untangle®

THE KASEYA VSA RANSOMWARE ATTACK

SECURITY BRIEF

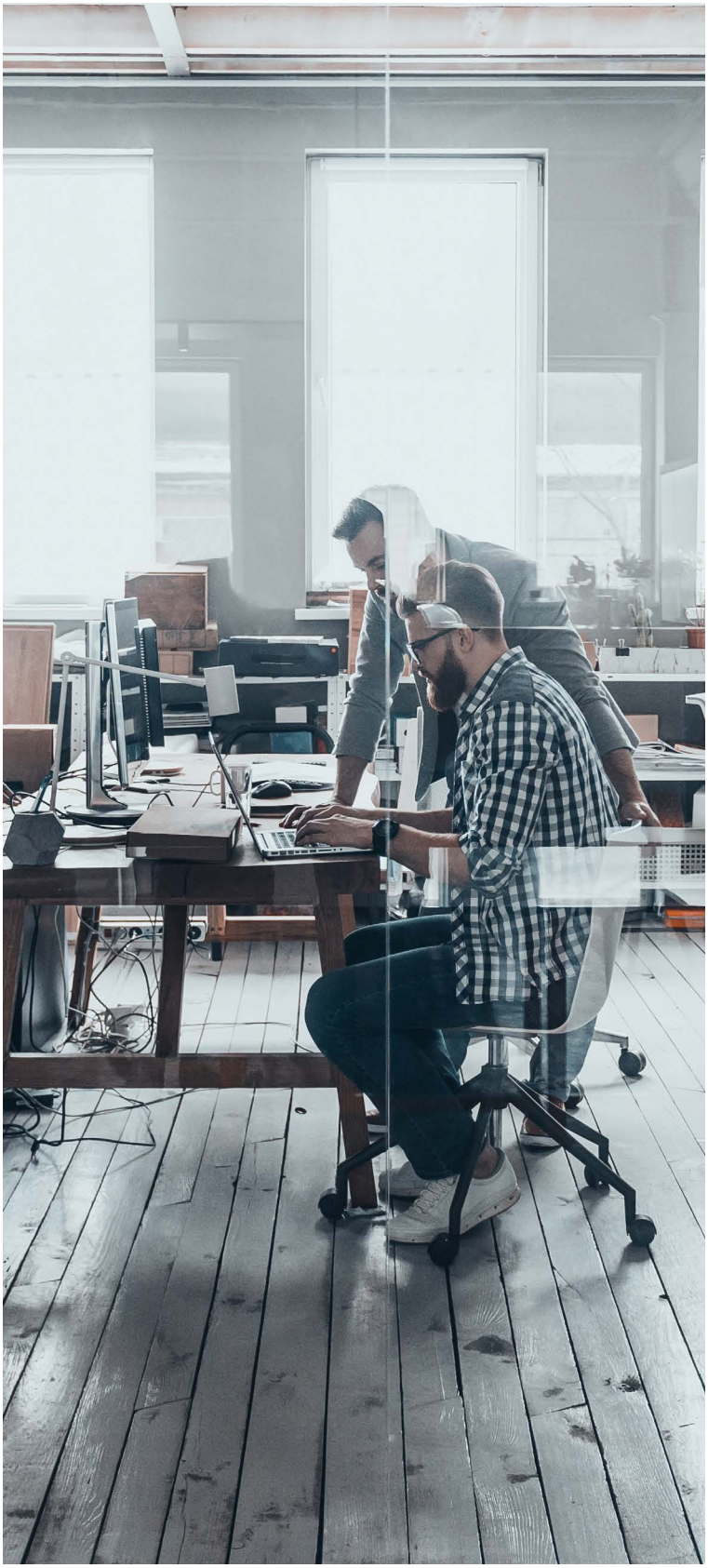
On July 2, 2021, Kaseya, a provider of IT and security management solutions for managed service providers (MSPs) and small to medium-sized businesses (SMBs), responded to alerts of a cyberattack on its Virtual Systems/Server Administrator (VSA), and quickly shut down access to it's software. The Kaseya VSA attack was discovered just before the USA July 4th Independence Day holiday, and the impact of the attack started unfolding throughout the weekend.

The attack was likely timed around the US holiday, as many businesses would be closed on the Monday following the 4th of July celebrations and many Americans also take their vacation before or after the holiday. Thus, the timing of this attack would have had businesses at reduced staff when news of the attack broke and IT staff rallied to ensure their systems were safe.

Kaseya's VSA is a management tool used by MSPs to manage their customers' networks, servers and devices such as employee laptops used in the office or at home, servers and desktop workstations.

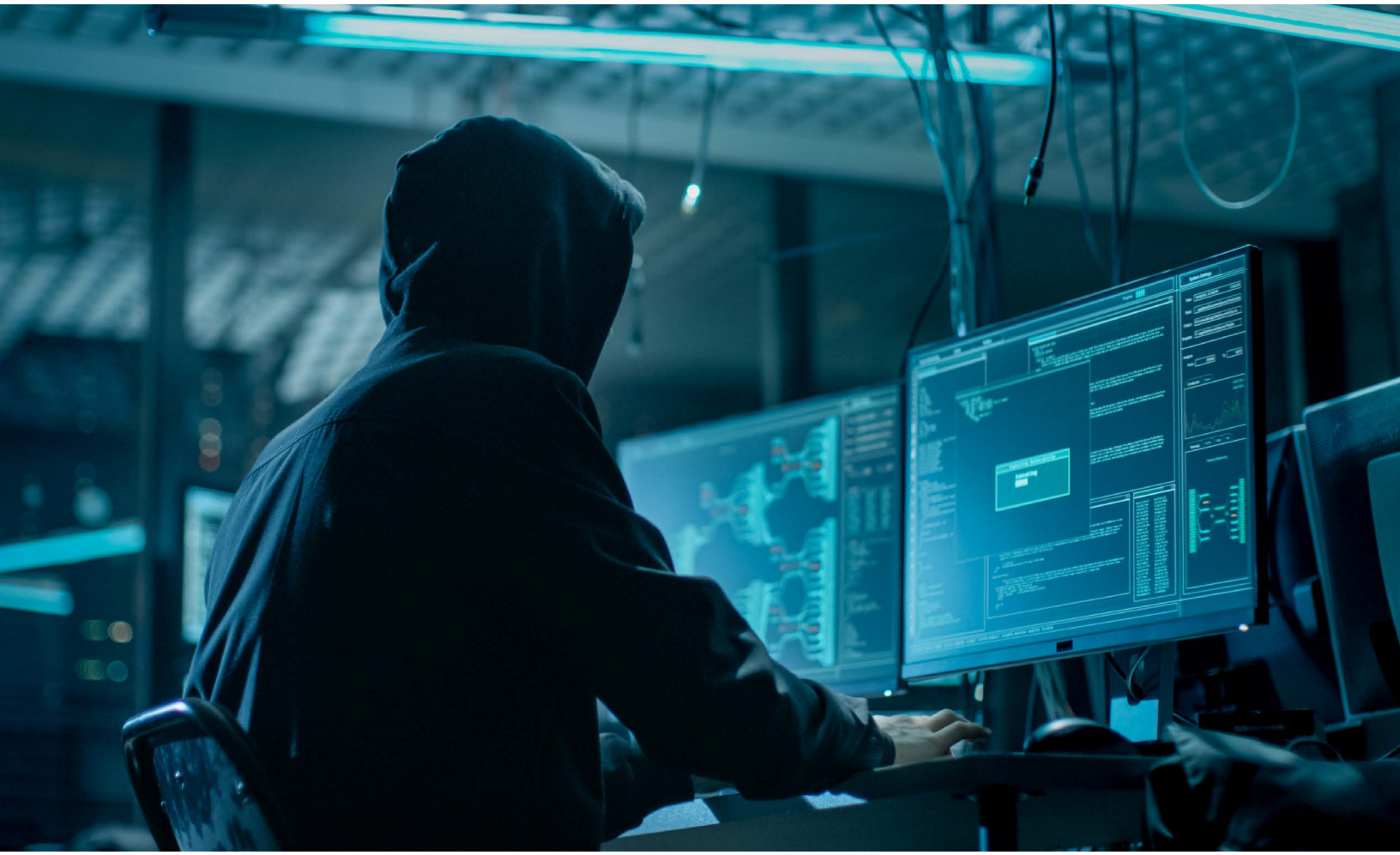
As a network management tool, Kaseya's VSA tool provides tremendous advantages. It is essentially a single pane of glass that allows management and monitoring of every part of a business network. As powerful as that is, in this particular case it's also a significant downfall if breached. Providing access to every aspect of a business's IT Infrastructure, it is not a tool that should fall into the wrong hands, which is exactly what happened with the Kaseya attack.

Once the VSA management tool was breached, the attackers were able to run their attack code to encrypt systems which were then rendered inaccessible without the decryption key.



A KNOWN ATTACKER

The Kaseya attack was carried out by known cybercrime gang REvil. This is the organization that recently extorted $11 million, in a very disruptive attack, from meat-processor JBS.



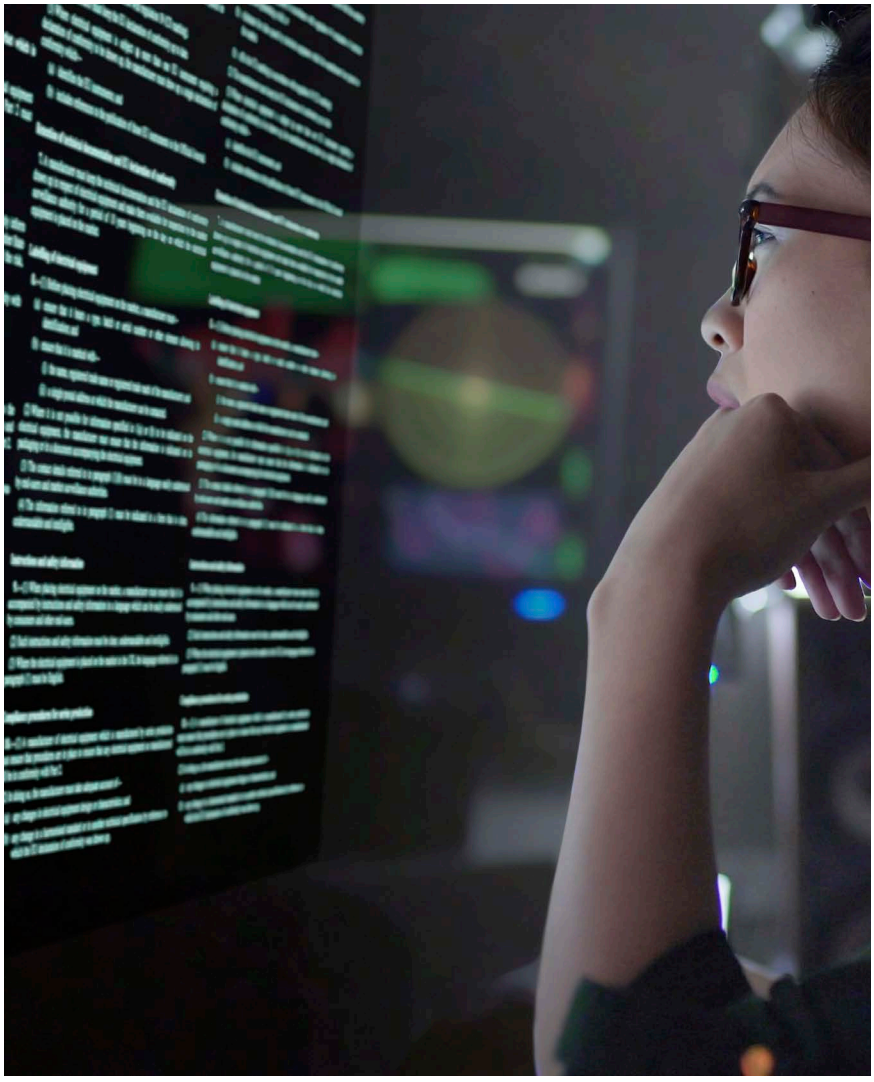
REvil took the credit almost immediately. Initially, the gang began seeking $5 million from MSPs and $45,000 from MSPs' customers that were affected. However, stating that the attack could affect one million systems, REvil demanded a lump sum of $70 million in Bitcoin in exchange for the decryption key that would unlock all affected systems and avoid the complexity of handling individual transactions.

The boldness of REvil to conduct another attack so soon after the JBS attack shows not only their confidence in pulling off another ransomware attack, it shows that with their success they are able to find talent with the skills to quickly conduct more attacks.

IMPACT ANALYSIS

MSPs generally offer their services to small or medium sized businesses who do not have their own IT, networking, and cyber security staff. These smaller companies outsource their IT needs to an MSP who provides IT services for them and generally has multiple clients for which they provide IT services.

Tools like VSA are particularly useful to an MSP who may be taking care of a handful or hundreds of businesses' IT needs. VSA makes it very easy for the MSP to check on all of their customers' networks from one single pane of glass that they can access from anywhere; from their home office, from their place of work or when they are on the road out and about.



Being able to log into VSA saves the MSP huge amounts of time so that they are able to provide services to more customers than otherwise would be possible without such streamlined aggregation of all the tools needed.

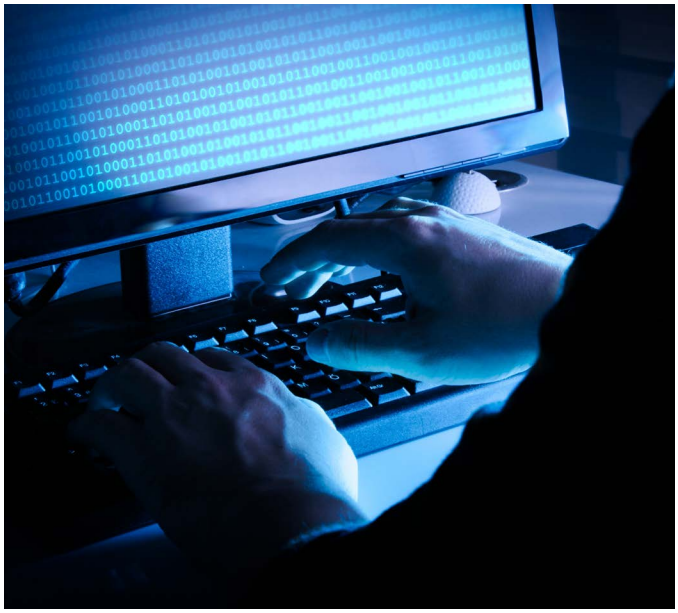
Attacking the tool that MSP's trust to manage and gain access to all their clients' systems gives the cybercriminals a way to infiltrate more businesses than if they were to go after them one at a time. This type of attack, known as a supply chain attack, is becoming more common with a prime example being the Solarwinds attack at the beginning of 2021.

While Kaseya said that only around 50 of its customers that use the on-premises VSA had been directly compromised, it's estimated that 800 to 1500 SMBs have been affected. It has been reported that no large corporations or critical infrastructure have been affected, however, SMBs in 17 countries have been compromised and include financial services, travel agencies, dental practices, architecture firms, plastic surgery centers, libraries and supermarkets.

TECH ANALYSIS

Ultimately, the breach was caused by the attackers being able to side load a Dynamic Link Library (DLL). Applications that run on Windows will run with an executable file with an .exe file type. Once running, the application can look for and use DLLs which are binaries of compiled code in separate files with a .dll file type. DLLs perform functions for the application.

DLLs are useful, as different features and functionality needed by an application can be placed in DLL's to keep them organized. Having a well organized set of DLLs can aid in keeping the code organized, rather than having thousands of lines of code all compiled into the overall executable.



Other advantages of DLLs are that different DLLs can be called based on certain criteria, so the application is able to run differently for such things as different geographical locations for example. A further advantage is that if something needs to be changed in the functionality within the DLL, then only the changed DLL needs to be updated and placed on an existing deployment rather than having to update every DLL and the main executable (.exe) as well.

Once located by the running applications, DLLs are loaded and trusted. However, if an attacker were able to convince the application to load their compiled code instead of the intended DLL, then their code would get the ability to do all sorts of privileged functions on the system it is running on.

In the case of the VSA attack, the DLL was able to get onto the affected systems and cause the systems to lock up, requiring a key for decryption.

DLL side loading is a known technique, and there are a few ways to minimize the chances of it being successful. When Windows needs to find a DLL, it has a well documented method of looking for it. It will first look in the directory that the executable file resides in, and then it will look in other locations, such as the current directory that is being used by the running application.

The easiest method for an attacker to use is to get their own malicious DLL into the working directory to get picked up. To guard against this, DLL's should be accessed using a full path name instead of letting Windows iterate through its methods of finding them. This gives the attacker less options to get their own DLL on the system. They would have to place it in the exact location specified rather than one of multiple possible locations.

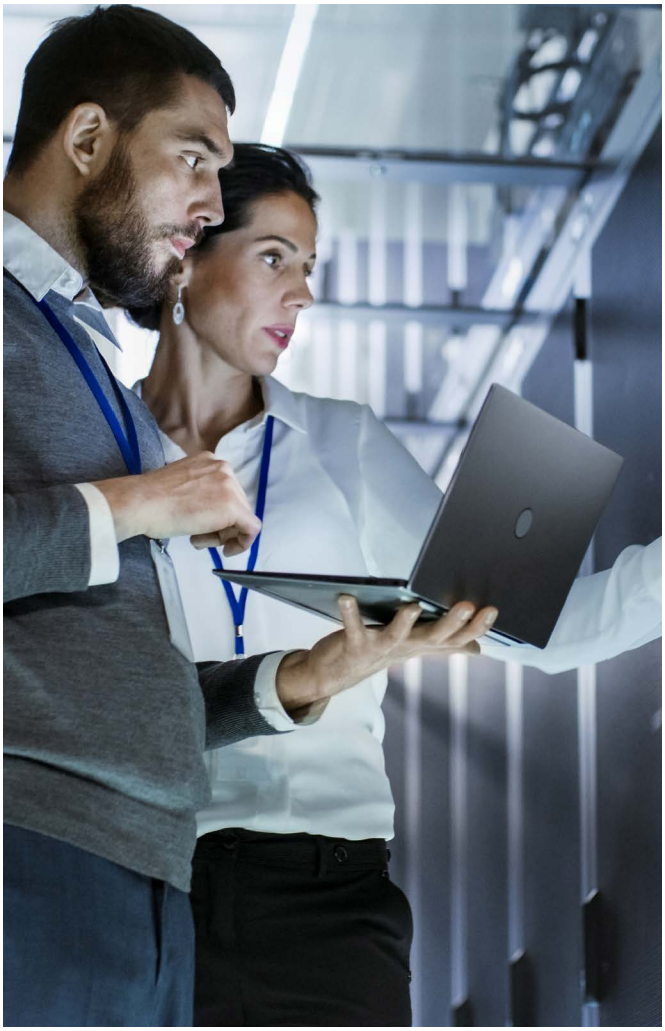
PREVENTION TECHNIQUES / PREVENTION MEASURES

To prevent an attack of this nature, the best defenses would be a layer of defenses that come together from all parties involved, which in this instance includes Kaseya, the MSPs and the customers that the MSPs serve.

- Vendors, such as Kaseya, need to be more vigilant than ever when thinking about how their code could be compromised. As a vendor trusted with the keys to every aspect of a business' network, thinking about how code could be compromised with every code review is a necessity.

- The MSPs that use Kaseya need to have a mindset of limited trust for any one IT system they use. MSPs get immense advantages using management tools such as Kasaya's VSA tool. But, if it is compromised, then that compromise is passed along to all of their clients' systems. The MSP must think about the impact of a breach on any tool they use and consider strategies to minimize the risk. The MSP must further make sure there are enough protective layers in place to stop such a breach, such as virus blocking, firewalls, endpoint security solutions, and threat analysis tools.

- Finally each business that the MSP supports must pay attention to putting in place protective systems and allow enough budget to do it properly.



Layering in further defenses, any business that uses a Windows based server can further fortify their systems by considering multiple types of security features. Firewalls, Endpoint Security Solutions, Threat Management and Threat Analysis tools, Virus Blocking tools and Intrusion Prevention systems can all work together to ensure that malicious files are blocked from getting to servers before they can do damage. As with any cyber security protective strategy, using multiple techniques is always the best way to approach defense. If one defense is breached, another one will step up and continue to neutralize the attempt.

A point of note in this case is that the attack compromised on-premises deployments of the VSA management tool. This is impactful when thinking of prevention and mitigation techniques. When deploying a tool on-premises it becomes the IT administrator, in this case the MSP, who is responsible for updating it. It can take time for a vendor such as Kaseya to contact every MSP that might be using their tool to ensure they make an update. When using a cloud based management tool, the update doesn't rely on the MSP's update schedule. Every update to a cloud based, or SaaS tool, can be made directly by the vendor, Kaseya in this case, who can push the update within minutes as soon as they have a fix.

Over the last few years, it has become more and more common for MSPs to use cloud based IT tools that are deployed in cloud environments such as Amazon and Azure, rather than deploy their IT stack in a server room. Some MSPs still feel that they have more control over their IT stack if it's deployed on premises where they have 100% control over it. For example, in Untangle's SMB IT Security Report respondents stated that 70% of their IT Infrastructure is deployed on premises, while 50% still have less than 10% deployed in the cloud. In some cases, MSPs do have more control when it's on premises. However, in this particular case the cloud based tools would have the breach blocked sooner as Kaseya would fix it as soon as they built the patch.

HOW UNTANGLE CAN HELP

Untangle enables organizations to address network concerns and remain vigilant against unauthorized network access. The Untangle Network Security Framework provides IT teams with the ability to ensure protection, monitoring and control for all devices, applications, and events, enforcing a consistent security posture across the entire digital attack surface.

Untangle's cloud based centralized management tool, Command Center, does not rely on customer update schedules. Every update can be pushed within minutes to improve the security posture of the whole network management system.

UNTANGLE NETWORK SECURITY FRAMEWORK

ADVANCED SECURITY

- Protection, encryption, control & visibility anywhere
- NG Firewall, IPS, VPN & more
- Onboard security for small network appliances & IoT devices
- Full security processing on-premises or in the cloud

INTELLIGENT SD-WAN

- Secure, WAN-optimized connectivity for every location
- Seamless scalability
- Untangle AI-based Precitive Routing technology for first packet, dynamic path selection
- Manage one or many appliances from Command Center

CLOUD MANAGEMENT AT SCALE

- Zero touch deployment
- Configure & push policies
- Advanced alerting & reporting
- Visibility across globally dispersed networks & endpoints

untangle

Untangle, Inc.
25 Metro Drive, Ste. 210
San Jose, CA 95110
www.untangle.com

For sales information, please contact us by phone in the US at +1 (866) 233-2296 or via e-mail at sales@untangle.com.

©2021 Untangle, Inc. All rights reserved. Untangle and the Untangle logo are registered marks or trademarks of Untangle, Inc. All other company or product names are the property of their respective owners.