Cisco's Talos team has developed an open-source tool that can protect the master boot record of Windows computers from modification by ransomware and other malicious attacks.

The tool, called MBRFilter, functions as a signed system driver and puts the disk's sector 0 into a read-only state. It is available for both 32-bit and 64-bit Windows versions and its source code has been published on GitHub.

The master boot record (MBR) consists of executable code that's stored in the first sector (sector 0) of a hard disk drive and launches the operating system's boot loader. The MBR also contains information about the disk's partitions and their file systems.

Since the MBR code is executed before the OS itself, it can be abused by malware programs to increase their persistence and gain a head start before antivirus programs. Malware programs that infect the MBR to hide from antivirus programs have historically been known as bootkits -- boot-level rootkits.

Microsoft attempted to solve the bootkit problem by implementing cryptographic verification of the bootloader in Windows 8 and later. This feature is known as Secure Boot and is based on the Unified Extensible Firmware Interface (UEFI) -- the modern BIOS.
host, and was brought under control at 9:36 a.m. According to Gizmodo, which was the first to report the story, at least 40 sites were made unreachable to users on the US East Coast. Many of the sites affected are among the most trafficked on the web, and included CNN, Twitter, PayPal, Pinterest and Reddit to name a few. The developer community was also touched, as GitHub was also made unreachable.

This event comes on the heels of a record breaking 620 Gbps DDOS attack about a month ago that brought down security expert Brian Krebs’ website, KrebsonSecurity. In that attack, Krebs determined the attack had been launched by botnets that primarily utilized compromised IoT devices, and was seen by some as ushering in a new era of Internet security woes.

This Is Why Half the Internet Shut Down Today [Update: It?s Getting Worse] [5]

Twitter, Spotify and Reddit, and a huge swath of other websites were down or screwed up this morning. This was happening as hackers unleashed a large distributed denial of service (DDoS) attack on the servers of Dyn, a major DNS host. It?s probably safe to assume that the two situations are related.

Major DNS provider Dyn hit with DDoS attack [6]

Attacks against DNS provider Dyn continued into Friday afternoon. Shortly before noon, the company said it began "monitoring and mitigating a DDoS attack" against its Dyn Managed DNS infrastructure. The attack may also have impacted Managed DNS advanced service "with possible delays in monitoring."

What We Know About Friday?s Massive East Coast Internet Outage [7]

Friday morning is prime time for some casual news reading, tweeting, and general Internet browsing, but you may have had some trouble accessing your usual sites and services this morning and throughout the day, from Spotify and Reddit to the New York Times and even good ol? WIRED.com. For that, you can thank a distributed denial of service attack (DDoS) that took down a big chunk of the Internet for most of the Eastern seaboard.

This morning?s attack started around 7 am ET and was aimed at Dyn, an Internet infrastructure company headquartered in New Hampshire. That first bout was resolved after about two hours; a second attack began just before noon. Dyn reported a third wave of attacks a little after 4 pm ET. In all cases, traffic to Dyn?s Internet directory servers throughout the US?primarily on the East Coast but later on the opposite end of the country as well?was stopped by a flood of malicious requests from tens of millions of IP addresses disrupting the
system. Late in the day, Dyn described the events as a very sophisticated and complex attack. Still ongoing, the situation is a definite reminder of the fragility of the web, and the power of the forces that aim to disrupt it.

**Either IoT will be secure or the internet will be crippled forever** [8]

First things first a disclaimer. I neither like nor trust the National Security Agency (NSA). I believe them to be mainly engaged in economic spying for the corporate American empire. Glenn Greenwald has clearly proven that in his book No Place to Hide. At the NSA, profit and power come first and I have no fucking clue as to how high they prioritize national security. Having said that, the NSA should hack the Internet of (insecure) Things (IoT) to death. I know Homeland Security and the FBI are investigating where the DDoS of doomsday proportions is coming from and the commentariat is already screaming RUSSIA! But it is really no secret what is enabling this clusterfuck. It?s the Mirai botnet. If you buy a ?smart camera? from the Chinese company Hangzhou XiongMai Technologies and do not change the default password, it will be part of a botnet five minutes after you connect it to the internet. We were promised a future where we would have flying cars but we?re living in a future where camera?s, light-bulbs, doorbells and fridges can get you in serious trouble because your home appliances are breaking the law.

**IoT at the Network Edge** [9]

Fog computing, also known as fog networking, is a decentralized computing infrastructure. Computing resources and application services are distributed in logical, efficient places at any points along the connection from the data source (endpoint) to the cloud. The concept is to process data locally and then use the network for communicating with other resources for further processing and analysis. Data could be sent to a data center or a cloud service. A worthwhile reference published by Cisco is the white paper, "Fog Computing and the Internet of Things: Extend the Cloud to Where the Things Are."

**Canonical now offers live kernel patching for Ubuntu 16.04 LTS users** [10]

Canonical has announced its ?Livepatch Service? which any user can enable on their current installations to eliminate the need for rebooting their machine after installing an update for the Linux kernel. With the release of Linux 4.0, users have been able to update their kernel packages without rebooting, however, Ubuntu will be the first distribution to offer this feature for free.
Dirty Cow is a silly name, but it's a serious Linux kernel problem. According to the Red Hat bug report, "a race condition was found in the way the Linux kernel's memory subsystem handled the copy-on-write (COW) breakage of private read-only memory mappings. An unprivileged local user could use this flaw to gain write access to otherwise read-only memory mappings and thus increase their privileges on the system."

---

**Ancient Privilege Escalation Bug Haunts Linux**

**October 21, 2016 Is Dirty COW a serious concern for Linux?**

**There is a Dirty Cow in Linux**

**Red Hat Discovers Dirty COW Archaic Linux Kernel Flaw Exploited In The Wild**

**Linux kernel bug being exploited in the wild**

**Update Linux now: Critical privilege escalation security flaw gives hackers full root access**

**Linux kernel bug: DirtyCOW ?easyroot? hole and what you need to know**

**'Most serious' Linux privilege-escalation bug ever discovered**

**New 'Dirty Cow' vulnerability threatens Linux systems**
Malware authors are taking aim at Linux computers, more precisely desktops and not servers, with a new trojan named FakeFile, currently distributed in live attacks.

Russian antivirus vendor Dr.Web discovered this new trojan in October. The company's malware analysts say the trojan is spread in the form of an archived PDF, Microsoft Office, or OpenOffice file.