

Aktuelle Warnung: Microsoft-signierte Malware ermöglicht gezielte Manipulation des Datenverkehrs

Bochum (Deutschland), 21. Juni 2021

Die Security-Experten*innen von G DATA haben ein Netzwerk-Rootkit entdeckt, das Netzwerkanfragen auf einen Server mit einer chinesischen IP-Adresse umleitet. Damit ist es möglich, den Datenverkehr gezielt zu manipulieren. Ein Rootkit ermöglicht es einem Angreifer unter anderem, schädliche Aktivitäten effektiv vor dem Nutzer zu verstecken. Besonders brisant: Die Schadsoftware gibt sich als Netzwerktreiber aus und ist Mitte Mai 2021 von Microsoft mit einem gültigen Zertifikat signiert worden. Ein weiterer Treiber mit zahlreichen Parallelen zur vorliegenden Datei wurde bereits im März signiert.



„Wir waren erst unsicher, ob die Datei wirklich schädlich ist und glaubten an eine falschpositive Erkennung. Stutzig wurden wir deshalb, weil Netzwerktreiber eigentlich nicht ihren eigenen Code verschleiern. Das ist eine Taktik, die häufig bei Malware verwendet wird, um die Erkennung durch Sicherheitslösungen zu erschweren“, sagt Karsten Hahn, Virus Analyst bei G DATA CyberDefense AG.

Information für Forscherkolleg*innen

115034373fc0ec8f75fb075b7a7011b603259ecc0aca271445e559b5404a1406
04e88b7717aadc6b56dfa006b9414fc2c899c398d7e003627770e07fed52edfd
4a229ab274e364df92cc46ecbc9faab32f7b0955dab982658313f2faf9410863
63d61549030fcf46ff1dc138122580b4364f0fe99e6b068bc6a3d6903656aff0
659e0d1b2405cadfa560fe648cbf6866720dd40bb6f4081d3dce2dffe20595d9
6c856c3c315c0f213684045da3203692c07c3da5df755155fd8b128fb447c437
8249e9c0ac0840a36d9a5b9ff3e217198a2f533159acd4bf3d9b0132cc079870
9804787b31e0025dd2ae9344ca1beae2e701cdf8fd77a60f424295dc9280dc89
a3e8ea5e593176f9e66c17f6a200fa665c7ef409c97f49aadf5a55ad6b0be97e
a5c873085f36f69f29bb8895eb199d42ce86b16da62c56680917149b97e6dac4
b16c3ed44cd04b033621ada7f9ab89d830949b3c9dc26999d862ddbeb7cc5a8
6bbc58fd69ce5fed6691dd8d2084e9b728add808ffd5ea8b42ac284b686f77d9
abff9b75ae2eea49a765f79d9c67c997edb6c67a2cc720c6187dd2f67980acab7
cb8e536680732b474a5c26970ace2087667622caa3dd82c1c56731a7c5a1c8ce
d0a03a8905c4f695843bc4e9f2dd062b8fd7b0b00103236b5187ff3730750540
d64f906376f21677d0585e93dae8b36248f94be7091b01fd1d4381916a326afe
e0afb8b937a5907f9e55a1d1cc7574e9304007ef33fa80ff3896e997a1beaf37
f83c357106a7d1d055b5cb75c8414aa3219354deb16ae9ee7efe8ee4c8c670ca

G DATA CyberDefense AG Unternehmenskommunikation

G DATA CyberDefense AG

G DATA Campus

Königsallee 178

44799 Bochum

www.gdata.de

E-Mail: presse@gdata.de

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

Fax: +49 (0) 234 9762-299