

ASSIGNMENT WORK ON CYBER CRIME

Information Security & Cyber Law

(DCO-603)



(Apple Targeted in \$50 Million Ransomware Hack of Supplier Quanta)

Submitted to:

Dr. Sunil

Assistant Professor

Computer Engineering

Submitted by:

Aatif Nayeem

DCS- VI Semester

18DCS003

Section of Computer Engineering

Department of University Polytechnic

Faculty of Engineering & Technology, Jamia Millia Islamia

New Delhi – 110025

2020-21

CASE STUDY

BloombergQuint (An Indian business and financial news organization, a joint venture of Bloomberg News and Quintillion Media) published that “*Apple Targeted in \$50 Million Ransomware Hack of Supplier Quanta*” at 12:00 PM on April 21, 2021.

According to BloombergQuint news, As Apple Inc. was revealing its newest line of iPads and flashy new iMacs on Tuesday, one of its primary suppliers was enduring a ransomware attack from a Russian operator claiming to have stolen blueprints of the U.S. company’s latest products.

The ransomware group REvil, also known as Sodinokibi, published a blog on its darkweb site early on Tuesday in which it claimed to have infiltrated the computer network of Quanta Computer Inc. The Taiwan-based company is a key supplier to Apple, manufacturing mostly Macbooks. It similarly produces goods for the likes of HP Inc., Facebook Inc. and Alphabet Inc.’s Google.

By early on April 20, REvil’s ‘Happy Blog’ -- a site where the cartel publicly names and shames victims in hopes of coaxing ransom payment -- declared Quanta its latest victim. In their post, also reviewed by Bloomberg, the hackers claim they’d waited to disclose the Quanta compromise until the date of Apple’s latest big reveal, contending the parts supplier had expressed no interest in paying to

Quanta acknowledged an attack without explaining if or how much of its data was stolen.

“Quanta Computer’s information security team has worked with external IT experts in response to cyber attacks on a small number of Quanta servers,” the company said in a statement. “We’ve reported to and kept seamless communications with the relevant law enforcement and data protection authorities concerning recent abnormal activities observed. There’s no material impact on the company’s business operation.

By the time Apple’s product launch was over, REvil had posted schematics for a new laptop, including 15 images detailing the guts of what appears to be a Macbook designed as recently as March 2021, according to the documents reviewed by Bloomberg.

The images which was posted by REvil group are:

Happy Blog

Blog search

Search

Quanta Computer INC.

Quanta Computer Incorporated (TWSE: 2382) (Chinese: 廣達電腦; pinyin: Guǎngdá Diànnǎo) is a Taiwan-based manufacturer of notebook computers and other electronic hardware. Its customers include Apple Inc., Dell, Hewlett-Packard Inc., Alienware, Amazon.com, Cisco, Fujitsu, Gericom, Lenovo, LG, Maxdata, Microsoft, MPC, BlackBerry Ltd, Sharp Corporation, Siemens AG, Sony, Sun Microsystems, Toshiba, Verizon Wireless, and Vizio.

Products:

Apple Watch

Apple Macbook Air

Apple Macbook Pro

ThinkPad Z60m

In order not to wait for the upcoming Apple presentations, today we, the REvil group, will provide data on the upcoming releases of the company so beloved by many. Tim Cook can say thank you Quanta. From our side, a lot of time has been devoted to solving this problem. Quanta has made it clear to us that it does not care about the data of its customers and employees, thereby allowing the publication and sale of all data we have.

P.S.

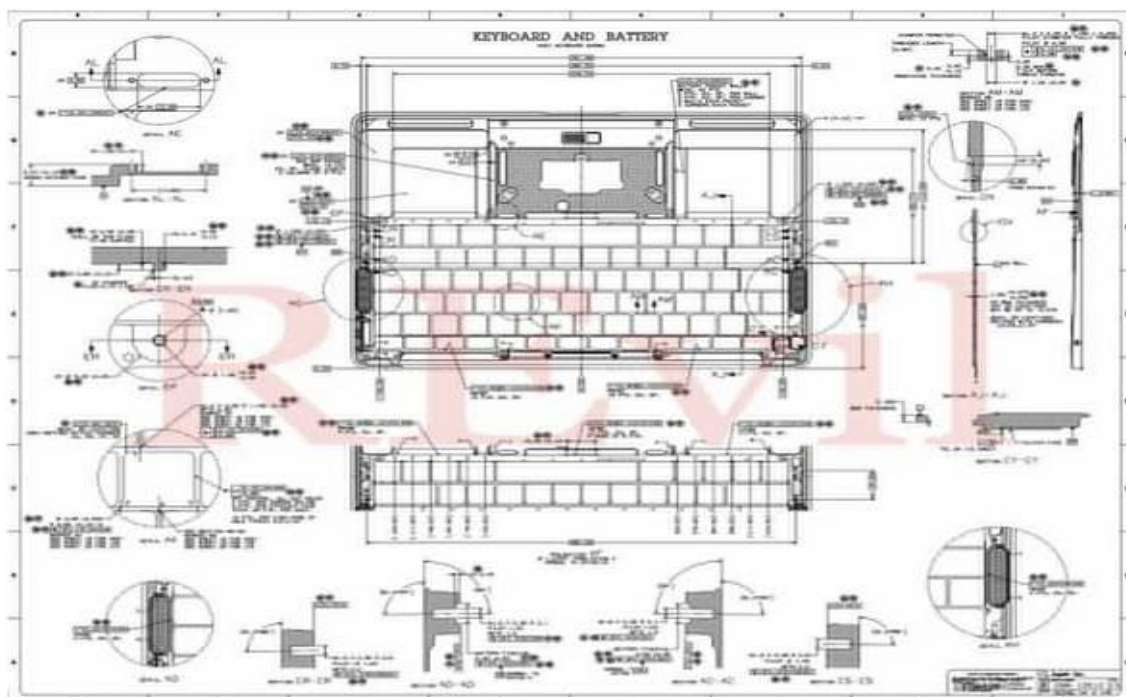
Our team is negotiating the sale of large quantities of confidential drawings and gigabytes of personal data with several major brands.

We recommend that Apple buy back the available data by May 1.

More and more files will be added every day.

The same is in pdf format

Proofs:



Some of the Questions which arises are:

What is Ransomware?

Ransomware is a type of malicious software (malware) that threatens to publish or blocks access to data or a computer system, usually by encrypting it, until the victim pays a ransom fee to the attacker. In many cases, the ransom demand comes with a deadline. If the victim doesn't pay in time, the data is gone forever.

Who are REvil?

REvil is a ransomware-as-a-service (RaaS) operation that has extorted large amounts of money from organizations worldwide over the past year. Its name stands for Ransomware Evil and was inspired by the Resident Evil movie series. According to recent reports from security firms, it is the most widespread ransomware threat and the group behind it doubles down on its extortion efforts by also stealing business data and threatening to release it.

Under which section of IT Act this Cyber Crime belongs?

By reading the news and after the case study I decided that this cyber crime comes under the section 66A of IT Act.

As section 66A of IT Act states that

- a) any information that is grossly offensive or has menacing character; or
- b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device; or
- c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages, shall be punishable with imprisonment for a term which may extend to three years and with fine.

Explanation. -For the purpose of this section, terms "electronic mail" and "electronic mail message" means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message.

What are the penalties of this Cyber Crime?

The penalties and punishment of this Cyber Crime is that the person should be punishable with imprisonment for a term which may extend to three years and with fine.