Celebrity jewelry house Graff falls victim to ransomware

By Pieter Arntz

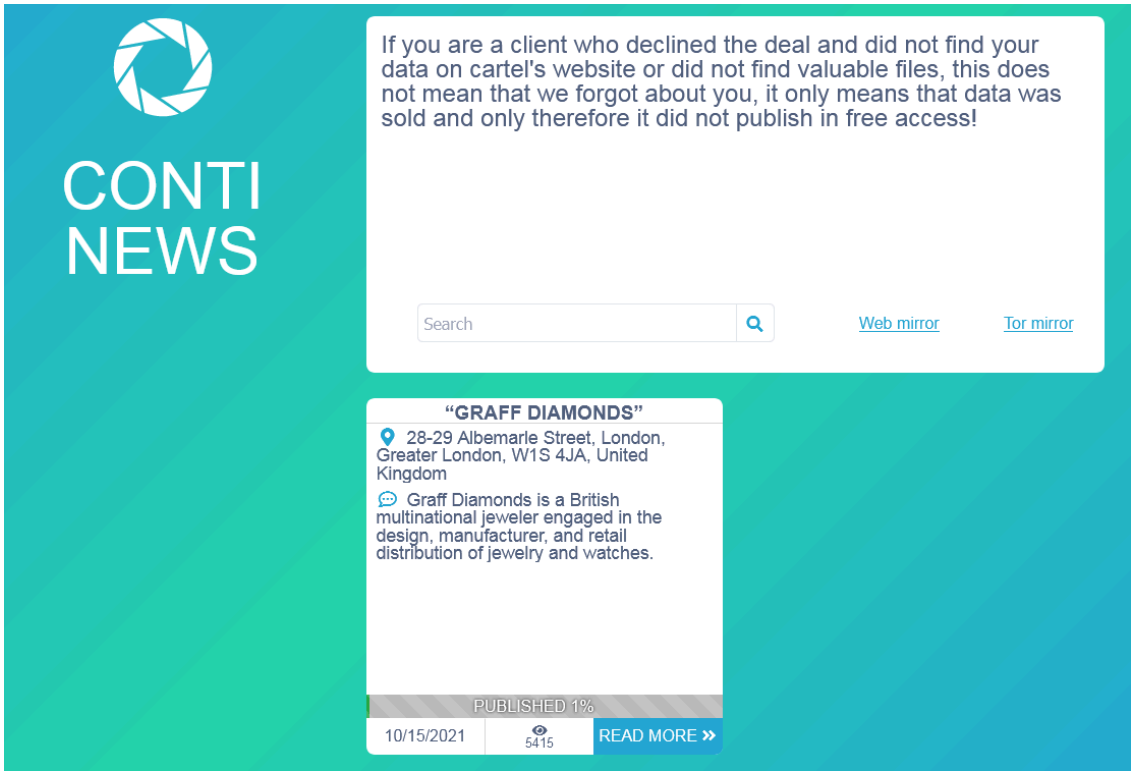
Published: 2021-10-31 · Archived: 2026-04-05 19:47:06 UTC

Data on countless celebrities, including politicians, is apparently now in the hands of ransomware attackers after a group using the Conti variant compromised systems of one of the world's most exclusive jewelry houses, Graff.

Despite what mathematicians like to think, there is an exception to every rule. When we wrote in our Demographics of Cybercrime Report that money (or its absence) changes our sense of safety, that wasn't meant to imply that the rich feel like they're bigger targets. Quite the opposite, those that don't have money were found to feel less safe online. But the fact that the rich are, in fact, more attractive targets is of course true.

High-end targets

The personal information of celebrities like Oprah Winfrey, David and Victoria Beckham, Tom Hanks, and Melania and Donald Trump were stolen during a ransomware attack on Graff. The Conti Ransomware gang have claimed responsibility.



Conti is one of the gangs that, besides encrypting files, exfiltrate data from the compromised systems. When the victim refuses to pay the ransom, the gang publishes the exfiltrated data, or sells them to the highest bidder. Conti recently announced that they will also publish data as soon as details or screenshots of the ransom negotiations process are leaked to journalists.

The Conti gang also recently made the news recently when they put the access to compromised networks up for sale, as well as when some underpaid turncoat leaked their manuals, technical guides, and software on an underground forum.

According to Graff, the vast majority of clients have not been the victim of personal data loss and those that were affected have been informed by mail.

The target

From the all-caps official statement on its site, Graff is shaken but not stirred.

> "PLEASE BE ASSURED THAT WE REACTED SWIFTLY TO SHUT DOWN OUR NETWORK AND DIRECTLY INFORMED THOSE INDIVIDUALS WHOSE PERSONAL DATA WAS AFFECTED, ADVISING THEM ON APPROPRIATE STEPS TO TAKE. WE ALSO NOTIFIED THE INFORMATION COMMISSIONER'S OFFICE AND CONTINUE TO WORK WITH LAW ENFORCEMENT AGENCIES. FORTUNATELY, THANKS TO OUR ROBUST BACK-UP FACILITIES, NO DATA WAS IRREVOCABLY LOST. WE WERE ABLE TO REBUILD AND RESTART OUR SYSTEMS WITHIN DAYS TO CONTINUE TO OPERATE EFFECTIVELY AND ALL OUR SHOPS AND ECOMMERCE PLATFORM WERE UNAFFECTED AND CONTINUED TO OPERATE WITHOUT INTERRUPTION."

The investigation

A spokesman for the UK's Information Commissioner's Office (ICO), which can impose fines of up to 4% of a company's turnover for failing to comply with the Data Protection Act, said:

> "We have received a report from Graff Diamonds Ltd regarding a ransomware attack. We will be contacting the organization to make further enquiries in relation to the information that has been provided."

Unfortunately, knowing who did it and knowing who to arrest, and how, are two very different things when it comes to cybercrime. Sometimes attribution is hard, but even in cases where law enforcement knows who is behind the attack, it doesn't make it easy to apprehend the evil-doers.

In this case, the group that was behind the attack made a public confession and published proof, but we don't know the real names of the people in this group. We have good reason to assume that they are in Russia, but even of that we can't be sure.

It is only in rare cases that cybercriminals travel to countries where they run the risk of being extradited to the US or another country where there is a warrant out for them.

What's next?

In the case of high-end jeweler Graff, it doesn't sound as if they have plans to pay the ransom, so it is highly likely that more of the exfiltrated data will be published on the Conti leak site.

The data that were stolen do not seem to be of an alarmingly private nature. Conti has been known to attack targets in the public health sector where far more delicate information is to be found. But maybe with this attack it has angered some people that have the power to make things happen.

Want to know more about Conti?

- Malwarebytes threat profile
- CISA alert on Conti Ransomware

About the author

Was a Microsoft MVP in consumer security for 12 years running. Can speak four languages. Smells of rich mahogany and leather-bound books.
