Vorwort

Über das Automation Science

Was ist das Automation Science™ eigentlich? Nun, dieses kleine Format hieß früher einmal „Automation für Arme“ und entstand eher aus einer Laune und Interesse heraus…

Viele Gespräche die ich mit Kunden oder Kollegen besprochen habe, zeigten mir, dass es für viele Informationen kein eigenes Bild (im Kopf) der Menschen gibt, auf das direkt Bezug genommen wird. Oft wurde ich zu Einzelheiten befragt, die viele einfach nicht verstehen oder die Vorstellung fehlte. Auch hielt sich bei vielen meiner Kollegen mit Fachausbildung, dass Wissen - in den Tiefen des Verstehens - dann doch eher begrenzt. Es kann sich nun einmal nicht Jeder mit allem befassen - oder? Nun genau ab da fing es an, denn daran wollte ich etwas ändern und habe mich auf die Themen bezogen, die gerade vor kurzen aktuell waren. Und so entstand eine Vielzahl von unterschiedlichen Bereiche (Software Hacking, Viren- und Trojaner-ReEngineering, Hardware Tipps, Beispiele für Automaten und einiges andere) die ich etwas spielerisch *umschrob*, aber immer mit Fokus, auf eine einfache Erklärung, wie Bebilderung.

Seit 2018 schreibe ich jedoch an Dokumentationen, Anleitungen und des öfteren habe ich Anfragen von Agenturen, Zeitschriften und Co gehabt. Es ist jedoch etwas anderes für ein Blatt zu schreiben, als locker für einen selber. Weshalb ich auf diese Angebote bis jetzt nicht zurück kam. Dies liegt schon alleine daran, dass ich nicht des Schreibens-willen, sondern aus philosophisch-technischer Bestrebung versuche die Zusammenhänge zu erklären. Weshalb ich mich 2019 dafür entschlossen habe, meine Arbeiten im Hintergrund auch mehr zu benennen und das Format (hier) nun Automation Science *(kurz: ASCi)* nenne.

Dies geht nicht zuletzt auf meine Arbeiten als Speaker und Philosoph zurück und wie ich selber gerne zu sagen pflege: „Ein guter Philosoph, fängt immer beim Wort an“ - und da geht es auch schon los. Das ein Wort wie *Qualität* heute so sehr gedehnt, von den Meisten (manchmal absichtlich) falsch verstanden und gleichzeitig auch missbraucht wird - hätte sich selbst Aristoteles, nie zu träumen gewagt.

Motivation

Eben so beiläufig wie ausgibt, nutzen wir gerne ein Wort wie *Automation*, jedoch ohne uns bewusst zu machen, unter welchen Aspekten es im Eigenen (Sinne) zu nutzen sei. Wie in allen Sprachgebräuchen geht Sinnhaftigkeit, mit ihrer Häufigkeit und Anwendung, erst verloren. Wann immer eine unzureichend verstandene Maßlosigkeit wie: „das geht ganz *automatisch*“, durch Ihre Verwendung also verloren geht, braucht es einer neuen Idee. Sie besteht meist nicht den Verstand eines neuen Maße oder um neues zu predigen; sondern das Bestehende, besser verstehen zu lernen. Und so sehe ich es als eine wichtige Aufgabe an, verstehen und das Dahinter, wieder mehr in den Fokus zu setzen und das Denken zu schärfen.

Publikation

Ich habe beschlossen dieses Format (*ASCi - Automation Science)* ab der heutigen Ausgabe, nicht mehr vorrangig für Firmen-Kollegen und -Kolleginnen bereit zu stellen, sondern über einen öffentliche Publikationsform (Feed & Website) bereit zu stellen. Dies erleichtert die Weitergabe, verkürzt zu gleich die eMail Fluten und ermöglicht es mir auch, auf anderen Wegen ein Feedback zu den bereitgestellten Themen einzuholen. Durch einige Planänderungen meines Sabbatical, werde ich bis Ende August 2019 noch an den Vorbereitungen von ASCi und deren Magazinseite arbeiten.

Ab da an werden alle Beiträge erst einmal über LAoP (meine online Akademie der Philosophie) als öffentlicher Download bereitgestellt. Die gezielte Magazinseite von dort aus alle Beiträge und der Feed geladen werden können, wird es dann aber erst Anfang 2020 geben.

Mit freundlichen Grüßen

Michael Kaufmann

Für mehr Sicherheit durch Two-Factor-Authentication

Doch wie sicher ist die Methode wirklich bei Angriffen durch Man-in-the-Middle oder Phishing?

Ich habe mich dafür entschieden dies einmal zu testen und habe dafür ein in einem Live-Szenario ein Hacking Framework in Anwendung gebracht. Da dies keine Anleitung als Selbstversuch darstellt, gehe ich nur auf das eigentliche Vorgehen ein, nicht auf die direkt verwendeten Tools, Umgebungen oder Benutzeraccounts. Dabei ziele ich auch weniger auf das Verfahren, als die Anwendung ab, die ich kurz beschreibe um einen solchen Angriff durchzuführen.

DISCLAIMER

Ich weis darauf hin, dass dieses Dokument (AfA002) keine Anleitung zum Selbstversuch darstellt! Es ist verboten, fremde Accounts und Tools in den Einsatz zu bringen oder diese ungefragt zu verwenden, um Identitäten, Zugänge fremder oder Nutzsysteme ohne Einverständnis der Nutzer und-, oder derer Besitzer selbst; anzugreifen, zu übernehmen oder zu Gunsten weiterer Delikte oder Straftaten zu verwenden. Dieses Dokument dient allein der Verdeutlichung und Aufklärung. Das Einsetzen von Hacker-Tools an sich, ist in Deutschland unter Strafe gestellt. Weiteres regelt das StGB: § 149, § 202, § 202a, § 202b, § 202c, $ 206

Damit soll auch klar werden, wie am schnellsten auf Daten-Fremder zugegriffen werden kann. Auch möchte ich damit zeigen, dass auch nicht all-zu-technisch versierte Menschen, ein solches Angriffsszenario durchführen können. Bei zeige ich auch, das mir die 2FA egal sein kann, um an Kontodaten und mehr zu kommen oder einen Social Account zu übernehmen.

Wie umsichtig die meisten mit Ihren eigenen Zugangsdaten umgehen und wie wenig sicher sie letztlich sind, zeigen auch die zuletzt in den Medien aufgegriffenen Geschehnisse.

So wurden ca. 2,2 Milliarden Zugangsdaten (lauf dem Plattner Institut) von NutzerInnen in fünf darauf folgenden *Collections* gestohlen. Ob es sich nun um das absichtliche stehlen von Privatdaten im großen Stiel - wie etwas bei Equifax handelt - oder um Massen-Doxxing, bei dem es um das unerkannte eindringen in Systeme und das reine sammeln von Privatdaten geht. Die Angriffe und deren Szenarien sind stets die selben.

Schon lange geht es nicht mehr um das besitzen von eigentlich tiefen Kenntnissen von Computersystemen. Wie auch beim Promi-Doxxer *0rbit* zuletzt zeigte, ist ein tiefes Fachwissen nur von Nöten, wenn eigene Software und Strategien erarbeitet werden sollen. Da Cracker schon sehr früh damit anfingen Werkzeuge für erkannte Angriffe zu entwickeln, braucht es heute kaum noch höheres Wissen, um Szenerien eines Angriffes voll automatisiert auszuführen.

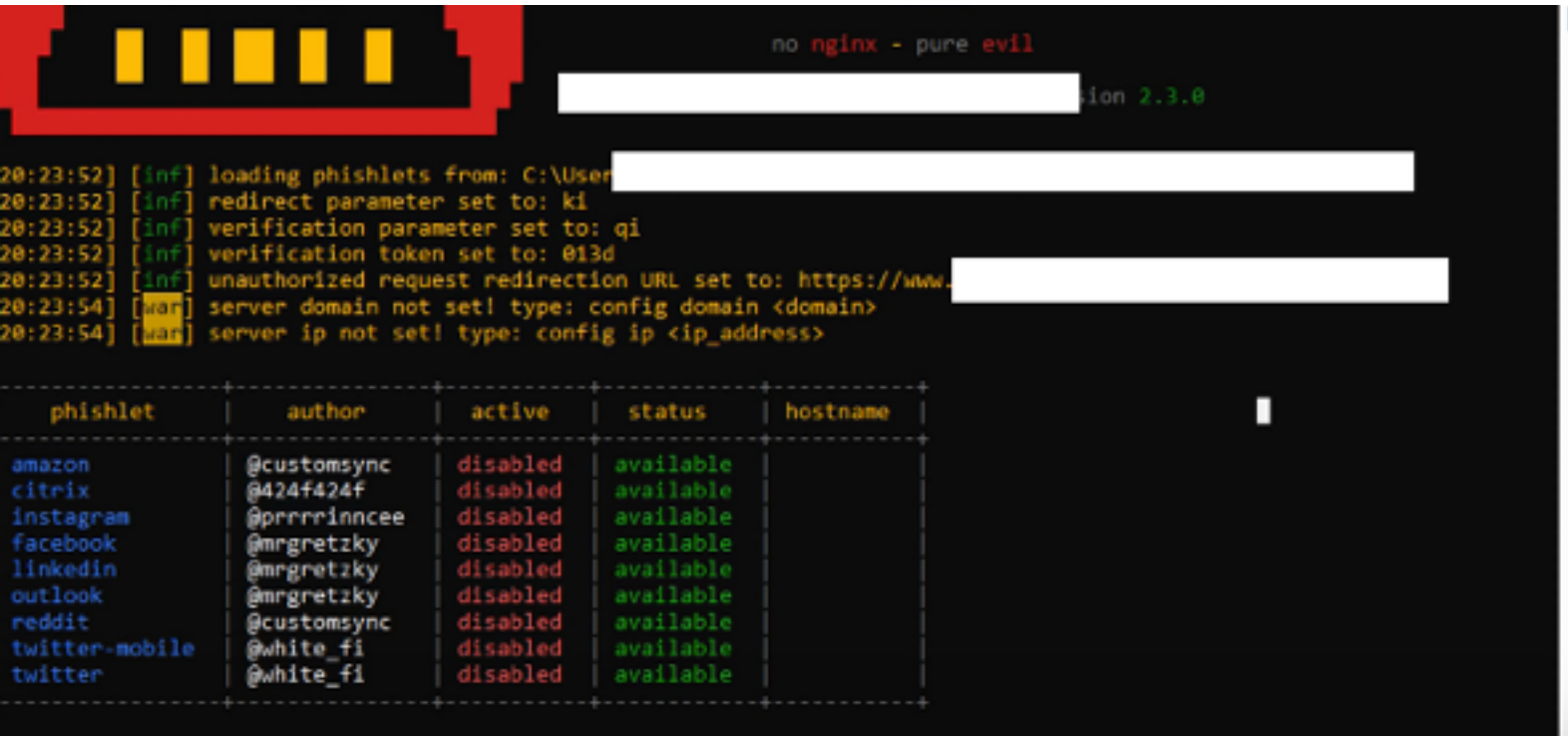
Schauen wir uns daher in Folge eine Szenario an, bei dem ich mit Erfolg versucht habe, einen direkten Zugriff auf ein Soziales Netzwerk zu bekommen.

Aufbau und Funktionsweisen

Die Methoden der meisten Angreifer-Tools sind Attacken, wie die, die durch Man-in-the-middle durchgeführt werden. Das es viele solche Szenarien gibt solch eine Prozedur durchzuführen, sind diese Toole meist auch erweiterbar. Heißt, sie sind durch zusätzlichen Code ausbaufähig.

Diese werden daher auch als Hacking- oder Crack-Framework bezeichnet. Sie können ebenfalls, bestehende Tools einbinden um sie nacheinander oder gleichzeitig ansteuern zu können.

Das von mir in diesem Zusammenhang genutzte Hacker-Framework, hat schon einiges an Szenarien installiert. So benötige ich für einen einfachen Angriff, keine großen Erweiterungen und auch *eigentlich* kein Know-how, um einen Angriff auszuführen.



Screenshot mit Angriffsvektoren. Angaben der Umgebung und weitere Informationen wurden ausgeblendet

Die jeweilig nutzbaren Angriffsvektoren werden hier als **phishlet** (=phishing; abgreifen von Daten) bezeichnet. Diese lassen sich für gezielte Angriffe (zum Beispiel um Servern oder spezielle Software angreifen zu können) erweitern.

Allgemeines

Um einen Angriff ausführen zu können, benötige ich nun einen Server der möglichst direkt im Internet angesprochen werden kann, auf dem sich dann mein Opfer am Ende anmeldet. Dies kann auf unterschiedlichste Weise funktionieren. Zum Beispiel über einen Schadcode (Java-Script, Flash) in Add Werbung oder Bannern auf Web-Seiten. Auch bestehende Codebausteine zu Benutzerbezogene Aufzeichnung (speichern von Aufrufen usw.) auf Websites, die sich hier hervorragend ausnutzen und umbiegen lassen.

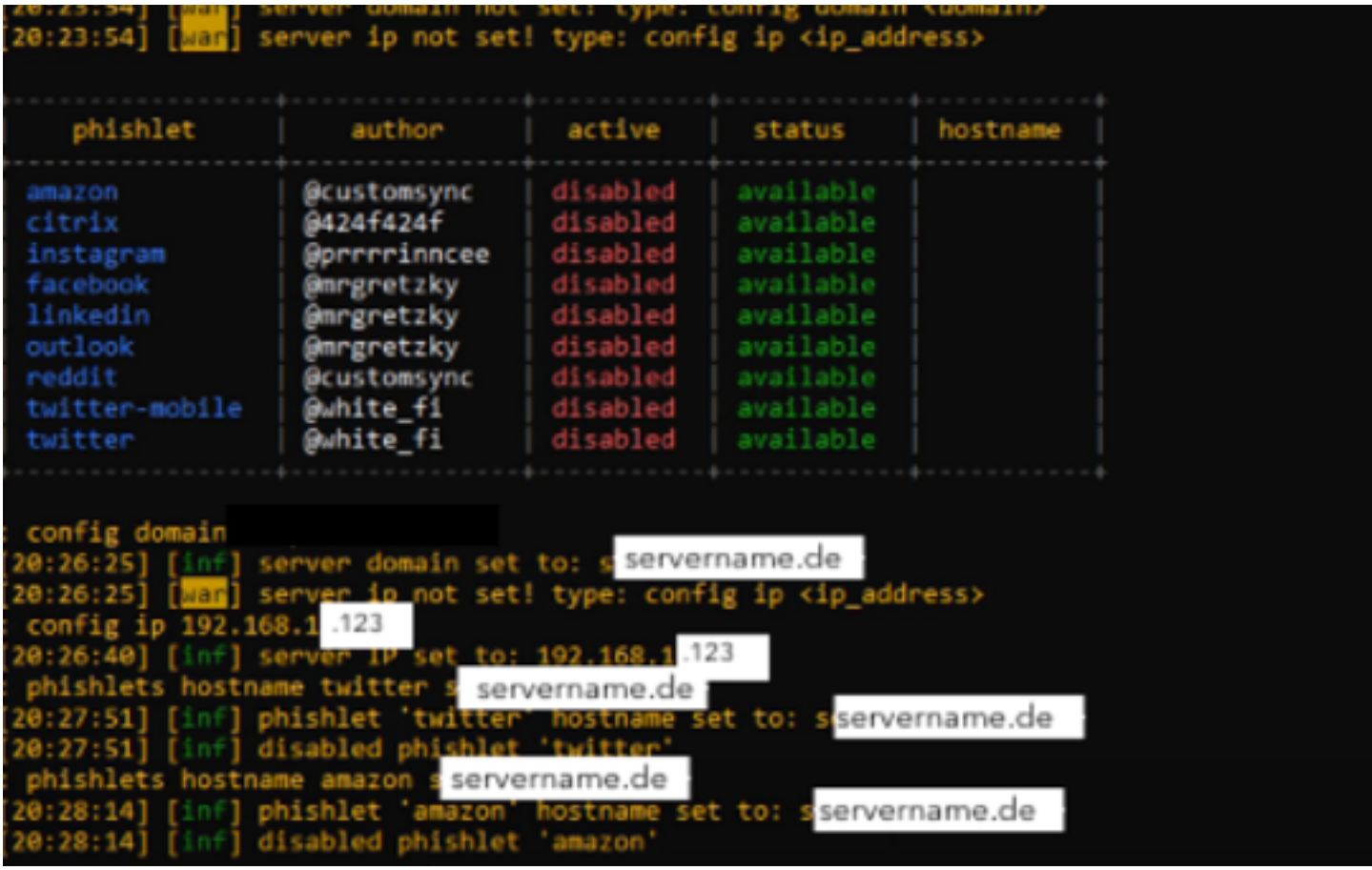
In meinem Beispiel möchte ich einen Angriff per E-Mail durchführen, bei dem das Opfer auf eine Link klickt. Dieser führt zu einem von mir (meist gekaperten) Server. Dieser leitet wiederum zu vielen anderen Servern weiter, zu dem am Ende ein Server mit einer F3ZZ Domain steckt. Das Opfer bemerkt dabei nicht, dass es auf einer fremden Website landet, als der, auf die sich gehen wollte.

F3ZZ bedeutet in Übrigen, dass ein Zeichen einer anderen Sprache, innerhalb einer Domain auftaucht und dort absichtlich versteckt wurde. So lassen sich viele Domains fälschen. Mit einem freien SSL Zertifikat, wird die Website dann sogar HTTPS verschlüsselt und sieht sicher für das Opfer aus.

Los geht es

Als erstes lasse ich mal eine Verbindung zu meinen Rechnern über die IP (der Hintergrund der Datenübermittlung ist Verschlüsselt und wird über mehrere Proxies ins Ausland weitergeleitet) herstellen.

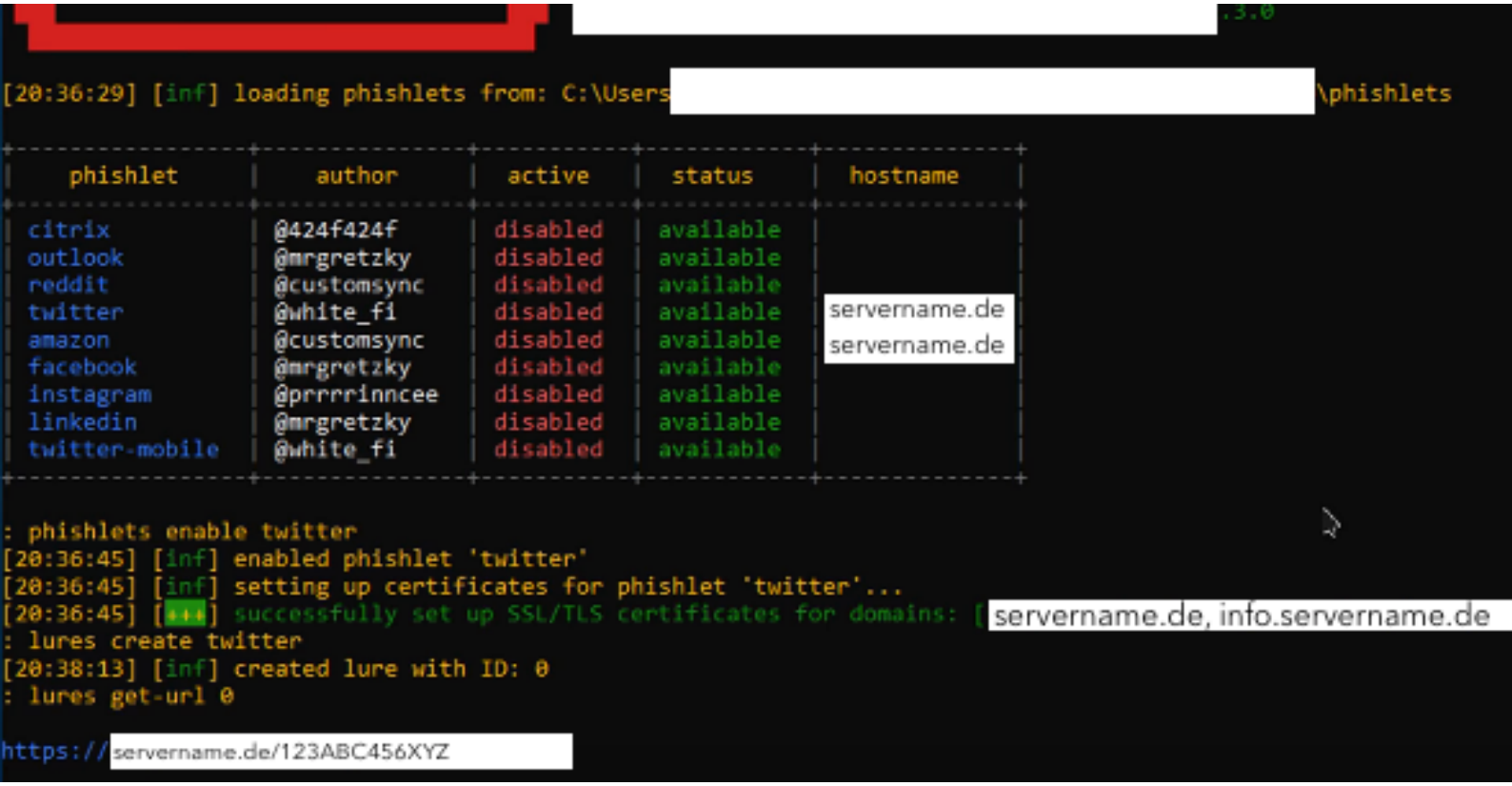
Dann benötige ich natürlich noch die Domain meines *gehackten* Servers, über die das Opfer gelangen soll.



INFOS

Die hier eingetragen Domain und eigene IP-Adress ist beispielhaft verwendet und wurden rein aus Dokumentationsgründen überschrieben. Die Domain wurde in diesen Szenario nicht verwendet noch angegriffen!

Sind die *phishlets* eingetragen und der Server aktiviert, werden die verwendeten Attacken nun auch in der Tabelle angezeigt.



Ich möchte nun einen Attacke ausführbar machen und starte das phishlet *twitter.* Um zusätzlich als Man-in-the-middle zu agieren, wird zusätzlich meine Verbindung zum Server noch einmal über ein SSL/TLS Zertifikat abgesichert und verschlüsselt.

Nach dem nun das Framework die Session aufgebaut hat, lasse ich mit eine Schlüssel-URL erzeugen, die ich später in einer E-Mail einbauen kann, um mein Opfer dazu zu bringen, diese URL anzuklicken.

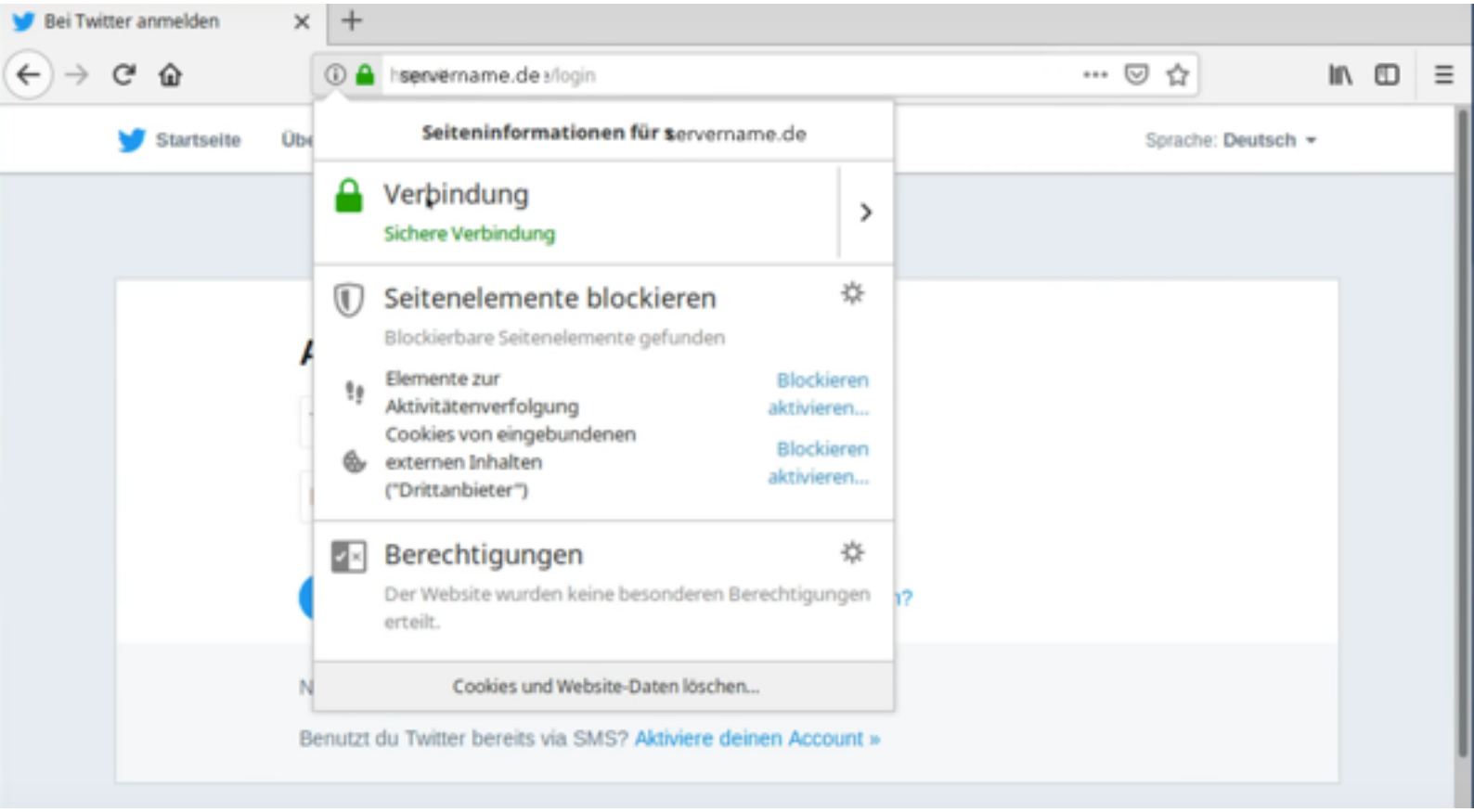
Hier als Beispiel Schlüssel-URL als https://servername.de/123ABC456XYZ angegeben.

Phishing me

Das Prinzip von phishing Mails hat sich seit her eigentlich kaum verändert. Wir können die URL natürlich auch sehr weit treiben und sie in Artikeln verstehen uns sonst etwas. Natürlich könnten wir sie auch bei Gewinnspielen oder Ade-Werbeanzeigen unterbringen. Denn tatsächlich werden diese Angaben von den Werbebetreibern der Server nicht überprüft.

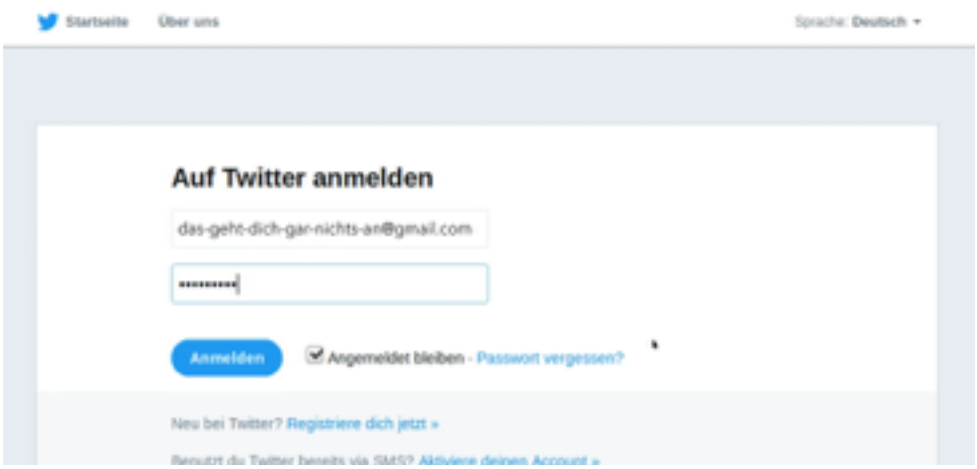
Kommen wir aber zurück zu unseren Angriff…

Ich spiele nun das Opfer und klicken auf den Link in der FakeMail. Nach dem Aufrufen werden wir überrascht sein, denn auch die Verschlüsselung sieht richtig aus.



Einzig und allein unsere Domain würde uns verraten. Dies liegt aber daran, dass wir uns eben keine F3ZZ Domain zugelegt haben.

Ist dem Opfer nichts weiter aufgefallen, dann brauche ich nur noch darauf zu warten, bis es seine Daten auf meinem gehackten Server eingegeben hat.



Nach drücken des Anmeldebuttons wird eine Weiterleitung zum Twitter-Server durchgeführt und die Daten werden direkt als Login übergeben.

Erst jetzt wird die 2FA ausgelöst, doch nun ist es schon zu spät.

In der Zwischenzeit haben wir die Daten unseres Opfers mitgeschnitten und nicht nur die Anmeldedaten umverschlüsselt abgegriffen. Was wir zusätzlich noch bekommen haben, sind all seine Schlüsselspeicher, in dem sich auch die Cookies befinden. Damit sind alle Angaben für uns nur noch als Speicherspaß anzusehen. Für uns ist der Cookie deutlich interessanter, da wir uns damit - direkt - ohne weitere Angaben von Daten, von unserem Rechner aus, bei Twitter anmelden können.

Cookie auslesen

Um den Cookie unseres Opfers auszulesen laden wir einfach die letzte Session:

phishlet	author	active	status	hostname
amazon	@customsync	disabled	available	
facebook	@mrgretzky	disabled	available	
outlook	@mrgretzky	disabled	available	
twitter	@white_fi	enabled	available	
citrix	@424f424f	disabled	available	
instagram	@prrrrinncee	disabled	available	
linkedin	@mrgretzky	disabled	available	
reddit	@customsync	disabled	available	
twitter-mobile	@white_fi	disabled	available	

: sessions

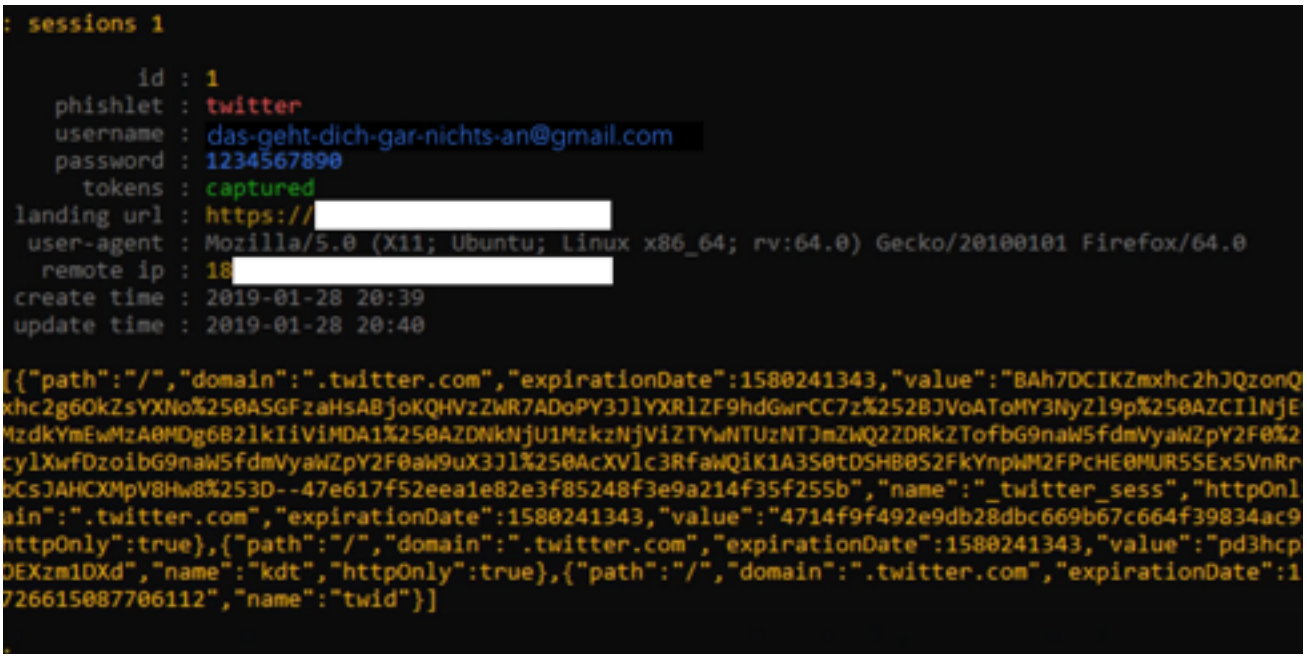
id	phishlet	username	password	tokens	remote ip	time
1	twitter	das-geht-dich....@gmail.com	1234567890	captured		

Nach dem wir unseres Session geladen haben, können wir uns den Cookie ausgeben lassen. Wir kopieren uns einfach den Inhalt unseres Cookies und können Ihn über unseren Browser übergeben. Natürlich werden alles Angreifer wissen, das auch Spuren des eigenen Rechners hinterlassen werden kann. Daher werden meist ProxyServer oder Cloud Browser und weitere Dienst genutzt, um sich auf den Dienst aufzuschalten.

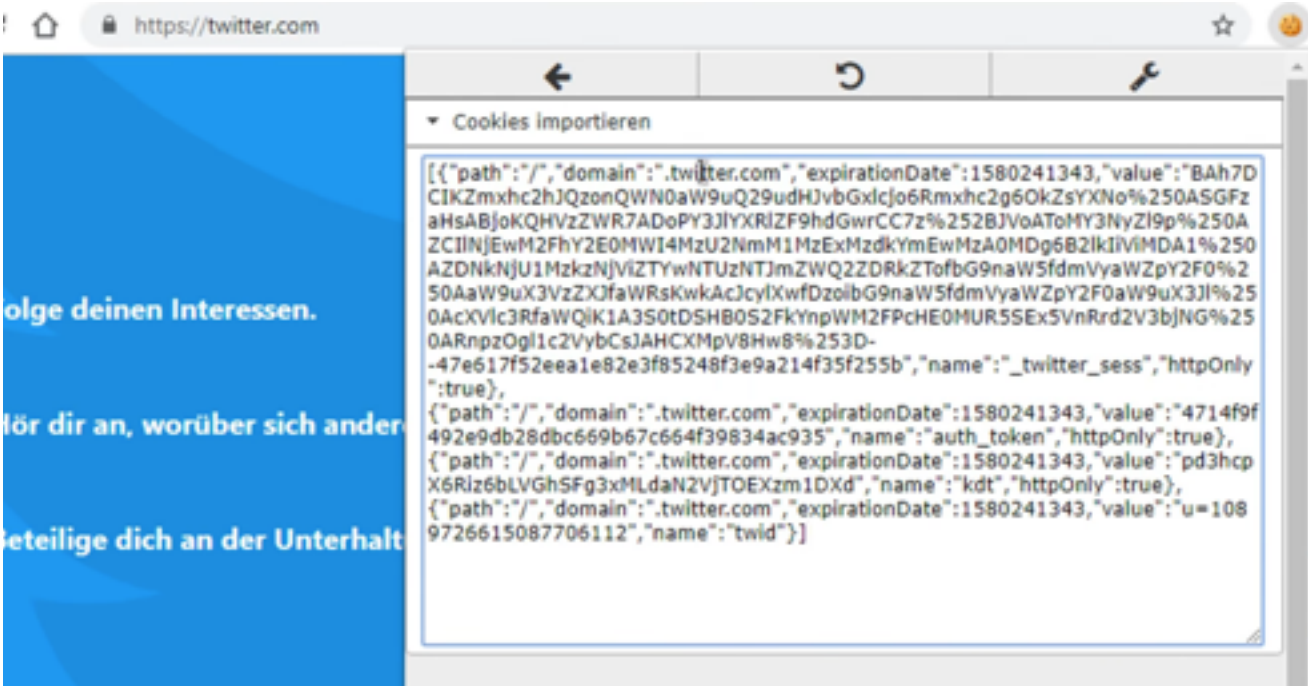
Diese Dienste benenne ich hier nicht weiter und sind für uns auch nicht wirklich von Interesse, da ich den Angriff hier nur als Demo darstelle und keine realen Personen oder Accounts fremder angegriffen und bestohlen werden.

Login auf Twitter

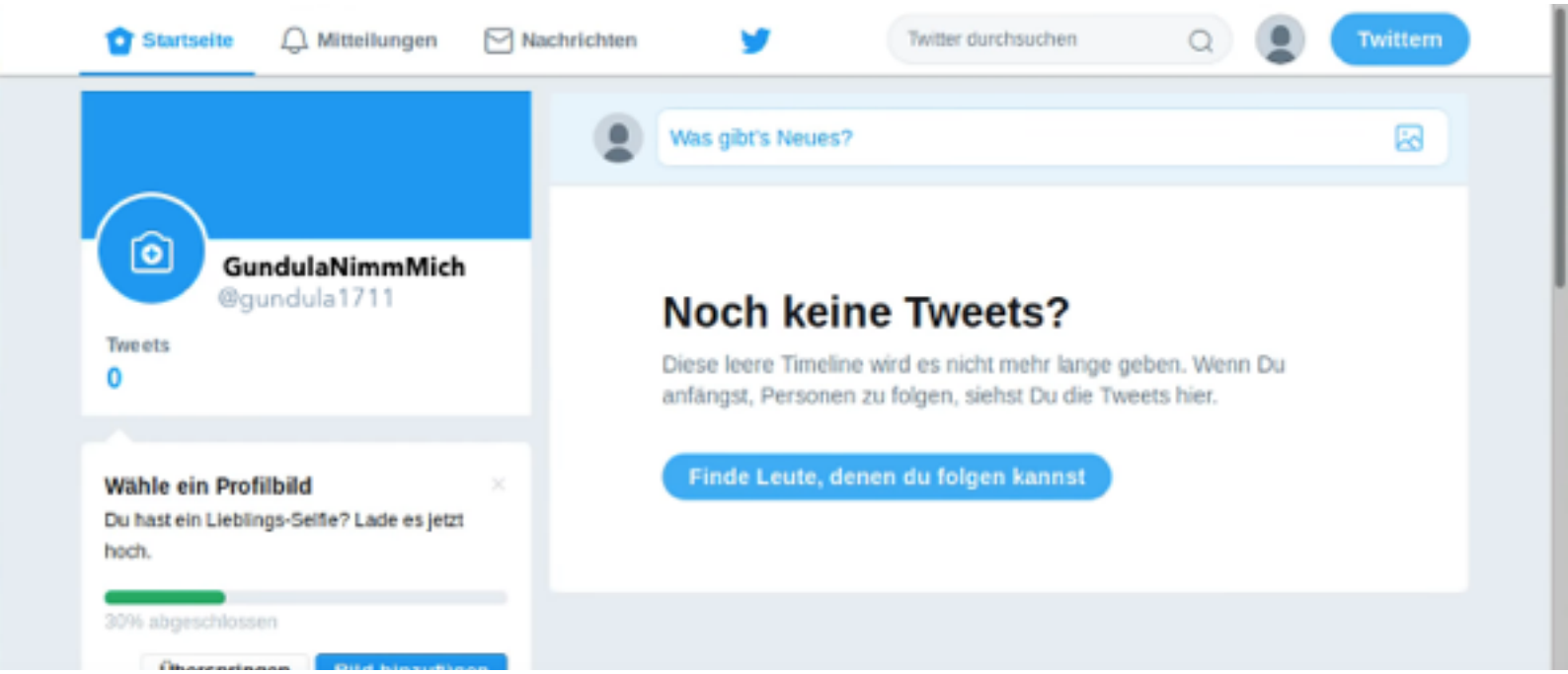
Da ich nun den Cookie unseres Opfers kenne, kann ich mir diesen anzeigen lassen um Ihn mir zu kopieren.



Das Übertragen eines bestehenden Cookies in den Browser kann einfach über ein weiteres PlugIns erledigt werden:



Ist der Cookie einmal übergeben, brauch nur noch die Website aktualisiert werden und ich bin angemeldet als unser Opfer.



Ich kann nun Daten, Informationen, Bilder, Videos und mehr sammeln oder im Namen einer anderen Person schreiben. Es wird deutlich unangenehmer, wenn ich einen Amazon oder E-Bay Account finde.

Es gibt sicher genug Möglichkeiten sich gegen solche Angriffe zu schützen. Zum Beispiel sollten deine Accountdaten verschlüsselt und mit einem speziellen Tool gesichert werden. Auch sollten deine Passwörter min 21 Stellen haben.

Fazit

Es ist recht einfach, Daten anderer Personen abzugreifen und es lässt sich in nur wenigen Schritten (auch ohne Fachkenntnisse) von einem Angreifer aus umsetzen. Der Schaden kann enorm für die potenziellen Opfer sein. Eine 2FA ist sicherlich sehr nützlich, bringt jedoch bei Phishing-Angriffen keine Punkte. Die 2FA-Fragen oder direkte -Handy-Bestätigung, hilft hier nicht weiter, da sie erst nach einem Angriff in Ausgeführt werden. Dann ist es jedoch meist schon zu spät.

Autor: Michael Kaufmann - 04.01.2019