Report

Writing a Yara Rule

Sakarie Sa’ad Osman (Sap iD:30025)

Riphah International University

Date: 19 May 2024

Yara Rules

-CT Intelligence feed

Netflix Squatting Campaign

X-Force has identified a new squatting campaign used by threat actors to target the media sector. The campaign has a global scope assumingly luring users into giving away their login credentials.

Threat Type

Squatting Domain, Phishing Domain, Credential Theft

Overview

We observed 3 squatting domain registrations related to a victim in the media sector. The campaign was identified starting with the registration on 2023-10-01 at 17:29:10 up to the latest registration on 2024-05-16 at 08:13:36.

For all registered domains we could identify NameSilo, LLC as the registrar based in the United States. The email address used for registering the domains was anonymized.

The registered domains could not be resolved to any hosting IPs throughout our analysis. However, the registrar NameSilo, LLC covers a pool of 143.435.783 domains where at least 0.24% can be considered as potentially malicious.

Yara Rules

The following list shows the nameservers that are configured as authoritative nameservers for the domain and their malicious score which is the percentage of malicious domains with the same nameserver.

- The NameServers

Domain: my-membership-netflix.com

Name server: ns1.cronustime.org

Name server malicious score: 2.15%

Domain: my-membership-netflix.com

Name server: ns2.aphroditelove.eu

Name server malicious score: 2.13%

Domain: my-membership-netflix.com

Name server: ns3.areswarrior.com

Name server malicious score: 2.19%

Domain: reactivate-account-netfiix.com

Name server: ns11.cronustime.org

Name server malicious score: 3.11%

Yara Rules

Domain: reactivate-account-netfiix.com

Name server: ns12.aphroditelove.eu

Name server malicious score: 2.98%

Domain: reactivate-account-netfiix.com

Name server: ns13.areswarrior.com

Name server malicious score: 3.00%

Domain: supportsnetflix.com

Name server: ns11.cronustime.org

Name server malicious score: 3.11%

Domain: supportsnetflix.com

Name server: ns12.aphroditelove.eu

Name server malicious score: 2.98%

Domain: supportsnetflix.com

Name server: ns13.areswarrior.com

Name server malicious score: 3.00%

Yara Rules

Not forgetting to mention the WhoIs Server: X-Force was able to retrieve the WhoIs server information where we were also able to determine the number of domains each WhoIs server manages and as well adding the malicious rating of the domains in the pool.

Domain: my-membership-netflix.com

Whois server: whois.namesilo.com

Whois server malicious score: 0.25%

Domain: reactivate-account-netfiix.com

Whois server: whois.namesilo.com

Whois server malicious score: 0.25%

Domain: supportsnetflix.com

Whois server: whois.namesilo.com

Whois server malicious score: 0.25%

Yara Rules

Recommendations

Do not click or open links in mails directly, instead type in the main URL in your browser or search the brand/company via your preferred search engine.

Ensure anti-virus software and associated files are up to date.

Search for existing signs of the indicated IOCs in your environment.

Block all URL and IP-based IOCs at the firewall, IDS, web gateways, routers, or other perimeter-based devices, a course of action, resources, or applications to remediate this threat.

Keep applications and operating systems running at the current released patch level.

Reference

Proprietary IBM X-Force Threat Intelligence

Yara Rules

My Conclusion:

Based on this threat Intelligence feed I have written the Yara Rule which will have/contain all the String seen in this feed.

The code will be posted below.

```
rule NetflixReport
{
    meta:
    description = "squatting campaign used by threat actors to target the media sector. The campaign has a global scope assumingly luring users into giving away their login credentials. Threat Type"
    Author = "Sakarie Sa'ad Osman"
    date = "21-05-2024"

    strings:
        $domain1 = "my-membership-netflix.com"
        $domain1 = "reactivate-account-netfiix.com"
        $domain1 = "supportsnetflix.com"



    condition:
        any of them

}
```