National Cyber Security Centre
a part of GCHQ

Alert: DNS hijacking activity targeting government and commercial organisations worldwide

Version 2.0

Reference: NCSC-Ops/03-19

5 February 2019

About this document

This NCSC alert highlights recent DNS hijacking activity that has affected a number of domains globally. It provides a summary of available information and tailored mitigation advice.

Handling of the Report

Information in this report has been given a Traffic Light Protocol (TLP) of WHITE, which means it can be shared within and beyond the CiSP community with no handling restrictions.

Disclaimer

This report draws on information derived from NCSC and industry sources. Any NCSC findings and recommendations made have not been provided with the intention of avoiding all risks and following the recommendations will not remove all such risk. Ownership of information risks remain with the relevant system owner at all times.

Introduction

The NCSC is investigating a large-scale Domain Name System (DNS) hijacking campaign that has reportedly affected government and commercial organisations worldwide.[1] The majority of the entities targeted are in the Middle East, but some impact has also been reported in Europe and the United States. While the NCSC is not currently aware of any compromised entities in the UK, the techniques exhibited could feasibly be deployed against UK targets.

In the campaign, attackers are believed to have compromised credentials that have given them the ability to manipulate DNS records, giving them the ability to redirect traffic to attacker-owned infrastructure.

Techniques

Industry reporting has identified two principal techniques being deployed:

- DNS A (Address) record hijacking

A DNS A record maps a domain name to the IP address of the computer hosting that domain. In this technique the attacker alters the A record to point the target domain towards a new IP address owned by the attacker, after accessing the DNS provider's administration panel using previously compromised credentials. The attacker can then create a proxy, mirroring the target domain, and passes user traffic to the legitimate IP address through this. A new TLS certificate is issued by the attacker for the domain, which means traffic will pass through without triggering browser security warnings for users.

- DNS NS (Name Server) record hijacking

An NS record specifies the server(s) which are providing DNS services for that domain. This hijacking technique operates similarly to the previous, but the attackers alter the NS record instead of the A record. As in the first technique, a certificate is created for the victim domain, which allows browsers to establish a connection without errors.

The initial infection vector used to compromise the credentials is not yet known, but it is plausible that multiple techniques are being exploited to gain a foothold.

[1] https://blog.talosintelligence.com/2018/11/dnspionage-campaign-targets-middle-east.html, https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijacking-campaign-dns-record-manipulation-at-scale.html

Indicators of Compromise

A number of indicators of compromise have been reported in open source as relating to recent incidents that may be connected to this campaign. Organisations are advised to monitor for these on their networks.[2]

Indicator	Type	Date seen
hxxp://hr-suncor[.]com/Suncor_employment_form[.]doc	URL	27/11/2018
hxxp://hr-wipro[.]com/Wipro_Working_Conditions[.]doc	URL	10/01/2019
hr-wipro[.]com	Domain	27/11/2018
hr-suncor[.]com	Domain	27/11/2018
0ffice36o[.]com	Domain	27/11/2018
185[.]20[.]184[.]138	IP address	27/11/2018
185[.]161[.]211[.]72	IP address	27/11/2018
185[.]20[.]187[.]8	IP address	27/11/2018
185[.]174[.]101[.]168	IP address	14/01/2019
185[.]161[.]211[.]79	IP address	14/01/2019
185[.]236[.]78[.]63	IP address	14/01/2019

The following files, associated with the delivery of RAT malware, were reportedly seen on 27 November 2018.

Indicator	Type
9c8507a1fd7d2579777723b53fee1f3e	MD5 hash
48b620df71087bd333284c91e52f0cfed1f2d00e	SHA1 hash
82285B6743CC5E3545D8E67740A4D04C5AED138D9F31D7C16BD11188A2042969	SHA256 hash
807482efce3397ece64a1ded3d436139	MD5 hash
Suncor_employment_form.doc	Filename
9ea865e000e3e15cec15efc466801bb181ba40a1	SHA1 hash
9EA577A4B3FAAF04A3BDDBFCB934C9752BED0D0FC579F2152751C5F6923F7E14	SHA256 hash
C00C9F6EBF2979292D524ACFF19DD306	MD5 hash
1022620DA25DB2497DC237ADEDB53755E6B859E3	SHA1 hash
45A9EDB24D4174592C69D9D37A534A518FBE2A88D3817FC0CC739E455883B8FF	SHA256 hash
D2052CB9016DAB6592C532D5EA47CB7E	MD5 hash
1C1FBDA6FFC4D19BE63A630BD2483F3D2F7AA1F5	SHA1
2010F38EF300BE4349E7BC287E720B1ECEC678CACBF0EA0556BCF765F6E073EC	SHA256

[2] See https://www.us-cert.gov/ncas/alerts/AA19-024A for more information and a STIX version of these indicators.

Response

This activity has been widely reported in open source and NCSC is working with industry partners and international government counterparts to understand its impact and identify defensive measures. The Department of Homeland Security published an emergency directive to US government entities on 22 January.[3]

It is recommended that organisations responsible for registering domains follow the NCSC's mitigation advice below.

Mitigation

The following practices will help to mitigate the attacks outlined above, and includes some general good practice for domain management.

Steps to take with your registry/registrar

- Ensure 2-factor authentication is enabled in all registrar or registry accounts, and the passwords are not easily guessed, are stored securely, and not re-used across services.
- Attackers may attempt to use account recovery processes to gain access to domain management, so ensure that contact details are accurate and up-to-date. This is particularly relevant for DNS, as it's common for domains to be registered before corporate email accounts are available.
- Many registrars and registries offer 'lock' services to require additional security enhancing steps before changes can be made. Understand any 'lock' services available to you, and consider applying them, particularly to high-value domains.
- Ensure any available logging is enabled so that you can review changes which have been made.

Steps to take with your DNS hosting

- Ensure 2-factor authentication is enabled in all DNS hosting accounts, and the passwords are not easily guessed, and not re-used across services.
- Ensure you have backups of your critical DNS zones to allow you to recover in the event of a breach.
- Consider use of configuration-as-code approaches to manage changes to your DNS zones.
- Ensure any available logging is enabled so that you can review changes which have been made.

[3] https://cyber.dhs.gov/ed/19-01/

Monitoring

- Monitor critical DNS records for unexpected changes, such as Name Server records, the Address records associated with Name Server records, MX records and the DNS records associated with critical services that would be high value targets. DNS monitoring services are widely available.
- Monitor Certificate Transparency logs for TLS certificates being issued for your domains. Unexpected certificates may be an indication that an attacker has control of DNS associated with the domain. Certificate Transparency log access and monitoring services are available, such as crt.sh, and CertSpotter

Management

- Ensure that individuals involved in DNS management have an awareness of the importance of DNS accounts, and the threat of these accounts being targeted e.g. by phishing
- A domain name may be hijacked if its registration is not renewed and it expires. Ensure that contact and billing details are correct with your registrar to avoid this.
- Subdomains may be delegated to different teams, or to third parties e.g. through NS or CNAME records. Ensure that these parties meet your security needs and ensure that you promptly withdraw such delegations when no longer in use to avoid 'subdomain takeover'[4] issues. Eligible public sector domain owners should register their subdomains in Web Check[5] which includes detection of some subdomain takeover vulnerabilities.
- Consider formalising a 'registry function' in your organisation to oversee domain name management. This is most relevant where multiple teams have registered and operate domains.

[4] https://www.hackerone.com/blog/Guide-Subdomain-Takeovers

[5] https://www.ncsc.gov.uk/blog-post/web-check-helping-you-secure-your-public-sector-websites