Cyberkriminelle haben Corona-Weichen gestellt - ESET veröffentlicht Threat Report für das zweite Quartal 2020

Die Corona-Pandemie hat auch ein halbes Jahr nach dem Ausbruch das Arbeits- und Privatleben fest im Griff. Die ESET-Forscher sehen in den Aktivitäten der Kriminellen, dass sie sich auf die Situation eingestellt haben. Insbesondere Web- und E-Mail-Attacken haben stark zugenommen. Ein weiteres beliebtes Ziel: Das Remote Desktop Protokoll (RDP) von Microsoft. Gerade Mitarbeiter, die von zu Hause aus arbeiten, greifen hierüber auf das Firmennetzwerk zu. Die Kriminellen versuchen, dieses Protokoll zu missbrauchen und sich in die Verbindung zwischen Unternehmens-IT und Home-Office einzuklinken, um Schadprogramme einzuschleusen oder Hintertüren einzurichten. Seit Jahresbeginn haben sich die Angriffsversuche darüber mehr als verdoppelt. Aber nicht nur auf Cyberbedrohungen geht der Report ein. Der Bericht gibt auch einen Lagebericht zu bekannten APT-Gruppen und deren momentane Aktivitäten.
"Unsere Forschungsdaten zeigen eine kontinuierliche Welle an Web- und E-Mail-Attacken, die die Corona-Pandemie als Thema haben. Angriffe, die auf das Remote Desktop Protokoll abzielen, haben ebenfalls zugenommen", so Roman Kovac, Chief Research Officer bei ESET.

Phishing-Mail gibt sich als Paketzustelldienst aus

Einen besonders hohen Anstieg beobachteten die ESET-Forscher bei Phishing-Mails. Hauptsächlich setzen die Kriminellen derzeit auf Nachrichten, die auf den ersten Blick vom Paketzustelldienst DHL stammen. Gegenüber dem ersten Quartal sehen die Experten bei dieser Kampagne eine Verzehnfachung des Aufkommens. Die meisten dieser E-Mails enthalten Anhänge mit den Namen "DHL_Receipt.pdf.htm" oder "DHL_Document.pdf.html". Dies sind gefälschte Formulare, die versuchen, an die Anmeldeinformationen zu DHL-Onlinediensten zu gelangen. Eine mögliche Erklärung kann die Zunahme der Online-Bestellungen durch die Corona-Pandemie sein. Gerade dieses stärkere Bestellverhalten könnte auch die Steigerung bei den Android-Bedrohungen begründen.

Android-Bedrohungen nehmen zu

Laut aktuellen Umfragen des Digitalverbandes BITKOM shoppt mehr als jeder zweite Anwender mit dem Smartphone - Tendenz steigend. Mobile Shopping ist heute bereits fast so verbreitet wie der Kauf per Laptop. Eine Steigerung zeigt auch die Android-Bedrohungslage: Um 18 Prozent sind die Malware-Erkennungen bei diesem Betriebssystem im Vergleich zum Vorjahresquartal gestiegen. Sehr beliebt waren auch im zweiten Quartal Attacken mit Bezug zur Corona-Pandemie. Ein typisches Szenario waren Banking-Trojaner, die über schadhafte Webseiten verbreitet wurden und vorgaben, Seiten der Gesundheitsministerien zu sein. Darüber hinaus sahen die Experten Fälle, in denen sich eine Android-Ransomware als kanadische Covid-19-App ausgab.

RDP-Angriffe haben Beschäftigte im Home-Office als Ziel

Seit der Corona-Pandemie hat sich der berufliche Alltag vieler Beschäftigten radikal verändert. Viele Mitarbeiter erledigen heute große Teile ihrer Arbeit per Fernzugriff auf das Firmennetzwerk. Dabei kommt häufig das Remote Desktop Protokoll (RDP) zum Einsatz. Trotz der zunehmenden Bedeutung von RDP (und anderer Remote-Access-Dienste) vernachlässigen Unternehmen häufig deren Einstellungen und Schutz. Das wissen auch Cyberkriminelle. Insbesondere Ransomware-Gruppen versuchen, daraus einen finanziellen Vorteil zu schlagen. ESET-Forschungen bestätigen einen Anstieg an Attacken auf Clients, um in schlecht gesicherte Netzwerke einzudringen. Seit Jahresbeginn haben sich die Angriffsversuche mehr als verdoppelt.

Exklusiver Blick auf die Aktivitäten der APT-Gruppen

Advanced-Persistent-Threat-(APT)-Gruppen greifen in der Regel mit gezielten Angriffen kritische Infrastrukturen sowie Behörden und Unternehmen an. Dabei geht es diesen Gruppen darum, sich im jeweiligen Netzwerk einzunisten, um an vertrauliche Daten zu gelangen. Im Threat Report berichten die ESET-Forscher über aktuelle Aktivitäten von Winnti, Turla oder Gamaredon.