Erkennung „bösartiger“ Domains

Tobias Niedl
Betreuer: Lothar Braun
Seminar Future Internet SS2011
Lehrstuhl Netzarchitekturen und Netzdienste
Fakultät für Informatik, Technische Universität München
Email: niedl@in.tum.de

KURZFASSUNG

Als „bösartig“ werden Domains bezeichnet, die zu illegalen bzw. kriminellen Aktivitäten im Internet verwendet werden, beispielsweise in sog. Botnetzen. Neben Botnetzen können „bösartige“ Domains jedoch auch in anderen Zusammenhängen auftreten. Traditionell wurde und wird mittels Sperrlisten (engl. „blacklists“) versucht, die Nutzung solcher Domains zu unterbinden. Blacklists sind zwar ein einfaches und effizientes Mittel, besitzen jedoch den Nachteil, dass das Erkennen und Aufnehmen einer Domain in eine Blacklist eine gewisse Zeit in Anspruch nimmt. Entsprechend ist es das Ziel verschiedener Forschungsarbeiten, „bösartige“ Domains schnell und automatisiert zu erkennen, bevor ein Schaden durch ihre Verwendung entsteht. Diese Arbeit stellt drei solcher Arbeiten vor: „Proactive Domain Blacklisting“, „EXPOSURE“ und das „Fast-flux Botnet observation“-Verfahren. Wobei sich letzteres speziell auf die Erkennung von sog. Fast-flux Domains konzentriert, um die zugehörigen Botnetze näher untersuchen zu können.
Alle drei Verfahren nutzen bestimmte Eigenschaften von Domains bzw. Nameservern, um Domains zu klassifizieren, d.h. zu entscheiden ob diese „gut“ oder „böse“ sind. Da die Verfahren verschiedene Ziele verfolgen, werden unterschiedliche Ansätze verfolgt, die zu unterschiedlichen Ergebnissen führen.

Schlüsselworte

Malicious Domains, Botnet, Proactive Domain Blacklisting, EXPOSURE, Fast-flux Domains

1. EINLEITUNG

Eine Domain an sich ist weder „gut“ noch „böse“. Erst ein bestimmter Verwendungszweck bzw. eine bestimmte Anwendung lässt eine Domain als „böse“ erscheinen. Zu solchen Anwendungen gehören u.a. sog. Botnetze, die das „Domain Name System“ (DNS) und somit bestimmte Domains nutzen. Der Begriff Botnetz beschreibt ein Netzwerk von infizierten Computern (sog. „Bots“), die durch die Installation von Schad-Software (engl. „malware“) Teil des Netzwerks wurden. Die Bots stehen unter der Kontrolle eines Administrators, dem sog. „Botmaster“ (vgl. [1]). Dieser kann das Botnetz zu den verschiedensten Zwecken nutzen, z.B. für „Distributed Denial of Service“-Angriffe (DDoS), zum Versenden von Spam-E-Mails, zum sammeln sensibler Benutzerinformationen wie Bankverbindungs- oder Kreditkartendaten (vgl. [8]) usw. Außerdem können Botnetze auch zum Bereitstellen bzw. Vermitteln von Webinhalten genutzt werden, als „Content Distribution Netzwork“ (CDN) (vgl. [6]).
Da Botnetze auf eine Steuerung durch den „Botmaster“ angewiesen sind, müssen die einzelnen Bots regelmäßig Kontakt zu dessen Steuerungsrechner aufnehmen [8]. Würde die IP-Adresse des Steuerungsrechners fest in den Bots kodiert werden, könnte der „Botmaster“ relativ schnell gefunden und dessen Steuerungsrechner abgeschaltet werden. Das Botnetz wäre dann nicht mehr in der Lage, neue Anweisungen zu erhalten und somit unschädlich gemacht. Um diese Gefahr zu umgehen, nutzen Botnetze Domainnamen bzw. das DNS.
Werden Botnetze zur Bereitstellung von Webinhalten verwendet (als CDN), nutzen sie ebenfalls das DNS. Dann sind unter einem Domainnamen (einer sog. Fast-flux Domain) die meist illegalen Web-Inhalte abrufbar.

Neben Botnetzen gibt es auch andere Verwendungszwecke von Domains, die diese als „bösartig“ erscheinen lassen. Wird beispielsweise eine sog. Phishing-Seite auf einem regulären Webserver betrieben, so gilt die dazu genutzte Domain ebenfalls als bösartig. Phishing-Seiten werden von Kriminellen betrieben und sind den Webseiten von Unternehmen nachempfunden. Sie versuchen die Kunden der entsprechenden Unternehmen zur Eingabe ihrer Kennwörter (bei Banken auch PINs und TANs) zu bewegen.
Botnetze und Phishing-Seiten dienen an dieser Stelle als Beispiel, um aufzuzeigen in welchem Zusammenhang in dieser Arbeit von „bösartigen“ Domains gesprochen wird.

In dieser Arbeit werden drei Ansätze vorgestellt und verglichen, die versuchen zu erkennen, ob eine Domain für kriminelle Zwecke verwendet wird. „Proactive Domain Blacklisting“ [9] und „EXPOSURE“ [8] versuchen Domains zu finden, die bisher noch nicht durch bösartige Aktivitäten aufgefallen sind. Das „Proactive Domain Blacklisting“-Verfahren versucht anhand bekannter „bösartiger“ Domains, die bereits auf einer Blacklist geführt werden, ähnliche Domains zu finden, bevor diese ebenfalls zu bösartigen Zwecken verwendet werden können. „EXPOSURE“ versucht mithilfe von Datamining-Methoden „bösartige“ Domains im live DNS-Verkehr zu erkennen. Beide Verfahren können „bösartige“ Domains unabhängig davon erkennen, ob diese in Botnetzen eingesetzt werden oder nicht.
Das Ziel des „Fast-flux Botnet observation“-Verfahrens [6] ist hingegen *nicht*, bisher unbekannte Schad-Domains zu finden. Stattdessen werden Domains aus verschiedenen Quellen analysiert, um zu erkennen, ob diese als Fast-flux Domains in Botnetzen eingesetzt werden. Anschließend werden die zugehörigen Botnetze näher untersucht. Da Fast-flux Domains nur im Zusammenhang mit Botnetzen auftreten, kann das

doi: 10.2313/NET-2011-07-2_11

Verfahren – im Gegensatz zu den beiden anderen Methoden – nur Schad-Domains finden, die in bzw. für Botnetze genutzt werden.

Die genannten Verfahren werden hier gegenüber gestellt, da sie Beispiele für unterschiedliche Techniken zur Erkennung „böser“ Domains darstellen. „Proactive Domain Blacklising“ versucht eine Erkennung anhand statistischer Eigenschaften der Domains. „EXPOSURE“ nutzt Verkehrsanalysen sowie maschinelles Lernen und das „Fast-flux Botnet observation“-Verfahren stellt schließlich einen Mechanismus für eine spezielle Klasse von Schad-Domains dar, nämlich Fast-flux Domains von Botnetzen.

Alle drei Verfahren versuchen aus bestimmten Eigenschaften einer Domain jeweils automatisch zu erkennen, ob diese zu bösartigen Zwecken verwendet wird. Entsprechend müssen bei den Ergebnissen vier Fälle unterschieden werden:

- *true positive*: Eine Domain wird für bösartige Zwecke eingesetzt und vom angewendeten Verfahren als solche erkannt
- *false positive*: Eine Domain wird nicht für bösartige Zwecke verwendet, aber als solche eingestuft
- *false negative*: Eine Domain wird für bösartige Zwecke eingesetzt, aber nicht als bösartig erkannt
- *true negative*: Eine Domain wird nicht für bösartige Zwecke verwendet und auch nicht als solche eingestuft

Das Ziel aller Verfahren ist es, eine möglichst hohe „true positive“- bzw. „true negative“-Rate und eine möglichst geringe „false positive“- bzw. „false negative“-Rate zu erreichen.

Der Aufbau dieser Arbeit gliedert sich im Weiteren wie folgt: In Abschnitt 2 werden die für diese Arbeit wichtigsten Bestandteile und Funktionsweisen des DNS erläutert. In Abschnitt 3 werden die Verfahren „Proactive Domain Blacklisting“, „EXPOSURE“ und „Fast-Flux Botnet observation“ genauer vorgestellt und in Abschnitt 4 verglichen. Abschnitt 5 fasst diese Arbeit schließlich kurz zusammen.

2. DAS „DOMAIN NAME SYSTEM“ (DNS)

Menschen können sich i.d.R. aussagekräftige Namen wie „tumuenchen.de“ besser merken, als Ziffernkolonnen von IP-Adressen wie „129.187.39.3“. Allerdings funktioniert das Finden von Hosts im Internet nur über solche schwer merkbaren IP-Adressen. Das DNS übernimmt die Aufgabe, Domains bzw. Hostnamen, mit denen Benutzer arbeiten, in die zugehörigen IP-Adressen umzuwandeln, die in den Knoten des Internet verwendet werden (vgl. [11]).

2.1 Domain Bestandteile

Eine Domain besteht aus mehreren Teilen, wobei die einzelnen Teile durch einen Punkt getrennt werden. Die Informationen im Domainnamen werden von links nach rechts immer allgemeiner oder „unschärfer“. Am rechten Ende steht die Topleveldomain (TLD), wie *.com* oder *.de*.

Links von der TLD folgt der Domainname. Vor dem Domainnamen können keine, eine oder mehrere Subdomains stehen, d.h. weitere Domainnamen. Durch die verschiedenen Domainnamen bzw. die TLD entsteht eine Hierarchie. Für jeden Domainnamen innerhalb einer Domain kann ein eigener DNS-Server in der DNS-Hierarchie verantwortlich sein.

2.2 DNS Hierarchie

Das DNS arbeitet als eine verteilte Datenbank, die hierarchisch organisiert ist. An der Wurzel stehen die sog. Root-Server. Diese kennen die DNS-Server, die für die verschiedenen TLDs verantwortlich sind. In den DNS-Servern der TLDs sind für jeden registrierten Domainnamen die verantwortlichen „authoritive“ Nameserver hinterlegt. Die „authoritive“ Nameserver wiederum kennen schließlich die IP-Adresse für einen Domainnamen.

Die einzelnen DNS-Server speichern jeweils nur bestimmte Teile der DNS-Datenbank in sog. „Ressource Records“ (RRs). Ein RR ist ein 4-Tupel und besteht aus aus den Feldern „Name“, „Value“, „Type“ und „TTL“ („Time-to-live“). Es gibt verschiedene RR-Typen, die jeweils die Bedeutung der Felder Name und Value festlegen. Für diese Arbeit sind vor allem die Typen „Address“ (A) und „Nameserver“ (NS) von Bedeutung.
Beim Typ A enthält das Feld Name einen Domainnamen und das Feld Value die IP-Adresse des zugehörigen Hosts. Einer Domain können mehrere IP-Adressen zugeordnet sein. Dann existieren mehrere A-RRs mit gleicher Domain und den verschiedenen IP-Adressen. Bei einer Anfrage für eine solche Domain werden alle A-RRs als Antwort zurück gegeben. Das anfragende Programm entscheidet sich dann für die Verwendung einer dieser IP-Adressen. Durch dieses „Round Robin“-Verfahren kann eine Lastverteilung auf DNS-Basis erzielt werden (vgl. [8, 14]).
Beim RR-Typ NS enthält das Feld Name einen Domainnamen und das Feld Value den Domainnamen eines dazu gehörigen „authoritive“ Nameservers. Auch hier sind mehrere NS-RRs für mehrere Nameserver möglich.

Das Finden einer IP-Adresse zu einem Domainnamen wird als „auflösen“ eines Domainnamens bezeichnet. Diesen Prozess übernimmt ein sog. „Resolver“. Dieser ist i.d.R. Teil des Betriebssystems und schickt eine DNS-Anfrage an einen Nameserver, der die eigentliche Arbeit übernimmt. Das TTL-Feld in einem RR gibt an, wie lange ein RR von einem solchen Server bzw. dem „Resolver“ zwischengespeichert werden darf (engl. „caching“), bevor eine neue Anfrage gestartet werden muss. Durch das „Caching“ wird die Last im DNS verringert, da Hosts in einem Zeitraum ort dieselbe Domain mehrmals aufrufen und somit mehrmalige DNS-Anfragen vermieden werden. Der Richtwert für den TTL-Wert eines Domaineintrags (A-RR) liegt für „typische Hosts“ in der Größenordnung mehrerer Tage (vgl. [10]).

3. VERFAHREN ZUR ERKENNUNG „BÖSARTIGER“ DOMAINS

Alle drei im folgenden vorgestellten Verfahren zielen darauf ab, Domains zu erkennen, die bereits in Botnetzen genutzt oder mit hoher Wahrscheinlichkeit in Zukunft in solchen verwendet werden.

doi: 10.2313/NET-2011-07-2_11

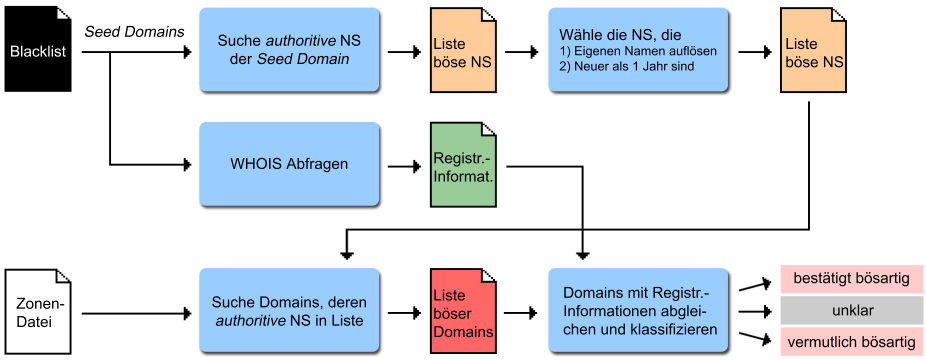

Abbildung 1: Ablauf des „Proactive Domain Blacklisting"-Verfahrens

3.1 Proactive Domain Blacklisting

Die Betreiber von Botnetzen registrieren meist mehrere Domains in Gruppen (vgl. [4]), die dann nach und nach verwendet werden. Wird eine verwendete Domain in eine Blacklist aufgenommen (oder gesperrt), können die Botnetzbetreiber schnell auf eine andere Domain wechseln und so einen Ausfall des Botnetzes vermeiden.
Das Verhalten der Botnetz-Betreiber, die meist mehrere Domains in einem Durchlauf registrieren bzw. administrieren, wird im „Proactive Domain Blacklisting"-Verfahren [9] dazu genutzt, weitere Schad-Domains, evtl. auch vor deren erster Nutzung, zu erkennen. D.h. ausgehend von einer oder mehreren Domains, die von einem Botnetzbetreiber administriert werden und die bereits auf einer Blacklist stehen, können weitere, evtl. ungenutzte Domains des Betreibers anhand verschiedener Eigenschaften gefunden werden. Die gefundenen Domains können dann auf eine Blacklist gesetzt oder durch den Registrar gesperrt werden, bevor weiterer Schaden durch ihre Verwendung entsteht.

3.1.1 *Untersuchte Eigenschaften*

Das Verfahren nutzt Eigenschaften des „authoritive" Nameserver einer untersuchten Domain. Dazu zählen der Domainname des NS, das Alter dieser NS-Domain und ob der Nameserver seinen eigenen Domainnamen selbst auflöst. Ist der Domainname des NS noch nicht lange registriert (jünger als ein Jahr) und übernimmt der NS selbst seine Namensauflösung, spricht dies für die Nutzung von sog. „double-flux" Techniken in einem Botnetz. „Double fluxing" funktioniert ähnlich wie „single fast-flux" (siehe Abschnitt 3.3.1), allerdings übernimmt nicht ein regulärer „authoritive" NS die Namensauflösung der Domain, sondern das Botnetz selbst[1].

Darüber hinaus werden zwei Eigenschaften der untersuchten Domain betrachtet, nämlich das Registrierungsdatum und der Registrar, also das Unternehmen, bei dem die Domain registriert ist. Die Verwendung aller genannten Eigenschaften wird im folgenden Abschnitt erläutert.

3.1.2 *Ablauf des Verfahrens*

Als Eingabe dient eine Blacklist, von der zufällige Domains ausgewählt werden, die sog. „Seed Domains." Diese werden dann weiter untersucht. Es werden die „authoritive" Nameserver, die einmal eine solche „Seed Domain" aufgelöst haben, bestimmt und auf einer Liste festgehalten.
Da die so erstellte Liste „böser" Nameserver auch die Nameserver großer „Internet Service Provider" (ISPs) enthalten kann, die normalerweise für mehr „normale" als „bösartige" Domains verantwortlich sind, wird in einem zweiten Schritt versucht, diese ISP-Nameserver herauszufiltern. Dazu wird die ursprüngliche Liste auf die Nameserver verkürzt, die die folgenden zwei Kriterien erfüllen:

1. Frische: Die Domain des Nameservers ist erst vor kurzem (innerhalb des letzten Jahres) registriert worden

2. Selbst-auflösend: Der Nameserver ist selbst für die Auflösung seines Domainnamens verantwortlich

Im nächsten Schritt werden die Registrierungsinformationen der „Seed Domains" mittels „WHOIS"-Abfragen ermittelt. Dadurch werden das Registrierungsdatum und der Registrar der Dominas bekannt gemacht. „WHOIS" [7] ist ein Client-Server Protokoll zur Abfrage von Domain-Informationen.

Als letztes findet die eigentliche *pro-aktive* Untersuchung von Domains statt. Dazu ist eine Quelle für Domains nötig, die auf ihre „Bösartigkeit" untersucht werden sollen. Prinzipiell ist jede Liste von Domains als Quelle nutzbar. Allerdings müssen neben den zu untersuchenden Domains auch deren NS-RRs, sowie das Registrierungsdatum bekannt sein. In [9] wird als Quelle die Zonen-Datei der *.com* TLD verwendet. Darin sind neben allen Domainnamen, die auf *.com* enden, auch deren „authoritive" Nameserver, also die NS-RRs, aufgeführt. Die Nutzung der *.com* Zonen-Datei stellt jedoch nur ein Beispiel zum Testen des Verfahrens dar. Es können auch andere Listen oder die Zonen-Dateien anderer TLDs genutzt werden, wenn diese zur Verfügung stehen.
Die Auswertung erfolgte über mehrere Wochen. Da täglich die aktuelle Zonen-Datei zur Verfügung stand, ist durch das Erscheinen von neuen Domains implizit auch deren Registrierungsdatum bekannt. Abbildung 1 stellt den Aufbau bzw. Ablauf des Verfahrens nochmals graphisch dar.

Die Auswertung der Zonen-Datei läuft dabei wie folgt ab: Wenn zum Zeitpunkt T eine Schad-Domain auf einen Nameserver A wechselt, werden alle Domains in der Zonen-Datei gesucht, die ebenfalls zum Zeitpunkt T auf den Nameserver

[1] Für eine detaillierte Darstellung von „single flux" und „double flux" Netzen sei auf [15] verwiesen

doi: 10.2313/NET-2011-07-2_11

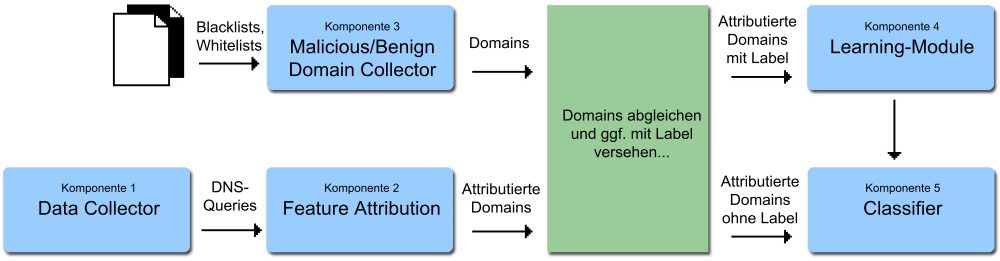

Abbildung 2: Die Architektur von EXPOSURE (nach [8])

A wechselten. Wenn eine Schad-Domain zu einem Zeitpunkt T auf Selbst-auflösung umgestellt wird, werden die Domains gesucht, die ebenfalls zum Zeitpunkt T auf Selbst-auflösung gewechselt wurden (vgl. [9]). Abschließend werden die Domains der Zonen-Datei jeweils einer Kategorie zugeordnet:

- Nachweislich bösartig: Die Domain wurde als „bösartig“ erkannt und steht bereits auf einer Blacklist
- Unbekannt: Es ist nicht eindeutig, ob die Domain zu bösartigen Zwecken verwendet wird
- Vermutlich bösartig: Die Domain wird vermutlich für bösartige Zwecke eingesetzt werden. Andere Verfahren (URIBL gold, SiteAdvisor) schätzen die Domain ebenfalls als „bösartig“ ein

3.2 EXPOSURE

Im Gegensatz zum „Proactive Domain Blacklisting“, das aktiv nach „bösartigen“ Domains innerhalb einer Zonen-Datei sucht, ist EXPOSURE ein System, das passiv arbeitet. Es analysiert den DNS-Verkehr von „authoritive“ Nameservern und stuft eine angefragte Domain anhand von 15 Kriterien als „gutartig“ oder „bösartig“ ein. EXPOSURE nutzt dazu Verfahren des maschinellen Lernens. Mit einem Trainingsset werden dem System Regeln beigebracht wie es „bösartige“ Domains erkennen kann. Das verwendete Trainingsset besteht aus den DNS-Antworten von „authoritive“ Nameservern auf rekursive DNS-Anfragen. Die Daten des Trainingssets stammen aus dem „Security Information Exchange“-Programm [5].

3.2.1 Untersuchte Eigenschaften

Die Domains werden anhand von 15 verschiedenen Attributen (engl. „features“) untersucht, die sich in folgende Klassen einteilen lassen: Zeit-basierte Eigenschaften, DNS-Antwort-basierte Eigenschaften, TTL-basierte Eigenschaften und Domainnamen-basierte Eigenschaften.

Die untersuchten Zeit-basierten Eigenschaften sind nicht fest an eine Domain gebunden, sondern ergeben sich stattdessen aus der Analyse des DNS-Verkehrs, der Aufschluss über die Zeitpunkte und Häufigkeiten von Anfragen gibt.
Zu den untersuchten Eigenschaften gehört u.a. die Lebensdauer der Domain. Eine Domain wird als kurzlebig eingestuft, wenn sie nur innerhalb eines relativ kurzen Zeitfensters von wenigen Tagen nachgefragt wird. Ein solches Verhalten wird als „abnormal“ eingestuft, da eine gewöhnliche Domain, auch wenn sie nicht sehr bekannt ist, doch mehrmals über den Beobachtungszeitraum hinweg nachgefragt werden sollte (vgl. [8]). Im Weiteren wird u.a. geprüft, ob sich die Anfragen für eine Domain zu bestimmten Tageszeiten regelmäßig häufen.

Die DNS-Antwort-basierten Eigenschaften unterteilen sich wie folgt: Es wird die Anzahl der IP-Adressen in den A-RRs bestimmt. Viele IP-Adressen sind zwar ein Indiz, deuten alleine jedoch noch nicht auf eine „bösartige“ Domain hin, da mehrere IP-Adressen auch von regulären Internet-Diensten zur Lastverteilung verwendet werden. Zusätzlich wird daher untersucht, zu wie vielen verschiedenen Ländern die IP-Adressen in den A-RRs gehören und wie viele Domains unter jeder einzelnen IP-Adresse zu erreichen sind.

Aufgrund der Infrastruktur von Botnetzen, deren Bots über verschiedene Internetzugänge verfügen und die über verschieden lange Zeiträume erreichbar sind, ändern sich die TTL-Werte „bösartiger“ Domains öfter, als die Werte gewöhnlicher Domains. Daher werden die TTL-Werte in den DNS-Antworten ebenfalls untersucht. Zu den TTL-basieren Eigenschaften gehört der durchschnittliche TTL-Wert in den A-RRs, sowie die TTL Standardabweichung. Im Weiteren wird gezählt, wie oft sich die TTL-Werte für eine Domain ändern und zu welchem prozentualem Anteil ein bestimmter TTL-Bereich von einer Domain genutzt wird. Ein TTL-Wert im Bereich [0,100) wird nach [8] besonders häufig für Schad-Domains verwendet.

Schließlich werden zwei Eigenschaften untersucht, die auf dem Domainnamen selbst basieren. Damit sollen Domainnamen erkannt werden, die durch einen Algorithmus erzeugt werden. Einige Botnetze wie „Conficker“, „Kraken“ und „Torpig“ erzeugen mehrmals täglich mehrere hundert Domains mittels eines „Domain Generation Algorithmus“ (GDA). Einige der erzeugten Domains registriert der Botnetzbetreiber und leitet sie auf die Steuerungsrechner des Botnetzes weiter. Die Bots fragen die generierten Domains an, bis ein Name aufgelöst wird und somit eine Kommunikation mit dem Steuerungsrechner möglich ist (vgl. [13]).
„EXPOSURE“ untersucht den prozentualen Anteil von Ziffern im Domainnamen sowie den prozentualen Anteil des längsten sinnvollen Substrings, d.h. ein Wort aus einem englischen Wörterbuch (engl. „longest meaningful substring“) um solche algorithmisch generierten Domainnamen zu finden. Da es jedoch auch bekannte Domains gibt, die keinen sinnvollen Ausdruck enthalten, z.B. „google.com“ oder „yahoo.com“, werden Domainnamen zusätzlich einer Google-Suche unterzogen (vgl. [8]).

doi: 10.2313/NET-2011-07-2_11

3.2.2 Komponenten

Das System besteht aus folgenden Komponenten: Ein „Data Collector“ sammelt die DNS-Anfragen eines Netzwerks ein, das beobachtet werden soll. Eine zweite Komponente, die „Feature Attribution“, versieht die gesammelten Domains mit deren Eigenschaften. Ein drittes Teilsystem „Malicious/Benign Domain Collector“ sammelt, unabhängig von den ersten beiden Komponenten, Domainnamen von Black- und Whitelists. Für diese Domainnamen ist somit explizit bekannt, ob sie „gut-“ oder „bösartig“ sind.

Die vom „Data Collector“ gesammelten und mit Attributen versehenen Domainnamen werden mit den explizit „gut-“ oder „bösartigen“ Domainnamen, die der „Malicious/Benign Domain Collector“ gesammelt hat, abgeglichen. Ist ein Domainname auf einer White- bzw. einer Blacklist enthalten, wird bei den bereits attribuierten Domainnamen jeweils zusätzlich ein Label für „gut“ oder „böse“ gesetzt. Ist eine Domain nicht explizit in einer White- oder Blacklist enthalten, wird kein Label gesetzt.

Die Domainnamen, die mit Label versehen sind, werden an die vierte Komponente, das „Learning Module“ übergeben. Dessen Ergebnisse, sowie die Domainnamen, die nicht mit einem Label versehen sind, werden der fünften Komponente übergeben, dem „Classifier“. Dieser entscheidet anhand der gelernten Muster und den Attributen einer Domain jeweils, ob diese zu bösartigen Zwecken verwendet wird, oder nicht.

Abbildung 2 stellt die Architektur von EXPOSURE nochmals graphisch dar.

3.2.3 Nutzung des Systems

Die Nutzung von „EXPOSURE“ unterteilt sich in zwei Phasen. In einem „offline Experiment“ wurden DNS-Anfragen verschiedener „authoritive“ Nameserver untersucht. Die Daten stammten vom „Security Information Exchange“ [5] und bestehen aus ca. 100 Mrd. DNS-Anfragen über einen Zeitraum von zweieinhalb Monaten. Da diese Datenmenge zu groß für eine Analyse war, wurde sie mittels zweier Maßnahmen verkleinert: Zum einen wurden, mittels einer Whitelist von Alexa [2], die Anfragen für die 1.000 bekanntesten Domainnamen herausgefiltert. Zum anderen wurden Anfragen für Domains, die älter als ein Jahr sind, entfernt. Damit reduzierte sich die Datenmenge auf die Hälfte. Mit diesen Daten wurde das System trainiert.

In einer zweiten Phase wurde EXPOSURE im Netzwerk eines ISP mit ca. 30.000 Kunden eingesetzt. In einem Zeitraum von zwei Wochen wurden dort im live DNS-Verkehr die DNS-Anfragen untersucht, um neue Schad-Domains zu finden. Anders als im „offline Experiment“ wurden die gesammelten DNS-Anfragen vor der Analyse nicht gefiltert.

3.3 Fast-flux Botnet observation

Wie bereits erwähnt, können Botnetze auch als Hosting-Plattform verwendet werden, um Webinhalte bereitzustellen bzw. zu vermitteln (vgl. [6]). Botnetze verwenden dazu eine Technik namens „Fast-flux“, die ein schnelles Mapping zwischen Domainnamen und IP-Adressen auf DNS-Basis ermöglicht (vgl. [6]). Das Ziel ist es, die meist illegalen Webseiten möglichst lange bereitzustellen und die eigentlichen Quellen zu verschleiern. Durch die Fast-flux-Technik wird das Finden der Webserver und das Unterbinden der kriminellen Aktivitäten wesentlich erschwert (vgl. [15]). Da dieselbe Technik auch von regulären Internet-Diensten zur Last-Balancierung verwendet wird, ist das Finden von Fast-flux Domains bzw. die Unterscheidung von „gutartigen“ und „bösartigen“ Domains jedoch schwierig.

3.3.1 Gewöhnliche und Fast-flux Domains

Für eine gewöhnliche Webseite (ohne Lastverteilung auf DNS Basis) stellt sich der Prozess nach dem Aufruf im Browser wie folgt dar: Der Webbrowser nutzt den „Resolver“ des Betriebssystems, um die IP-Adresse des eingegebenen Domainnamens zu erhalten. Zu dieser IP-Adresse baut der Webbrowser eine TCP-Verbindung auf Port 80 auf, um anschließend einen „HTTP-Request“ an den Webserver zu senden. Der Webserver antwortet – falls keine Fehler aufgetreten sind – mit einer „HTTP-Response“ Nachricht, die das angeforderte Objekt enthält (vgl. [12]), siehe Abb. 3.

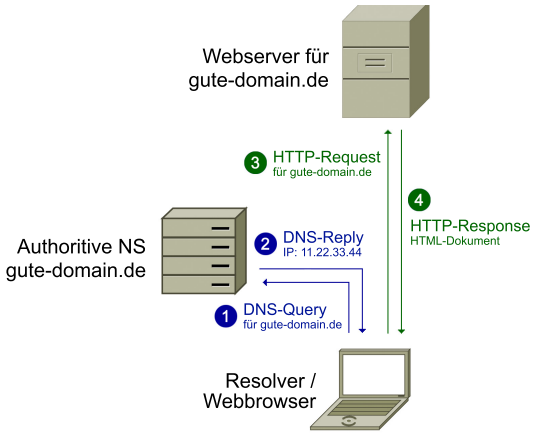

Abbildung 3: Vereinfachter Webseitenaufruf von einem gewöhnlichen Webserver (nach [15])

Würden Kriminelle solche „gewöhnlichen“ Webserver verwenden, könnten diese anhand ihrer IP-Adresse schnell gefunden und vom Netz getrennt werden. Das Fast-flux-Verfahren führt in den geschilderten Ablauf eine bzw. mehrere zusätzliche Schichten ein. Der „Resolver“ liefert auch hier eine IP-Adresse für den Domainnamen. Allerdings gehört diese IP-Adresse nicht zu einem Webserver, sondern zu einem Bot, der Teil eines Botnetzes ist. Der Webbrowser baut eine TCP-Verbindung auf Port 80 zu diesem Bot auf. Dieser nimmt die Anfrage entgegen und leitet sie an den zentralen Computer des Botnetzes weiter, das sog. „Mothership“. Das „Mothership“ sendet dann die angefragten Daten an den Bot, der sie wiederum an den Webbrowser weiterleitet (s. Abb. 4).

3.3.2 Ziel und Ablauf des Verfahrens

Ziel des „Fast-flux Botnet observation“-Verfahren ist – im Gegensatz zu „Proactive Domain Blacklising“ und „EXPOSURE“ – nicht das Finden unbekannter bzw. ungenutzter Schad-Domains, sondern die Untersuchung bestehender Botnetze, die Fast-flux Techniken verwenden. Dazu nutzt das Verfahren das „ATLAS“-System von Arbor Networks [3].

Dazu werden aus verschiedenen Quellen Domains gesam-

doi: 10.2313/NET-2011-07-2_11

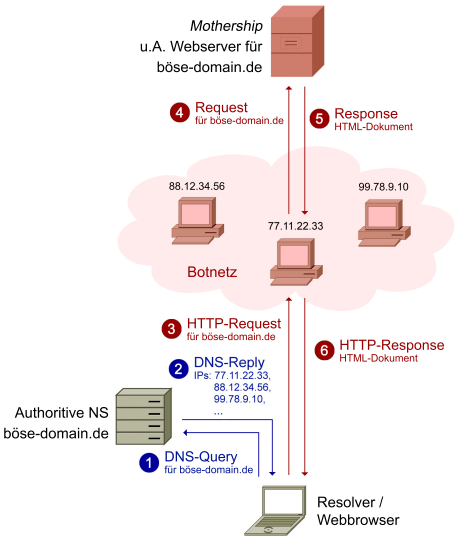

Abbildung 4: Vereinfachter Webseitenaufruf in (single) Fast-flux Botnet („single flux“) (nach [15])

melt, die bekanntermaßen zu bösartigen Zwecken verwendet werden. Zu diesen Quellen zählen Spam-E-Mails, Blacklists und die manuelle Analyse von Schad-Software.

Die gefundenen Domains werden anschließend einen „Quantifier“ übergeben, der anhand verschiedener Kriterien für jede Domain entscheidet, ob diese für Fast-flux Netzwerke verwendet wird oder nicht. Da viele reguläre Internet-Dienste eine Lastbalancierung auf DNS-Basis nutzen, besteht die Schwierigkeit darin, Fast-flux Domains, die für Botnetze verwendet werden, von regulären Domains zu unterscheiden, die eine gewöhnliche DNS-Lastbalancierung verwenden.

3.3.3 Verwendete Eigenschaften

Um zu entscheiden, ob eine Domain zu einem Fast-flux Netzwerk gehört, untersucht das „Fast-flux Botnet observation“-Verfahren u.a. die folgenden Eigenschaften. Hat eine Domain im A-RR einen TTL-Wert von weniger als 900 Sekunden, gilt dies als erstes Indiz dafür, dass es sich um eine Fast-flux Domain handelt. Für „gutartige“ Domains, die keine DNS-Lastbalancierung nutzen, wird ein TTL-Wert von einigen Tagen vorgeschlagen (vgl. [10]). Botnetze verwenden kurze TTL-Werte (nach [15] durchschnittlich 3 bis 10 Minuten) da die Erreichbarkeit einzelner Bots weder sichergestellt noch vorausbestimmt werden kann.

Im Weiteren werden die einzelnen IP-Adressen, die einer Domain zugeordnet sind, analysiert. Dazu gehört die Anzahl der IP-Adressen einer Domain (d.h. die Anzahl der A-RRs für eine Domain). Je mehr IP-Adressen für eine Domain gefunden werden, desto höher ist die Wahrscheinlichkeit, dass es sich um IP-Adressen aus einem Botnetz handelt. Zusätzlich wird der durchschnittliche „Abstand“ der IP-Adressen betrachtet, d.h. in welchen Adress-Bereichen die IP-Adressen liegen, und zu welchen „Autonomous Systems“ (ASs) sie gehören. Wenn reguläre Internet-Dienste Lastverteilung nutzen, werden die genutzten IP-Adressen i.d.R. im gleichen oder zumindest in benachbarten Netzen liegen und mit einer hohen Wahrscheinlichkeit nicht über viele verschiedene ASs im Internet verteilt sein. Die einzelnen Bots eines Botnetzes werden dagegen mit hoher Wahrscheinlichkeit weltweit verteilt sein, um eine hohe Verfügbarkeit des Botnetzes zu gewährleisten. Dies kann anhand der IP-Adress-Abstände und den „Autonomous System Numbers“ (ASNs) festgestellt werden.

Darüber hinaus werden auch einige Eigenschaften des bzw. der „authoritive“ NS untersucht. Sind mehr als drei solcher NS für eine Domain eingetragen, gilt dies als verdächtig. Werden mehrere NS verwendet, wird die Anzahl die ASNs der NS IP-Adressen gezählt. Sind die NS auf mehr als zwei ASs verteilt, gilt dies ebenfalls als verdächtig. Der „Abstand“ der IP-Adresse des NS zu den IP-Adressen der Domain wird ebenfalls betrachtet. Ein großer Abstand bedeutet, dass NS und Webserver in weit voneinander entfernten Netzen liegen, was ungewöhnlich ist.

4. VERGLEICH

Die vorgestellten Verfahren verwenden zur Klassifizierung der Domains verschiedene Eigenschaften von Domains bzw. deren Nameserver. Im folgenden sollen die Erfolgsraten und die genutzten Eigenschaften verglichen werden.

4.1 Erfolgsraten

Das „Proactive Domain Blacklisting“-Verfahren nutzt die Eigenschaften der verwendeten „authoritive“ Nameserver: die NS-Domainnamen, das Alter der NS-Domainnamen und ob der NS seinen Domainnamen selbst auflöst. Zusätzlich gehen in die Untersuchung der Zeitpunkt der Registrierung und der Registrar einer Domain ein.
Das Verfahren nutzt somit relativ wenig Informationen, kann aber dennoch registrierte und ungenutzte Schad-Domains finden, die zusammen mit bereits verwendeten „bösartigen“ Domains registriert bzw. verwaltet werden, sog. Cluster. Je nach Größe der Eingabe, d.h. wie viele „Seed Domains“ verwendet werden, werden unterschiedlich große Cluster gefunden. Bei 25 zufällig gewählten „Seed Domains“ wurden durchschnittlich 443 Schad-Domains gefunden, was einem Faktor von 17,7 entspricht. Die „true positive“-Rate liegt dann bei 74,1%, die „false positive“-Rate bei 1,3%. Wird eine größere Eingabemenge verwendet, nämlich alle 3.653 Domains in der Blacklist, die auf *.com* enden, so umfasst das Cluster 11.053 Einträge. Die „true positive“-Rate beträgt dann noch 73,7% und die „false positive“-Rate 6,6%. Die beste durchschnittliche „true positive“-Rate mit 81,4% erreichte das Verfahren bei einer Eingabegröße von 50. Dabei erreichte das Cluster eine durchschnittliche Größe von 649,7, was einem Faktor von 13,0 entspricht (vgl. [9]).

Das Verfahren hat jedoch zwei Nachteile: Zum einen benötigt es Ausgangsinformationen in Form von „Seed Domains“, die von Blacklists entnommen werden. D.h. es müssen bereits Domains zu bösartigen Zwecken verwendet (und erkannt) werden, bevor das Verfahren weitere Domains finden kann. Zum anderen ist eine Liste mit zu untersuchenden Domains nötig. Neben den Domains sollte auch deren NS-RRs und das Registrierungsdatum in der Liste enthalten sein. Je umfangreicher die zu untersuchende Liste, desto mehr potentielle Schad-Domains kann das Verfahren finden. In [9] wird die Verwendung der Zonen-Datei der *.com* TLD zum Testen des Verfahrens beschrieben. Dadurch können jedoch nur Schad-Domains gefunden werden, die auf *.com* enden. Die

doi: 10.2313/NET-2011-07-2_11

Nutzung weiterer Zonen-Dateien anderer TLDs ist prinzipiell möglich (und sinnvoll). Allerdings könnte der Zugriff auf die TLD Zonen-Dateien bestimmter Länder wie *.ru* eventuell schwierig sein (vgl. [9]), da hier die jeweiligen Registrare die Datei bereitstellen müssten.

„EXPOSURE“ analysiert live DNS-Verkehr und nutzt im Vergleich zum „Proactive Domain Blacklisting“ wesentlich mehr Domain-Eigenschaften zur Klassifizierung. Der Einsatz von „EXPOSURE“ erfolgte in zwei Phasen (siehe Abschnitt 3.2). Während des „offline Experiments“ erreichte das System eine Erkennungsrate von 98% mit einer „false positive“-Rate von 7,9%. In der „online Phase“ bei einem ISP wurden in einem Zeitraum von zwei Wochen 100 Millionen DNS-Anfragen analysiert. Dabei wurden 3.317 „bösartige“ Domains entdeckt, die dem System nicht aus den Trainingsdaten bekannt waren. Die „false positive“-Rate lag dabei bei 0% (vgl. [8]).
„EXPOSURE“ kann jedoch nur Schad-Domains finden, die nachgefragt, d.h. bereits von Botnetzen verwendet werden. Das Verfahren findet Schad-Domains mit verschiedenen TLDs, allerdings ist dazu der DNS-Verkehr zur Auswertung notwendig.

Da das Ziel des „Fast-flux Botnet observation“-Verfahrens nicht das Finden neuer, ungenutzter Schad-Domains ist, sondern die Analyse der Botnetze, die Fast-flux Techniken verwenden, lassen sich die Ergebnisse hier nicht direkt vergleichen. Als Datenquellen werden zwar u.a. Spam-E-Mails und Blacklists verwendet, allerdings dienen die dort gefundenen Domains nicht dazu, weitere Domains zu finden. Stattdessen wird versucht zu entscheiden, ob eine solche Domain eine Fast-flux Domain darstellt. Dazu werden verschiedene Eigenschaften der Domain bzw. der zugehörigen IP-Adressen untersucht (siehe Abschnitt 3.3.3) und die Domain entsprechend bewertet. Allerdings legt [6] keine Zahlen über den Erfolg dieser Maßnahmen offen.

4.2 Verwendete Eigenschaften

Wie schon festgestellt, nutzt das „Proactive Domain Blacklisting“ Eigenschaften der „authoritive“ Nameserver. Es wird eine Liste der NS erstellt, die bereits einmal eine Schad-Domain aufgelöst haben. Dann wird das Alter dieser Nameserver bzw. deren Domainnamen betrachtet. Zur Untersuchung werden nur die Nameserver herangezogen, die jünger als ein Jahr sind. Außerdem wird die Liste dieser „bösartigen“ Nameserver auf diejenigen verkleinert, die ihren Domainnamen selbst auflösen.
Neben diesen Nameserver-Eigenschaften werden der Registrar und das Registrierungsdatum der Domains selbst in die Untersuchung aufgenommen. Alle genannten Eigenschaften werden von den beiden anderen vorgestellten Verfahren nicht verwendet.

„EXPOSURE“ nutzt insgesamt 15 Eigenschaften. Einige davon sind Zeit-basiert und können nur über eine Beobachtung des DNS-Verkehrs festgestellt werden, z.B. ob eine Domain ausschließlich innerhalb eines kurzen Zeitraumes nachgefragt wurde. Weitere Eigenschaften basieren auf der Auswertung der DNS-Antworten, beispielsweise wie viele IP-Adressen einer Domain zugeordnet sind und in welchen Ländern diese IP-Adressen liegen. Darüber hinaus wird der TTL-Wert der A-RRs näher untersucht, beispielsweise wie lange ein A-RR durchschnittlich gültig ist. Abschließend werden zwei Eigenschaften untersucht, die sich auf den Domainnamen selbst beziehen, nämlich der Anteil der enthaltenen Ziffern und der Anteil des längsten enthaltenen „meaningful substring“.

Um zu entscheiden, ob eine Domain zu einem Fast-flux Netzwerk gehört, untersucht das „Fast-flux Botnet observation“-Verfahren neun Eigenschaften von Domains. Ebenso wie in „EXPOSURE“ wird die Anzahl der IP-Adressen für eine Domain sowie der TTL-Wert der A-RRs betrachtet. Die weiteren sieben Eigenschaften wie IP-Adressabstände, Anzahl von ASNs oder Anzahl der *authoritive* Nameserver usw. (siehe Abschnitt 3.3) werden von den anderen Verfahren nicht verwendet.

5. ZUSAMMENFASSUNG

Die vorgestellten Verfahren „EXPOSURE“, „Proactive Domain Blacklisting“ und „Fast-flux Botnet observation“ verfolgen das Ziel, „bösartige“ Domains zu erkennen, d.h. Domains, die zu kriminellen oder illegalen Zwecken von bzw. in Botnetzen verwendet werden. Alle drei erreichen dieses Ziel mit verschiedenen Ansätzen.

„EXPOSURE“ und „Proactive Domain Blacklisting“ versuchen „bösartige“ Domains zu finden, die bereits registriert aber noch nicht als „bösartig“ aufgefallen sind. D.h. die Domains wurden noch nicht auf eine Blacklist gesetzt oder gesperrt. Während „EXPOSURE“ versucht, derartige Domains bei deren Nutzung im live DNS-Verkehr zu erkennen, geht „Proactive Domain Blacklisting“ einen Schritt weiter und versucht anhand bekannter Schad-Domains weitere Domains zu finden, die bisher noch nicht für kriminelle Zwecke verwendet wurden, deren Einsatz zu solchen Zwecken aber absehbar ist.

„Fast-flux Botnet observation“ verfolgt hingegen nicht das Ziel, unbekannte Schad-Domains zu finden. Stattdessen werden Domains aus verschiedenen Datenquellen untersucht, um festzustellen, ob es sich dabei um Fast-flux Domains handelt. Das Ziel ist das Finden von Fast-flux Domains sowie die Untersuchung der zugehörigen Botnetze.

Alle drei Verfahren nutzen bestimmte Eigenschaften der untersuchten Domains bzw. deren *authoritive* Nameserver. Trotz des einheitlichen Ziels – das Erkennen „bösartiger“ Domains – nutzen die Verfahren weitgehend verschiedene Eigenschaften. Lediglich der TTL-Wert der A-RRs sowie die Anzahl der IP-Adressen für eine Domain wird sowohl von „EXPOSURE“ als auch vom „Fast-flux Botnet observation“-Verfahren verwendet.

6. LITERATUR

[1] Abu Rajab, Moheeb and Zarfoss, Jay and Monrose, Fabian, Terzis, Andreas. A multifaceted approach to understanding the botnet phenomenon. In *Proceedings of the 6th ACM SIGCOMM conference on Internet measurement*, IMC '06, pages 41–52, New York, NY, USA, 2006. ACM.

[2] Alexa. Top Sites. http://www.alexa.com/topsites. Letzter Zugriff: 28.04.2011.

[3] Arbor Networks. ATLAS. http://atlas.arbor.net. Letzter Zugriff: 28.04.2011.

doi: 10.2313/NET-2011-07-2_11

[4] Christian Kreibich, Chris Kanich, Kirill Levchenko, Brandon Enright, Geoffrey M. Voelker, Vern Paxson und Stefan Savage. Spamcraft: an inside look at spam campaign orchestration. In *Proceedings of the 2nd USENIX conference on Large-scale exploits and emergent threats: botnets, spyware, worms, and more*, LEET'09, pages 4–4, Berkeley, CA, USA, 2009. USENIX Association.

[5] Internet System Consortium. Security Information Exchange (SIE) Portal. https://sie.isc.org/. Letzter Zugriff: 28.04.2011.

[6] Jose Nazario und Thorsten Holz. As the net churns: Fast-flux botnet observations. In *3rd International Conference on Malicious and Unwanted Software*, pages 24–31, September 2008.

[7] L. Daigle. WHOIS Protocol Specification. RFC 3912, IETF, September 2004.

[8] Leyla Bilge, Engin Kirda, Christopher Kruegel und Marco Balduzzi. EXPOSURE: Finding Malicious Domains Using Passive DNS Analysis. In *18th Annual Network and Distributed System Security Symposium*, San Diego, Februar 2011.

[9] Mark Felegyhazi, Christian Kreibich und Vern Paxson. On the potential of proactive domain blacklisting. In *Proceedings of the 3rd USENIX conference on Large-scale exploits and emergent threats: botnets, spyware, worms, and more*, LEET'10, Berkeley, CA, USA, April 2010.

[10] P. Mockapetris. DOMAIN NAMES - CONCEPTS AND FACILITIES. RFC 1034, IETF, November 1987.

[11] Paul Albitz und Cricket Liu. *DNS und BIND*. O'Reilly, Köln, 1997. Deutsche Ausgabe der 2. Auflage, ISBN 3-930673-54-1.

[12] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, T. Berners-Lee. Hypertext Transfer Protocol – HTTP/1.1. RFC 2616, IETF, Juni 1999.

[13] Sandeep Yadav, Ashwath K. K. Reddy, A.L. Narasimha Reddy, Supranamaya Ranjan. Detecting algorithmically generated malicious domain names. In *Proceedings of the 10th annual conference on Internet measurement*, IMC '10, pages 48–61, New York, NY, USA, 2010. ACM.

[14] T. Brisco. DNS Support for Load Balancing. RFC 1794, IETF, April 1995.

[15] The Honeynet Project & Research Alliance. Know Your Enemy: Fast-Flux Service Networks. http://www.honeynet.org/book/export/html/130, Juli 2007. Letzter Zugriff: 28.04.2011.

doi: 10.2313/NET-2011-07-2_11