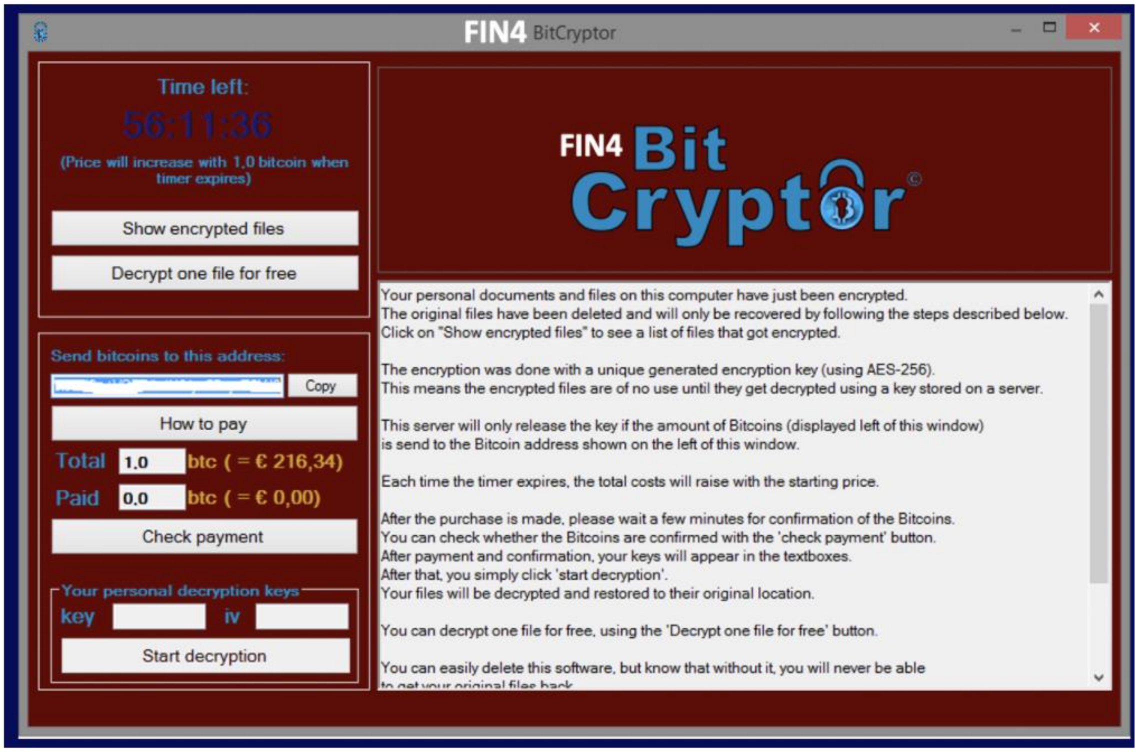
First Update - 9:00am Monday

- Hospital A, Hospital B, and Hospital C each noticed that when trying to log into their centralized log management systems, the following message pops up.



Time left:

56:11:36

(Price will increase with 1,0 bitcoin when timer expires)

Send bitcoins to this address:

[redacted]

Total 1,0 btc (= € 216,34)

Paid 0,0 btc (= € 0,00)

Your personal decryption keys

key

iv

Your personal documents and files on this computer have just been encrypted.
The original files have been deleted and will only be recovered by following the steps described below.
Click on "Show encrypted files" to see a list of files that got encrypted.

The encryption was done with a unique generated encryption key (using AES-256).
This means the encrypted files are of no use until they get decrypted using a key stored on a server.

This server will only release the key if the amount of Bitcoins (displayed left of this window)
is send to the Bitcoin address shown on the left of this window.

Each time the timer expires, the total costs will raise with the starting price.

After the purchase is made, please wait a few minutes for confirmation of the Bitcoins.
You can check whether the Bitcoins are confirmed with the 'check payment' button.
After payment and confirmation, your keys will appear in the textboxes.
After that, you simply click 'start decryption'.
Your files will be decrypted and restored to their original location.

You can decrypt one file for free, using the 'Decrypt one file for free' button.

You can easily delete this software, but know that without it, you will never be able
to get your original files back

The ransomware notes, that pops up on the infected log servers

- The hospitals have disclosed that each incident started with a user in the technology department opening an email attachment resource. This activity has not yet been seen in Hospital X.

Action: Conduct research to understand what type of threat could be involved, who is the threat actor behind the threat, and how they are motivated, and what attack tactics they are using or might use in the future. Add a threat profile to the report template. Follow the steps below to do so:

1. Review the ransomware attack details provided by Hospital A, B, and C. Gain a understanding of the attack vector, specifically the ransomware message as shown in the image above and the method of entry.

2. Conduct detailed research to identify the ransomware type used in the attacks. Determine the specifics of the ransomware, such as its encryption methods, demand specifics (e.g., bitcoin payment).
3. Investigate potential threat actors and their motivations. Understand who is behind these attacks (state-sponsored, criminal gangs, hacktivists) and why they target healthcare institutions. Use the **MITRE attack framework (opens in a new tab)**to investigate the threat and threat actors.

Second Update - 11:00am Monday

- Five more hospitals report being targeted. All hospitals have a few things in common, including they all endorsed the new healthcare law that was passed. You've learned from your legal team that your hospital endorsed the law as well.
- They've noticed that the attackers are consistently targeting Windows systems that contain centralized log files and backups. They are also taking advantage of an unpatched Windows vulnerability to execute the attack.
- *Tip*: The IP address for your main log server is the IP address of your Azure virtual machine. You store all of your logs and backup logs in your data center on-site. Full backups are conducted once on the first of every month. Though you always change the default passwords, you haven't enforced strong passwords consistently with your users.

Action: Use Nessus to run a vulnerability scan against the VM (127.0.0.1 target) and analyze results. Summarize what you found. Consider the key vulnerabilities that were exploited within the other companies. Assess your assets and current mitigating controls to confirm if the threat could be relevant to your company. Make a recommendation for the order in which the findings should be addressed and what action is required. Running Nessus scans has been explained in the lesson, Vulnerability scanning, Finding security vulnerabilities.

Conduct an abbreviated penetration test against your user's accounts. Access the provided list of password hashes from your company and try to crack your own user's passwords using HashCat. Are there any weak passwords you discovered?

Tip: As you pull together your command line string for hashcat, you can find and use the default dictionary provided within HashCat, leverage your own .dict file, or try other attack modes within HashCat.

Third Update - 1:00pm Monday

You've received the following note from your helpdesk team.

- Several doctors, nurses, and administrative staff have called in noting that they are being asked to pay one million dollars in Bitcoin to access their systems. The control systems used to monitor patient stats are no longer available through the standard user interface. Some doctors report being unable to render treatments because they cannot view detailed information about patient status.
- You attempt to log into your log analysis tool, but that's no longer accessible.
- Your security leader has declared this a critical security incident.

Action: Outline the next steps you recommend taking in the report template.