infoblox

Threat Intel

MUDDLING MALSPAM : L'UTILISATION DE DOMAINES USURPÉS DANS LES SPAMS MALVEILLANTS

Auteurs:
Stelios Chatzistogias
Laura da Rocha
Renée Burton

TABLE OF CONTENT

Au premier abord, c'est une histoire d'échec de recherche, mais en réalité, c'est une histoire de découvertes inattendues.

En mars 2024, nous avons publié un article de blog sur un acteur que nous appelons Muddling Meerkat, qui mène des opérations DNS pour le moins curieuses via le Chinese Great Firewall. Nous avons passé beaucoup de temps à faire des recherches, mais nous n'avons pas réussi à comprendre le but de ces opérations sur plusieurs années. Au lieu d'abandonner ce travail, nous avons décidé de publier ce que nous savions sur cette activité afin que d'autres partagent leurs idées et que, collectivement, nous parvenions à comprendre la véritable nature de Muddling Meerkat. Et ça a porté ses fruits ! Le blog a attiré des idées de professionnels des réseaux et de la sécurité ; certains ont pu fournir des données anonymes sur leur vision de Muddling Meerkat, ou du moins des « domaines cibles » que nous voyons dans le DNS.

De nombreuses suggestions pour des recherches supplémentaires se concentraient sur les opérations de spam. Certaines entreprises avaient reçu des notifications d'abus pour des domaines qu'elles possédaient, généralement des domaines internes qui n'étaient pas utilisés en externe. Les rapports d'abus étaient la preuve d'une distribution de spam à grande échelle à de grands fournisseurs de messagerie tels que Google et Yahoo, et dans la majorité des cas, l'adresse IP source du spam était attribuée à la Chine. Cela semblait correspondre aux activités de Muddling Meerkat, dans lesquelles nous avons observé des faux enregistrements de serveur de messagerie (MX) provenant de l'espace IP chinois, ainsi que des requêtes MX similaires entrant dans les réseaux d'entreprise via des résolveurs ouverts.

L'un des fichiers de données partagés avec nous a conduit à une révélation : nous possédions nous-mêmes plusieurs domaines « cible » de Muddling Meerkat ! Ainsi, nous pouvons utiliser les rapports d'abus et les journaux des serveurs DNS pour mieux comprendre les activités de spam liées au DNS. Mais nous disposons également d'une bonne collection de spams, et nous avons pu rechercher des campagnes qui ont reflété le comportement de Muddling Meerkat au fil du temps.

Cet article est le résultat de notre chasse aux spams. Honnêtement, nous ne sommes pas sûrs d'avoir avancé dans l'analyse de Muddling Meerkat, ce qui pourrait sembler être un échec. Cependant, en suivant ces pistes, nous avons beaucoup appris sur l'utilisation de l'usurpation de domaine dans les campagnes modernes de spam malveillant (malspam). Nous allons partager quelques-unes de nos « captures » qui montrent les méthodes les plus intéressantes employées par les acteurs pour usurper des domaines aujourd'hui, toutes adoptant des comportements de type Muddling Meerkat. Nous avons pu relier ces campagnes aux rapports d'abus reçus des destinataires et à nos journaux DNS autoritaires. De plus, comme nous possédons certains des domaines usurpés, nous avons capturé quelques-uns en tant que retours vers nos serveurs de messagerie. En explorant ces sources, nous avons découvert que les domaines cibles de Muddling Meerkat sont passés d'environ de 20 à plus de 650 domaines.

Le plus surprenant est l'ampleur de l'usurpation de domaine dans le spam. Il existe plusieurs mécanismes conçus pour protéger les utilisateurs contre le spam en général et le spoofing en particulier, mais nous avons découvert que le spoofing était encore largement utilisé. La plupart des campagnes sont envoyées depuis des adresses IP chinoises, et la diversité des types de campagnes est vraiment remarquable. Malgré les mesures de sécurité, l'utilisation de domaines usurpés reste financièrement avantageuse. Dans ce document, nous examinerons les points suivants :

- Des campagnes modernes qui utilisent des codes QR dans des pièces jointes PDF pour escroquer les citoyens chinois,
- L'usurpation d'identité d'une marque populaire ciblant les utilisateurs japonais pour voler leurs identifiants de connexion,
- D'anciennes campagnes d'extorsion, probablement menées par des reliquats de botnet, qui tentent d'inciter les utilisateurs à payer sur le portefeuille de cryptomonnaies du cybercriminel, et
- Des campagnes financières mystérieuses qui ne semblent avoir aucun contenu malveillant mais qui n'ont également aucun but.

De plus, nous décrirons comment nous avons utilisé nos propres journaux de serveur DNS faisant autorité pour tenter de cerner Muddling Meerkat, mais nous avons plutôt intercepté ces campagnes de spam.

FALSIFICATION DE DOMAINE DANS LE SPAM

Les acteurs malveillants peuvent falsifier (usurper) l'adresse de l'expéditeur d'un e-mail. Ils le font pour donner l'impression que l'e-mail est plus légitime. En utilisant un domaine enregistré depuis de nombreuses années, ils sont plus susceptibles de contourner les mécanismes de sécurité qui vérifient l'âge du domaine de l'expéditeur pour identifier les spams malveillants. D'autre part, si l'acteur usurpe un domaine bien connu tel que amazon[.]com, il existe plusieurs mécanismes que le serveur de messagerie destinataire peut utiliser pour déterminer si un e-mail utilisant l'un de ces domaines a été usurpé. Nous pensons que ce risque de détection est la raison pour laquelle les spammeurs utilisent des domaines anciens et négligés, le même type de domaine que Muddling Meerkat privilégie pour leurs opérations.

Lorsqu'un serveur de messagerie reçoit un e-mail, il effectue plusieurs vérifications dans le DNS pour tenter de valider l'expéditeur. Il comparera ensuite ces résultats aux en-têtes des e-mails. Ces vérifications incluent des actions telles que la vérification que l'adresse IP à partir de laquelle l'e-mail a été reçu est autorisée à envoyer des e-mails pour ce domaine. Certaines de ces vérifications reposent sur des enregistrements DNS spécifiques qui, souvent, n'existent pas pour les domaines anciens et négligés, et peuvent entraîner un échec « indirect ».

Après les contrôles standard et l'application éventuelle d'algorithmes de sécurité, l'e-mail peut être marqué comme spam ou mis de côté. Dans d'autres cas, il pourrait atteindre la boîte de réception de l'utilisateur. L'acteur du malspam espère que ses e-mails synthétiques échapperont à suffisamment de filtres anti-spam pour parvenir jusqu'aux utilisateurs et en tirer des bénéfices.

SERVEURS DNS AUTORITAIRES ET SPAM

Il se trouve que nous possédons certains domaines inutilisés qui n'ont pas activement hébergé de contenu depuis près de 20 ans. Ils sont dépourvus de la plupart des enregistrements DNS, y compris ceux qui sont généralement utilisés pour vérifier l'authenticité d'un domaine expéditeur, par exemple les enregistrements SPF (Sender Policy Framework). Les domaines sont courts et appartiennent à des TLD très réputés : parfaits pour Muddling Meerkat et les spammeurs.

Ironiquement, plusieurs de nos anciens domaines sont souvent cités, par exemple, dans la liste des 1 million de domaines les plus populaires de Tranco. Nous soupçonnons que leur popularité est entièrement due au spam. Sans trop s'éloigner du sujet principal de ce blog, la popularité de nos domaines inactifs illustre parfaitement l'une des raisons pour lesquelles ces genres de classements doivent être pris avec des pincettes. Nous avons passé beaucoup de temps à étudier la popularité des domaines et les menaces ; consultez nos articles précédents.[1,2] (Pour lire les notes de bas de page, veuillez consulter ce PDF en ligne.)

Le DNS nous offre une perspective unique sur l'abus de nos domaines. Nous enregistrons les requêtes pour tous nos domaines sur notre serveur DNS autoritaire. Ces journaux nous offrent une vue sur un large éventail d'activités DNS, allant de l'analyse de l'internet à la distribution de spam. Dans le cas des e-mails, le serveur de messagerie du destinataire effectuera plusieurs requêtes DNS vers le serveur faisant autorité pour le domaine de l'expéditeur, y compris les enregistrements DNS TXT. D'après nos journaux, nous pouvons voir l'adresse IP des résolveurs DNS utilisés par ces serveurs de messagerie et nous faire une idée de la répartition géographique du spam qui falsifie nos domaines.

Nous avons également configuré des enregistrements DomainKeys Identified Email (DKIM) pour que les fournisseurs qui reçoivent du spam de nos domaines puissent nous envoyer des rapports d'abus par e-mail. Ces rapports d'abus incluent l'adresse IP de l'expéditeur de spam et les informations de l'horodatage. Nous pouvons les combiner avec les requêtes d'enregistrement TXT DNS pour obtenir une vue assez claire de la manière dont nous sommes faussement associés à la distribution de spam. Nos serveurs de messagerie ne transmettent pas d'e-mails, ils se contentent uniquement de les recevoir.

Comme nous nous intéressons à l'activité de spam potentielle de Muddling Meerkat, nous devons isoler les requêtes des autres acteurs potentiels. Le DNS est rempli de données indésirables. De nombreuses sociétés de recherche, comme la nôtre, effectuent des requêtes DNS pour collecter des informations et créer une empreinte synthétique dans les enregistrements historiques. Nos serveurs ne devraient pas recevoir de requêtes DNS car tous les domaines sont inactifs, pourtant ils reçoivent des milliers de requêtes chaque jour, parfois des dizaines de milliers. La figure 1 présente une comparaison du nombre de requêtes

reçues par notre serveur d'autorité pour quatre domaines différents de Muddling Meerkat au fil du temps. Le graphique du haut concerne tous les types d'enregistrements, celui du bas les requêtes MX. Ces graphiques chronologiques indiquent que l'activité liée aux e-mails n'est pas nécessairement corrélée avec l'activité DNS globale des domaines.

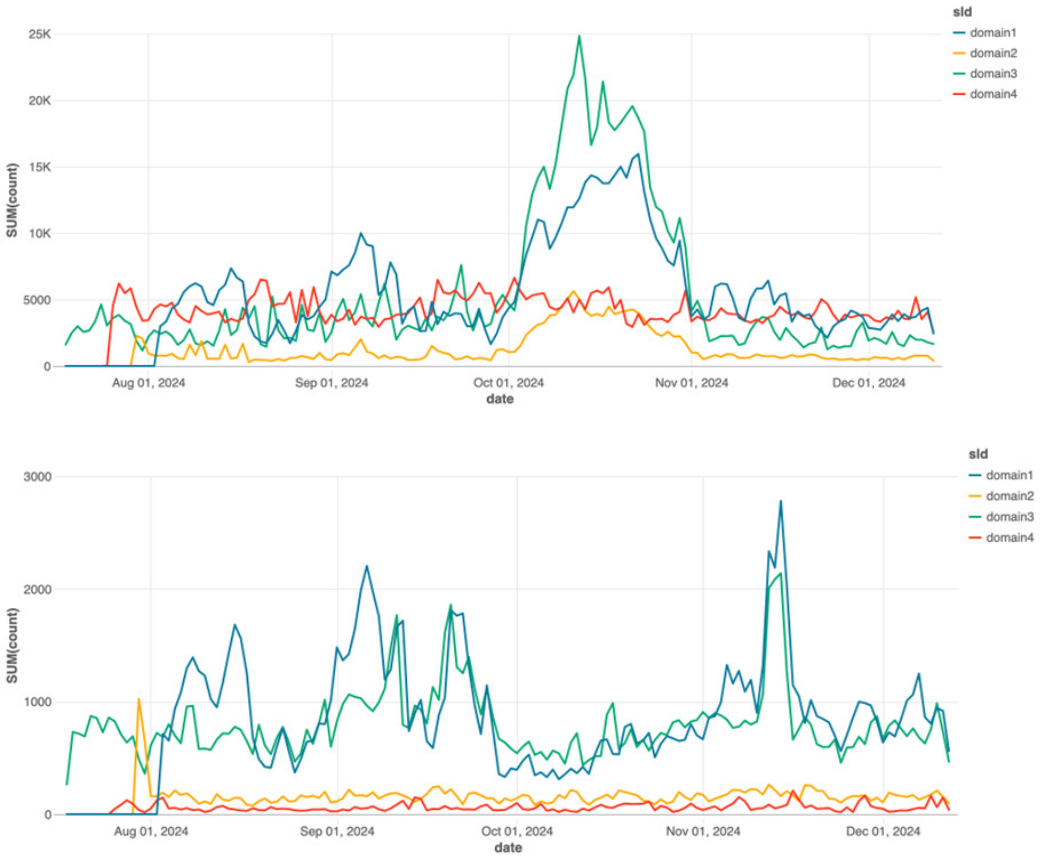

Figure 1. Graphique supérieur : volume de requêtes pour tous les types d'enregistrements DNS sur notre serveur faisant autorité par domaine ; graphique inférieur : volume de requêtes pour les enregistrements MX

La plupart des requêtes que nous recevons sur nos serveurs autoritaires ne correspondent pas aux modèles Muddling Meerkat, nous avons donc utilisé diverses empreintes basées sur des recherches antérieures pour isoler l'activité potentielle générée par l'acteur. Nous avons également comparé ces résultats aux rapports d'abus que nous avons reçus par e-mail.
Les requêtes DNS de Muddling Meerkat utilisent différents types d'enregistrements, mais les plus inhabituelles du point de vue des enquêtes sont les requêtes d'enregistrements MX pour des sous-domaines courts et aléatoires. Dans l'exemple suivant, si le domaine cible est target. domain, la requête ressemblerait à :

```
<rand>.target.domain
```

Le terme « cible » est ici très vague, comme nous l'avons expliqué dans notre précédent article[3], parce que l'acteur cible ces domaines pour les utiliser dans ses campagnes, plutôt que de les cibler dans le cadre d'une attaque contre les propriétaires de domaines ; l'acteur abuse de ces domaines qu'il ne possède pas dans un but inconnu. Nous avons limité notre analyse des requêtes à celles dont les noms d'hôte n'étaient vus que comme un sous-domaine d'un seul domaine que nous desservions et nous avons cherché à dégager des tendances.
La longueur des noms d'hôte observés de manière unique variait, mais ceux qui comportaient trois caractères étaient les plus fréquents (voir figure 2). Ce résultat est conforme aux données que nous avons reçues d'autres détenteurs de domaines. Nous avons également vérifié que les requêtes provenaient de grands fournisseurs de services de messagerie, tels que Google, et de fournisseurs de services de sécurité de la messagerie, tels que Proofpoint.

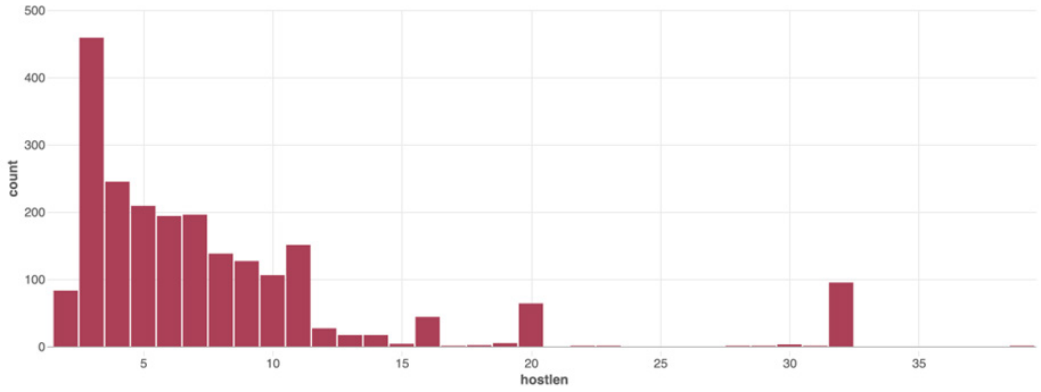

Figure 2. La longueur des noms d'hôte observés de manière unique dans les requêtes MX sur nos serveurs DNS autoritaires

Sachant que nos domaines étaient utilisés par Muddling Meerkat et qu'ils étaient usurpés par des cybercriminels menant des campagnes de malspam, nous avons traqué les campagnes actives avec nos filtres anti-spam.

PIÈGE N° 1 : CAMPAGNES DE PHISHING PAR CODE QR

Le plus grand groupe de campagnes de phishing que nous avons observé en usurpant nos anciens domaines ciblait les résidents de la Chine. Ces campagnes ont été menées de manière persistante depuis au moins la fin de 2022 et distribuent des pièces jointes contenant un code QR qui mène à un site de phishing ; voir la figure 3. D'après nos données DNS, les rapports d'abus et les informations collatérales, nous pensons que les attaques proviennent de Chine. Les campagnes exploitent une tactique qui implique que le destinataire ouvre la pièce jointe de l'e-mail et utilise WhatsApp pour scanner un code QR. Cette méthode en deux étapes pose des défis supplémentaires pour sécuriser les utilisateurs, car le pirate incite les victimes à passer de leur ordinateur portable à une application de messagerie chiffrée, contournant ainsi de nombreuses mesures de sécurité courantes. Les cybercriminels emploient également des algorithmes de génération de domaines enregistrés (RDGAs) pour créer des domaines aléatoires actifs uniquement pendant une courte période.

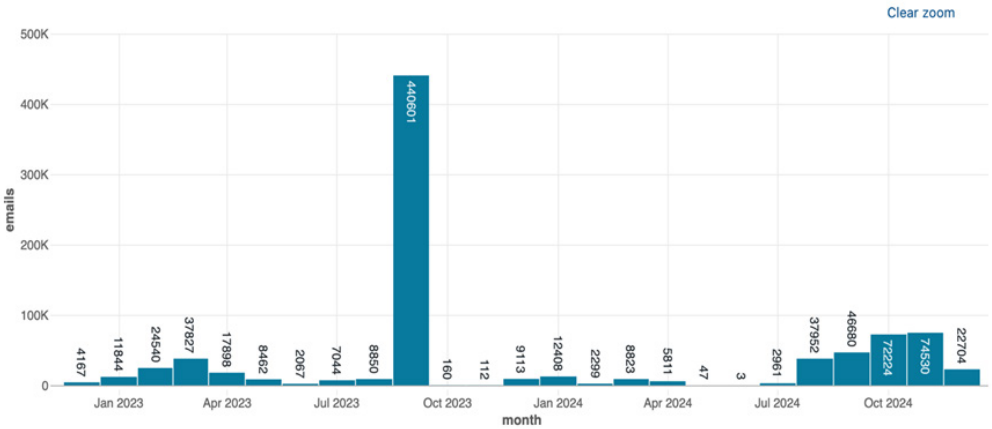

Figure 3. Évolution du volume des e-mails de phishing par code QR chinois

Ces campagnes de malspam utilisent des domaines d'expéditeur usurpés qui incluent un grand nombre de domaines cibles confirmés de Muddling Meerkat, y compris des domaines que nous possédons. Grâce à l'analyse du spam de ces campagnes et à la comparaison des enregistrements DNS historiques, nous avons augmenté le nombre de domaines cibles connus de Muddling Meerkat d'environ 20 en mars 2024 à plus de 650 aujourd'hui. Les campagnes de codes QR, cependant, contiennent également de nombreux domaines que Muddling Meerkat pourrait bien utiliser, mais que nous ne pouvons pas confirmer via le DNS.

Ces campagnes utilisent des adresses e-mail d'expéditeurs dont la structure correspondait à ce que nous avons observé dans les requêtes DNS de Muddling Meerkat. Le nom d'utilisateur de l'expéditeur était une courte chaîne aléatoire sous la forme `<rand>@spoofed[.]domain`. Le tableau 1 montre un échantillon des adresses e-mail des expéditeurs de la campagne au fil du temps. Les domaines tels que `jx[.]com` et `hm[.]com` étaient déjà connus pour être des domaines cibles de Muddling Meerkat.

dm@**jx**[.]**com**	ino@**jjnywnd**[.]**com**
ab@**hm**[.]**com**	gwhy@**isathtooy**[.]**net**
zb@**iizlopn**[.]**com**	atmrp@**kym**[.]**net**
mu@**ibqg**[.]**net**	qivlzn@**kt**[.]**com**
xzu@**iejzhopjx**[.]**org**	atmrp@**kym**[.]**net**
iud@**irnvasa**[.]**net**	

Tableau 1 : exemple d'adresses d'expéditeurs pour la campagne de codes QR ; les e-mails des expéditeurs suivent le schéma <2-9 random chars>@<spoofed[.]domain>

L'e-mail comprend généralement un leurre fiscal en mandarin et a commencé en décembre 2022 ou avant. Ces adresses semblent provenir de l'espace IP chinois, principalement 4134 (Chinanet) et 56046 (China Mobile). La figure 4 montre quelques lignes d'objets d'e-mails et leurs traductions en anglais.

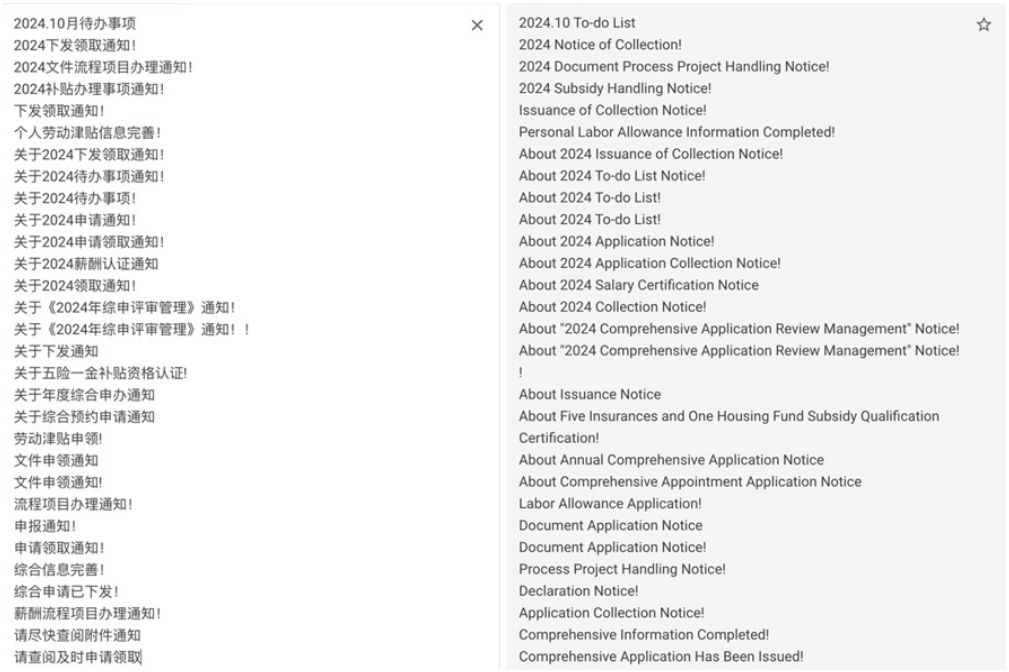

Figure 4 : exemple d'objets d'e-mails de campagnes de codes QR traduits

Une autre caractéristique distinctive de ce malspam est que la plupart des documents de code QR sont chiffrés avec un mot de passe à quatre chiffres, qui est inclus quelque part dans le corps de l'e-mail, mais pas de manière cohérente. Parfois, ils sont entre parenthèses ou peuvent être entourés d'autres symboles. La figure 5 présente deux exemples de la façon dont les mots de passe sont intégrés dans les e-mails.

Figure 5. Deux exemples de la manière dont la valeur et le format du mot de passe à quatre chiffres peuvent varier dans différents e-mails ; les cases rouges et vertes soulignent les différentes façons dont le mot de passe apparaît dans un e-mail

Les pièces jointes contiennent un code QR avec un logo intégré et des instructions pour que le destinataire utilise AliPay/WeChat pour scanner le document ; voir la figure 6. Ces e-mails sont similaires à ceux utilisés par les cybercriminels du monde entier pour exploiter les populations vulnérables en promettant des subventions et des avantages financiers.

Figure 6. Contenu et traduction de la pièce jointe ; la partie surlignée comprend l'instruction d'utiliser Alipay/WeChat pour scanner le code QR

Des utilisateurs sur X (anciennement Twitter) ont signalé l'arnaque. Selon le tweet[4] de la figure 7, un utilisateur a été invité à saisir un numéro de carte et des informations d'identification après avoir scanné le code QR. Il lui a ensuite été demandé de saisir le montant et le code de vérification, qu'il a supposé correspondre à un paiement sur son compte. Peu de temps après, un message texte l'a averti qu'il avait payé 590 euros avec sa carte au pirate. C'est un excellent retour sur investissement pour un e-mail de spam !

Figure 7. Tweet d'un utilisateur qui a été trompé par l'arnaque de phishing par code QR

Ce stratagème s'appuie sur des domaines de phishing de deuxième étape qui ont une durée de vie très courte et qui semblent être délimités géographiquement. Ils ne sont pas résolus dans le DNS après environ un jour et se trouvent dans des TLD couramment utilisés comme sbs, shop, life, bond et cn. Ces domaines sont constitués d'un ensemble aléatoire de caractères, par exemple `aaaefiuibew[.]cn` ou `6ttox81[.]sbs`.

Nous ne sommes pas en mesure de dire si cette activité provient de Muddling Meerkat. Il semble plus probable qu'il s'agisse d'un système de phishing-as-a-service (PhaaS) courant. Bien que les campagnes utilisent les domaines négligés que nous observons avec Muddling Meerkat, elles semblent usurper largement des domaines aléatoires, y compris ceux qui n'existent pas. L'acteur malveillants peut utiliser cette technique pour éviter des e-mails répétés du même expéditeur. Malgré les efforts déployés pour protéger les utilisateurs contre les spams malveillants, certains de ces spams parviennent à se frayer un chemin et sont suffisamment rentables pour être maintenus.

Les autres domaines d'expéditeurs observés dans cette activité sont présentés dans le tableau 2.

len2	len3	len4	len5
jt[.]net	iac[.]com	idhs[.]org	ivkpc[.]net
hc[.]com	izr[.]com	jxrn[.]org	jbdct[.]net
kk[.]net	koh[.]com	jirh[.]org	jfctl[.]org
jg[.]com	jwq[.]org	ismh[.]com	irnpc[.]net
kx[.]com	kcy[.]org	ikat[.]com	lahuf[.]net
len6	**len7**	**len8**	**len9**
jxjfwz[.]net	kbgpnek[.]org	jqmyuxk[.]com	hfababhqf[.]org
jxnsdf[.]net	ipcwfrn[.]com	jwruoytd[.]org	jfrcjfqjr[.]com
jwnlhr[.]org	iouwttz[.]com	ktfnmbxa[.]org	jkdduscaj[.]net
kindhy[.]net	jhrzbuk[.]org	jlsiwslr[.]org	jkjiwbpki[.]com
khznrl[.]com	hrggzxa[.]com	hrfliqoj[.]net	kwbjjlygw[.]net

Tableau 2. Exemples de domaines usurpés observés dans les campagnes de phishing par code QR

Une fois que nous avons réalisé que les campagnes de codes QR usurpaient des domaines qui ne correspondaient pas à ce que nous attendions de Muddling Meerkat, nous nous sommes tournés vers le DNS et notre collection de spams pour rechercher d'autres campagnes susceptibles d'être menées par l'acteur Muddling Meerkat.

PIÈGE N° 2 : CAMPAGNES DE PHISHING JAPONAISES

Sur nos serveurs DNS autoritaires, nous avons remarqué qu'un pourcentage inhabituellement élevé de requêtes liées aux e-mails incluait des noms d'hôte à trois lettres. Alors que nous tentions de distinguer les requêtes susceptibles d'être générées par Muddling Meerkat de celles attribuables aux scanners et à d'autres sources, le volume et la régularité de ces requêtes nous ont paru constituer une piste d'investigation prometteuse. Par conséquent, nous avons cherché des preuves de spam ayant la même structure de requête.

Nous avons découvert une série de campagnes ciblant les utilisateurs japonais avec des e-mails faisant référence à des marques populaires telles que Electronic Toll Collection (ETC, utilisé sur les autoroutes à travers le Japon), Sumitomo Mitsui Banking Corporation (SMBC, l'une des plus grandes banques japonaises), ainsi qu'Amazon et Mastercard. Les e-mails invitent l'utilisateur à s'authentifier auprès du service en raison d'un problème de sécurité ou autre. Un bouton inclus dans l'e-mail conduit l'utilisateur vers un système de distribution de trafic (TDS) et le redirige vers une fausse page de connexion si certains critères sont remplis.[5] Cette méthode est courante dans la publicité malveillante et est utilisée pour masquer la page de destination finale afin d'éviter qu'elle ne soit détectée par les sociétés de sécurité. La fausse page de connexion vole les informations d'identification de la victime lorsqu'elle les saisit. La figure 8 montre un exemple de ces e-mails de spam.

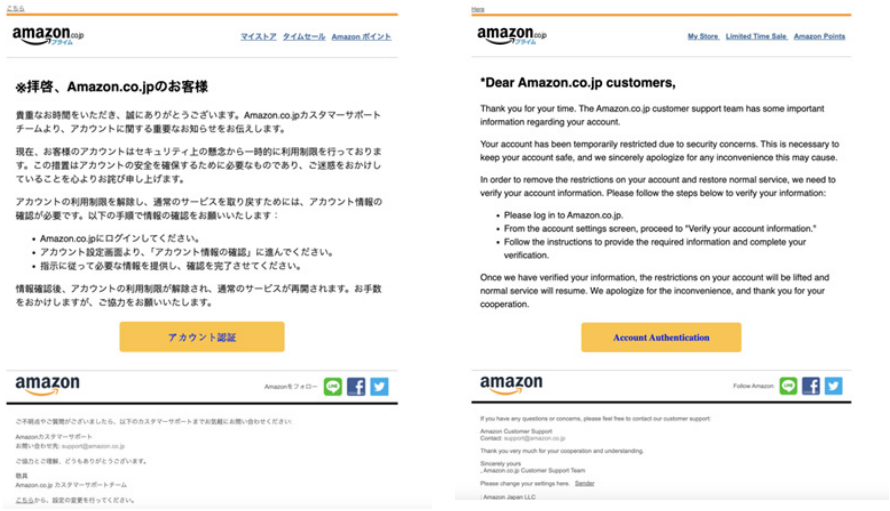

Figure 8. Exemple original d'e-mail de spam ciblant les utilisateurs japonais avec de faux avertissements Amazon et une traduction automatique de l'e-mail

Une fois que l'utilisateur clique sur le bouton « Authentification du compte » :

- Ils seront dirigés vers `ubrjubf[.]com`, pointant vers l'IP `43.128.150[.]42`
- L'utilisateur sera ensuite redirigé vers un autre domaine , `unpwple[.]com`, qui se résout sur l'IP `43.133.182[.]243`.
- L'utilisateur arrive sur une fausse page de connexion au compte Amazon ; voir la figure 9

Figure 9. Fausse page de connexion Amazon ; référence de l'image : https://urlscan.io/result/5c9bbf63-883f-4eab-b4fc-45e2809a8ac2/

Nous avons observé plusieurs variantes de spam concernant Amazon, ainsi que des leurres utilisant Mastercard et SMBC Vpass.[6] Cet acteur malveillant utilise une infrastructure d'hébergement dédiée et fait tourner les campagnes sur les mêmes domaines et adresses IP.[7] Les deux adresses IP dédiées observées étaient `43.128.150[.]42` et `43.133.182[.]243`. Le tableau 3 fournit une liste des domaines RDGA utilisés dans les campagnes.

43.128.150[.]42	43.133.182[.]243
eujsubf[.]com, eujsxikw[.]com,	anzcinf[.]xyz, anzconc[.]xyz,
ikhcok[.]com, insjibr[.]com,	infkokf[.]com, omfkiht[.]xyz,
insjkf[.]com, khcpw[.]com,	omfkybg[.]xyz, inybinf[.]com,
maczplw[.]com, maczunf[.]com,	unpwple[.]com, inybubf[.]com,
pknribt[.]com, pknrinf[.]com,	pplaaej[.]com, eccteukx[.]com,
pknrinr[.]com, pknrohv[.]com,	espoeubf[.]com, unpwmlw[.]com,
pknrybg[.]com, pknrynf[.]com,	pplaaeu[.]com, ecctenje[.]com,
ubrjpnf[.]com, ubrjubf[.]com,	unpwibr[.]com, ecctepje[.]com,
unpwinf[.]com, uwkxubs[.]com,	pplaaep[.]com, pplaaea[.]com,
wkxaubf[.]com, wkxaunf[.]com	espoeunf[.]com, espoekwl[.]com

Tableau 3. Échantillon de domaines RDGA sur des adresses IP dédiées utilisées dans des campagnes ciblant les utilisateurs japonais

Comme les campagnes décrites dans la section précédente, les e-mails de ces campagnes utilisent des domaines d'expéditeur usurpés, y compris des domaines appartenant à Infoblox Threat Intel. Ils suivent également le format que nous avons trouvé prévalent sur nos serveurs DNS autoritaires avec un sous-domaine de trois caractères, ainsi que dans les rapports d'abus que nous avons reçus des fournisseurs de messagerie. Le tableau 4 présente un échantillon des adresses e-mail des expéditeurs.

ak@fdd.**xpv[.]org**	iipnf@gvy.**zxdvrdbtb[.]com**
mh@thq.**cyxfyxrv[.]com**	zmrbcj@bce.**xnity[.]net**
mfhez@shp.**bzmb[.]com**	nxohlq@vzy.**dpyj[.]com**
gcini@vjw.**mosf[.]com**	

Tableau 4. Un échantillon d'adresses d'expéditeurs pour des e-mails de phishing japonais avec des sous-domaines de trois lettres ; les noms d'hôte de trois lettres sont colorés en rouge, tandis que le domaine usurpé est en gras

Ce n'était pas le seul type de campagne que nous avons observé ciblant les utilisateurs japonais. Un autre appât majeur comprenait MyEtherWallet, un portefeuille de cryptomonnaies populaire, et utilisait des domaines similaires. Les messages de spam incluent parfois du texte japonais, par exemple, « (重要なお知らせ) MyEtherWallet ご利用確認のお願い », qui se traduit par « [Avis important] Demande de confirmation de l'utilisation de MyEtherWallet », et demandent aux utilisateurs de se connecter à leur compte. Voir la figure 10 pour un exemple d'e-mail en anglais. Bien que le lien semble mener au véritable site web, il mène en réalité à un domaine similaire créé par le cybercriminel.

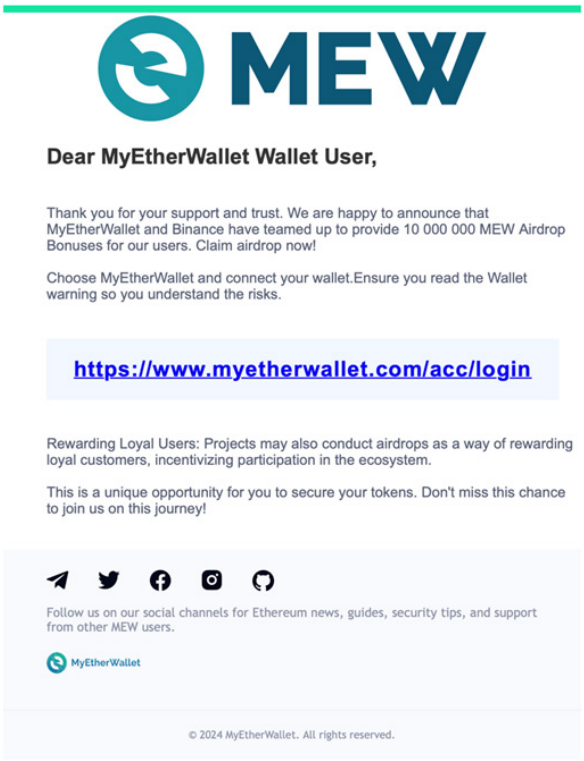

Figure 10. Exemple de campagne de spam ciblant les utilisateurs japonais ; cet e-mail avait pour objet « Binance Distribution of MyEtherWallet (MEW) Airdrop » et conduisait l'utilisateur à `myetherwallatak[.]org`

Les domaines similaires ont conduit à une copie miroir du site Web MyEtherWallet et ont été utilisés pour voler les identifiants des utilisateurs. Ces domaines se trouvent dans plusieurs TLD différents, y compris com et org ; voir le tableau 5 pour un échantillon.

myetherwalletie[.]com	myetherwalletih[.]com	myetherwalletik[.]com
myetherwalletiv[.]com	myetherwalletjp[.]com	myetherwalletrt[.]com
myetherwallettv[.]com	myetherewallet[.]org	myetherswallet[.]org
myetherwallata[.]org		

Tableau 5. Exemples de domaines similaires utilisés pour hameçonner les identifiants des utilisateurs japonais.

Dans la campagne de phishing par code QR, les domaines Muddling Meerkat ont été observés dans les soi-disant adresses d'expéditeur, c'est-à-dire les adresses e-mail visibles pour le destinataire. Cependant, dans cette variante japonaise, les domaines apparaissent dans la section « de la part de » du message, qui est utilisée pour la distribution technique via SMTP. Nous avons identifié une autre série de campagnes de spam malveillantes utilisant les mêmes domaines que ceux observés dans les opérations de Muddling Meerkat, y compris un format de sous-domaine similaire, mais nous ne pouvons pas confirmer qu'elles sont l'œuvre de Muddling Meerkat. Le tableau 6 présente un échantillon des domaines usurpés.

len2	len3	len4	len5
xl[.]com	tgt[.]org paf[.]org	iddm[.]org	fhqqc[.]com
gz[.]net	bcc[.]com	yqqb[.]org	mseur[.]com
ed[.]org	zla[.]com	nvso[.]net	ofddy[.]com
df[.]org	tgf[.]net	nqui[.]com	agejx[.]net
wx[.]com		duth[.]net	mlngi[.]com
len6	**len7**	**len8**	**len9**
kwwezx[.]net	gbiutoj[.]com	mitsxpjh[.]com	nxbfvjkhr[.]org
bwidqv[.]com	jeihdgt[.]com	wtfmbcvt[.]com	lkhyleslk[.]net
piuxic[.]com	qspdwhc[.]com	jgggzbmq[.]org	nmshofzmh[.]net
xdgzas[.]com	grjfgpw[.]net	qqegowhv[.]org	ykbhnoers[.]com
nwfffu[.]org	vudgfcm[.]net	invphyzf[.]com	mqnbqsygn[.]org

Tableau 6. Exemples de domaines usurpés observés dans les campagnes MyEtherWallet

L'une des lacunes dans la compréhension de ces campagnes est que le nombre de domaines que nous avons découverts est probablement trop faible pour valider que tous les domaines se chevauchent avec Muddling Meerkat. Cependant, cet ensemble de campagnes est un autre exemple de la façon dont les acteurs de la menace liés à la Chine utilisent l'usurpation de domaine pour leurs opérations de spam.

Sur ce, retournons à nos filtres anti-spam.

PIÈGE N° 3 : CAMPAGNES D'EXTORSION CONNUES

Non seulement avons-nous découvert une usurpation de domaine dans le code QR et les campagnes en langue japonaise, mais nous l'avons également trouvée dans des campagnes exploitant des tropes de spam bien connus. Les e-mails d'extorsion affirmant qu'un pirate informatique a accédé à l'appareil de l'utilisateur et enregistré des activités embarrassantes sont monnaie courante dans le monde du malspam. Nous avons été quelque peu surpris de découvrir qu'ils utilisent également des domaines d'expéditeur usurpés, mais avec une particularité : l'acteur usurpe l'adresse e-mail de l'utilisateur et le met au défi de la vérifier. L'e-mail informe l'utilisateur que son appareil a été compromis, et comme preuve, l'acteur prétend que le message a été envoyé depuis le compte de l'utilisateur. Et pourtant, ce n'est pas le cas ; les en-têtes d'e-mail indiquent qu'il est passé par des adresses IP chinoises, et non par celles de l'utilisateur. Voir la figure 11 ci-dessous pour un exemple du contenu de l'email.

L'e-mail indique à l'utilisateur de payer l'expéditeur en échange de la suppression du malware de son appareil et inclut une adresse de portefeuille Bitcoin, qui varie d'un message de spam à l'autre. Nous ne savons pas s'il s'agit d'un service d'extorsion ou si le même acteur utilise plusieurs portefeuilles. Dans les exemples que nous avons recueillis, les victimes sont invitées à payer 1 800 dollars américains. Bien qu'il puisse sembler surprenant que de nombreux utilisateurs lisent ces e-mails de spam, et encore moins qu'ils agissent en conséquence, il semblerait que l'escroquerie fonctionne. En vérifiant le solde de ces portefeuilles avec `bitref[.]com`, nous constatons qu'ils contiennent des fonds importants ; l'un d'entre eux contenait près de 26 000 USD.

Bonjour ! J'ai malheureusement une mauvaise nouvelle à vous annoncer. Il y a quelque temps, votre appareil a été infecté par mon cheval de Troie privé, R.A.T (Remote Administration Tool), si vous voulez en savoir plus à ce sujet, utilisez simplement Google. Mon cheval de Troie m'a permis d'accéder à vos fichiers, à vos comptes et à votre caméra. Vérifiez l'expéditeur de cet e-mail, je l'ai envoyé depuis votre compte e-mail. Pour être sûr de lire cet e-mail, vous le recevrez plusieurs fois. Vous aimez vraiment regarder des vidéos cochonnes! Je vous ai enregistré (via la caméra de votre appareil)! Ensuite, j'ai supprimé mes malwares pour ne pas laisser de traces. Si vous doutez encore de mes intentions sérieuses, il suffit de quelques clics de souris pour partager la vidéo de vous avec vos amis, vos parents, tous vos contacts e-mail, sur les réseaux sociaux et le darknet. Il vous suffit de transférer 1 800 USD en bitcoins (BTC) sur mon compte. Une fois la transaction réussie, je procéderai à la suppression de tout. Soyez-en sûr, je tiens mes promesses. Vous pouvez facilement acheter des bitcoins (BTC) ici : https://cex.io/buy-bitcoins https://nexo.com/buy-crypto/bitcoin-btc https://bitpay.com/buy-bitcoin/?crypto=BTC https://paybis.com/ https://invity.io/buy-crypto Ou simplement chercher d'autres échangeurs sur Google. Ensuite, envoyez les bitcoins (BTC) directement dans mon portefeuille, ou installez le logiciel gratuit : Atomicwallet, ou : Exodus wallet, puis recevez et envoyez au mien. Mon adresse Bitcoin (BTC) est : 1GtGZpzfRkAVBL48F68mi8bTcatwpTZGm8 Oui, c'est à cela que ressemble l'adresse, copiez et collez mon adresse, c'est (cAsE-sEnSEtiVE). Vous disposez d'un délai maximum de 3 jours après l'ouverture de cet e-mail. Comme j'ai accès à ce compte e-mail, je saurai si cet e-mail a déjà été lu. Tout se passera dans le respect de l'équité. Un conseil de ma part, changez régulièrement tous les mots de passe de vos comptes et mettez à jour votre appareil avec les correctifs de sécurité les plus récents.

Figure 11. Un exemple de spam d'extorsion qui utilise des domaines d'expéditeur usurpés

Il semble probable que ces campagnes, et peut-être beaucoup d'autres utilisant des domaines d'expéditeur usurpés, proviennent de robots spammeurs persistants. Les pirates ne valident pas les adresses e-mail des victimes pour s'assurer qu'elles sont bien reçues ou lues. Nous avons des cas où l'adresse e-mail du destinataire était associée à l'un de nos domaines qui a hébergé du contenu pour la dernière fois en 2007 et qui n'a pas eu d'utilisateurs d'e-mail depuis plus de 15 ans. Il n'existe aucun dossier de violation qui pourrait expliquer pourquoi ces e-mails ont été déclenchés, et nous ne savons pas si, en réalité, ces utilisateurs ont jamais existé.

Cette campagne, ainsi que d'autres campagnes de spam similaires que nous avons trouvées, évoque des images de canons à spam abandonnés à la dérive dans l'espace Internet. Nous avons également vu d'anciens vers transmis, un autre signe de restes de botnet laissés à l'abandon pendant que les spammeurs malveillants passaient à des techniques telles que les codes QR et les fausses pages de compte comme celles que nous avons montrées ci-dessus. Ces campagnes, désormais probablement en pilote automatique, semblent être des échos plus probables que le travail plus récent d'un acteur sophistiqué comme Muddling Meerkat.

PIÈGE N° 4 : E-MAILS MALVEILLANTS SUSPECTS

Ce programme de recherche a débuté par un mystère, et nous conclurons cet article par un autre : une campagne de spam très active utilisant des domaines d'expéditeur usurpés et comprenant des pièces jointes de feuilles de calcul Excel apparemment anodines sans but évident. Nous ne pouvons pas expliquer le motif de ces e-mails, qui usurpent les mêmes types de domaines que Muddling Meerkat utilise.

Ces e-mails proviendraient de 上海亚凯, qui se traduit par « Shanghai Yakai», le nom d'une entreprise de fret chinoise. Les adresses e-mails varient considérablement et incluent des noms d'utilisateur synthétiques tels que « Edward.Evelyn » et « Heidi.Gracie ». Les campagnes ont été observées deux jours sur trois en 2024, mais n'ont pas varié. La ligne d'objet indique que l'e-mail contient de nouvelles mises à jour des tarifs de fret, et la pièce jointe est une feuille de calcul unique nommée : 上海亚凯国际运价表.xlsx. Nous n'avons trouvé aucun contenu malveillant dans ces fichiers.

Il n'y a pas de bouton d'action (CTA) dans l'e-mail. En apparence, il s'agit simplement d'un ensemble de tarifs de fret mis à jour en permanence pour une société de transport maritime chinoise. Mais dans quel but ? Ces e-mails ne semblent pas être envoyés aux clients qui ont oublié de modifier leur adresse e-mail ou de se désabonner. L'utilisation de l'usurpation de domaine élimine toute légitimité, et il est difficile de comprendre pourquoi une entreprise de transport ou un acteur malveillant enverrait de tels e-mails. Le tableau 7 présente un échantillon des domaines des expéditeurs.

len4	len5	len6	len7
igeb[.]net	accou[.]com	axegal[.]com	awpking[.]com
kwfm[.]com	drsmj[.]com	devsmx[.]com	comitis[.]com
pqhh[.]com	eddim[.]com	glypix[.]com	donmenn[.]com
rrbc[.]com	hetoo[.]com	gulart[.]net	fundsle[.]com
tkee[.]net	horek[.]com	jomila[.]net	karnege[.]com
tnmc[.]com	memsz[.]com	mzylla[.]com	mtrplay[.]com
ukei[.]net	svard[.]net	okayme[.]com	rajprem[.]com
utpz[.]com	tapli[.]net	theiwl[.]com	techsox[.]com
vbhh[.]com	uweko[.]com	vaites[.]com	tjipbpo[.]com
wuwo[.]com	youbi[.]com	ynglet[.]com	wulthur[.]net

Tableau 7. Exemple de domaines d'expéditeurs usurpés utilisés dans le spam de la société de fret Shanghai Yakai

Une technique de campagne similaire a été observée dans les spams personnels, mais au lieu de messages provenant d'une entreprise de fret, l'e-mail fournit des valeurs de fonds communs de placement d'une société d'investissement indienne. Ces messages, que Google Mail signale comme des spams suspects, contiennent également une feuille de calcul inoffensive et un fichier PDF. Dans ce cas, le nom d'utilisateur de l'expéditeur est celui d'une ancienne connaissance, et il est probable que son compte de messagerie ait été piraté à un moment donné pour être utilisé dans des opérations de spam. Mais comme dans le cas du spam chinois relatif au fret, on ne voit pas très bien en quoi ces messages ont une valeur pour l'auteur du spam.

VUE DEPUIS LE SERVEUR DNS FAISANT AUTORITÉ

Muddling Meerkat a mené d'étranges opérations DNS pendant plus de six ans. Celles-ci impliquent de fausses réponses du Chinese Great Firewall et l'utilisation de domaines longtemps négligés qu'ils ne contrôlent pas. Bien que leur activité DNS comprenne plusieurs types d'enregistrements, les fausses réponses concernent les enregistrements MX du domaine de base ou cible. Par exemple, des réponses DNS contenant des enregistrements MX pour `kb[.]com` sont observées à partir d'adresses IP chinoises, même si `kb[.]com` n'a aucun enregistrement MX. De plus, ces faux enregistrements incluent un nom d'hôte court et aléatoire qui n'est observé qu'une seule fois au fil du temps, par exemple, `x4rd.kb[.]com`, qui pourrait être un enregistrement MX observé pour `kb[.]com`. Lors de notre première publication en mars 2024, nous avions identifié environ 20 domaines de ce type, mais nous en avons maintenant confirmé plusieurs centaines d'autres.

En plus de rechercher des preuves d'opérations de spam de la part de l'acteur malveillant, nous avons également analysé les journaux DNS sur nos serveurs faisant autorité et tenté de les faire correspondre aux fausses réponses DNS observées dans les données collatérales pour

les domaines que nous possédons. L'hypothèse était que si nous pouvions voir une requête pour l'un des faux domaines d'enregistrement MX, par exemple `x4rd[.]our[.]domain`, nous pourrions utiliser l'adresse IP du requérant pour mieux comprendre les opérations de Muddling Meerkat. Malheureusement, nous n'avons pas pu établir de correspondance définitive entre les enregistrements de Muddling Meerkat et les requêtes sur nos serveurs.

Que signifie l'impossibilité de trouver cette correspondance ? Cela signifie que la personne ou l'entité qui reçoit les fausses réponses MX, par exemple `x4rd[.]our[.]domain`, n'utilise pas ces réponses dans des requêtes DNS ultérieures et ne semble pas les utiliser pour du spam. Cette absence de motivation claire semble anéantir l'idée d'un botnet recevant des domaines à utiliser dans des e-mails falsifiés. Alors, à quoi servent les réponses ? Aucune idée. Muddling Meerkat reste un mystère. Vous avez des idées ou un point de vue différent ? Nous aimerions connaître votre avis.

CONCLUSION

Nous n'avons pas pu déterminer ce que Muddling Meerkat préparait, mais notre enquête a finalement été couronnée de succès : nous avons beaucoup appris sur la manière dont les acteurs malveillants utilisent des domaines usurpés dans les malspam, ce qui peut nous renseigner sur les façons de les contrer. Pour les chercheurs en menaces comme nous, cette perspicacité est souvent tout aussi importante que de connaître les intentions qui les motivent.

On ne peut pas toujours avoir ce qu'on veut dans la vie, mais il se pourrait que vous découvriez qu'on peut obtenir ce dont on a besoin.[8]

INFOBLOX THREAT INTEL

Infoblox Threat Intel est le principal créateur de la threat intelligence DNS originale, se distinguant parmi une multitude de collecteur. Qu'est-ce qui nous distingue ? Deux choses : des compétences DNS exceptionnelles et une visibilité inégalée. Le DNS est complexe à analyser et à suivre, mais grâce à notre expertise et à notre accès privilégié, nous pouvons cibler les cybermenaces avec une grande efficacité. Nous sommes proactifs, pas seulement défensifs, et nous utilisons nos connaissances pour empêcher la cybercriminalité de sévir là où elle prend naissance. Nous croyons également au partage des connaissances pour soutenir la communauté de sécurité au sens large en publiant des recherches détaillées et en publiant des indicateurs sur GitHub. En outre, nos informations sont intégrées de manière transparente dans nos solutions Infoblox de détection et de réponse DNS, de sorte que les clients bénéficient automatiquement de leurs avantages, ainsi que de taux de faux positifs ridiculement bas.

Siège social
2390 Mission College Boulevard, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

Version : 20241223v1