of malicious components or devices into hardware systems.
2) Regular physical inspections can identify signs of tampering or unauthorised modifications using visual inspections or specialised equipment.
3) Physical security measures like locking up devices, using cable locks, or installing security cameras can prevent unauthorised access to hardware devices.
4) - Be cautious when connecting to unknown hardware or devices that make a connection to your device via a port or close-range communication system.
5) Limit access to sensitive hardware components to authorised personnel only and use remote wipe to erase sensitive information from a hardware device in the event of a security breach or theft.
6) Educate users and personnel on the importance of security, potential threats, and attack vectors through training, awareness programs, and simulated phishing attacks.
7) Conduct regular penetration testing to identify vulnerabilities and weaknesses in hardware systems and networks.
8) Implement regular software updates and strong passwords, encryption for sensitive data, antivirus software, intrusion detection systems, network segmentation, firewalls, authentication, authorisation measures, and access controls to secure hardware devices.
9) Try to be electronically sound by gathering knowledge about new hardware hacking tools and techniques to defend yourself from being a victim. This information can be gathered through following some hardware hacking events organised worldwide:
    - **DEFCON:** An annual hacker conference held in Las Vegas, Nevada, where hardware hackers showcase their latest creations and discuss current trends and advancements in the field.

- **Chaos Communication Congress (CCC):** An annual gathering of the international hacker community, where hardware hackers present their latest projects and ideas.
- **Black Hat:** A yearly security conference held in Las Vegas, Nevada, where security researchers and hardware hackers present their findings and discuss the latest security threats and vulnerabilities.
- **Hackers on Planet Earth (HOPE):** A biennial conference held in New York City that focuses on hacker culture, technology, and politics. Hardware hacking is one of the many topics covered at the conference.
- **Hardware Hacking Village (HHV):** A gathering of hardware hackers that takes place during DEFCON and other hacker conferences, where attendees can learn about hardware hacking, share their own projects, and collaborate with others in the community.

Detection/Prevention Mechanism for Master Tools

Hardware Hacking Tool	Targeted Systems	Detection/Prevention Mechanisms
Flipper Zero	IoT devices, car keys, smart homes, access control systems, and more	Limit physical access to devices, monitor Bluetooth, and implement device authentication
Rubber Duck	Windows, macOS, Linux	Disable USB ports, implement whitelisting, and monitor for suspicious USB activity
Raspberry Pi	Embedded systems, IoT devices, and more	Implement device authentication, limit network access, and monitor for unauthorized access
Arduino	Embedded systems, IoT devices, and more	Implement device authentication, limit network access, and monitor for unauthorized access
HackRF One	Wireless communications, IoT devices, and more	Implement encryption, use strong authentication, and monitor for unauthorized access
LAN Turtle	Wired networks, IoT devices, and more	Implement network segmentation, use strong authentication, and monitor for suspicious network activity
Packet Squirrel	Wired networks, IoT devices, and more	Implement network segmentation, use strong authentication, and monitor for suspicious network activity
Shark Jack	Wired networks, IoT devices, and more	Implement network segmentation, use strong authentication, and monitor for suspicious network activity
O.MG Cable	Windows, macOS, Linux	Disable USB ports, implement whitelisting, and monitor for suspicious USB activity

Hardware Hacking Tool	Targeted Systems	Detection/Prevention Mechanisms
Signal Owl	Wireless networks, IoT devices, and more	Implement network segmentation, use strong encryption, and monitor for suspicious network activity
Plunder Bug	Wired networks, IoT devices, and more	Implement network segmentation, use strong authentication, and monitor for suspicious network activity
Bash Bunny	Windows, macOS, Linux	Disable USB ports, implement whitelisting, and monitor for suspicious USB activity
Key Croc	Windows, macOS, Linux	Disable USB ports, implement whitelisting, and monitor for suspicious USB activity

Conclusion & Suggestions

In conclusion, hardware hacking is a practice of modifying or repurposing electronic devices for a specific use or to gain access to restricted features or functionality. It has a wide range of applications, including personal use, research, and product development. However, it's important to be aware of the potential risks and make sure to understand the consequences of any changes made to the device.

With the increasing popularity of hardware hacking, it will be interesting to see how it will continue to evolve in the future and how it will be applied in various fields. As well as we know that guns are not always used to kill somebody, they also help us to defend ourselves, during this research, researcher found out that if we are able to defend ourself effectively than despite being harmful, hardware hacking can become helpful too. Hardware hacking involves the modification and manipulation of electronic devices for various purposes. It can be helpful in several ways, including:

- Improving functionality: Hardware hackers often modify devices to enhance their performance or add new features.
- Security research: By finding and exploiting vulnerabilities in electronic devices, hardware hackers can identify and report security issues, helping to improve the overall security of the device.
- Innovation: Hardware hacking can lead to the creation of new technologies and advancements in the field of computer science.
- Cost savings: By hacking devices, individuals and organisations can save money by repurposing old or outdated equipment.

References

- "Best 15 Gadgets For Ethical Hackers on Amazon 2022" (Best Kali Linux Tutorials, September 11, 2022) <https://www.kalilinux.in/2021/06/hardwares-for-hackers.html> accessed January 30, 2023
- "Offensive Security Tool: Proxmark3 | Black Hat Ethical Hacking" (Black Hat Ethical Hacking, April 8, 2022) <https://www.blackhatethicalhacking.com/tools/proxmark3/> accessed January 30, 2023
- Mohieldin S, "Hardware Hacking 101: Introduction to JTAG" (River Loop Security, May 6, 2021) <https://riverloopsecurity.com/blog/2021/05/hw-101-jtag/> accessed January 30, 2023
- "Hardware Hacking and Social Engineering Tools in Kali Linux - GeeksforGeeks" (GeeksforGeeks, December 27, 2022) <https://www.geeksforgeeks.org/hardware-hacking-and-social-engineering-tools-in-kali-linux/> accessed Feb 20, 2023
- "An Introduction to Hardware Hacking" (2020) <https://www.cyberark.com/resources/threat-research-blog/an-introduction-to-hardware-hacking> accessed January 12, 2023
- Worsley S, 'A Fundamental Guide to Hardware Hacking' (EXPLIoT) <https://store.expliot.io/blogs/iot/a-fundamental-guide-to-hardware-hacking> accessed Feb 04, 2023
- 'Flipper Zero — Portable Multi-Tool Device for Geeks' (Flipper Zero-Portable Multi-tool Device for Geeks) <https://flipperzero.one> accessed January 30, 2023
- 'Hacking Tools & Media | Hak5 Official Site'(Hak5) <https://shop.hak5.org/> accessed Feb 15, 2023
- 'The Flipper Zero Is a Swiss Army Knife of Antennas' The Flipper Zero is a Swiss Army knife of antennas - The Verge (2022) <https://www.theverge.com/23433594/flipper-zero-hacking-gadget-wireless-pentesting-open-source-antenna> accessed January 30, 2023
- 'When Cyber-Attacks Target Hardware' (CNRS 2022) <https://news.cnrs.fr/articles/when-cyber-attacks-target-hardware> accessed January 30, 2023
- 'Matisoft Case Studies Page' <https://www.matisoftlabs.com/case-studies/stuxnet> accessed January 30, 2023
- 'Operation Cloud Hopper: What You Need to Know - Wiadomości Bezpieczeństwa' <https://www.trendmicro.com/vinfo/pl/security/news/cyber-attacks/operation-cloud-hopper-what-you-need-to-know> accessed January 30, 2023