Richtlinie zum „Software-Sprint“

SpyCheck

Schlussbericht

Zuwendungsempfänger*in:

Itermann & Wansing GbR

Das diesem Bericht zugrundeliegende Vorhaben wurde mit Mitteln des Bundesministeriums für Forschung, Technologie und Raumfahrt unter dem Förderkennzeichen 01IS25S12 gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei dem*der Autor*in.

Kurze Darstellung der Aufgabenstellung und Motivation in der Förderphase

Wir wollten eine einfache Lösung schaffen, um durch passive Netzwerkanalyse Spyware/Stalkerware auf Smartphones und Computern zu erkennen. SpyCheck läuft auf einem separaten Linux-Laptop und öffnet dort einen WiFi-Hotspot oder eine freigegebene Ethernet-Verbindung. Es gleicht Domainnamen und IP-Adressen im Netzwerkverkehr mit Listen bekannter Überwachungsanbieter (Indicators of Compromise, IoCs) ab und sucht außerdem nach Auffälligkeiten im Datenverkehr.

Ähnliche Projekte waren TinyCheck von Kaspersky, dessen Python-Quellcode nicht mehr verfügbar ist, und dessen Fork SpyGuard, der ebenso veraltet und schwer zu installieren ist. SpyCheck ist eine moderne Neufassung in der Programmiersprache Go, die auf Linux-Betriebssystemen läuft und einfach zu benutzen ist.

Die Linux-Integration (Paketfilterung, WLAN-Hotspot, Ethernet-Bridge), die Integration der Datenquellen, das Frontend und die Dokumentation waren wichtige Meilensteine.

Beitrag des Projektes zu den Zielen der Förderinitiative „Software Sprint“

SpyCheck trägt zur individuellen Sicherheit der nutzenden Personen bei. Es fördert zudem eine Sensibilisierung für das Thema Datensicherheit und Überwachung und stärkt damit die digitale Resilienz der Gesellschaft.

Ausführliche Darstellung der Ergebnisse in der Förderphase

Wir haben eine einsatzbereite Version von SpyCheck fertiggestellt und veröffentlicht. Damit wurden fast alle Meilensteine erreicht, lediglich die Dokumentation ist noch ausbaufähig. Wir werden sie nach Ende der Förderphase vervollständigen und auch die Pflege und ggf. Weiterentwicklung der Software betreuen.

Unsere Erfahrung, dass es wichtig ist, Prioritäten zu setzen, wurde in der Förderphase erneut bestätigt. Der Grad der Begleitung durch die Open Knowledge Foundation war dabei genau richtig. Insbesondere die verpflichtenden zweiwöchentlichen Montags-Updates waren für uns sehr hilfreich.

Zielgruppe, Nutzen und mögliche Weiterentwicklungen

Der Zielgruppe steht ein niedrigschwelliges Werkzeug zur Verfügung, um Smartphones und Computer einfach auf Aktivitäten von Überwachungssoftware zu untersuchen. Den Quellcode unter eine freie Lizenz zu stellen ist für uns eine Selbstverständlichkeit und trägt auch zum Vertrauen in die Software bei. Die Weiterentwicklung von SpyCheck wird hauptsächlich in einer Anpassung an die technologische Weiterentwicklung des Internets und einem besseren Tooling zum Verwalten der IoC-Listen bestehen.

Durch das Projekt haben wir ein besseres Verständnis für die Funktionsweise von Spyware insbesondere auf Android-Smartphones erhalten und wertvolle Erfahrungen in der Entwicklung von interaktiven Web-Frontends und im Schreiben von gut lesbarem Quellcode gesammelt.

Kurze Darstellung der Arbeiten, die zu keiner Lösung geführt haben

Arbeiten bzw. Lösungsansätze, die wir nicht weiterverfolgt haben, gab es nicht.

Kurze Angabe von Präsentationsmöglichkeiten für mögliche Nutzer*innen

- https://codeberg.org/spycheck/spycheck
- https://spycheck.org/
- https://chaos.social/@spycheck

Kurze Erläuterung zur Einhaltung der Arbeits- und Kostenplanung

Bei unserer Recherche zu IoCs entstand ein höherer Aufwand als erwartet. Eine Anpassung der Planung wurde dadurch aber nicht notwendig.

Kurze Darstellung von etwaigen Ergebnissen bei anderen Stellen

Im Laufe der Entwicklung sind wir auf einzelne weitere Projekte aufmerksam geworden, die mittels Traffic-Analyse Schadsoftware aufspüren, aber technisch komplizierter einzurichten sind. Das hat unsere Fokussierung auf eine einfache Installation und Nutzung bestärkt.