Sucht, was ihr wollt!

Systemeinbrüche aufdecken mit LOKI

LOKI durchsucht ähnlich wie Virenscanner Clients und Server nach Einbruchsspuren. Aber besser als Virenscanner lässt er sich leicht mit selbst erstellten Signaturen füttern und kann damit direkt auf neue Bedrohungen reagieren.

Von Olivia von Westernhagen

Wer im Internet nach Informationen zu Angriffen auf Unternehmensnetzwerke oder zu aktuellen Schadcode-Kampagnen sucht, kann sich über einen Mangel an Informationen nicht beschweren: Sicherheitssoftwarehersteller, unabhängige Experten und staatliche Behörden wie das US-CERT informieren umfassend zu aktuellen Fällen. Mit dabei sind fast immer Dateinamen und -hashes, IP-Adressen von Command-and-Control-Servern und Codeauszüge aus schädlichen Skripten. Noch detailliertere Informationen zu Schadcode nebst sämtlichen Komponenten bieten die automatisch generierten Analyseberichte von Online-Services wie VirusTotal oder Hybrid-Analysis.

All diese Informationsbausteine liefern Hinweise auf erfolgreiche Einbrüche (Indicators of Compromise, kurz IoC). Netzwerkadmins, aber auch sicherheitsbewussten Privatleuten drängt sich geradezu der Gedanke auf, damit auch die eigenen Systeme und Netze nach Anzeichen auf Kompromittierungen zu durchsuchen.

Genau dafür gibt es den kostenlosen IoC-Scanner LOKI. Er läuft ohne vorherige Installation auf Windows, Linux oder macOS, zum Beispiel auf Domain Controllern, Web- und Fileservern oder sämtlichen Clients im Netzwerk. Das schlanke Kommandozeilentool gleicht Dateien und laufende Prozesse ähnlich wie ein Virenscanner mit einer lokal gespeicherten Signaturdatenbank ab. Während man in klassischer Antivirensoftware in der Regel nicht „mal eben schnell" eigene Datei-Signaturen einpflegen kann, geht das mit LOKI ganz einfach.

LOKIs in Python geschriebener Quellcode ist aus dem GitHub-Repository seines Entwicklers Florian Roth abrufbar. Auf der „Releases"-Unterseite steht die aktuelle Version des Tools (0.28.1) in einem Zip-Archiv bereit, in dessen Unterordnern sich neben einer fertig kompilierten EXE-Datei auch alle zusätzlich vom Scanner benötigten Komponenten befinden.

Das Kommandozeilentool kann wie jede andere Software im Netzwerk verteilt werden. Denkbar ist etwa die Bereitstellung auf einem Netzlaufwerk und die anschließende Ausführung als Scheduled Task mittels entsprechender Gruppenrichtlinien. Für einen vollständigen Systemscan muss LOKI mit Admin-Rechten ausgeführt werden.

Um auf einem Windows-PC das Verzeichnis Programme nach IoC zu scannen, tippen Sie auf der Kommandozeile

```
loki -p C:\Programme
```

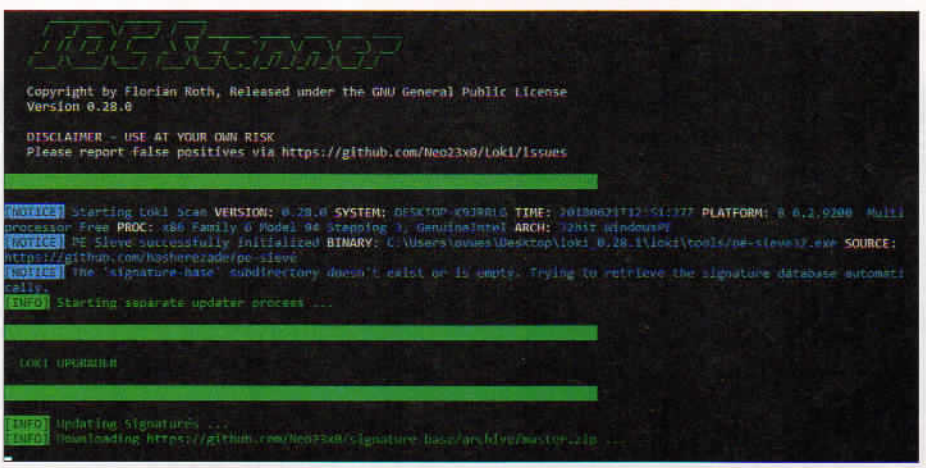
Der Parameter `--update` weist LOKI an, seine Signaturdatenbank zu aktualisieren. Sonst macht LOKI das nur beim allerersten Start. Die zum Scanner gehörende Datenbank stammt größtenteils von Florian Roth, der sie regelmäßig aktualisiert. Sie ist aber nach Belieben auch aus anderen Quellen erweiterbar. Dazu später mehr.

Der Parameter `-h` gibt eine Liste weiterer möglicher Parameter aus.

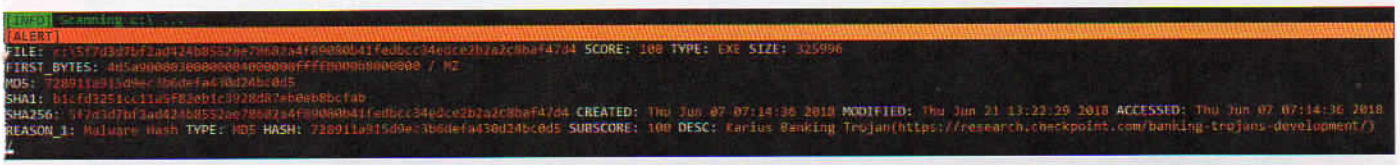
Scanvorgang

Zunächst testet LOKI laufende Prozesse auf bestehende Netzwerkverbindungen und gleicht sie mit Adressen von Command-and-Control-Servern ab, über die Angreifer aus der Ferne auf infizierte Rechner zugreifen können. Seit der Anfang Januar erschienenen Version 0.26.0 führt LOKI an dieser Stelle auch eine (signaturunabhängige) Überprüfung auf Prozessanomalien mit dem PE-Sieve-Tool von der Malware-Forscherin hasherazade durch, um etwa schädliche DLLs zu entdecken, die sich in legitime Prozesse eingeklinkt haben.

Anschließend vergleicht LOKI die Hashes der gescannten Dateien mit MD5-, SHA1- und SHA256-Hashes bekannter Malware- und APT-Komponenten. Außerdem spürt er anhand von regulären Ausdrücken verdächtige Kombinationen aus Dateinamen und -endungen sowie Pfaden und Ordnernamen auf. LOKI ermittelt bei allen Dateien den Typ und entscheidet anhand dessen, ob er sie näher untersucht. In der Regel sind das ausführbare Dateien, es können aber auch Memory Dumps (.dmp) sein, die auf Einbruchsspuren durchsucht werden.



Vor dem ersten Scan startet LOKI den integrierten Upgrader, um die Signaturen herunterzuladen.



Mit den hinzugefügten DIY-Signaturen findet LOKI Karius problemlos – das Wegputzen ist Sache des Users.

LOKI kann auch sogenannte Yara-Regeln auf Dateien und laufende Prozesse anwenden. Das sind regelbasierte Signaturen, die bekannte Dateieigenschaften wie Format, Größe oder enthaltene Strings und Bytefolgen kombinieren. In der IT-Sicherheitsszene hat sich das Yara-Projekt mittlerweile stark etabliert: Die Threat-Intelligence-Services von ESET und Kaspersky und der Open-Source-Virenscanner ClamAV arbeiten mit der Yara-Syntax, und auch das US-CERT veröffentlicht zu einzelnen IoCs häufig gleich die passenden Regeln.

Die knapp 370 Yara-Regeln in LOKIs Signaturdatenbank erkennen neben Malware auch zahlreiche typische Hackertools und Skripte für den unbefugten Zugriff auf Webserver. Neben signaturbasierten Scans führt LOKI weitere Tests durch, deren Aufzählung hier den Rahmen sprengen würde; eine gute Zusammenfassung bietet die Readme-Datei bei GitHub.

Die Ausgaben im Kommandozeilenfenster während des Scans gliedern sich in „Infos“ (grün), „Notices“ (blau), „Warnings“ (gelb) und „Alerts“ (rot), abhängig von Scores, die den Schweregrad einer Bedrohung beschreiben. Funde umfassen neben dem Score auch genaue Pfadangaben beziehungsweise Process IDs sowie kurze Beschreibungen und Links zu weiterführenden Informationen, die LOKI der Signaturdatenbank entnimmt.

Abschließend speichert LOKI seinen Output als Logdatei (im selben Ordner, in dem sich der Scanner befindet) und gibt Hinweise darauf, ob Handlungsbedarf besteht. Anders als ein herkömmlicher AV-Scanner verschiebt oder löscht LOKI keine Dateien, sondern überlässt dem Nutzer die Verantwortung, selbstständig auf Funde zu reagieren.

DIY-Signaturen

Man kann LOKI beibringen, neue Schädlinge zu erkennen, indem man neue Signaturen schreibt. Zum Beispiel kann man der Signaturdatenbank die IoCs hinzufügen, mit denen er den neuen Banking-Trojaner Karius findet.

Eine Websuche mit einer Stichwort-Kombination wie „IoC Karius banking trojan“ führt unter anderem zu einem Blogeintrag des Sicherheitssoftwareherstellers Check Point. Darin findet man als IoCs Dateinamen nebst Pfaden, Dateihashes und eine Domain, an die der Trojaner seine Datenbeute schickt:

```
injector32\64.exe
proxy32\64.dll
mod32\64.dll
728911a915d9ec3b6defa430d24bc0d5
857430b8c9dc78ce4eabbe57cb3ae134
http://proxyservice.site/updates/
↳gateway.php
```

Um diese IoCs der Signaturdatenbank hinzuzufügen, navigieren Sie in den Unterordner „iocs“. Dort befinden sich die Dateien „filename-iocs.txt“, „hash-iocs.txt“ und „c2-iocs.txt“. Aus ihnen bezieht LOKI die regulären Ausdrücke für den Pfad- und Dateinamen-Abgleich (filename-iocs.txt), die Schadcode-Hashes (hash-iocs.txt) und die Command-and-Control-Server-Adressen (c2-iocs.txt). Da LOKI diese Dateien bei jedem Signatur-Update mit aktualisierten Versionen überschreibt, empfiehlt es sich, für eigene Signaturen neue Dateien anzulegen. Damit der Scanner die darin enthaltenen Signaturen als solche erkennt, müssen die Dateinamen je nach Signaturtyp die Strings „filename“, „hash“ oder „c2“ enthalten. Legen Sie zum Ausprobieren beispielsweise die Dateien „my-filenames.txt“, „my-hashes.txt“ und my-c2.txt“ an.

In my-filenames.txt tragen Sie die Pfade und Dateinamen aus der Karius-Analyse ein. Darauf folgt ein Score, den LOKI zur Einschätzung des Bedrohungsgrads heranzieht. Ein Blick in LOKIs Quellcode verrät, dass Werte größer 40 für Warnings und größer 70 zu Alerts führen; Karius hat auf jeden Fall Letzteres verdient. Tippen Sie also Folgendes in eine eigene Zeile in my-filenames.txt:

```
injector32\\64\.exe;80
proxy32\\64\.dll;80
mod32\\64\.dll;80
```

Die Dateihashes fügen Sie in die Datei my-hashes.txt und die URL in my-c2.txt ein. Auch hier ist wieder wichtig, dass jeder IoC in einer eigenen Zeile steht. Dieses Mal folgt auf das Semikolon allerdings kein Score, sondern ein Kommentar, den LOKI bei der Erkennung ausgibt. Der Eintrag in my-c2.txt sieht zum Beispiel so aus:

```
http://proxyservice.site/updates/
↳gateway.php;Karius Banking Trojan
↳(https://research.checkpoint.com/
↳banking-trojans-development/)
```

Nach dem Speichern der Signaturdateien im IoC-Ordner fühlt LOKI dem Schädling erfolgreich auf den Zahn.

LOKI ermöglicht auch das Definieren von Ausnahmen. Gerade in größeren Unternehmen ist dies hilfreich, um viel genutzte Programme von vornherein von LOKIs Liste zu streichen. Der Ausschluss mittels Hashes erfolgt analog zu den „normalen“ Hash-IoCs über eine Datei, deren Namen den String „falsepositive“ enthält. Möchte man Dateinamen, Ordner oder komplette Pfade dauerhaft vom Scan ausschließen, editiert man die Datei „exclude.cfg“ im LOKI-Unterordner „config“.

Einfach ausprobieren

LOKI bietet viele Möglichkeiten, mit eigenen Signaturen herumzuexperimentieren. Ein vollständiger Systemscan kann mitunter recht zeitaufwendig sein; das trifft vor allem dann zu, wenn LOKI auf eine größere Zahl Memory Dumps oder SWF-Dateien stößt.

Mehr Speed verspricht Spark Core, Roths neuer, in Go programmierter Scanner. Er nutzt dieselbe (auch hier beliebig erweiterbare) Signaturdatenbank wie LOKI, ist aber nicht quelloffen, da es sich um die abgespeckte Gratis-Version eines kostenpflichtigen Produkts handelt. Über ct.de/yu72 finden Sie einen Vergleich der Fähigkeiten beider Scanner und haben die Möglichkeit, Spark Core herunterzuladen.

(ovw@ct.de) c't

LOKI-Download und weitere hilfreiche Links: ct.de/yu72