Mnoho Linuxových systémů je dlouhodobě infikováno nenápadným malwarem

cdr.cz/clanek/mnoho-linuxovych-systemu-je-dlouhodobe-infikovano-nenapadnym-malwarem

Zdroj: Shutterstock

Od roku 2021 infikoval tisíce linuxových systémů zákeřný malware s názvem Perfctl, který se vyznačuje nejen svou nenápadností, ale také širokým spektrem aktivit, které může vykonávat. Bezpečnostní experti upozorňují na jeho schopnost využívat zranitelnosti a nesprávné konfigurace, což ho činí obzvláště nebezpečným.

Malware s názvem Perfctl byl poprvé zaznamenán bezpečnostními výzkumníky z Aqua Security a od té doby představuje velkou hrozbu pro tisíce **linuxových systémů** po celém světě. Tento malware má schopnost zůstat skrytý v systému po dlouhou dobu, což znesnadňuje jeho detekci a následné odstranění. S využitím více než 20 000 známých chyb v konfiguraci systémů a závažných zranitelností, jako je CVE-2023-33246, se Perfctl zaměřuje na širokou škálu zařízení připojených k internetu.

Co je Perfctl?

Perfctl je škodlivý software, který zneužívá linuxové systémy především ke dvěma účelům: těžbě kryptoměn a fungování jako proxy server, který slouží k maskování původu internetového provozu. Malware se dokáže infiltrovat do systému tím, že se tváří jako legitimní procesy a soubory, což značně ztěžuje jeho odhalení. Název Perfctl je kombinací názvu linuxového monitorovacího nástroje 'perf' a zkratky 'ctl', běžně používané u příkazových nástrojů.

Zdroj: Shutterstock

Zajímavostí je, že Perfctl přebírá názvy souborů a procesů, které jsou velmi podobné těm, jež jsou v linuxových systémech běžné, což mu umožňuje se snadno skrýt. Malware se často instaluje jako rootkit, což znamená, že se ukrývá i před administrátorskými nástroji a operačním systémem.

Jak Perfctl funguje?

Po infikování systému Perfctl využívá několik technik, které mu umožňují přežít restart systému a pokračovat ve svých činnostech, i když jsou hlavní komponenty odstraněny. Mezi tyto techniky patří například úprava uživatelského prostředí při přihlášení (skript .profile) nebo kopírování samotného **malwaru** z paměti na různé části disku, čímž zajišťuje svou stálou přítomnost.

Další z jeho schopností je manipulace s linuxovým procesem pcap_loop, který monitoruje síťový provoz. Pomocí takzvaného hookingu dokáže Perfctl tento proces změnit tak, aby se administrátorovi nezobrazovaly žádné podezřelé aktivity. Malware rovněž potlačuje chyby při spouštění (mesg), aby uživatelé neviděli žádné varovné hlášky.

Perfctl také využívá anonymní komunikační sítě, jako je TOR, k odesílání dat a přijímání příkazů od útočníků. Po úspěšné infiltraci dokáže instalovat další malware, což zvyšuje jeho nebezpečnost pro infikovaný systém.

Šíření a zranitelnosti

Jednou z klíčových vlastností Perfctl je jeho schopnost využít širokou škálu zranitelností. Zvláště nebezpečná je jeho schopnost zneužít zranitelnost CVE-2023-33246, která se vyskytuje v systému Apache RocketMQ, populárním řešení pro zasílání zpráv a streamování dat na linuxových systémech. Tato zranitelnost byla ohodnocena nejvyšším stupněm závažnosti (10 z 10), což znamená, že útočník může snadno získat plný přístup k napadenému systému.

Dalším faktorem, který přispívá k šíření Perfctl, je existence tisíců linuxových **systémů** s nesprávnou konfigurací. Podle Aqua Security se jedná o více než 20 000 běžných nesprávných nastavení, které mohou být snadno zneužity k infikování systému. Výzkumníci odhadují, že potenciálně zranitelných systémů jsou miliony, což činí Perfctl velkým nebezpečím zejména pro organizace a jednotlivce po celém světě.

Kryptoměny a proxy servery

Jednou z hlavních funkcí malwaru Perfctl je těžba kryptoměn. Malware využívá systémové prostředky, jako je výpočetní výkon procesoru, k těžbě kryptoměn, čímž výrazně zpomaluje výkon infikovaného systému. Uživatelé si mohou všimnout zvýšené spotřeby energie a přehřívání zařízení, což jsou běžné indikátory kryptoměnové těžby.

Kromě těžby kryptoměn dokáže Perfctl infikovaný systém využívat jako proxy server. Tento proces, známý jako proxy-jacking, umožňuje útočníkům směrovat svůj internetový provoz přes infikované zařízení, čímž maskují svou pravou identitu a místo připojení. Taková aktivita může být pro uživatele nebezpečná, protože jejich IP adresa může být zneužita k nelegálním činnostem.

Detekce a prevence

Perfctl je obtížné detekovat, protože se dokáže velmi dobře skrýt. Pokud se však uživatelé setkají s neobvyklým chováním systému, jako je vysoké využití procesoru během nečinnosti nebo náhlé zpomalení systému, měli by začít pátrat po známkách infekce. Mezi hlavní indikátory patří neznámé procesy a soubory s podezřelými názvy, stejně jako neobvyklé aktivity na síti.

Prevence spočívá především v aplikaci bezpečnostních záplat a oprav, zejména pro zranitelnosti, jako je CVE-2023-33246. Důležité je také pravidelně kontrolovat nastavení systému a opravit známé chyby v konfiguraci, které by mohly být zneužity. Administrátoři by měli sledovat své systémy a nasazovat **bezpečnostní** nástroje, které dokážou detekovat známky kompromitace.

nahlásit chybu

Lukáš "Francesco" Čihák

více článků, blogů a informací o autorovi

Diskuse ke článku Mnoho Linuxových systémů je dlouhodobě infikováno nenápadným malwarem

Žádné komentáře.

Pro psaní komentářů se, prosím, přihlaste nebo registrujte.