

G DATA Bedrohungsanalyse 2020: Cyberattacken im Sekundentakt

Zahl der abgewehrten Cyberattacken stieg vom ersten zum zweiten Halbjahr um mehr als 85 Prozent

Bochum (Deutschland), 16. Februar 2021

Die Pandemie bleibt ein Fest für Kriminelle – Sie nutzen die Verunsicherung der Menschen für Angriffe aus. Laut der aktuellen Bedrohungsanalyse von G DATA CyberDefense stieg die Zahl der abgewehrten Angriffsversuche im zweiten Halbjahr 2020 um 85 Prozent. Pro Minute haben Cyberkriminelle im vergangenen Jahr 76 neue Versionen einer Schadsoftware veröffentlicht. Auch Sicherheitslücken wie Shitrix und Sunburst haben den Angreifern gute Dienste für ihr schädliches Treiben geleistet.

Die Gefahr durch Cyberattacken hat sich auch im vergangenen Jahr weiter signifikant erhöht. Die aktuelle Bedrohungsanalyse von G DATA CyberDefense zeigt, dass sich die Zahl der abgewehrten Angriffsversuche innerhalb von sechs Monaten um mehr als 85 Prozent erhöht hat – im Vergleich vom ersten zum zweiten Halbjahr 2020. Hatte sich die Zahl der verhinderten Attacken vom zweiten auf das dritte Quartal noch nahezu verdoppelt, war die Zahl der Angriffe im vierten Quartal leicht rückläufig

„Wir gehen davon aus, dass im vergangenen Jahr zahlreiche Unternehmen auf Grund des hastigen Umzugs ins Homeoffice einem Angriff zum Opfer gefallen sind - dies aber noch nicht gemerkt haben. Cyberkriminelle nutzen nach wie vor jegliche Schwäche in der IT-Sicherheit gnadenlos aus. Kritische Sicherheitslücken, fehlende Updates oder unvorsichtige Angestellte stehen meist am Anfang einer erfolgreichen Attacke. Und die aktuell bestehende Verunsicherung der Menschen beschleunigt die Entwicklung erheblich“, sagt Tim Berghoff, Security Evangelist bei G DATA CyberDefense AG.

Alte Malware im neuen Gewand

Auffällig ist, dass Cyberkriminelle auf bewährte Schadsoftware setzen, die zum Teil schon seit mehreren Jahren im Einsatz ist, aber ständig weiterentwickelt wird. Wie groß die Gefahr an dieser Stelle ist, belegt folgende Zahl: Mehr als 16,1 Mio. verschiedene Malware-Samples entdeckten die Cyber-Defense-Experten von G DATA. Gegenüber dem Vorjahr ein Anstieg von 228,6 Prozent. Pro Tag bedrohen durchschnittlich 44.135 neue Malware-Samples IT-Systeme in Deutschland. Heißt: Pro Minute veröffentlichten Cyberkriminelle 76 neue Versionen einer Schadsoftware.

Erstmals lag Emotet, die Allzweckwaffe des Cybercrime, nicht nur in der Gefährlichkeit vorn, sondern auch in der Anzahl verbreiteter Samples: mit insgesamt 888.793 verschiedenen Versionen. Im gesamten Vorjahr waren es lediglich 70.833 Samples – ein Anstieg um 1.154,8 Prozent. Dabei war Emotet in der ersten Jahreshälfte weitgehend inaktiv, sodass in diesem Zeitraum nur 27.804 neue Samples auftauchten. Mehr als 860.000 Versionen stammen also aus dem zweiten Halbjahr. Anders gesagt: Pro Minute haben die Kriminellen drei neue Varianten veröffentlicht. Dabei fungiert Emotet als Türöffner und verschafft Cyberkriminellen Zugang zu den IT-Netzwerken. Die Malware lädt automatisiert andere Schadprogramme wie Trickbot und Ryuk nach, um weitere Zugangsdaten auszuspähen und das System zu verschlüsseln.

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

Platz	Name	Varianten	Art
1 (6)	Emotet	888.793	Malware Distributor
2 (-)	QBot	98.800	Remote Access Trojaner
3 (-)	Urelas	64.136	Downloader
4 (2)	njRAT	63.969	Remote Access Trojaner
5 (10)	NanoCore	52.736	Remote Access Trojaner
6 (-)	Trickbot	50.043	Malware Distributor
7 (-)	AgentTesla	47.739	Information-Stealer
8 (-)	RemcosRAT	43.902	Remote Access Trojaner
9 (-)	Dridex	43.583	Malware Distributor
10 (7)	Shifu	36.892	Banking-Trojaner
Vorjahresplatzierung in Klammern			

Wie dynamisch sich Cybercrime entwickelt, wird deutlich, dass sechs der zehn Bedrohungen neu in der Übersicht sind. Weit abgeschlagen hinter Emotet folgen QBot und Urelas. Dabei nutzt Qbot aktuell ein Angriffsmuster, das bis jetzt nur von Emotet bekannt war. Die Angreifer senden bei einer bereits bestehenden Mail-Konversation eine gefälschte Antwort. Für den Empfänger ist diese falsche Mail kaum von einer legitimen Nachricht zu unterscheiden, sodass die Opfer den Mailanhang öffnen oder den Link anklicken. Der ursprüngliche Banking-Trojaner besitzt zusätzlich Wurmelemente und ist als Credential Stealer aktiv, um Anmeldedaten von Anwendern zu kopieren. Somit ist auch Qbot eine Allzweckwaffe für Cyberkriminelle. Auf Platz drei der Malware-Top-10 findet sich der Downloader Urelas, mit dem Angreifer weitere Schadsoftware nachladen, sobald sie ein System infiltriert haben.

Der König ist tot – lang lebe ... ja, wer eigentlich?

Gerade im Bereich dieser digitalen Türöffner ist 2021 einiges an Bewegung zu erwarten. Den Ende Januar gab es einen international koordinierten Schlag gegen die Betreiber von Emotet, der jahrelang als "König der Schadsoftware" betitelt wurde. Große Teile der Infrastruktur hinter Emotet wurde – unter anderem mit technischer Unterstützung durch G DATA außer Gefecht gesetzt. Das dürfte zumindest mittelfristig eine Marktlücke im Untergrund hinterlassen, um deren Füllung sich nun andere Tätergruppen bemühen.

Lücken mit schwerwiegenden Folgen

Aber nicht nur gut getarnte Malware öffnen Angreifern die Tür zu privaten Rechnern oder Unternehmensnetzwerken. Wie jedes Jahr machen es auch zahlreiche Sicherheitslücken in Anwendungen und Betriebssystemen Angreifern leicht, IT-Systeme zu infiltrieren. Zwei der größten seien hier stellvertretend genannt: Shitrix und Sunburst. Shitrix zählte zu den gefährlichsten Lücken der vergangenen Jahre, die in Citrix ADC das Ausführen von beliebigen Anwendungen aus der Ferne möglich machte. Und war damit als hoch kritisch einzustufen. Alleine in Deutschland waren mehr als 5.000 Unternehmen gefährdet, darunter auch Betreiber kritischer Infrastrukturen wie Krankenhäuser, Energieversorger oder Behörden.

Zum Jahresende mussten Regierungsbehörden und Privatunternehmen feststellen, dass ihre Netzwerke kompromittiert waren. Der Ursprung lag in der Netzwerkverwaltungssoftware des Herstellers SolarWinds. Über Monate hinweg haben Kriminelle unbemerkt von außen immer neue Einzelkomponenten zu einer Spionagesoftware zusammengefügt, die fest in die Netzwerkverwaltung integriert wurde. Die verseuchten Software-Updates erregten keinen Verdacht und wurden in zahlreichen Unternehmen weltweit

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

Pressemitteilung

installiert. Die Angriffe waren vor allem auf die USA konzentriert, aber auch in Deutschland gab es verwundbare Systeme.

„Der Kampf gegen Cyberkriminelle erfordert von Unternehmen und Privatanwendern ein entschlossenes Vorgehen. Denn auch Cyberkriminelle nutzen den aktuellen Digitalisierungsschub für sich aus und verstärken ihre Angriffsbemühungen. Dabei setzen sie auch auf automatisierte Attacken, um Netzwerke zu infiltrieren. Wer jetzt nicht in IT-Sicherheit investiert, der verspielt seine Digitalisierungsdividende leichtfertig“, sagt Tim Berghoff, Security Evangelist bei G DATA CyberDefense AG.

Unternehmen müssen sich auf immer raffiniertere Attacken einstellen, denn mit Malware-as-a-Service führen Kriminelle komplexe Angriffe durch, die nur schwer zu verteidigen sind. Hier braucht es nicht nur eine zeitgemäße Endpoint Protection, sondern auch aufmerksame Angestellte, die durch umsichtiges Handeln Angriffsversuche im Keim ersticken können.



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