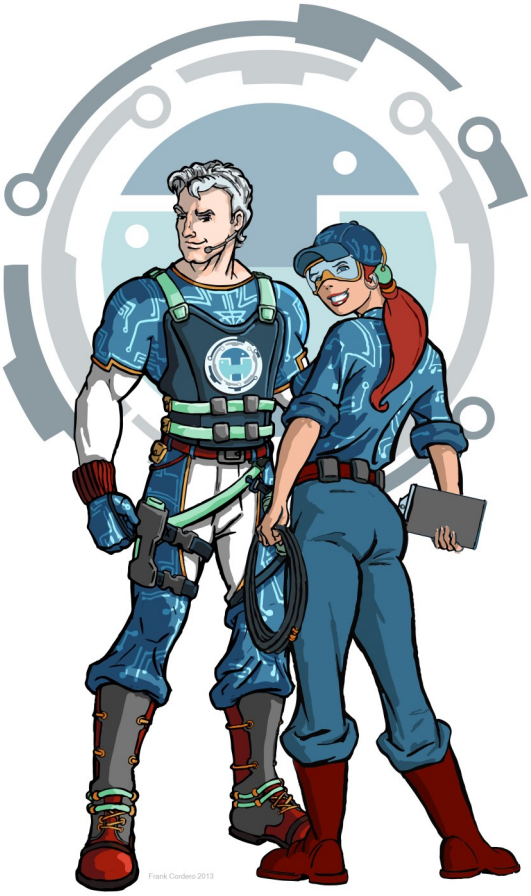
TechTips Newsletter

Insider Tips To Make Your Business Run Faster, Easier And More Profitably



REvil Ransomware attack: How bad is it? It's very bad

Over the usually sedate long holiday weekend, a major cybersecurity incident roiled the world. The cybercriminal gang known as REvil claimed responsibility for an enormous ransomware attack on scores of managed service providers worldwide, causing businesses and organizations to grind to a halt. REvil apparently gained access to the systems of Miami-based Kaseya Ltd., a provider of IT management and patch management software to MSPs.

Through the breach, REvil was able to deploy ransomware to networks. Reportedly, more than 1 million systems were hit and possibly infected in the attack. On its Dark Web website, REvil demanded $70 million in cryptocurrency for a "universal decryptor software key." If paid, it would be the largest ransom ever extorted.

Continued on next page...

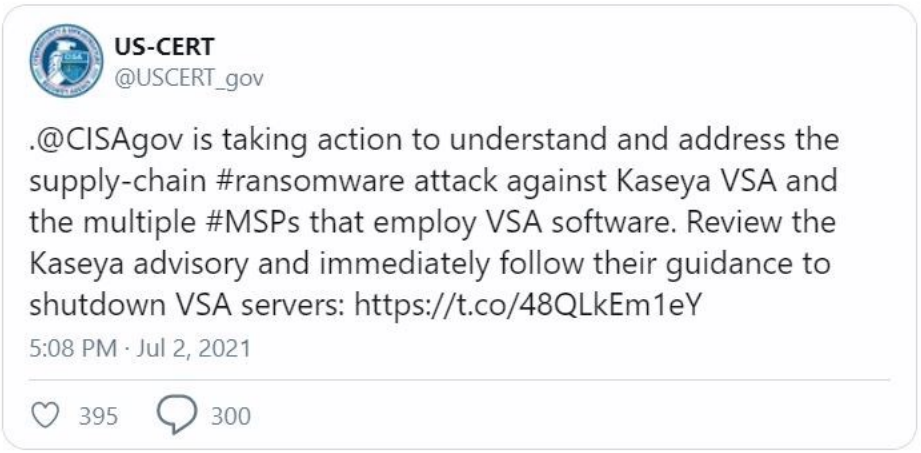
July 2021

This monthly publication provided courtesy of Adam Cambreleng, Inside Account Manager here at Tech Hero

Our Mission

To build a community of successful minded entrepreneurs that inspires excellence, encourages collaboration and expands the capacity of all members to achieve great things.

The timing is probably no coincidence. IT staffs are usually at lower levels during holiday weekends, especially those holidays that occur during the summer. With fewer IT security pros around, it raised the odds that the attack would be successful. The incident is the latest in a growing and concerning number of supply-side attacks. Bleeping Computer has a good under-the-hood analysis of how the REvil ransomware attack was accomplished



U.S. President Joe Biden ordered a probe of the incident, and while REvil is believed to be a Russian-linked entity, Biden said he wasn't certain who was behind the attack. On its Twitter page, the U.S. Cybersecurity and Infrastructure Security Agency said it is taking action to "address the supply-chain ransomware attack."

Kaseya has dedicated a page on its website to continual updates, noting it was the "victim of a sophisticated cyberattack." Kaseya said it would update the situation on its website as it learned more about the repercussions. The major fear is that the attack may have hit companies involved with important or even crucial infrastructure.

—*Peter King, TechGenix*

tech hero

Cloud Portal

Did you know about our new Cloud Portal? This new tool will allow you to open tickets directly with us here at Tech Hero at the click of a button!

To try it out, just go down to your system tray and look for the small blue IT icon. After you've double clicked on it you will need to sign in (You will only need to do this once!)

Once you are in you can click around explore the software.

If you have any questions, feel free to reach out to us at the number below!

(800) 900-TECH x2

vmware PARTNER

PROFESSIONAL SOLUTION PROVIDER

Free Consultation to review your VMware Licensing!

Contact your Tech Hero sales representative to schedule a FREE review of your VMware licensing.

Find out ways to save money, ways to receive free upgrades, and a better understanding on the VMware license models.

tech hero

1-(800) 900-TECH (option 2)

Sales@TechHero.com

MERCEDES-BENZ EXPERIENCES DATA LEAK, U.S. CUSTOMERS AFFECTED

Mercedes-Benz has released the results of an investigation into a data leak incident that affects their USA operations. The incident was reported to the automobile giant by an unnamed third party. Below is an excerpt of the report, namely explaining Mercedes-Benz's findings and the roots of the case:

"On June 11, 2021, a vendor informed Mercedes-Benz that sensitive personal information of less than 1,000 Mercedes-Benz customers and interested buyers was inadvertently made accessible on a cloud storage platform. This confirmation was part of an ongoing investigation conducted in cooperation with the vendor. The issue was uncovered through the dedicated work of an external security researcher.

It is our understanding the information was entered by customers and interested buyers on dealer and Mercedes-Benz websites between January 1, 2014 and June 19, 2017. No Mercedes-Benz system was compromised as a result of this incident, and at this time, we have no evidence that any Mercedes-Benz files were maliciously misused."

Mercedes-Benz initially believed that as many as 1.6 million records could have been compromised. These records include personal data that mostly comprises credit scores, driver license numbers, Social Security numbers, credit card information, and dates of birth.

Continued on next page...

Later in the report, Mercedes-Benz states that many affected parties have been notified about the data leak. The company says they are offering free subscriptions to a credit monitoring service to any victims of the leak. According to the post, Mercedes-Benz will provide the subscription for 24 months. The automobile manufacturer is also in the process of notifying the relevant government agencies about this incident.

The company ends the report with the following statement:

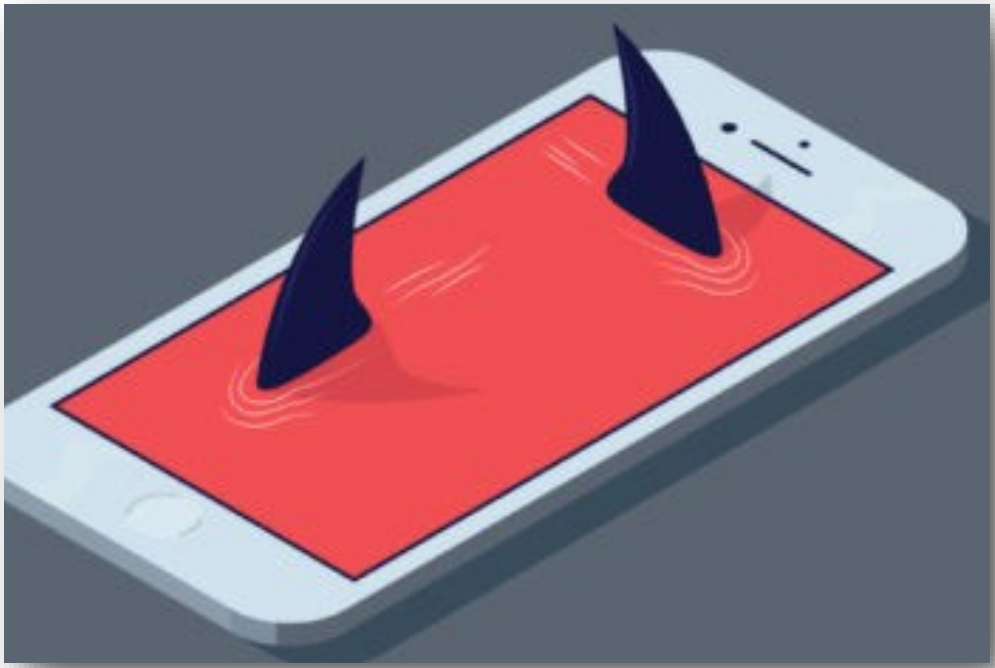
"*Any individuals who have questions or concerns about this incident should contact the Mercedes-Benz Customer Assistance Center at 1-800-367-6372.*"

As a whole, this data leak is not nearly as serious as some that occurred recently, but it is proof that this epidemic of data breaches and data leaks is far from over.

—*Derek Kortepeter for Techgenix*

Client Spotlight

Ally Building Solutions provides finish products, installation, and design studio services to new home production builders, custom builders and multi-family projects in Orlando, Jacksonville, Ocala and Tampa, FL.



VISHING ATTACKS ON THE RISE WITH NEWEST CAMPAIGNS

A research blog post from Armorblox is showing that voice phishing (or vishing) attacks are seeing a rise in activity. Vishing simply takes the concepts found in social engineering attacks like phishing emails and applies them to voice interactions. That shady man on the phone claiming to be an IRS agent so that he can steal your personal data? That's a vishing attack.

Armorblox bases its research on two specific tech support scams that have affected roughly 25,000 individuals. In both cases, the attacks started as regular email phishing but escalated to vishing via data collection. In regular phishing attacks, you are redirected to a fake site or asked to respond to an email for attackers to steal your data. However, in these attacks, the emails (which impersonated Geek Squad and Norton) required the target to call a number to continue the scam. The emails were able to bypass spam filters in Microsoft Exchange Online Protection and Proofpoint.

Continued on next page...

In the Geek Squad vishing attack, Armorblox states the following about the methodology of the criminals:

"*The email was sent from a Gmail account and was titled "Order Confirmation," carefully treading the line between vagueness and urgency-inducing specificity. The email contained HTML stylings similar to genuine emails sent from Geek Squad, and included a renewal confirmation for an annual protection service.*

Instead of including any links, the only call to action in the email was a phone number of the "Billing Department" that the victims could call to process order returns."

As for the attack impersonating Norton, the attackers tried similar tactics:

"*Like the Geek Squad email, this one was also sent from a Gmail account and had the same curiosity-inducing title: Order Confirmation. This email didn't have any HTML stylings and was more plain-text compared to the Geek Squad email.*

Just like with the other vishing email, this email also did not contain any links or other conventional payloads. The only payload was a phone number included in the mail body, inviting victims to call the number if they wanted to cancel their subscription."

Armorblox called both numbers listed in each attack email and quickly discovered that they were being phished for data. These attacks prove that every individual should practice defensive measures and common sense when engaging in any correspondence. For these emails to get past spam filters of respected companies, it shows that vishing has become more complex in its methodologies.

Simply put, always be wary of anyone seeking your data. You are the best line of defense against these attacks. —*Derek Kortepeter for Techgenix*