DXC TECHNOLOGY

Security threat intelligence report

REvil supply chain ransomware attack impacts 1,000+ firms

New Linux variant of REvil broadens ransomware reach

Rclone shown to be early indicator of compromise

Kernel driver tool Netfilter distributed using signed binary files

Dell addresses multiple vulnerabilities with client platform security updates

Hackers exploit VPN flaw to break into South Korean nuclear research facility

August 2021

Table of contents

Message from Mark Hughes

Ransomware is bad enough, but supply chain attacks amplify the threat by enabling a single breach to affect downstream customers. In one of the largest such attacks to date, the threat group behind the REvil ransomware compromised IT service supplier Kaseya, locking up accounts for hundreds of customers across 17 countries. The key lesson: As good as you might be at safeguarding against such attacks, you're only as good as your core suppliers.

Mark Hughes
President
Security
DXC Technology

About this report

Fusing a range of public and proprietary information feeds, including DXC's global network of security operations centers and cyber intelligence services, this report delivers an overview of major incidents, insights into key trends and strategic threat awareness.

Intelligence cutoff date:
July 9, 2021

Threat updates

1,000+

Number of companies likely infected in the recent Kaseya supply chain ransomware attack

Source: The Hacker News

$11M

Amount JBS Holdings is said to have paid in ransomware after a recent attack

Source: The Wall Street Journal

74%

Percentage of companies surveyed that said they are being affected by the shortage of cybersecurity professionals

Source: Varonis

REvil supply chain ransomware attack impacts 1,000+ firms

On July 2, Kaseya, an information technology (IT) software company, announced its on-premises VSA remote monitoring and management software was compromised in a cyber attack. Reports emerged that the Russia-linked REvil (aka Sodinokibi) had exploited zero-day vulnerabilities in Kaseya's VSA software to conduct a supply-chain ransomware attack against multiple Kaseya managed service providers (MSP) and customers.

Although VSA is the only product affected by the attack, Kaseya has also taken its SaaS servers offline until further notice. According to Kaseya, approximately 40 of its direct customers were compromised in the attack, in addition to potentially affecting 1,500 downstream businesses.

As of July 5, Kaseya announced that it is developing a patch to address the zero-day vulnerability. Kaseya has also engaged security firm FireEye Mandiant with the forensic investigation to assist in determining the root-cause of the attack. Furthermore, Kaseya has notified law enforcement and government cybersecurity agencies, including the Cybersecurity and Infrastructure Security Agency (CISA) and Federal Bureau of Investigation (FBI).

Organizations should assess the risk that exploitation of the Kaseya VSA product poses to their environment. If Kaseya on-premises VSA is not used as an enterprise IT management tool, the risk maybe low per the Kaseya advisory.

Background

Kaseya provides enterprise grade IT management software to MSPs and IT teams. According to Kaseya, exploitation of the VSA on-premises product began July 2 when customers reported the deployment of ransomware on their endpoints. All on-premises Kaseya customers were subsequently notified to shutdown their VSA servers. The company also shut down its SaaS services until further updates can be released. At this time, there are no indications that Kaseya's VSA codebase has been maliciously modified or its SaaS solution exploited.

Threat actors behind REvil operations claimed responsibility for the attack through its dedicated leak site. CrowdStrike Intelligence believes the REvil group is likely operating from Eastern Europe or the Russian Federation. The group sells access to its ransomware through a ransomware-as-a-service model, which is a partnership program with eCrime affiliates. The exploitation chain in the Kaseya attack likely leveraged a combination of authentication bypass, arbitrary file upload, and code injection vulnerabilities to upload, distribute, and execute the REvil ransomware payload.

New Chinese APT Backdoor Attack Targets Russian Defense Sector

While analyzing newly discovered RoyalRoad samples observed in the wild, the Cybereason Nocturnus Team detected one that not only exhibits anomalous characteristics, but also delivers PortDoor malware. This is a previously undocumented backdoor assessed to have been developed by a threat actor likely operating on behalf of Chinese state-sponsored interests. Examination of available data related to the phishing lure revealed the target of the attack was a general director working at the Rubin Design Bureau, a Russian-based defense contractor that designs nuclear submarines for the Russian Federation's Navy.

Source: Cybereason

Next Steps

DXC Technology will continue to monitor Kaseya, CISA and FireEye Mandiant updates to identify the full scope and residual risks of the ransomware attack, and DXC will continue to track the REvil threat actors TTPs.

Recommendations

Institute system privilege policies that provide users the minimum privileges necessary to perform their functions. Further recommendations include:

- Limit personnel authorized to create privileged accounts
- Use a privileged account management (PAM) tool
- Implement privileged account monitoring and screen capture

Ensure critical patches are installed on all systems as well as network infrastructure. Ransomware operators exploit vulnerabilities to escalate privileges in order to deploy ransomware on a victim's system. Enforce the use of multifactor authentication.

New Linux variant of REvil broadens ransomware reach

Even as successful as the REvil Ransomware as a Service (RaaS) has been — with the Kaseya attack reportedly being one of the largest ever — the group behind the malware has been observed revamping the tool to broaden its potential attack surface.

REvil has traditionally targeted Windows environments, but a new variant can infiltrate Linux-based ESXi hypervisor infrastructure and NAS devices. ESXi makes it possible to share hard drives across multiple virtual machines (VM) so, once compromised, attackers can encrypt storage for broad swaths of systems. With NAS devices being shared resources, the same is true with these backend machines.

REvil was first observed in April of 2019, according to AT&T Alien Labs, and the Linux variant was first reported in May of this year.

Alien Labs reports that, before encrypting files, "REvil runs the esxcli command line tool to list all running ESXi VMs and terminate them. By doing this, the attacker ensures no other VM is handling the files to be encrypted, avoiding corruption issues of the encrypted files. However, the executable has a specific parameter to run in silent mode, which avoids debugging without stopping any VMs."

Published indicators of compromise include:

SHA256 Hashes:

- 796800face046765bd79f267c56a6c93ee2800b76d7f38ad96e5acb92599fcd4
- Ea1872b2835128e3cb49a0bc27e4727ca33c4e6eba1e80422db19b505f965bc4
- d6762eff16452434ac1acc127f082906cc1ae5b0ff026d0d4fe725711db47763
- 3d375d0ead2b63168de86ca2649360d9dcff75b3e0ffa2cf1e50816ec92b3b7d

Extensions:

- .naixq
- .7rspj
- .rhkrc

Impact

RaaS groups are upgrading malware tools to increase the attack surface and have a larger impact upon compromise. Organizations that have reviewed ways to hold off traditional attacks on Windows infrastructure need to be constantly vigilant about evolving threats, particularly Linux-based ESXi hypervisor infrastructure and NAS devices. Please refer to Cybersecurity and Infrastructure Security Agency (CISA) guidelines for a list of mitigation steps to reduce the risk of being compromised.

DXC perspective

The ransomware group DarkSide has recently launched malware that will impact Linux systems. REvil is in close competition with DarkSide and most likely developed this Linux variant in response.

The DXC Threat Intelligence team will continue to monitor for new details as additional information becomes available. A joint advisory released by the CISA and the Federal Bureau of Investigation (FBI) provides a robust list of mitigations and recommendations to both reduce the risk of compromise and prevent ransomware attacks.

Sources

AT&T Alien Labs Research
Blue Hexagon

Japanese Industrial organizations targeted for data exfiltration

Security researchers recently disclosed details of a campaign that deploys malicious backdoors for the purpose of exfiltrating information from numerous industrial targets in Japan. Dubbed "A41APT" by Kaspersky researchers, these attacks are "using previously undocumented malware to deliver as many as three payloads, such as SodaMaster, P8RAT, and FYAnti," The Hacker News reports. The TTP leverages a multi-stage attack process, with the initial intrusion happening via abuse of SSL-VPN by exploiting unpatched vulnerabilities or stolen credentials.

Source: The Hacker News

CopperStealer Performs Widespread Theft

Analysis of a CopperStealer sample – which cybersecurity firm Proofpoint describes as a "password and cookie stealer with a downloader function" – has been found to target Facebook and Instagram business and advertiser accounts. Secondary sample reversing identified additional versions that target other major service providers, including Apple, Amazon, Bing, Google, PayPal, Tumblr and Twitter. Researchers observed suspicious websites advertised as "KeyGen" or "Crack" sites promising users methods to circumvent licensing restrictions of legitimate software.

Source: Proofpoint

Rclone shown to be early indicator of compromise

Ransomware threat actors have been observed using the open-source tool Rclone to exfiltrate data in ransomware campaigns. The stolen data is then used as leverage to pressure targets into paying ransom demands. Rclone is frequently used with Mega.io to stage the exfiltrated data. Internal file servers with unfiltered Internet access are common targets. According to NCC Group data exfiltration often takes place long before the ransomware is deployed, often days in advance.

NCC incident response teams have observed outbound traffic to subdomains of Userstorage.mega.co[.]nz such as Gfs270n071.userstorage.mega.co[.]nz. NCC reports: "The domains typically resolve to IP addresses associate with the MEGA ASN 205809 but not in all cases. Where MEGA is not used, there is typically a large volume of outbound traffic to a single IP address which can be seen as a spike in any network monitoring."

Impact

Ransomware groups have continuously been observed exfiltrating data from compromised environments with the intent of using it to pressure victims to pay the ransom before the stolen data is leaked by the threat actors.

DXC perspective

The process of exfiltrating data is a detection opportunity. Organizations should be monitoring for unusual network activity. Indications of abnormal outbound traffic should create alerts to security personnel. Early detection may prevent the next stage of the attack, which is the encryption of data.

Source

NCC Group

Kernel driver tool Netfilter distributed using signed binary files

A custom malware loader is being used to deploy a previously unreported kernel driver rootkit tracked as Netfilter. Recent samples indicate the malicious tool was deployed using legitimately signed binary files (Microsoft Corporation certificates) by an unidentified threat actor.

Multiple Netfilter loader payloads have been distributed using the URL hxxp[:]//45.113.202[.]180:608/sdl since at least March 2021.

It is currently unclear how the operator behind this tooling accessed these certificates, or whether additional malicious tooling has been signed and distributed using this tactic. Analysis of the Netfilter tool is ongoing.

Deploying the implant as a signed device driver will likely hinder detection by network defense teams, given the prevalence of legitimate executables also using identical Microsoft signing certificates.

Microsoft advises: "The actor's activity is limited to the gaming sector specifically in China and does not appear to target enterprise environments. We are not attributing this to a nation-state actor at this time. The actor's goal is to use the driver to spoof their geo-location to cheat the system and play from anywhere. The malware enables them to gain an advantage in games and possibly exploit other players by compromising their accounts through common tools like keyloggers."

Impact

Supply chain attacks in any form or level of compromise are of concern. DXC will be monitoring for similar attacks using the TTPs described above.

DXC perspective

It is currently unknown how the rootkit successfully negotiated Microsoft's certificate signing process. Microsoft has stated it is investigating this incident and refining the signing process, partner access policies and validation.

Sources

Microsoft Security Response Center
G DATA

Analyzing the Conti ransomware gang

The FBI has connected Conti to more than 400 cyberattacks against organizations worldwide -- three-quarters based in the U.S. -- with ransom demands as high as $25 million. This makes Conti one of the greediest groups out there. Taking the normally loathsome patterns of ransomware gangs to a new level, Conti also stands out as unreliable as the group has a been known to dupe victims who pay ransoms with non-working decryption keys.

Source: Unit 42

Vulnerability updates

Dell addresses multiple vulnerabilities with client platform security updates

Dell released remediations for multiple security vulnerabilities affecting the BIOSConnect and HTTPS Boot features of its client BIOS, the cumulative score of the vulnerability chain coming in as 8.3 (High).

Dell says the "BIOSConnect feature is a Dell preboot solution that is used to update system BIOS and recover the operating system (OS) using the SupportAssist OS Recovery on Dell Client platforms," while the "Dell HTTPS Boot feature is an extension to UEFI HTTP Boot specifications to boot from an HTTP(S) Server."

The company reported the vulnerabilities below as a vulnerability chain:

- CVE-2021-21571: "Dell UEFI BIOS https stack, leveraged by the Dell BIOSConnect feature and Dell HTTPS Boot feature, contains an improper certificate validation vulnerability. A remote unauthenticated attacker may exploit this vulnerability using a person-in-the-middle attack, which may lead to a denial of service and payload tampering."

- CVE-2021-21572, CVE-2021-21573, CVE-2021-21574: “Dell BIOSConnect feature contains a buffer overflow vulnerability. An authenticated malicious admin user with local access to the system may potentially exploit this vulnerability to run arbitrary code and bypass UEFI restrictions.”

DXC perspective

Please refer to the Dell security advisory for resolution methods and workarounds.

Source

Dell Security Advisory

Other news

NAIKON a threat actor that has been tied to China

Cyber espionage by Chinese targeting neighboring nations

In 2016 North Korean hackers planned a $1B raid on Bangladesh’s national bank and came within an inch of success

CISA and the Multi-State Information Sharing and Analysis Center (MS-ISAC) release a Ransomware Guide

Nation state and geopolitical

Hackers exploit VPN flaw to break into South Korean nuclear research facility

The internal network of South Korea’s Korea Atomic Energy Research Institute (KAERI) was infiltrated on May 14. The perpetrators are believed to be threat actors called Kimsuky working on behalf of North Korea. The intruders appear to have exploited a vulnerability in an unnamed VPN. The investigation is ongoing to determine the full scale of the attack. The KAERI security team has since blocked the attackers’ IP addresses and updated its security controls.

The Korea Internet Security Association (KISA) ordered all government agencies to delete instances of an unspecified South Korean electronic document management program from their networks after discovering a vulnerability in an unspecified software program that allegedly causes network vulnerabilities.

The provider of the program claimed the vulnerability is not in its software but in the mechanism governing the launch of an unspecified plug-in.

DXC perspective

Cyber-espionage and exploit proof of concept testing are just two of the motives for this attack. DXC will continue to investigate the vulnerabilities exploited to determine relevance to other organizations.

Source

NikkeiAsia

DXC in security

Recognized as a leader in security services, DXC Technology helps customers prevent potential attack pathways, reduce cyber risk, and improve threat detection and incident response. Our expert advisory services and 24x7 managed security services are backed by 3,000+ experts and a global network of security operations centers. DXC provides solutions tailored to our customers' diverse security needs, with areas of specialization in Cyber Defense, Digital Identity, Secured Infrastructure and Risk Management. Learn how DXC can help protect your enterprise in the midst of large-scale digital change. Visit dxc.com/security.

Stay current on the latest threats
dxc.com/threats

Get the insights that matter.
dxc.com/optin

About DXC Technology

DXC Technology (NYSE: DXC) helps global companies run their mission critical systems and operations while modernizing IT, optimizing data architectures, and ensuring security and scalability across public, private and hybrid clouds. The world's largest companies and public sector organizations trust DXC to deploy services across the Enterprise Technology Stack to drive new levels of performance, competitiveness, and customer experience. Learn more about how we deliver excellence for our customers and colleagues at **dxc.com**.