شرکت نرم افزاری امن پرداز®
Amnpardaz Software Corporation



گزارش بلومبرگ از کشف نخستین نهان‌افزار در سرورهای HP (iLO Bleed)

AMNPARDAZ

AMNPARDAZ

مقدّمـه

در سال ۲۰۲۰، **شرکت نرم‌افزاری امن‌پرداز** هنگام بررسی یک سرور HPE که به دلیل تخریب داده‌ها به این شرکت تحویل داده شده بود، موفق به کشف یک تهدید بی‌سابقه در عمیق‌ترین لایه زیرساخت شد. امن پرداز با انتشار گزارش فنی رسمی خود در دی‌ماه ۱۴۰۰ (دسامبر ۲۰۲۱)، پرده از وجود یک بدافزار در سفت‌افزار ماژول مدیریتی iLO برداشت که آن را Implant.ARM.iLOBleed.a نامید.

اهمیت این کشف در حوزه امنیت سایبری بسیار فراتر از یک آسیب‌پذیری معمولی است؛ چرا که ماژول iLO بالاترین سطح دسترسی ممکن به سخت‌افزار، منبع تغذیه، دیسک‌ها و گذرگاه های ارتباطی سرور را در اختیار دارد. نفوذ به این لایه به معنای اعطای کنترل مطلق بر سرور و در نهایت، دسترسی کامل به اطلاعات حیاتی و کل زیرساخت سازمان است. با وجود گذشت بیش از پنج سال از کشف این تهدید، تهدیدات سفت‌افزاری همچنان یکی از رایج‌ترین و خطرناک‌ترین روش‌های حمله به زیرساخت‌های حیاتی کشور محسوب می‌شوند و سبب نفوذ گروه‌های APT به دیتاسنترهای متعددی شده‌اند.

کشف این بدافزار در سطح جهان به عنوان **نخستین نمونه مستند** از بدافزار واقعی در سفت افزار iLO شناخته شد و سبب شد تا بسیاری از خبرگزاری‌های بزرگ دنیا و محافل امنیت سایبری به تحلیل و بررسی اهمیت این موضوع بپردازند. در این میان، خبرگزاری **بلومبرگ (Bloomberg)** با انتشار گزارشی در ۹ فوریه ۲۰۲۲ به قلم جردن رابرتسون، این رویداد را به عنوان یک «کشف تکان‌دهنده» و «معمایی در ایران» در سطح بین‌المللی پوشش داد. در ادامه، متن این خبر ارائه می‌شود.

Discovery of Server Malware in Iran


Bloomberg the Company & its Products | Bloomberg Terminal Demo Request | Bloomberg Anywhere Remote Login | Bloomberg Customer Support

Bloomberg

US Edition | Sign In | Subscribe

Live Now | Markets | Economics | Industries | Tech | AI | Politics | Wealth | Pursuits | Opinion | Businessweek | Equality | Green | CityLab | Crypto | More

Newsletter
Cybersecurity

Iran Hack Startles the Global Cybersecurity Community

By Jordan Robertson
February 9, 2022 at 3:15 PM GMT+3:30
Updated on February 9, 2022 at 8:34 PM GMT+3:30

Save

A mystery in Iran

In the final days of 2021, a cybersecurity firm in Iran detailed a startling discovery: a mysterious piece of malicious code in a server made by Texas-based Hewlett Packard Enterprise Co.

The Tehran-based company, Amnpardaz Software Co., is little known outside of Iran. The same can be said about cybersecurity inside the country: For most of the world, visibility inside Iran is vanishingly low.

معمّـــایی در ایـــــران

در روزهای پایانی سال ۲۰۲۱، یک شرکت امنیت سایبری در ایران جزئیات کشفی تکان دهنده را منتشر کرد: یک قطعه کد مخرب مرموز در سروری ساختِ شرکت Hewlett Packard Enterprise Co مستقر در تگزاس.

It caught security professionals' attention, then, when Amnparadz in December announced its discovery of the malware. Amnparadz said its technicians had first spotted the suspicious software in 2020 when a customer supplied an HPE server that appeared to be malfunctioning.

هنگامی‌که **«امن‌پرداز»** در ماه دسامبر خبر کشف این بدافزار را منتشر کرد، توجه متخصصان امنیت سایبری را به خود جلب کرد. امن‌پرداز اعلام کرد که متخصصان این شرکت نخستین بار در سال ۲۰۲۰ این نرم‌افزار مشکوک را زمانی شناسایی کردند که یک مشتری، سرور HPE را که به نظر می رسید دچار نقص فنی شده است، به آن‌ها تحویل داد.

A Hidden Power in Cybersecurity

A mystery in Iran

In the final days of 2021, a cybersecurity firm in Iran detailed a startling discovery: a mysterious piece of malicious code in a server made by Texas-based Hewlett Packard Enterprise Co.

The Tehran-based company, Amnpardaz Software Co., is little known outside of Iran. The same can be said about cybersecurity inside the country: For most of the world, visibility inside Iran is vanishingly low.

The most infamous hack there happened more than a decade ago – the suspected U.S. and Israeli operation to sabotage Iranian nuclear

۴ **شرکت نرم‌افزاری امن‌پرداز (Amnparadz Software Co.) که در تهران مستقر است، خارج از ایران چندان شناخته‌شده نیست. وضعیت امنیت سایبری در داخل این کشور نیز همین‌گونه است: از نگاه بیشتر نقاط جهان، دید و شفافیت نسبت به اتفاقات داخل ایران بسیار پایین است.**

The most infamous hack there happened more than a decade ago - the suspected U.S. and Israeli operation to sabotage Iranian nuclear equipment with advanced tools, known as Stuxnet. There have been few revelations since then.

۵ **شناخته‌شده‌ترین و جنجالی‌ترین** هک در ایران بیش از یک دهه پیش رخ داد: عملیات مشکوک آمریکا و اسرائیل برای خرابکاری در تجهیزات هسته‌ای ایران با ابزارهای پیشرفته که به «استاکس‌نت» معروف شد. از آن زمان تاکنون، افشاگری‌های اندکی صورت گرفته است.

Anatomy of the Advanced Attack

The malware disabled key security controls on the server, Amnparadz said. The company said it found evidence that hackers had used the malware to remotely access the server for at least six months and then triggered a self-destruct cycle to erase evidence of the attack.

۶ **امن‌پرداز اعلام کرد که این بدافزار کنترل‌های امنیتی کلیدی سرور را غیرفعال کرده بود. به گفتهٔ این شرکت، شواهدی در دست است که هکرها دست‌کم شش ماه از این بدافزار برای دسترسی از راه دور به سرور استفاده کرده و سپس یک چرخهٔ خودتخریبی را برای پاک کردن شواهد حمله فعال کرده‌اند.**

۷ در گزارش **امن‌پرداز** آمده است: «مهاجمان تصمیم گرفته بودند دیسک‌های سرور را پاک کنند و ردپای خود را کاملاً محو کنند. بدیهی است که آن‌ها فکر نمی‌کردند بدافزارشان کشف شود.»

"The attackers had decided to wipe the server's disks and completely hide their tracks," Amnparadz wrote in its report. "Clearly, they didn't think their malware will be found."

۸ این کشف نشان‌دهندهٔ یک عملیات هک پیشرفته است که در آن مهاجمان ماه‌ها به گردآوری داده‌ها پرداخته و در تمام این مدت پنهان مانده‌اند. هویت مهاجمان همچنان یک معماست، اما ماهیت اصلی عملیات حکایت از انگیزه‌ای فراتر از جرایم سایبری متعارف دارد.

The discovery reveals an advanced hacking operation in which attackers spent months gathering data while maintaining their secrecy. The identity of the intruders remains a mystery, though the thrust of the operation suggests a motive beyond traditional cybercrime.

HPE Response and Sanctions Context

۹ HPE در بیانیه‌ای اعلام کرد که این بدافزار از یک آسیب پذیری در سفت‌افزار iLO استفاده کرده است که این شرکت در سال ۲۰۱۷ آن را برطرف کرده بود. در این بیانیه آمده است: «ما نمی‌دانیم این سرور چگونه وارد ایران شده است. ما به‌صورت مستقیم یا غیرمستقیم به ایران، یا به هیچ مشتری‌ای که بدانیم قصد ارسال محصولات‌مان به ایران را دارد، فروش انجام نمی‌دهیم.»

In a statement, HPE said the malware used a vulnerability in the iLO firmware that the company fixed in 2017. "We do not have visibility into how the server got into the country. HPE does not directly or indirectly sell into Iran or to any customers we know intend to send products to Iran," the company said in its statement.

۱۰ به دلیل تحریم‌های دولت آمریکا، شرکت‌های آمریکایی با ممنوعیتی تقریباً کامل برای فروش محصول به ایران مواجه‌اند؛ اما این فناوری‌ها اغلب از راه شبکه‌های گستردهٔ فروشندگان مستقل و واسطه‌ها به‌صورت غیرقانونی تهیه می‌شوند.

American companies face a near-total ban on selling products to Iran because of U.S. government sanctions, but the technologies can often be acquired illicitly through vast networks of independent resellers and third parties.

Expert Assessment
and the Cyber Arms Race

Upon studying Amnparadz's findings, Eclipsium Inc., an Oregon-based firmware security company, said the malware had "proven to be stealthy, persistent and damaging," with a capability of taking "virtually omnipotent control" over a breached machine.

۱۱ **شرکت .Eclipsium Inc، فعال در حوزهٔ امنیت فریم‌ور و مستقر در اورگان، پس از بررسی یافته‌های امن‌پرداز اعلام کرد این بدافزار «پنهان‌کار، ماندگار و مخرب» است و می‌تواند «کنترلی تقریباً مطلق» بر دستگاهی که به آن نفوذ کرده اعمال کند.**

۱۲ در گذشته، هک‌های پیشرفته‌ای که به دست‌کاری فریم‌ور و سخت‌افزار رایانه دست می‌زنند به‌ندرت شناسایی می‌شدند؛ اما امروز این نوع هک‌ها بیشتر شناسایی می‌شوند. (بیشتر هک‌ها با سوءاستفاده از آسیب‌پذیری‌های نرم‌افزارهای رایانه‌ای انجام می‌شوند.)

Once rarely detected, advanced hacks involving manipulations of computer firmware and hardware are now spotted more frequently. (Most hacks involve attacking flaws in computer software).

۱۳ در واکنش، شرکت‌های فناوری محصولات تازه‌ای عرضه می‌کنند تا جلوی چنین حملاتی را بهتر بگیرند. برای نمونه، مایکروسافت از سال ۲۰۱۹ سیستم‌هایی را عرضه کرده که از تراشه‌های سیلیکونی جدید بهره می‌برند؛ به گفتهٔ این شرکت، این تراشه‌ها برای کمک به جلوگیری از بارگذاری کد مخربِ پنهان‌شده در فریم‌ور توسط گروه‌های هکری تحت حمایت دولت‌ها طراحی شده‌اند.

In response, technology companies are rolling out new products to better block such attempts. Microsoft Corp., for example, in 2019 began pushing systems that use new silicon chips, which the company said are designed to help stop nation-state hacking groups from being able to load malicious code buried in firmware.

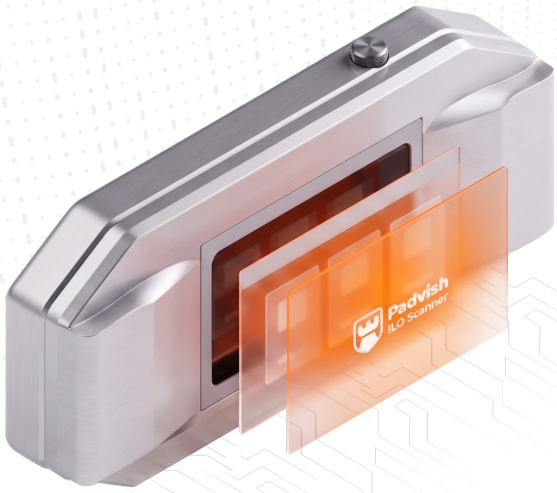
۱۴ اما تعداد انبوه قطعات و حجم عظیم کد سطح‌پایین در سیستم‌های رایانه‌ای امروزی، در کنار گستردگی زنجیرهٔ تأمین فناوری، مزیتی ذاتی برای مهاجمان ایجاد می‌کند.

However, the sheer number of components and the amount of low-level code present in modern computer systems, along with the vastness of the technology supply chain, gives attackers an inherent advantage.

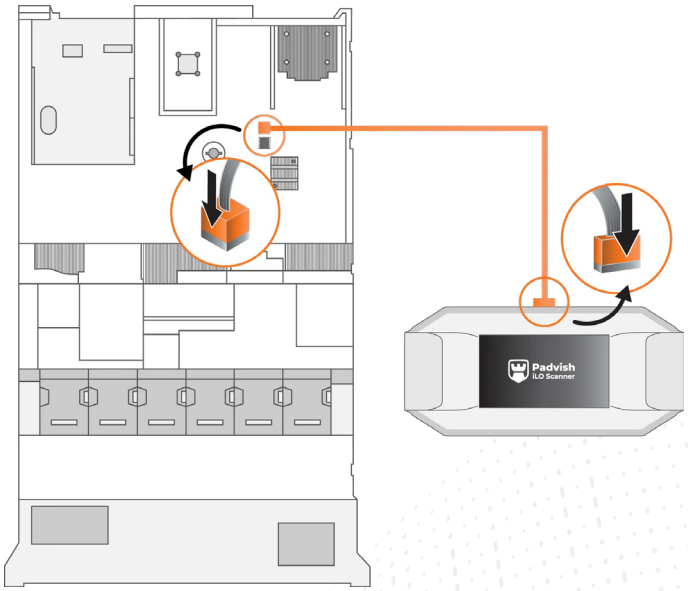
۱۵ امن‌پرداز دربارهٔ عاملان این حمله گمانه‌زنی نکرد. این کشف نشان می‌دهد که مسابقهٔ تسلیحاتی سایبری تمام‌شدنی نیست و این مسابقه ادامه خواهد یافت.

Amnparadz didn't speculate on who was behind the attack. But if the firm's discovery is any indication, the cyber arms race will only continue.

پایان یک بن‌بست؛ راهکار امن‌پرداز



پاسخ قاطع **گروه شرکت‌های امن‌پرداز** به این چالش جهانی، طراحی و تولید **Padvish iLO Scanner** بود. این دستگاه، یک پلتفرم سخت‌افزاری کاملاً مستقل، پرتابل و ایزوله (Air-Gapped) است که قواعد بازی را در امنیت دیتاسنتر تغییر می‌دهد. بدون نیاز به روشن بودن سرور یا خروج آن از رک، تکنسین می‌تواند با اتصال یک گیرهٔ اختصاصی به تراشهٔ SMD NOR Flash، محتوای سفت‌افزار را استخراج کرده و با الگوریتم‌های هوشمند دستگاه، آن را اعتبارسنجی کند.



در صورت تشخیص آلودگی یا پاک‌شدگی محتوای تراشه، **اسکنر پادویش** مستقیماً سفت‌افزار اصیل را از طریق بستهٔ به‌روزرسانی معتبر که با امضای دیجیتال محافظت می‌شود، روی چیپ بازنویسی می‌کند. توسعهٔ **Padvish iLO Scanner** صرفاً ارائهٔ یک ابزار عیب‌یابی نیست؛ این راهکار به معنای مسدودسازی کامل خطرناک‌ترین نقطهٔ کور در لایهٔ Sub-OS سرورهای سازمانی است.

اطلاعات بیشتر

جمع‌بندی

کشف iLOBleed توسط **امن‌پرداز**، نخستین نمونهٔ مستند از بدافزار واقعی در سفت‌افزار iLO در جهان است که مورد تأیید HPE و شرکت مستقل Eclipsium قرار گرفته است. این کشف نشان می‌دهد که لایهٔ سفت‌افزار کنترلر مدیریتی سرور – که همواره روشن است، خارج از دید ابزارهای امنیتی متعارف قرار دارد و به‌روزرسانی معمول نمی‌تواند آلودگی آن را حذف کند – به هدفی واقعی برای مهاجمان پیشرفته تبدیل شده است. پاسخ امن‌پرداز، سامانهٔ سخت‌افزاری **Padvish iLO Scanner** است که با دسترسی مستقیم به تراشه و اعتبارسنجی سفت‌افزار، این نقطهٔ کور را قابل بررسی و قابل پاک‌سازی می‌کند.

AMNPARDAZ



شرکت نرم افزاری امن پرداز®
Amnpardaz Software Corporation

www.amnpardaz.com info@amnpardaz.com 021 - 43912000