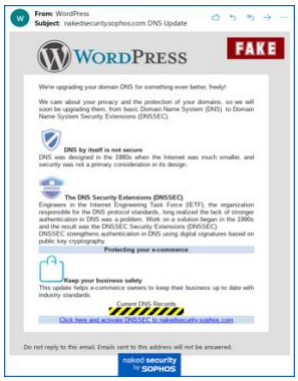
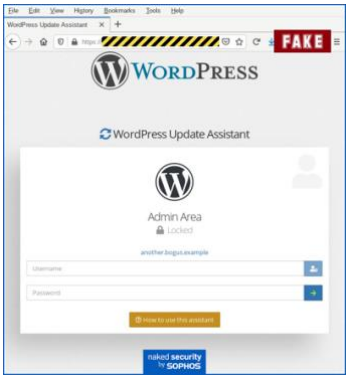
Vorsicht vor neuartigem „Secure DNS“-Betrug
Extrem glaubwürdig zielt er auf Website-Besitzer und Blogger

Viele Webseite- oder Blog-Betreiber nutzen einen Cloud-Provider oder ein dediziertes Hosting-Unternehmen wie WordPress, um ihren Server zu verwalten und die Inhalte Lesern, Zuschauern und Zuhörern zur Verfügung zu stellen. Und weil es sehr einfach ist, den Hosting-Provider eines Blogs oder einer Web-Seite, beispielsweise im HTTP-Header eindeutig zu identifizieren, erhalten Anwender jede Menge (Spam-)Nachrichten. Darunter sind Angebote, Aufforderungen den Anbieter zu wechseln, die Inhalte zu optimieren und das Google-Ranking zu verbessern. Natürlich versuchen auch Cyberkriminelle auf diesen Zug aufzuspringen und die Nutzer mit Phishing-Mails auf falsche Pfade zu leiten, um diese schlussendlich auf schädliche Webseiten zu locken. Oft erkennt man Phishing-Mails anhand seltsamer Mailadressen oder aufgrund schlechter Texte mit vielen Rechtschreib- und Grammatikfehlern. Nun endeckten die Security-Experten von Sophos eine Phishing-Nachricht, die überraschend echt aussah. Sie schien angeblich von WordPress zu kommen und es wurde behauptet, dass der Domain bald neue DNS-Sicherheitsfunktionen hinzugefügt werden.





Gehen Nutzer auf das Angebot der augenscheinlich glaubwürdigen Mail ein, gelangen sie via Link auf eine Landing-Page, die ebenfalls erstaunlich professionell und vertrauenswürdig gestaltet ist. Selbstverständlich wird gleich zu Anfang nach dem Nutzernamen und dem Passwort gefragt, ganz wie man es gewohnt ist. Besonders raffiniert bei dieser Art von Phishing-Mails ist, dass sich mit dem Click auf den Link in der Mail automatisch das benötigte Landing-Page-Design einstellt und öffnet. Damit wiegt sich der Nutzer stets in seiner Comfort-Zone und ahnt nichts Böses.

Paul Ducklin, Principal Research Scientist bei Sophos erklärt dazu: „Dieser DNS-Betrug ist einfach und raffiniert zugleich. Technisch gesehen handelt es sich nicht um trickreiche JavaScripts oder komplexe Web-Umleitungen. Optisch ist es jedoch überraschend glaubwürdig, nicht zuletzt, weil die Cyberkriminellen über 98 verschiedene Webhosting-Markenlogos und Symbole verfügen, mit denen sie ihre Phishing-Seite automatisch anpassen und so versuchen, den Anwender von der Glaubwürdigkeit der Nachricht zu überzeugen.“

Wie kann man solchen Betrugsmaschen vorbeugen?

- Niemals über Links anmelden, die in E-Mails angeboten werden. Wenn man eine E-Mail mit der Aufforderung erhält, dass man sich beim Dienst X anmelden solle, sollten die vorgeschlagenen Links in der E-Mail nicht beachtet werden werden. Sicherer ist der Weg zum Login, indem man die URL selbst eingibt. Auf diese Weise fällt man nicht versehentlich

auf gefälschte Links herein.

- Nutzung der Zwei-Faktor-Authentifizierung wann immer es geht. Die Zwei-Faktor-Authentifizierung macht ein Passwort viel weniger nützlich und schafft eine wesentlich höhere Hürde für die Gauner.
- Nutzung eines Passwortmanagers. Ein Passwortmanager generiert nicht nur automatisch starke und zufällige Passwörter, sondern ordnet jedes Passwort auch einer bestimmten URL zu. Das macht es viel schwieriger, das richtige Passwort auf die falsche Seite zu setzen, weil der Passwortmanager einfach nicht weiß, welches Konto er verwenden soll, wenn er mit einer unbekannten Phishing-Seite konfrontiert wird.
- Anti-Virus mit Live-Web-Filterung. Produkte wie Sophos Home (kostenlos für Windows und Mac) blockieren nicht nur das Eindringen von Malware auf dem Computer, sondern verhindern auch, dass Webverbindungen zu riskanten Websites überhaupt aufgebaut werden, selbst wenn diese Websites keine Malware enthalten.

Eine detaillierte Analyse darüber, wie professionell Cyberkriminelle ihre Betrugsmasche am Beispiel mit WordPress durchführen, beschreibt Sophos hier:
https://nakedsecurity.sophos.com/2020/06/29/beware-secure-dns-scam-targeting-website-owners-and-bloggers/

Pressekontakt:

Sophos
Jörg Schindler, PR Manager CEEMEA
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de