Upozornění na nový způsob DDoS útoků NoName057(16)

portal.nukib.gov.cz/informacni-servis/informace/upozorneni-a-hrozby/upozorneni-na-novy-zpusob-ddos-utoku-noname057-16

Ruská hacktivistická skupina NoName057(16), které v minulosti způsobila několik DDoS útoků na české instituce, aktualizovala klienta označovaného jako DDoSia, jímž provádí DDoS útoky na aplikační vrstvu webové aplikace napadené organizace.

Dříve doporučovaná metoda blokace nelegitimních požadavků na základě HTTP hlavičky požadavku `User-Agent: Go-http-client/1.1` již není s novou verzí použitelná. Klient nově obsahuje seznam různých hodnot pro tuto hlavičku (viz níže) a náhodně vybírá při požadavku jednu hodnotu z tohoto seznamu. Seznam hodnot vychází z běžně používaných „user agentů" současných webových prohlížečů a tak blokace na základě tohoto seznamu by způsobila odepření poskytování služby i legitimním uživatelům.

Nový způsob blokace

Dle analýzy klienta DDoSia provedené německým BSI (viz příloha, *TLP:GREEN*) je ale možné blokovat nelegitimní HTTP požadavky pocházející z nové verze tohoto DDoS klienta na základě HTTP hlavičky požadavku `Accept` a její specifické hodnoty:

```
Accept: text/html,application/xhtml+xml,application/xml,
```

Autoři aplikace DDoSia totiž udělali chybu a tato HTTP hlavička odeslaná z klienta obsahuje na posledním místě hodnoty znak `,` (čárka). Uvedení tohoto znaku odporuje RFC9110 a běžné prohlížeče nebo jiné legitimní aplikace nikdy jako koncový znak čárku nepoužívají. Zároveň hodnota `text/html,application/xhtml+xml,application/xml,` je vždy neměnná a je využita u všech neligitmních požadavků pocházejích z tohoto klienta.

Ostatní způsoby blokace (na základě uvedených ASN nebo v kraním případě geofencing) zůstávají v platnosti i s novou verzí.

V případě, že skupina NoName057(16) bude opět provádět útoky na české instituce, dá se předpokládat, že už bude využita nová verze klienta. Nedá se ale vyuloučit, že starší verze je stále aktivní. Proto doporučujeme být připraveni na blokaci jak na základě HTTP hlavičky `User-Agent`, tak `Accept`. Blokace se dá provést vhodným nastavením HTTP serveru (např. nginx, Apache httpd). Zároveň doporučujeme přidat logování HTTP hlavičky `Accept` do přístupového (access) logu, aby bylo možné tento typ útoku odhalit.

Stále platí, že NÚKIB od partnerů získává v reálném čase seznam domén, na které je prováděn DDoS a proaktivně napadané organizace v případě DDoS útoku kontaktuje.

Příkad HTTP požadavku zasílaného z DDoS klienta DDoSia

```
GET /attackFEJVUXWIANOD HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/118.0.0.0 Safari/537.36 Edg/118.0.2088.76 GLS/97.10.7399.100
Accept: text/html,application/xhtml+xml,application/xml,
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Content-Type: application/json
Connection: close
```

Hodnoty HTTP hlavičky User-Agent používané klientem

- Mozilla/5.0 (iPhone; CPU iPhone OS 15_6_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/19
- Mozilla/5.0 (iPhone; CPU iPhone OS 16_1_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/15
- Mozilla/5.0 (Linux; Android 11; SM-A115M Build/RP1A.200720.012; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/102.0.5005.125 Mobile Safari/537.36 Instagram 306.0.0.35.109
- Mozilla/5.0 (Linux; Android 13; SAMSUNG SM-T220) AppleWebKit/537.36 (KHTML, like Gecko) SamsungBrowser/23.0 Chrome/115.0.0.0 Mobile Safari/537.36
- Mozilla/5.0 (Linux; Android 13; SM-F711U) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Mobile Safari/537.36 EdgA/114.0.1823.43
- Mozilla/5.0 (Linux; Android 6.0.1; SM-G532MT Build/MMB29T; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/99.0.4844.88 Mobile Safari/537.36
- Mozilla/5.0 (Linux; Android 9) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/119.0.6045.66 Mobile DuckDuckGo/1 Lilo/1.2.3 Safari/537.36
- Mozilla/5.0 (Macintosh; U; PPC; en-US; rv:0.9.3) Gecko/20010802
- Mozilla/5.0 (Macintosh; U; PPC Mac OS X Mach-O; en-US; rv:1.7.6) Gecko/20050319
- Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36 Edg/118.0.2088.76 GLS/97.10.7399.100
- Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Ubuntu Chromium/102.0.5143.178 Chrome/102.0.5143.178 Safari/537.36
- Mozilla/5.0 (X11; Linux x86_64; SMARTEMB Build/3.12.9076) AppleWebKit/537.36 (KHTML, like Gecko) Chromium/103.0.5060.129 Chrome/103.0.5060.129 Safari/537.366864797660130609714981900799081393217269435300143305409394463459185543183397
- Mozilla/5.0 (X11; U; Linux i586; en-US; rv:1.0.0) Gecko/20020623 Debian/1.0.0
- Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.2.1) Gecko/20021208 Debian/1.2.1
- Mozilla/5.0 (X11; U; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Ubuntu Chromium/115.0.5738.217 Chrome/115.0.5738.217 Safari/537.36

Klasifikace

TLP:AMBER

Autor

Národní úřad pro kybernetickou a informační bezpečnost

Datum

23. 11. 2023

Přílohy

2023-11-21_ReSponS_Updated DDoSia Attack Behavior-1.pdf

Reakce

1