

QEMU abused to evade detection and enable ransomware delivery

 sophos.com/en-us/blog/qemu-abused-to-evade-detection-and-enable-ransomware-delivery

April 16, 2026

Sophos analysts are investigating the active abuse of [QEMU](#), an “open-source machine emulator and virtualizer,” by threat actors seeking to hide malicious activity within virtualized environments. Attackers are drawn to QEMU and more common hypervisor-based virtualization tools like Hyper-V, VirtualBox, and VMware because malicious activity within a virtual machine (VM) is essentially invisible to endpoint security controls and leaves little forensic evidence on the host itself.

The abuse of QEMU is a recurring technique that has been used by threat actors for many years:

- November 2020: Mandiant [described](#) a threat actor using QEMU on Linux systems to host tools and establish reverse SSH tunnels to command and control (C2) infrastructure.
- March 2024: Kaspersky [reported](#) threat actors abusing it for covert network tunneling.
- May 2025: Sophos [documented](#) attackers using it to deploy the QDoor backdoor and ultimately deliver 3AM ransomware.

However, Sophos analysts have observed an uptick in cases involving QEMU for defense evasion, with two distinct campaigns identified since late 2025: STAC4713 and STAC3725.

STAC4713

First observed in November 2025, STAC4713 is a financially motivated campaign associated with PayoutsKing ransomware. Several incidents in this campaign involved QEMU as a covert reverse SSH backdoor to deliver attacker tools and harvest domain credentials.

To deploy QEMU, the attackers begin by creating a scheduled task named ‘TPMProfiler’. This task launches a QEMU VM (`qemu-system-x86_64.exe`) under the SYSTEM account via a virtual hard disk image that has an uncommon file extension. In previous incidents, the disk image masqueraded as `vault.db`, but it switched to being disguised as a DLL (`bisrv.dll`) in January 2026.

The scheduled task also establishes persistence by enabling port forwarding from custom ports (32567, 22022) to port 22 (SSH). On boot, the disk image uses [AdaptixC2](#) or OpenSSH to establish a reverse SSH tunnel to a remote IP address. This action creates a covert remote access channel into the hidden VM, thus bypassing endpoint detections.

The QEMU VM hosts an [Alpine](#) 3.22.0 disk image that contains attacker tools. The tooling differs across incidents but commonly includes `tinker2` (AdaptixC2), `wg-obfuscator` (custom WireGuard traffic obfuscator), `BusyBox`, `Chisel`, and `Rclone`.

Sophos analysts also observed the following activity when investigating this campaign:

- The threat actors used the Volume Shadow Copy Service (VSS) user interface (vssuirun.exe) to create a volume shadow copy snapshot. They also leveraged the print command to copy the Active Directory database (NTDS.dit) and the SAM and SYSTEM hives to temp directories over SMB.
- The threat actors abused native tools such as Microsoft Paint, Notepad, and Microsoft Edge, as well as the freely available third-party [WizTree](#) tool, for network share discovery and file access.
- Initial access methods varied across intrusions. Older incidents leveraged exposed SonicWall VPNs that did not have multi-factor authentication (MFA) enabled, while a January 2026 incident exploited a SolarWinds Web Help Desk vulnerability ([CVE-2025-26399](#)). In February, [Microsoft](#) and [Huntress](#) reported similar observations of this vulnerability leading to QEMU deployment.

Links to PayoutsKing ransomware

It is highly likely that the STAC4713 campaign is linked to data theft and PayoutsKing ransomware deployment. Counter Threat Unit™ (CTU) researchers attribute the PayoutsKing ransomware and extortion operation, which emerged in mid-2025, to the [GOLD ENCOUNTER](#) threat group. Sophos analysis indicates that the group focuses on hypervisors and has encryptors targeting both VMware and ESXi environments. PayoutsKing operators have explicitly stated that they do not operate under a ransomware-as-a-service (RaaS) model or work with affiliates, suggesting that tactical differences across these observed incidents are due to deliberate attacker choices rather than separate threat actors.

Beginning in February 2026, Sophos analysts identified a notable shift in GOLD ENCOUNTER tactics, including different initial access vectors and the abandonment of QEMU for covert remote access. In a February 2026 incident, the threat actors gained access via an exposed Cisco SSL VPN; in a March 2026 case, they targeted employees through email spam and impersonated IT support over Microsoft Teams to trick users into downloading QuickAssist. In both instances, the threat actors used the legitimate ADNotificationManager.exe binary to sideload a Havoc C2 payload (vcruntime140_1.dll) and then leveraged Rclone to exfiltrate data to a remote SFTP location.

STAC3725

First observed in February 2026, the STAC3725 campaign exploits the CitrixBleed2 vulnerability ([CVE-2025-5777](#)) to gain access and then installs a malicious ScreenConnect client to maintain persistence. The threat actors deploy a QEMU VM to install additional tools for conducting enumeration and credential theft.

Following initial access to the victim's environment via NetScaler, the threat actors stage a ZIP archive (an.zip). An executable within the archive (an.exe) creates and starts a service named AppMgmt, which adds a new local admin user (CtxAppVCOMService) and installs the ScreenConnect client via a .msi file that was also likely bundled in the archive.

The ScreenConnect client executable (ScreenConnect.ClientService.exe) reaches out to its relay server (vtps . us) and establishes a session under system privileges. It then creates a ZIP archive in the victim's Documents directory (e.g., C:\Users\
<username>\Documents\ScreenConnect\Files\qemu_custom.zip), which is extracted via 7-Zip. The qemu-system-x86_64.exe file extracted from this archive uses a virtual disk image named custom.qcow2 to boot and run an Alpine Linux VM on the host.

Rather than deploying a pre-built toolkit, the attackers manually install and compile their full attack suite within the VM, including Impacket, KrbRelayx, Coercer, BloodHound.py, NetExec, Kerbrute, Metasploit, and supporting libraries for Python, Rust, Ruby, and C++. Observed malicious activity included downloading credentials, enumerating Kerberos usernames via Kerbrute, performing Active Directory reconnaissance via BloodHound, and running FTP servers via pyftplib for payload staging or data exfiltration. In addition to the QEMU activity, the ScreenConnect client adds a WDigest registry key to store credentials, installs FTK Imager to remove all Microsoft Defender exclusions, executes discovery commands, and installs a vulnerable kernel driver (K7RKScan_1516.sys).

Follow-on activity differed across intrusions, suggesting that initial access brokers originally compromised the victims' environments and then sold the access to other threat actors. In one incident, the threat actors maintained access to the environment by deploying [Total Software Deployment](#) and [Total Network Inventory](#) tools, as well as another rogue ScreenConnect client. In another case, the threat actors used [NetBird](#) to establish encrypted peer-to-peer connectivity, attempted to extract browser session cookies via cookie_exporter.exe, and executed a PowerShell script to disable Microsoft Defender.

Recommendations, protections, and indicators

The abuse of QEMU represents a growing evasion trend where threat actors leverage legitimate virtualization software to conceal malicious actions from endpoint protection agents and audit logs. A hidden VM with a pre-loaded or compiled attack toolkit can enable a threat actor to have long-term access to a network, providing the ability to deploy malware, harvest credentials, and move laterally without leaving evidence on the host itself.

Organizations should audit their environments for unauthorized QEMU installations, unexpected scheduled tasks (particularly those running under a SYSTEM account), and unusual port forwarding rules targeting port 22. Network defenders should monitor outbound SSH tunnels originating from non-standard ports and should flag virtual disk images with uncommon file extensions (e.g., .db, .dll, .qcow2).

Table 1 lists Sophos protections associated with this threat.

Name	Description
ATK/AdaptixC2-F	Detects AdaptixC2
Collection_2c	Detects print command used to dump credentials
win-eva-prc-susp-qemu-1	Detects QEMU usage with a port forward
AppC/Qemu-Gen	Application Control detection for QEMU
WIN-DET-CREDS-NTDS-DUMP-FILE-1[2]	Detects a dump of NTDS.dit

Table 1: Sophos protections associated with this threat

The threat indicators in Table 2 can be used to detect activity related to this threat. Note that IP addresses can be reallocated. The domain and IP addresses may contain malicious content, so consider the risks before opening them in a browser.

Indicator	Type	Cont
7ae413b76424508055154ee262c7567705dc1ac00607f5ac2e43d032221b34b3	SHA256 hash	Adap agen asso STAC
25e4d0eacff44f67a0a9d13970656cf76e5fd78c	SHA1 hash	Adap agen asso STAC
f7a11aeaa4f0c748961bbebb2f9e12b6	MD5 hash	Adap agen asso STAC
f3194018d60645e43afabac33ceb4e852f95241b410cd726b1c40e3021589937	SHA256 hash	Adap agen asso STAC
6c09b0d102361888daa7fa4f191f603a19af47cb	SHA1 hash	Adap agen asso STAC

Indicator	Type	Cont
b752ebfc1004f2c717609145e28243f3	MD5 hash	Adap agen asso STAC
c6b848c6a61685724fa9e2b3f6e3a118323ee0c165d1aa8c8a574205a4c4be59	SHA256 hash	QEM malic imag cont attac (vaul asso STAC
66dc383e9e0852523fe50def0851b9268865f779	SHA1 hash	QEM malic imag cont attac (vaul asso STAC
a65f0144101d93656c5f9ad445b3993336e1f295a838351aeca6332c0949b463	SHA256 hash	Legit QEM exec (qem x86_ asso STAC STAC
903edad58d54f056bd94c8165cc20e105b054fa8	SHA1 hash	Legit QEM exec (qem x86_ asso STAC STAC
b186baf2653c6c874e7b946647b048cc	MD5 hash	Legit QEM exec (qem x86_ asso STAC STAC

Indicator	Type	Cont
61c14c01460810f6f5f760daf8edbdba82eea908b1a95052f8e0f9c4162c2900c	SHA256 hash	QEM malic imag conta attac (bisn asso STAC
3a33b5bceb1eba4cc749534b03dd245f965d8f200aa02392baad78f5021a20ff	SHA256 hash	Cust Wire traffic binar obfus asso STAC
8c8e75dc4b4e1f201b56133a00fa9d1d711ccb50	SHA1 hash	Cust Wire traffic binar obfus asso STAC
6f55743091410dad6cdb0b7e474f03e7	MD5 hash	Cust Wire traffic binar obfus asso STAC
144[.]208[.]127[.]190	IP address	Susp serve SSH within VM c (bisn asso STAC

Indicator	Type	Cont
74[.]242[.]216[.]76	IP address	Susp serve desti SSH tunne estab vault asso STAC
194[.]110[.]172[.]152	IP address	Susp serve desti an S rever asso STAC
98[.]81[.]138[.]214	IP address	Susp serve desti SSH tunne estab vault asso STAC
158[.]158[.]0[.]165	IP address	Susp serve desti SSH tunne estab vault asso STAC
vtps[.]us	Domain name	Malic Scre relay asso STAC

Table 2: Indicators for this threat

About the author



Morgan Demboski

Morgan is a Threat Intelligence Analyst for the Sophos Managed Detection and Response (MDR) team, where her focuses include tactical cyber intelligence, data enrichment, and monitoring emerging threats. With a Masters in Intelligence and Security Studies, her areas of interest span beyond the cyber realm to include geopolitics and international security. In past roles, Morgan worked in the Network Detection and Response (NDR) space, where she focused on tracking attack patterns, analyzing command-and-control infrastructure, and threat research reporting.