infoblox

Threat Intel

MUDDLING MEERKAT: O GRANDE MANIPULADOR DE FIREWALLS

Autores:
Dra. Renée Burton
e Anônimo

ÍNDICE

RESUMO EXECUTIVO

Este artigo apresenta um agente desconcertante, o Muddling Meerkat, que parece ser um agente estatal da República Popular da China (RPC). O Muddling Meerkat conduz operações ativas por meio do DNS, criando grandes volumes de consultas amplamente distribuídas que são posteriormente propagadas pela internet por meio de resolvedores de DNS abertos. Suas operações estão ligadas a dois tópicos intimamente ligados à China e aos agentes chineses: o Grande Firewall Chinês (GFW) e ataques distribuídos de negação de serviço (DDoS) do Slow Drip, ou prefixo aleatório. Embora as operações do Muddling Meerkat pareçam à primeira vista ataques de DDoS de DNS, parece improvável que a negação de serviço seja seu objetivo, pelo menos no curto prazo. As operações confusas do Muddling Meerkat são de longa duração, tendo aparentemente começado em outubro de 2019, e demonstram alto grau de especialização em DNS.

As operações do Muddling Meerkat são complexas. Na verdade, são tão complicadas que é possível supor que o Muddling Meerkat não represente uma ameaça. Mas na segurança cibernética, especialmente no complexo mundo do DNS, devemos pensar estrategicamente. Em fevereiro de 2024, a Agência de Segurança Cibernética e de Infraestrutura dos EUA (CISA) e vários parceiros internacionais emitiram um comunicado dizendo: "Nos últimos anos, os EUA observaram uma mudança estratégica na atividade de ameaças cibernéticas da RPC, que deixou de se concentrar na espionagem e passou a se posicionar previamente para possíveis ataques cibernéticos disruptivos contra a infraestrutura essencial dos EUA".[1] Embora esse aviso específico tenha se concentrado nas técnicas de "viver da terra" utilizadas pelo agente Volt Typhoon, a mensagem de que "os agentes cibernéticos da RPC se misturam com as atividades normais do sistema e da rede, evitam a identificação pelas defesas da rede e limitam a quantidade de atividade capturada em configurações comuns de registro" é assustadoramente semelhante ao quão bem escondido o Muddling Meerkat permanece.[2]

O QUE É O MUDDLING MEERKAT

O Muddling Meerkat tem a capacidade aparente de controlar o GFW e faz isso de uma forma nunca antes relatada. Embora partes de suas operações sejam semelhantes aos ataques Slow Drip, a motivação e o objetivo do Muddling Meerkat não são claros. Os dados mostram que suas operações:

- Utilizam servidores no espaço IP chinês para conduzir campanhas fazendo consultas de DNS de subdomínios aleatórios para endereços IP em todo o mundo e, em última análise, investigando redes DNS globalmente
- Utilizam consultas de registro MX, além de outros tipos de registro, para nomes de host aleatórios curtos de um conjunto de domínios fora do controle do agente nos domínios de nível superior (TLDs) .com e .org
- Induzem registros MX falsos de endereços IP chineses injetados pelo GFW
- Utilizam domínios "superantigos", normalmente registrados antes do ano 2000, evitando listas de bloqueio de DNS e colidindo com muitos domínios corporativos do Active Directory
- Escolhem domínios para ataques com base em extensão e idade, em vez de seu status e propriedade atuais. Embora muitos dos domínios estejam abandonados ou tenham sido reaproveitados para utilização questionável, outros domínios são utilizados ativamente por entidades legítimas
- Executam campanhas de um a três dias em uma base razoavelmente contínua
- Não parecem usar spoofing em larga escala de endereços IP de origem, mas, em vez disso, iniciam consultas de DNS a partir de servidores dedicados
- São limitados em tamanho para evitar detecção e interrupções de serviço
- São possivelmente conduzidos em componentes discretos, criando diversos padrões de DNS com o passar do 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

- Começaram em ou por volta de 15 de outubro de 2019[3]

A Figura 1 apresenta uma visão simplificada das operações do Muddling Meerkat como conhecemos hoje.

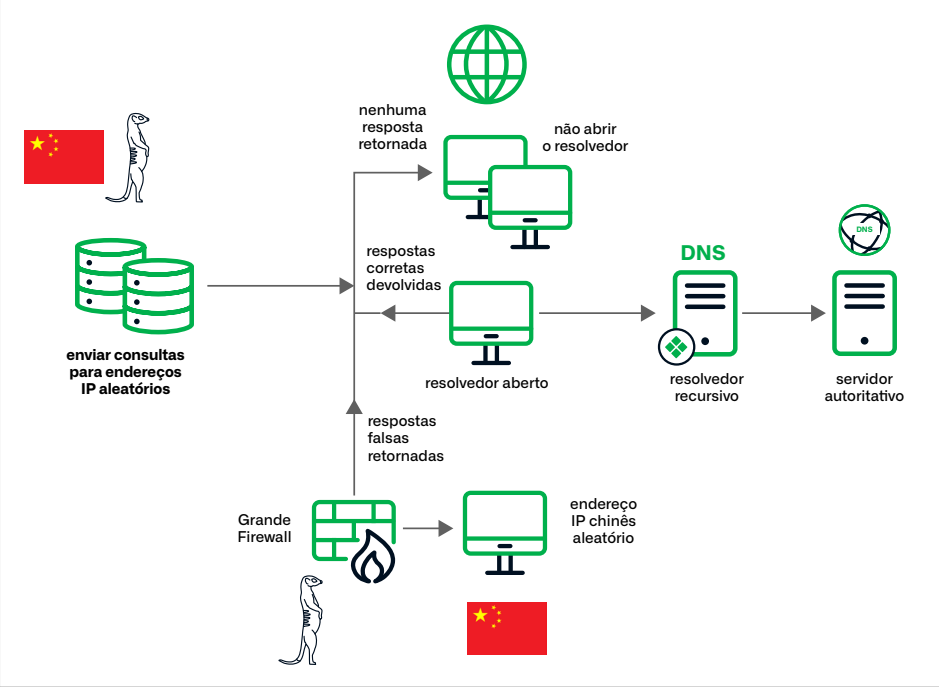

Figura 1. Uma visão geral das operações do Muddling Meerkat, conforme entendido atualmente. Observa-se que o Great Firewall apresenta respostas falsas a consultas MX, um comportamento que não foi documentado anteriormente.

Nossa descoberta do Muddling Meerkat foi casual e o agente poderia ter passado despercebido por muitos anos se não fosse pela visibilidade dos dados de várias organizações. Este artigo é uma pesquisa conjunta com pesquisadores de ameaças e fornecedores de segurança não revelados, bem como com a Merit Network, corporação independente sem fins lucrativos controlada pelas universidades públicas de Michigan e a DomainTools.[4] Cada um dos colaboradores tem acesso a alguma forma de coleta passiva de DNS e pode observar o Muddling Meerkat de uma perspectiva única. É impossível observar a totalidade das atividades do Muddling Meerkat de qualquer ponto de vista. Combinando informações, temos uma imagem da atividade do agente que não seria possível de forma independente. Todas as descobertas no artigo, salvo indicação em contrário, são confirmadas por duas fontes independentes ou extraídas diretamente dos resolvedores de DNS da Infoblox.

HISTÓRICO

Tomei a medida incomum de escrever este artigo na primeira pessoa. Em parte, a primeira pessoa parece mais apropriada para contar uma história estranha como essa. Além disso, meus estudos e publicações anteriores sobre os agentes chineses de ameaças a DNS ajudaram a fundamentar minhas conclusões sobre o Muddling Meerkat. No início da minha carreira, colegas da National Security Agency (NSA) e eu passamos milhares de horas estudando um agente chinês que fez ataques de DDoS baseados em DNS durante vários anos. Chamamos esse agente de ExploderBot e publicamos discretamente essas descobertas em meados de 2018. Depois de operar quase diariamente desde 2014, causando estragos nos provedores de serviços de Internet, o ExploderBot encerrou suas operações pouco mais de um mês após a publicação de nosso artigo. Não foram mais vistos desde 18 de maio de 2018. A natureza dos ataques de DDoS do DNS

3 Há algumas evidências de que as operações começaram alguns meses antes, em junho de 2019, mas não posso confirmar essa data.

4 https://www.merit.edu/

chinês mudou e escrevi um estudo longitudinal sobre as mudanças no fim de 2020. Desde então, não passei muito tempo analisando ataques de DDoS de DNS, chineses ou não. Na Infoblox, temos detectores que procuram sinais de atividade e bloqueiam automaticamente os domínios relacionados para os clientes do nosso produto Advanced DNS Protection (ADP), mas esse sistema funciona em grande parte sem a necessidade de intervenção humana.

O Muddling Meerkat chamou minha atenção enquanto investigava um agente de ameaça de DNS que disponibiliza serviços para outros agentes de ameaça que lidam com jogos de azar chineses ilegais e aplicativos falsos. Não foram os jogos de azar que se destacaram, mas sim as consultas e respostas anômalas para registros do servidor de e-mail DNS (MX). Embora eu tenha descoberto que o Muddling Meerkat também utiliza outros tipos de registros, este artigo se concentrará nos registros MX porque sua natureza específica dentro do DNS permite uma análise mais limpa.

A GFW atua para impedir que os residentes chineses acessem sites ou serviços que o governo considera inadequados ou ilegais.[5] Mas também é conhecido por injetar respostas falsas em consultas a DNS. A GFW é aplicada a todo o tráfego IP que entra ou sai do espaço IP chinês. É fácil demonstrar o comportamento de resposta falsa do GFW, como mostrarei mais adiante, na seção Investigação do Grande Firewall da China. O GFW pode ser descrito como um "operador secundário", o que significa que ele não altera as respostas do DNS diretamente, mas injeta suas próprias respostas, entrando em uma condição de corrida com qualquer resposta do destino original pretendido. Quando a resposta do GFW é recebida primeiro pelo solicitante, ela pode envenenar o cache do DNS. Além do GFW, a China opera um sistema conhecido como Great Cannon (GC). O GC é um "operador no meio", o que lhe permite modificar os pacotes no caminho até o destino.[6] O GC tem sido utilizado para ataques de DDoS em grande escala. Em 2015, foi utilizado para atacar a organização não governamental GreatFire.org que monitora a censura no GFW.[7] Desde então tem sido utilizado intermitentemente para ataques de DDoS, inclusive aqueles destinados a impedir protestos em Hong Kong.[8] O verdadeiro escopo das operações de GC é desconhecido. Combinados, o GFW e o GC criam muito ruído e dados enganosos que podem dificultar as investigações sobre comportamento anômalo no DNS. Pessoalmente, fui procurar várias trilhas somente para concluir: ah, é só o GFW.

Além do ataque de registros MX, o Muddling Meerkat atraiu nossa atenção porque apresentou padrões de comportamento semelhantes, embora em volumes menores, aos ataques de DDoS de DNS. Em um ataque DDoS de DNS Slow Drip ou de prefixo aleatório, as consultas a subdomínios aparentemente aleatórios de um domínio de destino são feitas em grande escala, normalmente propagadas por meio de resolvedores abertos. Esses ataques surgiram originalmente em 2014 e as primeiras vítimas relatadas foram chinesas. Vários colegas e eu investigamos os registros de DNS de vários anos desses ataques, concluindo que a maioria dos ataques que causaram danos demonstráveis foi conduzida por um único agente, o ExploderBot. Identificamos vários artefatos matemáticos em consultas a DNS e pacotes IP do ExploderBot que permaneceram consistentes durante cinco anos. Também determinamos que o tráfego do ExploderBot, que incluía endereços IP de origem e destino falsificados, foi injetado próximo ao backbone da Internet. Os resolvedores abertos que recebiam as consultas as encaminhavam para seus próprios resolvedores recursivos e, em redes com muitos dispositivos não gerenciados que continham resolvedores abertos desconhecidos, o volume de consultas atrapalhava os provedores de servidores da Internet. Os endereços IP falsificados utilizados nas consultas de DNS do ExploderBot foram amplamente distribuídos, e as respostas do GFW serviram como pistas falsas, dificultando nossa análise por um longo tempo. Quando as operações do ExploderBot cessaram em maio de 2018, o que restou foi um curioso conjunto de ataques contínuos de baixo volume, com pouco impacto ou propósito aparente. Nos últimos anos, ataques de prefixo aleatório afetaram servidores de nomes com certa regularidade, mas não vi o mesmo nível de volume associado ao 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

Neste artigo, descreverei as operações do Muddling Meerkat no contexto do que sei sobre a GFW, explicarei como detectar sua atividade e descreverei algumas das armadilhas da tentativa de analisar agentes como o Muddling Meerkat. Em particular, quero alertar os leitores sobre os perigos dos resolvedores abertos e a utilização de domínios de pesquisa não registrados no DNS ou no Microsoft Active Directory, que podem levar à participação em ataques de DDoS e ao vazamento de informações de rede para os adversários.

UM POUCO DE JARGÃO

A linguagem do DNS é confusa. Quando a combinamos com pacotes IP, ela se torna ainda mais confusa. Várias vezes no decorrer desta pesquisa, meu coautor e eu tivemos que parar e nos perguntar: *de que IP estamos falando?* Veja como utilizo vários termos ao longo do artigo:

- O endereço IP que faz uma consulta de DNS ou recebe uma resposta para uma consulta de DNS é chamado de **endereço IP do consultante**. Esse nome se aplica independentemente de o pacote IP conter a consulta ou a resposta.
- O endereço IP que responde a uma consulta de DNS é chamado de **endereço IP de resposta**. Em um mundo perfeito, esses são resolvedores, mas como veremos mais adiante na seção intitulada A função dos endereços IP chineses, com o Muddling Meerkat, eles são apenas endereços IP.
- Um endereço IP incluído em um registro de recurso DNS de uma resposta é chamado de **endereço IP de resolução**.
- Quando falo em geral sobre registros de recursos do DNS em uma resposta, posso dizer que a **resposta** refere-se ao(s) valor(es) contido(s) no registro.

OPERAÇÕES DO MUDDLING MEERKAT

As operações do Muddling Meerkat são complexas e demonstram que o agente tem sólido conhecimento de DNS, além de conhecimento de internet. Para simplificar a exposição, abordarei apenas os componentes da operação relacionados aos registros MX do DNS ou às cadeias de resolução MX. Em todos os casos, há um domínio registrado, que *não* está sob o controle do agente, chamado de **domínio de destino**. Neste documento, discuto três tipos de atividade:

- Consultas por registros MX de um domínio de destino
- Consultas por registros MX de nomes de host aleatórios de um domínio de destino
- Consultas por registros A de nomes de host aleatórios de um domínio de destino

As consultas de nomes de host aleatórios de um domínio-alvo são típicas de um ataque DDoS Slow Drip. No entanto, as consultas do Muddling Meerkat são diferentes das do ExploderBot ou de outros ataques Slow Drip. Os nomes de host são curtos. Além disso, embora alguns ataques Slow Drip incluam uma variedade de tipos de consulta, o tipo mais comum ainda é um registro A para um endereço IPv4. Nunca vi antes o tipo de atividade de registro MX que caracteriza o Muddling Meerkat. A escolha dos domínios de destino também é notável, como veremos mais adiante na seção Domínios de destino do Muddling Meerkat.

Quanto ao nome Muddling Meerkat: O suricato (meerkat) é um membro da família dos mangustos. De aparência enganosamente fofa, é inteligente, trabalhador e excepcionalmente feroz para seu pequeno tamanho. O Muddling Meerkat (suricato bagunceiro) é conhecido por atacar os registros MX de DNS e conduzir operações que envolvem o Grande Firewall chinês, adicionando confusão e pistas falsas à análise de falhas. Devido ao amplo uso de resolvedores abertos para a operação, a atividade também "aumenta e diminui" com o tempo e o local, como os suricatas fazem em suas tocas.

INVESTIGAÇÃO DO GRANDE FIREWALL DA CHINA

O GFW desempenha um papel importante nos dados do Muddling Meerkat, pois podemos observar respostas falsas a consultas de DNS em coleções de dados de DNS selecionadas. Quando vemos uma resposta falsa, o IP de origem desse registro é um endereço IP chinês, consistente com a injeção pelo GFW ou modificação pelo GC. Perdendo apenas para os Estados Unidos, a China controla mais de 350 milhões de endereços IP, distribuídos geograficamente em todo o mundo. Para todo o tráfego que entra e sai desse espaço IP, o GFW pode injetar respostas às consultas de DNS utilizando decisões sigilosas e sem impacto no desempenho do usuário. Para fazer isso bem feito, é necessário muito conhecimento. A China aproveitou as empresas de tecnologia ocidentais na virada do século para criar componentes do firewall e implementar vários outros mecanismos de vigilância e, ao fazê-lo, desenvolveu suas próprias capacidades e conhecimentos.[10]

A China projetou um sistema que responderá com respostas falsas em vez de simplesmente usar um NXDOMAIN ou outro mecanismo de resposta que os firewalls de DNS normalmente utilizam.[11] Por isso você não precisa acreditar na minha palavra: pode sondar o firewall por conta própria. Os pesquisadores já haviam encontrado respostas falsas para centenas de milhares de domínios e concluíram que algumas dessas respostas haviam poluído o cache de determinados resolvedores recursivos.[12] Em minha pesquisa, tanto na publicada no ExploderBot quanto desde então, vi uma variedade estonteante de respostas de endereços IP do GFW.

A maneira mais fácil de demonstrar o impacto da GFW é fazer consultas de DNS a um endereço IP chinês aleatório que não seja um servidor DNS estabelecido. Stephen Bortmeyer apresentou uma descrição disso em um blog de 2015.[13] Os experimentos podem ser feitos na linha de comando com o utilitário dig ou com uma ferramenta online. Se você solicitar o registro A de um domínio popular, o endereço IP chinês invariavelmente retornará uma resposta, mesmo que não hospede nenhum serviço de DNS. A Figura 2 abaixo mostra um exemplo em que um endereço IP atribuído à China Unicom e que atualmente não hospeda nenhum serviço responde a uma consulta de DNS para o endereço IP do `google[.]com` com uma resposta 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. Um endereço IP da China Unicom que não hospeda nenhum serviço responde a consultas de DNS para o registro A do `google[.]com` *com um endereço IP na Itália. A resposta é um redirecionamento intencional e mudará em cada resposta. Crédito da imagem:* `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 (último acesso em 9 de janeiro de 2024)

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

Não se sabe como o GFW escolhe para quais domínios vai enviar respostas falsas como meio de censura. A consulta do mesmo endereço IP chinês para um domínio sem censura normalmente resultará em um erro de que não foi possível acessar nenhum servidor. Esse resultado demonstra que o GFW injeta respostas apenas para determinadas consultas. Na minha experiência, o GFW responde a todas as consultas de DNS, independentemente do tipo de recurso solicitado com um endereço IPv4. Por exemplo, se solicitarmos o mesmo endereço IP para o registro MX do `google[.]com`, ele retornará um endereço IPv4 diferente, dessa vez atribuído à Korea Telecom. Um registro MX adequado deve incluir uma cadeia de texto com um nome de domínio totalmente qualificado (FQDN), não um endereço IPv4. (Veja a Figura 3.) Uma consulta a um registro TXT ou outro tipo de registro não A também retornaria um endereço IPv4. Outros pesquisadores realizaram estudos longitudinais em grande escala sobre o GFW em 2021 e chegaram à mesma conclusão.[14] Um ano antes, outro grupo de pesquisadores relatou uma única instância de injeção de registro CNAME, mas não descreveu a resposta.[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. Um endereço IP Unicom da China retorna um endereço IPv4 aleatório em resposta a uma consulta MX para `google[.]com`. *Uma resposta correta retornaria o FQDN do servidor de e-mail. Crédito da imagem:* `diggui[.]com`.

Esses experimentos mostram em primeira mão como a GFW opera normalmente. Ele injeta seletivamente respostas de DNS para determinados nomes de domínio com respostas enganosas aleatórias. Quando insere pacotes falsos, sempre retorna um endereço IPv4, independentemente do tipo de registro solicitado. O Muddling Meerkat, por outro lado, apresenta registros MX falsos formatados corretamente a partir de endereços IP chineses.

REGISTROS MX PARA UM DOMÍNIO DE DESTINO

A característica mais notável do Muddling Meerkat é a presença de respostas falsas de registros MX de endereços IP chineses. Esse comportamento, nunca publicado antes, difere do comportamento padrão da GFW. Essas resoluções são originadas de endereços IP chineses que não hospedam serviços DNS e contêm respostas falsas, consistentes com o GFW. Entretanto, diferentemente do comportamento conhecido do GFW, as respostas MX do Muddling Meerkat não incluem endereços IPv4, mas sim registros de recursos MX formatados corretamente. Essa característica é realmente notável e amplamente inexplicável.

Usarei um dos muitos domínios-alvo do Muddling Meerkat, `kb[.]com`, para demonstrar sua atividade neste documento. Os registros de resposta MX do Muddling Meerkat são observáveis somente em dados coletados fora da cadeia normal de resolução de DNS porque a origem da resposta não é um resolvedor de DNS, mas um endereço IP chinês aleatório. Como os dados da Infoblox são derivados de nossos resolvedores recursivos, fiz parcerias com outros fornecedores para obter dados para análise.

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 (último acesso em 9 de janeiro de 2024)

15 Anonymous, 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 (último acesso em Jan. 9, 2024)

Um terceiro apresentou dados de consulta-resposta de DNS contendo registros de recursos MX para o domínio kb[.]com em um período de 120 dias, terminando no fim de janeiro de 2024. Especificamente, cada registro incluía uma consulta de DNS para o registro MX de kb[.]com e uma resposta contendo dois registros de recursos. Os registros de recursos foram formatados corretamente, contendo FQDNs com nomes de host aleatórios de kb[.]com, normalmente com três a seis caracteres. Exemplos de tais valores de registro MX:

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

Para quem não está familiarizado com os registros MX, essas respostas devem ser o FQDN do servidor de e-mail para kb[.]com. Para entregar o e-mail de um usuário em uma rede a um destinatário na redekb[.]com, são necessárias duas consultas ao DNS. A primeira é para os registros MX do domínio de e-mail do destinatário, aqui kb[.]com, e a segunda é para o endereço IP do FQDN contido no registro MX. Depois que o endereço IP é obtido, o servidor SMTP (Simple Mail Transport Protocol) pode enviar e-mails em nome de um usuário (consulte a Figura 4.)

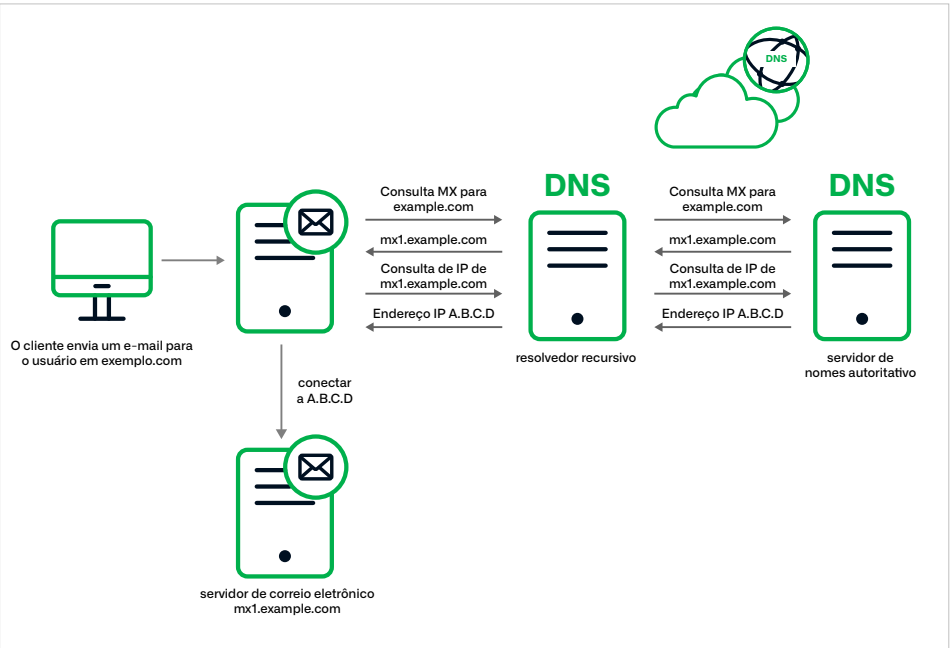

Figura 4. O processo típico de resolução de DNS para encontrar o endereço IP de um servidor de e-mail Na resolução padrão de um servidor de e-mail, ocorrerão consultas a um registro MX e a um registro A.

Nos dados de terceiros, os registros MX formatados corretamente são provenientes de endereços IP chineses aleatórios que *não* hospedam servidores DNS. Além disso, essas respostas, embora pareçam corretas à primeira vista, são falsas. O domínio kb[.]com atualmente tem servidores de nomes autoritativos na China com NS1, um serviço de nomes autoritativos que faz parte da IBM. Esses servidores de nomes autoritativos não retornam nenhuma resposta às consultas de registro MX para kb[.]com. Assim, observamos respostas de DNS provenientes do espaço IP chinês que diferiam do comportamento normal do GFW e eram falsas.

Os dados de terceiros continham não apenas alguns registros MX, mas milhares. Todos os nomes de host do conjunto de registros MX históricos foram vistos em um único dia durante esse período, totalizando mais de 8 mil FQDNs exclusivos. Um segundo fornecedor fez observações semelhantes. As respostas contêm nomes de host curtos e não são duplicadas. O volume é notável, mas bastante pequeno, certamente pequeno demais para ser eficaz em ataques de DDoS. Não apenas as respostas são falsas aqui, mas as próprias consultas também são suspeitas. O domínio `kb[.]com` já foi de propriedade de uma empresa de marketing dos EUA, mas agora hospeda jogos de azar em chinês com restrição geográfica. Não há motivo para os clientes enviarem e-mails para o domínio e, principalmente, não há motivo para solicitar resoluções de endereços IP chineses aleatórios. Como mostra a Figura 5, há resoluções MX para todos os dias da amostra, mas raramente há mais de 100 observações por dia.

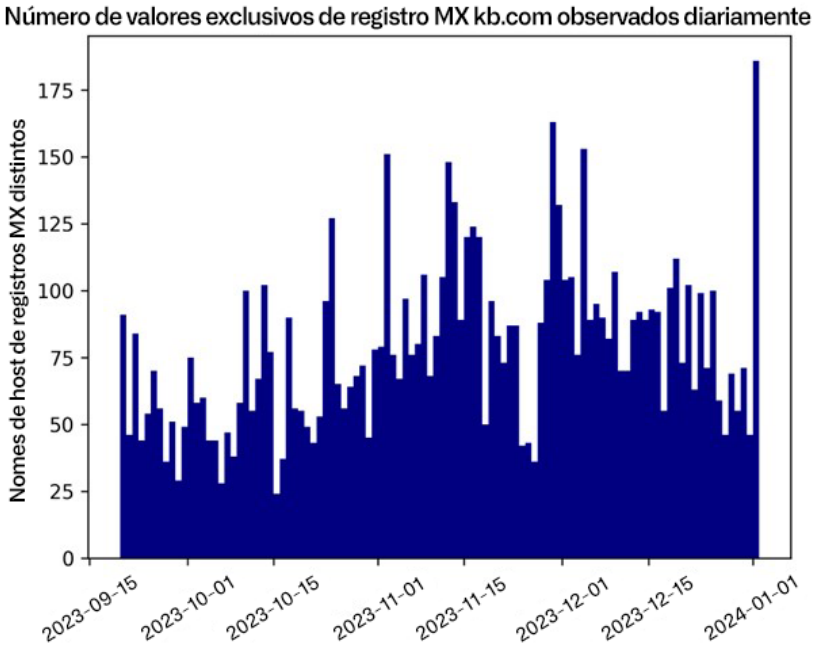

Figura 5. A contagem diária de valores de registro MX exclusivos para kb[.]com na coleção global de pDNS. São registros MX falsos que não existem no arquivo da zona do domínio.

Também analisamos respostas históricas para registros MX de `kb[.]com` durante vários anos (Figura 6). Os registros MX contendo um nome de host aleatório foram observados pela primeira vez em 15 de outubro de 2019. Verificamos de forma independente com outros fornecedores que as primeiras resoluções MX para domínios-alvo do Muddling Meerkat foram vistas pela primeira vez em 15 de outubro de 2019, ou por volta dessa data. Isso é verdade para todos os domínios-alvo que analisamos. Em geral, nos dados de terceiros, vemos um aumento inexplicável no número de resoluções MX a partir de 20 de setembro de 2023 e continuando no início de 2024.

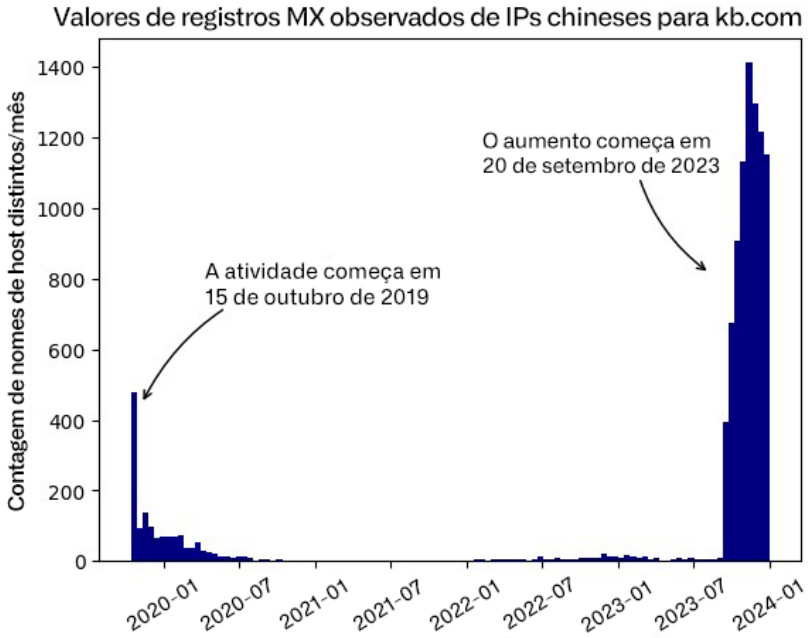

Figura 6. Contagem de valores exclusivos de registros MX falsos para `kb[.]com`*, agregados mensalmente ao longo do tempo e observados em coleções de dados de DNS de terceiros. Os endereços IP do respondedor para essas resoluções são endereços IP chineses aleatórios que não hospedam serviços de DNS, o que implica que a resposta vem do Grande Firewall. Todos esses são registros MX falsos que não existem no arquivo de zona do DNS*do `kb[.]com`.

É improvável que um resolvedor recursivo ou outro servidor sobre caminho normal de resolução de DNS tenha visto essas respostas. Comparando todo o histórico de registros MX para `kb[.]com` tanto do Infoblox quanto do DomainTools Farsight, vimos apenas um punhado de registros exclusivos. Desde janeiro de 2024, o servidor de nomes do `kb[.]com` não responde às solicitações de registros MX de nossos resolvedores. No passado, os servidores autoritativos retornaram respostas contendo esses valores:

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

Embora os servidores de nomes autoritativos para `kb[.]com` não respondam a consultas MX por meio do processo oficial de resolução de DNS, nossos resolvedores recursivos recebem solicitações para esses registros. Em circunstâncias normais, o recebimento dessas solicitações implicaria que os usuários em nossas redes de clientes precisariam enviar e-mail para um usuário em `kb[.]com`. Mas `kb[.]com` não serve correspondência. Os logs DNS passivos contêm muitas coisas estranhas e as consultas podem ser acionadas por aplicativos ou sites antigos. No entanto, neste caso, as consultas ocorrem com exatamente um mês de intervalo durante vários meses, contribuindo para a intriga. Como veremos em outros dados na próxima seção, esse comportamento provavelmente é desencadeado pelo Muddling Meerkat sondando nossas redes de clientes em busca de resolvedores abertos e, ocasionalmente, encontrando alguns.

Não consegui acionar manualmente respostas MX falsas do GFW para domínios-alvo do Muddling Meerkat ou outros. Talvez os registros sejam produzidos pelo GC ou em um contexto operacional específico do Muddling Meerkat. Por exemplo, as respostas podem ser acionadas por assinaturas dentro do pacote IP que identificam o agente. Sabemos que os pacotes IP do ExploderBot continham vários artefatos que poderiam servir como uma verificação da fonte, se desejado. O aparecimento de tais traços de identificação pode explicar por que outros pesquisadores viram injeções CNAME, mas apenas raramente. Infelizmente, tudo isso é especulação baseada em experiências anteriores e possíveis explicações para o comportamento aberrante da GFW/GC. Embora as respostas em si possam ser pacotes IP falsos, a Navalha de Occam aponta para uma variante do GFW, possivelmente o GC. Muitas coisas são possíveis, mas poucas são plausíveis.

REGISTROS MX PARA UM SUBDOMÍNIO ALEATÓRIO

O segundo componente de identificação das operações do Muddling Meerkat também envolve consultas de registros MX, mas para um subdomínio aleatório do domínio de destino, em vez do próprio domínio base. Nesse caso, em circunstâncias normais, a consulta seria acionada por um usuário que desejasse enviar e-mail não para o domínio base, mas para um subdomínio. Embora esse cenário ocorra no DNS normal, não é particularmente comum. Na maioria dos domínios de destino do Muddling Meerkat, não há servidor de e-mail funcional, criando uma situação ainda mais anômala. De fato, consultas por registros MX de subdomínios aleatórios de `kb[.]com` foram o que levou a toda essa investigação.

Os fenômenos que observamos em nossos resolvedores recursivos são um pequeno número de solicitações que ocorrem em um a três dias com nomes de host aleatórios. Essas solicitações incluem outros tipos de consulta além dos registros MX, mas devido à natureza específica dos registros MX em operações normais de rede, estou relatando somente descobertas sobre esse tipo. As consultas MX têm este formato:

```
<random>.target_domain
```

em que `random` é uma string alfanumérica de comprimento variável, normalmente entre três e seis caracteres.

Embora esta investigação tenha começado com `kb[.]com`, há cerca de 10 domínios de destino do Muddling Meerkat observados em nossas redes de clientes desde 1.° de setembro de 2023. As Figuras 7 e 8 mostram o volume de consultas MX para `kb[.]com` e `4u[.]com` visto em nossos resolvedores recursivos entre 1.° de setembro e 31 de dezembro com alguns FQDNs de amostra consultados em dias específicos. Durante esse período de quatro meses, nenhum subdomínio é repetido. Nossos parceiros da DomainTools Farsight e outros fornecedores não divulgados observam as mesmas tendências, embora com diferentes subdomínios aleatórios.

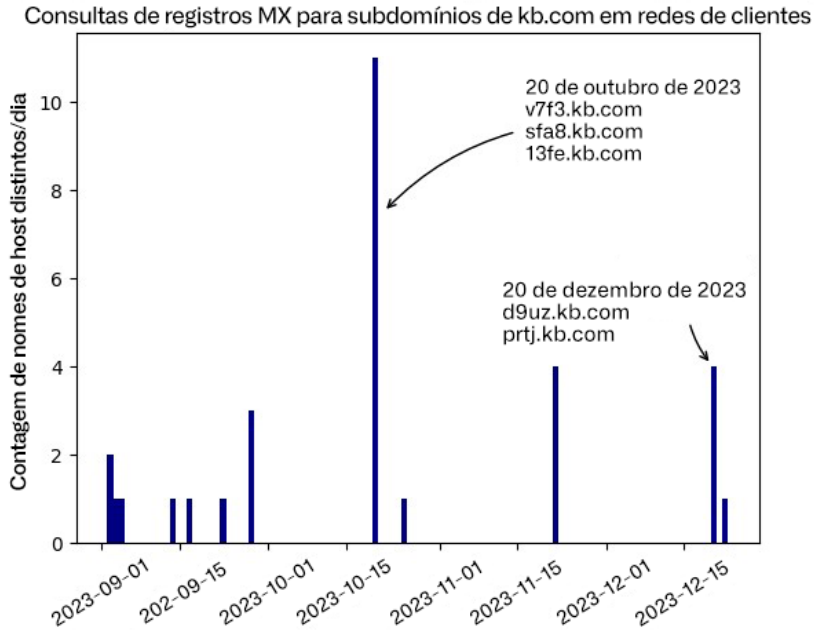

Figura 7. O número de FQDNs distintos com consultas de registro MX para `kb[.]com` *visto nos resolvedores recursivos da Infoblox durante quatro meses*

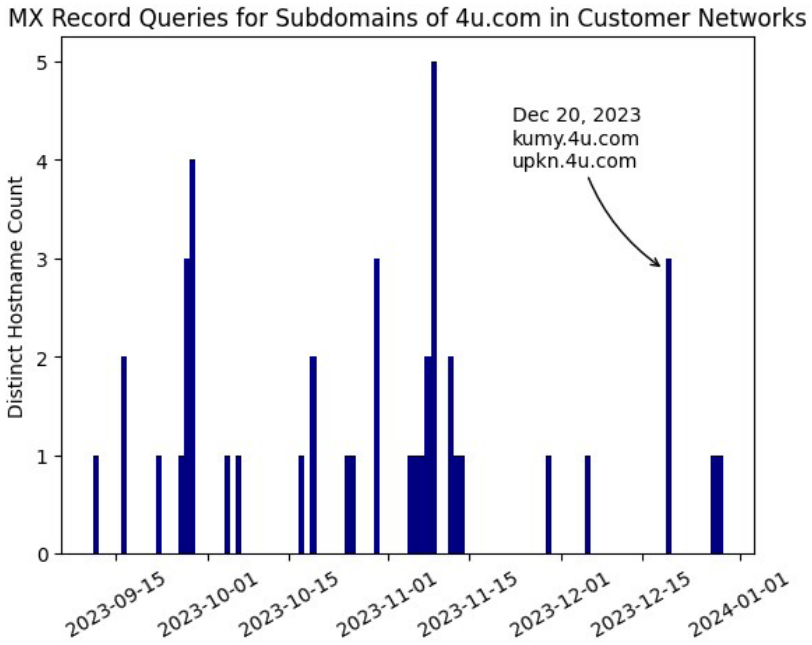

Figura 8. O número de FQDNs distintos com consultas de registro MX para `4u[.]com` *visto nos resolvedores recursivos da Infoblox em um período de quatro meses*

As Figuras 7 e 8 demonstram a natureza "pop-up" aperiódica das consultas do Muddling Meerkat com um ritmo operacional que dura de um a três dias e utiliza nomes de host aleatórios. Esse tipo de padrão é típico dos ataques de DDoS Slow Drip em geral e do ExploderBot especificamente. No entanto, existem algumas diferenças significativas entre o que foi relatado anteriormente na literatura e esses ataques. Mais notavelmente, nesses ataques, os volumes são muito menores do que esperaríamos para uma tentativa real de DDoS e aqueles vistos em ataques em larga escala no auge dessa atividade entre 2014 e 2017.

Em um estudo longitudinal publicado na revista *Digital Threats Research* and Practice em 2019, observei que o cenário do DDoS Slow Drip havia mudado consideravelmente desde nosso primeiro artigo sobre o ExploderBot.[16] Nessa pesquisa, realizada durante seis meses em 2018, foram observados vários tipos de consulta, mas o MX não era um deles. Os padrões dominantes descritos nesse artigo ainda são observados hoje, com baixos níveis de consultas com nomes de host longos e forte viés nas distribuições de caracteres. O Muddling Meerkat não tem semelhança com essas tendências.

REGISTROS IPV4 PARA SUBDOMÍNIOS ALEATÓRIOS

Além das consultas MX para subdomínios aleatórios do domínio de destino, nossos resolvedores recursivos recebem solicitações de registros A ou endereços IPv4. Obviamente essas consultas não recebem respostas de nossos resolvedores porque esse subdomínio não existe configurado no servidor de nomes autoritativo. Outros fornecedores cuja coleta vem de resolvedores recursivos têm observações semelhantes. Os dados do DomainTools Farsight, por exemplo, vêm de uma coleção de resolvedores recursivos em todo o mundo. Assim como a Infoblox, esses fornecedores observam picos regulares de consultas por subdomínios aleatórios dos domínios do Muddling Meerkat, incluindo consultas de registros A. A Figura 9 mostra essas tendências para um mês, janeiro de 2024.

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

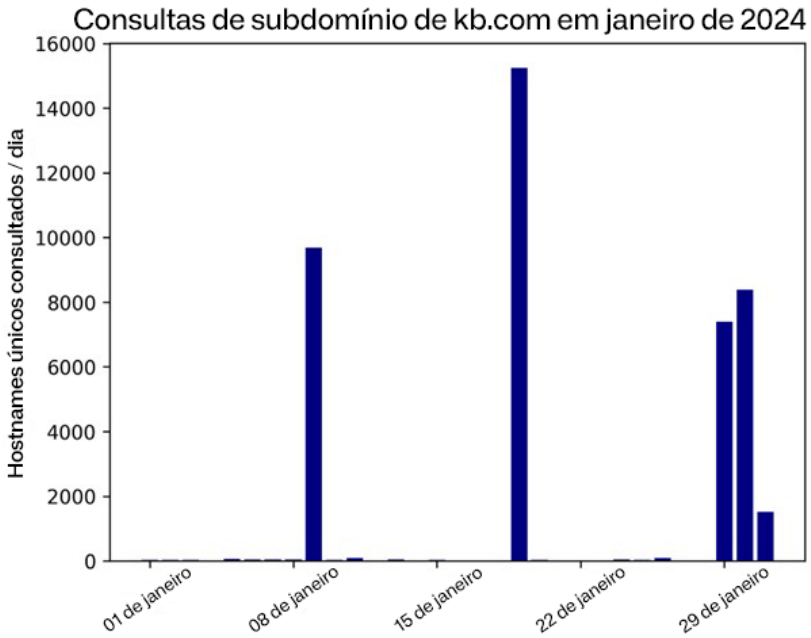

Figura 9. Consultas de nome de host exclusivo de `kb[.]com` *observadas no pDNS da Farsight em janeiro de 2024*

Existem também outros tipos de coleta com visibilidade do DNS, incluindo coleta de pacotes, honeypots e telescópios de internet. Trabalhando com a teoria de que a fonte dessas consultas em nossas redes eram resolvedores abertos e que o Muddling Meerkat provavelmente estava sondando um amplo espectro de espaço IPv4 para resolvedores abertos, pedi a outros fornecedores que ajudassem a localizar pacotes que continham registros de recursos na resposta. Encontramos respostas de registro A da mesma forma que encontramos respostas de registro MX.

Os únicos endereços IP que responderam às consultas dos registros A dos domínios do Muddling Meerkat estavam no espaço IP chinês. Esses endereços IP não estavam abertos na porta 53, o que significa que não eram resolvedores de DNS. Em outras palavras, essas respostas vieram do GFW e não dos servidores autoritativos.

O GFW é conhecido por injetar respostas a consultas de DNS com endereços IP de resolução que não são totalmente aleatórios. Em um estudo longitudinal que abrangeu nove meses e foi publicado em agosto de 2021 para o 30.º Simpósio de Segurança da Usenix, os pesquisadores descobriram que os endereços IP falsificados frequentemente apareciam de forma recorrente para determinados grupos de domínios.[17]

Utilizando resoluções de IP de subdomínios de `kb[.]com`, mapeamos a ocorrência de um endereço IP de resolução forjado com a linha do tempo das consultas. Em todos os casos, o endereço IP de resolução é visto repetidamente, com janelas de tempo distintas que duram de um a três dias, para subdomínios aleatórios curtos. As Figuras 10 e 11 mostram dois exemplos desse comportamento. Os dois endereços IP não estão realmente relacionados ao `kb[.]com`; estas são respostas falsas do GFW. Ambos os endereços IP são vistos em dias sobrepostos. Cada figura mostra a totalidade das resoluções para `kb[.]com` a esse endereço IP em 2022. Assim como acontece com os dados do resolvedor Infoblox e Farsight, o nome do host ou subdomínio não é repetido.

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 (último acesso em 9 de janeiro de 2024)

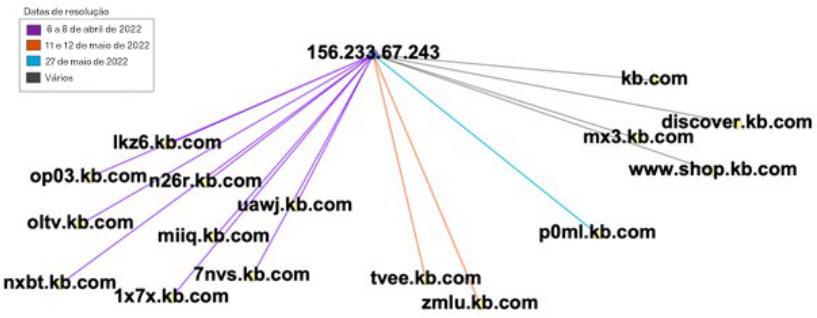

Figura 10. Resoluções de nome de host pelo GFW dentro do domínio `kb[.]com` *para o endereço IP 156[.]233[.]67[.]243 durante 2022. Esse endereço IP não está relacionado a* `kb[.]com` *e a resposta é forjada pelo GFW.*

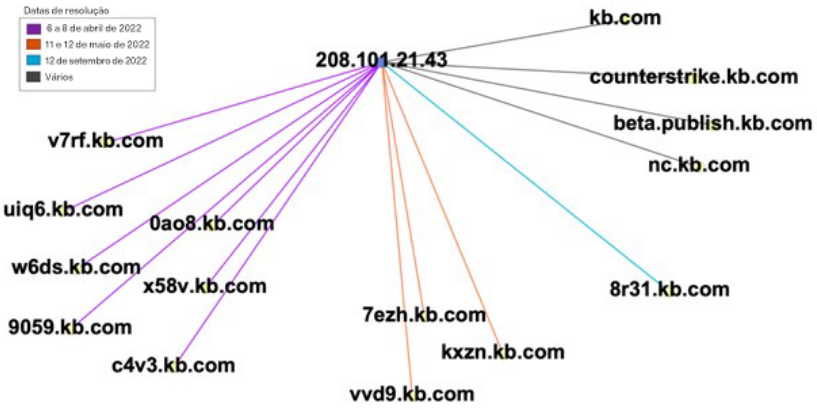

Figura 11. Resoluções de nome de host pelo GFW dentro do domínio `kb[.]com` *para o endereço IP 208[.]101[.]21[.]43 durante 2022. Esse endereço IP não está relacionado a* `kb[.]com` *e a resposta é forjada pelo GFW.*

Esses resultados indicam que o Muddling Meerkat está conduzindo operações que incluem consultas de DNS a um grande número de endereços IP de destino, independentemente de sua localização ou de portas abertas, e que o GFW está injetando respostas a esses domínios em dias específicos com um conjunto de endereços IP que são utilizados ao longo do tempo. Essa mesma atividade e esse mesmo tipo de respostas estão em andamento em janeiro de 2024. Embora esses números mostrem resoluções para `kb[.]com`, verificamos o mesmo padrão para todos os domínios-alvo conhecidos do Muddling Meerkat.

Aqui é onde as coisas ficam interessantes: normalmente, o GFW não injeta respostas para `kb[.]com` nem para quaisquer subdomínios. O GFW não está injetando respostas falsas a nenhuma solicitação aleatória de subdomínio de `kb[.]com`, apenas aqueles criados por Muddling Meerkat! Como discutimos anteriormente, o GFW injeta respostas a domínios populares ou a domínios que considera de alguma forma censuráveis aos interesses chineses. O artigo da Usenix acima mencionado valida esse fato. A Figura 12 mostra a resposta em 13 de janeiro de 2024 a uma consulta de registro A para `nxbt.kb[.]com` do endereço IP 111[.]193[.]204[.]201 que utilizamos anteriormente para obter respostas falsas ao `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. A resposta a uma solicitação de registro A de 111[.]193[.]204[.]204 para `nxbt[.]kb[.]com`*. Esse endereço IP está no espaço de endereços IP chinês e não está aberto na porta 53. A resposta é o que se espera para uma consulta desse tipo e é consistente com o comportamento conhecido do GFW. Crédito da imagem:* `diggui.com`*.*

DOMÍNIOS-ALVO DO MUDDLING MEERKAT

A escolha dos domínios-alvo do Muddling Meerkat demonstra a sofisticação do DNS. Os operadores do Muddling Meerkat induzem respostas seletivas do GFW que não ocorrem na censura normal do GFW. Para isso, eles escolheram domínios-alvo que não controlam que é muito improvável que os dispositivos de segurança bloqueiem. Além disso, utilizam tipos de consulta que não são comumente monitorados e criam um volume de consultas que se mistura com o tráfego normal de DNS. Observamos nomes de host aleatórios com tipos de consulta A (IPv4), CNAME, MX e AAAA (IPv6) nos resolvedores da Infoblox.

As consultas aleatórias de subdomínios que observamos são para domínios registrados há 20 anos ou mais, têm rótulos curtos e estão nos TLDs .com e .org. Os rótulos de domínio de destino têm principalmente dois ou três caracteres, mas vi alguns exemplos que tinham quatro caracteres (por exemplo, `boxi[.]com`). Na maioria dos casos, os domínios mudaram de mãos ao longo do tempo, mas a data de criação original ainda será mostrada no WHOIS. Exemplos: `kb[.]com`, `4u[.]com`, `id[.]com`, `od[.]com`, `ntl[.]com` e `nef[.]com`. Todos esses domínios foram observados no tráfego do Muddling Meerkat nos resolvedores da Infoblox durante dezembro de 2023 e janeiro de 2024.

Verifiquei aproximadamente 20 domínios-alvo em várias fontes. No entanto, provavelmente há muitos mais. É difícil isolar os domínios de destino por vários motivos que apresentarei aqui e discutirei com mais detalhes posteriormente na seção intitulada O papel dos endereços IP chineses. Primeiro, nem todos os domínios que atendem aos critérios básicos de idade e comprimento parecem ser direcionados. Por exemplo, não encontrei evidências de que `rr[.]com`, `ibm[.]com`, e `aol[.]com` são utilizados nas operações do Muddling Meerkat, embora atendam aos requisitos básicos. (*Sim*, `aol[.]com` *ainda ocorre no tráfego DNS*.) A maioria dos domínios encontrados em consultas em nossos resolvedores recursivos não está em uso (por exemplo, `4u[.]com`) ou não particularmente popular entre os clientes. Muitos, como `kb[.]com` e `od[.]com`, são utilizados para sites de jogos de azar offshore em chinês. Alguns, como `ni[.]com`, de propriedade da National Instruments, são domínios bem estabelecidos e muito usados.

A opção da utilização de domínios curtos e estabelecidos há muito tempo em TLDs de boa reputação é inteligente por mais motivos do que a probabilidade reduzida de ser bloqueado por dispositivos de segurança. Domínios com essas características também são utilizados com frequência:

- por organizações como domínios de pesquisa DNS ou domínios do Active Directory e
- em malware para criar pistas falsas para os investigadores

Consequentemente, um analista do SOC (Security Operations Center) que perceber consultas suspeitas a esses domínios-alvo será bloqueado pelas muitas fontes em potencial de malware que podem estar conectadas à consulta. Por exemplo, o domínio `kb[.]com` tem mais de 30 arquivos referentes a ele e 7 arquivos que se comunicam com ele, em amostras armazenadas pelo fornecedor VirusTotal.[18] O domínio `od[.]com` apresenta mais de 130 arquivos de referência.[19] Muitos são amostras antigas de malware e aumentam o ruído.

Por outro lado, um pesquisador como eu, tentando entender um quadro mais holístico da atividade, terá que filtrar consultas de DNS não relacionadas para isolar os verdadeiros domínios-alvo. Esse tipo de domínio é comumente utilizado para o Active Directory por uma organização, mesmo que ela não controle o domínio. (*Uma prática arriscada!*) Além disso, aplicativos, sites e pessoas causam consultas aberrantes no DNS. Entre os vários tipos de consulta utilizados pelo Muddling Meerkat, o MX é o mais fácil de analisar.

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

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

Para oferecer alguma perspectiva, analisei as resoluções MX nos resolvedores recursivos da Infoblox que ocorreram durante seis semanas a partir de 1.° de dezembro de 2023. Quando pensamos em domínios de servidores de e-mail, não esperamos ver muita variedade. Mas essa expectativa revela-se como um viés cognitivo. Contei o número de SLDs com as seguintes condições semelhantes ao Muddling Meerkat:

- nos TLDs .com e .org
- resultam em respostas NXDOMAIN
- têm mais de 10 nomes de host diferentes

Mais de 1.100 domínios atenderam aos critérios. Em resumo, muitos domínios têm consultas MX anômalas. Desses 1.100, reduzi o conjunto para incluir apenas aqueles em que o rótulo do domínio tinha menos de quatro caracteres. Isso resultou em 55 candidatos e mais de 22 mil consultas exclusivas durante o período do estudo. A partir desse conjunto de candidatos, fiz uma análise adicional para confirmar os domínios-alvo utilizando uma variedade de outros recursos.

O PAPEL DOS RESOLVEDORES ABERTOS

Um resolvedor aberto é um dispositivo em um endereço IP que responderá a consultas de qualquer cliente, mas não está configurado intencionalmente como um resolvedor recursivo para atender ao público em geral. Por outro lado, um resolvedor público no DNS é um resolvedor recursivo projetado para responder a consultas de qualquer cliente e normalmente é administrado por uma grande empresa, como Google, Cloudflare ou Yandex. Alguns pesquisadores incluem resolvedores públicos em sua definição de resolvedores abertos, mas eu não. Os resolvedores abertos são pontos de exploração bem conhecidos para ataques de DDoS. Podem ser utilizados para ampliar os ataques contra as vítimas em ataques de reflexão, em que as consultas de DNS são feitas para abrir resolvedores com fontes falsificadas contendo o endereço IP da vítima.[20] Também são utilizados em ataques Slow Drip para distribuir consultas ao servidor de nomes autoritativo de propriedade da vítima e em variações de ataques contra a infraestrutura intermediária.[21]

Uso o termo *endereço IP* aqui para descrever os resolvedores abertos em vez de um resolvedor de DNS porque os resolvedores abertos são muito complexos. Por exemplo, pode haver um dispositivo de Internet, como um firewall, na frente do endereço IP do resolvedor aberto que pode interceptar as consultas e, assim como o GFW, forjar uma resposta, fazendo parecer que o endereço IP de destino original respondeu à consulta de DNS. A resposta retornada pode ou não estar correta. Esse comportamento é semelhante ao descrito por pesquisadores sobre a interceptação de consultas de DNS por provedores de serviços de Internet (ISPs).[22]

Resolvedores abertos contribuem para ataques de DDoS e dificultam a análise. Eles criarão tráfego adicional para os servidores raiz e TLD porque não têm a amplitude de um cache DNS que um resolvedor público teria, frequentemente forçando-os a executar uma resolução completa. Na minha experiência com análise de tráfego de resolvedor aberto, muitos têm outras configurações incorretas em seu DNS, criando tráfego adicional, geralmente desnecessário. Por exemplo, podem não armazenar em cache dicas de raiz e consultar continuamente os endereços IP do servidor raiz. Quando combinados com o potencial de respostas forjadas, os resolvedores abertos criam muito ruído e produzem pistas falsas para os pesquisadores.

---

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, pp. 293–318, 2022. https://doi.org/10.1007/978-3-030-98785-5_13. https://annasperotto.org/publication/papers/2022/yazdani-pam-2022.pdf (último acesso em 14 de janeiro de 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 (último acesso em 14 de janeiro de 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 (último acesso em 14 de janeiro de 2024)

Encontrei resolvedores abertos pela primeira vez enquanto estudava os ataques de DDoS do ExploderBot. Nesses ataques, pacotes IP contendo consultas de DNS para subdomínios aleatórios de um domínio alvo foram lançados na Internet perto do backbone em vários locais. Os endereços IP de origem e destino foram forjados e, quando tomados juntos ao longo do tempo, cobriram uma grande quantidade do espaço de endereços IPv4. Em nossa pesquisa, encontramos todos os problemas mencionados acima, inclusive respostas forjadas do GFW e resolvedores abertos. O ExploderBot conduziu esses ataques normalmente em alguns dias, mas foram periódicos. Antes de 2016, havia operações várias vezes por mês, mas diminuíram nos anos seguintes e se tornaram muito irregulares. Embora tenha sido aparentemente um ataque de DDoS a um servidor de nomes autoritativo, o maior dano causado pelo ExploderBot foi à infraestrutura do ISP, incluindo resolvedores recursivos e balanceadores de carga. Sem resolvedores abertos, os ataques do ExploderBot não teriam sido notáveis, mas por vários anos, embora não fossem vinculados ao nome de um agente, sua atividade foi abordada em blogs e reportagens na mídia. Acredita-se que o ExploderBot esteja inativo. A atividade foi vista pela última vez na Infoblox em 18 de maio de 2018.

Os resolvedores abertos também desempenham um papel importante nas operações do Muddling Meerkat. As evidências sugerem que as consultas são enviadas para uma ampla variedade de endereços IP, muitos deles resolvedores abertos, do espaço IP chinês. Os endereços IP de destino para as consultas de DNS provavelmente mudam com o tempo, o que cria uma assinatura "pop up" em resolvedores recursivos como a Infoblox. Em outras palavras, suspeito que o Muddling Meerkat esteja ativamente bagunçando a internet com mais frequência do que observamos nos resolvedores de nuvem da Infoblox. Em vez disso, suspeito que em determinados intervalos, com duração de alguns dias, os endereços IP externos pertencentes aos nossos clientes são incluídos nos destinos do Muddling Meerkat. (Isso é especulação da minha parte; não tenho visibilidade de dados para ver o escopo completo das atividades.) Alguns de nossos clientes, sem querer, têm resolvedores abertos em sua rede que recebem suas consultas e as encaminham para nossos resolvedores para resolução. Independentemente do ritmo operacional, só veremos as consultas do Muddling Meerkat em nossos resolvedores quando um dispositivo do cliente as encaminhar.

O Muddling Meerkat ataca muitos resolvedores abertos. Alguns são servidores estabelecidos em um data center, enquanto outros são roteadores domésticos. Por exemplo, observamos vários endereços IP que são identificados como roteadores MikroTik pelo Shodan.[23] Em janeiro de 2024, esses endereços IP incluíam consultas dos exemplos de resolvedores abertos da Tabela 1.

Endereço IP do consultante	Nome da Consulta
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

Tabela 1. Exemplos de endereços IP de consultantes e consultas observados em janeiro de 2024. Todos esses endereços IP hospedavam resolvedores abertos em 31 de janeiro de 2024

SEM CONSULTANTES FALSIFICADOS

Devido à minha experiência com o ExploderBot, eu estava predisposto a achar que o Muddling Meerkat estava injetando consultas a DNS na Internet utilizando endereços IP de consulta falsificados e um amplo espectro de endereços IP de destinatários. As evidências que descobrimos, no entanto, indicavam o contrário: Endereços IP chineses selecionados eram a fonte de um número desproporcional de consultas de DNS. Com base nos dados (consulte exemplos na Tabela 2) parecia mais provável que o Muddling Meerkat estivesse utilizando servidores dedicados para suas operações.

23 Shodan.io é um mecanismo de busca disponível publicamente para atributos de servidor por endereço IP.

Apesar das evidências contrárias, queríamos testar a hipótese do consultante falsificado. A melhor maneira de fazer isso é por meio do que chamamos de **telescópio de rede**,[24] que aproveita os endereços IP não utilizados para os quais não deveria haver tráfego e coleta os pacotes roteados para eles. Os telescópios de rede são úteis para capturar eventos de grande escala que utilizam endereços IP falsificados. Vários operadores de telescópio, incluindo a Merit Network, podem observar o tráfego de aproximadamente 11 milhões de endereços IP. Embora esses endereços IP não sejam tecnicamente utilizados,recebem uma enorme quantidade de tráfego contendo uma grande variedade de protocolos.

No contexto de uma consulta de DNS falsificada, a cadeia de eventos seria mais ou menos assim:

- O invasor injeta um pacote IP que contém uma consulta de DNS supostamente do endereço IP A e direcionada para o endereço IP B.
- Supondo que o endereço IP B seja um resolvedor de DNS ou um proxy invisível como o GFW, um pacote de resposta é enviado de B para A.
- Esse pacote de resposta é recebido em A e é chamado de backscatter no telescópio porque é uma reflexão para um endereço que não iniciou a comunicação.

Os operadores de telescópio podem então medir eventos da internet pelo retroespalhamento que recebem. Esses operadores têm uma janela única para o tráfego da internet e certos ataques.

Os pesquisadores da Merit Network não encontraram evidências de respostas do Muddling Meerkat em seus dados de backscatter. Posteriormente, os pesquisadores da Merit Network entraram em contato com os operadores de outro grande telescópio no Center for Applied Data Analysis (CAIDA) para verificar se o Muddling Meerkat havia falsificado endereços IP de consulta nos intervalos monitorados pelo telescópio do CAIDA.[25] O CAIDA não capturou nenhum backscatter associado a essa atividade. Quando combinamos seus resultados com as observações anteriores de consultas de DNS em grande escala emitidas por endereços IP chineses, ficamos confiantes de que o Muddling Meerkat não está falsificando amplamente os endereços IP dos consultantes em suas operações. Essa é a principal diferença entre o Muddling Meerkat e o ExploderBot.

O PAPEL DOS ENDEREÇOS IP CHINESES

Devido à complexidade envolvida nas operações do Muddling Meerkat e ao impacto da GFW, é difícil determinar se eventos específicos com endereços IP chineses são “reais”. O que quero dizer com “real” é que pode não ficar claro se um endereço IP específico está “respondendo” a uma consulta como resultado da GFW. Da mesma forma, pode ser difícil separar os endereços IP falsificados daqueles que originaram as consultas.

Nossa abordagem para esse problema foi tirar conclusões a partir de estatísticas gerais. Conforme explicado anteriormente na seção intitulada Registros IPv4 para subdomínios aleatórios, observamos que os endereços IP chineses “responderam” às consultas do Muddling Meerkat quando se sabia que esse endereço IP não tem a porta 53 aberta. Com um grande número desses tipos de exemplos, podemos concluir que as “respostas” são resultados da GFW e não respostas “reais”.

Quando observamos o comportamento do consultante, alguns endereços IP se destacam. Esses endereços IP ocorrem com frequência muito maior do que os IPs de resolvedores abertos. São a fonte de consultas que estavam fora da resolução normal do DNS, inclusive para endereços IP que estavam hospedando resolvedores abertos. Alguns desses endereços IP de consulta foram relatados repetidas vezes por varredura agressiva e outras práticas questionáveis.[26] A Tabela 2 apresenta um exemplo de endereços IP de origem e consultas.

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

Endereço IP do consultante	Nome da consulta
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

Tabela 2. Amostra de endereços IP de consultantes e consultas observadas em janeiro de 2024. Esses endereços IP não estavam hospedando resolvedores abertos em 31 de janeiro de 2024. Algumas dessas consultas foram direcionadas a resolvedores abertos conhecidos.

LOCALIZANDO A ATIVIDADE DO MUDDLING MEERKAT

Podemos observar o Muddling Meerkat em parte de várias fontes. Os resolvedores recursivos, como o nosso, podem observar tanto as consultas de subdomínios aleatórios quanto as consultas de registros MX dos domínios de destino. Quando resolvidas por meio do DNS global, a grande maioria dessas consultas resultará em uma resposta NXDOMAIN. Se não houver resolvedores abertos ou públicos na rede, não acredito que você verá o Muddling Meerkat nos registros de DNS. Infelizmente, muitos sistemas de registro de DNS registram somente as resoluções bem-sucedidas e os proprietários da rede podem não perceber a atividade devido a essa limitação.

Para aqueles que podem observá-las é provável que as consultas do Muddling Meerkat apareçam de forma intermitente, semelhante aos exemplos das Figuras 6 e 7, e dependam do tamanho da rede. Na Infoblox, vemos mais tráfego do Muddling Meerkat do que uma organização comum, porque resolvemos consultas de DNS para clientes em todo o mundo. Nossos resolvedores recursivos na nuvem lidaram com mais de 33 trilhões de consultas somente em 2023.

Além dos registros de consulta DNS, os pesquisadores devem encontrar vestígios do Muddling Meerkat em várias outras fontes:

- A raiz, o TLD e os servidores de nomes autoritativos terão evidências de atividade do Muddling Meerkat que remontam a outubro de 2019 e possivelmente antes. Como o agente não controla os domínios de destino e está consultando amplos intervalos de IP para os registros, os resolvedores abertos encaminharão as consultas e resultarão em solicitações em cada servidor dentro da cadeia de resolução.
- Caches de resolvedores recursivos também capturam evidências de Muddling Meerkat
- Os proprietários de honeypots de DNS provavelmente receberão consultas, dependendo da amplitude com que o Muddling Meerkat consulta endereços IP.
- Os dados de fluxo podem conter indicações de atividade, especialmente se monitorarem o espaço chinês de IPs, ou mostrarem uma variedade incomum de conexões de porta 53 com os servidores de nomes autoritativos, especialmente decorrentes de endereços IP de resolvedores abertos.

As consultas a quaisquer domínios apresentados no fim deste relatório devem ser consideradas suspeitas. Mas lembre-se da ampla utilização desses domínios para domínios de pesquisa do Active Directory e do DNS. Além do domínio de destino, deve haver consultas de registros MX, especialmente para subdomínios aleatórios curtos. Há outras consultas suspeitas para um subconjunto de domínios do Muddling Meerkat que não estão incluídas neste relatório. Essas são consultas de registro A que parecem vazar informações de rede para o servidor autoritativo. No entanto, não consigo vincular essa atividade definitivamente ao Muddling Meerkat.

ATRIBUIÇÃO E MOTIVAÇÃO

O Muddling Meerkat parece ser um agente estatal chinês. Como podemos observar respostas de registros MX de endereços IP chineses que não estão abertos na porta 53 de domínios-alvo do Muddling Meerkat durante vários anos, tenho certeza de que essas respostas são resultados da GFW. Ao mesmo tempo, as respostas MX adequadas do GFW nunca foram relatadas antes e os pesquisadores, inclusive eu, não conseguiram acionar o comportamento manualmente. Para induzir respostas seletivas como as que observamos durante quatro anos, parece que o Muddling Meerkat deve estar de alguma forma conectado aos operadores da GFW. Embora eu também não saiba como essas respostas seletivas são acionadas, é possível que as assinaturas contidas nos pacotes IP, como as observadas no tráfego do ExploderBot, sejam utilizadas para sinalizar uma resposta diferente do GFW.

A motivação para essas operações não é clara. Os dados que temos sugerem que as operações são realizadas em "estágios" independentes. Alguns incluem consultas MX para domínios de destino e outros incluem um conjunto mais amplo de consultas por subdomínios aleatórios. Os dados de eventos DNS que contêm registros MX do GFW geralmente ocorrem em datas separadas daquelas em que vemos consultas MX em resolvedores abertos. Como os nomes de domínio são os mesmos em todos os estágios e as consultas são consistentes em todos os nomes de domínio, ambos em um período de vários anos, esses estágios certamente devem estar relacionados, mas não chegamos a uma conclusão sobre como se relacionam ou por que o agente usaria essas abordagens em estágios.

Considerando a pesquisa realizada até o momento, veja a seguir algumas ideias sobre possíveis motivações:

- Trata-se de um ataque DDoS? Não, pelo menos não na forma atual. O volume de consultas observado é muito baixo para afetar servidores autoritativos ou resolvedores intermediários. Também não há indicação de que haja um ataque de reflexo envolvido.
- Trata-se de exfiltração de dados? Isso é altamente improvável. O agente não controla os servidores de nomes autoritativos, utiliza rótulos de subdomínio curtos com capacidade mínima de transportar informações, parece transmitir pacotes amplamente e não controla o caminho de retorno.
- É uma varredura de resolução aberta? Também improvável. Entre as várias maneiras de encontrar resolvedores abertos, todas são mais simples do que o que observamos nesses eventos.
- Trata-se de um trabalho de mapeamento pela internet? Bem, possivelmente. Embora pareça uma operação altamente complicada para mapear redes.
- É um posicionamento prévio para ataques de DDoS? Possivelmente. Para ser eficaz para DDoS, o agente precisaria alterar consideravelmente a operação.
- É algum tipo de pesquisa de internet? Possivelmente. Se for esse o caso, trata-se de um programa de pesquisa de longa duração e sem um objetivo claro que eu possa discernir.
- É o resultado de um bug de software ou de algum outro aplicativo? Não. Essa explicação foi apresentada anteriormente pelos céticos em resposta à pesquisa do ExploderBot que realizamos. Nada nos dados apoia a conclusão de que são consultas incidentais ao DNS. As atividades do Muddling Meerkat são muito deliberadas e inteligentes.

É possível que algum outro agente estatal esteja fingindo ser o GFW e falsificando tanto consultas quanto respostas? Muitas coisas são possíveis, mas nem todas são plausíveis.

CONCLUSÃO E RECOMENDAÇÕES

Quando você passa tanto tempo como eu olhando para o DNS, às vezes se pergunta se há algo de normal nele. Depois de anos trabalhando nessa área, ainda aprendo coisas novas regularmente e observo o comportamento de novos agentes. Muitas vezes descobrimos um novo agente em consequência de algum outro agente não relacionado. Nesse caso, a investigação de uma rede chinesa ilegal de jogos de azar me levou a descobrir registros MX anômalos. Depois de seguir uma série de pistas falsas, formei uma imagem mais clara das operações do Muddling Meerkat quando trabalhei com pesquisadores externos para compartilhar dados e análises. No fim, embora eu esteja escrevendo este relatório, a análise e as conclusões são o resultado de um trabalho conjunto em que diferentes partes trouxeram uma perspectiva diferente para descobrir um comportamento não documentado anteriormente do GFW e uma misteriosa operação de DNS de vários anos.

Nossa pesquisa também destaca possíveis vulnerabilidades de rede que surgem da negligência e da complexidade das comunicações modernas pela internet. Em particular, recomendo que os administradores de rede:

- Procuram ativamente eliminar resolvedores abertos de suas redes. A identificação desses dispositivos pode ser difícil, mas empresas como a Infoblox e organizações como a Shadow Server Foundation podem oferecer informações essenciais para ajudar.
- Não utilize domínios que não sejam de sua propriedade para o Active Directory nem domínios de pesquisa de DNS. É muito provável que você vaze informações sobre sua rede e aplicativos de usuário para o servidor de nomes autoritativos, bem como para outros dispositivos fora de seu controle. Esse tipo de informação pode permitir que um agente mal-intencionado realize um reconhecimento passivo da rede para ataques direcionados.
- Incorpore detecção e resposta de DNS (DNSDR) em sua pilha de segurança. Somente um resolvedor de DNS pode lidar efetivamente com as ameaças inerentes ao DNS. A maioria dos produtos de segurança nem mesmo reconhecerá a diferença entre uma consulta MX e uma consulta de registro A.
- Relate a atividade do Muddling Meerkat para a comunidade. Como é impossível observar todo o escopo a partir de um único ponto de vista, é importante ter uma compreensão dessa ameaça por meio de crowdsourcing. Em particular, a comunicação de domínios adicionais do Muddling Meerkat ajudará outras pessoas a encontrar resolvedores abertos e atividades em sua rede.

Em última análise, compartilho as preocupações expressas pela CISA sobre a RPC e a ameaça de posicionamento prévio para ataques cibernéticos em todo o mundo. Em minha experiência profissional, descobri que os agentes de ameaças chineses são extremamente hábeis em gerenciar, compreender e aproveitar o DNS para muitas finalidades, seja censura, crime cibernético ou ataques de DDoS. Eles também têm alguns dos melhores pesquisadores da área. Seja qual for o objetivo real do Muddling Meerkat, não devemos subestimar o talento e a paciência da RPC para alcançá-lo.

INDICADORES DE ATIVIDADE (DOMÍNIOS-ALVO)

Observe que esses domínios não são indicadores de comprometimento ou necessariamente mal-intencionados. Alguns dos domínios utilizados pelo Muddling Meerkat estão estacionados, outros hospedam sites de jogos de azar e outros conteúdos possivelmente ilegais, e outros são domínios legítimos ativos. O escopo completo dos domínios-alvo do Muddling Meerkat é provavelmente muito maior.

Esses domínios não hospedam nenhum site, hospedam conteúdo ilegal ou estão estacionados. Provavelmente podem ser bloqueados sem impacto: `4u[.]com`, `kb[.]com`, `oao[.]com`, `od[.]com`, `boxi[.]com`, `zc[.]com`, `s8[.]com`, `f4[.]com`, `b6[.]com`, `p3z[.]com`, `ob[.]com`, `por exemplo[.]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`

Esses domínios hospedam sites e o bloqueio deles pode afetar negativamente sua rede: `ni[.]com`, `tt[.]com`, `pr[.]com`, `dec[.]com`

Endereços IP usados para lançar ataques:

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

INFORMAÇÕES SOBRE AMEAÇAS DA INFOBLOX

A Infoblox Threat Intel é a principal criadora de inteligência original contra ameaças ao DNS, destacando-se em um mar de agregadores. O que nos diferencia? Duas coisas: habilidades avançadas de DNS e visibilidade inigualável. O DNS é notoriamente complicado de interpretar e procurar, mas nosso profundo conhecimento e acesso exclusivo nos dão uma passagem para os bastidores do funcionamento interno da Internet. Somos proativos, não apenas defensivos, utilizando nossos insights para interromper o crime cibernético onde ele começa. Também acreditamos no compartilhamento de conhecimento para apoiar a comunidade de segurança mais ampla, publicando pesquisas detalhadas e divulgando indicadores no GitHub. Além disso, nossa inteligência é perfeitamente integrada às nossas soluções Infoblox DNS Detection and Response, de modo que os clientes obtêm automaticamente os benefícios dessa inteligência, juntamente com taxas ridiculamente baixas de falsos positivos.

infoblox.

A Infoblox une rede e segurança para oferecer desempenho e proteção incomparáveis. Confiada por empresas da Fortune 100 e inovadores emergentes, oferecemos visibilidade e controle em tempo real sobre quem e o que se conecta à sua rede, para que sua organização funcione mais rapidamente e detecte ameaças mais cedo.

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

+1,408,986,4000
www.infoblox.com

Versão: 20240216v1