

## PRESSEMITTEILUNG

PandaLabs Report Q2 2016:

## Ransomware und gezielter Datendiebstahl waren die beliebtesten Angriffsmethoden von Cyberkriminellen im zweiten Quartal 2016

- PandaLabs entdeckte im zweiten Quartal 2016 durchschnittlich 200.000 neue Malware-Exemplare pro Tag und verzeichnete damit einen deutlichen Rückgang gegenüber Q1, als täglich rund 227.000 Schädlinge identifiziert wurden.
- Von April bis Juni 2016 waren Ransomware-Attacken und der Diebstahl von digitalen Zugangsdaten die am häufigsten genutzten Methoden der Cyberkriminellen.
- Weitere Themen des aktuellen PandaLabs-Reports: Infektionen von POS-Terminals, der fortschreitende Cyberkrieg und wie Mobilgeräte die Türen für Hackerangriffe öffnen.

*Duisburg, den 28. Juli 2016* –PandaLabs, das Sicherheitslabor von Panda Security, hat seinen neuesten Bericht mit Zahlen und Fakten über die Malware-Entwicklung im zweiten Quartal 2016 veröffentlicht. Mit durchschnittlich 200.000 neuen Schädlingen pro Tag wurde ein deutlicher Rückgang in der Malware-Neuentwicklung gegenüber dem vorangegangenen Quartal verzeichnet. Vergleicht man die neuen Zahlen für die Monate April bis Juni 2016 mit denen aus den Vorjahren, so lässt sich feststellen, dass die Malware-Entwicklung insgesamt erstmals leicht rückläufig ist – jedoch auf sehr hohem Niveau.

Trojaner behaupten auch im zweiten Quartal dieses Jahres weiterhin ihre Spitzenposition in der Liste der erfassten Malware, was die Zunahme von Ransomware-Attacken in dieser Kategorie bestätigt. Erpressungssoftware ist ein internationales Geschäft geworden, das jährlich Milliarden von Kosten verursacht.

## Bei Hackern beliebt: Ransomware und gezielter Datendiebstahl

In den vergangenen drei Monaten haben wir eine Reihe von verschiedenen Cyber-Angriffen erlebt mit dem Ziel, möglichst schnell viel Geld zu machen. Die beliebtesten Methoden, derer sich die Hacker dabei bedienten, waren Ransomware-Angriffe und der gezielte Diebstahl von persönlichen Kundeninformationen und Zugangsdaten zu Kundenkonten.

So wurde unter anderem die US-amerikanische Non-Profit-Gesundheitsorganisation MedStar Health Opfer eines großangelegten Ransomware-Angriffs, der dazu führte, dass die Organisation ihre digitalen Systeme für mehrere Tage vom Netz nehmen musste. Im Mai erlitt das Kansas Heart Hospital ebenfalls einen schweren Ransomware-Angriff. Auch das professionelle NASCAR-Rennsportteam CSLFR hatte sich im vergangenen Quartal einen Verschlüsselungstrojaner eingefangen, der Daten im Wert von ca. drei Millionen US-Dollar verschlüsselte und für deren Herausgabe ein Lösegeld verlangte.

Auch der gezielte Datendiebstahl war im zweiten Quartal 2016 eine bei Hackern beliebte Angriffstaktik. Im April wurden beispielsweise die Kontaktinformationen von rund 1,1 Millionen Nutzern der Dating-Plattform beautifulpeople.com gestohlen. Die Daten beinhalteten nicht nur die echten Namen und Adressen der Mitglieder, sondern auch persönliche Details wie sexuelle Vorlieben, den Beziehungsstatus oder die Höhe ihres Einkommens. Der bekannte Hardware-Hersteller Acer wurde ebenfalls Opfer einer Hackerattacke auf seine US-amerikanische E-Commerce-Seite, bei der die Daten von 34.500 Nutzern entwendet wurden. Das besonders Erschreckende an diesem Fall: Die betreffende Acer-Seite war ein Jahr lang kompromittiert, ohne dass das Unternehmen dies bemerkte.

## Zunahme von Angriffen auf POS-Terminals und Finanzinstitute

Eine ebenfalls weit verbreitete Hackermethode ist die Nutzung von POS-Terminals, zum Beispiel mithilfe der PunkeyPOS-Malware. Diese von PandaLabs entdeckte Schadsoftware infizierte mehr als 200 POS-Terminals in Restaurants in den USA und stahl Informationen von Kreditkarten, die dort zum Bezahlen benutzt wurden.

Lukrativer ist da nur noch das direkte Hacken von Banken. Das passierte der Zentralbank von Bangladesch. Cyberkriminelle konnten erfolgreich 81 Millionen Dollar entwenden. Kurze Zeit später ereigneten sich zwei ähnliche Fälle: Ein Angriff richtete sich gegen eine Bank in Vietnam und ein weiterer gegen eine Bank in Ecuador.

## Sicherheitsverletzungen bei Mobilgeräten

Es scheint, dass Google große Anstrengungen unternimmt, wenn es um das Patchen der Sicherheitslücken in seinen Betriebssystemen geht. Monatliche Updates sollen möglichst schnell alle neu entdeckten Schwachstellen beseitigen. Trotzdem können alle vom Technologie-Riesen vorgenommenen Verbesserungen nicht verhindern,

dass Android angesichts der exponentiellen Zunahme von Angriffen ein stark gefährdetes System ist. Denn während alle mobilen Geräte, die direkt von Google vertrieben werden (wie zum Beispiel Smartphones und Tablets der Marke Nexus), die Updates sofort erhalten, müssen andere Android-Nutzer häufig Monate lang auf die Patches warten.

## Der fortschreitende Cyberkrieg

Wenn wir von Cyberkrieg sprechen, reden wir zumeist über digitale Attacken, die wahrscheinlich von unterschiedlichen Ländern gesponsert werden, auch wenn kaum Beweise zu finden sind, wer für den jeweiligen Angriff verantwortlich ist. Jedoch sind die USA im April dieses Jahres in die Offensive gegangen und haben bekanntgegeben, dass sie Cyberattacken gegen ISIS planen.

Zudem gab im Juni die Polizeibehörde von Südkorea einen Angriff von Nordkorea bekannt. Vermutlich begann die Cyberattacke vor mehr als einem Jahr und konzentrierte sich auf 140.000 Computer von Regierungsorganisationen und Rüstungskonzernen. Laut Polizeiangaben wurden mehr als 42.000 Dokumente gestohlen, von denen 95 Prozent verteidigungsbezogen waren, wie zum Beispiel die Pläne und Spezifikationen der Flügel des amerikanischen F 15 Fighters.

Alle aktuellen Informationen aus den PandaLabs zu einflussreichen Hackerattacken im zweiten Quartal 2016 erhalten Sie im vollständigen PandaLabs Report Q2 2016 unter <http://pandanews.de/wp-content/uploads/Pandalabs-2016-Q2-de.pdf>

## Über PandaLabs

PandaLabs ist das Anti-Malware-Labor des weltweit agierenden IT-Spezialisten Panda Security und fungiert als dessen zentrale Stelle für Malware-Treatment. PandaLabs entwickelt kontinuierlich und in Echtzeit die notwendigen Gegenmaßnahmen, um Panda-Security-Kunden vor allen Arten von schädlicher Software auf globalem Level zu schützen. PandaLabs ist somit verantwortlich für die Durchführung detaillierter Scans aller Malware-Arten. Ziel ist es, sowohl den Schutz für die Panda - Kunden zu verbessern, als auch die Öffentlichkeit aktuell und zeitnah zu informieren.

### Pressekontakt:

Kristin Petersen  
Presse & PR

PAV Germany GmbH  
Dr.-Alfred-Herrhausen-Allee 26  
47228 Duisburg

Tel: +49 2065 961 352  
Fax: +49 2065 961 195  
Kristin.Petersen@de.pandasecurity.com  
[www.pandanews.de](http://www.pandanews.de)  
[www.pandasecurity.com/germany/](http://www.pandasecurity.com/germany/)