infoblox

Threat Intel

MUDDLING MEERKAT: IL MANIPOLATORE DEL GREAT FIREWALL

Autori:
Dott.ssa Renée Burton
e Anonimo

INDICE DEI CONTENUTI

SOMMARIO ESECUTIVO

Il presente documento presenta un attore sconcertante, Muddling Meerkat, che sembra appartenere allo stato nazionale della Repubblica Popolare Cinese (RPC). Muddling Meerkat conduce operazioni attive tramite DNS creando grandi volumi di query ampiamente distribuite che vengono successivamente propagate su Internet utilizzando resolver DNS aperti. Le sue operazioni si intrecciano con due argomenti strettamente legati alla Cina e agli attori cinesi: il Great Firewall (GFW) cinese e gli attacchi Slow Drip, o attacchi DDoS (Distributed Denial-of-Service) con prefisso casuale. Sebbene le operazioni di Muddling Meerkat sembrino a prima vista attacchi DDoS al DNS, sembra improbabile che il denial of service sia il loro obiettivo, almeno nel breve termine. Le operazioni di Muddling Meerkat sono di lunga durata, a quanto pare a partire da ottobre 2019, e dimostrano un alto grado di competenza nel DNS.

Le operazioni di Muddling Meerkat sono complesse. In effetti, sono così contorte che si potrebbe pensare che Muddling Meerkat non rappresenti una minaccia. Ma nella sicurezza informatica, soprattutto nel complesso mondo del DNS, dovremmo pensare in modo strategico. Nel febbraio 2024, la Cybersecurity and Infrastructure Security Agency (CISA) degli Stati Uniti e diversi partner internazionali hanno emesso un avviso in cui si legge: "Negli ultimi anni, gli Stati Uniti hanno assistito a un cambiamento strategico nell'attività di minaccia informatica della RPC, passando da un focus sullo spionaggio a un pre-posizionamento per possibili attacchi informatici dirompenti contro le infrastrutture critiche statunitensi".[1] Sebbene quell'avviso specifico si concentrasse sulle tecniche di "living off the land" utilizzate dall'attore Volt Typhoon, il messaggio che "gli attori informatici della RPC si mimetizzano con le normali attività di sistema e di rete, evitano l'identificazione da parte delle difese di rete e limitano la quantità di attività che viene catturata nelle comuni configurazioni di registrazione" e ciò è molto simile al modo in cui Muddling Meerkat rimane ben nascosto.[2]

CHE COS'È MUDDLING MEERKAT

Muddling Meerkat ha l'apparente capacità di controllare il GFW e lo fa in un modo mai riportato in precedenza. Sebbene alcune parti delle sue operazioni siano simili agli attacchi Slow Drip, la motivazione e l'obiettivo di Muddling Meerkat non sono chiari. I dati ci mostrano che le sue operazioni:

- Utilizzano i server nello spazio IP cinese per condurre le campagne effettuando query DNS per sottodomini casuali a indirizzi IP in tutto il mondo, sondando in ultima analisi le reti DNS a livello globale
- Utilizzano le query dei record MX, oltre ad altri tipi di record, per i nomi host brevi e casuali di un insieme di domini al di fuori del controllo dell'attore nei domini di primo livello (TLD) .com e .org
- Inducono falsi record MX da indirizzi IP cinesi iniettati dal GFW
- Utilizzano domini "super vecchi", in genere registrati prima dell'anno 2000, evitando le blocklist DNS e la collisione con molti domini Active Directory aziendali
- Scelgono i domini da abusare in base alla loro lunghezza ed età piuttosto che al loro stato e proprietà attuali; mentre molti domini vengono abbandonati o sono stati riutilizzati per un uso discutibile, altri domini vengono utilizzati attivamente da entità legittime
- Conducono campagne di uno o tre giorni su base abbastanza continuativa
- Non sembrano utilizzare lo spoofing su larga scala degli indirizzi IP di origine, ma piuttosto avviano query DNS da server dedicati
- Sono di dimensioni limitate per evitare il rilevamento e le interruzioni del servizio
- Possono essere condotte in componenti discreti, creando diversi modelli DNS nel tempo

1 https://www.linkedin.com/posts/cisagov_with-us-and-international-government-partners-activity-7161082451354603520-pv0q

2 https://www.cisa.gov/resources-tools/resources/identifying-and-mitigating-living-land-techniques

- Sono iniziate il 15 ottobre 2019 o intorno a tale data[3]

Una visione semplificata delle operazioni di Muddling Meerkat così come le intendiamo oggi è mostrata nella Figura 1.

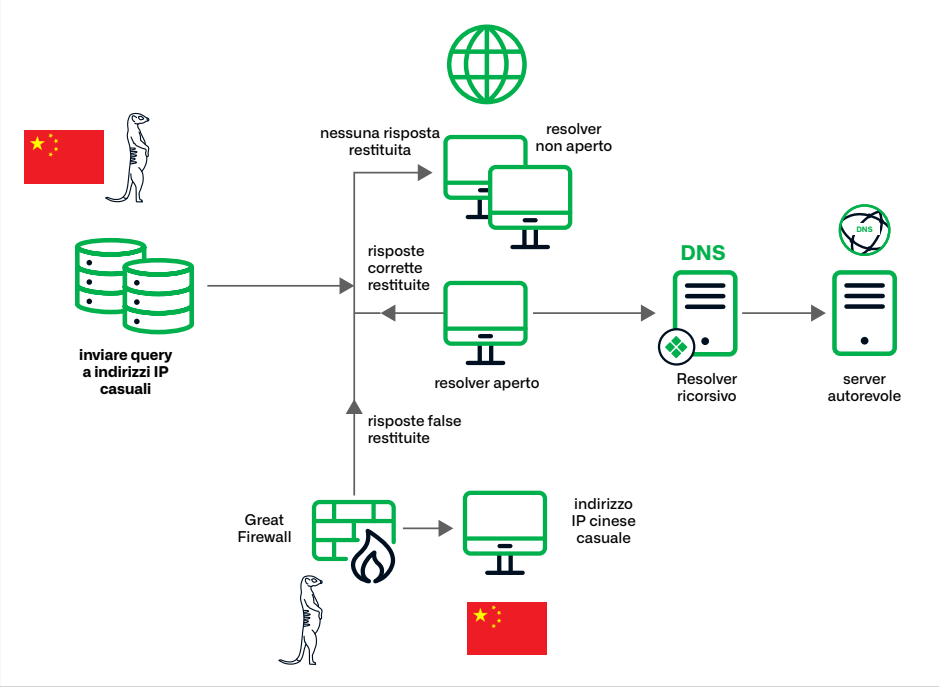

Figura 1. Una panoramica delle operazioni di Muddling Meerkat così come sono attualmente intese. Si osserva che il Great Firewall fornisce risposte false alle query MX, un comportamento che non è stato documentato in precedenza.

La nostra scoperta di Muddling Meerkat è stata fortuita e l'attore avrebbe potuto passare inosservato per molti altri anni se non fosse stato per la visibilità dei dati di più organizzazioni. Il presente documento è frutto di una ricerca congiunta condotta da ricercatori specializzati in minacce informatiche e fornitori di servizi di sicurezza non dichiarati, nonché da Merit Network, una società indipendente senza scopo di lucro gestita dalle università pubbliche del Michigan, e da DomainTools.[4] Ciascuno dei contributori ha accesso a una qualche forma di raccolta DNS passiva e può osservare Muddling Meerkat da una prospettiva unica. È impossibile osservare la totalità delle attività di Muddling Meerkat da un solo punto di osservazione. Combinando le informazioni, otteniamo un quadro dell'attività dell'attore che non sarebbe possibile indipendentemente. Ogni risultato all'interno dell'articolo, se non diversamente specificato, è confermato da due fonti indipendenti o tratto direttamente dai resolver DNS di Infoblox.

CONTESTO

Ho preso la decisione insolita di scrivere questo articolo in prima persona. In parte, perchè mi sembra più appropriato quando si racconta una storia strana come questa. Inoltre, i miei studi e pubblicazioni precedenti sugli attori di minacce DNS cinesi hanno contribuito a trarre le mie conclusioni su Muddling Meerkat. All'inizio della mia carriera, io e i colleghi della National Security Agency (NSA) abbiamo passato migliaia di ore a studiare un attore cinese che ha eseguito attacchi DDoS basati sul DNS per diversi anni. Abbiamo soprannominato questo attore ExploderBot e abbiamo pubblicato in sordina queste scoperte nella primavera del 2018. Dopo aver operato quasi quotidianamente dal 2014, devastando i provider di servizi Internet, ExploderBot ha cessato le operazioni poco più di un mese dopo la pubblicazione

3 Ci sono alcune prove che le operazioni siano iniziate con qualche mese di anticipo, a giugno 2019, ma non sono in grado di convalidare questa data.

4 https://www.merit.edu/

del nostro articolo. È scomparso dal 18 maggio 2018. La natura degli attacchi DDoS cinesi al DNS è cambiata e ho scritto uno studio longitudinale sui cambiamenti alla fine del 2020. Da allora, non ho passato molto tempo a esaminare gli attacchi DDoS al DNS, cinesi o di altro tipo. Infoblox dispone di rilevatori che cercano segni di attività e bloccano automaticamente i domini correlati per i clienti del nostro prodotto Advanced DNS Protection (ADP), ma questo sistema funziona in gran parte senza bisogno di intervento umano.

Muddling Meerkat è venuto alla mia attenzione mentre indagavo su un attore di minacce DNS che fornisce servizi ad altri attori di minacce che si occupano di gioco d'azzardo illegale cinese e di app false. Non si trattava di gioco d'azzardo, ma di query e risposte anomale per i record del mail server (MX) del DNS. Anche se ho scoperto che Muddling Meerkat utilizza anche altri tipi di record, questo articolo si concentrerà sui record MX perché la loro natura specifica all'interno del DNS consente un'analisi più pulita.

Il GFW agisce per impedire ai residenti cinesi di accedere a siti web o servizi che il governo considera inappropriati o illegali.[5] Ma è anche noto per iniettare false risposte nelle query DNS. Il GFW si applica a tutto il traffico IP in entrata o in uscita dallo spazio IP cinese. È facile dimostrare il comportamento di risposta falsa del GFW, come mostrerò più avanti, nella sezione Indagine sul Great Firewall cinese. Il GFW può essere descritto come un "operatore laterale", il che significa che non altera direttamente le risposte DNS ma inietta le proprie risposte, entrando in una condizione di gara con qualsiasi risposta dalla destinazione originale prevista. Quando la risposta GFW viene ricevuta per prima dal richiedente, può avvelenare la sua cache DNS. Oltre al GFW, la Cina gestisce un sistema denominato Great Cannon (GC). Il GC è un "operatore intermedio", che può modificare i pacchetti durante il percorso verso la loro destinazione.[6] Il GC è stato utilizzato per attacchi DDoS su larga scala. Nel 2015, è stato usato per attaccare l'organizzazione non governativa GreatFire.org che monitora la censura del GFW.[7] Da allora è stato utilizzato in modo intermittente per gli attacchi DDoS, compresi quelli destinati a prevenire le proteste a Hong Kong.[8] L'ambito reale delle operazioni del GC è sconosciuto. In combinazione, il GFW e il GC creano molte interferenze e dati fuorvianti che possono ostacolare le indagini sui comportamenti anomali nel DNS. Mi è capitato più volte di seguire diverse piste di indagine solo per concludere: oh, è solo il GFW.

Oltre all'abuso dei record MX, Muddling Meerkat ha attirato la nostra attenzione perché ha mostrato modelli comportamentali simili, sebbene con volumi inferiori, agli attacchi DDoS al DNS. In un attacco Slow Drip, o attacco DDoS al DNS con prefisso casuale, le query per sottodomini apparentemente casuali di un dominio di destinazione vengono effettuate su larga scala, in genere propagate tramite resolver aperti. Questi attacchi sono emersi originariamente nel 2014 e le prime vittime segnalate sono state cinesi. Diversi colleghi ed io abbiamo esaminato i log DNS per diversi anni di questi attacchi, concludendo che la maggior parte degli attacchi che hanno causato danni dimostrabili sono stati condotti da un singolo attore, ExploderBot. Abbiamo identificato diversi artefatti matematici nelle query DNS e nei pacchetti IP di ExploderBot che sono rimasti coerenti per cinque anni. Abbiamo anche stabilito che il traffico proveniente da ExploderBot, che includeva indirizzi IP di origine e di destinazione falsificati, veniva iniettato vicino alla dorsale di rete. I resolver aperti che ricevevano le query le inoltravano al proprio resolver ricorsivo e nelle reti con molti dispositivi non gestiti contenenti resolver aperti sconosciuti, il volume delle query interrompeva i provider di server Internet. Gli indirizzi IP falsificati utilizzati nelle query DNS di ExploderBot erano ampiamente distribuiti e le risposte del GFW sono servite come depistaggi che hanno ostacolato la nostra analisi per molto tempo. Quando le operazioni di ExploderBot sono cessate a maggio 2018, è rimasta una curiosa serie di attacchi continui a basso volume con un impatto o uno scopo poco evidente. Negli ultimi anni, gli attacchi con prefisso casuale hanno avuto un impatto sui name server con una certa regolarità, ma non ho visto lo stesso livello di volume associato a ExploderBot.[9]

5 https://www.cybereason.com/blog/malcious-life-podcast-the-great-firewall-of-china-part-1

6 https://citizenlab.ca/2015/04/chinas-great-cannon/

7 https://foreignpolicy.com/2015/04/10/great-cannon-china-internet-cyber-attack-baidu/

8 https://cybersecurity.att.com/blogs/labs-research/the-great-cannon-has-been-deployed-again

9 https://infosec.exchange/@ricci@discuss.systems/111508151184559310

In questo articolo descriverò le operazioni di Muddling Meerkat nel contesto di ciò che so sul GFW, spiegherò come rilevarne l'attività e discuterò alcune delle insidie del tentativo di analizzare attori come Muddling Meerkat. In particolare, voglio mettere in guardia i lettori sui pericoli dei resolver aperti e dell'uso di domini di ricerca non registrati in DNS o Microsoft Active Directory, che possono portare sia alla partecipazione ad attacchi DDoS che alla perdita di informazioni di rete a favore degli aggressori.

UN PO' DI GERGO

Il linguaggio nel DNS è confuso. Quando lo combiniamo con i pacchetti IP, lo diventa ancora di più. Diverse volte nel corso di questa ricerca, io e il mio coautore abbiamo dovuto fermarci e chiederci: *di quale IP stiamo parlando?* Ecco perciò come utilizzo diversi termini in questo documento:

- L'indirizzo IP che effettua una query DNS o riceve una risposta per una query DNS è chiamato **indirizzo IP richiedente**. Questo nome si applica indipendentemente dal fatto che il pacchetto IP contenga la query o la risposta.
- L'indirizzo IP che risponde a una query DNS è chiamato **indirizzo IP di risposta**. In un mondo perfetto, si tratta di resolver, ma come vedremo più avanti nella sezione intitolata Il ruolo degli indirizzi IP cinesi, con Muddling Meerkat, sono solo indirizzi IP.
- Un indirizzo IP incluso in un record di risorse DNS di una risposta è chiamato **indirizzo IP di risoluzione**.
- Quando parlo in generale di record di risorse DNS in una risposta, potrei dire che la **risposta** si riferisce al valore o ai valori contenuti nel record.

OPERAZIONI DI MUDDLING MEERKAT

Le operazioni di Muddling Meerkat sono complesse e dimostrano che l'attore ha una profonda conoscenza del DNS ed è esperto di Internet. Per semplificare questa esposizione, mi occupo solo dei componenti dell'operazione relativi ai record MX o alle catene di risoluzione MX del DNS. In tutti i casi, esiste un dominio registrato, *non* sotto il controllo dell'attore, chiamato **dominio di destinazione**. In questo articolo discuto tre tipi di attività:

- Query per record MX di un dominio di destinazione
- Query per record MX di nomi host casuali di un dominio di destinazione
- Query per record A di nomi host casuali di un dominio di destinazione

Le query per nomi host casuali di un dominio di destinazione rappresentano un attacco DDoS Slow Drip; tuttavia, le query di Muddling Meerkat differiscono da quelle di ExploderBot o di altri attacchi Slow Drip. I nomi host sono brevi. Inoltre, sebbene alcuni attacchi Slow Drip includano una serie di tipi di query, il tipo più comune è ancora un record A per un indirizzo IPv4. Non ho mai visto in precedenza il tipo di attività relativa a record MX che caratterizza Muddling Meerkat. Anche la scelta dei domini di destinazione è notevole, come vedremo più avanti nella sezione Domini di destinazione di Muddling Meerkat.

Per quanto riguarda il nome Muddling Meerkat: "meerkat" è il nome inglese del suricato, un membro della famiglia delle manguste. Di aspetto ingannevolmente carino, è intelligente, laborioso ed eccezionalmente feroce per le sue piccole dimensioni. Muddling Meerkat è noto per abusare dei record MX del DNS e condurre operazioni che coinvolgono il Great Firewall cinese, aggiungendo confusione e falsità all'analisi del problema. A causa dell'ampio uso di resolver aperti per l'operazione, l'attività "si alza e si abbassa" nel corso del tempo e da luogo a luogo, come fanno i suricati quando spuntano fuori dalle loro tane.

INDAGINE SUL GREAT FIREWALL CINESE

Il GFW svolge un ruolo importante nei dati di Muddling Meerkat in quanto possiamo osservare false risposte alle query DNS in raccolte di dati DNS selezionate. Quando vediamo una risposta falsa, l'IP di origine di quel record è un indirizzo IP cinese, coerente con l'iniezione da parte del GFW o la modifica da parte del GC. Seconda solo agli Stati Uniti, la Cina controlla oltre 350 milioni di indirizzi IP, distribuiti geograficamente in tutto il mondo. Per tutto il traffico in entrata e in uscita da questo spazio IP, il GFW può iniettare risposte nelle query DNS utilizzando decisioni segrete e senza impatti sulle prestazioni dell'utente. Per farlo bene ci vuole molta esperienza. La Cina ha sfruttato le aziende tecnologiche occidentali all'inizio del secolo per costruire componenti del firewall e implementare vari altri meccanismi di sorveglianza e, così facendo, ha sviluppato le proprie capacità e conoscenze.[10]

La Cina ha sviluppato un sistema che risponderà con risposte false anziché utilizzare semplicemente un NXDOMAIN o un altro meccanismo di risposta comunemente utilizzato dai firewall DNS.[11] Per questo motivo, non c'è bisogno di credermi sulla parola; è possibile testare il firewall da soli. I ricercatori hanno precedentemente trovato risposte false per centinaia di migliaia di domini e hanno concluso che alcune di queste risposte avevano inquinato la cache di alcuni resolver ricorsivi.[12] Nella mia ricerca, sia in quella pubblicata su ExploderBot che in seguito, ho visto una serie vertiginosa di risposte di indirizzi IP da parte del GFW.

Il modo più semplice per dimostrare l'impatto del GFW è quello di effettuare query DNS su un indirizzo IP cinese casuale, che non sia un server DNS stabilito. Stephen Bortmeyer ne ha fornito una descrizione in un blog del 2015.[13] Gli esperimenti possono essere eseguiti dalla riga di comando con l'utilità dig o con uno strumento online. Se si chiede il record A di un dominio popolare, l'indirizzo IP cinese restituirà invariabilmente una risposta, anche se non ospita alcun servizio DNS. La Figura 2 qui sotto mostra un esempio in cui un indirizzo IP assegnato a China Unicom, e che attualmente non ospita alcun servizio, risponde a una query DNS per l'indirizzo IP di `google[.]com` con una risposta falsa.

```
; <<>> DiG diggui.com <<>> @111.193.204.201 google.com A
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54398
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             60      IN      A       93.46.8.90

;; Query time: 214 msec
;; SERVER: 111.193.204.201#53(111.193.204.201)
;; WHEN: Tue Jan 09 00:15:06 UTC 2024
;; MSG SIZE  rcvd: 54
```

Figura 2. Un indirizzo IP China Unicom che non ospita servizi risponde alle query DNS per il record A di `google[.]com` *con un indirizzo IP in Italia. La risposta è un reindirizzamento intenzionale e cambierà in ogni risposta. Credito immagine:* `diggui[.]com`.

10 https://www.cybereason.com/blog/malcious-life-podcast-the-great-firewall-of-china-part-1

11 https://citizenlab.ca/2021/11/gfwatch-a-longitudinal-measurement-platform-built-to-monitor-chinas-dns-censorship-at-scale/

12 How Great is the Great Firewall? Measuring China's DNS Censorship. Nguyen Phong Hoang, et al., 30th USENIX Security Symposium (USENIX Security 21), https://www.usenix.org/system/files/sec21-hoang.pdf (ultimo accesso 9 gennaio 2024)

13 https://www.bortzmeyer.org/sichuan-pepper.html

Non si sa come il GFW scelga a quali domini inviare risposte false come mezzo di censura. L'interrogazione dello stesso indirizzo IP cinese per un dominio non censurato in genere genera un errore che indica che non è stato possibile raggiungere alcun server. Questo risultato dimostra che il GFW inietta le risposte solo per determinate query. Nella mia esperienza, il GFW risponde a tutte le query DNS, indipendentemente dal tipo di risorsa richiesta con un indirizzo IPv4. Ad esempio, se chiediamo allo stesso indirizzo IP il record MX di `google[.]com`, restituisce un indirizzo IPv4 diverso, questa volta assegnato a Korea Telecom. Un record MX corretto deve includere una stringa di testo con un nome di dominio completo (FQDN), non un indirizzo IPv4 (vedere la Figura 3). Una query per un record TXT o un altro tipo di record diverso da A restituirebbe in modo analogo un indirizzo IPv4. Altri ricercatori hanno condotto studi longitudinali su larga scala sul GFW nel 2021 e sono giunti alla stessa conclusione.[14] Un anno prima, un diverso gruppo di ricercatori ha riportato una singola istanza di iniezione di record CNAME, ma non ha descritto la risposta.[15]

```
; <<>> DiG diggui.com <<>> @111.193.204.201 google.com MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62080
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;google.com.                    IN      MX

;; ANSWER SECTION:
google.com.             60      IN      A       59.24.3.174

;; Query time: 208 msec
;; SERVER: 111.193.204.201#53(111.193.204.201)
;; WHEN: Tue Jan 09 00:25:37 UTC 2024
;; MSG SIZE  rcvd: 54
```

Figura 3. Un indirizzo IP China Unicom restituisce un indirizzo IPv4 casuale in risposta a una query MX per `google[.]com`. *Una risposta corretta restituirebbe l'FQDN del mail server. Credito immagine:* `diggui[.]com`.

Questi esperimenti mostrano come funziona tipicamente il GFW. Inietta selettivamente risposte DNS per determinati nomi di dominio con risposte fuorvianti casuali. Quando inserisce pacchetti falsi, restituisce sempre un indirizzo IPv4 indipendentemente dal tipo di record richiesto. Muddling Meerkat, d'altra parte, fornisce record MX falsi correttamente formattati da indirizzi IP cinesi.

RECORD MX PER UN DOMINIO DI DESTINAZIONE

La caratteristica più notevole di Muddling Meerkat è la presenza di false risposte di record MX da indirizzi IP cinesi. Questo comportamento, mai pubblicato prima, differisce dal comportamento standard del GFW. Queste risoluzioni provengono da indirizzi IP cinesi che non ospitano servizi DNS e contengono risposte false, coerenti con il GFW. Tuttavia, a differenza del comportamento noto del GFW, le risposte MX di Muddling Meerkat non includono indirizzi IPv4 ma record di risorse MX formattati correttamente. Questa caratteristica è davvero notevole e in gran parte inspiegabile.

Utilizzerò uno dei tanti domini di destinazione di Muddling Meerkat, `kb[.]com`, per dimostrare la sua attività nel corso di questo documento. I record di risposta MX per Muddling Meerkat sono osservabili solo nei dati raccolti al di fuori della normale catena di risoluzione DNS, perché la fonte della risposta non è un resolver DNS, ma un indirizzo IP cinese casuale.

14 How Great is the Great Firewall? Measuring China's DNS Censorship. Nguyen Phong Hoang, et al., 30th USENIX Security Symposium (USENIX Security 21), https://www.usenix.org/system/files/sec21-hoang.pdf (ultimo accesso 9 gennaio 2024)

15 Anonimo, et al. Triplet Censors: Demystifying Great {Firewall{\textquoteright}s} {DNS} Censorship Behavior, 10th USENIX Workshop on Free and Open Communications on the Internet (FOCI 20), https://www.usenix.org/conference/foci20/presentation/anonymous (ultimo accesso 9 gennaio 2024)

Poiché i dati Infoblox derivano dai nostri resolver ricorsivi, ho collaborato con altri fornitori per ottenere i dati da analizzare.

Una terza parte ha fornito dati di query e risposta DNS contenenti record di risorse MX per il dominio `kb[.]com` per un periodo di 120 giorni che termina alla fine di gennaio 2024. In particolare, ogni log includeva una query DNS per il record MX di `kb[.]com` e una risposta contenente due record di risorse. I record di risorse erano formattati correttamente e contenevano FQDN con nomi host casuali di `kb[.]com`, in genere lunghi da tre a sei caratteri. Esempi di tali valori record MX includono:

- `pq5bo[.]kb[.]com`
- `uff0h[.]kb[.]com`
- `biuti[.]kb[.]com`
- `8jxg1x[.]kb[.]com`
- `8p0[.]kb[.]com`

Per chi non ha familiarità con i record MX, queste risposte dovrebbero essere l'FQDN del mail server per `kb[.]com`. Per recapitare la posta da un utente su una rete a un destinatario nella rete `kb[.]com` sono necessarie due query DNS. La prima è per i record MX del dominio di posta del destinatario, qui kb[.]com, e la seconda è per l'indirizzo IP dell'FQDN contenuto nel record MX. Una volta ottenuto l'indirizzo IP, il server SMTP (Simple Mail Transport Protocol) può inviare posta per conto di un utente (vedere Figura 4).

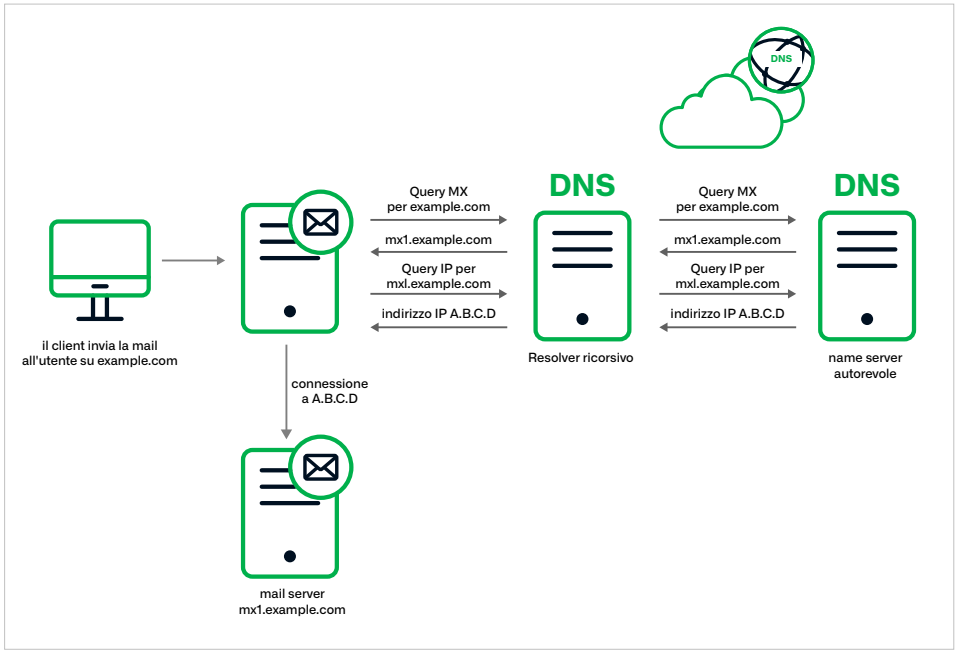

Figura 4. Il tipico processo di risoluzione DNS per trovare l'indirizzo IP di un mail server prevede che vengano effettuate sia query per un record MX che per un record A.

Nei dati di terze parti, i record MX formattati correttamente provengono da indirizzi IP cinesi casuali che *non* ospitano server DNS. Inoltre, queste risposte, pur sembrando corrette a prima vista, sono false. Il dominio `kb[.]com` dispone attualmente di name server autorevoli in Cina con NS1, un servizio di nomi autorevole che fa parte di IBM. Questi name server autorevoli non restituiscono alcuna risposta alle query di record MX per `kb[.]com`. Pertanto, abbiamo osservato risposte DNS provenienti dallo spazio IP cinese che differivano dal normale comportamento del GFW ed erano false.

I dati di terze parti contenevano non solo qualche record MX, ma migliaia. Ogni nome host all'interno del record MX storico è stato visualizzato in un singolo giorno durante questo intervallo di tempo, per un totale di oltre 8.000 FQDN univoci. Un secondo fornitore ha osservazioni simili. Le risposte contengono nomi host brevi e non sono duplicate. Il volume è notevole ma abbastanza piccolo, sicuramente troppo piccolo per essere efficace negli attacchi DDoS. Non solo le risposte sono false, ma anche le query stesse sono sospette. Il dominio `kb[.]com` era un tempo detenuto da una società di marketing statunitense, ma ora ospita servizi di gioco d'azzardo limitati geograficamente in lingua cinese. Non c'è motivo per i client di inviare posta al dominio, e soprattutto non c'è motivo di richiedere risoluzioni da indirizzi IP cinesi casuali. Come mostra la Figura 5, ci sono risoluzioni MX per ogni giorno nel campione, ma raramente ci sono più di 100 osservazioni al giorno.

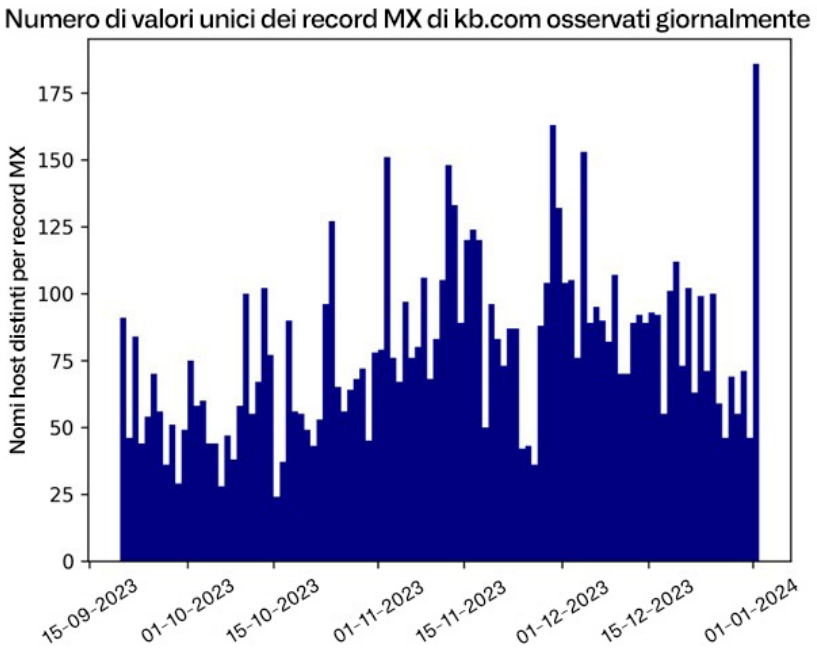

Figura 5. Il conteggio giornaliero dei valori unici dei record MX per kb[.]com nella raccolta globale pDNS. Si tratta di record MX falsi che non esistono nel file di zona del dominio.

Abbiamo anche analizzato le risposte storiche dei record MX di `kb[.]com` per diversi anni (Figura 6). I record MX contenenti un nome host casuale sono stati osservati per la prima volta il 15 ottobre 2019. Abbiamo verificato in modo indipendente con altri fornitori che le prime risoluzioni MX per i domini di destinazione di Muddling Meerkat sono state osservate per la prima volta il 15 ottobre 2019 o intorno a tale data. Questo è vero per tutti i domini di destinazione che abbiamo analizzato. Complessivamente, nei dati di terze parti, vediamo un inspiegabile aumento del numero di risoluzioni MX a partire dal 20 settembre 2023 e fino all'inizio del 2024.

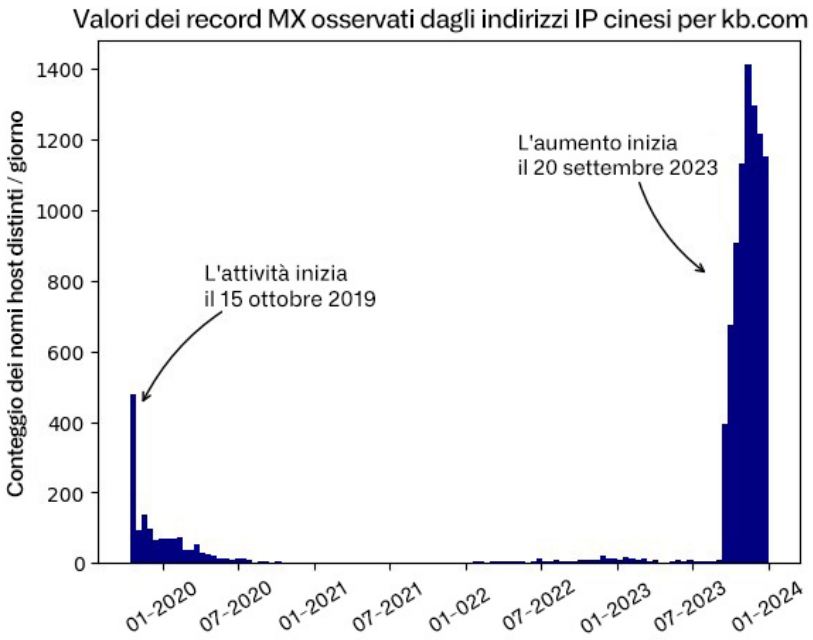

Figura 6. Conteggio dei valori di record MX falsi univoci per `kb[.]com`*, aggregati mensilmente nel tempo e osservati in raccolte di dati DNS di terze parti. Gli indirizzi IP di risposta per queste risoluzioni sono indirizzi IP cinesi casuali che non ospitano servizi DNS, il che implica che la risposta proviene dal Great Firewall. Sono tutti record MX falsi che non esistono nel file di zona DNS di* `kb[.]com`*.*

È improbabile che un resolver ricorsivo o un altro server lungo un normale percorso di risoluzione DNS abbia visto queste risposte. Confrontando l'intera cronologia dei record MX per `kb[.]com` sia da Infoblox che da DomainTools Farsight, abbiamo visto solo una manciata di record unici. A gennaio 2024, il name server per `kb[.]com` non risponde alle richieste di record MX dei nostri resolver. In passato, i server autorevoli hanno restituito risposte contenenti questi valori:

- `mail.kb[.]com`, `smtp1[.]com`, `smtp2[.]com`, `smtp3[.]com`

Sebbene i name server autorevoli per `kb[.]com` non rispondano alle query MX attraverso il processo ufficiale di risoluzione DNS, i nostri resolver ricorsivi ricevono richieste per questi record. In circostanze normali, la ricezione di queste richieste implica che gli utenti delle nostre reti di clienti devono inviare e-mail a un utente di `kb[.]com`. Ma `kb[.]com` non fornisce servizi di posta elettronica. I registri DNS passivi contengono molte cose strane e le query possono essere attivate da vecchie applicazioni o siti web. Tuttavia, in questo caso, le query si verificano esattamente a distanza di un mese l'una dall'altra nell'arco di diversi mesi, il che contribuisce ad aumentare la curiosità. Come vedremo da altri dati nella prossima sezione, questo comportamento è molto probabilmente innescato da Muddling Meerkat che sonda le reti dei nostri clienti alla ricerca di resolver aperti e occasionalmente ne trova alcuni.

Non sono stata in grado di attivare manualmente false risposte MX dal GFW, per i domini di destinazione di Muddling Meerkat o altri. Forse i record sono prodotti invece dal GC o in un contesto operativo specifico di Muddling Meerkat. Ad esempio, le risposte potrebbero essere attivate da firme all'interno del pacchetto IP che identificano l'attore. Sappiamo che i pacchetti IP di ExploderBot contenevano diversi artefatti che potevano servire come controllo della fonte, se lo si desiderava. La comparsa di tali tracce identificative potrebbe spiegare perché altri ricercatori hanno visto iniezioni di CNAME, ma solo raramente. Purtroppo, si tratta di speculazioni basate su esperienze precedenti e su possibili spiegazioni di comportamenti aberranti da parte del GFW/GC. Sebbene le risposte stesse possano essere pacchetti IP falsi, il rasoio di Occam indica una variante del GFW, forse il GC. Molte cose sono possibili, ma poche sono plausibili.

RECORD MX PER UN SOTTODOMINIO CASUALE

Il secondo componente identificativo delle operazioni di Muddling Meerkat coinvolge anche le query dei record MX, ma per un sottodominio casuale del dominio di destinazione, piuttosto che per il dominio di base stesso. In questo caso, in circostanze normali, la query verrebbe attivata da un utente che desidera inviare e-mail non al dominio di base, ma a un sottodominio. Sebbene questo scenario si verifichi nel normale DNS, non è particolarmente comune. Nella maggior parte dei domini di destinazione di Muddling Meerkat, non esiste un mail server funzionale, il che crea una situazione ancora più anomala. In effetti, le query per i record MX di sottodomini casuali di `kb[.]com` sono ciò che ha portato a questa intera indagine.

I fenomeni che osserviamo nei nostri resolver ricorsivi sono un piccolo numero di richieste che si verificano nell'arco di uno o tre giorni con nomi host casuali. Queste richieste includono altri tipi di query oltre ai record MX, ma a causa della natura specifica dei record MX nelle normali operazioni di rete, riporto solo i risultati su questo tipo. Le query MX hanno questa forma:

```
<random>.target_domain
```

dove `random` è una stringa alfanumerica di lunghezza variabile, in genere compresa tra tre e sei caratteri.

Sebbene questa indagine sia iniziata con `kb[.]com`, ci sono circa 10 domini di destinazione di Muddling Meerkat osservati nelle reti dei nostri clienti dal 1° settembre 2023. Le Figure 7 e 8 mostrano il volume delle query MX per `kb[.]com` e `4u[.]com` osservate presso i nostri resolver ricorsivi tra il 1° settembre e il 31 dicembre, insieme ad alcuni FQDN campione interrogati in giorni specifici. In questo periodo di quattro mesi, nessun sottodominio si ripete. I nostri partner di DomainTools Farsight e altri fornitori non divulgati osservano le stesse tendenze, anche se con sottodomini casuali diversi.

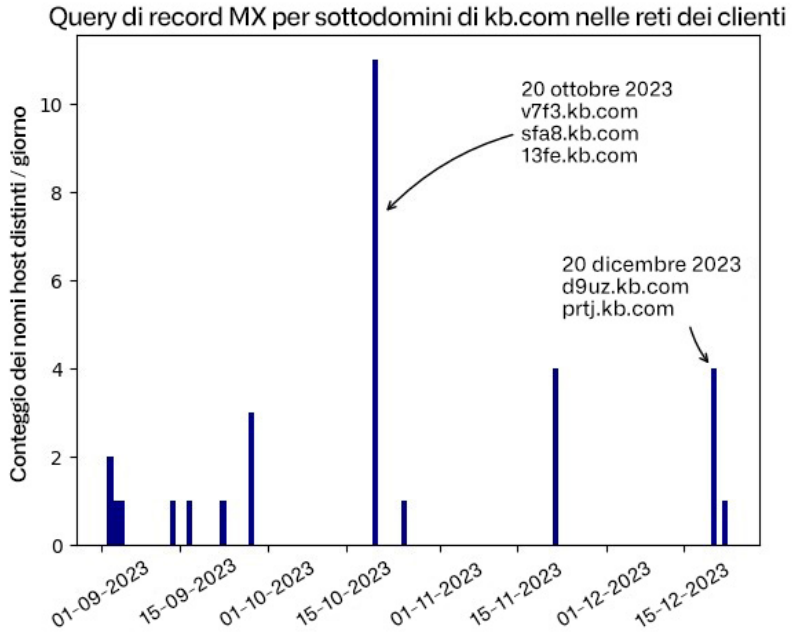

Figura 7. Il numero di FQDN distinti con query di record MX per `kb[.]com` osservati nei resolver ricorsivi di Infoblox durante quattro mesi

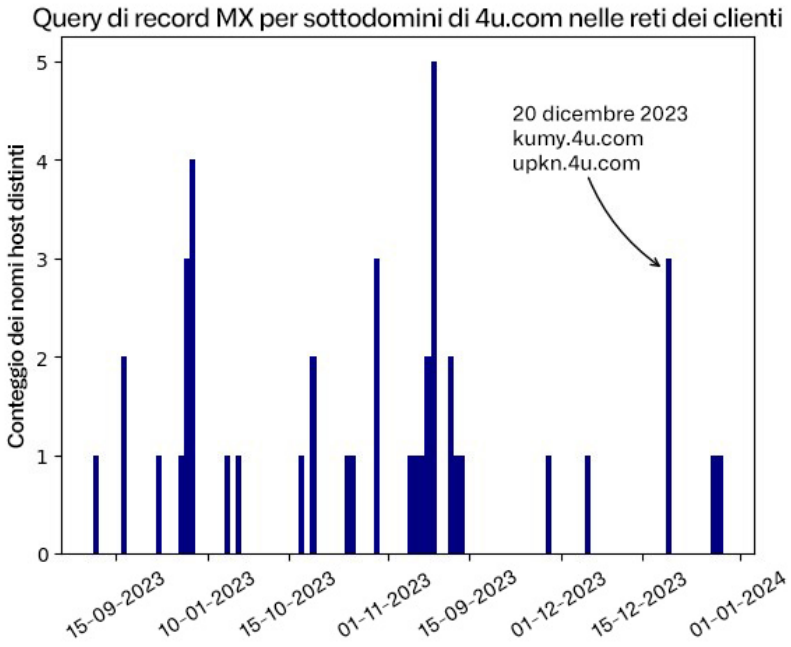

Figura 8. Il numero di FQDN distinti con query di record MX per `4u[.]com` *osservati nei resolver ricorsivi di Infoblox in un periodo di quattro mesi*

Le Figure 7 e 8 dimostrano la natura aperiodica "pop-up" delle query su Muddling Meerkat con un tempo operativo che dura da uno a tre giorni e utilizza nomi host casuali. Questo tipo di schema è tipico degli attacchi DDoS Slow Drip in generale e di ExploderBot in particolare. Tuttavia, ci sono alcune differenze significative tra quanto riportato in precedenza in altri documenti e questi attacchi. In particolare, in questi attacchi, i volumi sono molto inferiori a quelli che ci aspetteremmo da un vero tentativo di DDoS e da quelli visti negli attacchi su larga scala al culmine di questa attività tra il 2014 e il 2017.

In uno studio longitudinale pubblicato sulla rivista *Digital Threats Research and Practice* nel 2019, ho notato che il panorama degli attacchi DDoS Slow Drip era cambiato in modo significativo dal nostro primo articolo su ExploderBot.[16] In quella ricerca, condotta nell'arco di sei mesi nel 2018, sono stati osservati diversi tipi di query, ma MX non era uno di questi. I modelli dominanti descritti in quell'articolo si osservano ancora oggi, con bassi livelli di query con nomi host lunghi e una forte distorsione nelle distribuzioni dei caratteri. Muddling Meerkat non ha nulla a che vedere con queste tendenze.

RECORD IPV4 PER SOTTODOMINI CASUALI

Oltre alle query MX per sottodomini casuali del dominio di destinazione, i nostri resolver ricorsivi ricevono richieste di record A o indirizzi IPv4. Ovviamente, queste query non ricevono risposte dai nostri resolver perché non esiste un sottodominio di questo tipo configurato nel name server autorevole. Altri fornitori la cui raccolta proviene da resolver ricorsivi hanno osservazioni simili. I dati di DomainTools Farsight, ad esempio, provengono da una raccolta di resolver ricorsivi a livello globale. Come Infoblox, questi fornitori registrano picchi regolari di query per sottodomini casuali dei domini Muddling Meerkat, incluse le query per i record A. La Figura 9 mostra queste tendenze per un mese, gennaio 2024.

16 Renée Burton. 2018. Unsupervised Learning Techniques for Malware Characterization: Understanding Certain DNS-based DDoS Attacks. Digit. Threat. Res. Pract. 37, 4, Articolo 111 (Agosto 2018), 27 pagine. https://dl.acm.org/doi/10.1145/3377869

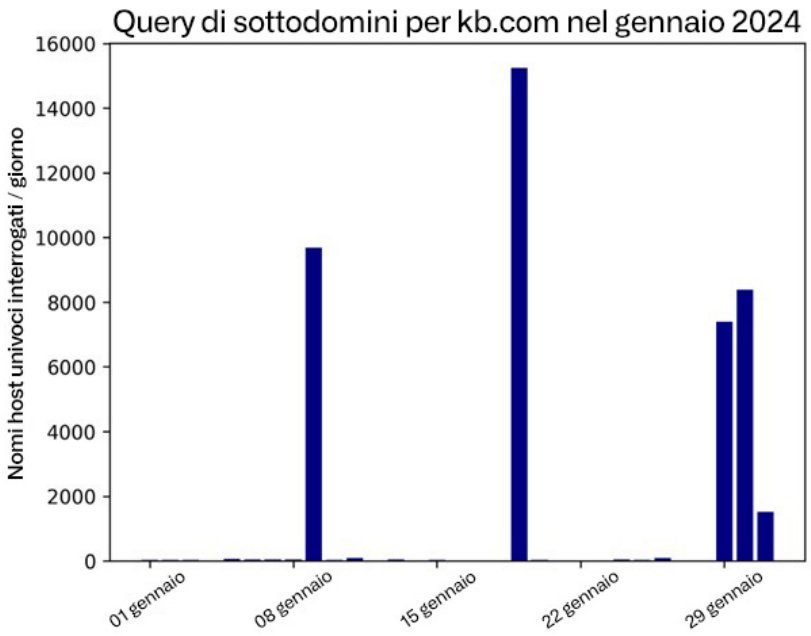

Figura 9. Query di nomi host univoci di `kb[.]com` *osservate nel pDNS Farsight a gennaio 2024*

Esistono anche altri tipi di raccolta con visibilità sul DNS, tra cui la raccolta di pacchetti, gli honeypot e internet telescopes. Partendo dalla teoria che la fonte di queste query all'interno delle nostre reti fossero i resolver aperti e che Muddling Meerkat probabilmente stesse sondando un ampio spettro di spazio IPv4 per i resolver aperti, ho chiesto ad altri fornitori di aiutarmi a localizzare i pacchetti che contenevano record di risorse nella risposta. Abbiamo trovato risposte con record A, proprio come abbiamo trovato risposte con record MX.

Gli unici indirizzi IP che hanno risposto alle query per i record A dei domini Muddling Meerkat si trovavano nello spazio IP cinese. Questi indirizzi IP non erano aperti sulla porta 53, il che significa che non erano resolver DNS. In altre parole, queste risposte provenivano dal GFW e non dai server autorevoli.

Il GFW è noto per iniettare risposte alle query DNS con indirizzi IP di risoluzione non del tutto casuali. In uno studio longitudinale di nove mesi e pubblicato nell'agosto 2021 per il 30° Usenix Security Symposium, i ricercatori hanno scoperto che gli indirizzi IP contraffatti apparivano spesso ripetutamente per determinati gruppi di domini.[17]

Utilizzando le risoluzioni IP dei sottodomini di `kb[.]com`, abbiamo mappato l'occorrenza di un indirizzo IP di risoluzione contraffatto con la sequenza temporale delle query. In ogni caso, l'indirizzo IP di risoluzione viene visualizzato ripetutamente, con finestre temporali distinte della durata di uno o tre giorni, per brevi sottodomini casuali. Le Figure 10 e 11 mostrano due esempi di questo comportamento. I due indirizzi IP non sono in realtà correlati a `kb[.]com`; queste sono risposte false da parte del GFW. Entrambi gli indirizzi IP vengono visualizzati in giorni sovrapposti. Ogni figura mostra l'insieme delle risoluzioni per `kb[.]com` a quell'indirizzo IP nel 2022. Come per i dati del resolver Infoblox e Farsight, il nome host, o sottodominio, non viene ripetuto.

17 How Great is the Great Firewall? Measuring China's DNS Censorship. Nguyen Phong Hoang, et al., 30th USENIX Security Symposium (USENIX Security 21), https://www.usenix.org/system/files/sec21-hoang.pdf (ultimo accesso 9 gennaio 2024)

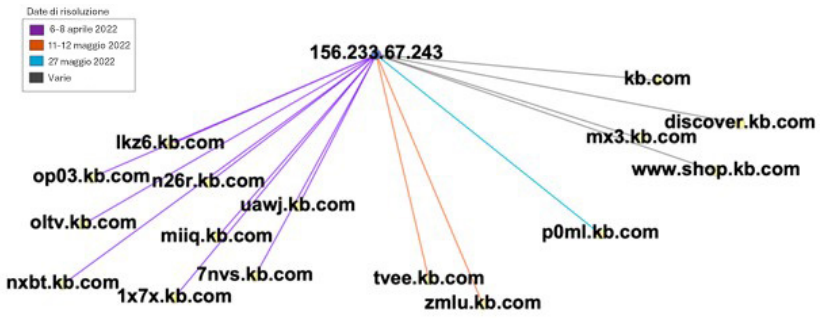

Figura 10. Risoluzioni dei nomi host da parte del GFW all'interno del dominio `kb[.]com` *all'indirizzo IP 156[.]233[.]67[.]243 nel 2022. Questo indirizzo IP non è correlato a* `kb[.]com` *e la risposta è falsificata dal GFW.*

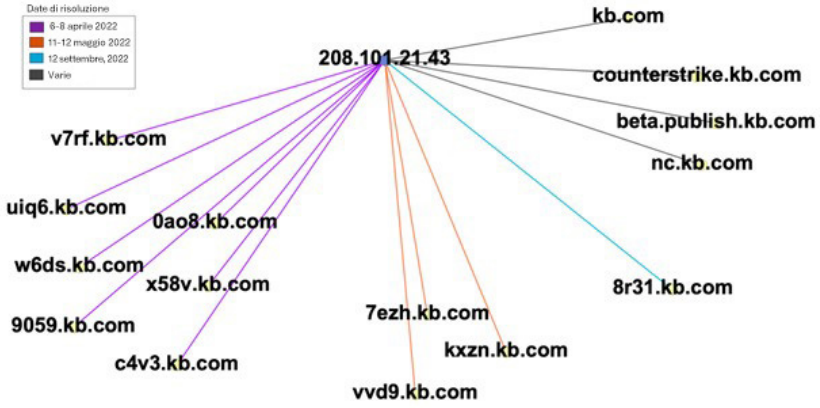

Figura 11. Risoluzioni dei nomi host da parte del GFW all'interno del dominio `kb[.]com` *all'indirizzo IP 208[.]101[.]21[.]43 nel 2022. Questo indirizzo IP non è correlato a* `kb[.]com` *e la risposta è falsificata dal GFW.*

Questi risultati indicano che Muddling Meerkat sta conducendo operazioni che includono query DNS a un gran numero di indirizzi IP di destinazione, indipendentemente dalla loro posizione o dalle porte aperte, e che il GFW sta iniettando risposte in questi domini in giorni specifici con una serie di indirizzi IP che vengono utilizzati nel tempo. Questa stessa attività e questo tipo di risposte sono in corso nel gennaio 2024. Sebbene queste cifre mostrino le risoluzioni per `kb[.]com`, abbiamo verificato lo stesso schema per tutti i domini di destinazione noti di Muddling Meerkat.

Ecco dove le cose si fanno interessanti: il GFW normalmente non inietta risposte per `kb[.]com` o qualsiasi sottodominio. Il GFW non sta iniettando risposte false in qualsiasi richiesta di sottodominio casuale di `kb[.]com`, ma solo in quelle create da Muddling Meerkat! Come abbiamo discusso in precedenza, il GFW inietta risposte a domini popolari o a domini che trova in qualche modo discutibili per gli interessi cinesi. Il suddetto documento Usenix convalida questo fatto. La Figura 12 mostra la risposta il 13 gennaio 2024 a una query di record A per `nxbt.kb[.]com` dall'indirizzo IP 111[.]193[.]204[.]201 che abbiamo usato in precedenza per ottenere risposte false a `google[.]com`.

```
; <<>> DiG diggui.com <<>> @111.193.204.201 nxbt.kb.com A
; (1 server found)
;; global options: +cmd
;; connection timed out; no servers could be reached
```

Figura 12. La risposta a una richiesta di record A da 111[.]193[.]204[.]204 per `nxbt[.]kb[.]com`*. Questo indirizzo IP è nello spazio degli indirizzi IP cinesi e non è aperto sulla porta 53. La risposta è ciò che ci si aspetta da una query di questo tipo ed è coerente con il comportamento noto del GFW. Credito immagine:* `diggui.com`*.*

DOMINI DI DESTINAZIONE DI MUDDLING MEERKAT

La scelta dei domini di destinazione di Muddling Meerkat dimostra la sofisticazione del DNS. Gli operatori di Muddling Meerkat inducono risposte selettive da parte del GFW che non si verificano nella normale censura del GFW. Per fare ciò, hanno scelto domini di destinazione che non controllano, che è molto improbabile che le appliance di sicurezza blocchino. Inoltre, utilizzano tipi di query che non vengono comunemente monitorati e creano un volume di query che si fonde con il normale traffico DNS. Abbiamo osservato nomi host casuali con tipi di query A (IPv4), CNAME, MX e AAAA (IPv6) presso i resolver Infoblox.

Le query di sottodomini casuali che abbiamo osservato sono per domini che sono stati registrati per 20 anni o più, hanno etichette brevi e si trovano nei domini di primo livello .com e .org. Le etichette del dominio di destinazione sono per lo più lunghe due o tre caratteri, ma ho visto alcuni esempi che erano di quattro caratteri (ad esempio, `boxi[.]com`). Nella maggior parte dei casi, i domini sono passati di mano nel tempo, ma la data di creazione originale verrà comunque mostrata in WHOIS. Gli esempi includono `kb[.]com`, `4u[.]com`, `id[.]com`, `od[.]com`, `ntl[.]com` e `nef[.]com`. Questi domini sono stati tutti osservati nel traffico di Muddling Meerkat presso i resolver Infoblox nei mesi di dicembre 2023 e gennaio 2024.

Ho verificato circa 20 domini di destinazione in più fonti; tuttavia, probabilmente ce ne sono molti di più. È difficile isolare i domini di destinazione per diversi motivi che introdurrò qui e discuterò più approfonditamente più avanti nella sezione intitolata Il ruolo degli indirizzi IP cinesi. Innanzitutto, non tutti i domini che soddisfano i criteri di base di età e lunghezza sembrano essere presi di mira. Ad esempio, non ho trovato prove che `rr[.]com`, `ibm[.]com` e `aol[.]com` vengono utilizzati nelle operazioni di Muddling Meerkat, sebbene soddisfino i requisiti di base (*sì*, `aol[.]com` *si verifica ancora nel traffico DNS*). La maggior parte dei domini che si trovano nelle query presso i nostri resolver ricorsivi non sono in uso (ad esempio, `4u[.]com`) o non sono particolarmente popolari tra i clienti. Molti, come `kb[.]com` e `od[.]com`, sono utilizzati per siti di gioco d'azzardo offshore in lingua cinese. Alcuni, come `ni[.]com`, di proprietà di National Instruments, sono domini ben consolidati e molto utilizzati.

La scelta di utilizzare domini brevi e di lunga data in TLD (top-level domain) ben noti è intelligente per più motivi, oltre che per la ridotta probabilità di essere bloccati dalle appliance di sicurezza. Domini con queste caratteristiche vengono spesso utilizzati anche:

- da organizzazioni come domini di ricerca DNS o domini di Active Directory e
- nei malware, per creare piste false per gli investigatori

Di conseguenza, un analista SOC (Security Operation Center) che nota query sospette verso questi domini di destinazione sarà ostacolato dalle numerose fonti potenziali di malware che potrebbero essere collegate alla query. Ad esempio, il dominio `kb[.]com` ha oltre 30 file che vi fanno riferimento e 7 file che comunicano con esso, nei campioni archiviati dal fornitore VirusTotal.[18] Il dominio `od[.]com` mostra oltre 130 file di riferimento.[19] Molti di questi sono vecchi campioni di malware e contribuiscono ad aumentare le interferenze.

D'altra parte, un ricercatore come me, che cerca di comprendere un quadro più olistico dell'attività, dovrà filtrare le query DNS non correlate per isolare i veri domini di destinazione. Questo tipo di dominio è comunemente utilizzato per Active Directory da un'organizzazione, anche se non controlla il dominio (*una pratica rischiosa!*). Inoltre, le applicazioni, i siti web e le persone possono generare query inusuali nel DNS. Tra i tipi di query utilizzate da Muddling Meerkat, MX è il più facile da analizzare.

18 https://www.virustotal.com/gui/domain/kb.com/relations

19 https://www.virustotal.com/gui/domain/od.com/relations

Per fornire una prospettiva, ho esaminato le risoluzioni MX presso i resolver ricorsivi Infoblox che si sono verificate durante sei settimane a partire dal 1° dicembre 2023. Quando pensiamo ai domini dei mail server, non ci aspettiamo di vedere una grande varietà. Ma questa aspettativa si rivela essere un pregiudizio cognitivo. Ho contato il numero di domini di secondo livello con le seguenti condizioni che sono simili a Muddling Meerkat:

- nel dominio di primo livello .com e .org
- restituiscono risposte NXDOMAIN
- hanno più di 10 nomi host diversi

Più di 1.100 domini hanno soddisfatto i criteri. In breve, molti domini hanno query MX anomale. Da quei 1.100, ho ridotto il set per includere solo quelli in cui l'etichetta del dominio era inferiore a quattro caratteri. Ciò ha portato alla selezione di 55 candidati e a oltre 22.000 query uniche durante il periodo di studio. Da questo set di candidati, ho condotto ulteriori analisi per confermare i domini di destinazione utilizzando una varietà di altre funzionalità.

IL RUOLO DEI RESOLVER APERTI

Un resolver aperto è un dispositivo su un indirizzo IP che risponderà alle query di qualsiasi client, ma non è configurato intenzionalmente come resolver ricorsivo per servire il pubblico in generale. Al contrario, un resolver pubblico in DNS è un resolver ricorsivo progettato per rispondere alle query di qualsiasi client ed è in genere gestito da una grande azienda, come Google, Cloudflare o Yandex. Alcuni ricercatori includono i resolver pubblici nella loro definizione di resolver aperti, ma io no. I resolver aperti sono noti punti di sfruttamento per gli attacchi DDoS. Possono essere utilizzati per amplificare gli attacchi contro le vittime negli attacchi di reflection, in cui le query DNS vengono effettuate tramite resolver aperti con fonti falsificate contenenti l'indirizzo IP della vittima.[20] Sono utilizzati anche negli attacchi Slow Drip per distribuire le interrogazioni al name server autorevole di proprietà della vittima e nelle varianti degli attacchi contro l'infrastruttura intermedia.[21]

Utilizzo il termine *indirizzo IP* per descrivere i resolver aperti piuttosto che un resolver DNS, perché i resolver aperti sono molto complessi. Ad esempio, potrebbe esserci un'appliance Internet, come un firewall, davanti all'indirizzo IP del resolver aperto che può intercettare le query e poi, proprio come il GFW, falsificare una risposta, facendo credere che l'indirizzo IP di destinazione originale abbia risposto alla query DNS. La risposta restituita può essere corretta o meno. Questo comportamento è simile a quello descritto dai ricercatori sull'intercettazione delle query DNS da parte dei provider di servizi Internet (ISP).[22]

I resolver aperti contribuiscono agli attacchi DDoS e ne ostacolano l'analisi. Creeranno traffico aggiuntivo verso i server root e TLD perché non hanno l'ampiezza di una cache DNS che avrebbe un resolver pubblico, costringendoli spesso a eseguire una risoluzione completa. In base alla mia esperienza nell'analisi del traffico dei resolver aperti, molti hanno altre configurazioni errate nel loro DNS, che creano traffico aggiuntivo, in genere non necessario. Ad esempio, potrebbero non memorizzare nella cache gli hint di root e interrogare continuamente gli indirizzi IP del server root. Se combinati con il potenziale di risposte falsificate, i resolver aperti creano un sacco di interferenze e producono false piste per i ricercatori.

---

20 A Matter of Degree: Characterizing the Amplification Power of Open DNS Resolvers, Yazdani, et al. Nature Switzerland AG 2022 O. Hohlfeld et al. (Eds.): PAM 2022, LNCS 13210, pagg. 293–318, 2022. https://doi.org/10.1007/978-3-030-98785-5_13. https://annasperotto.org/publication/papers/2022/yazdani-pam-2022.pdf (ultimo accesso 14 gennaio 2024)

21 NRDelegation Attack: Complexity DDoS Attack on DNS Recursive Resolvers, Yehuda Afek, et al., 32nd Usenix Security Symposium, 2023 https://www.usenix.org/conference/usenixsecurity23/presentation/afek (ultimo accesso 14 gennaio 2024)

22 Who is Answering My Queries: Understanding and Characterizing Interception of the DNS Resolution Path, Baujun Lui, et al., 27th Usenix Conference, 2018 https://www.usenix.org/conference/usenixsecurity18/presentation/liu-baojun (ultimo accesso 14 gennaio 2024)

Ho incontrato per la prima volta i resolver aperti mentre studiavo gli attacchi DDoS di ExploderBot. In questi attacchi, i pacchetti IP contenenti query DNS per sottodomini casuali di un dominio di destinazione sono stati rilasciati su Internet vicino alla dorsale in varie posizioni. Sia l'indirizzo IP di origine che quello di destinazione sono stati falsificati e, se presi insieme nel tempo, hanno coperto una grande quantità di spazio di indirizzi IPv4. Nella nostra ricerca, abbiamo riscontrato tutti i problemi sopra citati, comprese le risposte falsificate dal GFW e dai resolver aperti. ExploderBot ha condotto questi attacchi in genere per alcuni giorni, ma erano aperiodici. Prima del 2016, c'erano operazioni molte volte al mese, ma queste sono rallentate negli anni successivi e sono diventate molto irregolari. Pur essendo apparentemente un attacco DDoS a un name server autorevole, il danno maggiore causato da ExploderBot è stato all'infrastruttura dell'ISP, inclusi resolver ricorsivi e bilanciatori di carico. Senza resolver aperti, gli attacchi ExploderBot non sarebbero stati degni di nota, ma per diversi anni, sebbene non associati al nome di un attore, la loro attività è stata trattata da blog e resoconti dei media. Si ritiene che ExploderBot sia inattivo; l'ultima attività è stata osservata da Infoblox il 18 maggio 2018.

I resolver aperti svolgono anche un ruolo importante nelle operazioni di Muddling Meerkat. L'evidenza suggerisce che le query vengono inviate a un'ampia gamma di indirizzi IP, molti dei quali resolver aperti, dallo spazio IP cinese. Gli indirizzi IP di destinazione per le query DNS probabilmente ruotano nel tempo, il che crea una firma "pop-up" nei resolver ricorsivi come Infoblox. In altre parole, sospetto che Muddling Meerkat stia interferendo attivamente con Internet più spesso di quanto osserviamo con i resolver cloud di Infoblox. Sospetto inoltre che a certi intervalli, della durata di alcuni giorni alla volta, gli indirizzi IP esterni appartenenti ai nostri clienti siano inclusi nelle destinazioni di Muddling Meerkat (questa è una speculazione da parte mia; non ho la visibilità dei dati per vedere l'intera gamma delle attività). Alcuni dei nostri clienti hanno inconsapevolmente resolver aperti nella loro rete che ricevono le loro query e le inoltrano ai nostri resolver per la risoluzione. Indipendentemente dal ritmo operativo, vedremo solo le query di Muddling Meerkat sui nostri resolver quando un dispositivo del cliente le inoltra.

Muddling Meerkat abusa di molti resolver aperti. Alcuni sono server stabiliti in un data center, mentre altri sono router domestici. Ad esempio, abbiamo osservato una serie di indirizzi IP che sono stati identificati come router MikroTik da Shodan.[23] A gennaio 2024, questi indirizzi IP includevano query provenienti dai resolver aperti campione riportati nella Tabella 1.

Indirizzo IP richiedente	Nome della query
23[.]173[.]112[.]115	92ac[.]kb[.]com, mi2w[.]kb[.]com, 3k04[.]kb[.]com
103[.]47[.]134[.]195	zve3[.]kb[.]com, rjlf[.]kb[.]com, mayf[.]kb[.]com
38[.]54[.]105[.]163	q0ce[.]kb[.]com, h5ow[.]kb[.]com, 4e5r[.]kb[.]com

Tabella 1. Esempi di indirizzi IP e query osservati nel gennaio 2024; questi indirizzi IP ospitavano tutti resolver aperti al 31 gennaio 2024

NESSUN INDIRIZZO RICHIEDENTE FALSIFICATO

Grazie alla mia esperienza con ExploderBot, ero predisposta a pensare che Muddling Meerkat stesse iniettando query DNS su Internet utilizzando indirizzi IP richiedenti falsificati e un ampio spettro di indirizzi IP destinatari. Le prove che abbiamo scoperto, tuttavia, indicavano il contrario: alcuni indirizzi IP cinesi erano la fonte di un numero sproporzionato di query DNS. Sulla base dei dati (vedi la Tabella 2 per gli esempi), sembrava più probabile che Muddling Meerkat utilizzasse server dedicati per le proprie operazioni. Nonostante la controprova, abbiamo voluto verificare l'ipotesi degli indirizzi richiedenti falsificati. Il modo

23 Shodan.io è un motore di ricerca disponibile al pubblico per gli attributi del server in base all'indirizzo IP.

migliore per farlo è il cosiddetto **telescopio di rete**,[24] che sfrutta gli indirizzi IP inutilizzati verso i quali non dovrebbe esserci traffico e raccoglie i pacchetti che vengono indirizzati a loro. I telescopi di rete sono utili per catturare eventi su larga scala che sfruttano indirizzi IP falsificati. Un certo numero di operatori di telescopi di rete, tra cui Merit Network, sono in grado di osservare il traffico verso circa 11 milioni di indirizzi IP. Anche se questi indirizzi IP sono tecnicamente inutilizzati, ricevono un'enorme quantità di traffico contenente un'ampia varietà di protocolli.

Nel contesto di una query DNS falsificata, la sequenza di eventi sarebbe simile a questa:

- L'aggressore inietta un pacchetto IP che contiene una query DNS presumibilmente proveniente dall'indirizzo IP A e diretta all'indirizzo IP B.
- Supponendo che l'indirizzo IP B sia un resolver DNS o un proxy invisibile come il GFW, un pacchetto di risposta viene inviato da B ad A.
- Questo pacchetto di risposta viene ricevuto da A e viene chiamato backscatter sul telescopio perché è un riflesso verso un indirizzo che non ha avviato la comunicazione.

Gli operatori di telescopi di rete possono quindi misurare gli eventi Internet in base al backscatter che ricevono. Questi operatori hanno una finestra sul traffico Internet, e su determinati attacchi, che è unica.

I ricercatori di Merit Network non sono riusciti a trovare prove delle risposte di Muddling Meerkat nei loro dati backscatter. Successivamente, i ricercatori di Merit Network hanno contattato gli operatori di un altro grande telescopio di rete presso il Center for Applied Data Analysis (CAIDA), per verificare se Muddling Meerkat avesse falsificato gli indirizzi IP richiedenti negli intervalli monitorati dal telescopio CAIDA.[25] Il CAIDA non ha catturato alcun backscatter associato a questa attività. Quando combiniamo i loro risultati con le osservazioni precedenti di query DNS su larga scala innescate da indirizzi IP cinesi, siamo certi che Muddling Meerkat non stia ampiamente falsificando gli indirizzi IP richiedenti nelle sue operazioni. Questa è una differenza sostanziale tra Muddling Meerkat ed ExploderBot.

IL RUOLO DEGLI INDIRIZZI IP CINESI

A causa della complessità delle operazioni di Muddling Meerkat e dell'impatto del GFW, è difficile determinare se eventi specifici con indirizzi IP cinesi siano "reali". Ciò che intendo qui con "reale" è che potrebbe non essere chiaro se un indirizzo IP specifico stia "rispondendo" a una query come risultato del GFW. Allo stesso modo, può essere difficile separare gli indirizzi IP falsificati da quelli che hanno originato le query.

Il nostro approccio a questo problema è stato quello di trarre conclusioni dalle statistiche generali. Come spiegato in precedenza, nella sezione intitolata Record IPv4 per sottodomini casuali, abbiamo osservato che gli indirizzi IP cinesi hanno "risposto" alle query di Muddling Meerkat in cui è noto che quell'indirizzo IP non ha la porta 53 aperta. Con un gran numero di esempi di questo tipo, possiamo concludere che le "risposte" sono risultati del GFW e non risposte "reali".

Quando esaminiamo il comportamento degli indirizzi richiedenti, spiccano alcuni indirizzi IP. Questi indirizzi IP si verificano con una frequenza molto più elevata rispetto agli IP dei resolver aperti. Sono la fonte di query che non rientravano nella normale risoluzione del DNS, inclusi gli indirizzi IP che ospitavano resolver aperti. Alcuni di questi indirizzi IP richiedenti sono stati ripetutamente segnalati per scansioni aggressive e altre pratiche discutibili.[26] La Tabella 2 presenta un esempio di indirizzi IP sorgente e query.

24 https://en.wikipedia.org/wiki/Network_telescope

25 https://www.caida.org/

26 https://www.abuseipdb.com/check/183.136.225.14?page=8

Indirizzo IP richiedente	Nome della query
183[.]136[.]225[.]45	ybzz[.]kb[.]com, xv9k[.]kb[.]com, 0h5w[.]kb[.]com
183[.]136[.]225[.]14	y4fw[.]kb[.]com, mq5i[.]kb[.]com, h420[.]kb[.]com

Tabella 2. Esempi di indirizzi IP e query osservati nel gennaio 2024. Questi indirizzi IP non ospitavano resolver aperti al 31 gennaio 2024. Alcune di queste query erano indirizzate a resolver aperti noti.

INDIVIDUAZIONE DELL'ATTIVITÀ DI MUDDLING MEERKAT

Possiamo osservare Muddling Meerkat in parte da diverse fonti. I resolver ricorsivi, come il nostro, possono osservare sia le query per i sottodomini casuali, sia le query per i record MX dei domini di destinazione. Se risolte tramite il DNS globale, la maggior parte di queste query genererà una risposta NXDOMAIN. Se non ci sono resolver aperti o pubblici nella rete, molto probabilmente Muddling Meerkat non sarà visibile nei log DNS. Sfortunatamente, molti sistemi di registrazione DNS registrano solo risoluzioni riuscite e i proprietari di rete potrebbero non vedere l'attività a causa di questa limitazione.

Per coloro che possono osservarle, è probabile che le query Muddling Meerkat appaiano in modo intermittente, come negli esempi delle Figure 6 e 7, e dipendano dalle dimensioni della rete. In Infoblox, vediamo più traffico Muddling Meerkat rispetto a un'organizzazione tipica perché risolviamo le richieste DNS per i clienti di tutto il mondo. I nostri resolver ricorsivi cloud hanno gestito oltre 33 trilioni di query solo nel 2023.

Oltre ai log delle query DNS, i ricercatori dovrebbero essere in grado di trovare tracce di Muddling Meerkat in una serie di altre fonti:

- I name server root, TLD e name servers autoritativi conterranno tutti prove dell'attività di Muddling Meerkat risalente a ottobre 2019 e forse anche prima. Poiché l'attore non controlla i domini di destinazione e sta interrogando ampi intervalli IP per i record, i resolver aperti inoltreranno le query e genereranno richieste in ogni server all'interno della catena di risoluzione.
- Anche le cache dei resolver ricorsivi catturano le prove di Muddling Meerkat.
- I proprietari di un honeypot DNS riceveranno probabilmente query a seconda dell'ampiezza con cui Muddling Meerkat interroga gli indirizzi IP.
- I dati di flusso possono contenere indicazioni di attività, in particolare se monitorano lo spazio IP cinese o mostrano un'insolita varietà di connessioni sulla porta 53 ai name server autoritativi, in particolare derivanti da indirizzi IP di resolver aperti.

Le query a uno qualsiasi dei domini indicati alla fine del presente rapporto devono essere considerate sospette. Ma è necessario tenere presente l'ampio uso di questi domini per i domini di ricerca Active Directory e DNS. Oltre al dominio di destinazione, dovrebbero essere presenti query di record MX, in particolare per sottodomini casuali brevi. Ci sono altre query sospette per un sottoinsieme dei domini Muddling Meerkat, che non sono incluse in questo report. Si tratta di query di record A che sembrano far trapelare informazioni di rete al server autorevole. Tuttavia, non sono in grado di collegare definitivamente questa attività a Muddling Meerkat.

ATTRIBUZIONE E MOTIVAZIONE

Sembra che Muddling Meerkat sia un attore statale cinese. Poiché possiamo osservare le risposte dei record MX da indirizzi IP cinesi che non sono aperti sulla porta 53 dei domini di destinazione di Muddling Meerkat per diversi anni, sono fiduciosa che tali risposte siano i risultati del GFW. Allo stesso tempo, non sono mai state riportate risposte MX adeguate da parte del GFW e i ricercatori, me compresa, non sono stati in grado di attivare il comportamento manualmente. Al fine di indurre risposte selettive come quelle che abbiamo osservato nel corso di quattro anni, sembra che Muddling Meerkat debba essere in qualche modo collegato agli operatori del GFW. Anche se non so come vengano attivate queste risposte selettive, è possibile che le firme contenute nei pacchetti IP, come quelle osservate nel traffico di ExploderBot, vengano utilizzate per segnalare una risposta diversa dal GFW.

La motivazione di queste operazioni non è chiara. I dati in nostro possesso suggeriscono che le operazioni vengono eseguite in "fasi" indipendenti; alcune includono query MX per i domini di destinazione e altre includono una serie più ampia di query per sottodomini casuali. I dati degli eventi DNS contenenti i record MX del GFW si verificano spesso in date separate da quelle in cui vengono visualizzate le query MX nei resolver aperti. Poiché i nomi di dominio sono gli stessi in tutte le fasi e le query sono coerenti tra i nomi di dominio, entrambi per un periodo pluriennale, queste fasi devono sicuramente essere correlate, ma non siamo giunti a una conclusione su come siano correlate o perché l'attore dovrebbe utilizzare approcci così graduali.

Data la ricerca condotta finora, ecco alcune riflessioni sulle possibili motivazioni:

- Si tratta di un attacco DDoS? No, almeno non nella forma attuale. Il volume delle query osservate è troppo basso per influire sui server autoritativi o sui resolver intermedi. Non vi è alcuna indicazione che sia coinvolto un attacco di reflection.
- Si tratta di esfiltrazione di dati? Ciò è altamente improbabile. L'attore non controlla i name server autorevoli, utilizza etichette di sottodominio brevi con una capacità minima di trasportare informazioni, sembra trasmettere pacchetti su larga scala e non controlla il percorso di ritorno.
- Si tratta di una scansione per resolver aperti? Anche questo è improbabile. Tra i numerosi metodi per trovare resolver aperti, tutti sono più semplici di quanto osserviamo in questi eventi.
- Si tratta di uno sforzo di mappatura di Internet? Beh, forse sì. Anche se sembra un'operazione molto complicata per mappare le reti.
- È un pre-posizionamento per gli attacchi DDoS? Forse. Per essere efficace per gli attacchi DDoS, l'attore dovrebbe modificare l'operazione in modo significativo.
- Si tratta di una ricerca su Internet di qualche tipo? Forse. Se è così, è un programma di ricerca molto lungo e senza un obiettivo chiaro che io possa discernere.
- È il risultato di un bug del software o di qualche altra applicazione? No. Questa spiegazione è stata posta in precedenza dagli scettici in risposta alla ricerca ExploderBot che abbiamo condotto. Nulla nei dati supporta la conclusione che si tratti di query DNS accidentali. Le attività di Muddling Meerkat sono molto deliberate e molto intelligenti.

È possibile che qualche altro attore statale stia fingendo di essere il GFW e stia falsificando sia le query che le risposte? Molte cose sono possibili, non tutte sono plausibili.

CONCLUSIONE E RACCOMANDAZIONI

Quando si passa tanto tempo quanto me a osservare il DNS, a volte ci si chiede se c'è qualcosa di normale in esso. Dopo anni di lavoro in questo campo, imparo ancora regolarmente cose nuove e osservo nuovi comportamenti degli attori. Spesso scopriamo un nuovo attore come risultato di qualche altro fattore non correlato. In questo caso, indagare su una rete illegale di gioco d'azzardo cinese mi ha portato a scoprire record MX anomali. Dopo aver inseguito una serie di false piste, ho formato un quadro più chiaro delle operazioni di Muddling Meerkat quando ho collaborato con ricercatori esterni per condividere dati e analisi. Alla fine, anche se sto scrivendo questo report, l'analisi e le conclusioni sono il risultato di un lavoro congiunto in cui diverse parti hanno portato tutte una prospettiva diversa per scoprire un comportamento precedentemente non documentato del GFW e una misteriosa operazione DNS pluriennale.

La nostra ricerca evidenzia anche le potenziali vulnerabilità della rete che derivano dalla negligenza e dalla complessità delle comunicazioni moderne su Internet. In particolare, consiglio agli amministratori di rete di:

- Cercare ed eliminare attivamente i resolver aperti nelle proprie reti. Identificare questi dispositivi può essere difficile, ma aziende come Infoblox e organizzazioni come la Shadow Server Foundation possono offrire informazioni fondamentali per aiutare.
- Non utilizzare domini di cui non si è proprietari per i domini di ricerca Active Directory o DNS. È molto probabile che vengano divulgate informazioni sulla rete e sulle applicazioni utente al name server autorevole, nonché ad altri dispositivi al di fuori del proprio controllo. Questo tipo di informazioni può consentire a un malintenzionato di effettuare una reconnaissance passiva della rete per attacchi mirati.
- Incorporare il DNSDR (DNS Detection and Response) nel proprio stack di sicurezza. Solo un resolver DNS è in grado di gestire efficacemente le minacce inerenti al DNS. La maggior parte dei prodotti di sicurezza non riconoscono nemmeno la differenza tra una query MX e una query del record A.
- Segnalare l'attività di Muddling Meerkat alla comunità. Dato che è impossibile osservare l'intera portata da un unico punto di osservazione, è importante raccogliere in crowdsourcing la comprensione di questa minaccia. In particolare, la segnalazione di ulteriori domini Muddling Meerkat aiuterà gli altri a trovare i resolver aperti e l'attività nella loro rete.

In definitiva, condivido le preoccupazioni espresse dalla CISA sulla RPC e sulla minaccia di pre-posizionamento per gli attacchi informatici a livello globale. Nella mia esperienza professionale, ho scoperto che i criminali informatici cinesi sono estremamente abili nella gestione, comprensione e utilizzo del DNS per molti scopi, che si tratti di censura, criminalità informatica o attacchi DDoS. Hanno anche alcuni dei migliori ricercatori del settore. Qualunque sia il vero obiettivo di Muddling Meerkat, non dovremmo sottovalutare il talento e la pazienza della RPC nel raggiungerlo.

INDICATORI DI ATTIVITÀ (DOMINI DI DESTINAZIONE)

Notare che questi domini non sono indicatori di compromissione e non sono necessariamente dannosi. Alcuni dei domini utilizzati da Muddling Meerkat sono parcheggiati, altri ospitano siti di gioco d'azzardo e altri contenuti potenzialmente illegali e altri sono domini legittimi attivi. L'intero ambito dei domini di destinazione di Muddling Meerkat è probabilmente molto più ampio.

Questi domini non ospitano alcun sito web, ospitano contenuti illegali o sono parcheggiati. Probabilmente possono essere bloccati senza impatto: `4u[.]com`, `kb[.]com`, `oao[.]com`, `od[.]com`, `boxi[.]com`, `zc[.]com`, `s8[.]com`, `f4[.]com`, `b6[.]com`, `p3z[.]com`, `ob[.]com`, `eg[.]com`, `kok[.]com`, `gogo[.]com`, `aoa[.]com`, `gogo[.]com`, `zbo6[.]com`, `id[.]com`, `mv[.]com`, `nef[.]com`, `ntl[.]com`, `tv[.]com`, `7ee[.]com`, `gb[.]com`, `tunk[.]org`, `q29[.]org`

Questi domini ospitano siti web e bloccarli può influire negativamente sulla propria rete: `ni[.]com`, `tt[.]com`, `pr[.]com`, `dec[.]com`

Indirizzi IP utilizzati per lanciare attacchi:

- `183[.]136[.]225[.]45`
- `183[.]136[.]225[.]14`

INFOBLOX THREAT INTEL

Infoblox Threat Intel è il principale creatore di informazioni originali sulle minacce DNS e si distingue da una molteplicità di aggregatori. Cosa ci distingue? Due cose: competenze DNS e visibilità senza pari. Il DNS è notoriamente difficile da interpretare e investigare, ma la nostra profonda comprensione e l'accesso esclusivo ci permettono di dare uno sguardo dietro le quinte del funzionamento interno di Internet. Siamo proattivi, non solo difensivi, e usiamo le nostre intuizioni per interrompere il crimine informatico dove ha inizio. Crediamo anche nella condivisione delle conoscenze per supportare la più ampia comunità della sicurezza pubblicando ricerche dettagliate e rilasciando indicatori su GitHub. Inoltre, le nostre informazioni sono perfettamente integrate nelle nostre soluzioni Infoblox DNS Detection and Response, in modo che i clienti ne traggano automaticamente i vantaggi, insieme a tassi di falsi positivi estremamente bassi.

infoblox.

Infoblox unisce networking e sicurezza per offrire prestazioni e protezione senza pari. Scelti dalle aziende Fortune 100 e dagli innovatori emergenti, forniamo visibilità e controllo in tempo reale su chi e cosa si connette alla tua rete, in modo che la tua organizzazione funzioni più velocemente e blocchi le minacce in modo più rapido.

Sede centrale
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

Versione: 20240216v1