

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **143** ze dne **12.5.2026**

Nová hackerská taktika? Útoky skryté ve virtuálních strojích.

Bezpečnostní experti společnosti Sophos upozorňují na rostoucí trend, kdy útočníci zneužívají virtualizační nástroje k ukrytí škodlivé aktivity přímo uvnitř napadených systémů. Tento přístup jim umožňuje obcházet tradiční bezpečnostní opatření a dlouhodobě setrvat v infrastruktuře organizací bez odhalení.

"Útočníky přitahují QEMU i běžnější virtualizační nástroje založené na hypervizoru, jako jsou Hyper-V, VirtualBox a VMware, protože škodlivá aktivita probíhající uvnitř virtuálního stroje (VM) je pro bezpečnostní nástroje na koncových bodech v podstatě neviditelná a na samotném hostitelském systému zanechává jen minimum forenzních stop. Útočníci tak získávají čas i prostor pro další škodlivé aktivity a přípravu útoků," uvedla Morgan Demboski, analytička kybernetických hrozeb v týmu Managed Detection and Response (MDR) společnosti Sophos.

Nová úroveň skrytí útoků

Sophos identifikoval několik aktivních kampaní, ve kterých útočníci zneužívají virtualizaci k dlouhodobému přístupu do firemních sítí, krádeži přihlašovacích údajů, exfiltraci citlivých dat, a přípravě a nasazení ransomwaru. V některých případech útočníci využili i známé zranitelnosti, například CitrixBleed2, nebo špatně zabezpečené VPN přístupy bez vícefaktorového ověření.

Zneužívání QEMU je opakující se technika, kterou útočníci využívají již řadu let:

- listopad 2020: Společnost Mandiant popsala případ, kdy útočník využil QEMU na linuxových systémech k hostování nástrojů a vytvoření reverzních SSH tunelů do infrastruktury pro řízení a kontrolu (C2);
- březen 2024: Kaspersky informoval o zneužívání QEMU pro skryté síťové tunelování;
- květen 2025: Sophos zdokumentoval útoky, při nichž byl QEMU použit k nasazení backdooru QDoor a následnému šíření ransomwaru 3AM.

Analytici společnosti Sophos však zaznamenali nárůst případů, kdy je QEMU zneužíván k obcházení bezpečnostních opatření, přičemž od konce roku 2025 identifikovali dvě samostatné kampaně: STAC4713 a STAC3725.

Hrozba i pro české firmy

Virtualizační technologie, jako například VMware nebo řešení od společnosti Microsoft, jsou běžnou součástí IT infrastruktury mnoha organizací v Česku. Nový přístup útočníků tak představuje reálné riziko napříč sektory.

"Firmy by měly počítat s tím, že útočníci dnes kombinují legitimní nástroje s pokročilými technikami skrývání. Ve fázi detekce už se nemůžete spolehnout jen na monitoring koncových bodů, ale musíte zohlednit i širší kontext a chování v síti," upozornila Demboski a organizacím doporučila: "Zaměřte se na audit prostředí z hlediska neautorizovaných virtualizačních nástrojů, sledujte

MEATEST spol. s r.o. - sdělení pověřence pro ochranu osobních údajů číslo **143** ze dne **12.5.2026**

neobvyklou síťovou komunikaci, například SSH tunely, kontrolujte podezřelé plánované úlohy i systémové procesy a dbejte na důsledné zabezpečení vzdálených přístupů včetně vícefaktorového ověřování."

AV centrum ČR