M3AAWG | Messaging Malware Mobile Anti-Abuse Working Group

Messaging, Malware and Mobile Anti-Abuse Working Group

M3AAWG Brand Protection Kit Domain Management

February 2022

The reference URL for this document: www.m3AAWG.org/BPK-DM02-2022

Table of Contents

Introduction **3**

Minimum Security Requirements **3**

Create a domain inventory 3
Protect the domain 3
Update contact information 4
Make policies official 4
Document it all 4

Increased Security Measures: Quick Wins **4**

Use aliases for domain name control and notifications 4
Manage DNS authority appropriately 4
Choose the right registrar 4
Register similar domains (defensive registration) 5
Combine SSL certificate management with DNS management 5
Keep domain names secure 5
Back up DNS configuration 6
Consider monitoring for abusive third party domains 6

Attack Vectors and Mitigation **6**

Squatters, Lookalike Domains (Homographs) and Other Encroachments 6
Malicious Domain Mitigation: Domain Takedown Requests 6
Brand-Offensive Domains Mitigation 7
Which Domains Should Be Purchased, and Which Should Be Monitored? 7

Spoofing (for Email) 7
Spoofing Mitigation: Monitor and Submit a Complaint 8

Account Takeover (ATO) 8
Account Takeover Mitigation: Monitor and Submit a Complaint 9

Software Vulnerability 9
Software Vulnerability Mitigation: Update Software 9

Conclusion **9**

Recommended Resources **9**

Further reading about domain attack vectors and mitigation 9

Introduction

As a brand, how can a company best protect its online presence, customers and reputation? The M^{3}AAWG Brand Protection Kit is a series of best practice guides that provide practical information and recommendations for each relevant topic to help brands protect themselves from online abuse.

This document focuses on domain management. It outlines how to protect brands from threat actors who are keen to register domains that mimic a brand in order to steal information and/or assets.

M^{3}AAWG strongly recommends that all brands implement the minimum security requirements outlined in this document. As brands mature, M^{3}AAWG also recommends reviewing and considering the increased security measures outlined here to further protect the brand. Additionally, this best practices guide documents several attack vectors with recommended mitigations that should be reviewed and included in the security posture.

Minimum Security Requirements

Below is a list of basic security requirements. At a minimum, M^{3}AAWG strongly recommends that all organizations implement these measures to protect the brand, its reputation and customers.

Create a domain inventory

An inventory helps to decide which domains are most important to protect. Create a register of domains the company owns (even an Excel sheet is fine, although a dedicated data management tool is better. This can also be used for certificate and nameserver management). For each domain, supply a written explanation of its purpose and specify all the people responsible for its security and maintenance. Continue to document domains and staff as they are added, deleted or changed. Nameserver and other DNS management should also be a consideration. Whether tracking a relatively small number of active domains for a company or a massive portfolio, understanding how they are hosted in the DNS and configured is vitally important. Again, tools and outsourced providers are the best options here, with an eye towards ensuring that such providers integrate or play well with your DNS infrastructure provider.

Protect the domain

Make domain name protection an integral and ongoing component of the company's security policy. Keep registrant account information private and secure. Protect this account information for every unique user account and password. Recovery should only be possible by the most senior staff responsible for domain name administration under the most extreme circumstances.

When staff changes, change corresponding account information—especially passwords. Always use a name other than a transfer contact email address as the login to domain name self-administration pages. Use a role address rather than a personal address to ensure no loss of access due to personnel changes (i.e., the listed contact leaving the company or position). Hijackers can use the WHOIS service to identify transfer contact email addresses of targeted domain names, and will routinely check to see if a transfer contact email address doubles as an account username.

Secure every domain account with multifactor authentication (MFA).

Update contact information

Keep contact information accurate and current. Have a policy and process in place for any changes to your company's name, legal address, contact info (phone, email). When there is a change to any one of these, this should kick off an update cycle with all your registrars. Updating your company letterhead? Update your domain's "letterhead," too. Registrars are a key defense against hackers trying to take control of a domain. Making sure that details are current puts registrars in the best position to help keep your organization protected.

Make policies official

Establish appropriate policies and practices to codify these decisions and processes, particularly for things like domain decommissioning or reconfiguration. Be sure to document change control policy and the roles and responsibility of the relevant departments in the company to make changes.

Document it all

Policies, registers and regular communication with staff about their domains helps keep the business informed, prepared for incidents, ready to accept changes to their domains that need to happen, and poised to make strategic decisions.

Increased Security Measures: Quick Wins

Once the basics are in place, consider these increased security measures to further minimize risks to the brand's online presence.

Use aliases for domain name control and notifications

Use role accounts for notifications rather than sending them to a particular individual's personal account (domainregistrar@example.com). That way, DNS notifications won't vanish if the account they are tied to are deactivated due to turnover, vacation, illness, parental leave or the like.

Manage DNS authority appropriately

Decide how to handle authoritative DNS needs. Will the brand run local authoritative domain name servers using free/open-source software? Or an on-premises commercial DNS appliance? Or a cloud-based authoritative DNS service? Partner with your registrar, who may have preferred DNS services providers. All of these options have advantages and disadvantages, such as supporting DNSSEC, email authentication or other security requirements. Whichever is selected, audit the DNS configuration with free tools like https://zonemaster.iis.se/en/.

Choose the right registrar

Different registrars specialize in serving different market niches. For example, some registrars specialize in budget, one-off, mass-market registrations for hobbyist domains. Others may have features that are particularly attractive to efficient bulk domain registration by speculators. Others may target users with a particular first language (Chinese, French, German, Russian, Spanish, etc.).

As the owner of a high-value domain name closely tied to the brand, consider registering the domain via a registrar that specializes in registering and protecting critical assets. It may be appropriate to register a production domain or core domains with a corporate registrar rather than a retail registrar. For defensive registrations, however, a retail registrar may be more appropriate.

Suitable registrars will universally offer a minimum set of features, including:

- Redundant hardware to protect against outages associated with single points of failure
- Protection against accidental expiry of valuable domain registrations
- Domain name monitoring (is the domain up and responding normally?)

- Two-factor authentication to secure access to the domain management console
- A registrar lock, which is a service that includes clientTransferProhibited, clientUpdateProhibited and clientDeleteProhibited. These three statuses combined prevent the domain from being deleted, transferred to another registrar without authorization, or having its information modified.
- DNSSEC support

Register similar domains (defensive registration)

Consider proactively registering TLDs that might mimic the brand (brand.co.uk, for example, when the brand's domain is brand.com). Create a policy for registration of high-risk domains that are not used for production. These can include lookalike names, typos, common abbreviations or shortenings of your company name (e.g. "BofA" for "Bank of America"), combined with commonly abused terms like "login" or "account," or other vectors you have had to combat. You cannot register an infinite number of these, so prioritize and set a budget. Reevaluate based on ongoing experience. Such work should be coordinated with monitoring and malicious domain mitigation programs.

Combine SSL certificate management with DNS management

While SSL/TLS certificates aren't strictly DNS-related, they are often administered by the same team and exhibit similar legal or technical challenges. Consider consolidating their management with the domain administrator or team.

Also, as with domains, SSL certificate registrations should be monitored for lookalike registrations.

Include Certificate Authority Authorization (CAA) records for your domain to help avoid unauthorized TLS certificates being issued.

Keep domain names secure

Identify domain names as an asset and perform a risk assessment.

Set the appropriate Extensible Provisioning Protocol (EPP) domain status codes for the organization's domain names. Some relevant codes are:

- clientTransferProhibited
- clientDeleteProhibited
- clientUpdateProhibited

In addition to these, consider implementing a service known as a "registry lock." Through their registrars, registry lock allows registrants an extra out-of-band protection against unauthorized changes or deletions.

Some registrars also provide a registrar lock service, adding still another level of security above what registry lock offers. Registrar-locked domains require out-of-band confirmation before any changes are made.

Once the brand has locked the domain name, routinely check the WHOIS service to make certain it remains locked, and that the domain name information (including DNS configuration [assigned nameservers and what they say] as well as listed contact information) has not been modified without the organization's knowledge and consent. Consider using a third-party monitoring product for this that will alert you of changes.

Back up DNS configuration

Storing DNS configuration securely will mean the brand can always revert if settings are lost for any reason (e.g., account compromise). Develop a strategy for urgent restoration of domain name and DNS configuration as part of business continuity planning and tabletop exercises. Investigate whether business interruption and losses related to a domain name or DNS configuration incident are covered by the organization's insurance policies. Incorporate domain name hijacking into incident response and business continuity planning.

Consider monitoring for abusive third party domains

Look into monitoring third-party domains that could be problematic for your brand. There are companies that reliably provide this service. If you are not doing this, you are opening your brand to significant potential abuse.

Attack Vectors and Mitigation

Attackers would love to take advantage of the trust you've established in your domains. If they can't gain control of one of your actual domain names, they may do the next best thing and attempt to register a variant thereof.

Squatters, Lookalike Domains (Homographs) and Other Encroachments

Consider monitoring new domains (or have a service monitor them for you) for registration of lookalike names. This is a good initial step to understanding domains that attempt to mimic your brand. Many brands utilize a third party as a managed service provider.

Sources to find new domains:

- ICANN's Centralized Zone Data Service (CZDS). NB: While CZDS is a great starting place, as it offers domains from all the generic Top Level Domains, it doesn't include the country code Top Level Domains (ccTLDs). You may need to consider these additional zone files depending on your threat landscape.
- SSL cert registrations
- Paid services that provide data on newly registered or newly observed domain names

Once you find lookalike domains, they must be reviewed to determine whether they are benign or malicious. For the purposes of this document, "malicious domains" are those that are used to perpetrate activities like distribution of malware, command and control of botnets, phishing, business email compromise or the sending of spam. A domain that is registered and used in bad faith using a trademark registered and owned by a third party is not considered malicious if it is not, in addition to the trademark violation, also used for the malicious activities just described.

Should benign domains be monitored, or actually purchased? Should administrative proceedings be initiated? How should malicious domains be mitigated? Read on…

Generally, there are two classifications to consider when it comes to domain mitigation.

Malicious Domain Mitigation: Domain Takedown Requests

These are domains for which you have proof of malicious activity like phishing or credential theft.

Entities requesting domain takedown must provide detailed evidence of abuse. If the responsible organization determines that the domain is malicious or an infringement on the brand, they can contact the registrar organization, which can be found via the WHOIS information for the domain.

In some cases, if the hosting provider for the location is a separate entity, contacting them may mitigate hosted content faster. If the matter is strictly related to a trademark violation, it may be a matter for a UDRP proceeding or civil litigation. ICANN accredits registrars and can be contacted if the registrar is non-responsive.

Common evidence examples include screenshots of offending content or a sample lure email (with headers) that was sent from the domain.

Results of a "takedown" action by the domain's registrar can differ depending on the registrar, but should at a minimum result in denial of access to the domain by the malicious actor. Once a domain has been taken down, the domain should be monitored for resumed activity. Alternatively, the targeted brand can choose to purchase the domain. Some registrars will transfer the domain to the brand if the brand is willing to take on the responsibility for it going forward. This can be valuable for alerting potential victims that they have fallen for an attack, or for gathering statistics.

Keep in mind, though, that ICANN-accredited registrars will normally only consider a domain malicious if it was registered and is being used for phishing, malware distribution or botnet command and control. Compromised domains are a different issue altogether. Suspending them is usually not the best course of action.

Brand-Offensive Domains Mitigation

These are domains that infringe a company's trademark, but in a non-malicious fashion.

The takedown process for malicious domains, as detailed above, can be followed for brand-offensive domains as long as they are involved in phishing, malware distribution or botnet command and control (for gTLD domains). The process for ccTLD domains will depend on each ccTLD's own terms of service (TOS). Also, if the owner of the domain can be determined by examining the hosted content or the domain's WHOIS data, then an informal appeal can be made to the owner directly – except, of course, if there is reason to believe that the registrant is itself a malicious actor.

If these options are unsuccessful, a brand may consider filing a formal request to dispute the domain name via a Uniform Domain-Name Dispute-Resolution Policy (UDRP) or Uniform Rapid Suspension (URS) request. These procedures have a cost and last a few months, but if they are successful, the brand may take control of the offending domain.

Which Domains Should Be Purchased, and Which Should Be Monitored?

For domains that are suspicious but that do not present enough proof to warrant a takedown request, or for takedown requests that have been unsuccessful, a brand can either attempt to purchase the domain, or else monitor the domain for relevant changes in state to hosted content, or for other attributes such as DNS record changes. While there are pros and cons to both, best practices suggest purchasing a limited number of highly suspect or potentially useful domains and monitoring the rest via a combination of technology and human review. What you can't buy based on your risk tolerance and budget, you should monitor.

Spoofing (for Email)

Spoofing is when an attacker sends an email to a customer or employee that appears legitimate, but is not from the legitimate domain (e.g., microsoftt.com). An attacker does not need to control a spoofed domain in order to be able to emit spoofed email from it.

Spoofing Mitigation: Monitor and Submit a Complaint

- Consider monitoring and detecting lookalike domains by leveraging different open-source tool sets or third-party vendors that perform monitoring on your behalf.
- Once abuse is identified, a complaint can be submitted to the offending domain's registrar. Consult the "Malicious Domain Mitigation: Domain Takedown Request" section above.

When it comes to protecting your own domains from misuse in messaging, take full advantage of the Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) and Domain-based Message Authentication, Reporting & Conformance (DMARC) as described in "M³AAWG Trust in Email Begins with Authentication" and "M³AAWG Email Authentication Recommended Best Practices." You should protect all of your domains with these techniques, even if you don't normally send mail from some of those domains. You can also consider removing the MX records (the name of the mail servers and their IP addresses) for those domains from which you do not send email.

Account Takeover (ATO)

All an attacker needs to gain control of an organization's entire domain name portfolio (and to hamper authorized access to that portfolio) is often just a user account and password. Attackers need only guess, phish or apply social engineering techniques to a single point of contact to gain control of a domain registration account.

Email is the preferred and often the only method by which some registrars attempt to notify a registrant of account activity.

Attackers can also block delivery of email notifications to targeted registrants by altering DNS configuration information so that email notifications will not be sent to any recipient in the domains that the attacker controls through a compromised account (e.g., the registrant's identified administrative or technical contact email addresses hosted in the domain). Ideally, register a contact address that is outside the domain so that in case account takeover happens, you can still receive notifications.

Also, phishers use email addresses similar to domain name registrars or DNS providers in phishing scams to gain control over legitimate domain names. Often, the attacker's objective is to change the IP addresses of your name servers in order to control name resolution for your domain. An attacker who can gain control over your name servers can inflict different kinds of harm. They can gain access to email sent to the compromised organization's domain; set up a real-time copy of your organization's website; capture usernames and passwords; and use your domain as a source for spam or other criminal activities, causing harm to your organization's reputation and direct financial loss for your clients and providers. Stealthier attacks via your domain registration account include using your account and its attached payment information to create wholly new domains, or "domain shadowing,"[1] where subdomains of your existing domain are added that the attacker controls separately. In these attacks, you will not immediately notice an issue with your website or email. The miscreant leaves those untouched, and simply uses your money or existing domain to create new domains and subdomains that they point elsewhere using the DNS, and that they control on their own. This can lead to reputation problems and targeted phishing against your own domain(s), since they can create convincing subdomains like "login.yourcompany.com," or "email.yourcompany.com." These are very difficult to detect, since few registrars provide monitoring tools for new domains added to your account, or subdomains added to your domain name. Where these tools exist, you should take advantage of them. Scheduling a regular spot-check of your domain management

[1] See https://encyclopedia.kaspersky.com/glossary/domain-shadowing/

account to review any recent changes can mitigate these sorts of attacks. Another technique to spot domain shadowing is to get a report of new hostnames on your domain from a passive DNS provider.

Account Takeover Mitigation: Monitor and Submit a Complaint

- Ensure multifactor authentication is enabled for all accounts.
- Monitor for anomalous behavior (e.g., unusual log-in activity).
- Consider monitoring and detection of lookalike domains by leveraging different open-source tool sets or third-party vendors that perform monitoring on your behalf.
- Once abuse has been identified, submit a complaint to the offending domain's registrar. Consult the "Malicious Domain Mitigation: Domain Takedown Request" section above.
- Create and document your mitigation processes and share with relevant security departments.

Software Vulnerability

Attackers scan domain account registration and administration portals for web application vulnerabilities (e.g., SQL injection). A successful exploit of vulnerable application code can result in the disclosure of account credentials for many domain accounts.

Software Vulnerability Mitigation: Update Software

- Ensure your software is up to date and patched with the latest updates to limit exploitation of vulnerabilities.
- Introduce a responsible vulnerability disclosure program to understand vulnerabilities in the wild.

Conclusion

This document is a brief introduction to some of the issues around brand management and domain names. Brand owners should consider having a face-to-face meeting with individuals involved in the legal and technical aspects of the domain name process to ensure that all locally unique considerations have been surfaced and adequately discussed.

Recommended Resources

- Seek legal advice from trademark counsel to ensure that you are cost-effectively and properly protecting your names and marks in relevant jurisdictions.

- Consult with legal counsel on whether to use the ICANN Trademark Clearinghouse. See https://newgtlds.icann.org/en/about/trademark-clearinghouse.

Further reading about domain attack vectors and mitigation

"A Registrant's Guide to Protecting Domain Name Registration Accounts," ICANN SSAC-044, a more detailed description of security measures.

"About Zone File Access," https://www.icann.org/resources/pages/zfa-2013-06-28-en, and ICANN's Centralized Zone Data Service https://czds.icann.org/home (but remember, CZDS provides access to gTLD zone files, not ccTLDs).

M3AAWG Protecting Parked Domains BCP https://www.m3aawg.org/sites/default/files/m3aawg_parked_domains_bp-2015-12.pdf

As with all documents that we publish, please check the M^{3}AAWG website (www.m3aawg.org) for updates.