Spionagesoftware: Der Handel des Hacking Teams mit Zero-Days

27. Juli 2015

golem.de

Zero-Day-Exploits sind nicht nur ein lukratives Geschäft, sondern werden auch fernab des Deep Webs äusserst professionell gehandelt. Das Hacking Team musste gegen seine Konkurrenten aufholen - und tätigte dabei auch Fehlkäufe. Das zeigt eine jetzt veröffentlichte Analyse.

Das Hacking Team hinkte jahrelang seiner Konkurrenz in Sachen Exploits hinterher. Nur mühsam konnte sich das Unternehmen im Geschäft um Zero-Days etablieren. Und dieses Geschäft findet nicht nur im Deep Web statt, sondern wird äusserst professionell gehandhabt. Zu diesem Schluss kommt der IT-Sicherheitsexperte Vlad Tsyrklevich, der die geleakten E-Mails des Hacking Teams analysiert hat.

Ein geradezu mondänes Geschäft nennt Tsyrklevich den Handel mit Zero-Day-Exploits. Es unterliegt nach seiner Analyse den gleichen Mechanismen wie jeder andere Handel auch: Es gibt Qualitätsunterschiede, Kundenwünsche und Garantien. Allerdings muss das Vertrauen zwischen Kunden und Verkäufern äusserst hoch sein. Sie müssen sich etwa darauf verlassen, dass beide Seiten die Details zu den Schwachstellen nicht veröffentlichen, besonders dann, wenn der Verkäufer Exklusivität verspricht. Meist werden beispielsweise Ratenzahlungen vereinbart, die eingestellt werden, sollte eine Zero-Day-Lücke an die Öffentlichkeit gelangen.

Anbieter meist im Vorteil

Jenseits des professionellen Umgangs von Verkäufern und Kunden fluktuieren Qualität und Preise aber enorm. Und die verlangten Preise sagen nicht immer etwas über die Qualität der Schwachstellen aus. Hier haben Kunden meist das Nachsehen, wenn sie einen zu hohen Preis aushandeln oder einen schwachen Exploit kaufen. Besonders Zwischenhändler bieten laut Tsyrklevich meist auch minderwertige Schwachstellen an, bleiben aber meist auf den von ihnen angebotenen Zero-Day-Lücken sitzen.

Tsyrklevichs Analyse zufolge begann das Hacking Team bereits 2009, Kontakte zu zahlreichen Händlern herzustellen, die Zero-Day-Lücken anbieten. In dieser Zeit wechselte das Hacking Team vom Sicherheitsdienstleister zu einem Anbieter von Überwachungslösungen und sah sich starker Konkurrenz durch die etablierten Unternehmen wie Gamma oder der NSO Gruppe ausgesetzt.

Probleme mit der Konkurrenz

Die zunächst von Dsquare Security und Vupen eingekauften Exploits erwiesen sich als unzureichend, und das Verhältnis zwischen Vupen und dem Hacking Team wurde im Laufe der Zeit nicht besser. Das Hacking Team vermutete, das Vupen seine Exploits lieber an den Konkurrenten Gamma verkaufte. 2013 beklagte der Hacking-Team-Chef in einer E-Mail das Problem mangelnder Zero-Days. Sie würden sich nach alternativen Anbietern umsehen und

gleichzeitig eine interne Abteilung aufbauen, die selbst nach Exploits suchen solle. Vor allem Flash erschien ihnen als geeignete Plattform.

Hinweise vom Fuzzing, fertige Exploits von Zwischenhändlern

Mit dem IT-Sicherheitsexperten und Entwickler Rosario Valotta ging das Hacking Team im Mai 2013 einen Vertrag ein. Valotta sollte seine Fuzzing-Analysen diverser Browser zur Verfügung stellen. Anhand seiner Ergebnisse wollte das Hacking Team überprüfen, ob sich ein entdeckter Fehler auch als Exploit nutzen liesse. Valotta beendete seinen Vertrag im Januar 2014 wohl aus persönlichen Gründen. Im Februar 2015 kontaktierte er aber nochmals das Hacking Team. Er habe einen Fehler im Internet Explorer 11 entdeckt. Den habe das Hacking Team aber offenbar niemals zu einem funktionierenden Exploit weiterentwickeln können, resümiert Tsyrklevich, und es gebe keine Hinweis über eine Zahlung an Valotta. Der Fehler wurde von Microsoft nach der Veröffentlichung der Hacking-Team-Dokumente beseitigt.

Seite Ende 2013 gab das Hacking Team mehrere Hunderttausend US-Dollar für Exploits aus. Vom freiberuflichen Entwickler Vitaliy Toropov kauften sie insgesamt drei Flash-Lücken, die teilweise ebenfalls erst dann geschlossen wurden, als die internen Dokumente des Hacking Team an die Öffentlichkeit gelangten. Eine der gekauften Lücken wurde schon davor von Adobe gepatcht. Da darauf noch Garantie war, reichte Toropov eine weitere kostenlose Lücke nach.

Schwachstellen in NAS und Access Points gesucht

Vom Zwischenhändler Adriel Desautel und dessen Unternehmen Netragard erwarb das Hacking Team von Anfang 2014 bis Mai 2015 gleiche mehrere Dutzend Schwachstellen. Dabei war nicht nur Flash das Ziel, sondern auch Windows und dessen Media Center sowie Microsoft Office. Andere betrafen NAS-Geräte von Qnap oder Access Points von Netgear. Aber auch für OS X und Oracles Datenbankverwaltungssystem interessierte sich das Hacking Team. Nachdem die Interna des Unternehmens veröffentlicht wurden, gab Desautel sein Geschäft mit Exploits auf.

Der Entwickler Eugene Ching aus Singapur quittierte sogar sein Angestelltenverhältnis und gründete seine eigene Firma Qavar, als das Hacking Team Interesse an einem von ihm entdeckten Exploit zeigte. Beide unterzeichneten einen einjährigen Vertrag über 60.000 US-Dollar. Ching entwickelte für das Hacking Team einen Exploit für 32- und 64-Bit-Versionen von Windows bis Version 8.1 und erhielt dafür einen Bonus von 20.000 US-Dollar. Er wollte auch einen Exploit für eine Lücke im Videoplayer VLC nachreichen.

Zu teure Schwachstellen

Bei dem Zwischenhändler Vulnerabilities Brokerage International (VBI) des Entwicklers Dustin Trammel alias I)ruid verhandelte das Hacking Team ab Dezember 2013 unter anderem einen exklusiven Kauf einer Schwachstelle in Windows, die einen Ausbruch aus einer geschlossenen Umgebung erlaubte. Zunächst handelte das Hacking Team den Preis von 150.000 US-Dollar auf 95.000 US-Dollar herunter. Offenbar sei der Handel aber auch nach einer längeren Testphase nicht zustande gekommen, denn es gebe in den veröffentlichten E-Mails des Hacking Teams keine weiteren Hinweise darauf, schreibt Tsyrklevich.

Auch an eine Schwachstelle im Firefox-Browser aus dem VBI-Portfolio gelangte das Hacking Team. Sie wollten damit vor allem den Tor-Browser angreifen, der auf Firefox basiert. Für die exklusiven Rechte daran verlangte VBI 105.000 US-Dollar, die nicht-exklusiven Rechte hätten

sich auf 84.000 US-Dollar belaufen. Die Verhandlungen zwischen dem Hacking Team und VBI zogen sich aber derart in die Länge, dass der Exploit an einen unbekannten Dritten verkauft wurde. Das Hacking Team habe zudem über einen Einkauf von Schwachstellen im Adobe Reader und im Windows-Kernel nachgedacht, aber den Preis von 200.000 US-Dollar als zu hoch abgelehnt.

Weltweite Anbieter

Auch mit anderen Exploit-Anbietern hatte das HackingTeam Kontakt, darunter Ability Ltd aus Israel, dem Keen Team aus China, Cosenic aus Singapur, LEO Impact Security sowie Revuln und Security Brokers aus Italien. Deren Angebote entsprachen meist nicht den Anforderungen des Hacking Teams oder waren zu teuer.

Die meisten Exploits, über die das Hacking Team verfügt, sind inzwischen längst geschlossen, weitere wurden nach der Veröffentlichung der Dokumente gepatcht.