Digital Edge

DIGITAL EDGE CASE STUDY:
Cybersecurity Incident Response

Slava Rykhva
Security Engineer
Digital Edge Ventures
7 Teleport Drive
Staten Island, NY 10311

1. Summary

Digital Edge team was tasked to help contain and eradicate a virus outbreak. A response team was gathered and after the initial kick-off call, the team started cleaning/investigation activities.

2. Analysis

The outbreak happened December 4th 2018, before the involvement of Digital Edge's team. According to Symantec Endpoint Protection statistics – the initial infection happened to a particular workstation. By the end of the day, the infection spread to five workstations, including three user workstations and two servers. By the end of December 5th, another eleven workstations were infected.

Initial infection was reported by Symantec Endpoint Protection as "Heur.AdvML.S.C" and "WS.Malware.1". This is a generic classification that Symantec assigns detections caught by heuristic modules. The nature of such detection assumes that there was no better detail as to what the source of infection was, or what activities were performed by the malicious software. Initial infected files were not preserved during AV cleanup, thus deeper analysis isn't possible.

Based on the reported behavior and how quickly the infection spread, we believe that the initial infection was done by self-replicating work. This is used to establish further connection to an external server and carry malicious payload (e.g. infected computers would become the part of a larger botnet) as well as download additional malicious software.

By the time the Digital Edge team was involved, another trojan was detected on the network. We were able to collect some samples, and confirm that the new malware belonged to the family of trojans called "Emotet". This is a family of advanced and modular trojans which can perform three activities:

1. It acts as a dropper – meaning that it can be used to install other trojans
2. It acts as a downloader
3. It acts as a banking trojan itself, harvesting credentials for known banking sites.

EMOTET has been around for several years, and until now, it was among the most invasive trojans. Each known generation targets specific countries, and its spread in the US began in July 2018.

It is a polymorphic trojan, which can avoid standard signature-based detection methods, as well as having enough intelligence to detect when it's running in a sandbox environment (controlled virtual environments) and change its behavior accordingly. An example was seen when connection attempts were made from physical machines to Russian and Ukrainian Ips, however, when the same was done to a virtualized environment (both within our security lab and with virtualized servers on the network) in Japan and Singapore, servers did not respond.

3. Actions Taken

Digital Edge's team created an action plan once we had confirmed that our clients' network was affected by malware. It included the following steps:

1. Incident response team was formed
2. Digital Edge's technicians were sent onsite.
3. All traffic to and from any country other than the US was blocked at a Firewall level.
4. All workstations and servers were isolated from the network. This means that both infected and clean systems were disconnected. (This goal was to ensure that viruses are no longer spread across the network.)
5. Once all of the machines were disconnected, the Incident Response Team ran automated checks through an Anti-virus (Symantec Endpoint Protection, N-Able AV Defender) and Anti-malware (MalwareBytes, RKill, ComboFix) software scan on the servers. Once the automated scans were finished, a manual sweep was also done, looking for signs of undetected malicious software. While doing the manual sweep, IRT was looking for known patterns of malware self-enforcement by registering itself in services, posing as a browser toolbar or windows explorer helper, and putting itself as auto-start entries, to ensure that no malware code resided in the computer's memory (since it could restore itself).
6. After all activities were carried out, computer was rebooted several times, to ensure that malicious software would not recover.
7. While cleaning computers, Digital Edge technicians also ensured that SMB v1 support had been disabled on all machines.
8. Once technicians finished cleaning computer, it was hooked to network, and manually checked once again by Digital Edge senior personnel.

These activities were performed during the evening (12.6.18), overnight, and into Friday morning (12.7.18) all servers and most user workstations were confirmed clean.

Digital Edge Operations group started to monitor Symantec Logs manually on an hourly basis with escalation to notify incident response team if any new alerts got generated.

Once the first sweep was done, automated deep full system scans were initiated, and on December 8 these scans also reported a number of tracking cookies on several systems. These were tracking cookies, which were created by advertisement serving sites during regular browsing. We know the sites that created them, but the users never accessed those sites directly – they served advertisement blocks on many different sites, and user browsing history is regularly deleted with CCleaner application, which makes an investigation almost impossible. As such, no analysis was done to find the source of the cookies, but instead it was to ensure that no new malware was introduced in another round of deep scans (both automated and manual) that was run on affected systems.

On December 10th, another full automated scan revealed two more viruses on a File share server. They were analyzed and deleted before any more damage could be done. These files however, were isolated incidents and not related to the malware outbreak.

On December 13th, it was reported that there had been a suspected incident on several additional PCs. There was attempted traffic (failed DNS name resolution requests) for Russian sites, which were known to be advertisement-servicing sites, but also had been known to distribute malware. An investigation was launched, but no evidence of new malware infection was found.

On December 15th, we disabled Geo Filters on the Firewall and reviewed the network traffic for any suspicious activity. No new network intrusion events occurred. Wireshark was used to inspect traffic on a few workstations but no malicious activity was found.

4. Possible Source of Infection

During the investigation, the Digital Edge team studied available logs, archived emails, and firewall traffic. Unfortunately, those logs did not provide full technical details, and there was no possibility to reach a definite conclusion that the source of the infection had been due to the lack of collected data.

Based on attack vector, and cross-referencing data with similar attacks, available data suggests that one of the company users became a victim of phishing attack (either received fishing email or followed a fishing site on the internet). We cannot say who that user was with 100% certainty, but Symantec logs suggest that the initial infection came from one of the hosts.

5. Conclusion

Digital Edge's most important recommendation is to change all user passwords and inform users to change credentials for all sites they might have visited since December 4th.

Next, we highly recommend implementing changes to the company policy, for users who are administrators on their PCs. Regular user accounts should be restricted, and not run with highly elevated permission. If some legacy application requires to be run with Administrative privileges, those applications should be clearly known, as well as the computers on which they are running. Such hosts should be treated as high-risk environments, with more strict access and network restrictions policies.

Some other recommendations include:

- Disable macros support for MS Office applications. If macros support is required, then files within macro modules should be carefully analyzed and only then approved as trusted.
- Consider removing Apple Flash player on all computers.
- EMOTET Malware has been known to mask as Flash player.
- Create system-wide group policy to disable SMB v1 on all machines, to automatically control any new machines or reinstallations.
- Setup automated email notifications for any identified AV incident for analysis.
- Store traffic headers with Firewall to be able to run traffic analysis in similar configurations.
- Consider deployment of centralized traffic capture solution, which could assist with investigations regarding traffic flow (enabled on-demand, otherwise capture of traffic headers with SonicWall should be enough).
- Implement stronger Web Filter policies to limit users' web activity and provide logging.