The Ransomware Files, Episode 6: Kaseya and REvil

bankinfosecurity.com/interviews/ransomware-files-episode-6-kaseya-revil-i-5045

Critical Infrastructure Security , Cybercrime , Cybercrime as-a-service

Ransomware Gang Used Zero-Day Flaws for High-Profile Attack Jeremy Kirk (jeremy_kirk) • April 4, 2022 47 Minutes

The REvil ransomware gang's attack against the U.S. software company Kaseya in 2021 is not only among the largest ransomware attacks of all time, it's also one of the most intriguing.

It involves the use of zero-day software vulnerabilities known only to a handful of people, a race between attackers trying to snare ransom payments and defenders developing a patch, and a secret operation that hacked back against the REvil hackers. And in the end, a rare action happened: Someone was actually arrested.

This episode of "The Ransomware Files" talks to those who had a role in this incredible event. It also coincides with the release of new technical information about the software vulnerabilities exploited by the ransomware gang, which were found by the Dutch Institute for Vulnerability Disclosure, or DIVD.

REvil managed to exploit zero-day vulnerabilities in the Virtual Systems Administrator, which is remote management software made by Kaseya and widely used by managed service providers. The vulnerabilities allowed the group to spread its ransomware, which was disguised as a software update.

DIVD had warned Kaseya of the vulnerabilities in April, but REvil also discovered them, says Frank Breedijk, manager of DIVD's Computer Security Incident Response Team. Breedijk and DIVD's chairman, Victor Gevers, felt they had lost the race with the attackers.

"We were in this marathon to fix software that had quite a bit of technical debt in it," Breedijk says. "And then with the finish line in sight, on your right-hand side, all of a sudden comes Usain Bolt, passes you, flips you the bird and ransoms a whole bunch of systems."

The attack resulted in more than 1,500 organizations becoming infected with ransomware. Robert Cioffi is the founder of Progressive Computing, which is a New York-based managed service provider that used Kaseya's VSA to deliver services to its clients.

Cioffi feared he might lose his business after speaking with a colleague on the day of the attack in July 2021. All 80 of his customers were infected.

"I couldn't comprehend the words coming out of his mouth - that all of our customers were ransomwared," Cioffi says. "It just didn't make sense to me. What? How is it that everyone is ransomwared?"

There are other twists and turns. The FBI and its law enforcement partners hacked back at the hackers, snatching a universal decryption key. And after the REvil gang went dark for good, prosecutors announced the arrest of a Ukrainian man, Yaroslav Vasinskyi, for the attack against Kaseya. Vasinskyi is now awaiting trial in Texas (see: *US Nabs Alleged Ransomware Operators - One Tied to Kaseya*).

"The Ransomware Files" is a podcast miniseries available on Spotify, Apple Podcasts, Google, Audible, Stitcher and more. I'm speaking with those who have navigated their way through a ransomware incident to learn how they fought back and what tips they can pass on to others. No ransomware infection is ever welcomed. But there's invaluable knowledge gained. There should be no shame in getting infected, and it's important to share the lessons.

If you enjoyed this episode of "The Ransomware Files," please follow it on a podcast platform and leave a review. Also, the show has a Twitter handle, @ransomwarefiles, that tweets news and happenings about ransomware.

If you would like to participate in this project and tell the information security community about your organization's brush with ransomware, please get in touch with me at jkirk@ismg.io or direct message me here on Twitter. I'm looking for other people,

organizations and companies that can share their unique experiences for the benefit of all until ransomware, hopefully, is no longer a threat.

Credits

Speakers: Robert Cioffi, Founder, Progressive Computing; Frank Breedijk, Manager, CSIRT, DIVD; Victor Gevers, Chairman, DIVD; Jason Manar, Chief Information Security Officer, Kaseya; Jon DiMaggio, Chief Security Strategist, Analyst1; John Hammond, Senior Security Researcher, Huntress; Espen Johansen, Security Director, Visma; Adrian Stanila, Senior Information Security Researcher, Visma; George Zamfir, Security Analyst, Visma; Jeremy Kirk, Executive Editor, Information Security Media Group.

Production Coordinator: Rashmi Ramesh.

The Ransomware Files theme song by Chris Gilbert/© Ordinary Weirdos Music.

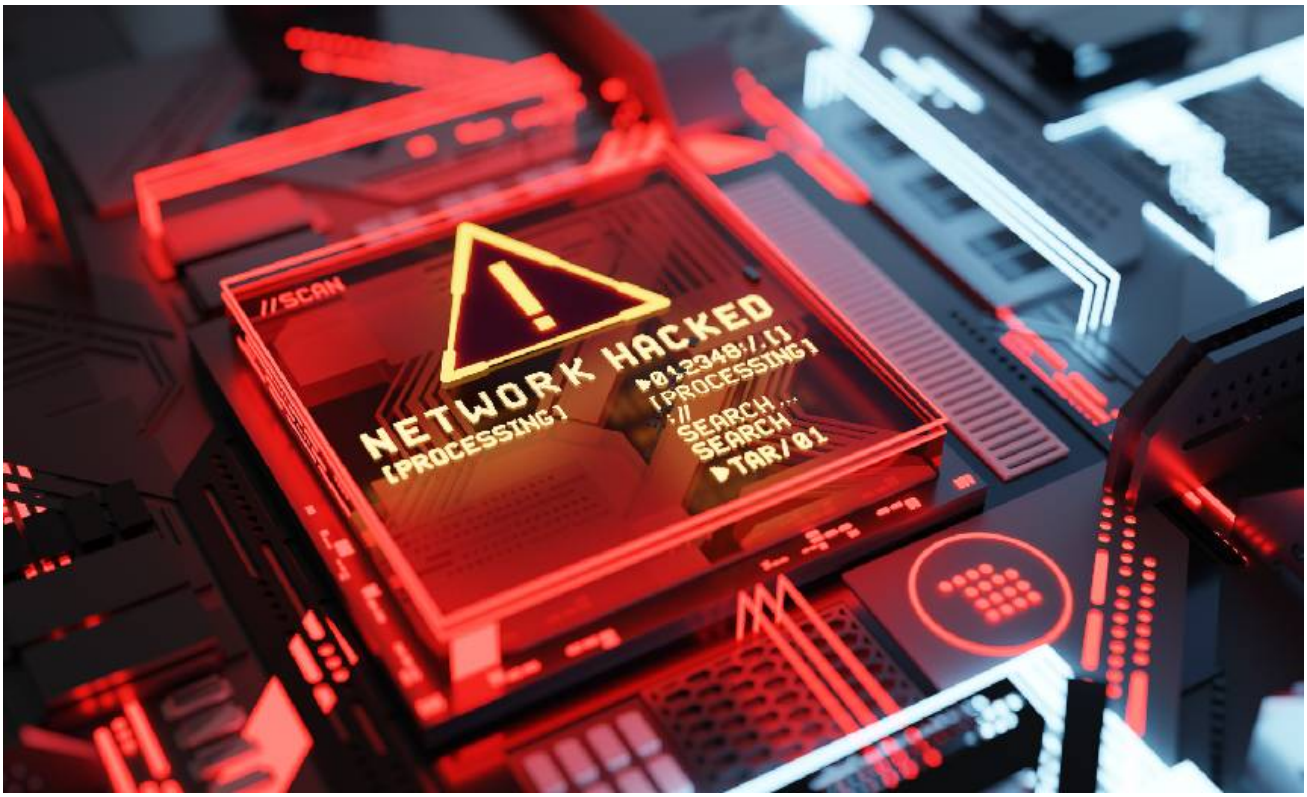
Music by Uppbeat andPodcastmusic.com.

Sources

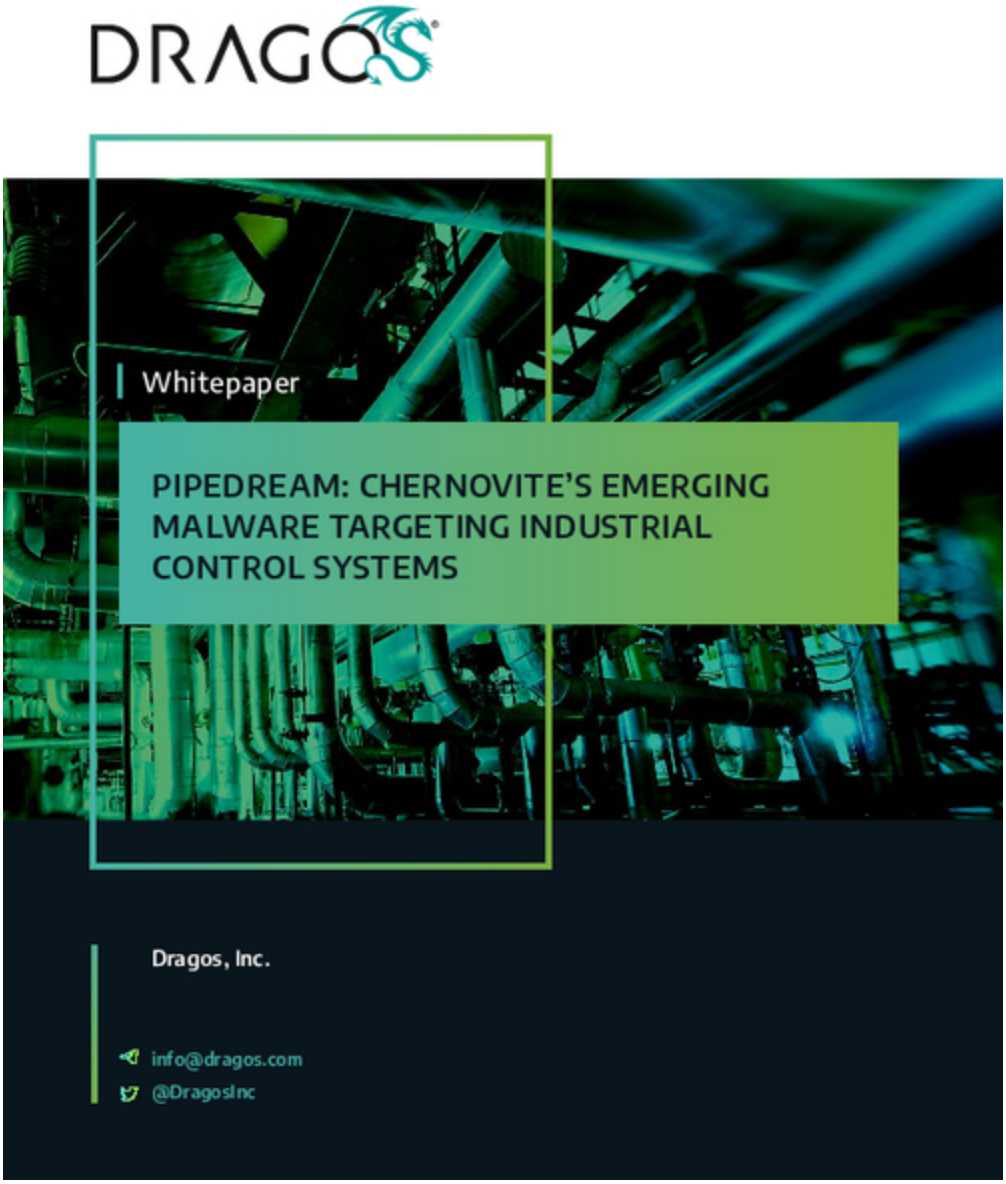
- Bisend, What is Classic ASP?, Jan. 28, 2019;
- Data Breach Today, REvil Revelations: Law Enforcement Behind Disruptions, Oct. 22, 2021;
- Double Pulsar, Kaseya Supply Chain Attack Delivers Mass Ransomware Event to US Companies, July 3, 2021;
- Dutch Institute for Vulnerability Disclosure, Why We are Only Disclosing Limited Details on the Kaseya Vulnerabilities, July 7, 2021;
- Huntress, The Hunt to Find Origins of Kaseya's VSA Mass Ransomware Incident, July 20, 2021;
- Reuters, Governments Turn Tables on Ransomware Gang REvil by Pushing it Offline, Oct. 22, 2021;
- The Record, Kaseya: More Than 1,500 Downstream Businesses Impacted by Ransomware Attack, July 6, 2021;
- Visma, Software Vendor Kaseya Exposed to Global Cyberattack, Affecting Retail Trade, July 3, 2021.
- Adrian Stanila, Kaseya War Stories, Nov. 22, 2021;
- Allan Liska, Ransomware: Understand. Prevent. Recover, Oct. 28, 2021.
- Huntress Labs, Reddit post: Critical Ransomware Incident in Progress, July 3, 2021;
- Kevin Beaumont, Twitter post, July 5, 2021.

Read Transcript

You might also be interested in …



OnDemand | Spotlight Discussion: Advanced Network Detection & Response



PIPEDREAM: CHERNOVITE's Emerging Malware Targeting Industrial Control Systems

The Definitive Email Cybersecurity Strategy Guide

Live Webinar | Five Ways Unified Visibility and Automation Can Mitigate Cyber Attack Surface Gaps

Spotlight Discussion | Expel Quarterly Threat Report: Cybersecurity Data, Trends, and Recs from Q1 2022

Live Webinar | Ransomware in Banking - Where is the Achilles Heel?

The Double-Edged Sword of Mobile Banking

Securing Digital Acceleration: The Community Bank and Credit Union Imperative

Live Webinar | Reduce Risk, Drive Growth & Build Trust, Continuously: How To Instill Continuous Trust Across The Customer Journey