Advanced Notification of a DNS Hijacking Campaign Targeting the MENA region

aeCERT Computer Emergency Response Team
فريق الاستجابة لطوارئ الحاسب الآلي

Security Advisory	ADV-19-11	**Criticality**	Critical	
Advisory Released On	21st of April 2019			

Impact

The attacker's goal is to alter DNS records of the target. They will then launch a man in the middle attack diverting legitimate users' traffic through their own server. This enables them to steal credentials used by the victim which are then forwarded to the legitimate services, assisting the attacker in avoiding detection. These credentials may then be used to assist in further compromising systems/networks of interest.

Solution

Refer to the solution section.

Summary

As the leading trusted secure cyber coordination center in the region, aeCERT has researched and discovered a DNS hijacking campaign targeting national security organizations in the MENA region. The attack may be used to steal credentials and gain access to an organizations network. It works by redirecting legitimate DNS traffic to an attacker operated DNS server.

Threat Details

Our intelligence sources have helped us discover a new cyber threat campaign that utilizes DNS hijacking attacks, which seems to be targeting public and private entities in the MENA Region including national security organizations within the region. The campaign's activities date back to January 2017 and have been ongoing since then.

The goal of this attack is to gain access to networks and ultimately systems which may contain material of interest to the attackers. This is carried out by utilizing DNS hijacking. DNS hijacking is modifying DNS name records to point users to different servers controlled by the attackers, which enables them to perform a man in the middle attack and compromise user credentials.

The campaign is focused around two types of victims. The first type of victims which are the primary focus of this campaign are the national security organizations, ministries of foreign affairs and energy organizations within the MENA region. To reach those organizations however, the attacker focused on third-party service providers that are providing their services to these organizations in order to obtain access through them. The second type of victims are telecommunication companies, internet service providers (ISP's) and numerous DNS registrars. The attacker mainly targeted the second type of victims to gain access to the main targets.

Attack Methodology:

The attackers' goal when using DNS hijacking is to steal credentials and gain access to networks and important systems. In the campaign, the attackers had three main objectives to achieve their goal and they are:

1- Gain control of the DNS records of the target.
2- Modify the DNS record and misdirect it.
3- Obtain user credentials that the users input in the redirected server.

To give you a better understanding of how the attack happened, we will summarize it in nine steps.

1- The attacker gains access to the entity.
2- The attacker obtains credential through the network.
3- The attacker exfiltrates material out of the network.
4- The attacker gains access to the DNS registry via the stolen credentials (of someone with credentials to alter DNS records).
5- The attacker redirects the DNS records to their own servers.
6- The victims are redirected to the attacker's server when sending DNS requests.
7- The victims input their credentials into the redirected servers.
8- The attacker harvests the credentials.
9- The attacker can now gain access using the harvested credentials.

How the Attack Works:

To start off the attack, the attackers gain initial access by using various methods such as exploiting vulnerabilities or sending phishing emails.

The attacker would then modify the targeted organization's DNS records, which points the users to the attacker's malicious DNS servers. It has been observed that the DNS servers can be hijacked for a few minutes or even a couple of days.

During 2019, we observed the following name servers being used in the campaign:

Domain	Active Timeframe
ns1[.]intersecdns[.]com	March - April 2019
ns2[.]intersecdns[.]com	March - April 2019
ns1[.]lcjcomputing[.]com	January 2019
ns1[.]lcjcomputing[.]com	January 2019

The attacker would then setup their own server to act as a man-in-the-middle and capture user credentials. This works by directing the user to the man-in-the-middle server where the user would input their credentials, the attacker would then harvest those credentials and redirect the user to the legitimate server. This makes the attack very hard to detect.

The attackers also utilize SSL certificates to their advantage. Once they gained access to the victims' network, they managed to steal the organization's SSL certificate. This allows the attacker to gain broader access to the network and harvest additional credentials. Stealing the SSL certificates gives the attackers a large level of confidentiality.

All the techniques used by the attackers contributed to them acquiring user credentials and being persistent on the targeted networks.

IOC

Virtual Private Servers (VPS) used in the campaign:

IP address	Month	Year	Country of targets
199.247.3.191	November	2018	Albania, Iraq
37.139.11.115	November	2018	Albania, UAE
185.15.247.140	January	2018	Albania
206.221.184.133	November	2018	Egypt
188.166.119.57	November	2018	Egypt
185.42.137.89	November	2018	Albania
82.196.8.43	October	2018	Iraq
159.89.101.204	December – January	2018-2019	Turkey, Sweden, Syria, Armenia, US
146.185.145.202	March	2018	Armenia
178.62.218.244	December – January	2018-2019	UAE, Cyprus
139.162.144.139	December	2018	Jordan
142.54.179.69	January - February	2017	Jordan
193.37.213.61	December	2018	Cyprus
108.61.123.149	February	2019	Cyprus
172.21.1.8	March	2019	Cyrpsu
212.32.235.160	September	2018	Iraq
198.211.120.186	September	2018	Iraq
146.185.143.158	September	2018	Iraq
185.203.116.116	May	2018	UAE
95.179.150.92	November	2018	UAE
174.138.0.113	September	2018	UAE
128.199.50.175	September	2018	UAE
139.59.134.216	July – December	2018	United States, Lebanon
45.77.137.65	March – May	2019	Syria, Sweden
142.54.164.189	March – May	2019	Syria
199.247.17.221	March – May	2019	Sweden

Tools:

bbfreeze	bcrypt	clusterd	idna	powersploit
joomraa	joomscan	netcat	ngrep	nmap
proxychains	rdphoney	reGeorgSocksProxy	Semtex	seth
ssh-auditor	sshuttle	sslsplit	tcpdump	Zebra_cURL

Exploits:

CVE-2018-0296	CVE-2018-1156	CVE-2017-1000253	CVE-2017-11104	CVE-2017-14189
CVE-2017-1000367	CVE-2017-5638	CVE-2016-8735	CVE-2016-8869	CVE-2016-8870
CVE-2017-3881	CVE-2014-6271	CVE-2013-2094	CVE-2017-6736	CVE-2017-12617
CVE-2009-1151	CVE-2018-0296	CVE-2018-7600		

Attacker Domains:

Domain	Active Timeframe	IP address
ns1[.]intersecdns[.]com	March - April 2019	95.179.150.101
ns2[.]intersecdns[.]com	March - April 2019	95.179.150.101
ns1[.]lcjcomputing[.]com	January 2019	95.179.150.101
ns2[.]lcjcomputing[.]com	January 2019	95.179.150.101

Solution

1- DNS records auditing.

2- Add Multi-factor authentication for all accounts that can modify DNS.

3- Monitor certificate transparency logs.

4- Change the passwords of all the accounts that can modify DNS.

5- Constantly monitor DNS records and set up notifications for any changes to DNS.

Contact Us

aeCERT
P.O. Box 116688
Dubai, United Arab Emirates

Tel (+971) 4 777 4003
Fax (+971) 4 777 4100
Email info[at]aeCERT.ae
Instagram @TheUAETRA
Twitter @TheUAETRA

For secure communications with aeCERT with regards to sensitive or vulnerability information please send your correspondences to aeCERT[at]aeCERT.ae