Hong Kong firm becomes latest marketing company hit with REvil ransomware

By Written by Jonathan Greig, ContributorContributor Oct. 5, 2021 at 3:27 p.m. PT

Archived: 2026-04-05 13:07:42 UTC

Hong Kong marketing firm Fimmick has been hit with a ransomware attack, according to a British cybersecurity firm monitoring the situation.

ZDNET Recommends

Fimmick has offices in Hong Kong and across China, serving several high-profile clients like McDonalds, Coca-Cola, Shell, Asus and others.

Their website is currently down, and there was no response to *ZDNet* requests for comment. Matt Lane, CEO of UK-based cybersecurity firm X Cyber Group, said his team routinely "scrutinizes the activities of cybercriminals for evidence of their behaviors" as a way to protect clients and customers.

On Tuesday, they discovered that REvil had breached Fimmick's databases and claimed to have data from a number of global brands. Lane shared screenshots showing REvil's threatening posts toward Fimmick that included information stolen from the company's website.

"We discovered this intelligence as part of those routine activities. We noted, with interest, that the attacker's 'Happy Blog' also appears to be temporarily unavailable but have no further information as to why that might be," Lane said, adding that the criminal group also shared a directory structure of the stolen data.

"You can see Cetaphil, Coca-Cola, Hana-Musubi and Kate Spade are listed."

Ransomware gangs have targeted marketing firms multiple times over the last few years because of their ties to larger companies with more valuable data.

John Hammond, the senior security researcher at Huntress, said that for ransomware operators, the most attractive targets are the ones that lead to even more targets.

"In the same vein that cybercriminals prefer a spray-and-pray approach -- always opting for the easiest targets and the low-hanging fruit -- ransomware gangs love a one-to-many approach, which requires less effort to bring greater results," Hammond said.

"Marketing firms, PR firms, and organizations that integrate closely with other businesses could have a plethora of data and information that make targeting the next victim even easier. Much like service providers, attacking one could start a domino effect to target others that the original victim worked with. Attacking a marketing firm or PR firm allows ransomware gangs to get a bigger bang for their buck."

Allan Liska, a ransomware expert with cybersecurity company Recorded Future, said there have been at least three other marketing firms hit with ransomware over the last year.

Wieden+Kennedy was attacked in November 2020 but was forced to notify Oregon Department of Justice officials in April after employees' personal information was exposed during the incident. MBA Group was hit in March and Empirical Research Partners in September.

"I don't know if they are particularly ripe compared to other industries, but I could see marketing firms being more vulnerable to attack, especially phishing attacks as they are used to dealing with a diverse client base and likely receive a lot of emails with attachments, which is a favorite initial access vector for many ransomware groups," Liska said.

"The actual number of marketing firms hit is likely much higher, but unlike hospitals or schools, when a marketing firm gets hit with ransomware, it doesn't make the news."

Security
