Research Methods and Professional Practice March 2022

Home / My courses / RMPP_PCOM7E March 2022 A / Unit 1 / Collaborative Learning Discussion 1 / Initial Post - Rouge Services

« Collaborative Learning Discussion 1

Shoumik Chakraborty

Initial Post - Rouge Services

77 days ago

2 replies

Last 56 days ago

Introduction:

Rouge Services offered “cheap, guaranteed uptime, no matter what”, which was misused by web-based customers to spam, carry on fraudulent activities, and spread malware.

Post multiple requests from ISPs and international organizations, the Rogue Service did not take down the malicious sites and services (owned by the customers of Rouge Service).

In retaliation, several government agencies and security vendors took down Rouge servers using DoS and targeted worm attacks (Association for Computing Machinery, N.D.).

Codes breached and Adhered

Rouge Services breached General ethical principles (Association for Computing Machinery, 2018) by avoiding their responsibility towards society and internet users who were being harmed by the malicious customers of Rouge Services. While retaining trustworthiness and adhering to “1.3 Be honest and trustworthy” (Association for Computing Machinery, 2018).

Rouge Services also breached the BCS code of conduct “PUBLIC INTEREST” while maintaining “PROFESSIONAL COMPETENCE AND INTEGRITY” (BCS, 2021)

Association for Computing Machinery (N.D.) states the Rouge Service was operating fairly within their jurisdiction, while their resources were maliciously used by customers and were forced to be closed by government organizations and security vendors which targeted their facility and destroyed the customer data of Rouge (Association for Computing Machinery, N.D.). Keeping in mind this has been a gross violation of all the principles of ACM and BCS. Since Rouge had multiple customers who are innocent and were affected grossly by the targeted attack. The question arises of who should be responsible.

Analysis

Rouge Services have documented SLAs which can't be breached, in this scenario they cannot take down the services due to allegations by other nations and jurisdictions.

The government officials of the affected country should get in touch with the appropriate justice system to carry out court orders instead of attacking a company, but it will have its challenge since this might take a long time and create bottlenecks in evidence gathering (Intersoft Consulting, N.D.).

This provides an opportunity for Rouge services and their customers to sue the government and the security vendors since they have destroyed data and intellectual properties held by Rouge Services and their customers.

References

Association for Computing Machinery. (2018) ACM Code of Ethics and Professional Conduct. Available from: https://www.acm.org/code-of-ethics [Accessed 13 March 2022].

Association for Computing Machinery. (N.D.) Case: Malware Disruption. Available from: https://ethics.acm.org/code-of-ethics/using-the-code/case-malware-disruption/ [Accessed 13 March 2022].

BCS. (2021) Code of Conduct for BCS Members. Available from: https://www.bcs.org/media/2211/bcs-code-of-conduct.pdf [Accessed 13 March 2022].

Intersoft Consulting. (N.D.) GDPR Third Countries. Available from: https://gdpr-info.eu/issues/third-countries/ [Accessed 13 March 2022].

Reply

Maximum rating: -

2 replies

1

Post by **Shiraj Ali** **65 days ago**

Peer Response

Shoumik,

To extend your analysis on Malware Disruption, I would like to add that when cybercriminals want to spread malware (malicious software), they employ a network of websites, servers, computers, and files (C Ife, 2021).

One of the most significant dangers to cybersecurity today is malware and botnets. As a result, law enforcement agencies, security firms, and researchers are always looking for ways to disrupt these harmful operations through what are known as takedown counter-operations. These takedowns have had a mixed record of success. Botnets and malware delivery operations responding to takedown attempts is also poorly known.

Researchers studied different independent malware delivery operations' upstream servers and dropper networks. Malware operators prefer to transfer their activities elsewhere following a takedown or, in one case, openly defy it. Researchers also observed that the malware operators analysed used distributed distribution architectures (especially CDNs) and a high reliance on a few "super binaries." They provide new information about how malware spreads, which should be incorporated into future anti-malware efforts (Ife et al. 2021).

C Ife, C., (2021) *Measuring and Disrupting Malware Distribution Networks: An Interdisciplinary Approach.*. Ph. D. University College London.

Ife, C., Shen, Y., Murdoch, S. and Stringhini, G., 2021. Marked for Disruption: Tracing the Evolution of Malware Delivery Operations Targeted for Takedown. *24th International Symposium on Research in Attacks, Intrusions and Defenses*,.

Reply

2 Post by **Shoumik Chakraborty** **56 days ago**

Summary Post

Introduction

Rouge Services offered guaranteed uptime for hosting client environments, this service was misused by the criminals to spread malware affecting innocent users. When agencies requested Rouge Service to discontinue their existing malicious customers, its request was disregarded due to SLA between Rouge System and their clients (Association for Computing Machinery, N.D).

The government agency along with security vendors took down all Rouge Service servers using DOS and targeted worm attack. During the attack, also affected innocent customers of Rouge and lead to service disruption and destruction of data (Association for Computing Machinery, N.D).

Analysis

Although Rouge service, the Government agencies, and Security Vendors have breached the BCS and ACM code of conduct.

Rouge Services Government agencies & Security vendors breached the BCS code of conduct “PUBLIC INTEREST” (BCS, 2021).

The crackdown on malware by law enforcement agencies always has mixed success since the malicious users move their systems to another network whenever there is a crackdown. (C Ife, 2021)

Conclusion

Now, the question arises if the crackdown by the government bodies over rouge services solved the problems related to malware? Or the whole process ended up disrupting services for innocent users.

Since the issues with the Rouge Service could have been handled by the government agencies by involving the law enforcement of the country hosting their servers instead of taking down all the customers (Intersoft Consulting, N.D.).

References

Association for Computing Machinery. (N.D.) Case: Malware Disruption. Available from: https://ethics.acm.org/code-of-ethics/using-the-code/case-malware-disruption/ [Accessed 13 March 2022].

BCS. (2021) Code of Conduct for BCS Members. Available from: https://www.bcs.org/media/2211/bcs-code-of-conduct.pdf [Accessed 13 March 2022].

C Ife, C., (2021) *Measuring and Disrupting Malware Distribution Networks: An Interdisciplinary Approach.*. Ph. D. University College London.

Intersoft Consulting. (N.D.) GDPR Third Countries. Available from: https://gdpr-info.eu/issues/third-countries/ [Accessed 13 March 2022].

Reply

Maximum rating: -

Add your reply

Your subject

Type your post

Choose Files no files selected

Submit

Use advanced editor and additional options

OLDER DISCUSSION

General feedback for formatives in Unit 1&2

NEWER DISCUSSION

Summary Post