A review of Trusting Trust, Internet Design and Cybercrime

1. A SUMMARY OF "REFLECTIONS ON TRUSTING TRUST" BY KEN THOMPSON

In his paper "Reflections on Trusting Trust", Ken Thompson presents a thought provoking article on the inherent risks of trusting code that is not entirely created by oneself. He emphasizes the vulnerability of computer systems to malicious attacks, particularly those targeting essential program-handling programs like compilers, assemblers, loaders, and even hardware microcode.

He discusses the concept of a "Trojan horse" program, which is a program that appears to be harmless but actually contains malicious code. Thompson explains how he created a Trojan horse program that could infect the compiler itself, allowing it to insert malicious code into any program compiled with it. He argues that this type of attack is difficult to detect and can be used to compromise the security of any system that relies on the compiler.

He criticizes the media's portrayal of hackers and similar groups, arguing that their actions constitute vandalism, trespass, and theft. He expresses concern over the inadequacy of the criminal code in addressing these activities and the efforts by vulnerable companies to update it. He also discusses the issue of computer security more broadly, arguing that it is important to take a holistic approach that includes both technical and social solutions.

He concludes by emphasizing the importance of trust in the people who write software, arguing that it is ultimately more important than trusting the software itself. The paper serves as a wake-up call, urging caution and responsibility in the rapidly evolving digital world.

2. A SUMMARY OF HOW INTERNET (INCLUDING IT'S SECURITY) WAS DESIGNED BY DAVID D. CLARK

In his talk at Google "Designing an Internet", David D. Clark presents an insightful idea about the multifaceted design considerations that shape the Internet's architecture. Security, scalability, reliability, flexibility, and efficiency are the key factors influencing its development.

To address security concerns such as unauthorized access and data integrity, protocols like firewalls and encryption are employed. The Internet's scalability is achieved through a hierarchical network architecture, enabling communication among numerous users and devices. Additionally, error correction and redundancy mechanisms ensure reliable data delivery.

Flexibility is embedded in the Internet's design through open standards and modularity, allowing for the incorporation of new technologies and applications. Its decentralized nature fosters adaptability and facilitates autonomous control by various entities.

Efficiency, crucial for swift data transmission, is achieved through high-speed networks and compression techniques. The Internet's evolution is driven by technical, economic, and social factors, emphasizing the need for reliable, scalable, and adaptable communication networks, cost-effective solutions, and fostering communication and collaboration.

3. A SUMMARY OF INVESTIGATING COMMERCIAL PAY-PER-INSTALL AND THE DISTRIBUTION OF UNWANTED SOFTWARE

The paper titled "Investigating Commercial Pay-Per-Install and the Distribution of Unwanted Software" investigates the commercial pay-per-install (PPI) ecosystem and its role in the distribution of unwanted software. The research reveals that PPI networks are actively involved in the distribution of unwanted software, including ad injectors, browser settings hijackers, and system utilities. The authors found that PPI networks are incentivized to circumvent user protections and continue to distribute harmful unwanted software. The study also highlights the various techniques used by PPI networks to evade detection, including the use of compressed files, password protection, and exploiting limitations in browsers.

3.1 Black-Market Services or Pay-per-install services or the cybercrimes

One of the black-market services discussed in the article is the use of PPI resellers to provide deceptive "promotional tools" that socially engineer web visitors into running PPI downloaders.

Pay-per-install services are a form of black-market service where cybercriminals pay to have their malware installed on already compromised machines. These services are a significant part of the malware ecosystem, providing a distribution network for various types of malware, including spyware, adware, and more destructive forms like ransomware.

The promotional tools include butterbars, ad banners, landing pages, and content unlockers. Butterbars are JavaScript stubs that generate a yellow bar at the top of a page alerting a victim that their "Flash player is out of date!" and initiate an auto-download or require a victim to click. Content lockers present victims with an enticing video, song, or PDF, but require a victim to install a "codec" to view the content. The research found that PPI resellers provide these tools to affiliates who do not operate download portals or peer-to-peer sharing sites.

Cybercriminals or the PPI resellers benefit from PPI services because they offer a low-cost, efficient way to spread malware. The services use a network of affiliates who are responsible for infecting and controlling the compromised hosts. Affiliates are often paid based on the number of successful installations, incentivizing them to infect as many machines as possible.

3.2 CounterMeasure

To safeguard against PPI network cybercrime, individuals and enterprises must implement robust countermeasures. These include keeping software up-to-date, exercising caution when downloading files, utilizing anti-virus software, and implementing comprehensive security policies.

Enterprises like IITH, in particular, should conduct regular security audits, provide employee training, and deploy advanced security systems.

Additionally, both individuals and enterprises can benefit from threat intelligence services, which provide valuable information on the latest cyber threats and vulnerabilities.

By adhering to these countermeasures and following cybersecurity best practices, individuals and enterprises like IITH can significantly reduce the risk of falling victim to PPI services cybercrime.