

Incident Response

Daniel M Beck

UMGC – SDEV-360

August 11, 2020

Incident Response

Introduction - What is Incident Management?

Incident Management aims “to restore the service to the customer as quickly as possible, often through a work around or temporary fixes, rather than through trying to find a permanent solution” (ITIL – A Guide to Incident Management). The Incident Management response being examined will be created based on the incident occurring where in one day, large sums of money were withdrawn from several networked ATM systems by the same user ID.

The Incident Management Response

This Incident Response was created because a hacker was able to withdraw large sums of money from several networked ATM systems by the same user ID in one day. The following shows the steps that are being taken to mitigate and protect against attacks.

Preparation

Although there was a successful attack, it is important to know what preparations were made to try and stop the attack. Reviewing these preparations after the attack is mitigated will help reinforce any new preparations and the ones currently in place.

Since these ATM's are connected to the same network, each one is equipped with malware, antivirus, and spyware protections. These protections monitor the network activity and continuously updated for improved defense against malware, antivirus, spyware, and other known malicious attacks. As security risks change daily, all systems are equipped with the updating ability to accept any necessary patches.

Firewalls are set into each terminal to create more defense against intrusions. The firewalls will monitor incoming and outgoing network traffic, deciding whether to allow or block specific traffic based on a defined set of security rules.

Event logs are set up in each machine to record any suspicious or unusual activity. The logs are recorded back to the bank's security team when suspicious activity is found.

Building of Incident Response team: Since threats are common with banking systems, an Incident Response team is created to mitigate any threat as quickly as possible. The team includes:

- An Incident Response manager who oversees and prioritizes different steps in detection, analysis, and containment of the incident. “In case of high severity incidents, IR manager also interfaces with the rest of the company, including corporate security, human resources, etc. to convey findings, status, and requirements” (Bandos, n.d.).
- Security analysts who are typically comprised of IT specialist and developers that created the software, that dig into identify the risk when an incident occurs and what is happening during that period.
- Threat researchers complement security analysts by providing threat intelligence and context to the incident. “They are constantly combing the internet, identifying intelligence that may have been reported externally. They then build an internal database of internal intelligence derived out of prior incidents” (Bandos, n.d.).

Detection and Reporting

With the preparation phase being set up, event logs detected large sums of money being withdrawn from several networked ATM systems by the same user ID in one day. An incident ticket has been generated, reporting the incident to the Incident Response team with a high-level of severity and the account holder has been notified of the breach and their account has been locked out.

An endpoint analysis shall be completed to determine what footprints may have been left behind by the threat actor. Gathering of artifacts needed to build a time line of activities. In the endpoint analysis, an analysis of “a bit-for-bit copy of systems from a forensic perspective and capture RAM to parse through and identify key artifacts to determine what occurred on a device” (Bandos, 2019).

A binary analysis shall be completed to Investigate malicious binaries or tools leveraged by the attacker and document the functionalities of those programs. This analysis is performed in two ways that include:

- A behavioral analysis that executes the malicious program in a virtual machine to monitor its behavior.
- A static analysis that aims to “reverse engineer the malicious program to scope out the entire functionality” (Bandos, 2019).

Enterprise hunting is done to “analyze existing systems and event log technologies to determine the scope of compromise. Document all compromised accounts, machines, etc. so that effective containment and neutralization can be performed” (Bandos, 2019). This analysis will also determine whether this attack can be used with other account holders or if it was isolated to one account.

Containment, Eradication, and Recovery

The first task for the Incident Response team, along with removing any inappropriate materials or components, is to confine and mitigate the vulnerability to prevent further disruption and/or spread to the other systems or users. Following that, conducting additional investigation and analysis that may be of perceived higher severity (Incident Management and Response). They will determine whether the firewalls, malware, antivirus, and/or spyware protections that

are in place were bypassed to gain access. If it was found that one of these protections were at fault, a new type of increased protection needs to be created or purchased.

Once the vulnerabilities are spotted, the Incident Response team needs to find out “if more affected hosts are discovered, repeat the incident response steps as needed. Redeploy securely configured systems to an operational state and confirm that the systems are functioning normally. Implement additional monitoring to look for future incident-related activity” (Incident Management and Response).

Acquire, preserve, secure, and document all evidence that pertains to the attack that may be used for law enforcement or legal purposes later. This will be important to be able to retrieve the money that was stolen as well as catching the attacker.

Post-Incident Activity

Considering that the attack was done with one user ID, the account holder will be asked to generate a new password and PIN code in case their previous one was compromised. The money that was taken from their account was returned along with the creation of new debit cards.

After the vulnerability has been mitigated, more work is needed to prevent similar occurrences from happening again in the future. Documenting every action that was taken to mitigate the issue so that if a similar instance may occur, the same steps can be taken to mitigate the vulnerability more effectively.

Closely monitoring for activities of this nature since threat actors will most likely reappear. Taking from the binary analysis of the threat will allow for the creation of notifications should this issue arise again (Bandos, 2019).

In the static analysis where the vulnerability was reverse engineered, the engineering team that completed the reverse engineering will continue to try and develop software that can mimic the attack. This will allow for the creation of increased securities within ATM network.

Conclusion

In order for an incident response to occur in an effective way, all the tasks and processes being performed must be viewed from an enterprise perspective meaning that the identification of interactions and communications, how tasks are done, how the processes relate, how information is exchanged, and how actions are coordinated, need to occur. An incident response “involves defining a process to follow with supporting policies and procedures in place, assigning roles and responsibilities, having appropriate equipment, infrastructure, tools, and supporting materials ready, and having qualified staff identified and trained to perform the work in a consistent, high-quality, and repeatable way” (Killcrece, 2013). With the procedures that are set within this response form, the vulnerability in the systems where, in one day, large amounts of money were withdrawn from several networked ATM systems by the same user ID, shall be mitigated and prevent future vulnerabilities of this nature from occurring.

References

Bandos, T. (2019, June 26). The Five Steps of Incident Response. Retrieved August 10, 2020, from <https://digitalguardian.com/blog/five-steps-incident-response>

Bandos, T. (n.d.). Incident Responder's Field Guide. Retrieved August 11, 2020, from <https://info.digitalguardian.com/rs/768-OQW-145/images/Incident-Response-eBook-teaser.pdf>

Incident Management and Response. (n.d.). Retrieved August 10, 2020, from <https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/resources/information-security-guide/incident-management-and-response>

ITIL – A Guide to Incident Management. (n.d.) [PDF]. UCISA.

Killcrece, G. (2013, July 2). Incident Management. Retrieved August 10, 2020, from <https://us-cert.cisa.gov/bsi/articles/best-practices/incident-management/incident-management>