infoblox

Threat Intel

MUDDLING MALSPAM: DIE NUTZUNG GEFÄLSCHTER DOMAINS IN BÖSARTIGEM SPAM

Autoren:
Stelios Chatzistogias
Laura da Rocha
Renée Burton

INHALTSVERZEICHNIS

Dies mag zunächst wie eine Geschichte über gescheiterte Forschung klingen, aber es ist eigentlich eine Geschichte darüber, wie die Forschung nach einer Sache suchen und am Ende etwas völlig anderes entdecken kann.

Im März 2024 veröffentlichten wir einen Blogbericht über einen Akteur, den wir Muddling Meerkat nennen, der rätselhafte DNS-Operationen über die chinesische Große Firewall durchführt. Wir hatten erheblich Zeit in unsere Forschung investiert, konnten jedoch den Zweck dieser mehrjährigen Operationen nicht ermitteln. Anstatt die Arbeit in der Schublade verschwinden zu lassen, beschlossen wir, unser Wissen über die Aktivität zu veröffentlichen, damit andere ihre eigenen Erkenntnisse teilen können und wir gemeinsam vielleicht die wahre Natur des Muddling Meerkat verstehen lernen. Es hat funktioniert! Der Blog bezog seine Ideen sowohl von Fachleuten aus dem Bereich Networking als auch aus dem Bereich Sicherheit. Einige konnten anonymisierte Daten über ihre eigene Sicht auf Muddling Meerkat oder zumindest die sogenannten „Ziel-Domains“ bereitstellen, die wir im DNS sehen.

Viele der Vorschläge für weitere Untersuchungen konzentrierten sich auf Spam-Operationen. Einige Unternehmen hatten Missbrauchsmeldungen für Domains erhalten, die ihnen gehörten, in der Regel interne Domains, die nicht extern genutzt wurden. Die Missbrauchsmeldungen waren ein Beweis für die großflächige Spam-Verbreitung an große E-Mail-Anbieter wie Google und Yahoo, und die IP-Quelle des Spams wurde überwiegend China zugewiesen. Dies schien mit den Aktivitäten von Muddling Meerkat übereinzustimmen, bei denen wir gefälschte Mail-Server-Einträge (MX) aus dem chinesischen IP-Raum sowie ähnliche MX-Anfragen sahen, die über offene Resolver in Unternehmensnetzwerke gelangten.

Eine der uns zur Verfügung gestellten Dateien führte zu einer Offenbarung: Wir besaßen selbst mehrere „Ziel“-Domains von Muddling Meerkat! Das bedeutete, dass wir Missbrauchsmeldungen, die uns für diese Domains geschickt wurden, sowie DNS-Protokolle der autoritativen Nameserver verwenden konnten, um die Spam-Aktivitäten aus der DNS-Perspektive besser zu verstehen. Aber wir haben auch selbst eine gute Spam-Sammlung und könnten nach Kampagnen suchen, die das Verhalten von Muddling Meerkat im Laufe der Zeit zeigen.

Dieses Bericht ist das Ergebnis unserer Spam-Jagd. Um ehrlich zu sein, sind wir uns nicht sicher, ob wir dem Verständnis von Muddling Meerkat näher gekommen sind, was auf den ersten Blick als Scheitern angesehen werden könnte. Aber als wir diesen Spuren folgten, erfuhren wir stattdessen viel über die Verwendung von Domain-Spoofing in modernen bösartigen Spam-Kampagnen (Malspam). Wir werden einige unserer „Fänge“ vorstellen, die zeigen, wie interessant die Art und Weise ist, wie Schauspieler heutzutage Domain-Spoofing einsetzen, wobei sie sich alle eines Verhaltens bedienen, das dem des Muddling Meerkat ähnelt. Wir konnten diese Kampagnen mit den Missbrauchsmeldungen, die wir von den Empfängern erhalten haben, und unseren zuverlässigen DNS-Protokollen in Verbindung bringen. Da wir außerdem einige der gefälschten Domains besitzen, konnten wir einige von ihnen als Bounces auf unsere Mailserver umleiten. Durch das Hin- und Herwechseln zwischen diesen Quellen erfuhren wir auch mehr über die Breite der Muddling Meerkat-Zieldomains und erweiterten unseren ursprünglich gemeldeten Satz von etwa 20 auf über 650 Domains.

Am überraschendsten ist, wie weit verbreitet das Domain-Spoofing in Spam ist. Es gibt mehrere Mechanismen, die Benutzer vor Spam im Allgemeinen und Spoofing im Besonderen schützen sollen, aber wir haben festgestellt, dass Spoofing immer noch weit verbreitet ist. Die meisten Kampagnen werden von chinesischen IP-Adressen gesendet, und die Bandbreite der Typen von Kampagnen ist bemerkenswert. Trotz Sicherheitsvorkehrungen lohnt sich die Nutzung gefälschter Domains finanziell immer noch. In diesem Bericht werden wir uns mit folgenden Themen befassen:

- Moderne Kampagnen, die QR-Codes in PDF-Anhängen nutzen, um chinesische Bürger zu bestehlen,
- Beliebte Markenimitation, die japanische Nutzer ins Visier nimmt, um Anmeldedaten zu stehlen,
- Alte Erpressungskampagnen, die möglicherweise von Botnet-Überresten gesteuert werden und versuchen, Benutzer dazu zu bringen, in die Krypto-Wallet des Bedrohungsakteurs einzuzahlen, und
- Mysteriöse Finanzkampagnen, die scheinbar keinen böswilligen Inhalt haben, aber auch kein Motiv.

Außerdem beschreiben wir, wie wir unsere eigenen zuverlässigen DNS-Serverprotokolle verwendet haben, um zu versuchen, Muddling Meerkat zu verstehen, aber stattdessen diese Spam-Kampagnen abgefangen haben.

DOMAIN-SPOOFING IN SPAM

Bedrohungsakteure können die Absenderadresse einer E-Mail fälschen (Spoofing). Sie tun dies, um die E-Mail glaubwürdiger erscheinen zu lassen. Durch die Verwendung einer Domain, die seit vielen Jahren registriert ist, ist es wahrscheinlicher, dass sie Sicherheitsmechanismen umgehen, die das Alter der Absender-Domain überprüfen, um bösartigen Spam zu identifizieren. Wenn der Akteur andererseits eine bekannte Domain wie amazon[.]com fälscht, gibt es mehrere Mechanismen, mit denen der empfangende Mailserver feststellen kann, wann eine E-Mail, die eine dieser Domains verwendet, gefälscht wurde. Wir glauben, dass Spammer dieses Risiko der Entdeckung nutzen, indem sie alte, vernachlässigte Domains verwenden – genau den gleichen Typ von Domain, den Muddling Meerkat für seine Operationen bevorzugt.

Wenn ein Mailserver eine E-Mail empfängt, führt er mehrere Prüfungen in DNS durch, um den Absender zu validieren. Anschließend werden diese Ergebnisse mit den E-Mail-Headern verglichen. Diese Prüfungen umfassen Maßnahmen wie die Überprüfung, ob die IP-Adresse, von der die E-Mail empfangen wurde, zum Senden von E-Mails für diese Domain berechtigt ist. Einige dieser Prüfungen basieren auf bestimmten DNS-Einträgen, die bei alten, vernachlässigten Domains oft nicht vorhanden sind und zu einem „weichen" Fehler führen können.

Nachdem der Server die Standardprüfungen durchgeführt und möglicherweise zusätzliche E-Mail-Sicherheitsalgorithmen angewendet hat, könnte die E-Mail als Spam markiert oder sogar in Quarantäne gestellt werden. In anderen Fällen könnte es in den Posteingang des Benutzers gelangen. Der Malspam-Akteur hofft, dass seine synthetischen E-Mails genug Spam-Fallen überwinden, um die Benutzer zu erreichen und Gewinne einzufahren.

AUTORITATIVE DNS-SERVER UND SPAM

Wir besitzen zufällig einige stillgelegte Domains, auf denen seit fast 20 Jahren keine Inhalte mehr aktiv gehostet werden. Ihnen fehlen die meisten DNS-Einträge, einschließlich derer, die normalerweise zur Überprüfung der Authentizität einer Absenderdomäne verwendet werden, z. B. SPF-Einträge (Sender Policy Framework). Die Domains sind kurz und haben sehr renommierte TLDs: perfekt für Muddling Meerkat und Spammer gleichermaßen.

Ironischerweise werden einige unserer alten Domains häufig zitiert, zum Beispiel in Trancos Top-1-Million-Domain-Liste. Wir vermuten, dass ihre Beliebtheit ausschließlich auf Spam zurückzuführen ist. Ohne zu weit vom Hauptthema dieses Blogs abzuschweifen, ist die Beliebtheit unserer inaktiven Domains ein gutes Beispiel dafür, warum Top-Listen mit Vorsicht zu genießen sind. Wir haben viel Zeit damit verbracht, die Beliebtheit und die Bedrohungen von Domains zu untersuchen. Lesen Sie dazu unsere früheren Artikel.[1,2] (Zum Lesen der Fußnoten bitte dieses PDF online anzeigen.)

DNS gibt uns einen einzigartigen Überblick über den Missbrauch unserer Domains. Wir protokollieren Abfragen für alle unsere Domains auf unserem autoritativen DNS-Server. Diese Protokolle geben uns einen Einblick in eine Vielzahl von DNS-Aktivitäten, von Internet-Scans bis hin zur Spam-Verbreitung. Im Falle von E-Mails stellt der Mailserver des Empfängers mehrere DNS-Abfragen an den autorisierenden Server für die Absender-Domain, einschließlich DNS-TXT-Einträgen. Aus unseren Protokollen können wir die IP-Adresse der DNS-Resolver ablesen, die von diesen Mailservern verwendet werden, und uns ein Bild von der geografischen Verteilung des Spams machen, der unsere Domains fälscht.

Wir haben auch DomainKeys Identified Email (DKIM)-Datensätze eingerichtet, damit Anbieter, die Spam von unseren Domains erhalten, uns Missbrauchsmeldungen per E-Mail senden können. Diese Missbrauchsmeldungen enthalten die IP-Adresse des Spam-Absenders und Zeitstempelinformationen. Wir können sie mit den DNS-TXT-Eintragsanfragen kombinieren, um einen ziemlich guten Überblick darüber zu erhalten, wie wir fälschlicherweise mit der Verbreitung von Spam in Verbindung gebracht werden. Unsere Mailserver übertragen keine E-Mails, sondern empfangen sie nur.

Da wir an potenziellen Spam-Aktivitäten von Muddling Meerkat interessiert waren, mussten wir potenzielle Anfragen von Akteuren von anderen isolieren. Es herrscht viel Trubel im DNS. Viele Forschungsunternehmen, wie auch wir, führen DNS-Abfragen durch, um Informationen zu sammeln und einen synthetischen Fußabdruck in historischen Aufzeichnungen zu erstellen. Unsere Server sollten keine DNS-Anfragen erhalten, da alle Domains inaktiv sind, aber sie erhalten täglich Tausende von Anfragen, manchmal sogar Zehntausende. Abbildung 1 zeigt einen Vergleich der Anzahl der Anfragen, die im Laufe der Zeit auf unserem autoritativen Server für vier verschiedene Muddling-Meerkat-Domains eingegangen sind. Die obere Grafik gilt für alle Typen von Datensätzen, die untere für MX-Abfragen. Diese Zeitachsen-Diagramme zeigen, dass die E-Mail-bezogenen Aktivitäten nicht unbedingt mit der gesamten DNS-Aktivität für die Domains korrelieren.

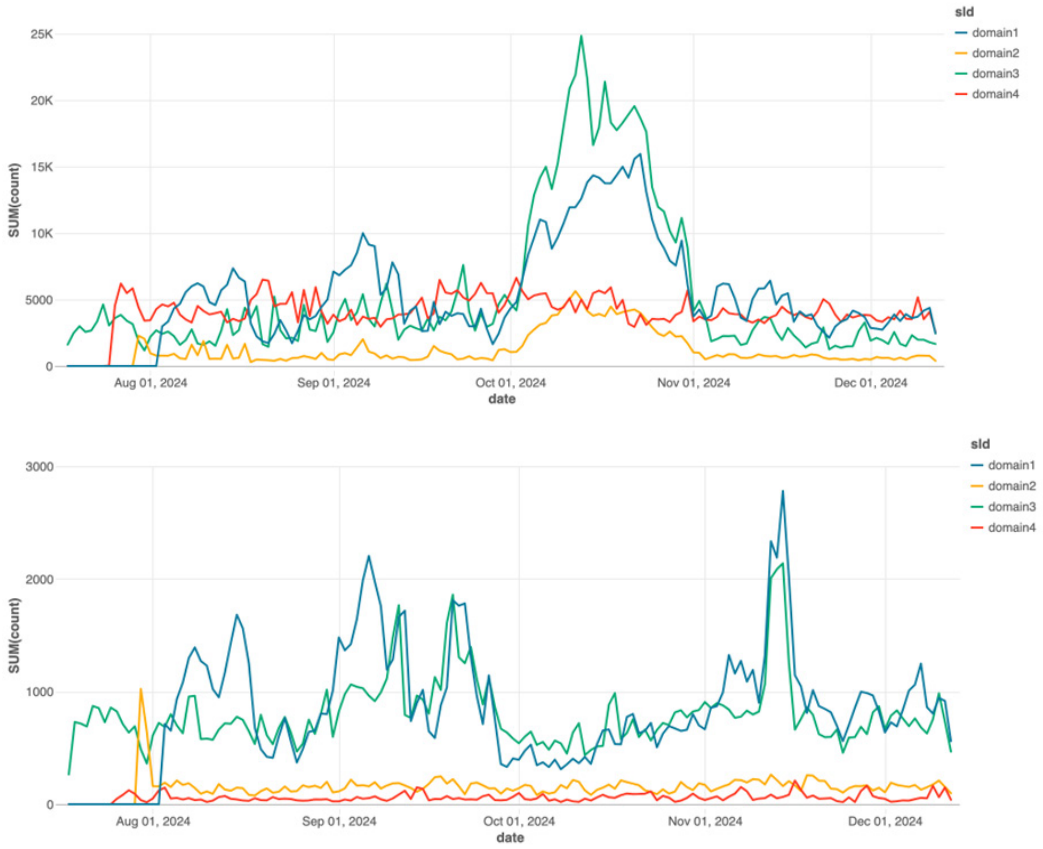

Abbildung 1. Oberes Diagramm: Abfragevolumen für alle Typen von DNS-Einträgen auf unserem autoritativen Server nach Domain; unteres Diagramm: Abfragevolumen für MX-Einträge

Die meisten Anfragen, die wir auf unseren autoritativen Servern erhalten, entsprechen nicht den Mustern von Muddling Meerkat. Daher haben wir verschiedene Fingerabdrücke verwendet, die auf früheren Untersuchungen basieren, um potenzielle Aktivitäten des Akteurs zu isolieren. Wir haben diese Ergebnisse auch mit den Missbrauchsmeldungen verglichen, die wir per E-Mail erhalten haben. Durcheinander bei Erdmännchen-DNS-Abfragen: Es werden verschiedene Typen von Einträgen verwendet, aber aus forensischer Sicht sind MX-Eintrags-Abfragen für kurze zufällige Subdomains am ungewöhnlichsten. Im folgenden Beispiel würde die Abfrage wie folgt aussehen, wenn die Zieldomain „target.domain“ lautet:

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

Der Begriff „Ziel“ ist hier ein dehnbarer Begriff, wie wir in unserem früheren Dokument[3] erläutert haben, da der Akteur diese Domains für den Einsatz in seinen Kampagnen ins Visier nimmt und nicht als Teil eines Angriffs auf die Domaininhaber; der Akteur missbraucht diese Domains, die ihm nicht gehören, für einen unbekannten Zweck. Wir haben unsere Analyse der Abfragen auf diejenigen beschränkt, deren Hostnamen nur als Subdomain einer einzigen von uns bedienten Domain angesehen wurden, und nach Trends gesucht. Die Länge der eindeutig beobachteten Hostnamen variierte, aber diejenigen, die drei Zeichen lang waren, waren am häufigsten; siehe Abbildung 2. Dies stimmte mit den Daten überein, die wir von anderen Domaininhabern erhalten hatten. Wir haben auch überprüft, dass die Abfragen von großen E-Mail-Anbietern wie Google und E-Mail-Sicherheitsanbietern wie Proofpoint kamen.

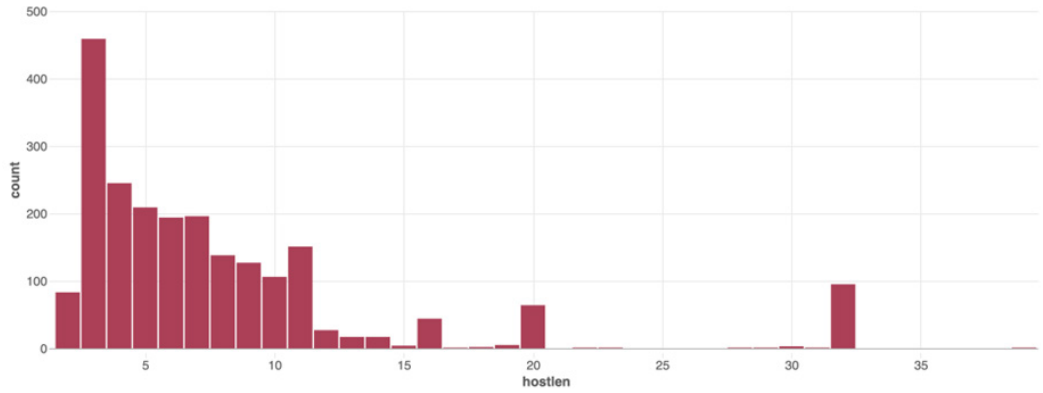

Abbildung 2. Die Länge der eindeutig beobachteten Hostnamen in MX-Abfragen bei unseren autoritativen DNS-Servern

Mit dem Wissen, dass unsere eigenen Domains von Muddling Meerkat genutzt und von Bedrohungsakteuren, die Malspam-Kampagnen durchführen, gefälscht wurden, machten wir uns in unseren Spam-Fallen auf die Suche nach aktiven Kampagnen.

FALLE #1: QR-CODE-PHISHING-KAMPAGNEN

Die größte Gruppe von Phishing-Kampagnen, die wir beobachtet haben und die unsere alten Domains fälschten, richtete sich an Bewohner des Großraums China. Diese Kampagnen laufen seit mindestens Ende 2022 ununterbrochen und verteilen Anhänge, die einen QR-Code enthalten, der zu einer Phishing-Website führt (siehe Abbildung 3). Aufgrund unserer DNS-Daten, Missbrauchsmeldungen und Begleitinformationen gehen wir davon aus, dass die Angriffe aus dem Großraum China stammen. Die Kampagnen nutzen eine Taktik, bei der der Empfänger den E-Mail-Anhang öffnen und WhatsApp verwenden muss, um einen darin enthaltenen QR-Code zu scannen. Diese zweistufige Methode stellt eine zusätzliche Herausforderung für die Sicherheit der Benutzer dar, da der Angreifer die Opfer von ihren Laptops zu einer verschlüsselten Chat-App umleitet und so viele gängige Sicherheitsmaßnahmen umgeht. Die Bedrohungsakteure verwenden auch Algorithmen zur Generierung registrierter Domains (RDGAs), um zufällige Domains zu erstellen, die nur für kurze Zeit aktiv sind.

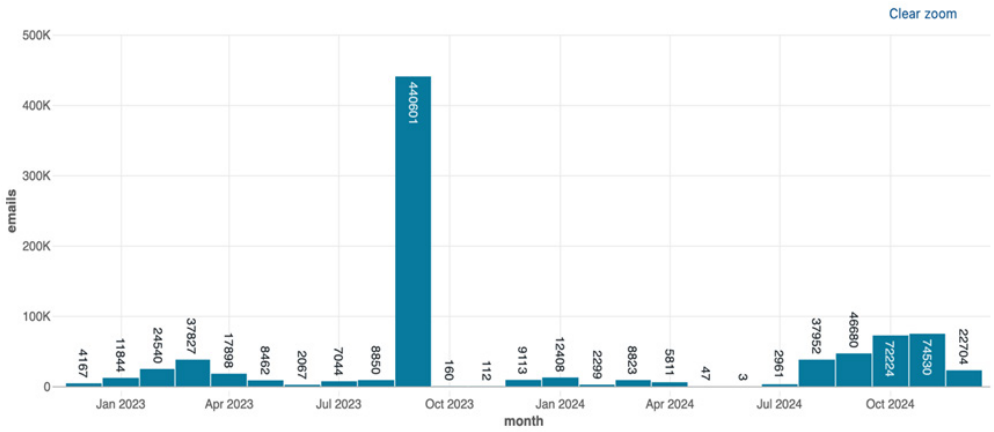

Abbildung 3: Anzahl der chinesischen QR-Code-Phishing-E-Mails im Laufe der Zeit

Diese Malspam-Kampagnen verwenden gefälschte Absender-Domains, die eine große Anzahl bestätigter Muddling-Meerkat-Zieldomains enthalten, darunter auch Domains, die uns gehören. Durch Spam-Analyse dieser Kampagnen und durch den Vergleich historischer DNS-Einträge konnten wir die Anzahl der bekannten Muddling-Meerkat-Zieldomains von etwa 20 im März 2024 auf heute über 650 erhöhen. Die QR-Code-Kampagnen enthalten jedoch auch viele Domains, die Muddling Meerkat möglicherweise verwendet, die wir aber nicht über DNS bestätigen können.

Diese Kampagnen verwenden E-Mail-Absenderadressen, deren Struktur mit dem übereinstimmt, was wir bei Muddling-Meerkat-DNS-Abfragen beobachtet haben. Der Benutzername des Absenders war eine kurze, zufällige Zeichenfolge in der Form `<rand>@spoofed[.]domain`. Tabelle 1 zeigt eine Auswahl der E-Mail-Absenderadressen der Kampagne im Laufe der Zeit. Domains wie `jx[.]com`und `hm[.]com` waren bereits als Muddling-Meerkat-Zieldomains bekannt.

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**	

Tabelle 1: Beispiel für Absenderadressen für die QR-Code-Kampagne. Die Absender-E-Mails haben das Muster <2-9 zufällige Buchstaben>@<spoofed[.]domain>

Die E-Mail enthält in der Regel einen steuerbezogenen Köder in Mandarin und wurde im Dezember 2022 oder früher versendet. Diese scheinen aus dem chinesischen IP-Raum zu stammen, hauptsächlich aus 4134 (Chinanet) und 56046 (China Mobile). Abbildung 4 zeigt einige der E-Mail-Betreffzeilen und ihre englischen Übersetzungen.

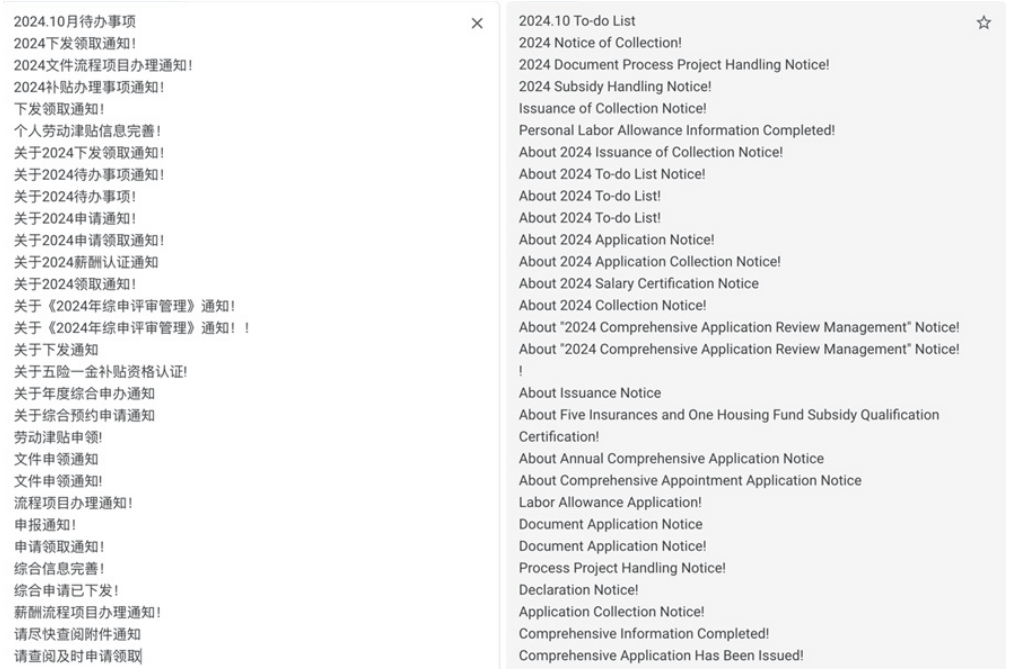

Abbildung 4: Beispiel für übersetzte Betreffzeilen von E-Mails im Rahmen von QR-Code-Kampagnen

Ein weiteres Unterscheidungsmerkmal dieses Malspams ist, dass die meisten QR-Code-Dokumente mit einem vierstelligen Passwort verschlüsselt sind, das irgendwo im E-Mail-Text enthalten ist, aber nicht auf einheitliche Weise. Manchmal stehen sie in Klammern oder sind von anderen Symbolen umgeben. Abbildung 5 zeigt zwei Beispiele dafür, wie Passwörter in E-Mails enthalten sind.

Abbildung 5. Zwei Beispiele, wie das vierstellige Passwort in verschiedenen E-Mails in Wert und Format variieren kann; die roten und grünen Felder heben die unterschiedlichen Arten hervor, wie das Passwort in einer E-Mail dargestellt wird

Die Anhänge enthalten einen QR-Code mit einem eingebetteten Logo und Anweisungen für den Empfänger, das Dokument mit AliPay/WeChat zu scannen; siehe Abbildung 6. Diese E-Mails unterscheiden sich nicht von denen, die wir weltweit von Cyberkriminellen sehen, die mit dem Versprechen von Subventionen und finanziellen Vorteilen auf gefährdete Bevölkerungsgruppen abzielen.

Abbildung 6. Inhalt und Übersetzung des Dateianhangs. Der hervorgehobene Teil enthält die Anweisung, Alipay/WeChat zum Scannen des QR-Codes zu verwenden

Twitter-Nutzer haben den Betrug gemeldet. Laut dem Tweet[4] in Abbildung 7 wurde ein Nutzer nach dem Scannen des QR-Codes aufgefordert, eine Kartennummer und Identifikationsinformationen einzugeben. Anschließend wurde er aufgefordert, den Betrag und den Verifizierungscode einzugeben, von dem er annahm, dass es sich um eine Zahlung auf sein Konto handelte. Kurz darauf wurde er per SMS benachrichtigt, dass er 590 Euro von seiner Karte an den Angreifer gezahlt hatte. Das ist eine beachtliche Rendite für eine Spam-E-Mail!

Abbildung 7. Tweet eines Benutzers, der auf den QR-Code-Phishing-Betrug hereingefallen ist

Dieses Schema beruht auf Phishing-Domains der zweiten Stufe mit einer sehr kurzen Lebensdauer, die anscheinend geografisch begrenzt sind. Sie werden nach etwa einem Tag nicht mehr im DNS aufgelöst und befinden sich in häufig missbrauchten TLDs wie sbs, shop, life, bond und cn. Diese Domains bestehen aus einer zufälligen Zeichenkombination, z. B. `aaaefiuibew[.]cn` oder `6ttox81[.]sbs`.

Wir können nicht sagen, ob diese Aktivität von Muddling Meerkat stammt. Es scheint sich eher um ein gängiges Phishing-as-a-Service-System (PhaaS) zu handeln. Obwohl die Kampagnen die vernachlässigten Domains verwenden, die wir bei Muddling Meerkat sehen, scheinen sie im Großen und Ganzen zufällige Domains zu fälschen, sogar solche, die nicht existieren. Der Schauspieler kann diese Technik verwenden, um wiederholte E-Mails vom gleichen Absender zu vermeiden. Trotz der Bemühungen, die Benutzer vor bösartigem Spam zu schützen, kommen einige dieser Fälschungen durch und sind eindeutig profitabel genug, um aufrechterhalten zu werden.

Weitere Absenderdomains, die in dieser Aktivität zu sehen sind, sind in Tabelle 2 aufgeführt.

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

Tabelle 2: Beispiele für gefälschte Domains, die in QR-Code-Phishing-Kampagnen verwendet wurden

Als wir feststellten, dass die QR-Code-Kampagnen Domains fälschten, die außerhalb dessen lagen, was wir von Muddling Meerkat erwarteten, kehrten wir zu DNS und unserer Spam-Sammlung zurück, um nach verschiedenen Kampagnen zu suchen, die möglicherweise vom Muddling Meerkat-Akteur durchgeführt wurden.

CATCH #2: JAPANISCHE PHISHING-KAMPAGNEN

Auf unseren maßgeblichen DNS-Servern stellten wir fest, dass ein ungewöhnlich hoher Prozentsatz der E-Mail-bezogenen Abfragen Hostnamen mit drei Buchstaben enthielt. Bei dem Versuch, die Anfragen, die von Muddling Meerkat stammen könnten, von denen zu trennen, die auf Scanner und andere Quellen zurückzuführen sind, schien uns das Volumen und die Konsistenz dieser Anfragen ein guter Ansatz für weitere Untersuchungen zu sein. Daraufhin suchten wir nach Hinweisen auf Spam, der dieselbe Abfragestruktur aufwies.

Wir haben eine Reihe von Kampagnen gefunden, die sich mit E-Mails an japanische Nutzer richteten und auf beliebte Marken wie Electronic Toll Collection (ETC, wird auf Autobahnen in ganz Japan verwendet), Sumitomo Mitsui Banking Corporation (SMBC, eine der größten Banken in Japan) sowie Amazon und Mastercard Bezug nahmen. In den E-Mails werden die Benutzer aufgefordert, sich aufgrund von Sicherheitsbedenken oder anderen Problemen beim Dienst zu authentifizieren. Über eine in der E-Mail enthaltene Schaltfläche gelangt der Benutzer zu einem Traffic Distribution System (TDS) und wird auf eine gefälschte Anmeldeseite weitergeleitet, wenn bestimmte Kriterien erfüllt sind.[5] Diese Methode ist bei Malvertising weit verbreitet und wird verwendet, um die endgültige Zielseite zu verschleiern und eine Erkennung durch Sicherheitsunternehmen zu vermeiden. Die gefälschte Anmeldeseite stiehlt die Anmeldedaten des Opfers, wenn diese eingegeben werden. Abbildung 8 zeigt ein Beispiel für diese Spam-E-Mails.

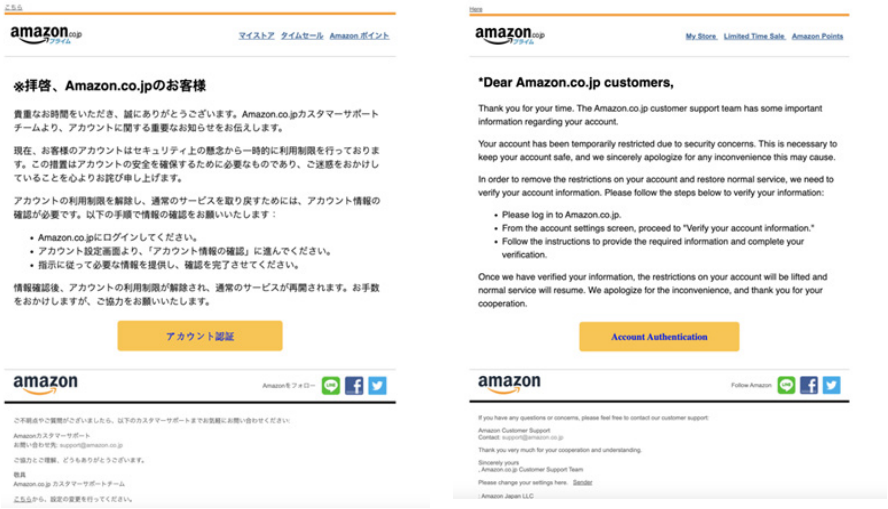

Abbildung 8: Beispiel für eine Original-Spam-E-Mail, die sich mit gefälschten Amazon-Warnungen an japanische Benutzer richtet, und eine maschinelle Übersetzung der E-Mail

Sobald der Benutzer auf die Schaltfläche „Kontoauthentifizierung“ klickt:

- Sie werden an `ubrjubf[.]com` weitergeleitet, Auflösung auf IP `43.128.150[.]42`
- Dann wird der Benutzer zu einer anderen Domain `unpwple[.]com` weitergeleitet, die auf die IP `43.133.182[.]243 aufgelöst wird.`
- Der Benutzer gelangt auf eine gefälschte Anmeldeseite für ein Amazon-Konto (siehe Abbildung 9).

Abbildung 9: Gefälschte Amazon-Anmeldeseite; Bildreferenz: https://urlscan.io/result/5c9bbf63-883f-4eab-b4fc-45e2809a8ac2/

Wir haben mehrere Varianten von Spam mit Amazon-Themen sowie Köder mit Mastercard und SMBC Vpass beobachtet.[6] Dieser Akteur nutzt eine dedizierte Hosting-Infrastruktur und rotiert Kampagnen über dieselben Domains und IP-Adressen.[7] Die beiden dedizierten IP-Adressen, die beobachtet wurden, waren `43.128.150[.]42` und `43.133.182[.]243`. Tabelle 3 enthält eine Liste der RDGA-Domains, die in den Kampagnen verwendet wurden.

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

Tabelle 3. Beispiel von RDGA-Domains auf dedizierten IP-Adressen, die in Kampagnen für japanische Benutzer verwendet werden

Wie bei den im vorherigen Abschnitt beschriebenen Kampagnen verwenden die E-Mails in diesen Kampagnen gefälschte Absenderdomains, darunter auch Domains, die Infoblox Threat Intel gehören. Sie folgen auch dem Format, das wir bei unseren maßgeblichen DNS-Servern mit einer dreistelligen Subdomain und in den Missbrauchsmeldungen, die wir von E-Mail-Anbietern erhalten haben, vorgefunden haben. Tabelle 4 zeigt eine Auswahl von Absender-E-Mail-Adressen.

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**	

Tabelle 4. Eine Auswahl von Absenderadressen für japanische Phishing-E-Mails mit dreibuchstabigen Subdomänen; die dreibuchstabigen Hostnamen sind rot markiert, während die gefälschte Domain fett hervorgehoben ist

Dies war nicht die einzige Art von Kampagne, die wir sahen und die sich an japanische Benutzer richtete. Ein weiterer großer Köder war MyEtherWallet, eine beliebte Krypto-Wallet, und die Verwendung von Lookalike-Domains. Die Spam-Nachrichten enthalten manchmal japanischen Text, z. B. „(重要なお知らせ) MyEtherWallet ご利用確認のお願い“, was übersetzt „[Wichtige Mitteilung] Bitte um Bestätigung der Nutzung von MyEtherWallet“ bedeutet, und fordern die Benutzer auf, sich in ihr Konto einzuloggen. Abbildung 10 zeigt ein Beispiel für eine E-Mail in englischer Sprache. Obwohl der Link scheinbar zur echten Website führt, leitet er tatsächlich zu einer ähnlichen Domain weiter, die vom Bedrohungsakteur erstellt wurde.

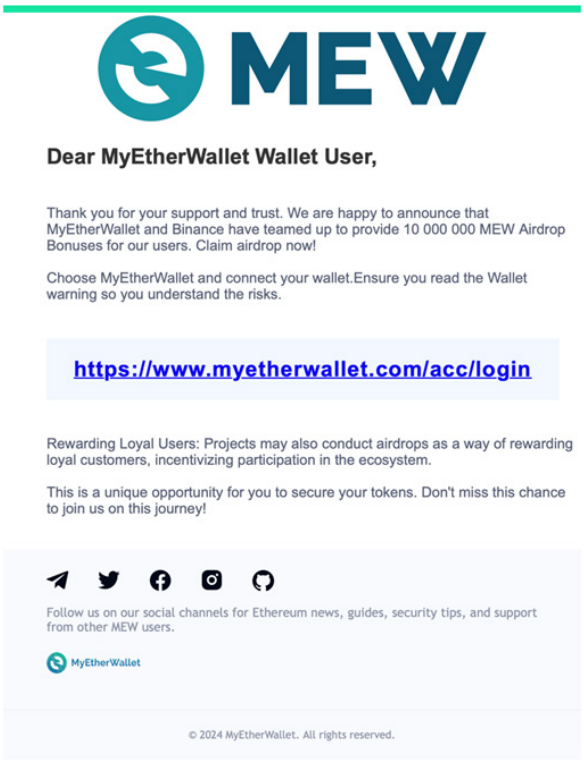

Abbildung 10: Beispiel für eine Spam-Kampagne, die auf japanische Benutzer abzielt; diese spezielle E-Mail hatte die Betreffzeile „Binance Distribution of MyEtherWallet (MEW) Airdrop“ und leitete den Benutzer zu `myetherwallatak[.]org`

Die Lookalike-Domains führten zu einer Spiegelkopie der MyEtherWallet-Website und wurden zum Diebstahl von Benutzerdaten verwendet. Diese Domains sind in verschiedenen TLDs enthalten, darunter com und org (siehe Tabelle 5 für ein Beispiel).

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

Tabelle 5: Beispiel für ähnliche Domains, die verwendet werden, um Anmeldedaten von japanischen Benutzern zu erschleichen

Bei der QR-Code-Phishing-Kampagne waren die Muddling Meerkat-Domains in den sogenannten Absenderadressen zu sehen, d. h. in den E-Mail-Adressen, die für den Empfänger sichtbar sind. In dieser japanischen Variante werden die Domains jedoch im „Empfangen von“-Teil der Nachricht angezeigt, der für die technische Zustellung per SMTP verwendet wird. Wir sind auf eine weitere Reihe bösartiger Spam-Kampagnen gestoßen, die dieselben Domains verwenden, die auch bei Muddling Meerkat-Operationen beobachtet wurden, einschließlich eines ähnlichen Subdomain-Formats. Wir können jedoch nicht bestätigen, dass sie von Muddling Meerkat stammen. Tabelle 6 bietet eine Auswahl der gefälschten Domains.

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		Holländisch [.] netto	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

Tabelle 6. Beispiele für gefälschte Domains, die in MyEtherWallet-Kampagnen zu sehen waren

Eine von mehreren Lücken im Verständnis dieser Kampagnen besteht darin, dass die Anzahl der von uns entdeckten Domains wahrscheinlich zu klein ist, um zu bestätigen, dass sich alle Domains mit Muddling Meerkat überschneiden. Diese Reihe von Kampagnen ist jedoch ein weiteres Beispiel dafür, wie mit China in Verbindung stehende Bedrohungsakteure Domain-Spoofing für ihre Spam-Operationen nutzen.

Damit kehrten wir zu den Spam-Fallen zurück.

FALL NR.3: BEKANNTE ERPRESSUNGSKAMPAGNEN

Wir haben nicht nur Domain-Spoofing im QR-Code und in japanischsprachigen Kampagnen gefunden, sondern auch in Kampagnen, die bekannte Spam-Tropen nutzten. Erpressungs-E-Mails, in denen behauptet wird, ein Hacker habe auf das Gerät des Benutzers zugegriffen und einige peinliche Aktivitäten aufgezeichnet, sind ein fester Bestandteil der Malspam-Welt. Wir waren etwas überrascht, dass auch hier gefälschte Absenderdomains verwendet werden, aber mit einem kleinen Unterschied: Der Betrüger fälscht die eigene E-Mail-Adresse des Benutzers und fordert ihn auf, dies zu überprüfen. In der E-Mail wird dem Benutzer mitgeteilt, dass sein Gerät kompromittiert wurde, und als Beweis gibt der Betrüger an, dass die Nachricht vom eigenen Konto des Benutzers gesendet wurde. Und doch war dies nicht der Fall. Die E-Mail-Header zeigen, dass sie über chinesische IP-Adressen und nicht über die des Benutzers gesendet wurde. Ein Beispiel für den E-Mail-Inhalt finden Sie in Abbildung 11 unten.

In der E-Mail wird der Benutzer aufgefordert, den Absender dafür zu bezahlen, dass er die Malware von seinem Gerät entfernt, und es wird eine Bitcoin-Wallet-Adresse angegeben, die je nach Spam-Nachricht variiert. Wir wissen nicht, ob es sich hierbei um einen Erpressungsdienst handelt oder ob derselbe Akteur verschiedene Wallets verwendet. In den von uns gesammelten Beispielen werden die Opfer aufgefordert, 1800 US-Dollar zu zahlen. Es mag überraschend erscheinen, dass viele Benutzer diese Spam-E-Mails tatsächlich lesen, geschweige denn darauf reagieren, aber der Betrug funktioniert anscheinend. Wenn wir das Guthaben dieser Wallets bei `bitref[.]com` überprüfen, können wir feststellen, dass sie beträchtliche Summen enthalten; eine Wallet enthielt fast 26.000 US-Dollar.

Hallo! Leider habe ich schlechte Nachrichten für Sie. Vor einiger Zeit wurde Ihr Gerät mit meinem privaten Trojaner R.A.T (Remote Administration Tool) infiziert. Wenn Sie mehr darüber erfahren möchten, verwenden Sie einfach Google. Mit meinem Trojaner konnte ich auf Ihre Dateien, Konten und Ihre Kamera zugreifen. Überprüfen Sie den Absender dieser E-Mail, ich habe sie von Ihrem E-Mail-Konto aus gesendet. Um sicherzustellen, dass Sie diese E-Mail lesen, erhalten Sie sie mehrmals. Sie schauen sich wirklich gerne Pornoseiten an und schauen sich schmutzige Videos an, während Sie viel versauten Spaß haben. ICH HABE SIE (über die Kamera Ihres Geräts) DABEI AUFGEZEICHNET, WIE SIE SICH SELBST BEFRIEDIGEN! Danach habe ich meine Malware entfernt, um keine Spuren zu hinterlassen. Wenn Sie immer noch an meinen ernsthaften Absichten zweifeln, brauchen Sie nur ein paar Mausklicks, um das Video von Ihnen mit Ihren Freunden, Verwandten, allen E-Mail-Kontakten, in sozialen Netzwerken und im Darknet zu teilen. Alles, was Sie tun müssen, ist, 1800 USD in Bitcoin (BTC) auf mein Konto zu überweisen. Nachdem die Transaktion erfolgreich abgeschlossen wurde, werde ich alles löschen. Seien Sie versichert, dass ich meine Versprechen halte. Sie können Bitcoin (BTC) ganz einfach hier kaufen: 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 Oder googeln Sie einfach nach einem anderen Tauschpartner. Danach senden Sie die Bitcoins (BTC) direkt an meine Wallet oder installieren Sie die kostenlose Software: Atomicwallet oder Exodus Wallet, installieren und dann empfangen und an meine senden. Meine Bitcoin (BTC)-Adresse lautet: 1GtGZpzfRkAVBL48F68mi8bTcatwpTZGm8 Ja, so sieht die Adresse aus, kopieren Sie sie und fügen Sie sie ein, sie ist (cAsE-sEnSEtiVE). Sie haben nach dem Öffnen dieser E-Mail nicht mehr als 3 Tage Zeit. Da ich Zugriff auf dieses E-Mail-Konto habe, weiß ich, ob diese E-Mail bereits gelesen wurde. Alles wird auf der Grundlage von Fairness durchgeführt. Ein Rat von mir: Ändern Sie regelmäßig alle Ihre Passwörter für Ihre Konten und aktualisieren Sie Ihr Gerät mit den neuesten Sicherheits-Patches.

Abbildung 11. Ein Beispiel für Erpressungs-Spam, der gefälschte Absenderdomains nutzt

Es ist wahrscheinlich, dass diese Kampagnen und möglicherweise viele andere, die gefälschte Absenderdomains verwenden, von veralteten Spam-Bots stammen. Zumindest überprüfen die Angreifer nicht die E-Mail-Adressen der Opfer, um sicherzustellen, dass sie empfangen oder gelesen werden. Es gab Fälle, in denen die E-Mail-Adresse des Empfängers mit einer unserer Domains verknüpft war, die zuletzt 2007 Inhalte gehostet hatte und seit über 15 Jahren keine E-Mail-Benutzer mehr hatte. Es gibt keine Aufzeichnungen über Sicherheitsverletzungen, die erklären könnten, warum diese E-Mails ausgelöst wurden, und es ist uns nicht bekannt, ob diese Benutzer tatsächlich jemals existiert haben.

Diese und andere ähnliche Spam-Kampagnen, die wir gefunden haben, rufen Bilder von verlassenen Spam-Kanonen hervor, die im Internetraum treiben. Außerdem konnten wir beobachten, wie alte Würmer übertragen wurden, ein weiteres Zeichen dafür, dass Botnet-Überreste weiter aktiv waren, während böswillige Spammer zu Techniken wie den QR-Codes und gefälschten Kontoseiten übergingen, wie wir sie oben gezeigt haben. Diese Kampagnen, die jetzt wahrscheinlich auf Autopilot laufen, scheinen eher Echos zu sein als die jüngste Arbeit eines raffinierten Akteurs wie Muddling Meerkat.

CATCH #4: MYSTERIÖSER MALSPAM

Diese ganze Forschungsagenda begann mit einem Rätsel, und wir werden diesen Beitrag mit einem anderen Rätsel beenden: einer sehr aktiven Spam-Kampagne, die gefälschte Absenderdomains verwendet und scheinbar harmlose Excel-Tabellen-Anhänge enthält, die keinen offensichtlichen Zweck haben. Wir können das Motiv für diese E-Mails nicht erklären, die die gleichen Typen von Domains fälschen, die Muddling Meerkat verwendet.

Diese E-Mails stammen angeblich von **上海亚凯**, was übersetzt „Shanghai Yakai“ heißt, dem Namen eines chinesischen Frachtunternehmens. Die E-Mail-Adressen unterscheiden sich stark und enthalten synthetische Benutzernamen wie „Edward.Evelyn“ und „Heidi.Gracie“. Im Jahr 2024 wurden alle zwei bis drei Tage Kampagnen beobachtet, die jedoch nicht variierten. Die Betreffzeile weist darauf hin, dass die E-Mail neue Frachtraten-Updates enthält, und der Anhang ist eine einzelne benannte Tabelle: **上海亚凯国际运价表**.xlsx. Wir haben in diesen Dateien keine schädlichen Inhalte gefunden.

Die E-Mail enthält keinen Call to Action (CTA). Auf den ersten Blick handelt es sich nur um eine fortlaufend aktualisierte Liste von Frachtraten für eine chinesische Reederei. Aber zu welchem Zweck? Diese E-Mails werden anscheinend nicht an Kunden gesendet, die vergessen haben, ihre E-Mail-Adresse zu ändern oder sich abzumelden. Durch die Verwendung von Domain-Spoofing wird jeglicher Anschein von Legitimität beseitigt, und es scheint unklar, warum entweder ein Versandunternehmen oder ein böswilliger Akteur solche E-Mails versenden sollte. Tabelle 7 zeigt eine Auswahl der Absenderdomains.

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

Tabelle 7. Ein Beispiel für gefälschte Absenderdomänen, die im Frachtspam von Shanghai Yakai verwendet werden

Eine ähnliche Kampagnentechnik wurde bei persönlichem Spam beobachtet, aber statt Nachrichten von einer Spedition enthielt die E-Mail Informationen zu Investmentfonds einer indischen Investmentgesellschaft. Diese Nachrichten, die von Google Mail als verdächtiger Spam markiert werden, enthalten auch eine harmlose Tabellenkalkulation und eine PDF-Datei. In diesem Fall ist der Benutzername des Absenders ein ehemaliger Bekannter, und es ist wahrscheinlich, dass sein E-Mail-Konto irgendwann gehackt wurde, um es für Spam-Aktionen zu nutzen. Aber wie beim chinesischen Fracht-Spam ist unklar, welchen Wert diese Nachrichten für den Spam-Versender haben.

ANSICHT VOM AUTORITATIVEN DNS-SERVER

Muddling Meerkat führt seit über sechs Jahren seltsame DNS-Operationen durch. Dazu gehören gefälschte Antworten der chinesischen Great Firewall und die Nutzung von lange vernachlässigten Domains, die sie nicht kontrollieren. Während ihre DNS-Aktivität mehrere Typen von Einträgen umfasst, beziehen sich die gefälschten Antworten auf MX-Einträge der Basis- oder Zieldomain. Beispielsweise werden DNS-Antworten mit MX-Einträgen für `kb[.]com` von chinesischen IP-Adressen beobachtet, obwohl `kb[.]com` keine MX-Einträge hat. Darüber hinaus enthalten diese gefälschten Datensätze einen kurzen, zufälligen Hostnamen, der im Laufe der Zeit nur einmal beobachtet wird – z. B. `x4rd.kb[.]com` – und der ein beobachteter MX-Eintrag für `kb[.]com` sein könnte. Als wir im März 2024 erstmals veröffentlichten, hatten wir etwa 20 solcher Domains identifiziert, inzwischen haben wir mehrere hundert weitere bestätigt.

Zusätzlich zur Suche nach Hinweisen auf Spam-Aktivitäten des Akteurs analysierten wir auch die DNS-Protokolle auf unseren autoritativen Servern und versuchten, sie mit den gefälschten DNS-Antworten abzugleichen, die in den Begleitdaten für die Domains, die uns gehörten, beobachtet wurden. Die Hypothese war, dass wir, wenn wir eine Abfrage für eine der gefälschten MX-Record-Domains sehen könnten, z. B. `x4rd[.]our[.]domain`, die IP-Adresse des Abfragenden verwenden könnten, um die Vorgänge von Muddling Meerkat besser zu verstehen. Leider konnten wir die Muddling-Meerkat-Datensätze nicht eindeutig mit den Abfragen auf unseren Servern in Verbindung bringen.

Was bedeutet es, dass diese Übereinstimmung nicht gefunden werden kann? Nun, es bedeutet, dass wer oder was auch immer die gefälschten MX-Antworten erhält, z. B. `x4rd[.]our[.]domain`, diese Antworten nicht in nachfolgenden DNS-Abfragen verwendet und sie anscheinend auch nicht für Spam verwendet. Dieser Mangel an klarer Motivation scheint die Vorstellung zu zerstören, dass ein Botnetz Domains erhält, die in gefälschten E-Mails verwendet werden. Wofür werden die Antworten dann verwendet? Keine Ahnung. Muddling Meerkat bleibt ein Rätsel. Haben Sie Ideen oder eine andere Perspektive? Wir sind ganz Ohr.

ZUSAMMENFASSUNG

Wir konnten nicht herausfinden, was Muddling Meerkat vorhat, aber unsere Untersuchung war letztendlich erfolgreich: Wir haben viel darüber gelernt, wie Schauspieler gefälschte Domains in Malspam verwenden, was uns Aufschluss darüber geben kann, wie man sie stoppen kann. Für Bedrohungsforscher wie uns sind diese Erkenntnisse oft genauso wichtig wie das Wissen um die dahinter stehenden Absichten.

Man kann nicht immer das bekommen, was man will, aber man kann durchaus feststellen, dass man das bekommt, was man braucht.[8]

INFOBLOX THREAT INTEL

Infoblox Threat Intel ist der führende Anbieter von Original-DNS-Bedrohungsdaten und hebt sich von der Masse der Aggregatoren ab. Was zeichnet uns aus? Zwei Dinge: extrem umfassende DNS-Kenntnisse und beispiellose Sichtbarkeit. DNS ist bekanntermaßen schwierig zu interpretieren und zur „Jagd“ einzusetzen, aber unser tiefes Verständnis und unser einzigartiger Zugang ermöglichen es uns, Cyberbedrohungen aufzuspüren. Wir sind proaktiv, nicht nur defensiv, und nutzen unsere Erkenntnisse, um Cyberkriminalität dort zu unterbinden, wo sie entsteht. Wir glauben auch an den Wissensaustausch, um die breitere Sicherheits-Community zu unterstützen, indem wir detaillierte Forschungsergebnisse und Indikatoren auf GitHub veröffentlichen. Darüber hinaus sind unsere Informationen nahtlos in unsere Infoblox DNS Detection and Response-Lösungen integriert, sodass Kunden automatisch von den Vorteilen profitieren und von extrem niedrigen Falsch-Positiv-Raten profitieren.

Firmenhauptsitz
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054, USA

+1 408 986 4000
www.infoblox.com

Version: 20241223v1