Hive Pro

THREAT ADVISORY

REvil Ransomware gang behind the Kaseya VSA Supply-Chain attack

TA202124

Threat Level Red

Publish Date – July 8, 2021

The REvil ransomware group was successful in carrying out a supply chain attack by exploiting the zero-day vulnerability (CVE-2021-30116) in the Kaseya VSA server and delivering a malicious script to all the computer devices managed by servers. The script delivered the REvil ransomware and encrypted the files of the clients managed by the server affecting almost 1 million computer devices.
Hive pro researcher has identified that there are three more zero-day vulnerabilities that were possibly used to target the clients:

- Authentication Bypass Vulnerability
- Arbitrary File Upload Vulnerability
- Code Injection Vulnerability

The Techniques used by the REvil ransomware includes:

TA0001: Initial Access
T1189: Drive-by Compromise
T1566: Phishing
T1566.001: Spear phishing Attachment
TA0002: Execution
T1059: Command and Scripting Interpreter
T1106: Native API
T1059.001: PowerShell
T1059.005: Visual Basic
T1059.003: Windows Command Shell
TA0003: Persistence
T1204: User Execution
T1047: Windows Management Instrumentation
T1204.002: Malicious File
TA0004: Privilege Escalation
T1134: Access Token Manipulation
T1134.002: Create Process with Token
T1134.001: Token Impersonation/Theft
T1574:Hijack Execution Flow
T1574.002:Hijack Execution Flow: DLL Side-Loading
TA0005: Defense Evasion
T1134: Access Token Manipulation
T1134.002: Create Process with Token
T1134.001: Token Impersonation/Theft
T1140: DE obfuscate/Decode Files or Information
T1055: Process Injection

TA0006: Credential Access
T1562: Impair Defenses
T1562.001: Disable or Modify Tools
T1070: Indicator Removal on Host
T1070.004: File Deletion
T1036: Masquerading
T1036.005: Match Legitimate Name or Location
T1112: Modify Registry
T1027: Obfuscated Files or Information
T1055: Process Injection
TA0007: Discovery
T1083: File and Directory Discovery
TA0008: Lateral Movement
T1069: Permission Groups Discovery
T1069.002: Domain Groups
T1012: Query Registry
T1082: System Information Discovery
TA0011: Command and Control
T1071: Application Layer Protocol
T1071.001: Web Protocols
T1573: Encrypted Channel
T1573.002: Asymmetric Cryptography
T1105: Ingress Tool Transfer
TA0010: Exfiltration
T1041: Exfiltration Over C2 Channel
TA0040: Impact
T1485: Data Destruction
T1486: Data Encrypted for Impact
T1490: Inhibit System Recovery
T1489: Service Stop

Threat Actor

Name	Known as	Origin	Target Locations	Target sectors
Pinchy Spider	Gold Southfield, Gold Garden	Russia	Worldwide	Financial gain

Vulnerability Details

CVE ID	Affected Versions	Affected CPEs	Vulnerability Name
CVE-2021-30116	Kaseya Virtual System Administrator	cpe:2.3:a:kaseya:virtual_system_administrator:*:*:*:*:*:*:*:*	Kaseya Virtual System Administrator unknown vulnerability

Indicators of Compromise

Type	Value
IPv4	161[.]35.239.148
Hash(SHA1)	d55f983c994caa160ec63a59f6b4250fe67fb3e8c43a388aec60a4a6978e9f1e 8dd620d9aeb35960bb766458c8890ede987c33d239cf730f93fe49d90ae759dd e2a24ab94f865caeacdf2c3ad015f31f23008ac6db8312c2cbfb32e4a5466ea2 45AEBD60E3C4ED8D3285907F5BF6C71B3B60A9BCB7C34E246C20410CF678FC0C

References

https://www.bleepingcomputer.com/news/security/kaseya-was-fixing-zero-day-just-as-revil-ransomware-sprung-their-attack/
https://otx.alienvault.com/pulse/60e40b4535299fb6755143cf
https://us-cert.cisa.gov/ncas/current-activity/2021/07/02/kaseya-vsa-supply-chain-ransomware-attack
https://www.tenable.com/blog/cve-2021-30116-multiple-zero-day-vulnerabilities-in-kaseya-vsa-exploited-to-distribute-ransomware
https://www.reddit.com/r/msp/comments/ocggbv/crticial_ransomware_incident_in_progress/
https://blog.truesec.com/2021/07/04/kaseya-supply-chain-attack-targeting-msps-to-deliver-revil-ransomware/