Newsletter Juni 2023

- Gefährliche Hardware
- Gefährliche Software
- Neues von den Domains: .bo, .lc, .hiphop, .lt, .web und .zip

Gefährliche Hardware

Der Einbruch beim Mainboardhersteller MSI hat das Unternehmen bereits empfindlich getroffen. Nun ist zusätzlich klar, dass es auch Auswirkungen auf Besitzer von MSI Hardware gibt. Unter den geklauten Daten befand sich auch der private digitale Schlüssel für Firmware-Updates. Dadurch ist es den Einbrechern möglich Firmware-Updates zu erstellen, die das entsprechende Mainboard als authentisch ansieht. Hacker könnten so versuchen, Rechnern vergiftete Updates unterzujubeln, die letztlich einen Vollzugriff auf das gesamte System ermöglichen.
Gegen diese Gefahr hilft nur der Austausch entsprechender Boards. Betroffen ist nicht nur MSI, sondern auch die Partner Lenovo und Supermicro, und das sowohl mit deren Endanwender-Systemen als auch Servern.
Ähnlich wie bei den schweren Prozessor-Sicherheitslücken Spectre und Meltdown aus dem Jahr 2017, müssen sich die Hardwarebesitzer nun fragen, ob sie mit dem Risiko leben können oder eigentlich funktionierende Geräte durch neue ersetzen.
Generell zeigt sich wieder einmal, dass es einigen Aufwand bedeutet, Betriebsgeheimnisse zu schützen. Der private Schlüssel war offensichtlich online verfügbar, sonst wäre er nicht Teil der Beute geworden. Theoretisch wäre es möglich gewesen, den Schlüssel nur auf einem nicht mit dem Internet verbundenen System vorzuhalten und die jeweiligen Firmwares dort zu signieren. MSI war das scheinbar zu mühsam. Die Zeche dafür bezahlen jetzt die Kunden.

Gefährliche Software

Google wirbt für seinen Play Store auch damit, dass die dort veröffentlichen Apps geprüft wurden und man grundsätzlich davon ausgehe, dass sie frei von Schadsoftware sind.
Soweit der Anspruch. Die Analysten von Dr. Web malen ein anderes Bild von der Realität. Ihnen gelang es, die Spionagesoftware SpinOK zu enttarnen. Bei SpinOK handelt es sich vordergründig um einen Hilfsbaustein für App-Programmierer, der diesen ermöglicht, die App-Nutzer bei der Stange zu halten, etwa durch Gewinnversprechen oder Minispiele. Für viele App-Anbieter sind solche Funktionen essenziell, da sich fast nur noch Geld damit verdienen lässt, Apps erst einmal kostenlos zu veröfffentlichen und dann Werbung auszuspielen oder Zusatzfunktionen als kostenpflichtige Erweiterung anzubieten. Dazu verlassen sich Programmierer meist auf Zusatzbausteine wie das besagte SpinOK.
Deren Macher konnten offenbar eine dreistellige Anzahl von Entwicklern von den eigenen Qualitäten überzeugen. Die erfolgreichsten SpinOK-Apps sind dabei der Videoeditor Noizz und das Datentransfertool Zapya, die jeweils mehr als 100 Millionen Downloads aufweisen.
Insgesamt kommt SpinOK auf etwa eine halbe Milliarde Downloads.

Neues von den Domains

.bo

Die bolivianische Registry weist darauf hin, dass Domains nur dann für Glücksspiele genutzt werden können, wenn die staatliche Glücksspielbehörde dem Domaininhaber eine entsprechende Lizenz erteilt hat.

.ec

Ecuador lockt mit einer ungewöhnlichen Rabattaktion. Im Juni registrierte .ec Domains kosten im 2. Jahr nur die Hälfte. Der Erst- und Folgejahrespreis bleibt allerdings bestehen.

.hiphop

Manche TLDs haben eine merkwürdige Reise hinter sich. Einst hatte GoDaddy .hiphop und alle weiteren Uniregistry TLDs aus dem Programm genommen, da man mit der irrationalen Preispolitik von Uniregistry nicht einverstanden war. Nun ist GoDaddy selbst Besitzer von .hiphop und kann damit den eigenen Anspruch an nachvollziehbare Preisentwicklungen selbst umsetzen.

.lt

Litauen passt sich internationalen Gepflogenheiten an und nutzt ab sofort Authinfos für den Transfer von Domains. Für bereits bestehende Domains wurde eine zufällige Authinfo automatisiert eingerichtet, so dass die Sicherheit für Altbesitzer gewährleistet bleibt.

.web

Das Gezerre um die am heißesten umkämpfte neue Domainendung scheint dem Ende zuzugehen. ICANN hat final entschieden, dass Verisign nicht gegen die Bewerbungsrichtlinien verstoßen hat, indem sie das Quasi-Subunternehmen NDC einen Antrag auf .web haben stellen lassen. Dabei hatte Verisign seine Verbindung zu .web verschwiegen. Andere .web Bewerber, insbesondere Afilias, fühlten sich dadurch getäuscht. Dieses sei aber irrelevant für die Zuteilung an NDC / Verisign.
Durch die Einwände der konkurrierenden Bewerber hat sich die Einführung von .web bereits jetzt um 9 Jahre verzögert. Die Erwartungen an die TLD sind entsprechend hoch. Noch gibt es aber keine konkreten Termine für den Start. Vormerkungen nehmen wir trotzdem bereits entgegen.

.zip

Viele haben befürchtet, dass Googles neue Domainendung aufgrund der Übereinstimmung mit der populären Dateiendung von Betrügern genutzt werden wird, um Nutzer zu verwirren und ihnen bösartige Software unterzujubeln. Diese Befürchtungen scheinen sich bereits kurz nach der Einführung zu bestätigen. Sicherheitsforscher haben analysiert, dass sehr viele der Registrierungen aussehen wie Updates, Dateianhänge oder Mitarbeiterinformationen. Weiterhin gibt es Domains, die nach bekannten offiziellen Formularen benannt sind.
Warum der Google Konzern, der viel Geld in Internetsicherheit investiert, sich zu so einem Schritt entschlossen hat, ist schwer nachvollziehbar. Nicht wenige der .zip Domains sind mittlerweile auf der hauseigenen Google Safe Browsing Liste gelandet, die gefährliche Webseiten brandmarkt.

Mit freundlichen Grüßen,

Ihr Global Village Team