Encrypted SAIL brain incident 1/8/2017:
Summary, Analysis, Timeline, Actions to take

EXECUTIVE SUMMARY

The main agency filesystem (SAILbrain) was found to be maliciously encrypted on Monday morning 1/8/2017) by staff. Staff were asked to logout and cease all file/folder activity. Server was restored to a known-good state using virtual machine snapshot backup. Analysis was performed over the next 24 hours. All files/folders were made available to staff by beginning of next work day. No known data was transmitted out of the agency. No data was lost during the incident.

TIMELINE

Staff (Tristan) reported to IT (me) at approx. 9:45 a.m. that staff couldn't open any documents on the 'sailbrain' fileserver. Seemingly all files had been changed from normal to ending with 'stopstorage@qq.com.java' making them unusable. This looked very suspicious. IT discussed with the acting Director plan of action: staff were asked to logout of their workstations and discontinue all activities on the fileserver until further notice.

IT discovered that not all files on the server had been modified. There were a great number of files that were NOT affected. Upon analysis, all files that were modified had been modified by the SAIL 'bookkeeping' staff id as owner. All files that were modified were in fact accessible by the 'bookkeeping' staff id. Files/folders in which this account did not have permissions to access were not affected. IT went to the home directory for 'bookkeeping', and found a text file named 'FILES ENCRYPTED.txt'.

The contents of this file indicated that 'all' files had been encrypted, and in order to get files back, an email needed to be sent to stopstorage@qq.com. Preliminary research online indicated that this email address had been abandoned some time ago - we were on our own.

A snapshot of the encrypted file server was created and taken offline. The last known good state of the fileserver (1/5/2018 9:30 p.m.) was then brought online. IT staff then allowed JUST accounting to complete payroll activities to fulfill all payroll requirements (payroll was due Wednesday), then logout. Then IT proceeded to spend the next 24 hours doing deep antivirus/antispyware/antimalware scans of the file servers and staff workstations.

The file server was inspected the next morning at 5:00 a.m. and was found to be 100% free of any encrypted files, leading IT to believe that the scanning/cleaning the previous day removed the source of the attack. Staff were notified via email 8:00 a.m. that all was well and they can login and use the files/folders normally.

ANALYSIS

No known data was transmitted offsite. The attack was rather crude (the presence of the text file, including typos) make it seem like it was an older variant of the well-known 'BTCware' ransomware attack. The email address to which instructions said to contact were believed to have been abandoned long ago. Other victims have tried to contact upon incident, with no response ever received. SAIL's antivirus/antispyware/antimalware system indicated that the systems were clean. After deep scanning using other tools, it was found that on the remote desktop server, there was a malware in the accounting staff account that is the suspected culprit. It does not seem like an active attack - it was a file that was lying dormant that decided to do its thing independently. The suspect file has been permanently deleted.

FINDINGS

The fact that the agency files/folders reside on a virtual server, and that regular full snapshots of the server are performed and kept, made it fairly trivial to restore the server to a known good state. The time spent/work was done on the post restore system analysis to root-cause and remove any offending issues.

All is online now. 0% data loss. An entire day of Staff not being able to access any files/folders for a day while IT was doing the analysis and deep scanning all files/folders/servers and workstations was lost. It could have been much worse, however, if not for the regularly scheduled snapshots and backups that were on hand. IT should investigate a secondary file/folder scanner to not rely 100% on one particular tool to find everything. Staff have too broad permissions/access. Not all staff need access to everything all the time. Network should be segmented to reduce the visibility in the case of an intrusion incident.

FURTHER ACTIONS

IT should work with leadership team to better segment the file server and divide the files/folders into departments, and grant permissions to things based on job role/need, rather than grant full access to everything for everyone. This will help to reduce the impact of a further incident.

IT will develop a multi-tiered approach to scan and remove any suspected virus/spyware/malware. Currently, SAIL uses one tool: Symantec's Enterprise Endpoint Security. It is an industry standard, but has been found to not be able to find everything all the time. More than one method should be deployed.

IT will continue to guarantee that backups are kept functioning.

IT will work to segment the network into a more secure environment - dividing it into servers, network, phones, workstations, etc. and to limit the communication between segments on a need-to-access basis. This will mitigate any intruders from having full visibility in the case of a breach. This work had been started already before the incident - should become a priority.