Die Rückkehr der Miner-Botnetze

Kaspersky Lab warnt vor illegalen Botnetzen zum Schürfen von Kryptowährung

Moskau/Ingolstadt, 12. September 2017

Kaspersky Lab hat zwei Botnetze [1] identifiziert, über die auf Kosten der Opfer heimlich Kryptowährung wie Zcash oder Monero generiert wird. Die IT-Sicherheitsexperten von Kaspersky Lab entdeckten beispielsweise ein aus 4.000 Rechnern bestehendes Botnetz, das den Besitzern monatlich mehr als 30.000 US-Dollar, sowie ein Netzwerk mit 5.000 Rechnern, das den Hintermännern im Monat mehr als 200.000 US-Dollar einbringt.

Kryptowährungen boomen derzeit [2], die bekannteste Währung ist Bitcoin. Über legitime Mining-Programme können Einheiten (Coins) der Währungen gewonnen werden, mittlerweile allerdings nur sehr zeit- und stromintensiv [3]. Je mehr Coins also existieren, desto aufwendiger wird das ‚Mining' und die Investitionen übersteigen den potenziellen Gewinn. Dies ist bei Bitcoins der Fall. Rund um den Trend von Kryptowährungen entstehen allerdings auch Bitcoin-Alternativen, was wiederum die Aufmerksamkeit von Cyberkriminellen auf sich zog, die heimlich Mining-Software auf tausenden von Rechnern installieren.

Ein weiteres Ergebnis von Kaspersky Lab: Die Gefahr, Opfer eines heimlich installierten Kryptowährungs-Miner zu werden, steigt. Waren im Jahr 2013 lediglich 205.000 Nutzer [4] von dieser Gefahr betroffen, stieg die Anzahl der betroffenen User im Jahr 2014 bereits auf 701.000. Allein in den ersten acht Monaten dieses Jahres wuchs die Zahl der attackierten Nutzer auf 1,65 Millionen weltweit an.

„Das Hauptproblem mit bösartigen Minern ist, dass deren Aktivitäten nur schwer zu erkennen sind. Der Grund: Die Malware verwendet legale Mining-Software, die tatsächlich auch von einem legitimen Nutzer installiert werden könnte", so Evgeny Lopatin, Malware-Analyst bei Kaspersky Lab. „Schädliche Miner gewinnen auch zunehmend an Wert im Untergrundmarkt, was alarmierend ist. Denn wir haben Cyberkriminelle identifiziert, die sogenannte Miner-Builder anbieten, also Software zur Erstellung eines eigenen Mining-Botnetzes. Das bedeutet, die von uns identifizierten Botnetze werden wohl nicht die letzten gewesen sein."

Wie Miner-Botnetze funktionieren

Die von Kaspersky Lab identifizierten Miner-Botnetze bestehen aus mit Malware infizierten Rechnern, auf denen heimlich legitime Programme zum Generieren virtueller – auf der Blockchain-Technologie basierende – Währungen (Mining) installiert werden.

Laut den Experten von Kaspersky Lab verbreiten die Cyberkriminellen die Mining-Software mittels Adware-Programmen, die von den Opfern freiwillig installiert werden. Nach der Installation der

Adware wird dann automatisch die schädliche Komponente, der ‚Mining Installer', nachgeladen und installiert. Weitere Aktivitäten der schädlichen Komponente auf den Opfergeräten sind:

- der Versuch, Sicherheitssoftware zu deaktivieren;
- das Tracken aller Anwendungsstarts sowie das Aussetzen der eigenen Aktivität, sollte eine Programm zur Überwachung von Systemaktivitäten oder laufenden Prozessen gestartet werden;
- das Vorhandensein einer Kopie der Mining-Software auf der Festplatte, die im Falle des Löschens wieder hergestellt werden kann.

Sobald die ersten Kryptowährungs-Coins abgebaut sind, werden sie zu den Wallets der Kriminellen transferiert – unbemerkt vom Opfer, außer dass dessen Computer langsamer arbeitet und mehr Strom verbraucht als üblich. Die beiden derzeit am häufigsten von Kriminellen geschürften Kryptowährungen sind laut den Erkenntnissen von Kaspersky Lab Zcash [5] und Monero; beides Währungen, mit denen sich zuverlässig die Transaktionen und die Wallet-Besitzer anonymisieren lassen.

Lösungen von Kaspersky Lab entdecken und blockieren die maliziöse Mining-Software als Risk.Tool.Win32.BitCoinMiner.hxao und PDM:Trojan.Win32.Generic.

Die Analyse „Miners on the Rise" ist unter https://securelist.com/miners-on-the-rise/81706/ abrufbar.

[1] https://securelist.com/miners-on-the-rise/81706/

[2] http://www.spiegel.de/wirtschaft/unternehmen/bitcoin-kryptowaehrung-springt-auf-hoechststand-a-1146863.html

[3] https://www.btc-echo.de/tutorial/wie-kann-ich-bitcoins-minen/ oder https://www.heise.de/ct/artikel/Hardware-fuers-Mining-von-Bitcoins-und-Ethereum-3741094.html

[4] Kaspersky-Nutze die auf freiwilliger Basis am cloudbasierten Kaspersky Security Network (KSN teilnehmen. Die von Kaspersky Lab erhobenen Daten werden anonym und vertraulich behandelt. Es werden keine persönlichen Daten wie zum Beispiel Passwörter gesammelt. Über das KSN erhält Kaspersky Lab Informationen über Infizierungsversuche und Malware-Attacken. Die dabei gewonnenen Informationen helfen vor allem den Echtzeitschutz für Kaspersky-Kunden zu verbessern. Ausführliche Informationen über das KSN sind in einem Whitepaper aufgeführt, das unter http://www.kaspersky.com/images/KESB_Whitepaper_KSN_ENG_final.pdf abrufbar ist.

[5] https://securelist.com/zcash-or-the-return-of-malicious-miners/76862/

Nützliche Links:

- Kaspersky Blog „Miners on the Rise":https://securelist.com/miners-on-the-rise/81706/
- Heimanwenderlösungen von Kaspersky Lab: https://www.kaspersky.de/home-security#pc

Über Kaspersky Lab

Kaspersky Lab ist ein global agierendes Cybersicherheitsunternehmen, das im Jahr 2017 sein 20-jähriges Firmenjubiläum feiert. Die tiefgreifende Threat Intelligence sowie Sicherheitsexpertise von Kaspersky Lab ist Basis für Sicherheitslösungen und -Services zum Schutz von Unternehmen, kritischen Infrastrukturen, staatlichen Einrichtungen sowie Privatanwendern weltweit. Das umfassende Sicherheitsportfolio des Unternehmens beinhaltet führenden Endpoint-Schutz sowie eine Reihe spezialisierter Sicherheitslösungen und -Services zur Verteidigung vor komplexen und aufkommenden Cyberbedrohungen. Mehr als 400 Millionen Nutzer und 270.000 Unternehmenskunden werden von den Technologien von Kaspersky Lab geschützt.

Weitere Informationen zu Kaspersky Lab finden Sie unter http://www.kaspersky.com/de/. Kurzinformationen erhalten Sie zudem über www.twitter.com/Kaspersky_DACH und www.facebook.com/Kaspersky.Lab.DACH. Aktuelles zu Viren, Spyware, Spam sowie Informationen zu weiteren IT-Sicherheitsproblemen und -Trends sind unter https://de.securelist.com/ und auf dem Kaspersky-Blog auf http://blog.kaspersky.de/ abrufbar.

Redaktionskontakt:

Berkeley Kommunikation GmbH
Florian Schafroth
florian.schafroth@berkeley.global
Tel.: +49-89-7472-62-43
Fax: +49-89-7472-62-17
Landwehrstraße 61
80336 München

Kaspersky Labs GmbH
Stefan Rojacher
stefan.rojacher@kaspersky.com
Tel.: +49-841-98-189-325
Fax: +49-841-98-189-100
Despag-Straße 3
85055 Ingolstadt