آزمایشگاه تخصصی آپا، قزوین

دانشگاه بین المللی امام خمینی (ره)

خبرنامه تحلیلی رویدادهای امنیتی (روزانه)

سه‌شنبه دوم مهر ماه ۱۳۹۸

کشف بدافزار[1] استخراج ارز دیجیتال[2] در سیستم‌عامل لینوکس[3]

نسخه ۱,۰,۰

نویسنده : مونا رضا زاده **سردبیر :** محمد پیشدار

[1]-Malware is any software intentionally designed to cause damage to a computer, server, client, or computer network.

[2]-A cryptocurrency is a digital asset designed to work as a medium of exchange that uses strong cryptography to secure financial transactions, control the creation of additional units, and verify the transfer of assets

[3]-Linux is a family of free and open-source software operating systems based on the Linux kernel.

یک بدافزار استخراج ارز دیجیتال در سیستم‌عامل لینوکس کشف شده است

تاریخ: ۱۳/ سپتامبر / ۲۰۱۹

بررسی اجمالی :

محققان حوزه امنیت اطلاعات موفق به کشف یک بدافزار جدید در سیستم‌عامل لینوکس شده‌اند. این بدافزار اِسکیدمَپ[1] نام داشته و فعالیت‌های خود در زمینه استخراج ارز دیجیتال را با جعل ترافیک شبکه و آمارهای مربوط به پردازنده مخفی نگه می‌دارد. اِسکیدمَپ علاوه بر استخرج ارز دیجیتال، دسترسی بدون وقفه به یک سیستم آلوده را نیز در اختیار مهاجم قرار می‌دهد [۱].

نگاه کلی :

سیستم‌های آسیب‌پذیر	سیستم‌عامل لینوکس		
شدت خطر	**در دولت**	**در تجارت**	**کاربران خانگی**
	بالا	**بالا**	**بالا**
راه‌های نفوذ	دستکاری ماژول امنیتی لینوکس، جایگزینی ماژول احراز هویت لینوکس با یک نسخه مخرب		
هدف	استخراج غیرمجاز ارز دیجیتال		

[1]-Skidmap

توضیحات فنی :

اخیرا محققان شرکت امنیتی تِرندمیکرو[1] بدافزاری به نام اِسکیدمَپ را در سیستم‌عامل لینوکس شناسایی کرده که با استفاده از رویت‌کیت‌ها[2] خود را مخفی می‌سازد. رویت‌کیت بدافزاری است که بدون اطلاع کاربر، کدهای دلخواه خود را روی سیستم قربانی نصب و اجرا می‌کند. اِسکیدمَپ با استفاده از رویت‌کِیت‌های هسته‌ای وجود خود را در سیستم‌های آلوده پنهان کرده و دسترسی نامحدود به منابع سیستم را برای مهاجم ممکن می‌سازد [۱].

نصب اولیه بدافزار اِسکیدمَپ از طریق فرایند کُرنتاب[3] سیستم‌عامل لینوکس (این فرایند به صورت دوره‌ای کارهای زمان‌بندی شده را برنامه‌ریزی می‌کند) صورت می‌گیرد. در مرحله بعد این بدافزار، پیلودهای[4] مخرب را نصب کرده و امنیت دستگاه آسیب‌پذیر را با دستکاری یکی از ماژول‌های امنیتی لینوکس به نام اِس.ای.لینوکس[5] به حداقل می‌رساند. بعد از انجام این مراحل یک درِپشتی[6] ایجاد شده و اِسکیدمَپ با جایگزینی ماژول احراز هویت لینوکس با یک نسخه مخرب، باعث پذیرش رمز عبور "اصلی[7]" برای هر کاربر در دستگاه هدف می‌گردد. بنابراین یک مهاجم می‌تواند با سطح دسترسی دلخواه و بدون نیاز به احراز هویت وارد سیستم شود. پس از آن این بدافزار با توجه به دستگاه مورد نظر قابلیت ارسال فایل‌های تار.جی‌زِد[8] (رمزگذاری شده) یا یک نرم‌افزار مستقل را خواهد داشت [۱].

بسیاری از عملکردهای اِسکیدمَپ نیاز به دسترسی سطح ریشه داسته و این بدافزار باید از رویت‌های هسته برای تامین دسترسی‌های خود استفاده کند. فرآیندی که شناسایی آلودگی و فعالیت استخراج ارز را بسیار سخت می‌کند. علاوه بر این اِسکیدمَپ با جعل ترافیک‌های مربوط به شبکه و پردازنده، آلودگی دستگاه را مخفی نگه می‌دارد. لازم به ذکر است که بار سنگین پردازنده یکی از روش‌های تشخیص استخراج ارز دیجیتال در سیستم بوده که بدافزار اِسکیدمَپ با جعل آمارها این موضوع را مخفی می‌کند [۱].

پیشنهادات [۱]

[1]-Trend Micro Inc is a Japanese multinational cyber security and defense company founded in Los Angeles, California with global headquarters in Tokyo, Japan, a R&D center in Taipei, Taiwan, and regional headquarters in Asia, Europe and the Americas.

[2]-A rootkit is a collection of computer software, typically malicious, designed to enable access to a computer or an area of its software that is not otherwise allowed and often masks its existence or the existence of other software. The term rootkit is a concatenation of "root" and the word "kit".

[3]-Crontab stands for “cron table” because it uses the job scheduler cron to execute tasks.

[4]-In computing and telecommunications, the payload is the part of transmitted data that is the actual intended message.

[5]-Security-Enhanced Linux is a Linux kernel security module that provides a mechanism for supporting access control security policies, including mandatory access controls. SELinux is a set of kernel modifications and user-space tools that have been added to various Linux distributions.

[6]-A backdoor is a malware type that negates normal authentication procedures to access a system. As a result, remote access is granted to resources within an application, such as databases and file servers, giving perpetrators the ability to remotely issue system commands and update malware.

[7]-master

[8]-tar.gz

- استفاده از ابزارهای امنیتی بروز

منابع :

1. Zdnet Website
https://www.zdnet.com/article/skidmap-malware-buries-into-the-kernel-to-hide-cryptocurrency-mining/