Security-Blindspot: Wie Angreifer QEMU nutzen, um Erkennungssysteme zu umgehen

Der Einsatz versteckter virtueller Maschinen (VMs) ermöglicht Cyberkriminellen langfristigen Zugriff, Anmeldeinformationen-Diebstahl, Datenexfiltration und die Bereitstellung von PayoutsKing-Ransomware.

Sophos-Analysten untersuchen den aktiven Missbrauch von QEMU (Quick Emulator), einem Open-Source-Maschinenemulator und Virtualisierungs-Tool. Angreifer nutzen QEMU und weitere gängigere, auf Hypervisoren basierende Virtualisierungs-Tools, wie Hyper-V, VirtualBox und VMware, seit längerer Zeit. Grund dafür ist, dass böswillige Aktivitäten innerhalb einer virtuellen Maschine (VM) für die Endpunktsicherheit nahezu unsichtbar sind und auf dem Host kaum forensische Spuren hinterlassen. Die Sophos-Analysten haben jedoch einen Anstieg von Fällen beobachtet, in denen QEMU zur Umgehung von Abwehrmaßnahmen eingesetzt wird. Dabei haben die Experten seit Ende 2025 zwei unterschiedliche Kampagnen identifiziert und untersucht: STAC4713 und STAC3725.

STAC4713 ist kein Ransomware-as-a-Service-Modell

STAC4713 wurde erstmals im November 2025 beobachtet und ist eine finanziell motivierte Kampagne, die mit der PayoutsKing-Ransomware in Verbindung steht. Mehrere Vorfälle in dieser Kampagne beinhalteten QEMU als versteckte reverse SSH-Backdoor, um Angreifer-Tools bereitzustellen und Domänen-Anmeldeinformationen zu sammeln. Es ist sehr wahrscheinlich, dass die STAC4713-Kampagne mit Datendiebstahl und der Bereitstellung von PayoutsKing-Ransomware in Verbindung steht. Forscher der Sophos Counter Threat Uni (CTU) schreiben die PayoutsKing-Ransomware und die Erpressungsoperation, die Mitte 2025 aufkam, der GOLD ENCOUNTER-Bedrohungsgruppe zu. Die Betreiber von PayoutsKing haben explizit erklärt, dass sie nicht nach dem Ransomware-as-a-Service-Modell (RaaS) arbeiten oder mit Partnern zusammenarbeiten, was darauf hindeutet, dass taktische Unterschiede bei diesen beobachteten Vorfällen auf bewusste Entscheidungen der Angreifer und nicht auf separate Bedrohungsakteure zurückzuführen sind.

Ab Februar 2026 identifizierten Sophos-Analysten eine bemerkenswerte Veränderung in den Taktiken von GOLD ENCOUNTER, darunter verschiedene Vektoren für den Erstzugriff und den Einsatz von QEMU für versteckten Fernzugriff. In einem Vorfall im Februar 2026 erlangten die Bedrohungsakteure Zugriff über ein exponiertes Cisco SSL VPN; in einem Fall im März 2026 zielten sie auf Mitarbeiter über E-Mail-Spam ab und gaben sich über Microsoft Teams als IT-Support aus.

STAC3725 mit manueller Komponente

Eine weitere Kampagne, STAC3725, wurde erstmals im Februar 2026 beobachtet und nutzt die CitrixBleed2-Schwachstelle, um Zugriff zu erlangen, und Malware zu installieren. Die Bedrohungsakteure stellen eine QEMU-VM bereit, um zusätzliche Tools für Aufklärung und Anmeldeinformationen-Diebstahl zu installieren.

Anstatt ein vorgefertigtes Toolkit bereitzustellen, installierten und kompilierten die Angreifer ihr vollständiges Angriffspaket manuell innerhalb der VM. Beobachtete böswillige Aktivitäten umfassten das Herunterladen von Anmeldeinformationen, das Aufzählen von Kerberos-Benutzernamen, das Durchforsten des Active Directory-Aufklärung und das Ausführen von FTP-Servern für die Bereitstellung von Nutzlasten oder für die Datenexfiltration.

Die Folgeaktivitäten variierten je nach Eindringen, was darauf hindeutet, dass ursprüngliche Zugriffsbroker die Umgebungen der Opfer zunächst kompromittierten und den Zugriff dann an andere Bedrohungsakteure verkauften. In einem Vorfall hielten die Bedrohungsakteure den Zugriff auf die Umgebung aufrecht, in einem anderen Fall nutzten die Bedrohungsakteure

NetBird, um verschlüsselte Peer-to-Peer-Verbindungen herzustellen, Browsersitzungs-Cookies zu extrahieren und ein PowerShell-Skript auszuführen, um Microsoft Defender zu deaktivieren.

Empfehlungen, Schutzmaßnahmen und Indikatoren
Der Missbrauch von QEMU stellt einen wachsenden Trend dar, bei dem Bedrohungsakteure legitime Virtualisierungssoftware nutzen, um böswillige Aktionen vor dem Endpunktschutz und der Audit-Protokollierung zu verbergen. Eine verborgene VM mit einem vorinstallierten oder kompilierten Angriffstoolkit kann einem Bedrohungsakteur Zugriff auf ein Netzwerk gewähren und die Möglichkeit bieten, Malware bereitzustellen, Anmeldeinformationen zu sammeln und sich (lateral) im Netzwerk zu bewegen, ohne Spuren auf dem Host zu hinterlassen.
Organisationen sollten ihre Umgebungen auf nicht autorisierte QEMU-Installationen, unerwartete geplante Aufgaben (insbesondere solche, die unter einem SYSTEM-Konto ausgeführt werden) und ungewöhnliche Port-Weiterleitungsregeln, die auf Port 22 abzielen, überprüfen. Sicherheitsexperten sollten zudem ausgehende SSH-Tunnel überwachen, die von nicht standardmäßigen Ports ausgehen, und virtuelle Festplattenabbilder mit ungewöhnlichen Dateierweiterungen (z. B. .db, .dll, .qcow2) markieren.

Weitere technisch ausformulierte Schutzmaßnahmen haben die Experten von Sophos im neuen englischsprachigen Blog-Text „QEMU abused to evade detection and enable ransomware delivery“ zusammengestellt.

Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.

Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
X/Twitter: @sophos_info

Pressekontakt:

Sophos
press@sophos.com

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de