WHEN ABANDONED INFRASTRUCTURE LIVES ON —

Rogue WHOIS server gives researcher superpowers no one should ever have

.mobi top-level-domain managers changed the location of its WHOIS server. No one got the memo.

DAN GOODIN - 9/11/2024, 12:00 PM

Aurich Lawson | Getty Images

Enlarge

It's not every day that a security researcher acquires the ability to generate counterfeit HTTPS certificates, track email activity, and the position to execute code of his choice on thousands of servers—all in a single blow that cost only $20 and a few minutes to land. But that's exactly what happened recently to Benjamin Harris.

Harris, the CEO and founder of security firm watchTowr, did all of this by registering the domain dotmobiregistry.net. The domain was once the official home of the authoritative WHOIS server for .mobi, a top-level domain used to indicate that a website is optimized for mobile devices. At some point—it's not clear precisely when—this WHOIS server, which acts as the official directory for every domain ending in .mobi, was relocated, from whois.dotmobiregistry.net to whois.nic.mobi. While retreating to his Las Vegas hotel room during last month's Black Hat security conference in Las Vegas, Harris noticed that the previous dotmobiregistry.net owners had allowed the domain to expire. He then scooped it up and set up his own .mobi WHOIS server there.

Misplaced trust

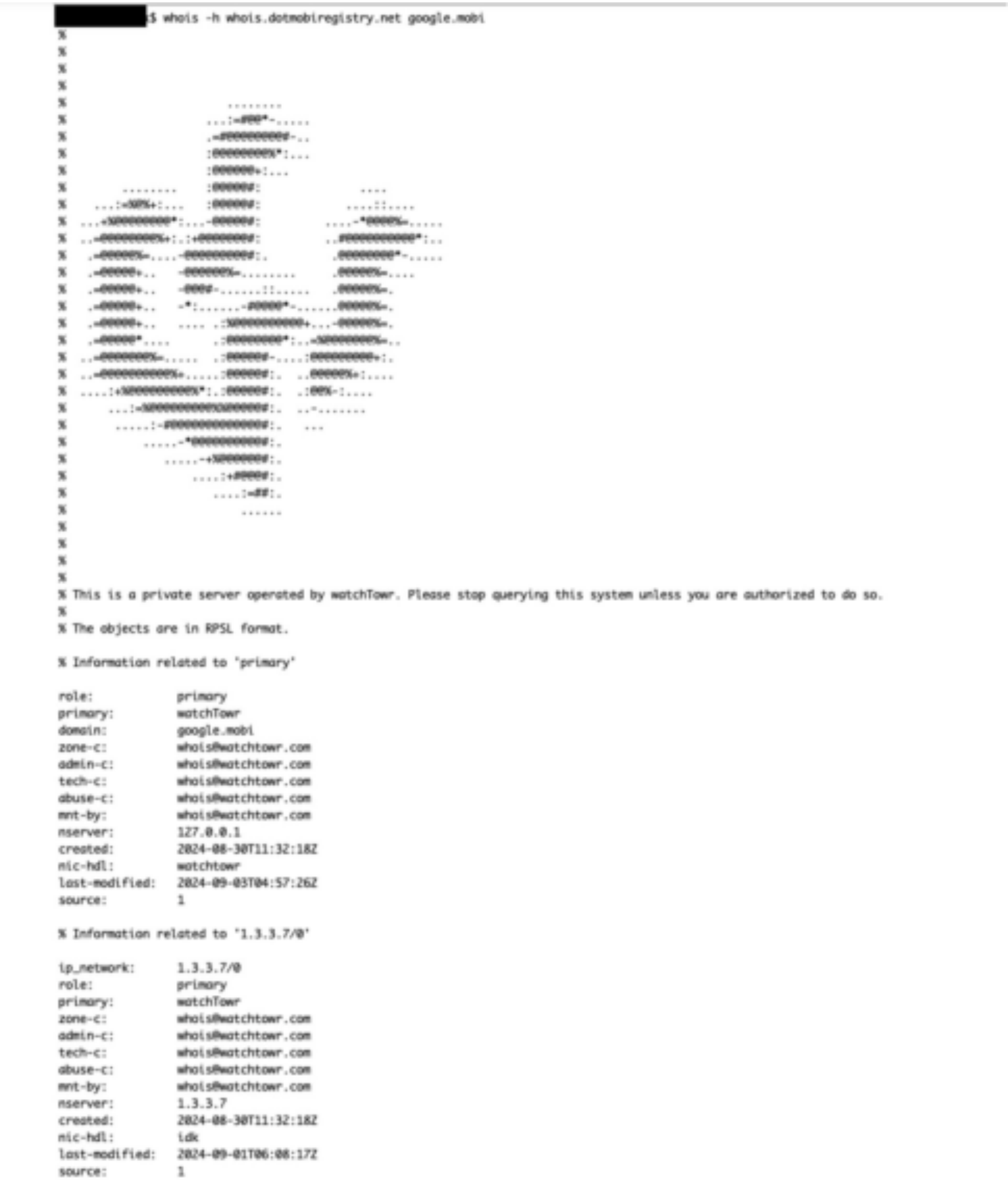
To Harris's surprise, his server received queries from slightly more than 76,000 unique IP addresses within a few hours of setting it up. Over five days, it received roughly 2.5 million queries from about 135,000 unique systems. The entities behind the systems querying his deprecated domain included a who's who of Internet heavyweights comprising domain registrars, providers of online security tools, governments from the US and around the world, universities, and certificate authorities, the entities that issue browser-trusted TLS certificates that make HTTPS work.

"watchTowr's research has demonstrated that trust placed in this process by governments and authorities worldwide should be considered misplaced at this stage, in [our] opinion," Harris wrote in a post documenting his research. "watchTowr continues to hold concern around the basic reality: watchTowr found this on a whim in a hotel room while escaping the Vegas heat surrounding Black Hat, while well-resourced and focused nation-states look for loopholes like this every day. In watchTowr's opinion, they are not likely to be the last to find inexcusable flaws in such a crucial process."

WHOIS has played a key role in Internet governance since its earliest days, back when it was still called the ARPANET. Elizabeth Feinler, an information scientist working for the Augmentation Research Center, became the principal investigator for NIC, short for the Network Information Center project, in 1974. Under Feinler's watch, NIC developed the top-level domain naming system and the official host table and published the ARPANET Directory, which acted as a directory of phone numbers and email addresses of all network users. Eventually, the directory evolved into the WHOIS system, a query-based server that provided a comprehensive list of all Internet host names and the entities that had registered them.

Despite its antiquated look and feel, WHOIS today remains an essential resource with tremendous consequences. Lawyers pursuing copyright or defamation claims use it to determine the owner of a domain or IP address. Anti-spam services depend on it to determine the true owner of email servers. Certificate authorities rely on it to determine the official administrative email address of a domain. The list goes on.

Harris populated his WHOIS database with junk data that corresponded to all real .mobi addresses. Administrative email addresses, and most other fields led to the watchtowr.com domain. For humor, he also added ASCII art. The WHOIS entry for google.mobi, for instance, looks like this:



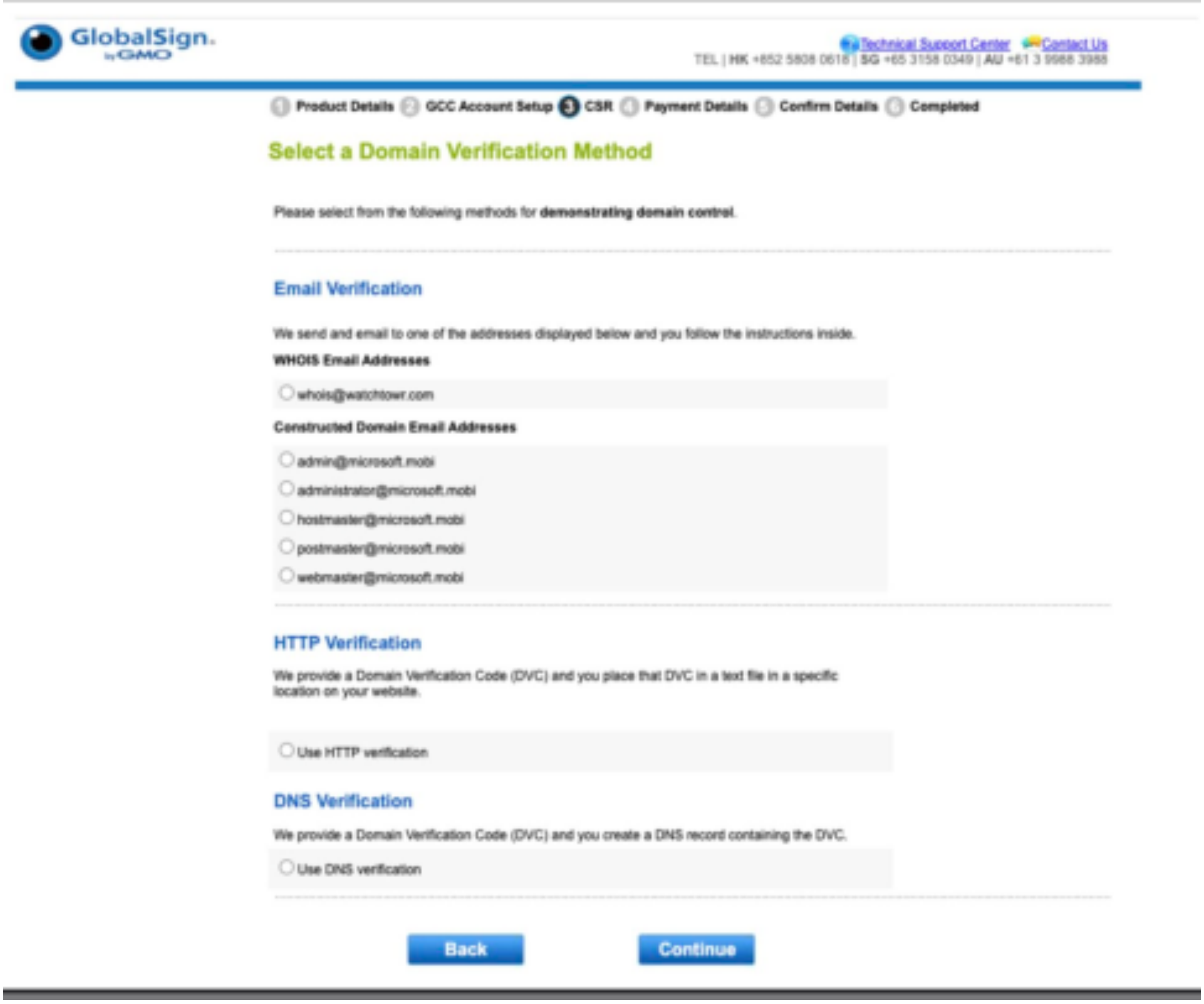
```
[redacted]$ whois -h whois.dotmobiregistry.net google.mobi
%
%
%
%
%                      .........
%                   ...:=##@*-.....
%                   .=@@@@@@@@@@#-..
%                   :@@@@@@@@@%*:...
%                   :@@@@@@@+:...
%       .........   :@@@@@@#:                   ....
%    ...:=%@%+:...  :@@@@@@#:                 .....::.....
%  ...+%@@@@@@@@@*:...-@@@@@@#:            ....-*@@@@%=.....
%  ..=@@@@@@@@@%+:.:+@@@@@@@@#:            ..#@@@@@@@@@@@@*:..
%   .=@@@@@@%=....-@@@@@@@@@@@#:.           .@@@@@@@@@*-.....
%   .=@@@@@@+..   -@@@@@@@%=........        .@@@@@@%=....
%   .=@@@@@@+..   -@@@#-......::......      .@@@@@@%=.
%   .=@@@@@@+..   -*:......-#@@@@@*-......@@@@@@%=.
%   .=@@@@@@+..   .... .:%@@@@@@@@@@@@+...-@@@@@@%=.
%   .=@@@@@@*....      .:@@@@@@@@@@*:..=%@@@@@@@@%=..
%  ..=@@@@@@@@%=.....  .:@@@@@@#-....:@@@@@@@@@@@+:.
%  ..=@@@@@@@@@@@@%+.....:@@@@@@#:.   ..@@@@@@%+:....
%  .....:+%@@@@@@@@@@@%*:..:@@@@@@#:.   .:@@%-:....
%      ...:=%@@@@@@@@@@%%@@@@@@@#:.   ..-.......
%       .....:-#@@@@@@@@@@@@@@@#:.    ...
%           .....-*@@@@@@@@@@@@#:.
%              .....-+%@@@@@@@#:.
%                  ....:+#@@@@#:.
%                     ....:=##:.
%                         ......
%
%
%
%
% This is a private server operated by watchTowr. Please stop querying this system unless you are authorized to do so.
%
% The objects are in RPSL format.

% Information related to 'primary'

role:           primary
primary:        watchTowr
domain:         google.mobi
zone-c:         whois@watchtowr.com
admin-c:        whois@watchtowr.com
tech-c:         whois@watchtowr.com
abuse-c:        whois@watchtowr.com
mnt-by:         whois@watchtowr.com
nserver:        127.0.0.1
created:        2024-08-30T11:32:18Z
nic-hdl:        watchtowr
last-modified:  2024-09-03T04:57:26Z
source:         1

% Information related to '1.3.3.7/0'

ip_network:     1.3.3.7/0
role:           primary
primary:        watchTowr
zone-c:         whois@watchtowr.com
admin-c:        whois@watchtowr.com
tech-c:         whois@watchtowr.com
abuse-c:        whois@watchtowr.com
mnt-by:         whois@watchtowr.com
nserver:        1.3.3.7
created:        2024-08-30T11:32:18Z
nic-hdl:        idk
last-modified:  2024-09-01T06:08:17Z
source:         1
```

watchTowr

Enlarge / **WHOIS information for google.mobi as shown by a rogue server at whois.dotmobiregistry.net**

The humor aside, the rogue WHOIS server gave him powers he never should have had. One of the greatest was the ability to dictate the email address certificate authority GlobalSign used to determine if a party applying for a TLS certificate was the rightful owner of the domain name the certificate would apply to. Like the vast majority of its competitors, GlobalSign uses an automated process. An application for example.com, for instance, will prompt the certificate authority to send an email to the administrative email address listed in the authoritative WHOIS for that domain. If the party on the other end clicks a link, the certificate is automatically approved.

When Harris generated a certificate signing request for microsoft.mobi, he promptly received an email from GlobalSign. The email gave him the option of receiving a verification link at whois@watchtowr.com. For ethical reasons, he stopped the experiment at this point.



TEL | HK +852 5808 0618 | SG +65 3158 0349 | AU +61 3 9988 3988

Select a Domain Verification Method

Please select from the following methods for **demonstrating domain control**.

Email Verification

We send and email to one of the addresses displayed below and you follow the instructions inside.

WHOIS Email Addresses

○ whois@watchtowr.com

Constructed Domain Email Addresses

○ admin@microsoft.mobi
○ administrator@microsoft.mobi
○ hostmaster@microsoft.mobi
○ postmaster@microsoft.mobi
○ webmaster@microsoft.mobi

HTTP Verification

We provide a Domain Verification Code (DVC) and you place that DVC in a text file in a specific location on your website.

○ Use HTTP verification

DNS Verification

We provide a Domain Verification Code (DVC) and you create a DNS record containing the DVC.

○ Use DNS verification

watchTowr

Enlarge / An email Harris received from GlobalSign after generating a certificate signing request for microsoft.mobi.

“Now that we have the ability to issue a TLS/SSL cert for a .mobi domain, we can, in theory, do all sorts of horrible things—ranging from intercepting traffic to impersonating the target server,” Harris wrote. “It’s game over for all sorts of threat models at this point. While we are sure some may say we didn’t ‘prove’ we could obtain the certificate, we feel this would’ve been a step too far—so whatever.”

The nefarious things Harris can do with his rogue WHOIS server aren't limited to obtaining counterfeit certificates. Many email servers and anti-spam services, including those used by government, military, and large organizations, queried his dotmobiregistry.net domain each time they received an email from a .mobi domain. The ability to track email chains over sustained periods of time could give him the ability to passively infer the parties involved in sending and receiving the communications.

Various WHOIS clients and security services also contain vulnerabilities, some of which make it possible for an attacker to execute malicious code on the querying device. Normally, exploits of these sorts of vulnerabilities would be considered unlikely because only a trusted WHOIS server would be in a position to capitalize on them. A rogue server like the one Harris created, however, would be under no such constraints.

A painful and reoccurring issue

"The purchase of a $20 domain that allowed the passive inference of .gov/.mil communications and the subversion of the Certificate Authority verification system should be a clear demonstration that the integrity of the trust and security processes we as Internet users rely on is, and continues to be, extremely fragile," Harris wrote in an online interview. "The systems and security we all take for granted is, in many places, truly held together in ways that would not pass approval in 2024."

Dozens of third-party sites and services also queried the rogue server as recently as Monday afternoon. A small sample: Google's VirusTotal; website analysis service URLScan; domain registrars domain.com, godaddy.com, and name.com; and WHOIS websites who.is, whois.ru, smallseo.tools, seocheki.net, centralops.net, and webchart.or.

Harris said that watchTowr has since engaged with National Counterintelligence and Security Center and security organization ShadowServer to take custody of the dotmobiregistry.net domain. He expects they will safeguard it to ensure that systems that continue to speak to this WHOIS server do not continue to be exposed to the threat.

After receiving a request for comment on Monday, a representative at GlobalSign said the company has initiated an investigation. A Google representative said that as an aggregator of tools, antivirus engines, security scanners, and other utilities, VirusTotal "may occasionally generate false positives, false negatives, or errors." VirusTotal aggregates WHOIS responses from WhoisDS and the WHOIS client included in Linux. Once those sources query the correct WHOIS server for .mobi addresses, VirusTotal will, too, the representative said.

While the Linux client appears to have recently started querying the correct .mobi WHOIS server, most other resources have not, as evidenced by the constant stream of queries that continue to pour into his rogue server as recently as Tuesday.

"The reality that this interconnected 'network' of WHOIS servers comes from a time where things were only hardcoded into numerous WHOIS clients, [meaning] that unfortunately, this won't be cleared up overnight," Harris told Ars.

It’s unclear if WHOIS lookups for other top-level domains suffer similar threats. In any event, the problem is that there’s no uniform naming convention for authoritative WHOIS servers or even, for that matter, a clear way to look them up. While some third parties have compiled lists of what they say are authoritative WHOIS servers, many of them erroneously list the now-deprecated dotmobiregistry.net as the authoritative WHOIS server for .mobi.

What's more, Harris said, the problem he has unearthed isn't restricted to retired domains. S3 buckets and other cloud infrastructure can also create threats when they're discarded and websites, deployment scripts, or other resources continue to reference them.

“The reality is that this issue exists in various forms (whether it be people using personal domains that they leave to expire, subsequently being registered by another individual who then subsequently has access to all accounts of the previous owner,” Harris told Ars. “We are of the opinion that this will continue to be a painful issue that reoccurs as we see the recycling of infrastructure/domains/etc.”

READER COMMENTS 95

DAN GOODIN
Dan Goodin is Senior Security Editor at Ars Technica, where he oversees coverage of malware, computer espionage, botnets, hardware hacking, encryption, and passwords. In his spare time, he enjoys gardening, cooking, and following the independent music scene. Dan is based in San Francisco. Follow him at @dangoodin on Mastodon. Contact him on Signal at DanArs.82.

WATCH

Unsolved Mysteries Of Quantum Leap With...

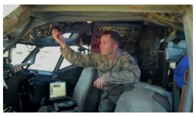
Unsolved Mysteries Of Quantum Leap With Donald P. Bellisario

Today "Quantum Leap" series creator Donald P. Bellisario joins Ars Technica to answer once and for all the lingering questions we have about his enduringly popular show. Was Dr. Sam Beckett really leaping between all those time periods and people or did he simply imagine it all? What do people in the waiting room do while Sam is in their bodies? What happens to Sam's loyal ally Al? 30 years following the series finale, answers to these mysteries and more await.

Unsolved Mysteries Of Quantum Leap With Donald P. Bellisario

Unsolved Mysteries Of Warhammer 40K With Author Dan Abnett

SITREP: F-16 replacement search a signal of F-35 fail?



Sitrep: Boeing 707

More videos

← PREVIOUS STORY

NEXT STORY →

Related Stories

Cloudflare gets into registrar business with wholesale domains and free privacy

Cloudflare aims to make HTTPS certificates safe from BGP hijacking attacks

Epic Google snafu leaks hidden whois data for 280,000 domains

Encrypt all the webpages: Let’s Encrypt to offer wildcard certificates for free

Today on Ars

Rocket Report: China leaps into rocket reuse; 19 people are currently in orbit

CEO of "health care terrorists" faces contempt charges after Senate no-show

Meet the winners of the 2024 Ig Nobel Prizes

Court clears researchers of defamation for identifying manipulated data

Unity is dropping its unpopular per-install Runtime Fee

OpenAI's new "reasoning" AI models are here: o1-preview and o1-mini

Unicode 16.0 release with new emoji brings character count to 154,998

Music industry's 1990s hard drives, like all HDDs, are dying

STORE
SUBSCRIBE
ABOUT US
RSS FEEDS

CONTACT US
STAFF
ADVERTISE WITH US
REPRINTS

NEWSLETTER SIGNUP

Join the Ars Orbital Transmission mailing list to get weekly updates delivered to your inbox. Sign me up →

VIEW MOBILE SITE

CNMN Collection
WIRED Media Group

Your California Privacy Rights | ✓✕ Manage Preferences

Ad Choices