Titel: Coineater: Automatisierte Erkennung von Krypto-Mining im Webbrowser

Einleitung: Das Mining von Kryptowährungen wird in der Regel auf leistungsfähiger Single-Purpose-Hardware oder GPUs durchgeführt. Die Berechnungen können jedoch leicht parallelisiert und auf viele weniger leistungsfähige Systeme verteilt werden. Cryptojacking ist eine neue Bedrohung im Internet und beschreibt Code, der in Webseiten eingebettet ist und ohne die Zustimmung von Webseiten-Besucherinnen deren CPU für Krypto-Mining nutzt. Im Zuge der Forschungsarbeiten wurde ein Web-Crawling-Framework erstellt, das in der Lage ist, Mining-Skripte effektiv zu erkennen, selbst wenn sie ihre bösartigen Aktivitäten verschleiern. Darüber hinaus kann unser Framework verwendet werden, um eine detaillierte Analyse von Kryptojacking-Kampagnen zu erstellen. Die Ergebnisse der Forschungsarbeiten flossen in die Entwicklung der Browser-Erweiterung CoinEater[2] für Chrome und Firefox ein, die zuverlässig Mining-Skripte auf Webseiten erkennt und blockiert.

Methode: Unser Framework besteht aus zwei Hauptteilen: einem automatisierten Browser, der Webseiten scannt und die Ergebnisse an einen zentralen Server zurückmeldet, sowie einem Orchestrierungsframework, das für den Betrieb der Infrastruktur und die Verwaltung der Scanaufträge und Ergebnisse im Backend verwendet wird (siehe Abbildung 1).

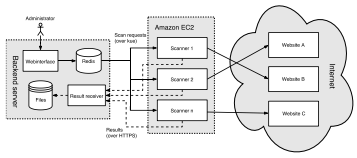

Abbildung 1: Aufbau des Scanning-Frameworks

Technologisch bauen wir auf einen Headless Chrome-Browser auf, der über das Chrome Developer Tools (DevTools) Protocol automatisiert wird. Für jede gescannte Website werden die folgenden Daten erhoben: Metadaten zu jeder Anfrage, JavaScript-Code und der komplette WebSocket-Verkehr der Webseite. Um Mining-Skripte in unseren großen Datensätzen zuverlässig zu erkennen ohne auf manuell erstellte Blocklisten angewiesen zu sein, haben wir einen dynamischen Erkennungsansatz entwickelt. Beim größten Anbieter von webbasiertem Mining, Coinhive.com, wurde der WebSocket-Verkehr zur Erkennung ausgewählt, da dieser aus JSON-Objekten mit einer Reihe von Key-Value-Paaren mit eindeutigen Namen besteht. Dies macht es einfach, Mining-Skripte zuverlässig zu identifizieren. Obwohl Coinhive eine dominante Marktposition hat, analysierten wir auch eine Reihe kleinerer Anbieter, um zu evaluieren, ob die gleiche Erkennungstechnik eingesetzt werden kann, um deren Mining-Skripte zu erkennen. Wir haben festgestellt, dass eine große Anzahl der getesteten Anbieter (z.B. coin-have.com, crypto-loot.com, minero.pw und

[2] https://github.com/fhstp/CoinEater

moneromine.rocks) genau das gleiche Protokoll verwendet und diese damit ohne Änderungen der Erkennungstechnik effektiv erkannt werden können. Andere Seiten (z.B. webmine.cz) verwendeten ein ähnliches JSON-basiertes Protokoll, das wir mit minimalem Aufwand integrieren konnten.

Ergebnisse: Wir haben die Alexa Top 1 Million Websites nach Kryptojacking gescannt, mehr als 13400000 einzigartige JavaScript-Dateien mit einer Gesamtgröße von 246 GB gesammelt und festgestellt, dass 3178 Webseiten Krypto-Mining ohne Zustimmung ihrer Besucherinnen durchführen. Etwa 85,6% der gefundenen Skripte stammten von Coinhive, 3,8% von CoinHave, 1,9% von Crypto-Loot und 8,7% von anderen. Wir konnten auch die API-Schlüssel für die Authentifizierung mit dem Backend-Server aus dem aufgezeichneten WebSocket-Verkehr extrahieren. Insgesamt haben wir 1210 eindeutige Schlüssel auf 3178 Webseiten gefunden. Der am häufigsten verwendete Schlüssel wurde auf 1116 verschiedenen Webseiten gefunden, während 961 Schlüssel nur auf einer einzigen Webseite gefunden wurden. Dies zeigt, dass die Mehrheit der Miner das Skript nur auf einer einzigen Webseite einsetzt oder sich für die Verwendung eindeutiger API-Schlüssel für jede Seite entscheidet. Gleichzeitig scheint es einige größere Operationen zu geben, die ihre Skripte auf einer großen Anzahl von Webseiten einsetzen.

Diskussion/Conclusio: Diese Arbeit stellt ein neuartiges Web-Crawling-Framework zur Erkennung von webbasiertem Krypto-Mining vor. Das Mining von Kryptowährungen im Webbrowser der Besucherin einer Website ohne deren Zustimmung ist eine neuartige Gefahr und eine zuverlässige Erkennung wird durch den vermehrten Einsatz von Proxy-Servern und Code-Obfuscation immer schwieriger. Unser Ansatz, nach dynamischen Artefakten der Mining-Skripte zu suchen, löst dieses Problem weitgehend. Wir konnten über 3000 Webseiten mit aktiven Mining-Skripten identifizieren, die die Nutzerin einer Webseite vor Beginn des Mining-Prozesses nicht um Erlaubnis bitten. Unser Framework ermöglicht es auch, detaillierte Analysen von Mining-Kampagnen durchzuführen. Wir fanden mehrere groß angelegte Kampagnen, von denen eine über 1000 infizierte Webseiten umfasste und das Mining-Skript sogar durch böswillige Werbung auslieferte. Aktuelle Browser-Erweiterung gegen Kryptojacking sind in der Lage, Verbindungen zu Coinhive, dem bisher größten Browser-Mining-Anbieter und ähnlichen Websites zuverlässig zu erkennen, scheitern aber oft an verschleierten Skripten sowie Proxy-Servern. Für unsere im Rahmen des Projekts entwickelte Browser-Erweiterung CoinEater erstellen wir alle zwei Wochen durch automatische Scans Blocklisten, die signifikant mehr Mining-Skripte zuverlässig blockieren, als bisherige Lösungen. Coineater ist Open-Source-Software und kann kostenlos unter https://github.com/fhstp/CoinEater geladen werden.