Name

APT – Advanced Persistent Threat

Geburtsdatum

1989

Herkunft

Moskau

Modus Operandi

Es handelt sich um eine Reihe von unbemerkten, komplexen und kontinuierlichen Computer-Hacking-Prozessen, die von organisierten Gruppen von Cyberkriminellen organisiert werden und sich im Allgemeinen an Regierungen, große Unternehmen oder Institutionen richten. Sie werden aufgrund ihrer Koordination und dem Einsatz ausgefeilter Techniken, um in die IT-Systeme der Opfer einzudringen, als fortgeschritten bezeichnet. Dabei werden insbesondere Schwachstellen und Hintertüren der Betriebssysteme ausgenutzt. ATPs zeichnen sich dadurch aus, dass sie solange wie möglich im Verborgenen bleiben, um so viele Informationen wie möglich zu stehlen. Sie suchen nach dem wertvollsten Kapital eines Unternehmens bzw. einer Organisation: die sensibelsten Unternehmens-informationen und Daten, die es ihnen ermöglichen, den Angriff sofort zu monetarisieren.

Festnahme

Diese Bedrohung wurde bereits von Panda Security identifiziert und neutralisiert.

Wenn Sie jedoch kein Panda Security Kunde sind und diese Malware in Ihrem Firmennetzwerk entdecken, kontaktieren Sie uns sofort und wir übernehmen die Festnahme für Sie.

Strafprotokoll

GhostNet
Der Großangriff wurde im März 2009 entdeckt. Der Ursprung liegt höchstwahrscheinlich in der Volksrepublik China. GhostNet infiltrierte die Computer von politischen, wirtschaftlichen und medialen Zielen in mehr als 100 Ländern.

Operation Aurora
Die Operation Aurora beschreibt eine Reihe von Cyberangriffen, die 2009 durchgeführt wurden und ihren Ursprung in China haben. Es wurde ein Zero-Day-Exploit verwendet, um einen Trojaner zu installieren, der dazu dient, Informationen zu stehlen. Im Jahr 2010 enthüllte Google diese Angriffe und behauptete, dass auch andere Unternehmen angegriffen worden seien. Zu diesen Unternehmen gehörten führende Banken, Verteidigungs-unternehmen, Sicherheitsdienstleister, Öl- und Gasunternehmen sowie andere Technologieunternehmen.

Stuxnet
Stuxnet, ein Computer-Wurm, der Computer unter Windows betraf, wurde im Juni 2010 entdeckt. Der Wurm ist dafür bekannt, Industriesysteme auszuspionieren und neu zu programmieren. Sein Zielobjekt war die nukleare Infrastruktur des Irans mit Siemens-Steuerungssystemen. Einige Medien schrieben den Wurm den Geheimdiensten der USA und Israels zu.

Red October
Im Oktober 2012 wurde ein Malware-Programm entdeckt, das vertrauliche Informationen von Regierungen und Forschungseinrichtungen stahl. Es wird angenommen, dass das Programm bereits seit mindestens fünf Jahren vor seiner Entdeckung auf der ganzen Welt tätig war und diplomatischen, kommerziellen und militärischen Luft-, Raumfahrt- und Forschungsorganisationen in Russland, dem Iran, den USA und mindestens 36 anderen Ländern sensible Informationen entwendet hat.

02065/961-200
vertrieb@de.pandasecurity.com