



## **Comeback des USB-Wurms? Neue Variante überquert gleich drei Kontinente**

*Die längst verstaubt geglaubte Masche des „Ich lasse mal einen USB-Stick mit Schadsoftware auf Parkplätzen zum Mitnehmen herumliegen“ wurde doch tatsächlich noch einmal aus der Cybercrime-Kiste geholt. Der bekannte Wurm PlugX tauchte in Nigeria, Ghana, Simbabwe und der Mongolei in einer neuen Variante auf.*

16.000 Kilometer voneinander entfernt treten die derzeitigen Ausbrüche einer neuen Art des PlugX-USB-Wurms auf: nach dem erstmaligen Auftauchen in Papua-Neuguinea im August 2022 poppten immer mehr Infektionen in Ghana, der Mongolei, Simbabwe und Nigeria hoch. Die Verbreitung über eine derartig große Distanz ist sehr ungewöhnlich.

### **So geht die neue Wurm-Version vor:**

Die neue Version, die Sophos X-Ops entdeckt hat, verbreitet sich über USB-Laufwerke und nutzt eine legitime ausführbare Datei, die sie in das Zielnetzwerk einschleust. Anschließend versteckt sie sich in einem gefälschten Verzeichnis namens "RECYLER.BIN", das dank einer zusätzlichen Verschleierung durch die Cyberkriminellen von Windows mit dem echten Windows-Papierkorb assoziiert wird. Der Wurm kopiert dann Dateien aus dem infizierten Netzwerk auf das USB-Laufwerk.

### **Weltweites Comeback des USB-Wurms?**



Die längst veraltet geglaubte USB-Malware-Verbreitung ist nicht totzukriegen: bereits im letzten Jahr hatte Sophos eine Anhäufung dieser Aktivität bemerkt. Der Wurm PlugX treibt seit mindestens 2008 sein Unwesen, sein Ursprung wird in der Sicherheitsszene übereinstimmend der Hacker-Gruppierung MustangPanda zugeordnet, eine Angreiferbande die mit chinesischer, staatlich geförderter Cyberspionage-Aktivität in Verbindung gebracht wird.

Gabor Szappanos, Threat Research Director, Sophos, über das Revival des USB-Wurms: „Im November vergangenen Jahres berichteten wir über verschiedene Verdichtungen aktiver feindlicher Aktivitäten gegen Regierungseinrichtungen in Südostasien, die sich ebenfalls dieser Retro-Methode via USB-Laufwerke bedienten. Der Wurm tauchte schließlich einen Monat später Tausende von Kilometern entfernt in Afrika auf. Nun umfasst diese erneute Anhäufung von USB-Wurm-Aktivitäten drei Kontinente. Im Vergleich zu internetbasierten Attacken halten wir Wechselmedien nicht für besonders mobil, aber diese Verbreitungsmethode hat sich in diesen Teilen der Welt als sehr effektiv erwiesen. Es existieren zahlreiche Akteure mit sehr unterschiedlichen Interessen, die sich der Vorteile eines USB-Sticks bedienen, uns scheint hier aber vor allem die Gruppierung MustangPanda der Drahtzieher zu sein. Ein Comeback des USB-Wurms auszurufen ist vielleicht zu früh, aber es ist ganz sicher keine ausgediente Technik von vor zehn oder zwanzig Jahren. Einige bekannte Bedrohungsakteure setzen weiterhin auf die Vorteile von USB, um ihre Schadsoftware zu verbreiten.“

Der ausführliche Artikel mit technischen Details steht auf dem Sophos News Blog bereit: [„A border-hopping PlugX USB worm takes its act on the road“](#).

## **Social Media von Sophos für die Presse**

Wir haben speziell für Sie als Journalist\*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.

Folgen Sie uns auf  und 

LinkedIn: <https://www.linkedin.com/groups/9054356/>

Twitter: @sophos\_info

## **Pressekontakt:**

Sophos

Jörg Schindler, PR-Manager Central & Eastern Europe

[joerg.schindler@sophos.com](mailto:joerg.schindler@sophos.com), +49-721-25516-263

TC Communications

Arno Lücht, +49-8081-954619

Thilo Christ, +49-8081-954617

Ulrike Masztalerz, +49-30-55248198