Schotten dicht

DNSpionage: Massive Angriffe auf Mail- und VPN-User

In einer weltumspannenden Operation haben Unbekannte etliche Firmen und Regierungsstellen im Nahen Osten angegriffen. Dafür haben sie unter anderem die DNS-Infrastruktur einer deutschen Firma missbraucht. Die ICANN will nun Domainbetreiber auf breiter Front wachrütteln und fordert den Einsatz der Sicherheitstechnik DNSSEC.

Von Dušan Živadinović und Monika Ermert

Die Internet Corporation for Assigned Names and Numbers (ICANN) fordert Domainverwalter (Registries und Registrare) sowie Betreiber von DNS-Resolvern dringend dazu auf, weltweit alle Domains mit der Sicherheitstechnik DNSSEC zu signieren und DNS-Antworten zu validieren. Validierende DNS-Resolver wie Stubby, die es für Linux, Windows und macOS gibt [1], stellen sicher, dass signierte DNS-Antworten (DNS-Replies) unverfälscht sind und von einer vertrauenswürdigen Quelle stammen.

Die Netzverwaltung reagiert mit ihrem Aufruf auf die als DNSpionage bezeichneten massiven Attacken auf Mail- und VPN-Server von Unternehmen und Behörden im Nahen Osten sowie auf die DNS-Infrastruktur von Firmen in den USA, Deutschland und Schweden.

Nach Ansicht von Microsoft und der Security-Firma CrowdStrike erfolgen die Attacken bereits seit mindestens Februar 2017. Die Angreifer, die Sicherheitsfirmen im Iran vermuten, haben dabei IP-Verkehr von zahlreichen Nutzern auf ihre eigenen, unter falscher Flagge segelnden Server umgelenkt (Domain-Hijacking).

Betroffen waren bisher diverse Server von mehr als 50 Institutionen und Firmen in zwölf Ländern (Albanien, Ägypten, Deutschland, Irak, Jordanien, Kuwait, Libanon, Libyen, Saudi-Arabien, Schweden, Vereinigte Arabische Emirate und USA). Microsoft zufolge könnten sogar 200 Ziele attackiert worden sein.

Unter falscher Flagge

Einzelheiten drangen bisher nur spärlich an die Öffentlichkeit. Den Ablauf der Attacken kann man aber grob in sechs Schritte unterteilen.

Im ersten Schritt verschaffen sich die Angreifer Zugang zu DNS-Servern, etwa über Phishing-Attacken auf Administratoren. Voraussetzung ist, dass die DNS-Server ohne DNSSEC-Schutz arbeiten. Dann biegen sie im zweiten Schritt DNS-Einträge beispielsweise von Mailservern um: Dabei ersetzen Sie auf dem für eine Domain zuständigen DNS-Server die korrekte IP-Adresse mit der Adresse eines eigenen, präparierten Servers. Im dritten Schritt lassen sie sich für den präparierten Server gültige Zertifikate etwa von Comodo oder Lets Encrypt für die entführte Domain ausstellen.

Schritt vier (Man-in-the-Middle-Attacke): Clients, die das DNS nach der IP-Adresse ihres Mailservers befragen, erhalten vom manipulierten DNS-Server die falsche IP-Adresse und steuern diese an. Dort nimmt ihre TLS-Verbindung ein transparenter Proxy der Angreifer mit korrektem TLS-Zertifikat auf.

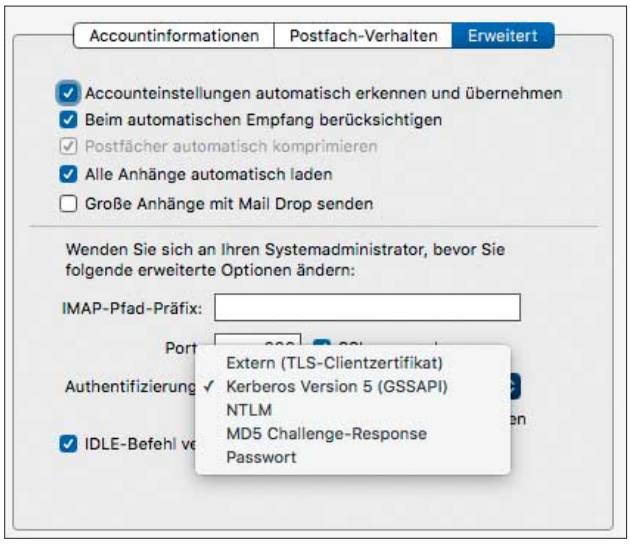
Schritt fünf: Der Proxy entschlüsselt die Verbindungen, schreibt die Zugangsdaten mit und reicht die Verbindungen an einen ebenfalls auf dem präparierten Server laufenden Loadbalancer weiter.

Schritt sechs: Der Loadbalancer meldet sich anstelle der Clients beim tatsächlichen Mailserver an und reicht die Antworten des Mailservers zurück an die Clients. Für die Clients sieht alles normal aus, sie können Mails abrufen und versenden. Die Umleitungen bleiben nur stundenweise aktiv, um möglichst keinen Verdacht zu erregen.

Angriff über Bande

Eine derartige Attacke startete Anfang Dezember 2018 und lief bis Januar 2019. Dabei haben die Spione zunächst Zugangsdaten des deutschen Registrars Key-Systems erbeutet und so Zugriff auf dessen EPP-Interface erhalten. Das EPP-Interface (Extensible Provisioning Protocol) nutzen Domain-Registrare, um Domain-Änderungen im weltweiten DNS einzurichten, also etwa Domain-Transfers.

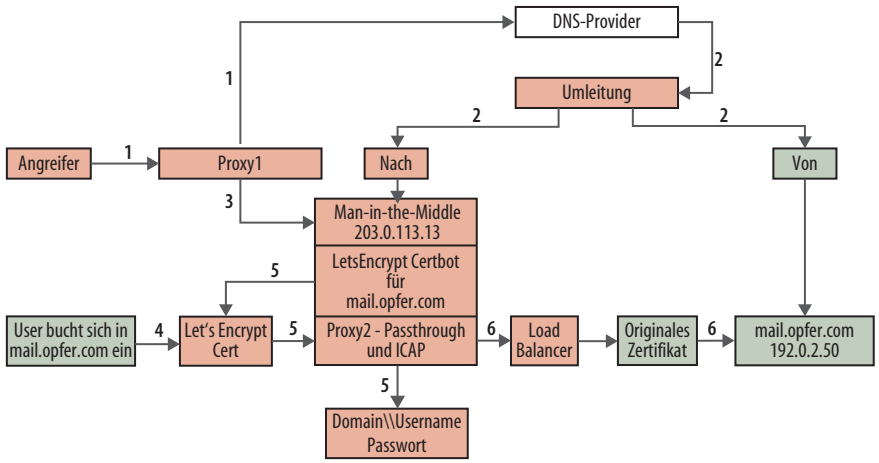
Key-Systems ist ein Dienstleister der US-amerikanischen Organisation Packet Clearing House (PCH), die unter anderem



Die Klartext-Authentifizierung ist bei Mail-Clients üblich. Im Firmenumfeld könnte man stattdessen aufwendige Verfahren wie Kerberos verwenden.

HTTPS genügt nicht

Weil Angreifer für beliebige IP-Adressen gültige Zertifikate erhalten können, lassen sich Clients in die Irre führen.



DNS-Dienste für weltweit mehr als 500 Top-Level-Domains betreibt (TLDs) – darunter auch für diverse TLDs von Ländern im Nahen Osten.

Phishing gegen Admins

Wie die EPP-Zugangsdaten den Angreifern in die Hände fielen, ist offen. Key-Systems nannte dazu auf Nachfrage von c't keine Details, bestätigte den Vorgang aber grundsätzlich. Möglicherweise infizierten die Angreifer den PC eines Registrar-Mitarbeiters mit einem von Ciscos Forschungsabteilung Talos beschriebenen Spionagewerkzeug. Talos-Mitarbeiter haben diesen Vorgang für andere Ziele derselben Angreifer detailliert dokumentiert (siehe ct.de/y589).

Dafür verstecken sie das Spionage-Tool in Office-Dokumenten, die sie über präparierte Webserver verteilen. Ein solcher Server enthielt eine vermeintliche Jobbörse. Beim Spionagewerkzeug handelt es sich um ein Fernadministrations-Tool, das mit der Angreifer-Infrastruktur über DNS-Tunnel kommuniziert – daher der Name DNSpionage.

Den EPP-Zugang nutzten die Angreifer, um einige Domains der schwedischen Firma Netnod zu kapern und den dafür bestimmten IP-Verkehr auf einen eigenen Server umzuleiten. Das gelang mit Netnod-Domains, die nicht per DNSSEC abgesichert waren. Die Umleitung blieb wiederum nur kurz aktiv.

Das genügte aber, um Zugangsdaten von Netnod-Admins zu erbeuten und so Zutritt zur DNS-Verwaltung von Netnod zu erlangen. In dieser Situation hilft natürlich weder DNSSEC noch irgendeine andere Sicherheitstechnik. Entsprechend konnte die Spionage-Truppe das für sie hinderliche DNSSEC auf anderen Netnod-Domains nach Bedarf stundenweise abschalten. So führten sie Domain-Hijacking-Attacken auf die US-Registry PCH aus und darüber auf Institutionen und Firmen von Ländern im Nahen Osten.

Aufgeflogen waren die Spione wegen eines Patzers: Als sie internen Mailverkehr von Netnod umleiten wollten, vergaßen sie, DNSSEC vorher abzuschalten. Deshalb scheiterte die Umleitung, denn Netnod setzt für seine Mitarbeiter validierende Resolver ein, welche die gefälschte Ziel-Adresse nicht weitergaben. So scheiterte der Mailabruf und bei der Ursachenforschung stießen Spezialisten schließlich auf das Domain-Hijacking im eigenen Haus.

Auffälligkeiten

Auffällig ist, dass die Umleitungen immer nur kurz in Betrieb waren. Clients, die validierende Resolver vor solchen Umleitungen bewahrten, konnten dann zwar keine Mails abrufen, aber weil danach alles wieder normal lief, schöpfte niemand Verdacht. Vor allem bei großen Servern genügt eine Stunde, um viele Zugangsdaten abzusaugen, weil etwa Smartphones das Postfach automatisch in kurzen Abständen öffnen.

Das ist für die Attacke auf zwei Mitarbeiter von PCH dokumentiert. Ihre Smartphones waren in Hotspots eingebucht, die ihnen den Zugriff auf den validierenden DNS-Resolver von PCH verwehrten. Deshalb mussten sie den Resolver des Hotspot-Anbieters nutzen.

Als sie diesen nach der IP-Adresse des Firmen-Mailservers befragten, gab er ihnen die im DNS untergeschobene IP-Adresse ohne Prüfung weiter. Da auch die Smartphones die DNS-Antworten nicht prüften, meldeten sich ihre Mail-Clients beim Man-in-the-Middle-Server an und gaben dort ihre Zugangsdaten preis. Die übrige PCH-Belegschaft war hingegen vom hauseigenen validierenden DNS-Resolver geschützt. Er erkannte die gefälschte IP-Adresse und gab sie nicht weiter.

Gegenmaßnahmen

Dass Spione Zugangsdaten von Mail-Usern in so großem Maßstab abfischen konnten, liegt sicherlich nicht allein daran, dass noch viele Domains unsigniert sind. Aber in allen hier beschriebenen Fällen dienten solche Domains als Hebel. Der nicht-validierende DNS-Resolver im Hotel-Hotspot tat sein Übriges. In Deutschland nutzen immerhin rund 50 Prozent der User validierende Resolver. Auch Smartphones kann man mit solchen Resolvern nachrüsten, beispielsweise mit DNSCloak für iOS und DNSCrypt-Proxy für Android (siehe ct.de/y589).

Die ICANN und DNS-Experten weltweit fordern, DNSSEC auf möglichst breiter Front einzusetzen. Auch hat die ICANN allen neuen Top-Level-Domains das Signieren vertraglich auferlegt. Mehrere nationale Registries fördern das Signieren privater Domains, beispielsweise durch kostenlose DNSSEC-Angebote.

Domaininhaber sollten zusätzlich den „Registry Lock“ nutzen, der Änderungen der DNS-Daten durch Dritte unterbindet. Administratoren sollten Logs von DNS-Servern durchgehend im Auge behalten und dazu etwa Monitoring-Tools nutzen, die bei Auffälligkeiten Alarm schlagen. Mit dem Dienst whatsmydns.net lässt sich anhand von 18 weltweit verteilten Resolvern schnell prüfen, ob diese eine Domain zur richtigen IP-Adresse auflösen.

(dz@ct.de) c't

Literatur

[1] Carsten Strotmann, Auskunft abgedichtet, So schützt DNS-Kommunikation Ihre Privatsphäre, c't 2/2019, S. 184

Infos zu DNSpionage, validierende Resolver: ***ct.de/y589***