Katrina Barkwell

7712173

**[2] What simple action did MalwareTech do that disabled the ransomware?**

He registered the (previously) unregistered domain WannaCrypt was trying to connect to.

**[3] What is the explanation provided by MalwareTech as to why this disabled the ransomware? Provide the explanation in your own words in no more than 2 sentences**

In a misguided attempt at anti-analysis, WannaCrypt used a single hardcoded domain to check if it was in sandbox and exit preventing further analysis. When MalwareTech registered this domain it caused all infections worldwide to think they were in a sandbox and exit, thus ending the spread.

**3) Read the paper titled The Akamai Network: A Platform for High-Performance Internet Applications (a link will be provided on the web site) and answer the following questions:**

**[1] What are peering points? Why are ISPs reluctant to invest in improved service for peering points?**

Peering points are the locations at which ISPs will connect and exchange traffic between users on each separate network (usually for free). There is little economic incentive for ISPs to improve service for peering points. Money can be made at the beginning with (website hosting) and at the last step (end users) - but there’s money to be gained in the middle.

**[1] Why is TCP particularly inefficient when used for transfer of video or other large files over large (> 3000 km) distances?**

TCP carries significant overhead. Middle mile congestion (which ISPs have no incentive to improve) makes packet loss more likely.

It’s particularly inefficient when used for video/large files because the significant overhead TCP carries. The receiver needs acknowledgements for every window of data packets sent, which means the distance between server and end user can become the bottleneck in download speeds and video quality (ie. throughput is inverse to network latency round time).

**[1] What is origin scalability? What is end-to-end application scalability?**

Origin scalability is your initially ability to scale. Unfortunate this is difficult to predict and easy to underprovision or overprovision for, resulting in a bad user experience or lost money. End-to-end application scalability means the whole experience from origin server capacity to network bandwidth is available at all points and works well. This means they are also prepares for unexpected peaks, events, or attacks.

**[2] What is Akamai's System Design Principle regarding network failures? Explain how this principle relates to the decision to use 'commodity' servers instead of expensive servers with significant hardware redundancy.**

Akamai's philosophy is that “failure are normal, and the delivery network must operate seamlessly despite them”. In the interest of designing with recovery in mind, robust commodity servers are used. Commodity servers are lower end servers dedicated to filling out server programs and associated tasks. There are diminishing returns on redundant hardware, but is still important to immediately identify and remove failing software. Because commodity servers are lower end they are considered easy to replace/disposable.