Case study: Cyber attack

Author’s name

[Institutional Affiliation(s)]

Author Note

Case Study: Cyber Attack

In the twenty-first century, organizations and governments are more concerned on the security on their cyber front then they are on their physical one. The thoughts of cyber-warfare have echoed throughout the world as the world witnessed one cyber-attack after the next. This paper will discuss a case study in which a gang of hackers disguising themselves as the notorious “fancy bears”, the Russian hackers who were involved in compromising the security of the white house in 2014. The goals and objectives of these hackers along with their techniques will also be discussed in this paper.

# Attack Case Study

## Overview

The part of the Russian establishment responsible for cyber-attacks is named as fancy bears. This name became a brand after devastating cyber-attacks on the white house in 2014. This attack was based on intimidating the enemy into thinking that the notorious group “fancy bears” was actually trying to attempt a DDOS attack on their server and thus tricking them to pay up (“RDoS attacks by fake Fancy Bear hit banks in multiple locations,” n.d.).

## Perpetrators

Perpetrators of this attack remain anonymous to this day, as they attempted to perform this attack using already compromised bot networks.

## Attack Scenario

### Goals

The group aimed at exploiting financial firms through sending them an intimidating ransom letter in which it disguises itself as “fancy bear”. The demand of money usually two bitcoins is also mentioned in this ransom letter (Bussoletti, 2019).

### Skills / Training

High level of knowledge in the field of network security especially exploit development and vulnerability analysis along with solutions to provide a high degree of anonymity.

### Preparation Time

This is hard to estimate. The majority of the time would probably be required to gain the maximum amount of anonymity and to test the weakest point in the backend server. The DDOS attack will then not be much of an issue.

### Personnel

A group of people who are highly trained in writing automated exploits on backend servers which have a lack of DDOS mitigation mechanisms.

### Equipment

A group of systems or preferably a network of previously compromised bots which would provide the number as well as the anonymity required for the attack.

### Timing Constraints

The basic time constraint for this attack will be equal to the time required by the company to install advanced DDOS mitigation mechanisms in its backend server.

### How It Happens?

The gang sends a detailed and intimidating ransom letter stating their aim and identity. It at the same time, also sends a small-scale demo DDOS attack for the company to understand the severity of the situation. The ransom letter also mentions the deadline for the money and the time for the attack afterwards (“A DDoS gang is extorting businesses posing as Russian government hackers | ZDNet,” n.d.).

### Collateral Results

Several other groups started to use the same technique disguising themselves as a known hacker group and sending ransom letters to companies. Such groups tried to impersonate famous hacking gangs such as Anonymous, Armada Collective etc.

### Recommended mitigation

In-time development and installation of DDOS mitigation mechanisms for backend servers to make sure that no downtime is recorded when the DDOS attack occurs.

## Risk Management

### Cyber-security architecture

The organization at risk for such an attack are those who have not prepared their back-end servers for such attacks. Cyber-security organizations which provide large scale network security services need to adapt quickly to be ready for such future incidents.

### Privilege Controls

The authorized users of the bank or the organization should also be given restricted access to the bank’s resources i.e. privileged access can increase the chances of an attack manifold.

## References

A DDoS gang is extorting businesses posing as Russian government hackers | ZDNet. (n.d.). Retrieved December 7, 2019, from https://www.zdnet.com/article/a-ddos-gang-is-extorting-businesses-posing-as-russian-government-hackers/

Bussoletti, F. (2019, October 28). Cybercrime, a fake Fancy Bear threats companies with DDoS attacks. Retrieved December 7, 2019, from Difesa e Sicurezza (difesaesicurezza.com) website: https://www.difesaesicurezza.com/en/defence-and-security/cybercrime-a-fake-fancy-bear-threats-companies-with-ddos-attacks/

RDoS attacks by fake Fancy Bear hit banks in multiple locations. (n.d.). Retrieved December 7, 2019, from https://www.group-ib.com/blog/fakeapt28