

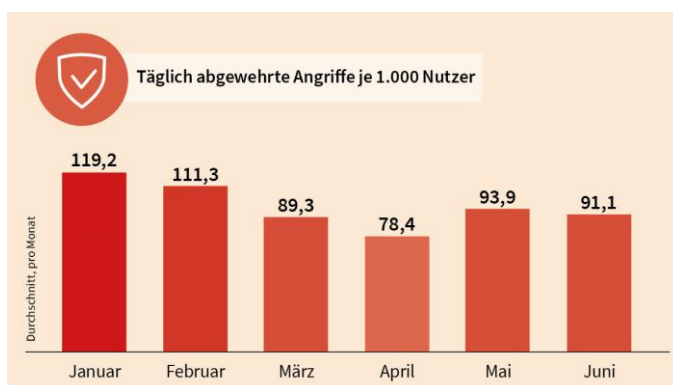
## G DATA Experten sehen illegales Cryptomining als neuen Trend

Deutscher IT-Sicherheits-Hersteller veröffentlicht Schadsoftware-Zahlen mit aktueller Top 10 der größten Bedrohungen im ersten Halbjahr 2018

Bochum (Deutschland), 30. August 2018

**Insgesamt haben die G DATA Analysten in den ersten sechs Monaten rund 2,4 Millionen neue Malware-Typen identifiziert. Die Bedrohungslage wandelt sich derzeit stark – neun der zehn meisterkannten Schädlinge aus dem vergangenen Jahr waren im ersten Halbjahr 2018 nicht mehr in den Top 10 vertreten. Ein Trend der Bösewichte 2018: Das heimliche und illegale Schürfen von Kryptowährungen – sogenanntes „Cryptomining“. Im G DATA Security Blog präsentieren die Experten diese und weitere Erkenntnisse..**

Schädlinge für den Windows-PC, die Kryptowährungen schürfen, sogenannte Miner, liegen nach aktuellen Analysen der G DATA Experten im Trend bei Cyberkriminellen. Diese Schadprogramme verstecken sich häufig auf Webseiten. Hierbei werden die Rechner von Besuchern dieser Seiten missbraucht, um einen finanziellen Gewinn für die Kriminellen zu erwirtschaften. Die Sicherheitsexperten des deutschen IT-Security-Herstellers G DATA haben in ihrer Analyse zum ersten Halbjahr 2018 festgestellt, dass dabei vor allem immer häufiger Webassembly, ein neuer Webstandard, von den Kriminellen ausgenutzt wird. Dieser Standard ist als Ergänzung zu Javascript gedacht, um eine schnellere Ausführung von Code zu erreichen. Genau diese Vorgehensweise ist ideal für Cryptominer.



### Aktuelle Top 10 der Bedrohungen für Nutzer

Nicht alle Cryptominer werden von G DATA als Schadprogramm eingestuft, da nicht immer eindeutig erkennbar ist, ob Nutzer dem Schürfen zugestimmt haben. Daher werden diese teils als Schädling, teils als „Potentiell unerwünschte Programme“ (PUP) kategorisiert. Unter den Top 10 der abgewehrten Malware-Bedrohungen finden sich gleich drei Miner, unter den Top 10 der abgewehrten PUP-Erkennungen sogar vier.

„Klassischerweise wurde Malware vor allem über ausführbare Dateien verbreitet“, sagt Ralf Benzmüller, Executive Speaker der G DATA Security Labs. „Wir sehen aber eine deutliche Zunahme webbasierter Angriffe, die zum Teil auch ganz ohne Dateien auskommen. Ebenfalls verbreitet sind Angriffe über Makros in Dokumenten, die Nutzer zur Interaktion auffordern.“

### Dateilose Schadsoftware nimmt zu

#### G DATA CyberDefense AG Unternehmenskommunikation

G DATA CyberDefense AG

G DATA Campus

Königsallee 178

44799 Bochum

[www.gdata.de](http://www.gdata.de)

E-Mail: [presse@gdata.de](mailto:presse@gdata.de)

Tel.: +49 (0) 234 9762-239

Fax: +49 (0) 234 9762-299

#### Pressemitteilung

Normalerweise hinterlassen Schaddateien Spuren auf den Festplatten des Rechners. Anders agiert sogenannte dateilose Malware. Diese Schadprogramme verstecken sich häufig auf präparierten Webseiten und nisten sich komplett im Arbeitsspeicher des attackierten Computers ein. Einmal im System können dateilose Schadprogramme die Benutzerrechte des aktuellen Anwenders ausnutzen. So können sensible Dateien gestohlen oder andere Schädlinge nachgeladen werden. Klassische Virens Scanner sind mit dem Aufspüren dieses Malwaretyps überfordert. Mit modernen Sicherheitslösungen und proaktiven Technologien, wie jenen von G DATA, sind Anwender umfassend geschützt. Derzeit sehen die G DATA Sicherheitsexperten einen weiteren Trend bei dieser Art von Schadprogramm.

#### **Jeden Tag 13.000 neue Malware-Samples**

Insgesamt haben die G DATA Security Labs 2.396.830 neue Samples als schädlich klassifiziert. Die Anzahl neuer Schadsoftware-Typen ist im ersten Halbjahr 2018 im Vergleich zum Vorjahr leicht rückläufig. Im Durchschnitt entdeckten die Analysten pro Minute etwa 9 neue Samples.

Der Artikel "[Malwarezahlen erstes Halbjahr 2018: Die Gefahr lauert im Web](#)" ist im G DATA Security Blog erhältlich.



#### **G DATA CyberDefense AG Unternehmenskommunikation**

G DATA CyberDefense AG

G DATA Campus

Königsallee 178

44799 Bochum

[www.gdata.de](http://www.gdata.de)

E-Mail: [presse@gdata.de](mailto:presse@gdata.de)

Tel.: +49 (0) 234 9762-239

Fax: +49 (0) 234 9762-299