

Member-only story

Kaseya supply chain attack delivers mass ransomware event to US companies

Kevin Beaumont · Follow

Published in DoublePulsar · 8 min read · Jul 2, 2021

286

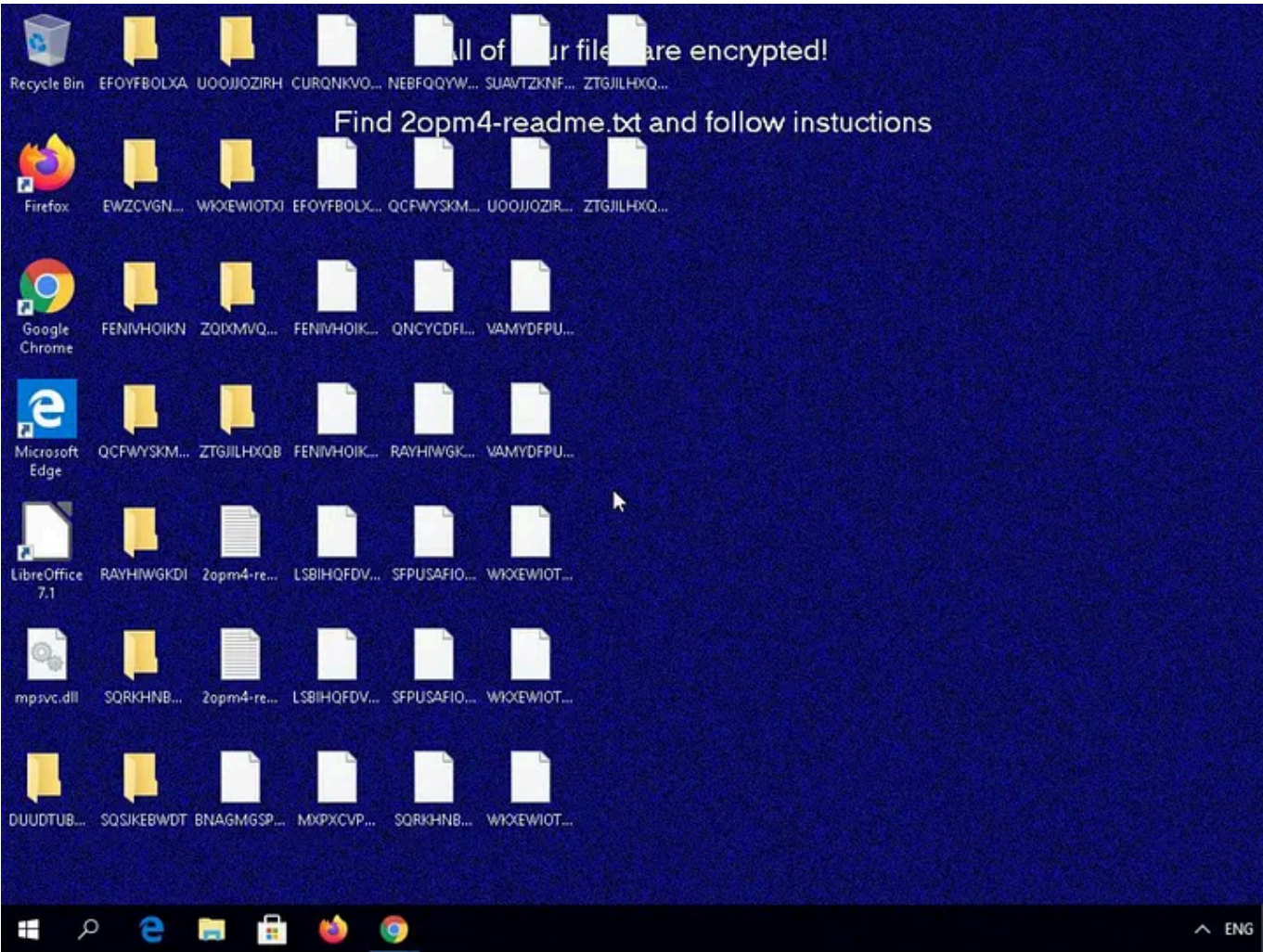
2

Kaseya VSA is a commonly used solution by MSPs — Managed Service Providers — in the United States and United Kingdom, which helps them manage their client systems. Kaseya’s website claims they have over 40,000 customers.

Four hours ago, an apparent auto update in the product has delivered REvil ransomware.

By design, it has administrator rights down to client systems — which means that Managed Service Providers who are infected then infect their client’s systems.

Infected systems look like this:



How this first unfolded


Initial exploit was a 0-day (CVE-2021-30116) (details have not been entered into CVE database, however it has been allocated for this). More CVEs may be issued.


So even if the latest version is used, at time of attack, attackers could remotely execute commands on the VSA appliance. Technical details of how to exploit the vulnerability are not being provided until the patch is available.


It is not a great sign that a ransomware gang has a zero day in product used widely by Managed Service Providers, and shows the continued escalation of ransomware gangs — [which I've written about before](#).

Create an account to read the full story.

The author made this story available to Medium members only.
If you're new to Medium, create a new account to read this story on us.

 Sign up with Google

 Sign up with Facebook

 Sign up with email

Already have an account? [Sign in](#)

 286  2



Written by Kevin Beaumont

17.4K Followers · Editor for DoublePulsar

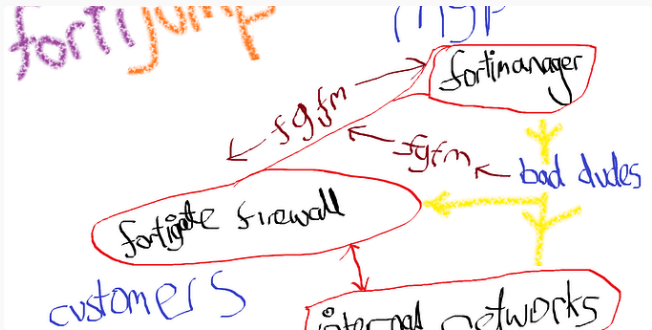
Everything here is my personal work and opinions.

Follow



Medium

To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.



Scope	Editions	Applicable OS
Device	Pro	Windows Insider Preview
User	Enterprise	
	Education	
	Windows SE	
	IoT Enterprise / IoT Enterprise LTSC	

User

Copy

./User/Vendor/MSFT/Policy/Config/WindowsAT/DisableATDataAnalysis

This policy setting allows you to control whether Windows saves snapshots of the screen and analyzes the user's activity on their device.

- If you enable this policy setting, Windows won't be able to save snapshots and users won't be able to search for or browse through their historical device activity using Recall.

Kevin Beaumont in DoublePulsar

Burning Zero Days: FortiJump FortiManager vulnerability used b...

Yes, I've made a logo in crayon and named this FortiJump.

Oct 22 205 4

Kevin Beaumont in DoublePulsar

Recall: Stealing everything you've ever typed or viewed on your own...

Photographic memory comes to Windows, and is the biggest security setback in a...

May 31 3.2K 46



Kevin Beaumont in DoublePulsar

Hacker group Handala Hack Team claim battery explosions linked to...

Tracking Iran linked group claims

Sep 19 59 2

Government-backed attackers may be trying to compromise your device!

Dear Customer,

Your device has been identified among a list of devices currently being targeted by a state-backed threat actor. Information attained by ESET's Threat Intelligence Division has identified a geopolitically motivated threat group as having attempted to target your machine within the last 14 days of this email.

As part of ESET's Advanced Threat Defense program (ESET-ATD), ESET is providing you access to the ESET Unleashed program, *designed to counter advanced targeted threats*, for you to install on up to 5 devices of yours.

Your personal download link is:

Kevin Beaumont in DoublePulsar

EIW—ESET Israel Wiper—used in active attacks targeting Israeli orgs

A look at wiping of Israeli orgs.


Oct 18 168 1

See all from Kevin Beaumont

See all from DoublePulsar

Recommended from Medium

Susan Brearley

 in MuddyUm

Sanskar Kalra


To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.


to


What's in YOUR wallet?

BloodHound for Active Directory Enumeration: Installation, Usage, and...


★ Jun 11


 612


 9



Aug 26

 2

 2



Lists

Tech & Tools

21 stories · 332 saves

Staff Picks

755 stories · 1416 saves

Medium's Huge List of Publications Accepting...

378 stories · 3817 saves

Natural Language Processing

1789 stories · 1391 saves


David Campbell


in Generative AI


AI Hallucinations: When Machine Learning Gets Creative (and...

Your AI is lying to you and here's why that's dangerous

★ Jul 17

 190

 4





Practical OSINT

OSINT In War Zone: A Practical Guide to Use X (Twitter) Advance...

This article will guide you through using X (formerly Twitter)'s advanced search...

★ Sep 6

 40




Vicente Aceituno Canal

in The CISO Den

A Journey to the Highest Cybersecurity Maturity: Discovery...

Discovery Cycle

★ Jul 3





Prof Bill Buchanan OBE FRSE

Homomorphic Encryption, Secure Shares and MPC Come Together T...

Your biometrics — such as your fingerprints, your face, and your iris — are some of your...

★ Jun 1

 59



To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.