Domain-Besitzer? Vorsicht vor dubiosen Bug-Bounty-Jägern!

Unternehmen nutzen immer häufiger Bug Bounty Programme zum Aufdecken potentieller Sicherheitslücken. Das florierende Geschäft ruft aber auch teilweise kriminell motivierte Trittbrettfahren auf den Plan – die sogenannten „Beg Bounty Hunter" haben vornehmlich kleine Unternehmen im Visier.

Die Suche nach Bugs in den eigenen Produkten und in der Folge das Schließen potentieller Einfallstüren für Cyberangriffe steht mit zunehmender Digitalisierung immer mehr im Fokus von Softwareherstellern. Zu diesem Zweck haben viele Unternehmen sogenannte Bug-Bounty-Programme ins Leben gerufen, mit denen das seriöse Auffinden und Melden von signifikanten Sicherheitslücken belohnt werden. Doch wie so oft bei beliebten Konzepten sind auch Betrüger nicht weit und gehen mit oft wenig IT-Security-Verständnis und dubiosen Methoden auf „Betteltour". Die deshalb auch als „Beg Bounty Hunter" bezeichneten Cyberganoven melden gefälschte Bugs und Fehlkonfigurationen und versuchen, gerne bei eher kleineren Unternehmen, mit dieser Masche und einem vorgetäuschten großen Gefahrenpotential als Helfer in der Not abzukassieren.

„Die Riege der Beg Bounty Hunter ist weitläufig und mit ganz unterschiedlichen Intentionen unterwegs. Von ethisch und gut gemeint bis hin zu grenzwertigen oder schlicht kriminellen Methoden ist alles dabei", so Chester Wisniewski, Principal Threat Researcher bei Sophos. „Fakt ist allerdings, dass keine der 'Schwachstellen', die ich in diesem Zusammenhang untersucht habe, eine Zahlung wert waren. Es existieren Millionen schlecht gesicherter Webseiten und viele der Domain-Inhaber wissen nicht, wie sie die Sicherheit verbessern können. Gerade diese Zielgruppe lässt sich mit entsprechend professionell klingenden Nachrichten über potentielle Sicherheitslücken leicht einschüchtern und von suspekten Dienstleistungen überzeugen. Empfänger solcher Mails sollten diese zwar ernst nehmen, denn sie können auf eine gefährliche Sicherheitslage hindeuten, sie sollten sich aber auf keinen Fall auf die angebotene Leistung einlassen. Sinnvoller ist es in einem solchen Fall, einen vertrauenswürdigen IT-Partner vor Ort um eine Bewertung der Situation zu bitten, um gegebenenfalls bestehende Gefahren beseitigen zu lassen."

Beg Bounty Hunter und ihre Taktik

Seit letztem Jahr mehren sich die Berichte, insbesondere von kleinen Unternehmen, dass vermeintliche Security-Experten sie wegen Schwachstellen bei ihrer Website kontaktieren. Die Forensiker von Sophos haben einige dieser Angebote analysiert: In jedem der Beispiele wurde der angebliche „Schwachstellenbericht" oder das „Beg Bounty" vom angeblichen Sicherheitsexperten an eine E-Mail-Adresse gesendet, die auf der Website des Empfängers offen zugänglich war. Damit liegt die Schlussfolgerung nahe, dass es sich bei den Nachrichten um eine Kombination aus automatisiertem Scannen nach vermeintlichen Sicherheitslücken oder Fehlkonfigurationen, einem anschließenden Kopieren der Scan-Ergebnisse in eine E-Mail-Vorlage und dem Nutzen einer undifferenzierten Mail-Adresse für den Versand handelt. Alles mit dem Ziel, ein Honorar für die Lösung des „Problems" zu erhalten.

Die Preisspanne bei den untersuchten Beg-Bounty-Nachrichten ersteckte sich von 150 bis 2.000 US-Dollar pro Fehler, je nach Schweregrad. Zudem brachten die Nachforschungen zu Tage, dass es bei Erstzahlungen für eine Schwachstelle teilweise zu einer Eskalation der Forderungen für weitere Schwachstellen kam. Die „Experten" verlangten plötzlich 5.000 US-Dollar für die Behebung weiterer, vermeintlicher Sicherheitslücken und auch die Kommunikation wurde aggressiver.

Dreist kommt weiter – ein Beispiel

Eines der von Sophos analysierten Beispiele beginnt gleich zu Beginn mit einer falschen Aussage. Der Beg Bounty Hunter behauptet, eine Schwachstelle auf der Webseite des Adressaten gefunden zu haben und erklärt, dass kein DMARC-Datensatz zum Schutz vor E-Mail-Spoofing existiert. Allerdings ist das weder eine Schwachstelle noch hat die Thematik direkt mit der Webseite zu tun. Die Veröffentlichung von DMARC-Datensätzen kann zwar dazu beitragen, Phishing-Angriffe zu verhindern, ist aber eine komplexe Aufgabe, die bei den meisten Unternehmen nicht weit oben auf der Liste der Security-Aufgaben steht. Und auch wenn das Problem also tatsächlich existiert, wird es im Zusammenhang mit der Beg-Bounty-E-Mail als größer dargestellt als es tatsächlich ist, um den Empfänger zur Zahlung einer Belohnung zu treiben.

Subject: Vulnerability Found (CLICK JACKING)
Reply-To: "Faisal Mehmood" <whitehattester@

Hello Team,
As an Ethical Hacker i found some Vulnerabilities in your site one of them is as following.
Issue : CLICK JACKING

Clickjacking, also known as a "UI redress attack", is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on another page when they were intending to click on the the top level page. Thus, the attacker is "hijacking" clicks meant for their page and routing them to another page, most likely owned by another application, domain, or both.
Using a similar technique, keystrokes can also be hijacked. With a carefully crafted combination of stylesheets, iframes, and text boxes, a user can be led to believe they are typing in the password to their email or bank account, but are instead typing into an invisible frame controlled by the attacker.
PoC:
<html>
<body>
<iframe height="500" width="500" src="https:/
utm_source= &utm_medium=referral&utm_content=homepage-top-bar-sign-in&utm_campaign=user-acquisition" ></iframe>
</body>
</html>

IMPACTS:
By using Clickjacking technique, an attacker hijack's click's meant for one page and route them to another page, most likely for another application, domain, or both.

Remediation:
Frame busting technique is the better framing protection technique. Sending the proper X-Frame-Options HTTP response headers that instruct the browser to not allow framing from other domains
For Fix:
it is missing a X-FRAME header. a user with the help of some tricky css can trick user click on the one click actions. . You should apply a X-FRAME header
Note: I'm hoping to receive a bounty reward for my current finding. I will be looking forward to hear from you on this and will be reporting other vulnerabilities accordingly.

Kind Regards
Faisal Mehmood

Die meisten untersuchten Fälle beruhten auf simplen Internetscans, die fehlende SPF- oder DMARC-Einträge zu Tage förderten wie unser Beispiel oben. Andere Beg-Bounty-E-Mails bezogen sich zwar auf tatsächliche Schwachstellen, die allerdings ohne großes Fachwissen mit kostenlosen Tools gefunden und gefixt werden können.

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
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