Mutmasslicher Staatstrojaner wirft Fragen auf

24. November 2014

Marie-Astrid Langer, NZZ

Die Softwarefirma Symantec will einen neuen staatlichen Computervirus gefunden haben. Wie genau sie das getan hat, verrät sie aber nicht.

Ein neu entdecktes Spionage-Programm sorgt international für Aufsehen: Seit mindestens 2008 soll ein komplexer Computervirus Unternehmen und Behörden ausgespäht haben, vor allem in Saudiarabien und in Russland. Dies hat die Softwarefirma Symantec am Sonntagabend bekannt gegeben. Das Programm sei so komplex und aufwendig, dass nur Staaten als Auftraggeber in Frage kämen, schreibt Symantec in einem Blogpost.

Komplexer Trojaner

Konkret handele es sich bei «Regin» oder auch «backdoor.regin», wie die Entdecker den Virus nennen, um einen Trojaner, dessen komplexe und vielschichtige Struktur eine technische Kompetenz demonstrierten, die man nur selten zu sehen bekomme, so Symantec. Regin ermögliche seinen Programmierern Überwachung und Ausspähung im grossen Stil und wurde bereits zur Spionage von Regierungsorganisationen, Infrastruktur-Firmen, Unternehmen, Forschungsstellen sowie gegen Privatpersonen eingesetzt. In jedem vierten der nun aufgedeckten Fälle soll «Regin» zur Spionage von Telekommunikations-Anbietern genutzt worden sein.

Die gestohlenen Informationen würden verschlüsselt gespeichert und übermittelt. Der dabei entstehende Datenverkehr sei eine der wenigen Gelegenheiten, um das Spionage-Programm aufzuspüren, schreibt Symantec. Aktiv sei das Programm zwischen 2008 und 2011 eingesetzt worden; 2013 sei dann eine neue Version aufgetaucht. Bis 2011 sei das Programm besonders in Russland und Saudiarabien eingesetzt worden, aber auch in Mexiko und Irland beispielsweise.

In der Schweiz wurden keine Infektionen festgestellt, wie eine Unternehmenssprecherin gegenüber der NZZ sagte.

«Regin» bestehe aus fünf verschiedenen Stufen, von denen bis auf die erste alle verschlüsselt seien, heisst es im Whitepaper des Sicherheitsanbieters.

Das habe die Entdeckung erschwert. Zu lesen ist auch, dass «Regin» zur Verbreitung eine damals unbekannte Lücke in Yahoos Instant Messenger genutzt haben soll. Unklar ist, wie genau die Schadsoftware mit Servern der Angreifer kommunizierte.

Ungeklärte Fragen

Auch viele weitere Fragen zu «Regin» liess Symantec offen, etwa welches Land hinter dem Virus steckt oder wie es Symantec geschafft hat, den so extrem schwer aufzuspürenden

Trojaner überhaupt ausfindig zu machen. Auch auf die Frage, wie und warum der Virus ausgerechnet jetzt - drei Jahre nach dem letzten grösseren Angriff - aufgedeckt wurde, antwortete Symantec auch auf Nachfrage nicht. Symantec selbst hat sich auf Anti-Viren-Programme spezialisiert; hinter der Nachricht dürfte also auch ein gewisses Eigeninteresse des Unternehmens stecken.

Häufig kooperieren Sicherheitsfirmen mit Regierungsbehörden wie der CIA oder Europol, wenn sie neue Computerviren oder Ringe von Hackern aufdecken. So können die Behörden direkt auf die Entdeckungen der Software-Spezialisten reagieren und unmittelbar gegen Verdächtige vorgehen. Im Fall von «Regin» scheint eine derartige Kooperation aber nicht der Fall zu sein - was umso bemerkenswerter ist angesichts der Bedeutung, die Symantec «Regin» zuschreibt.