《全新勒索病毒爆发 分析师指责网络安全性能差》

The data-scrambling software epidemic that paralyzed computers globally is under control in Ukraine, where it likely originated, as companies and governments around the world counted the cost of a crisis that is disrupting ports, hospitals and factories.

More than 24 hours after it emerged, the hackers have nearly gathered 4 bitcoin, worth just over 10,000 US dollars at current prices, according to the attackers' publicly available bitcoin wallet.

It's a relatively meager haul given the virulence of the malware outbreak, and some researchers are citing it as further evidence that the cyberattack was intended not to make money but to send a message.

Ransomware, which has been powered by the growth of digital currencies such as Bitcoin, is a fast-growing and lucrative market for cybercriminals. It works by scrambling computers' data, only unscrambling it in return for money.

But Matthieu Suiche, founder of Dubai-based Comae Technologies, said in a blog post that the engineering of the bug suggested that those behind it had no intention of ever retrieving the data, even if they were paid. In other words, he said in a telephone interview, the ransom demand was "a mega-diversion."

Analysts believe the reason for a quick spread of the malicious software that is crippling computers globally is the widespread ignorant approach to information security and the lack of software updates.

Andrey Bryzgin of Russian cyber security company Group-IB said on Wednesday that such attacks are efficient "because the approach to information security is still very immature."

He said it was too soon to know who is behind the latest attack.

Ukraine and Russia appeared hardest hit by Tuesday's violent outbreak of data-scrambling software that locks up computer files with all-but-unbreakable encryption and then demands a ransom for its release.

Russia's Rosneft oil company said some of its gas stations have been affected by the outbreak of malicious software, but production operations haven't been hurt. Russian media reported that Rosneft subsidiary Bashneft was also affected.

In the US, it affected companies such as the drugmaker Merck and food conglomerate Mondelez International.

Logistics firm FedEx said deliveries by its TNT Express subsidiary have been slowed by the global cyberattack. In an announcement on Wednesday, the company based in Memphis, Tennessee, said it had been "significantly affected" by the malicious program.

FedEx said that the domestic, regional and intercontinental operations of TNT Express, a courier delivery unit, were “largely operational, but slowed.” The company added that the impact of the cyberattack “could be material.”

The virus’ pace appeared to slow by Wednesday, in part because the malware appeared to require contact between computer networks.

(Source: AP)