

Malware burrows deep into computer BIOS to escape AV

 theregister.co.uk/2011/09/14/bios_rootkit_discovered/

Dan Goodin

Security

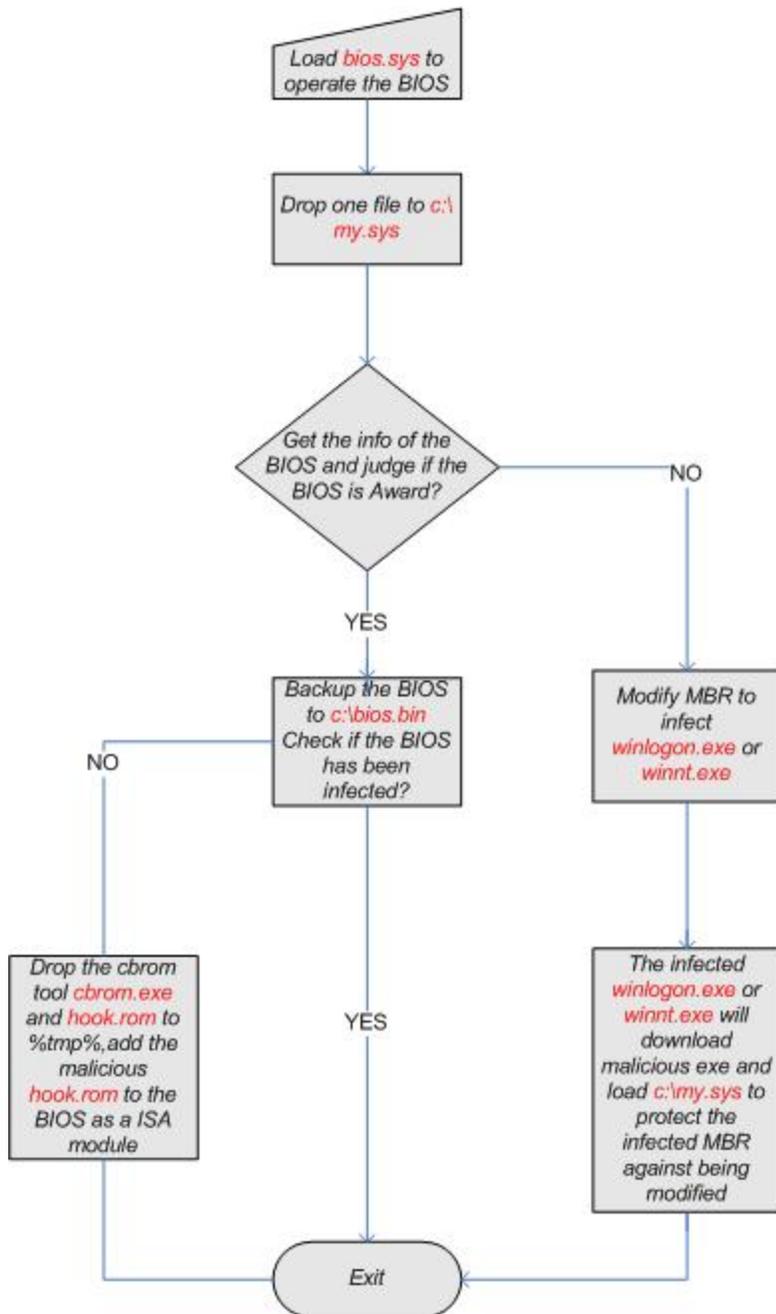
Mebromi rootkit also targets master boot record

Dan Goodin Wed 14 Sep 2011 // 04:53 UTC

Researchers have discovered one of the first pieces of malware ever used in the wild that modifies the software on the motherboard of infected computers to ensure the infection can't be easily eradicated.

Known as Trojan.Mebromi, the rootkit reflashes the BIOS of computers it attacks to add malicious instructions that are executed early in a computer's boot-up sequence. The instructions, in turn, alter a computer's MBR, or master boot record, another system component that gets executed prior to the loading of the operating system of an infected machine. By corrupting the processes that run immediately after a PC starts, the malware stands a better chance of surviving attempts by antivirus programs to remove it.

In addition to posing a threat to end users, Mebroot could create serious obstacles to antivirus developers in producing products that scrub computers clean of detected threats without harming the underlying system.



A flowchart from Symantec detailing Mebromi's BIOS tampering process.

"Storing the malicious code inside the BIOS ROM could actually become more than just a problem for security software, giv[en] the fact that even if antivirus detect[s] and clean[s] the MBR infection, it will be restored at the next system startup when the malicious BIOS payload would overwrite the MBR code again," Webroot researcher Marco Giuliani wrote in a [blog post](#) published Tuesday. "Developing an antivirus utility able to clean the BIOS code is a challenge, because it needs to be totally error-proof, to avoid rendering the system unbootable at all."

He went on to say the job of ridding malicious instructions added to the BIOS ultimately should be left to the makers of the motherboards that store the startup code. Because the BIOS is stored on an EEPROM, or electronically erasable programmable read-only-memory

chip, modifications have the potential to render a computer largely inoperable with no easy way to fix it.

The discovery represents one of the few times researchers have documented malware used in the wild that modifies the BIOS. In the late 1990s, malware known as CIH/Chernobyl did much the same thing on machines running Windows 9x by exploiting a privilege escalation bug in the Microsoft operating systems. In 2007, proof-of-concept software known as IceLord also reportedly made changes to the BIOS of infected machines, but there are no reports it has ever been used in actual attacks.

Mebromi is able to attack only BIOS ROMs made by Award, a manufacturer that was purchased by Phoenix in the late 1990s. The malware checks the BIOS ROM each time the PC boots up. If it's made by Award and the malicious instructions aren't found, Mebromi adds the code by reflashing the chip on the motherboard. According to Giuliani, it was first documented by the Chinese security company [Qihoo 360](#), and primarily infects computers in that country.

Symantec researchers have more about Mebromi [here](#). ®

This article was updated to clarify the type of chip stores the BIOS.

Other stories you might like

- [Stolen university credentials up for sale by Russian crooks, FBI warns](#)

[Forget dark-web souks, thousands of these are already being traded on public bazaars](#)

[Jessica Lyons Hardcastle](#) Fri 27 May 2022 // 22:34 UTC 

Russian crooks are selling network credentials and virtual private network access for a "multitude" of US universities and colleges on criminal marketplaces, according to the FBI.

According to a warning issued on Thursday, these stolen credentials sell for thousands of dollars on both dark web and public internet forums, and could lead to subsequent cyberattacks against individual employees or the schools themselves.

"The exposure of usernames and passwords can lead to brute force credential stuffing computer network attacks, whereby attackers attempt logins across various internet sites or exploit them for subsequent cyber attacks as criminal actors take advantage of users recycling the same credentials across multiple accounts, internet sites, and services," the Feds' alert [\[PDF\]](#) said.

[Continue reading](#)

- [Big Tech loves talking up privacy – while trying to kill privacy legislation](#)

[Study claims Amazon, Apple, Google, Meta, Microsoft work to derail data rules](#)

[Thomas Claburn in San Francisco](#) Fri 27 May 2022 // 21:48 UTC 2 

Amazon, Apple, Google, Meta, and Microsoft often support privacy in public statements, but behind the scenes they've been working through some common organizations to weaken or kill privacy legislation in US states.

That's according to [a report](#) this week from news non-profit The Markup, which said the corporations hire lobbyists from the same few groups and law firms to defang or drown state privacy bills.

The report examined 31 states when state legislatures were considering privacy legislation and identified 445 lobbyists and lobbying firms working on behalf of Amazon, Apple, Google, Meta, and Microsoft, along with industry groups like TechNet and the State Privacy and Security Coalition.

[Continue reading](#)

- [SEC probes Musk for not properly disclosing Twitter stake](#)

[Meanwhile, social network's board rejects resignation of one its directors](#)

[Katyanna Quach](#) Fri 27 May 2022 // 21:26 UTC 2 

America's financial watchdog is investigating whether Elon Musk adequately disclosed his purchase of Twitter shares last month, just as his bid to take over the social media company hangs in the balance.

A letter [\[PDF\]](#) from the SEC addressed to the tech billionaire said he "[did] not appear" to have filed the proper form detailing his 9.2 percent [stake](#) in Twitter "required 10 days from the date of acquisition," and asked him to provide more information. Musk's shares made him one of Twitter's largest shareholders. The letter is dated April 4, and was shared this week by the regulator.

Musk quickly moved to try and buy the whole company outright in a deal initially worth over \$44 billion. Musk sold a chunk of his shares in Tesla worth \$8.4 billion and [bagged](#) another \$7.14 billion from investors to help finance the \$21 billion he [promised](#) to put forward for the deal. The remaining \$25.5 billion bill was secured via debt financing by Morgan Stanley, Bank of America, Barclays, and others. But the takeover is not going smoothly.

[Continue reading](#)

- [Cloud security unicorn cuts 20% of staff after raising \\$1.3b](#)

[Time to play blame bingo: Markets? Profits? Too much growth? Russia? Space aliens?](#)

[Jessica Lyons Hardcastle](#) Fri 27 May 2022 // 19:19 UTC 6 

Cloud security company Lacework has laid off 20 percent of its employees, just months after two record-breaking funding rounds pushed its valuation to \$8.3 billion.

A spokesperson wouldn't confirm the total number of employees affected, though told *The Register* that the "widely speculated number on Twitter is a significant overestimate."

The company, as of March, counted more than 1,000 employees, which would push the jobs lost above 200. And the widely reported number on Twitter is about 300 employees. The biz, based in Silicon Valley, was founded in 2015.

[Continue reading](#)

- [Talos names eight deadly sins in widely used industrial software](#)

[Entire swaths of gear relies on vulnerability-laden Open Automation Software \(OAS\)](#)

[Jeff Burt](#) Fri 27 May 2022 // 18:30 UTC 

A researcher at Cisco's Talos threat intelligence team found eight vulnerabilities in the Open Automation Software (OAS) platform that, if exploited, could enable a bad actor to access a device and run code on a targeted system.

The OAS platform is widely used by a range of industrial enterprises, essentially facilitating the transfer of data within an IT environment between hardware and software and playing a central role in organizations' industrial Internet of Things (IIoT) efforts. It touches a range of devices, including PLCs and OPCs and IoT devices, as well as custom applications and APIs, databases and edge systems.

Companies like Volvo, General Dynamics, JBT Aerotech and wind-turbine maker AES are among the users of the OAS platform.

[Continue reading](#)

- [Despite global uncertainty, \\$500m hit doesn't rattle Nvidia execs](#)

[CEO acknowledges impact of war, pandemic but says fundamentals 'are really good'](#)

[Dylan Martin](#) Fri 27 May 2022 // 16:08 UTC 

Nvidia is expecting a \$500 million hit to its global datacenter and consumer business in the second quarter due to COVID lockdowns in China and Russia's invasion of Ukraine. Despite those and other macroeconomic concerns, executives are still optimistic about future prospects.

"The full impact and duration of the war in Ukraine and COVID lockdowns in China is difficult to predict. However, the impact of our technology and our market opportunities remain unchanged," said Jensen Huang, Nvidia's CEO and co-founder, during the company's first-quarter earnings call.

Those two statements might sound a little contradictory, including to some investors, particularly following the [stock selloff](#) yesterday after concerns over Russia and China prompted Nvidia to issue lower-than-expected guidance for second-quarter revenue.

[Continue reading](#)

- [Another AI supercomputer from HPE: Champollion lands in France](#)

[That's the second in a week following similar system in Munich also aimed at researchers](#)

[Dan Robinson](#) Fri 27 May 2022 // 15:30 UTC 

HPE is lifting the lid on a new AI supercomputer – the second this week – aimed at building and training larger machine learning models to underpin research.

Based at HPE's Center of Excellence in Grenoble, France, the new supercomputer is to be named Champollion after the French scholar who made advances in deciphering Egyptian hieroglyphs in the 19th century. It was built in partnership with Nvidia using AMD-based Apollo computer nodes fitted with Nvidia's A100 GPUs.

Champollion brings together HPC and purpose-built AI technologies to train machine learning models at scale and unlock results faster, HPE said. HPE already provides HPC and AI resources from its Grenoble facilities for customers, and the broader research community to access, and said it plans to provide access to Champollion for scientists and engineers globally to accelerate testing of their AI models and research.

[Continue reading](#)

- [Workday nearly doubles losses as waves of deals pushed back](#)

[Figures disappoint analysts as SaaS HR and finance application vendor navigates economic uncertainty](#)

[Lindsay Clark](#) Fri 27 May 2022 // 14:30 UTC 9 

HR and finance application vendor Workday's CEO, Aneel Bhusri, confirmed deal wins expected for the three-month period ending April 30 were being pushed back until later in 2022.

The SaaS company boss was speaking as Workday recorded an operating loss of \$72.8 million in its first quarter [[PDF](#)] of fiscal '23, nearly double the \$38.3 million loss recorded for the same period a year earlier. Workday also saw revenue increase to \$1.43 billion in the period, up 22 percent year-on-year.

However, the company increased its revenue guidance for the full financial year. It said revenues would be between \$5.537 billion and \$5.557 billion, an increase of 22 percent on earlier estimates.

[Continue reading](#)

- [UK monopoly watchdog investigates Google's online advertising business](#)

[Another probe? Mountain View is starting to look like a pincushion at this rate](#)

[Richard Currie](#) Fri 27 May 2022 // 14:00 UTC 3 

The UK's Competition and Markets Authority is lining up yet another investigation into Google over its dominance of the digital advertising market.

This latest inquiry, [announced Thursday](#), is the second major UK antitrust investigation into Google this year alone. In March this year the UK, together with the European Union, said it wished to examine Google's "[Jedi Blue](#)" [agreement](#) with Meta to allegedly favor the former's Open Bidding ads platform.

The news also follows [proposals](#) last week by a bipartisan group of US lawmakers to create legislation that could force Alphabet's Google, Meta's Facebook, and Amazon to divest portions of their ad businesses.

[Continue reading](#)

- [Microsoft slows some hiring for Windows, Teams, and Office](#)

['Making sure the right resources are aligned to the right opportunity' ahead of next fiscal year](#)

[Richard Speed](#) Fri 27 May 2022 // 13:31 UTC 5 

Microsoft has hit the brakes on hiring in some key product areas as the company prepares for the next fiscal year and all that might bring.

According to reports in the [Bloomberg](#), the unit that develops Windows, Office, and Teams is affected and while headcount remains expected to grow, new hires in that division must first be approved by bosses.

During a talk this week at JP Morgan's Technology, Media and Communications Conference, Rajesh Jha, executive VP for the Office Product Group, noted that within three years he expected approximately two-thirds of CIOs to standardize on Microsoft Teams. 1.4 billion PCs were running Windows. He also remarked: "We have lots of room here to grow the seats with Office 365."

[Continue reading](#)

- [Recession fears only stoking enterprise tech spending for Dell, others](#)

[Staving off entropy with digital transformation, hybrid office, and automation projects](#)

[Paul Kunert](#) Fri 27 May 2022 // 13:00 UTC 

Enterprises are still kitting out their workforce with the latest computers and refreshing their datacenter hardware despite a growing number of "uncertainties" in the world.

This is according to hardware tech bellwethers including Dell, which turned over \$26.1 billion in sales for its [Q1 of fiscal 2023 ended 29 April](#), a year-on-year increase of 16 percent.

"We are seeing a shift in spend from consumer and PCs to datacenter infrastructure," said Jeff Clarke, vice-chairman and co-chief operating officer. "IT demand is currently healthy," he added.

[Continue reading](#)