

## REvil gang tries to extort Apple, threatens to sell stolen blueprints

By Sergiu Gatlan

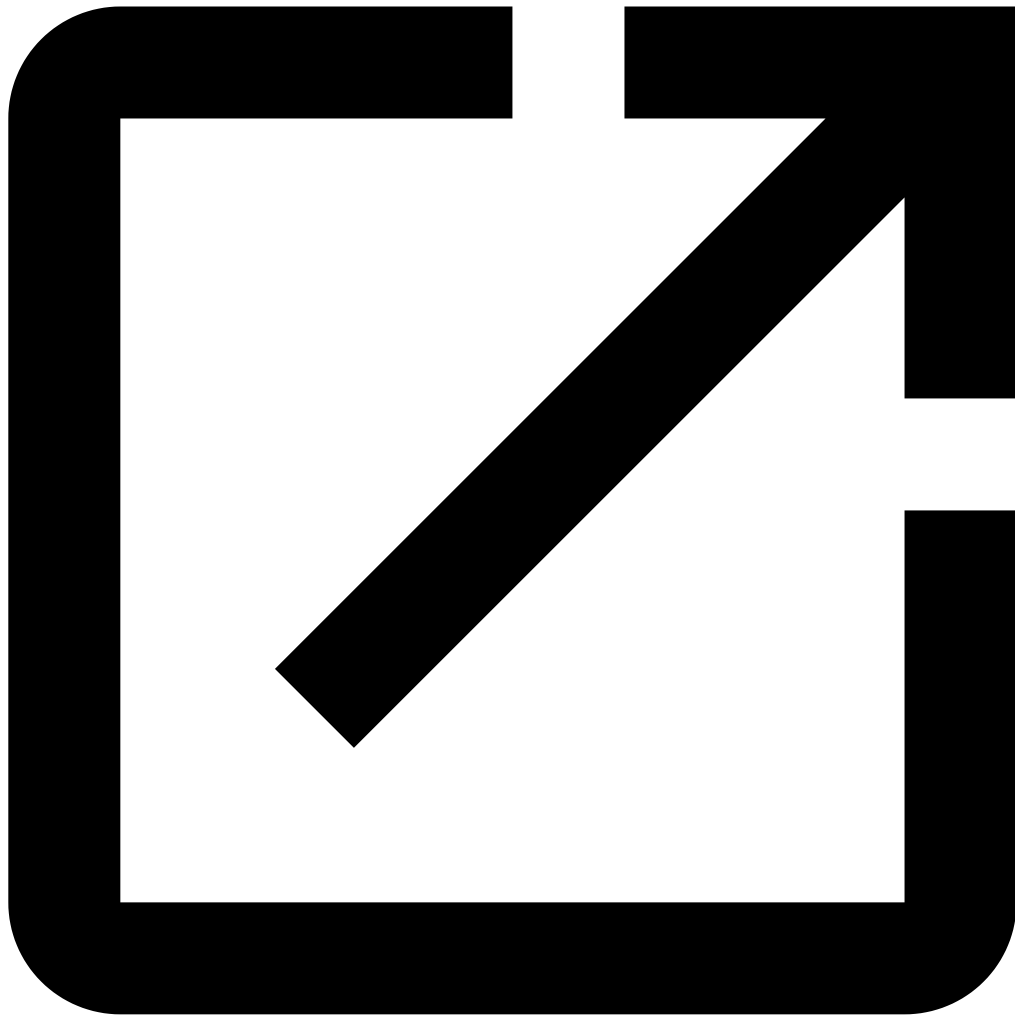
Published: 2021-04-20 · Archived: 2026-04-05 13:05:58 UTC



The REvil ransomware gang asked Apple to "buy back" stolen product blueprints to avoid having them leaked on REvil's leak site before today's Apple Spring Loaded event.

The ransomware gang wants Apple to pay a ransom by May 1st to prevent its stolen data from being leaked and added that they are also "negotiating the sale of large quantities of confidential drawings and gigabytes of personal data with several major brands."

REvil tried to extort Apple only after [Quanta Computer](#), a leading notebook manufacturer and one of Apple's business partners, refused to communicate with the ransomware gang or pay the ransom demanded after they allegedly stole "a lot of confidential data" from Quanta's network.



Visit Advertiser website [GO TO PAGE](#)

Quanta is a Taiwan-based original design manufacturer (ODM) and an Apple Watch, Apple Macbook Air, and Apple Macbook Pro maker.

Quanta has a long list of high-profile customers, including Apple, Dell, Hewlett-Packard, Alienware, Lenovo, Cisco, and Microsoft.

Based on the number of ODM laptop units sold, Quanta is the world's second-largest original design manufacturer of laptops, only behind Compal who was [also targeted by ransomware](#) last year.

According to the Tor payment page shared with BleepingComputer, Quanta has to pay \$50 million until April 27th, or \$100 million after the countdown ends.

## Your network has been infected!



Your documents, photos, databases and other important files encrypted



To decrypt your files you need to buy our special software - General-Decryptor



Follow the instructions below. But remember that you do not have much time

### General-Decryptor price

the price is for all PCs of your infected network

You have **6 days, 08:38:15**

\* If you do not pay on time, the price will be doubled

\* Time ends on **Apr 27, 06:48:26**

Current price

**123028 XMR**  
≈ 50,000,000 USD

After time ends

**246056 XMR**  
≈ 100,000,000 USD

### Quanta ransom demand

So far, REvil leaked over a dozen schematics and diagrams of MacBook components on its dark web leak site, although there is no indication that any of them are new Apple products.

In a negotiation chat on REvil's payment site seen by BleepingComputer, REvil warned that "drawings of all Apple devices and all personal data of employees and customers will be published with subsequent sale" if Quanta did not begin negotiating a ransom.

After that time frame expired, REvil published the schematics on their data leak site.

You have 3 hours left to contact us for a dialogue, after which you can forget about discounts when paying and keep this incident confidential.

Drawings of all Apple devices and all personal data of employees and customers will be published with subsequent sale

6 hours ago

### Quanta payment page chat

[REvil](#) is a ransomware-as-a-service (RaaS) operation known for recruiting affiliates to breach corporate networks, steal unencrypted data, and encrypt devices.

Once a ransom payment is made, the REvil core developers and the affiliates split the payment, with the affiliates generally getting the larger share.

REvil has been on a hacking spree over the last month, demanding extremely high ransom demands in attacks targeting [Acer \(\\$50 million\)](#), [Pierre Fabre \(\\$25 million\)](#), and [Asteelflash \(\\$24 million\)](#).

Cybersecurity researchers have told BleepingComputer that they believe REvil has been making extremely high demands to start at a higher negotiation price.

"Quanta Computer's information security team has worked with external IT experts in response to cyber attacks on a small number of Quanta servers," a Quanta spokesperson told BleepingComputer.

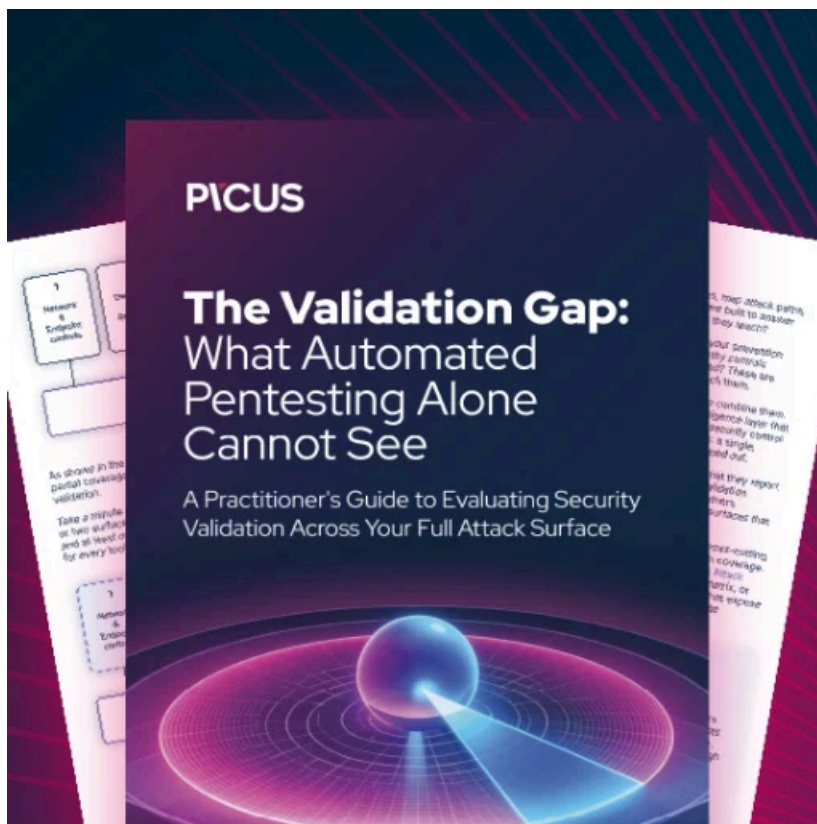
"We've reported to and kept seamless communications with the relevant law enforcement and data protection authorities concerning recent abnormal activities observed. There's no material impact on the Company's business operation.

"The information security defense mechanism was activated in no time while conducting a detailed investigation to ensure containment and recovery of data are in process and a small range of services impacted by the attacks were brought back to normal.

"Consequently, we upgraded the level of cybersecurity by reviewing and enhancing current infrastructure for information security and protection."

An Apple spokesperson was not available for comment when contacted by BleepingComputer earlier today.

*Update: Added statement from Quanta.*



### **Automated Pentesting Covers Only 1 of 6 Surfaces.**

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

---

Source: <https://www.bleepingcomputer.com/news/security/revil-gang-tries-to-extort-apple-threatens-to-sell-stolen-blueprints/>