

Malware-Top-10 2019: Angriffe im Sekunden-takt

Neun neue Malware-Samples pro Minute bedrohen PCs und Netzwerke

Bochum (Deutschland), 23. Januar 2020

Mehr als 4,9 Millionen Malware-Samples haben die Cyber-Defense-Spezialisten von G DATA 2019 identifiziert. Das Ziel der Cyberkriminellen: Passwörter und vertrauliche Daten auslesen oder Daten und Systeme verschlüsseln. Die zehn aktivsten Malware-Familien hat G DATA in der aktuellen Jahres-Top-Ten zusammengestellt.

„Die Technik der Antiviren-Hersteller wird immer besser und identifiziert tägliche neue Angriffe auf Unternehmensnetzwerke oder private PCs und Laptops“, sagt Tim Berghoff, Security Evangelist bei der G DATA CyberDefense AG. „Daher sind Malware-Autoren gezwungen, ihre Schadsoftware mit raffinierten Methoden vor der Entdeckung durch Schutzprogramme zu schützen – ein ewiges Katz-und-Maus-Spiel.“

Allerdings gelingt dies nicht immer. Im letzten Jahr entdeckten die Experten von G DATA pro Tag mehr als 13.500 Varianten von bekannten Malware-Familien. Am aktivsten war mit Abstand die Ransomware „GandCrab“: Über 408.000 Versionen identifizierten die Malware-Analysten in Bochum – durchschnittlich mehr als 1.100 neue Varianten pro Tag. Die Ransomware verschlüsselt Daten und Netzwerke und fordert von den Nutzern Lösegeld. Erst dann lassen sich die Daten wieder entschlüsseln. Allerdings hat die Gruppe hinter der Malware bereits zum 1. Juni 2019 ihre Aktivitäten offiziell beendet.

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



Aber anscheinend ist das System noch aktiv und verbreitet weiter den schädlichen Code. Auf den Plätzen zwei und drei folgen „hjrAT“ mit 208.000 und „BlackShades“ mit 193.000 Versionen. Beide gehören zu der Gruppe von „Remote Access Trojaner“, mit denen Cyber-Kriminelle die administrative Kontrolle auf dem Zielsystem übernehmen. Die bekannteste Malware-Familie „Emotet“ landet in den Jahrescharts auf Platz sechs – mit über 70.800 verschiedenen Samples. Durchschnittlich 194 neue Versionen der Allzweckwaffe des Cybercrime erschienen pro Tag. Dabei fungiert Emotet nur als Türöffner und verschafft Cyberkriminellen Zugang zu den IT-Netzwerken. Zum Vergleich: Im Vorjahreszeitraum entdeckten die Malware-Analysten rund 28.000 neue Varianten.

Die Malware-Top 10 im Überblick:

Platz	Name	Varianten	Art
1	GandCrab	408.182	Ransomware
2	njRAT	208.235	Remote Access Trojaner
3	BlackShades	193.105	Remote Access Trojaner
4	Tinba	127.589	Banking-Trojaner
5	AveMariaRAT	102.374	Remote Access Trojaner
6	Emotet	70.833	Malware Distributor
7	Shifu	61.225	Banking-Trojaner
8	AZORult	60.834	Information-Stealer
9	SakulaRAT	53.799	Remote Access Trojaner
10	Nanocore	50.535	Remote Access Trojaner

G DATA CyberDefense AG
Unternehmenskommunikation

G DATA CyberDefense AG

G DATA Campus

Königsallee 178

44799 Bochum

www.gdata.deE-Mail: presse@gdata.de

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

Fax: +49 (0) 234 9762-299

Informationen stehlen, Systeme verschlüsseln

Fünf der zehn aktivsten Malware-Familien sind Remote Access Trojaner (RAT). Das bedeutet: Die Schadsoftware ermöglicht eine vom Nutzer unbemerkte Fernsteuerung und administrative Kontrolle eines fremden Rechners. Die Manipulationsmöglichkeiten reichen vom Ausspähen von Passwörtern über das Auslesen vertraulicher Daten bis zum Löschen der Festplatte oder Verschlüsselung von Dateien. Immer noch aktiv sind auch Banking-Trojaner wie „Tinba“ oder „Shifu“. Sie nutzen die „Man-in-The-Browser“-Technik, um Login-Daten für Banking-Applikation auszulesen.

Auffällig ist, dass ein Großteil der Malware schon seit mehreren Jahren im Umlauf ist. So wurden SakulaRAT und Tinba bereits 2012 erstmals entdeckt, Nanocore im Jahr 2013. Dies hängt auch mit den Verschleiertechniken der Cyberkriminellen zusammen, mit denen sie die Schadsoftware tarnen. Die jüngste Malware in den Top 10 ist AveMariaRAT. Diesen RAT identifizierten Sicherheitsforscher im Jahr 2018 zum ersten Mal. Insgesamt sind aktuell 332 unterschiedliche Malware-Familien in den Datenbanken von G DATA klassifiziert.

Emotet und kein Ende

Zum Jahresende hat der ehemalige Banking-Trojaner Emotet wieder von sich reden gemacht. Nachdem es zur Jahresmitte 2019 ruhig um die „Allzweckwaffe des Cybercrime“ geworden war, sind die Cyberkriminellen seit dem Herbst wieder deutlich aktiver geworden. In Deutschland waren unter anderem öffentliche Verwaltungen, Hochschulen und wieder einmal Kliniken Opfer der ausgeklügelten Angriffe. „Die initialen Spam-Mails sehen sehr authentisch aus, sodass viele Nutzer diese für echt halten und den infizierten Anhang öffnen“, sagt Tim Berghoff. „Die Nutzer klicken dann auf den infizierten Anhang und das Unheil nimmt seinen Lauf.“ Die Malware lädt automatisiert andere Schadprogramme wie Trickbot und Ryuk nach, um weitere Zugangsdaten auszuspähen und das System zu verschlüsseln. Emotet funktioniert sogar Powershell um und nutzt es als schädliche Funktion. Die Folge: Betroffene Unternehmen und Verwaltungen waren tagelang ohne IT und offline.