Widespread DNS Hijacking Activity Targets Multiple Sectors

crowdstrike.com/blog/widespread-dns-hijacking-activity-targets-multiple-sectors/

January 25, 2019

January 25, 2019

Matt Dahl Research & Threat Intel

CrowdStrike® Intelligence™ has been researching reports of widespread DNS hijacking activity since information on the attacks became publicly available earlier this month.[1] The information allowed for the discovery of at least a subset of domains affected by this campaign. CrowdStrike can confirm that numerous organizations in sectors such as government, insurance, and civilian aviation, as well as internet service providers (ISPs) and infrastructure providers, were affected going back as far as February 2017.

The ultimate objective of this activity is currently unclear. However, DNS hijacking attacks would allow the responsible actors to capture the contents of web traffic to affected domains, during the time periods in which they were hijacked, and potentially use the captured data in follow-on operations. Given current information, CrowdStrike is unable to make adversary or country-level attribution of this activity.

Malicious Infrastructure and Identified Targets

Based on available information, CrowdStrike’s threat intelligence team has been able to identify 28 organizations in 12 different countries whose domains were hijacked. The organizations affected were primarily located in the Middle East and North Africa (MENA) region, but there was also a limited number of affected entities in Europe and the United States.

TIMELINE OF MALICIOUS INFRASTRUCTURE AND HIJACKED DOMAINS

Malicious IP Address	Active Time Period	Affected Organizations’ Country (Sector)
142.54.179[.]69	February 2017	Jordan (Government)
89.163.206[.]26	February 2017	Jordan (Government)
185.15.247[.]140	December 2017 and January 2018	Kuwait (Government) Albania (Government)
146.185.143[.]158	August 2018	UAE (Government)
128.199.50[.]175	September 2018	UAE (Unidentified Sector)
185.20.187[.]8	September 2018	UAE (Law Enforcement) UAE (Government) Lebanon (Government) Lebanon (Civil Aviation)
82.196.8[.]43	October 2018	Iraq (Government)

188.166.119[.]57	October 2018 and November 2018	Egypt (Government) Libya (Government)
206.221.184[.]133	November 2018	Egypt (Government)
37.139.11[.]155	November 2018	UAE (Unidentified Sector)
199.247.3[.]191	November 2018	Iraq (Government) Albania (Government)
185.161.209[.]147	November 2018	Lebanon (Insurance)
139.162.144[.]139	December 2018	Jordan (Government)
37.139.11[.]155	December 2018	UAE (Unidentified Sector)
178.62.218[.]244	December 2018	UAE (Government) Cyprus (Government)
139.59.134[.]216	December 2018	Sweden (Internet Infrastructure) Saudi Arabia (Internet Services) Lebanon (Internet Services)
82.196.11[.]127	December 2018	Sweden (Internet Infrastructure) U.S. (Internet Infrastructure)
46.101.250[.]202	December 2018 and January 2019	Saudi Arabia (Government)

Actor-owned Domains Used as Name Servers for Hijacked Infrastructure

cloudipnameserver[.]com
cloudnamedns[.]com
lcjcomputing[.]com
mmfasi[.]com
interaland[.]com

Once hijacked, targeted domains ceased resolving to their normal IP addresses and began resolving to actor-controlled infrastructure. The actors would also create certificates for the domains, primarily through Let’s Encrypt, a certificate authority that provides free X.509 certificates for TLS encryption. This would allow visitors to continue to establish trusted connections, despite the fact that they were pointing at malicious infrastructure. Available data shows that most affected domains were hijacked for very short periods of time, sometimes a day or less, with one domain showing resolutions to a malicious IP address for over a month.

Internet Infrastructure Providers Affected

Particularly notable are a small number of domains owned by significant ISPs or infrastructure providers. The affected ISP domains belonged to a private entity appearing to provide services to a wide range of customers in all sectors, while another affected entity provided services to government, research and academic organizations within its own country.

Two other affected organizations operate core functions of the internet globally, such as internet exchange points, root DNS servers and numerous top-level domains (TLDs). A compromise of internet infrastructure operators such as these could support data collection against a wide range of organizations.

Assessment

While the precise objectives behind this DNS hijacking activity are unclear, this tactic could be used by malicious actors to support a number of missions:

- Direct collection of data from web traffic to affected domains
- Collection of credentials from captured traffic for use in obtaining access to networks of future targets
- Delivery of malware from actor-owned infrastructure

This activity was likely meant to support intelligence collection operations against the entities whose domains were hijacked and possibly associated organizations likely to visit those sites. In addition, the activity targeting the ISPs and infrastructure providers could potentially have supported information collection against a range of currently unidentified targets.

Public reporting has indicated there are factors that point to a possible Iranian nexus for this activity. While the CrowdStrike Intelligence team agrees that the heavy focus on affected Middle Eastern governments would support the traditional intelligence collection interests of Iran, there is currently not enough information to make any definitive assessment around country or adversary-level attribution at this time.

Finally, it should be noted that given current information, it is unclear if this hijacking activity is linked to one or multiple actors. Considering the extended period of time over which this activity took place and the variance in malicious infrastructure, it is possible that multiple entities were involved in carrying out this DNS hijacking.

1. Information on related activity was also published in November 2018 in this blog: "DNSpionage Campaign Targets Middle East."

Additional Resources

- *For more information on how to incorporate intelligence on dangerous threat actors into your security strategy, please visit the CrowdStrike Falcon X Intelligence product page.*
- *Read Stories from the front lines of incident response and get insights that can help inform your security strategy for 2019 in the CrowdStrike Services Cyber Intrusion Casebook 2018.*
- *Download the CrowdStrike 2020 Global Threat Report.*
- *Test Falcon Prevent™ next-gen antivirus for yourself with a free 15-day trial.*

Related Content

Who is EMBER BEAR?

A Tale of Two Cookies: How to Pwn2Own the Cisco RV340 Router

PROPHET SPIDER Exploits Citrix ShareFile Remote Code Execution Vulnerability CVE-2021-22941 to Deliver Webshell