IBM entdeckt digitalen Wolf im Schafspelz

IBM entdeckt digitalen Wolf im Schafspelz

Hacker stehlen Millionenbeträge mittels Dyre-Trojaner / Malware und Social Engineering immer raffinierter / Schwachstelle Mensch
Die Experten von IBM Security haben einen laufenden Angriff von Cyberkriminellen aufgedeckt, die teilweise mehr als eine Million US-Dollar von einzelnen Unternehmen erbeuteten. Die Operation, die von den Sicherheitsforschern auf den Namen "Dyre Wolf" getauft wurde, setzt neben der bekannten Dyre-Malware auf Social Engineering: Dabei geben sich Hacker etwa als Callcenter-Mitarbeiter von Banken aus, um an Kontodaten von Organisationen zu gelangen - mit verheerenden Folgen.
"Während sich betrügerische Malware zur Erbeutung von Kontodaten meist gegen Privatpersonen richtet, haben es die Entwickler von Dyre gezielt auf Unternehmen abgesehen", sagt Gerd Rademann, IBM Business Unit Executive Security Systems DACH. "Seit dem ersten Auftreten der Malware im Jahr 2014 hat sie sich enorm entwickelt und ist mittlerweile so ausgereift, dass Cyberkriminelle immer größere Coups damit landen konnten."
Laut den Sicherheitsforschern von IBM ist es organisierten Cyberkriminellen jüngst gelungen, einzelne Unternehmen teils um über eine Million US-Dollar zu erleichtern. Dafür setzten die Hacker neben der bereits im Jahr 2014 entdeckten Dyre-Malware vor allem auf raffiniertes Social Engineering.
Die IBM Forscher tauften die aktuelle Operation der Cyberkriminellen auf den Namen "Dyre Wolf". Schon im Oktober 2014 berichteten Mitarbeiter des IBM Tochterunternehmens Trusteer über einen enormen Anstieg bei den mit der Dyre-Malware infizierten Systemen: Sprunghaft stieg die Zahl von 500 auf fast 3.500 an. Seine starke Verbreitung verdankt Dyre einem Mechanismus, bei dem zunächst eine zweite Malware namens Upatre großflächig über Spam-Mails an die Opfer versendet wird. Nach dem Öffnen eines präparierten Anhangs in der fingierten Mail wird Dyre automatisch auf dem infizierten System installiert.
Täuschen, zuschlagen, ablenken
Sobald Dyre ein System infiziert hat, leitet es Mitarbeiter von Unternehmen auf eine fingierte Website, wenn diese über ihren Internet-Browser auf die Online-Präsenz der hauseigenen Bank zugreifen wollen. Dort wird der Nutzer, unter dem Vorwand technischer Schwierigkeiten, aufgefordert, sich telefonisch an einen Servicemitarbeiter zu wenden. Hinter der angezeigten Telefonnummer stecken dann die Hacker, die so raffiniert sind, dass sie genau wissen, wann ein Opfer anruft und als welche Bank sie sich ausgeben müssen. Damit bringen sie die ahnungslosen Mitarbeiter dazu, die Kontoinformationen und Zugangsdaten ihres Arbeitsgebers preiszugeben.
Sobald das Opfer den Hörer auflegt, haben die Kriminellen die Transaktion bereits abgeschlossen und Geld über mehrere Banken und Länder hinweg auf ihr eigenes Konto überwiesen. Die vielen Stationen, die das Geld weltweit durchläuft, erschwert die Rückverfolgung. Um ihre Spuren weiter zu verwischen, starten manche Kriminelle im Anschluss an die erfolgreiche Überweisung eine DDoS-Attacke auf die IT-Systeme des bestohlenen Unternehmens. Dabei werden die Server mit einer großen Anzahl von Anfragen überlastet und gezielt lahmgelegt. IBM vermutet, dass es sich dabei um ein Manöver handelt, um von dem Geldtransfer abzulenken.
Das schwächste Glied
Dyre Wolf zeigt einmal mehr: Die IT-Abwehrkette von Organisationen ist immer nur so stark wie ihr schwächstes Glied - und dieses Glied sind häufig die Mitarbeiter. Das bestätigt auch der IBM Cyber Security Intelligence Index, aus dem hervorgeht, dass bei rund 95 Prozent aller Cyberangriffe irgendeine Art von menschlichen Versagen einkalkuliert wird. Viele Angreifer verlassen sich auf jemanden, der auf einen präparierten Link in einer E-Mail klickt oder einen infizierten Anhang herunterlädt und es ihnen so im besten Fall ermöglicht, Millionen zu stehlen, ohne dass das Opfer etwas davon merkt.
Den Blog-Post dazu auf Englisch finden Sie unter: http://ibm.co/1NEBHxt
Den kompletten englischen Bericht finden Sie unter: http://ibm.co/1DrOxQm
Mehr Informationen auf www.ibm.com/security , @IBMSecurity auf Twitter

Kontaktinformation
Hans-Jürgen Rehm
Unternehmenskommunikation IBM Deutschland Smarter Computing, Security
+49-7034-15-1887
+49-171-5566940
hansrehm@de.ibm.com
<img src="http://www.pressrelations.de/new/pmcounter.cfm?n_pinr_=591339" width="1" height="1">

Pressekontakt

IBM Deutschland

71137 Ehningen

Firmenkontakt

IBM Deutschland

71137 Ehningen

IBM gehört mit einem Umsatz von 95,8 Milliarden US-Dollar im Jahr 2009 zu den weltweit größten Anbietern im Bereich Informationstechnologie (Hardware, Software und Services) und B2B-Lösungen. Das Unternehmen beschäftigt derzeit 399.400 Mitarbeiter und ist in über 170 Ländern aktiv.Die IBM in Deutschland mit Hauptsitz bei Stuttgart ist die größte Ländergesellschaft in Europa.Mehr Informationen über IBM unter: ibm.com/de/ibm/unternehmen/index.htmlIBM ist heute das einzige Unternehmen in der IT-Branche, das seinen Kunden die komplette Produktpalette an fortschrittlicher Informationstechnologie anbietet: Von der Hardware, Software über Dienstleistungen und komplexen Anwendungslösungen bis hin zu Outsourcingprojekten und Weiterbildungsangeboten.