Mandatory Assignment 4

Bendik Egenes Dyrli, Øystein Andreassen, Anne Grethe Heltne

03.11.2017

Case summary

The case follows “Logan Industries” which is a multi-national catalog sale corporation with 30 offices, spread across 30 states and 3 countries with 2600 employees. The company believes that having anti-virus products installed on their desktops and servers are adequate preparation for a malware attack. The company is infected by a worm called “BadBoy” which it fails to recognize , and spreading itself by email attachments and using social engineering to entice the victim to launch the attachment, thus infecting its own system. The worm also tries to be persistent by creating copies of itself on the infected system's startup items, it also writes itself into existing executables on the system to further make removal problematic.

It also had an intention to spread across other computers, and did so by mailing itself to everyone that was to be found in the Outlook address book. After the so called “transportation” of the virus was done, the machine would reboot and never recover.

Because of no good routines for reinstalling systems, and it taking time for the anti-virus manufacturer to create a solution to automatically detect and clean systems and files the whole incident from first infection to when the H.Q. is up and running again spans over a whole week, and estimated loss of $18M.

Countless of companies were in need of shutting down their services, due to malicious attacks infiltrating their work computers.

Use case 1

Case

First infection on the 5th of February, which an employee downloaded, renamed and executed an attachment which pretended to be from the CEO of the company.

Solution

Users should be trained on how to recognize malicious emails and suspect attachments, even from within the company and trustworthy sources. If a user is in doubt they should be taught to forward the email to the IT department that could help verify the legitimacy of the email.

Abuse case 2

Case

On the 7th of February, a sales manager uses his laptop and subsequently infects his laptop and a server, which had previously been “cleaned” of the virus.

Solution

Infected system should be completely removed to prevent further infection, instead of manually cleaning having an imaging service one could simply reinstall the computers instead of cleaning them.
IT should also have actively searched and removed emails from users inboxes which contained the “.app” extension, while also denying email with the extension from being sent even inside the organization.