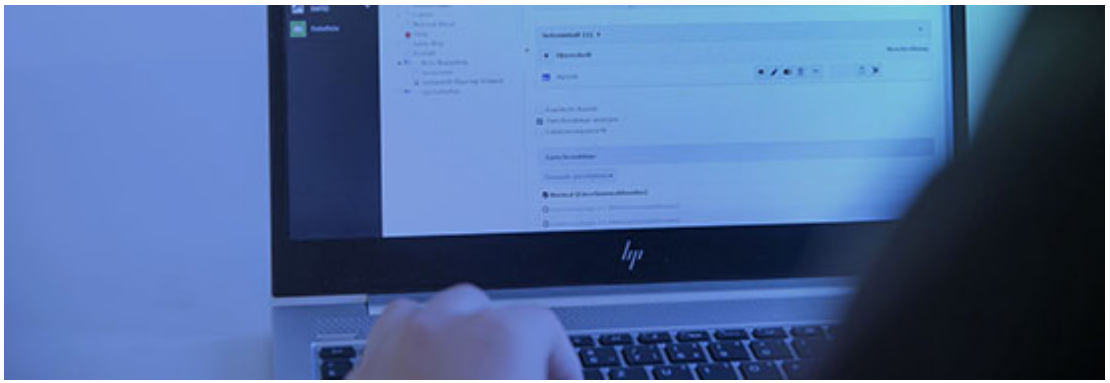
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundesamt für Cybersicherheit BACS

Woche 1: Gehackte Websites für die Suchmaschinen-Optimierung missbraucht

10.01.2023 - Der Meldeeingang des NCSC ist in der ersten Woche 2023 mit 559 Meldungen im Vergleich zur Vorwoche wieder gestiegen. Eine Meldung zu einer Google-Suche, welche dubiose Suchresultate lieferte, stellte sich als eine Suchmaschinen-Manipulation heraus. Zahlreiche Webseiten wurden mit dem Ziel gehackt, den Suchalgorithmus von Google hinters Licht zu führen.



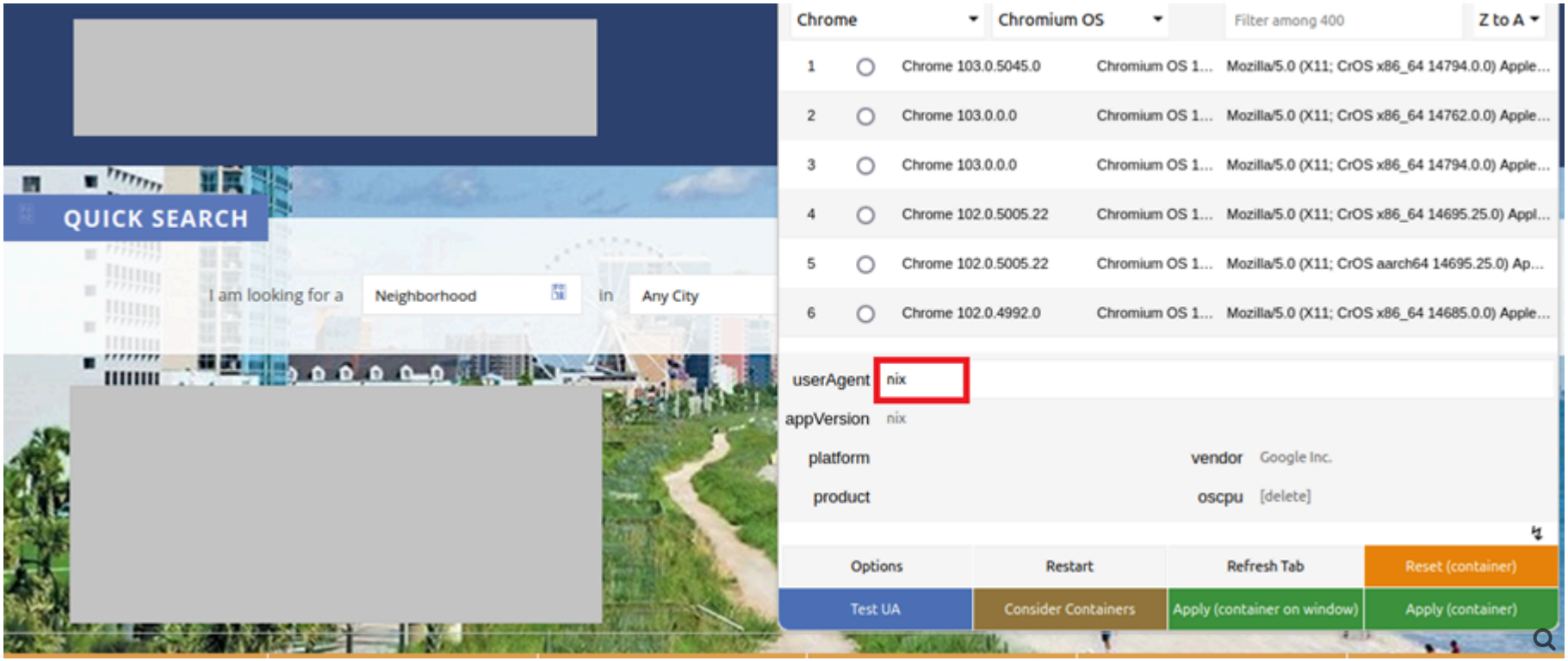
Letzte Woche ging eine Meldung beim NCSC ein, dass die Google-Suche nach einer Schule zu dubiosen Suchresultaten führe. Dabei fiel vor allem eine verdächtige Javascript-Datei auf. Eine Google-Suche nach der verdächtigen Domäne in dieser Datei zeigte nicht weniger als 5500 Websites mit dem gleichen Verhalten: Google zeigte bei den Resultaten zwar jeweils den korrekten Titel der gefundenen Website

an, unterhalb des Titels wurden allerdings, statt des üblichen Ausschnitts des Webseiteninhalts, diverse Fehlermeldungen eingeblendet. Öffnete man die Webseite mittels Google Cache – eine Kopie der Webseite, die von Google zwischengespeichert wird - wurde diese Fehlermeldung ebenfalls angezeigt. Öffnete man die Webseite jedoch direkt, mittels Eingabe der URL, dann wurde die Webseite ohne Fehlermeldung dargestellt.

Eine Suche nach der verdächtigen Domäne ergab zahlreiche Treffer mit dem korrekten Titel, aber mit Fehlermeldungen in der Beschreibung

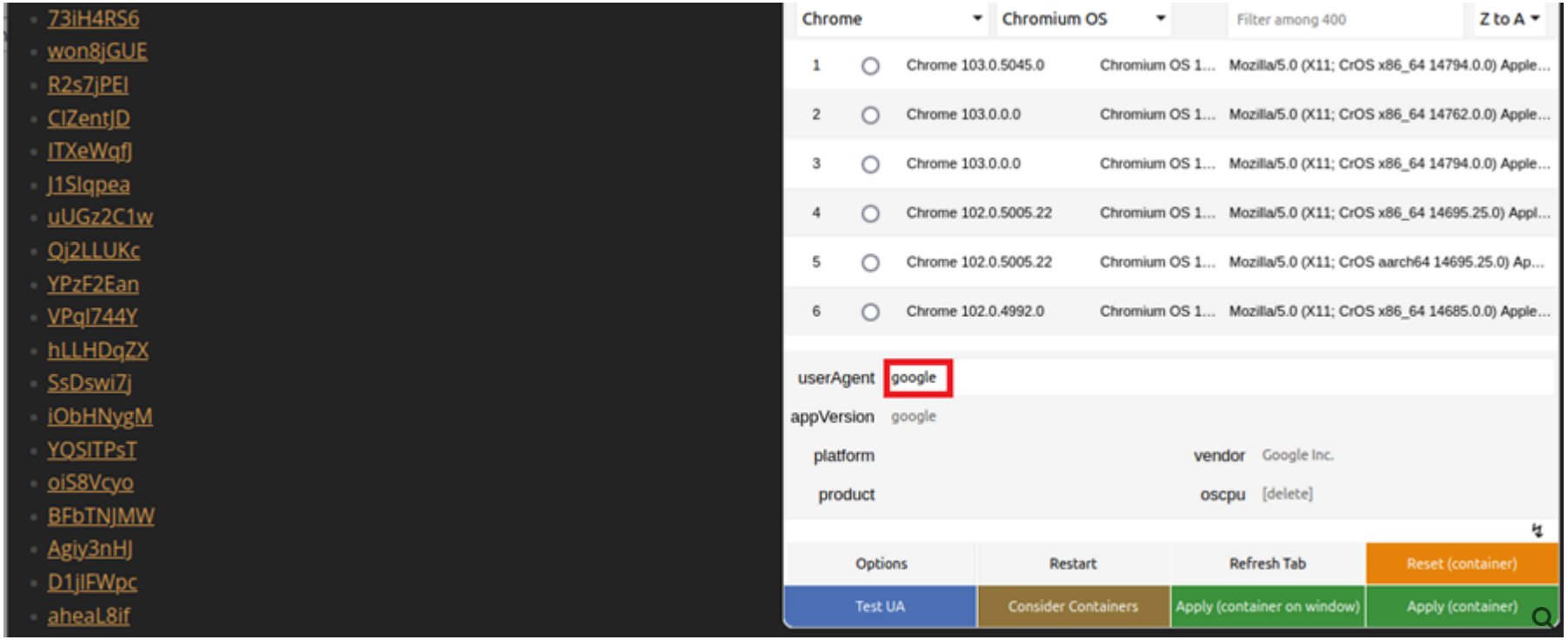
Die Vermutung lag nahe, dass in diesem Fall unterschiedliche Seiteninhalte - abhängig vom sogenannten «User-Agent» - angezeigt werden. Der «User-Agent» wird jeweils bei jedem Aufruf einer Webseite mitgesendet und gibt dem Webserver Informationen über Betriebssystem und dem verwendeten Browser des Besuchers. Solche Daten können neben statistischen Erhebungen auch dazu verwendet werden, Webseiten-Inhalte auf einen speziellen Browsertyp zu optimieren. Gerade im Webseiten-Design wird dies beispielsweise benutzt, um zwischen Notebooks, Tablets und Mobiltelefonen zu unterscheiden und den Webseiten-Inhalt an das jeweilige Bildschirm-Format anzupassen. Auch Suchmaschinen benutzen beim Durchforsten des Internets eine spezielle Kennung und geben sich dadurch als solche zu erkennen.

Ein Test bei den gefundenen Websites bestätigte den Verdacht: Das Öffnen der Website mit einem «User-Agent» eines gängigen Browsers (hier mit «nix» gekennzeichnet) führte zur korrekten Anzeige der erwarteten Website.



Mit einem gängigen «User-Agent» wird die erwartete Seite angezeigt.

Setzte man allerdings als «User-Agent» «Google» ein, dann änderte sich das Aussehen der Webseite komplett. Anstelle des Inhalts wurde eine Reihe von Links eingeblendet, welche sich hinter Buchstaben- und Zahlenkombinationen versteckten.



Fügt man dem «User-Agent» das Wort «Google» hinzu, ändert sich die Seite und es werden zahlreiche Links hinter Buchstaben- und Zahlenkombinationen eingeblendet.

Suchmaschinen-Optimierung

Doch was bezwecken die Angreifer mit diesem Vorgehen? Es handelt sich dabei um einen typischen Versuch, Suchmaschinen-Resultate zu manipulieren. Die sogenannte «Search Engine Optimization» oder zu Deutsch «Suchmaschinen-Optimierungen» gibt es in den verschiedensten Variationen. Im aktuellen Fall nutzten die Angreifer gehackte Websites und schleusten dort Schadcode ein, um Google hinters Licht zu führen und das Ranking zu verbessern. Dadurch erhöht sich die Chance, dass potenzielle Opfer auf die manipulierten

Suchresultate klicken und dadurch auf dubiosen Websites landen. Auffallend viele der betroffenen Websites wurden durch die CMS-Software «Kentico» betrieben. So dürften nicht gepatchte Schwachstellen in diesem CMS Ursache der manipulierten Websites gewesen sein.

Der eingeschleuste Schadcode prüft den «User-Agent». Kommt der Aufruf von Google, dann werden die oben beschriebenen Links eingeblendet, welche von Google gespeichert und indexiert werden. Da nun auf den diversen gehackten Webseiten immer die gleichen Links eingeblendet werden geht Google davon aus, dass diese interessant sind und taxiert diese als relevanter als diese eigentlich sind. Die Links wandern in den Suchresultaten entsprechend nach oben und haben dann eine höhere Reichweite. Für alle anderen Besucher der Website, die mittels direkter URL auf die Website gelangen und auch für den Webseitenbesitzer, wird der normale Inhalt eingeblendet. Dadurch fällt die Manipulation weniger auf und kann über lange Zeit ihre Wirkung entfalten.

Empfehlungen für Website-Betreibende:

- **Angriffe auf Content Management Systeme lassen sich durch das zeitnahe Einspielen von Updates mit wichtigen Sicherheitsaktualisierungen massiv reduzieren.**
- **Neben der normalen Authentifizierung (Benutzername und Passwort) für den Zugriff auf den Administrationsbereich empfiehlt das NCSC den Einsatz einer Zwei-Faktor-Authentifizierung.**
- **Der Administrator-Zugriff sollte auf die von den Administratoren verwendeten IP-Adressen eingeschränkt werden.**

Weitere Informationen zum Schutz der CMS finden Sie unter:

Massnahmen zum Schutz von CMS (/ncsc/de/home/infos-fuer/infos-unternehmen/aktuelle-themen/massnahmen-schutz-cms.html)

Aktuelle Zahlen und Statistiken

Die Anzahl Meldungen der letzten Woche nach Kategorien sind publiziert unter:

Aktuelle Zahlen (/ncsc/de/home/aktuell/aktuelle-zahlen.html)

Letzte Änderung 10.01.2023

https://www.ncsc.admin.ch/content/ncsc/de/home/aktuell/im-fokus/2023/wochenrueckblick_1.html