GROUP 2

Tracking IP addresses and catching cyber criminals

Introduction:

The digital age has kicked off towards a new era of connectivity, strengthening the individuals and businesses as well. On the other hand, this network has also created opportunities for cybercriminals to exploit the available vulnerabilities and do the significant harm. The challenge in tracing and catching these criminals for the law enforcement is evolving with the threats.

A tool that can be used by an investigator is IP address tracing. The presence of IP address with every device itself helps the authorities in tracing back to the malicious activity. But in the presence of change of method these crimes are become high level and keeping this very complex.

This report depicts the complication in the IP address tracing method and how it can limit the search of the criminals. The techniques, ITRACE, Hop-by-Hop traceback, Backscatter are examined here(Abolfazl Amirkhan). Alongside, how the practices like proxy servers, NAT, IP spoofing can influence the difficulty.

As the IP addresses can be masked easily this method alone would not be capable of finding the culprits. From Larson's(2017) work, we can understand the disadvantages that can be caused to the investigation due to the IP spoofing. As the IP addresses are dynamic by nature, it will be another hinderance, particularly when dealing with shared networks(Yinjie Chen).

Another significant role in this process is of the privacy laws. Legal and ethical considerations will play an important role on what can the investigators gather to find the attacker. So, it is really difficult to make a balance between the privacy rights and safety (Larson). As the crime can be across the borders the cooperation between the law enforcement of the respective jurisdictions is essential.

Despite the demerits of adapting this method, this is the approach that can be tried believing any techniques like spoofing have not been used by the attacker. By considering the pros and cons the law enforcement can decide on the effective utilization of this technique. This report can be a useful insight for the professionals to make the upcoming policies and implement them efficiently.

Background

There are many tools used currently to help assist law enforcement with catching criminals. Catching cyber-criminals can be tricky but a great way to help assist in this is by IP address tracing. With the tools such as Hop-by-Hop traceback, Backscatter, and ITRACE (Abolfazl Amirkhan).

When reviewing several investigative reports on how IP addresses can assist with catching cybers-criminals there were several issues that were presented.

Issues

IP tracing alone cannot effectively help create a cyber-criminal profile given the numerous tools that can be used to circumvent the identity of the host. For instance, IP spoofing, utilizing public networks and proxies to mask the identity of the host. Other complicated factors include "whether the IP address is static or dynamic8 and whether the user was on an unsecured or secured network." (Larson, 2017) For instance, NAT is used for wireless routers of small businesses and homes but "this mechanism enables multiple hosts with different private IP addresses connecting to Internet through one public IP address. Therefore, it creates difficulties for law enforcement to identify the cyber criminals, who are accessing illegal content." (Yinjie Chen, 2011) Or how public address can be used to commit a cybercrime although an IP address alone will narrow down the suspect list, it rarely leads directly to the suspect (Larson, 2017)Another issue that was found is the law. Yes, the law that helps put cybercriminals away is the same one that helps provide cybercriminal cushion to invade being picked. This is specifically related to privacy laws, which are becoming more important and relevant in modern times. Typically, a search warrant is used to obtain various evidence. An IP address can be used to get one. Criminals have "typically argue that they have a "reasonable expectation of privacy in the contents of [their] computer", and when law enforcement uses techniques that allow them to view that content without a warrant, their Fourth Amendment rights are violated.". (Larson, 2017) Another issue that has been raised when dealing with cyber-criminals is that across borders it is difficult when trying to collect information on this person due to privacy laws, the timing of collection of evidence, and the unwillingness of some countries to help charge and prosecute their citizens for those crimes.

Solution was presented by others to solve the issue

With the cooperation from the ISP, source IP address filtering can be applied to validate the packet being passed from the ISP to the Internet, meaning that a user cannot spoof the source IP address. (HO, 2010)

Law enforcement and ISP providers work together to prevent measures such as "ISPs similarly allow users to obtain new IP addresses when they desire" (Larson, 2017)

Results after implementing these precautions (success/failure)

There is still no regulation in place to force ISPs to set up filters and also different ISPs may encounter various issues when setting up the filter. Even if all ISPs in the world agreed to apply the source IP address filter, it might still take a while for all ISPs to implement it. (HO, 2010)

References

Abolfazl Amirkhan, D. V. (n.d.). *IPT Framework: A Technical & Administrative Approach for IP Packets.* Iran.

HO, W. C. (2010). *E-mail forensics: tracing and mapping digital evidence from IP address* . Auckland, New Zealand.

Larson, E. (2017). *Tracking Criminals with Internet Protocol Addresses: Is Law Enforcement Correctly* .

Yinjie Chen, Z. L. (2011). *Identifying Cyber Criminals Hiding behind.*