

Forum:[Hack Forums](#)

Thread: [{Hacks, Scams, and Exploits} - #3 - Internet Census 2012](#)

Pr0m3th3us - July 3, 2026, 11:45 am

Preface

Most botnets exist to steal, extort, or destroy. This one was different. In 2012, an anonymous "hacker"...no name, no handle, no country of origin, nothing...built one of the largest botnets ever assembled, commandeered hundreds of thousands of devices across the globe, and ran the most comprehensive scan of the entire internet ever attempted. Then published the results for free, and vanished. Poof. No ransom. No stolen data. No victims in any conventional sense. Just a 568 gigabyte dataset, a research paper posted to a security mailing list, and a lot of questions about what it means when someone does something clearly illegal for what appears to be genuine plain old curiosity.

The Exploits

This story starts with a simple observation that any halfway curious person poking around with network tools could have made in 2012. An enormous number of internet-connected devices such as routers, modems, set-top boxes, embedded systems, etc...were sitting on the open internet with their Telnet port exposed and their login credentials set to factory defaults. We're talking combinations like root/root, admin/admin, admin/password or just no password at all. The creator of what they would later name the "Internet Census 2012" developed a binary that was uploaded to insecure devices found during an initial scan. Which included a Telnet scanner that would fire different default login combinations at devices such as root/root or admin/admin, or would attempt to access devices without a password at all. The hackers own write-up described finding a device with default credentials in fifty seconds flat. Not fifty minutes. Fifty seconds....

So rather than report the vulnerability and move on, the hacker had a different idea entirely. If these devices were already sitting wide open, why not use them to answer a question nobody had ever properly answered, what does the entire internet actually look like? And so the Carna botnet was born. It was a botnet of 420,000 devices, named after Carna, the Roman goddess of physical health, vitality, and the well-being of the human body. The name itself is telling, the hacker framed the project as a kind of "diagnostic", a health check on the body of the internet hilariously enough. The binary uploaded to each compromised device was lightweight and non-destructive. It didn't steal data, didn't spy on users, didn't install persistent malware. It just scanned, reported back, and kept looking for more open devices to recruit. The botnet operated without data exfiltration, denial-of-service attacks, or other harmful payloads, focusing solely on scanning activities using Nmap-based tools to probe for active hosts, open ports, and services, remaining active from March to December 2012 and generating billions of probes including 52 billion ICMP pings and 71 billion TCP SYN scans across 660 million IP addresses.

The craziest part...the identity of the hacker remains completely unknown to this day. No nationality, no sex, no handle, no affiliation. The only contact point they left was a PGP key embedded in the published report. Parth Shukla, an information security analyst with Australia's Computer Emergency Response Team (AusCERT), decided to email the hacker via that PGP key after the report was published in March 2013. He was surprised when the hacker actually responded, and ultimately handed over all the data on the more than 1.2 million vulnerable devices found around the globe. "No one else had been in touch with him," Shukla said, he was the only person the hacker

chose to share the full dataset with. That detail is remarkable on its own, the hacker had built something unprecedented, published it publicly, and apparently just waited to see if anyone would reach out.

The dataset itself was staggering in scope. The Internet Census 2012 revealed that approximately 1.3 billion IPv4 addresses were in use as of 2012, comprising 420 million directly pingable hosts and an additional 729 million addresses identifiable only through reverse DNS records. Around 70 million devices responded on port 80 (HTTP), many of which were embedded systems such as routers and set-top boxes. The hacker also published the data as [an animated GIF](#), a 24-hour time-lapse portrait of the entire internet lighting up and dimming as different parts of the world came online and went to sleep. It became one of the most striking visualizations of the internet ever produced. The hacker noted in their write-up that 2012 may have been the last possible moment to do this kind of IPv4 census, as the growing adoption of IPv6 would eventually make a complete scan of all addresses computationally impossible. They had caught the internet at a specific moment in time, and they knew it.

As for charges and prosecution, obviously as you can tell by now, none of it ever happened. The Internet Census 2012 was described in academic literature as a non-peer-reviewed paper by an anonymous hacker about an illegally-conducted survey of insecure machines. They still to this day have never come forward, and as far as the public record shows, has never been identified. The legal exposure was real, unauthorized access to hundreds of thousands of devices across multiple jurisdictions is a serious matter regardless of intent, but without knowing who did it, there was no case to bring. They did what they came to do, published it, handed the data to one person who asked for it, and disappeared.

Impact

In a strictly legal sense, the owners of those 420,000 compromised devices were victims, code was uploaded to their hardware without their knowledge or consent. In practice, most of them never knew it happened, and the hacker went out of their way to minimize any burden. The Carna botnet creator made some effort to reduce the burden imposed on devices by limiting the number of simultaneous connections the scanner could make, avoiding probing further into networks beyond insecure routers, and even removing other malware found on devices if it interfered with Carna's scans. That last point is genuinely strange, the hacker was cleaning up other people's infections while conducting their own unauthorized operation. It does nothing to make it legal, but it does paint an odd picture of someone who actually cared about not causing harm.

The harder impact was on the security research community itself, which was forced into an uncomfortable debate it hadn't fully had before. Legal issues came up immediately. The Internet Census Carna botnet data was illegally obtained as the hacker infected machines around the world without permission. AusCERT's legal team ultimately concluded that Shukla had not asked the hacker to conduct the illegal research and was therefore not a party to the crime. But there were clear ethical considerations about using data that was violating the rights of so many device owners. Shukla's position was that since he was the only one with the full dataset, it was imperative to do something with it to spread awareness of just how serious the underlying vulnerability was. That reasoning...the data exists, it reveals a real problem, therefore using it is justified...became a live debate in academic and security circles that continues to this day. Critics argued that the societal benefits of revealing the information did not outweigh the harm caused, noting that the Internet Census 2012 only supplied evidence of the scale of an existing and well-known problem rather than revealing a previously unknown one.

The findings themselves also made the scale of the default-credential problem impossible to ignore. The realization that there were potentially millions of vulnerable enterprise network devices, industrial control systems, and home networking gear sitting open on the internet needed patching

was impossible to dismiss. Security researchers, ISPs, and device manufacturers all had to reckon with findings that put hard numbers on something the industry had been hand-waving about for years.

What Changed

The most direct legacy of the Carna botnet isn't what it did, it's what it predicted. The same attack surface it documented in 2012, the ocean of embedded Linux devices sitting open on Telnet with default credentials, became the exact foundation that the Mirai botnet was built on four years later. The Carna botnet project provided insight into what was running on the internet in 2012, and the same anonymous hacker who hijacked home routers using weak default credentials and installed software on those devices demonstrated exactly the technique that Mirai would later weaponize at catastrophic scale. The difference was that Mirai's creators had no interest in internet cartography, they used the same access to launch some of the most powerful DDoS attacks ever recorded, taking down major DNS infrastructure and knocking large portions of the internet offline in 2016. Carna was the proof of concept. Mirai was the weapon.

In terms of direct policy change, the Carna project contributed to a growing push by regulators and device manufacturers to eliminate default credentials entirely. The UK became one of the first countries to legally ban default passwords on consumer IoT devices, with the Product Security and Telecommunications Infrastructure Act coming into force in 2024, over a decade after Carna documented why it mattered. The US followed with similar IoT security labeling requirements. These changes were slow and incremental, driven by a long accumulation of incidents, but Carna was an early and unusually dramatic data point in that argument. The observation the hacker made about a growing number of IPv6 hosts on the internet, and 2012 being the last time a census of this kind was possible turned out to be correct, the internet has since become too large and too fragmented across IPv4 and IPv6 to ever map the same way again. The hacker knew they were capturing something unrepeatable, and they were right.

Sources

Darknet Diaries Ep. 13 — Carna Botnet: <https://darknetdiaries.com/episode/13/>

Original Internet Census 2012 Paper (Internet Archive):

https://archive.org/details/Carna_Internet_Census

Threatpost — Carna Botnet Analysis Enumerates Vulnerable Devices:

<https://threatpost.com/carna-botnet-analysis-renders-scary-numbers-on-vulnerable-devices/100813/>

Threatpost — Exposed Devices Used as Botnet to Scan Internet (2013):

<https://threatpost.com/exposed-devices-used-botnet-scan-internet-032013/77644/>

Dark Reading — From Carna to Mirai: Recovering From a Lost Opportunity:

<https://www.darkreading.com/endpoint-security/from-carna-to-mirai-recovering-from-a-lost-opportunity>

Dark Reading — What the Carna Botnet Also Found:

<https://www.darkreading.com/vulnerabilities-threats/what-the-carna-botnet-also-found>

eWeek — Carna Botnet Exploit Unmasked:

<https://www.eweek.com/security/carna-botnet-exploit-unmasked-researcher-reveals-details/>

ResearchGate — The Internet Census 2012 Dataset: An Ethical Examination:

https://www.researchgate.net/publication/279069631_The_Internet_Census_2012_Dataset_An_Ethical_Examination

Groklopedia — Carna Botnet: https://groklopedia.com/page/Carna_botnet

Full disclosure: I used Claude to help me locate sources to go over, I read the articles, I listened and re-listened to "Darknet Diaries" podcast while doing this write-up, as he was an inspiration. I used Claude to go over my write-up for grammar errors, punctuation (im really bad about using

apostrophes), and cleaning up the overall writing but keeping my writing style instead of changing it so much i couldn't recognize it. I also told it to point out if i made errors in reporting in my write up. ChatGPT was used for the Image.

InspectorGadget - July 4, 2026, 11:34 am

We really didn't know how well we had it in the early 2000's and 2010's... Every cyber security approach was simply 'whatever is easiest'.

Raijin - July 5, 2026, 12:55 pm

Thanks for this, I had never heard about it.