Pressemeldung

**3. Mai 2016**

**Experten von BAE Systems decken neue Cyber-Bedrohung auf**

*Cyber-Kriminelle nehmen öffentliche Einrichtungen mit modifizierter Form*

*der QBOT Malware ins Visier*

Ein Team führender Cyber-Experten hat eine neue Variante der bösartigen QBOT-Software identifiziert, die mehr als 54.000 PCs in Tausenden von Organisationen weltweit infiziert hat. Durch einen QBOT-Angriff auf eine Institution des öffentlichen Sektors hatte BAE Systems die Gelegenheit näher zu untersuchen, wie die aktualisierte Version der Schadsoftware PCs infiziert, wie sie sich selbst aktualisiert und weshalb sie von den meisten Antivirenprogrammen nicht entdeckt wird.

Analysten von BAE Systems entdeckten Anfang 2016, als bei einem Angriff auf diese Institutionmehr als 500 PCs infiziert wurden, dass an der ursprünglichen QBOT Malware eine Reihe von Änderungen vorgenommen wurden, die es erschwerten, diese zu entdecken und abzuwehren. Eine der Änderungen bewirkte, dass jedes Mal, wenn der Code der Malware ausgegeben wurde, dieser zusätzliche Inhalte hatte. Dadurch sah er für diejenigen, die nach bestimmten Signaturen von Malware fahnden, wie ein komplett neues Programm aus.

Darüber hinaus erzeugen automatisierte Aktualisierungen der Malware alle sechs Stunden neue verschlüsselte Versionen, wodurch die Bemühungen, die Software auf den Kunden-PCs zu aktualisieren, konterkariert wurden. Dies half dem Virus sich weiter zu verbreiten. Die neue QBOT-Schadsoftware prüft auch, ob Anzeichen dafür vorliegen, dass sie sich in einer sogenannten „Sandbox“ befindet – ein Werkzeug, das verwendet wird, um Malware zu erkennen, bevor es den Posteingang der PC-Nutzer erreicht. Diese Methode wird von vielen Institutionen als Verteidigungsmaßnahme gegen bösartige E-Mail-Inhalte genutzt. Die Ersteller der Malware unternehmen nun große Anstrengungen, diese zu überlisten.

Professionelle Cyber-Kriminelle haben vor allem öffentliche Einrichtungen wie Polizeistationen, Krankenhäuser und Universitäten angegriffen. Einer Analyse von BAE Systems zufolge läuft QBOT derzeit auf mehr als 54.000 PCs. Da die Schadsoftware nur schwer zu entdecken ist und die Infizierung automatisiert verläuft, besteht die Gefahr, dass QBOT sich weiter verbreitet, es sei denn, Unternehmen und Institutionen ergreifen Maßnahmen, um sich zu schützen.

**Adrian Nish, Leiter der Cyber Threat Intelligence bei BAE Systems**, sagt: „Viele Einrichtungen des öffentlichen Sektors im Bereich der kritischen Infrastrukturen und Dienstleistungen haben oft nur begrenzte Budgets und werden häufig ein bevorzugtes Angriffsziel. In diesem Fall hatten die Cyberkriminellen Pech, denn einige veraltete PCs führten dazu, dass die Schadsoftware die PCS zum Abstürzen brachte, anstatt sie zu infizieren. Durch diese Serie von Abstürzen wurde die Einrichtung auf die Ausbreitung des Problems aufmerksam.“

„Dieser Fall zeigt, dass Einrichtungen des öffentlichen Sektors wachsam bleiben müssen, und dass sie sich gegen neue Cyber-Bedrohungen verteidigen müssen. QBOT tauchte zwar zum ersten Mal bereits im Jahr 2009 auf. Aber um einer Entdeckung zu entgehen und um andere PCS schnell zu infizieren, ist diese neue Version mit modernsten Werkzeugen ausgestattet.“

Das Team von BAE Systems hat die Malware untersucht um herauszufinden, wie sie funktioniert und wie gestohlene Daten hochgeladen wurden. Darüber hinaus konnten sie ermitteln, wie die Programmierer die gestohlenen Daten jedes Mal so veränderten, um eine Erkennung und ein Abfangen zu vermeiden.

Das Weißbuch von BAE Systems über die QBOT Schadsoftware steht zum Download [hier](https://resources.baesystems.com/pages/view.php?ref=39115&k=46713a20f9) zur Verfügung.

**Bei Rückfragen kontaktieren Sie bitte:**

Wolfgang Dobler, Dobler Communications

Tel.:  +49 (0) 69 24 750 3430

Mobil: +49 (0) 163 989 6663

Email: [wd@dobler-communications.de](mailto:wd@dobler-communications.de)

oder in Großbritannien:

Nick Haigh, BAE Systems Applied Intelligence

Tel.: +44 (0) 3300 467573

Mobil: +44 (0) 7525 390982

Email: [nick.haigh@baesystems.com](mailto:nick.haigh@baesystems.com)

**Über BAE Systems**

BAE Systems entwickelt einige der weltweit führenden Verteidigungs-, Luftfahrts- und Sicherheitstechnologien. Wir beschäftigen 83.400 qualifizierte Mitarbeiter in über 40 Ländern. In Zusammenarbeit mit Kunden und Partnern entwickeln wir vor Ort Produkte und Systeme, die militärische Fähigkeiten liefern, nationale Sicherheit und Menschen schützen und kritische Informationen und Infrastrukturen sichern.

Wir helfen Unternehmen, Staaten und Behörden in aller Welt, sich gegen Cyber-Angriffe zu verteidigen, netzbedingte Risiken zu verringern, regulatorische Anforderungen zu erfülllen und ihre Abläufe zu transformieren.

Dabei setzen wir auf unsere einzigartigen Lösungen, Systeme, Prozesse und unser Know-how – vielfach auch unter Erfassung und Auswertung massiver Datenmengen. Gemeinsam mit unseren Cyber Special Forces – einige der weltweit talentiertesten Mitarbeiter – können wir Schutz vor Cyber-Angriffen, Betrug und Wirtschaftskriminalität bieten und wissensbasierte und praxisbezogene Überwachung liefern sowie bei der Lösung komplexer Datenprobleme unterstützen.

BAE Systems Applied Intelligence, der Bereich von BAE Systems, der auf Cybersicherheit spezialisiert ist, beschäftigt, über 4.200 Mitarbeiter in 18 Ländern (EMEA-Region, Amerika sowie APAC -Region).

Weitere Informationen zu BAE Systems Applied Intelligence unter: [www.baesystems.com/businessdefence](http://www.baesystems.com/businessdefence)