RELIAQUEST®

June 26, 2024

Intelligence Summary
Recent ReliaQuest Publications

Access our entire Intel library via ReliaQuest GreyMatter®!

Key Points

- Our latest Threat Spotlight explains the risks that organizations face from software supply chain attacks. The report contains recommendations and best practices to better secure your organization from this threat.
- This week's ReliaQuest Shadow Talk podcast discusses new tactics for Scattered Spider and the reported arrest of the group's leader, ReliaQuest's newest report on software supply chain attacks, and insider threats.
- Recent Intel Updates cover vulnerabilities in VMware vCenter, Kubernetes, Trellix, Phoenix SecureCore UEFI firmware, and new tactics by the Scattered Spider group focusing on cloud applications.

Threat Spotlight Report: Software Supply Chain Risk Management

This Threat Spotlight provides insights into the threat of software supply chain attacks and includes comprehensive recommendations for organizations to implement a risk management program.

What You Need to Know: Industries that are heavily dependent on third-party software are particularly susceptible to this attack type due to their larger attack surface. ReliaQuest forecasts that nation-state–linked threat groups will continue to conduct software supply-chain attacks. Furthermore, this technique will likely be adopted by financially motivated threat actors in the long-term future.

What ReliaQuest is Doing: The ReliaQuest Threat Research team monitors and reports on supply-chain attacks. We offer enhanced security and immediate notifications to Digital Risk Protection (DRP) customers and provide detection rules and response plays to identify and remediate malicious activities from supply-chain compromises.

What You Can Do: A supply-chain risk management process that focuses on establishing a supplier inventory, documenting security requirements, vetting suppliers regularly, and creating supplier agreements can reduce the impact on business operations.

Intel Update: Critical Vulnerabilities in VMware vCenter Server Pose Remote Code Execution and Privilege Escalation Risks

Target audience	CISOs, SOC analysts, SOC managers

On June 18, 2024, VMware released fixes for vulnerabilities in VMware vCenter Server, a key management platform for VMware vSphere. CVE-2024-37079 and CVE-2024-37080 are critical severity heap-overflow vulnerabilities allowing remote code execution, with CVE-2024-37081 rated as a high severity local privilege escalation vulnerability caused by a misconfiguration in sudo. Exploiting these issues can lead to remote code execution and privilege escalation, compromising numerous virtual environments. These affect vCenter Server versions 7.0 and 8.0 and VMware Cloud Foundation 4.x and 5.x. VMware has issued updates in versions 8.0 U2d, 8.0 U1e, and 7.0 U3r for vCenter Server, while Cloud Foundation patches are available through KB88287. No active exploitation has been observed, but historical targeting of vCenter flaws underscores the urgency for immediate action to secure virtual environments.

Learn more about this vulnerability and review ReliaQuest's recommendations here.

Intel Update: Scattered Spider Hackers Switch Focus to Cloud Apps for Data Theft

Target audience	CISOs, SOC analysts, SOC managers, threat intelligence analysts, threat intelligence managers

The Scattered Spider gang (aka Octo Tempest, 0ktapus, Scatter Swine, and UNC3944) has demonstrated a shift in focus to data theft from SaaS applications. Attacks by the group have employed social engineering attacks such as SMS phishing, SIM swapping, and account hijacking to access on-premise systems. They have expanded their tactics to target cloud infrastructure and SaaS applications, leveraging compromised accounts to infiltrate victim environments and create new virtual machines while disabling security protections. They have also been observed disabling Microsoft Defender to deploy tools for lateral movement and have used tunneling utilities to bypass VPNs and multi-factor authentication. Organizations are advised to focus on SaaS applications with robust centralized logging and enforce stricter access policies to mitigate risks.

Learn more about this campaign and review ReliaQuest's recommendations here.

Intel Update: Critical Vulnerability (CVE-2023-32191) in Rancher Kubernetes Engine Exposes Sensitive Credentials

Target audience	CISOs, SOC analysts, SOC managers

On June 18, 2024, Kubernetes disclosed a critical vulnerability, CVE-2023-32191, in the Rancher Kubernetes Engine (RKE), a popular Kubernetes distribution. The flaw involves the storage of sensitive credentials such as SSH keys, AWS access keys, Azure AD client secrets, Kubernetes encryption keys, and cloud provider credentials within a ConfigMap named "full-cluster-state" in the kube-system namespace. This configuration grants administrative-level control over the entire cluster to anyone with read access to the ConfigMap, posing significant risks to confidentiality, integrity, and availability. To mitigate this vulnerability users should upgrade to RKE versions 1.4.19 or 1.5.10, or Rancher versions 2.7.14 or 2.8.5, which relocate the cluster state to a more secure secret accessible only by users with admin or cluster-owner roles.

Learn more about this vulnerability and review ReliaQuest's recommendations here.

Intel Update: Critical Vulnerability in Trellix IPS Manager Flaw Allows Remote Code Execution

Target audience	CISOs, SOC analysts, SOC managers

On June 19, 2024, ReliaQuest became aware of a critical vulnerability in Trellix IPS Manager, tracked as CVE-2024-5671, caused by insecure deserialization in certain workflows. This flaw, with a CVSSv3 score of 9.8, allows unauthenticated remote attackers to execute arbitrary code, posing a severe risk to network security. Exploiting this vulnerability can lead to complete control over affected systems, resulting in data theft, service disruption, and network compromise. It impacts Trellix IPS Manager versions prior to 11.1.x. No known exploitations of CVE-2024-5671 have been reported in the wild. However, organizations should urgently update to mitigate this vulnerability.

Learn more about this vulnerability and review ReliaQuest's recommendations here.

Intel Update: Phoenix SecureCore UEFI Firmware Flaw Allows Privilege Escalation and Code Execution

Target audience	CISOs, SOC analysts, SOC managers

On June 20, 2024, ReliaQuest became aware of a security flaw in Phoenix SecureCore UEFI firmware, identified as CVE-2024-0762. Dubbed "UEFIcanhazbufferoverflow," it affects multiple Intel Core processor families. This vulnerability stems from an unsafe variable in the TPM configuration, leading to a buffer overflow and enabling local attackers to execute malicious code within the UEFI firmware, escalating their privileges. Phoenix Technologies and Lenovo have released updates to mitigate the flaw, which impacts AlderLake, CoffeeLake, CometLake, IceLake, JasperLake, KabyLake, MeteorLake, RaptorLake, RocketLake, and TigerLake processors. This highlights the critical need for securing UEFI firmware to prevent persistent control by threat actors and underscores the importance of prompt patching.

Learn more about this vulnerability and review ReliaQuest's recommendations here.

Threat Profile: BlackMeta

Target audience	Threat intelligence analysts, threat intelligence managers

BlackMeta is a hacktivist group that primarily carries out DDoS attacks on organizations in Israel and countries it perceives to be supporting Israel, including the USA and other NATO countries. In November 2023, the group launched its Telegram channel, which posts information about targets and claimed attacks. Targets have spanned a wide variety of sectors including banks, telecommunications, healthcare, technology, and travel organizations. Their attacks appear to be strictly disruptive, and there have not been any in which they have attempted to extort targets.

ShadowTalk Podcast

In this week's episode, we discuss the latest news in cybersecurity and threat research, including: Scattered Spider leader reportedly arrested and the group's pivot to target SaaS solutions, ReliaQuest's research into supply chain compromise, and insider threats and the difficulties of proving intent.

See all our intelligence updates from the past seven days in GreyMatter.