Week 05 Assignment 5-3

William Slater

CYBR 625 – Business Continuity Planning and Recovery

Bellevue University

After Action Report and IR Discussion

Sue Sampson, M.S. - Professor

September 30, 2012

After Action Report and IR Discussion

This brief paper will discuss a recommended After Action Report for a case study involving a large Chicago-based retailer. It will also review recommended improvements for the Incident Response Report.

Disaster for Discussion

The chosen scenario was a disaster that was triggered at a Chicago-based retailer by a botnet attack that occurred as the result of a zero-day exploit in the Microsoft Internet Explorer web browser by botnet malware originating from eastern Europe (Desmond, M., 2006).

Disaster Summary

The following figure from Desmond's article summarizes the botnet malware disaster that occurred at the Chicago-based retailer that occurred between November 1, 2005 and December 13, 2005.

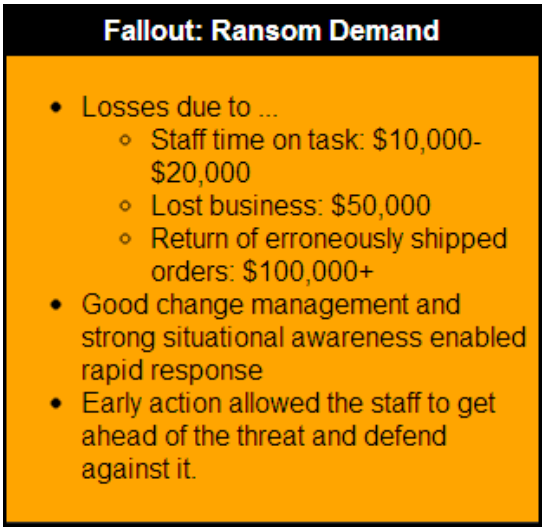

Figure 1 (Desmond, M., 2006).

After Action Report

The following After Action Report form was taken from the Whitman and Mattord, text.

After Action Report	
Disaster Type:	Botnet Malware Exploit from eastern European gang impacted e-commerce at a major Chicago-based retailer during December 2005, at the peak of the online buying season. The attackers then demanded $100,000 ransom to stop the attack.
Trigger:	Botnet Malware exploited a zero-day exploit in the Microsoft Internet Explorer browser. In one day, over 2000 bogus orders were created.
Team Lead:	Probably the IT Security Manager and/or the CISO.
Notification Method:	Probably e-mail and phones.
Response Time:	Less than one day.
Actions during the disaster:	
1. The company's IT team were notified when bogus orders started to originate from the e-commerce website.	
2. Log analysis revealed that it was originating from sources in Eastern Europe.	
3. The company's IT staff moved quickly to implement a CAPTCHA solution. CAPTCHA stands for Completely Automated Public Turing test to tell Computers and Humans Apart. It thwarted the botnet malware because increased the complexity required for customers to interact with the retailer's e-commerce website, and it prevented the botnet from placing bogus order transactions.	
4. The Microsoft Internet Explorer vulnerability patch was applied.	
Actions during the disaster were complete when:	The actions were completed after the CAPTCHA solution was put into place and the Microsoft patch was implemented.
Actions after disaster:	
1. The company's IT Security team documented the impacts of the disaster.	
2. The company's management reviewed the steps taken during the disaster to understand how well the Disaster Response worked and to see if anything could have been done better.	
Actions before disaster:	
1. There was a Disaster Response Plan in place.	
2. The Security Team members and the IT Server Support Team members each understood their roles and how to perform their responsibilities. Having good analysis skills and technical skills with which to respond lessened the economic impacts of the disaster.	
3. The company's IT Security Team leadership was decisive and capable of effective leadership during a disaster.	

(Whitman and Mattord, 2007).

Incident Response Review

The presence of a Disaster Response plan as well as quick thinking and responsiveness of the IT staff led to a rapid resolution of this issue. While it was unclear from the scenario write-up, local law enforcement and the FBI should have both been contacted, because anytime such activities that are the obvious result of criminals, particularly those based in outside the United States, it becomes a matter that requires the involvement of trained law enforcement professionals.

Conclusion

Most retail companies do a large percentage of their business between the last week of November and Christmas day. The attackers chose an opportune time to unleash this botnet malware in order to catch the retailer at a critical time so they could cause a panic and collect their ransom. Having good plan and a competent staff ensured that the damage was minimal. Nevertheless, it was the right thing to do to review the actions taken during a disaster and document these in an After Action report to keep as a Lessons Learned. Such documentation will also allow for any necessary improvements that should be made, so other IT staff members will know what to do if and when a similar event occurs in the future. Finally, everyone should be aware of the importance of involving local law enforcement and the FBI, especially because they may be aware of related events such as a cyber attack on other targets inside the U.S.

References

Desmond, M. (2006). Worst Case Scenarios: When Disaster Strikes. An article of disaster case studies published at Redmond Magazine's website on February 1, 2006. Retrieved from http://redmondmag.com/Articles/2006/02/01/WorstCase-Scenarios-When-Disaster-Strikes.aspx?p=1 on September 27, 2012.

Gregory, P. (2008). IT Disaster Recovery and Planning for Dummies. Indianapolis, IN: Wiley Publishing.

Nelson, B., Et al. (2010). Guide to Computer Forensics and Investigations, fourth edition. Boston, MA: Course Technology, Cengage Learning.

Van Wyk, K R. and Forno, R. (2001). Incident Response. Sebastopol, CA: O'Reilly.

Wallace, M. and Webber, L. (2011). The Disaster Recover Handbook: A Step-by-Step Guide to Ensure Business Continuity and Protect Vital Operations, Facilities, and Assets, second edition: New York, NY: American Management Association.

Watters, J. (2010). The Business Continuity Management Desk Reference: Guide to Business Continuity Planning, Crisis Management & IT Disaster Recovery. Northamptonshire, UK: Leverage Publishing.

Whitman, M. E. and Mattord, H. J. (2007). Principles of Incident Response & Disaster Recovery. Boston, MA: Course Technology – Cengage Learning