Twitter
LinkedIn
Email

مهران سیفعلی‌نیا

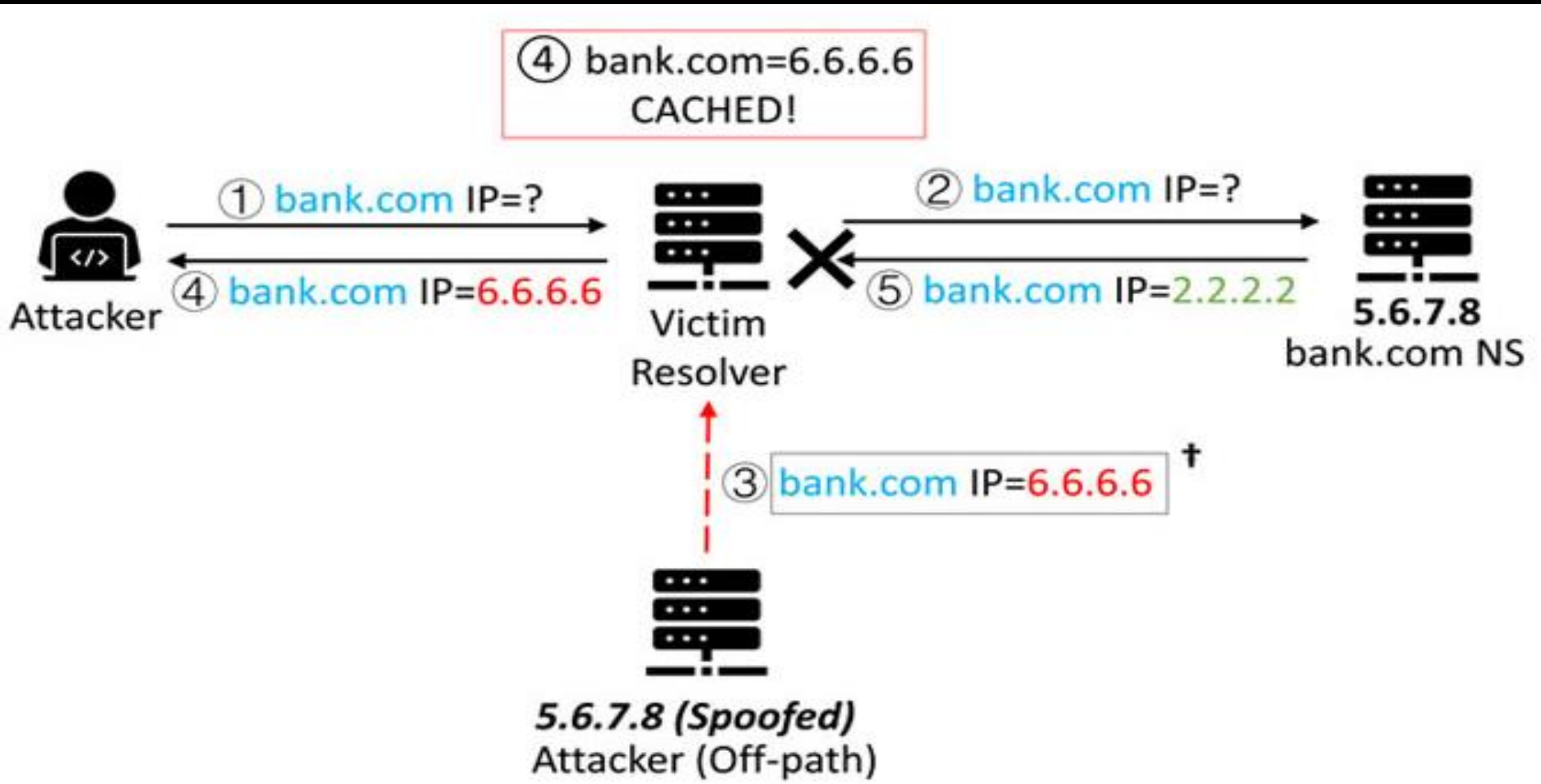
Web Penetration Tester
Python Programmer

SAD DNS

نقض جدید حملات احیای مسموم‌سازی DNS

منبع: TheHackerNews

1 Critical
2 Cache poisoning



گروهی از دانشگاهیان دانشگاه California و Tsinghua مجموعه‌ای از رخنه‌های امنیتی بحرانی[1] را کشف کرده‌اند که می‌تواند منجر به احیای دوباره‌ی حملات مسموم‌سازی حافظه‌ی موقت[2] DNS گردد.

3 Off-Path
4 Side Channel
5 weaponizable

حملات SAD DNS (Side-Channel AttackeD DNS) روشی است که به یک شخص خرابکار امکان پیاده‌سازی حملات خارج از مسیر[3] را می‌دهد، به این شکل که ترافیک‌هایی که به یک مبدا خاص ارسال می‌شوند را به سرور تحت کنترل خودش هدایت می‌نماید، در نتیجه می‌تواند ارتباط را استراق سمع یا دستکاری نماید.

محققان می‌گویند: «این یک نقطه‌ی عطف بسیار مهم است – اولین حمله‌ی شبکه‌ی کانال جانبی[4] با امکان مسلح‌سازی[5] که می‌تواند عوارض امنیتی بسیار جدی را ایجاد نماید.» این حمله به مهاجم خارج از مسیر اجاره می‌دهد تا رکوردهای مخرب DNS را در حافظه‌ی موقت DNS ذخیره نماید.

آسیب‌پذیری CVE-2020-25705، از یافته‌های ارائه شده در کنفرانس کامپیوتر و امنیت ارتباطات ACM می‌باشد. (CCS ‘20)

این رخنه بر روی سیستم‌عامل‌های:

Linux 3.18-5.10
Windows Server 2019 (version 1809)
macOS 10.15
FreeBSD 12.1.0.

و نسخه‌های جدیدتر اثر می‌گذارد.

6 DNS resolvers
7 secure domain name system
8 randomization-based defenses
9 source port

- DNS Forwarderها، تبدیل به سطح جدید حملات می‌شوند

تحلیل‌گران DNS[6] به طور معمول در شبکه برای ارتقاء عملکرد پاسخگویی، پاسخ‌های مربوط به جستجوهای انجام شده توسط IPهای مختلف را در دوره‌های زمانی خاصی ذخیره می‌کنند اما همین سازوکار می‌تواند با جعل یک آدرس IP، برای مسمومسازی حافظه‌ی نهان ورودی‌های DNS یک وب‌سایت استفاده شود و تمامی کاربرانی که در تلاش برای مراجعه به سایت هستند را به سایتی دیگر که مهاجم انتخاب کرده است هدایت نماید.

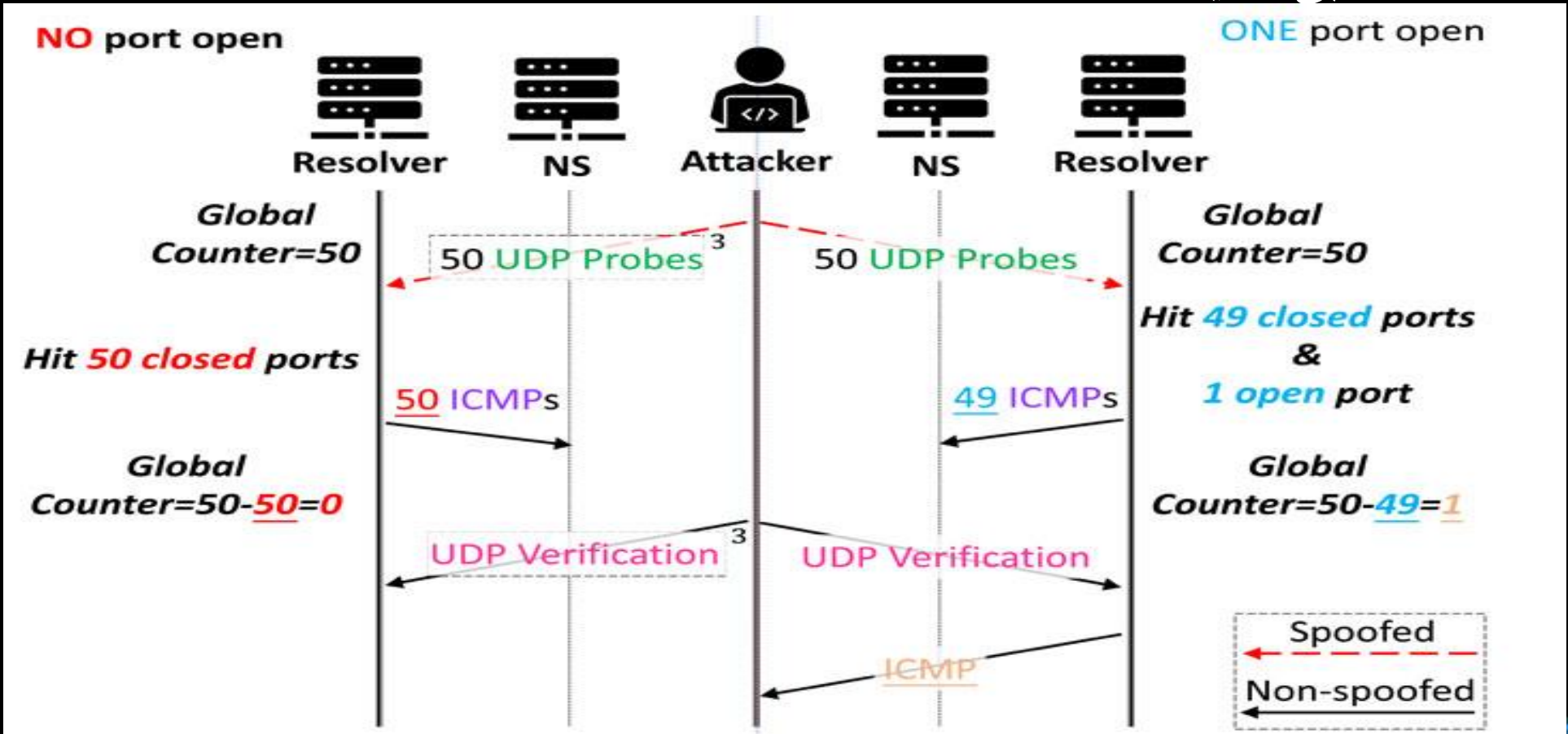
به‌هرحال، بیشترین تاثیر این حملات ضربه‌ای است که به پروتکل‌هایی نظیر DNSSEC (Domain Name System Security Extensions) می‌زند. وظیفه‌ی این پروتکل‌ها ساخت سیستم نام دامنه‌ی امن[7] است که این کار را با اضافه کردن امضاهای رمزنگاری شده به رکوردهای موجود و دفاع احتمالی[8] (مبتنی بر احتمال) انجام می‌دهند. این دو مورد به تحلیل‌گران DNS اجازه می‌دهد برای هر جستجو از ID انتقال(TxID) و پورت منبع[9] متفاوتی استفاده کنند.

10 incentives
11 compatibility
12 stacks
13 Cloudflare
14 Google

```
$ dig @          test2.test.xiaofengtest.net +timeout=999

; <<>> DiG 9.11.5-P4-5.1ubuntu2.1-Ubuntu <<>> @          test2.test.xiaofengtest.net +timeout=999
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7660
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;test2.test.xiaofengtest.net.   IN      A

;; ANSWER SECTION:
test2.test.xiaofengtest.net. 300 IN     A       1.2.3.4

;; AUTHORITY SECTION:
test2.test.xiaofengtest.net. 3534 IN    NS      ns.test2.test.xiaofengtest.net.

;; ADDITIONAL SECTION:
ns.test2.test.xiaofengtest.net. 294 IN  A       54.177.157.64

;; Query time: 172 msec
;; SERVER:          #53(          )
;; WHEN: Thu Apr 02 20:54:05 UTC 2020
```

باید توجه کرد که به‌دلیل وجود «انگیزش[10] و سازگاری[11]»، هنوز امکان پیاده‌سازی گسترده این دو معیار جلوگیری وجود ندارد. محققان می‌گویند که یک روش حمله‌ی کانال جانبی ابداع کرده‌اند که می‌تواند در برابر محبوب‌ترین نرم‌افزارهای پُشته‌های[12] DNS باموفقیت استفاده شود. در این صورت تحلیل‌گران DNS نظیر 1.1.1.1های فضای‌ابری[13] و 8.8.8.8های گوگول[14] آسیب‌پذیر خواهند بود.

- یک حمله‌ی کانال جانبی جدید



حملات SAD DNS با استفاده از یک ماشین در معرض خطر در هر شبکه‌ای کار می‌کنند. این ماشین باید قابلیت ایجاد و ارسال یک درخواست به خارج از **ارسال کننده‌ها**[15] یا **تحلیل‌گران DNS** را داشته باشد؛ مثل شبکه‌های بی‌سیم عمومی که توسط یک روتر بی‌سیم در کافی‌شاپ‌ها، مراکز خرید یا فرودگاه‌ها مدیریت می‌شود.

سپس با سوءاستفاده از یک کانال جانبی در پُشته‌ی پروتکل اقدام به اسکن و کشف پورت‌هایی می‌نماید که برای شروع جستجوی DNS مورد استفاده قرار می گیرند و بعد از آن تعداد زیادی پاسخ جعلی DNS را با Brute-Force نمودن TxID ها تزریق می‌نماید.

به‌طور دقیق‌تر، محققان از یک کانال موجود در درخواست‌های نام دامنه استفاده می‌نمایند که کار آن کاهش دقیق تعداد پورت‌ها با ارسال بسته‌های جعلی UDP می باشد که هرکدام با یک آدرس IP متفاوت به سرور قربانی ارسال می‌شود و در نتیجه می‌توان بر اساس پاسخ دریافت شده فهمید که کدام یک از درخواست‌های جعل شده به پورت منبع بر روی ICMP برخورد کرده‌اند.

این روش سرعت اسکن را تا هزار پورت در ثانیه افزایش می‌دهد، به‌طور کلی حدودا 60 ثانیه زمان لازم است تا کل 65536 پورت (با در نظر گرفتن پورت 0) اسکن شود. با وجود پورت‌های منبعی که شناسایی شدند، نتها کاری که مهاجم باید انجام دهد این است که یک IP آدرس برای هدایت مجدد ترافیک سایت وارد نماید و حمله‌ی مسموم‌سازی حافظه‌ی موقت Cache را با موفقیت پیاده‌سازی نماید.

16 Aggressively
17 Global rate limit

- جلوگیری از حملات SAD DNS

در کنار شرح دادن روش‌هایی برای توسعه‌ی حملات که به مهاجم اجازه‌ی اسکن پورت‌های بیشتری را می‌دهد و همچنین تزریق رکوردهای هزر اضافه برای مسموم‌سازی حافظه‌ی موقت DNS، این مطالعه نشان داد که بیش از 34% از تحلیل‌گران دردسترس در اینترنت آسیب‌پذیر می‌باشند که 85% آن‌ها را سرویس‌های DNS محبوب مانند گوگل و فضای‌ابری تشکیل می‌دهند.

محققان توصیه کرده‌اند که برای مقابله با SAD DNS، درخواست‌های خروجی ICMP را غیرفعال کنید و تنظیمات مربوط به Timeout جستجوهای DNS بسیار سختگیرانه[16] اعمال نمایید. همچنین یک ابزار برای بررسی سرویس‌های DNS تجمیع کرده‌اند که وضعیت آسیب‌پذیر بودن سرویس را بررسی می‌نماید. علاوه‌بر این، این گروه با تیم امنیتی لینوکس کرنل نیز برای ارائه‌ی یک وصله‌ی امنیتی هم‌کاری نموده‌اند که محدودیت عمومی[17] ICMP را تصادفی کرده تا نوسانات کانال‌های جانبی را کاهش دهد.

محققان به این نتیجه رسیدند که «کانال جانبی ارائه شده‌ی جدید و عمومی که مبتنی بر محدودیت عمومی ICMP می‌باشد، به صورت جامع توسط سیستم‌عامل‌های مدرن پیاده‌سازی شده‌اند که اجازه‌ی اسکن کارآمد پورت‌های منبع UDP را در جستجوهای DNS می‌دهد.»