LoJax Erster UEFI-Virus entdeckt

27.09.2018, 12:26 Uhr

UEFI-Viren waren bisher eher eine Art Labor-Experiment. Jetzt ist der erste Virus dieser Art im Internet aufgetaucht. COMPUTER BILD verrät, warum der so gefährlich ist und was Sie tun können.

Achtung: Eine Hackergruppe macht mit dem ersten UEFI-Virus das Internet unsicher!

Das Sicherheitsunternehmen Eset hat erstmals einen UEFI-Virus in freier Wildbahn entdeckt. Diese Viren sind extrem gefährlich und es gibt kaum Schutzmöglichkeiten dagegen. Betroffen sind alle Computer ab 2006, die die sogenannte LowJack-Technologie einsetzen. Das sind unter anderem alle Notebooks der vergangenen Jahre. COMPUTER BILD erklärt, warum der Virus so gefährlich ist und wie Sie sich dagegen schützen.

LoJax: Extrem gefährlicher UEFI-Virus greift an

UEFI ist der Nachfolger vom BIOS und befindet sich in einem Chip auf dem Mainboard. Ein Virus, der sich dort einnistet, übersteht selbst den Wechsel einer Festplatte und wird aktiv, bevor das Betriebssystem sowie darauf laufende Schutzprogramme starten. Er kann also in der Regel ungehindert wüten und beispielsweise den gesamten Datenverkehr des PCs umleiten oder die Kontrolle darüber übernehmen. Thomas Uhlemann, Security Specialist bei ESET Deutschland, sagt dazu: „Die von uns entdeckte Kampagne stellt eine neue Dimension der Cyberangriffe dar. Malware, die selbst das Austauschen der Festplatte übersteht, ist potentiell eine Gefahr für alle User, da sie selten in der Hand nur einer Gangstergruppe bleibt. Die Anwender sind jetzt aufgerufen, auch zukünftig regelmäßig zu prüfen, ob Aktualisierungen für das BIOS oder das UEFI bereitstehen und diese auch zeitnah einzuspielen.“ Bisher waren UEFI-Viren eher ein wissenschaftliches Experiment, das zeigen sollte, dass solche Schädlinge möglich sind. Nun ist mit LoJax aber der erste dieser extrem gefährlichen Viren in der freien Wildbahn gesichtet worden. Die meisten PCs sind diesem Virus ungeschützt ausgeliefert!

Bisher nur gezielte Angriffe

Die Sicherheitsexperten von Eset haben den neuen Schädling bisher nur auf sehr wenigen PCs gefunden, die hauptsächlich zu Regierungsorganisationen im Balkan, in Mittel- und in

Osteuropa gehören. Von einer akuten Gefahr für die Masse ist daher vorerst nicht auszugehen. Allerdings tauschen Hackergruppen häufig Code-Schnipsel aus. Es ist also durchaus möglich, dass bald ein großangelegter Angriff mit Erpresserviren kommt, die sich im UEFI-Speicher festsetzen.

Bekannte Hackergruppe steckt hinter dem Virus

Wie Eset herausfand, steckt hinter dem noch laufenden Angriff die Hackergruppe Sednit (auch bekannt als APT28, Sofacy oder Fancy Bears). Diese vermutlich staatliche Hackergruppe ist extrem gut organisiert und wahrscheinlich auch für den Bundesnetz-Hack im vergangenen Jahr verantwortlich.

LoJax war ursprünglich Diebstahlschutz

LoJax ist eine manipulierte Version des Diebstahlschutzes LoJack. Dieser sollte selbst die Neuinstallation des Betriebssystems überstehen, weshalb die Hersteller ein BIOS/UEFi-Module gebaut haben, das von vielen Hardware-Herstellern als Teil der vorinstallierten Firmware an die Endkunden geliefert wurde. Den Diebstahlschutz LoJack gibt es immer noch und an der aktuellen Version ist auch nichts auszusetzen. Der Schädling LoJax basiert auf einer alten Version dieser Software, die von Hackern für ihre Bedürfnisse verändert wurde.

Jetzt müssen Hersteller reagieren

Die neue Schädlingsart macht es notwendig, dass Hersteller reagieren. Hersteller von Schutzprogrammen müssen eine Möglichkeit finden, das UEFI auch zu schützen, nicht nur Infektionen darauf zu erkennen. Und Hardware-Hersteller müssen Sicherheitslücken schließen sowie Firmware-Updates bereitstellen und zwar so, dass normale Nutzer auch benachrichtigt werden und nicht nach diesen Updates suchen müssen. Denn die Vergangenheit hat schon mehrfach gezeigt: Wenn ein Schädling eine raffinierte Angriffs- oder Verbreitungsmöglichkeit nutzt, tun das bald sehr viele – und darauf müssen die PCs der Nutzer vorbereitet sein!

So schützen Sie sich vor LoJax

Die einzige Möglichkeit, eine Infektion mit LoJax zu erkennen, ist ein UEFI-Scanner. Bisher gibt es den nur in den Schutzprogrammen von Eset, andere Hersteller ziehen nun – da es eine echte Bedrohung dieser Art gibt – sicher bald nach. Ist der PC erst einmal mit einem UEFI-Virus infiziert, lässt dieser sich nur noch durch Profis entfernen. Sie sollten daher alles dafür tun, dass das nicht passiert. So beugen Sie einer UEFI-Infektion vor:

1. SecureBoot: Wenn SecureBoot aktiv ist, kann nur signierte Firmware starten. Das sind Viren normalerweise nicht, da es extrem aufwendig ist, eine solche Signierung zu fälschen. Sie sollten daher unbedingt SecureBoot aktivieren. Wie genau Sie das machen, erklären die BIOS- und UEFI-Tipps.
2. Firmware-Updates: Bisher erscheinen zwar nur sehr selten UEFI-Firmware-Updates, schauen Sie aber trotzdem einmal beim Hersteller Ihres PCs nach, ob es für Ihr Gerät welche gibt. Falls ja, installieren Sie sie. Sofern die neue Firmware dabei die bisherige Firmware komplett überschreibt und nicht nur Kleinigkeiten aktualisiert, kann die Installation eventuell sogar UEFI-Viren überschreiben und damit entfernen.