Sie ging Anfang August 2011 durch die Medien als „Operation zwielichtige Ratte" – eine Hacker-Attacke, die rund fünf Jahre lang lief und neben Regierungen und großen Organisationen natürlich auch Unternehmen aller Art ins Visier nahm. Operation Shady RAT ist nicht die erste solcher Aktivitäten, die Liste ist lang: Operation Aurora, Operation Night Dragon und so weiter.

Operation Shady RAT – eine Geschichtsstunde der Neuzeit

Isabell Unseld, McAfee GmbH

Unter den Opfern befinden sich neben bekannten Namen wie RSA, Lockheed Martin, Sony und PBS noch viele andere. Jetzt kann man sich fragen: „Und was habe ich damit zu tun?" Viel, denn die Angreifer sind interessiert an Daten und vertraulichen Informationen. Zwangsweise muss hier also auch die Sicherheit von Daten und Datenbanken diskutiert werden. Das wird dann ein Thema, sobald jemand auf eine Datenbank zugreift, um sich Informationen zu ziehen.

Betroffenheit an allen Fronten

Man kann mit Überzeugung sagen, dass wahrscheinlich jedes Unternehmen in jedem Industriezweig attackiert wurde, das eine signifikante Größe hat und über intellektuelles Eigentum beziehungsweise Geschäftsgeheimnisse verfügt. Es gibt Unternehmen, die davon wissen, und solche, die nicht wissen, dass sie angegriffen wurden. Dabei sind solche Angriffe kein neues Phänomen; seit etwa fünf Jahren nehmen sie stetig zu, werden ausgereifter, schwerer zu entdecken und oft auch nicht öffentlich gemacht. Dabei ist alles interessant: Source Codes, der Inhalt von Datenbanken, E-Mail-Archive, Verhandlungsunterlagen, Verträge und so weiter.

Was mit den erbeuteten Daten passiert, ist letztlich nicht bekannt. Wir wissen nur, dass es sich um eine Daten-Menge im Petabyte-Bereich handelt. Wenn jedoch auch nur ein kleiner Teil davon dazu genutzt wird, um es einem Wettbewerber zu ermöglichen, bessere Produkte herzustellen oder einen Mitbewerber bei einer Ausschreibung zu schlagen, kann es sich um einen massiven ökonomischen Verlust handeln, der nicht nur einzelne Unternehmen oder Wirtschaftszweige betrifft, sondern bei wiederholtem Auftreten die wirtschaftliche Entwicklung eines Landes. Trotzdem ist die öffentliche Wahrnehmung solcher Attacken eher minimal und das Verständnis für die Folgen gering.

Was steckt hinter Operation Shady RAT?

Zunächst einmal handelt es sich natürlich nicht um eine Ratte – „RAT" steht für den Begriff „Remote Access Tool". Es handelt sich auch nicht um eine brandneue Attacke, und die meisten Opfer haben diese spezifischen Infektionen schon beseitigt, obwohl offen bleibt, ob sie die Ernsthaftigkeit der Lage überhaupt realisiert oder nur die betroffenen Systeme ohne weitere Analyse eines möglichen Datenverlustes gereinigt haben.

Es wurden verschiedene Malware-Varianten und andere relevante Indikatoren entdeckt und zwar mit Hilfe von Generic Downloader.x und generischen BackDoor.t-Signaturen. Wer damit schon einmal zu tun hatte, erkennt sie durch die Nutzung von verschlüsselten HTML-Vermerken in Webseiten, die als Command Channel einer infizierten Maschine genutzt werden.

Entdeckt wurden die Angriffe auf einem Server, der unter Kontrolle der Angreifer stand, ein sogenannter „Command & Control Server". Server dieser Art werden von den Angreifern benutzt, um Attacken zu organisieren und zu koordinieren. Hier konnten Logs erfasst werden, die das volle Ausmaß der Opferzahl seit Mitte 2006 enthüllen, als die Log-Sammlung anfing. Mit Sicherheit ist davon auszugehen, dass die Angreifer nicht nur einen Server dieser Art nutzen, sondern – ganz im Sinne von Lastverteilung und Hochverfügbarkeit – eine ganze Reihe dieser Systeme in Betrieb haben. Es ist durchaus möglich, dass der Angriff schon viel eher begann, der früheste Anhaltspunkt für den Start der Gefährdung liegt jedoch bei Mitte 2006. Der Vorgang selbst war nicht ungewöhnlich für eine gezielte Attacke: Eine sogenannte „Spear-Phishing-E-Mail", die ein Exploit enthält, wird an eine Person gesendet, die in der richtigen Position eines Unternehmens sitzt. Wenn das Exploit auf einem ungepatchten System geöffnet wird, verursacht es den Download der entsprechenden Malware. Diese Malware initiiert einen sogenannten „Backdoor-Kommunikationskanal" zum „Command & Control Webserver" und liest die codierten Angaben in den versteckten Details des Webseiten-Codes aus.

Nun folgen andere Eindringlinge, die auf die infizierte Maschine zugreifen und sich sehr schnell bestimmte Privilegien verschaffen. Sie bewegen sich „seitwärts" innerhalb der angegriffenen Organisation, um neue, dauerhafte Verankerungen durch weitere infizierte Maschinen mit implementierter Malware anzubringen. Außerdem zielen sie auf eine schnelle Ent-

wendung der Daten, die sie gerne besitzen würden.

Das hohe Ausmaß der Gefährdung liegt auch darin begründet, dass die Angreifer nicht nur für kurze Zeit den Zugriff auf einzelne Daten und Systeme hatten, vielmehr agierten sie über einen langen Zeitraum in den Systemen der infizierten Unternehmen und Organisationen. Dies eröffnete ganz andere Möglichkeiten des Datenzugriffs, aber auch der Interpretation und des Erkennens innerbetrieblicher Abläufe und Organisationsstrukturen und -veränderungen. Man muss davon ausgehen, dass dieses Wissen für weitere Angriffe verwendet werden kann und wohl auch wird.

Es existiert ein durchaus funktionierender Schwarzmarkt im Internet für gestohlene Informationen und so kann es sein, dass die Zweckentfremdung gestohlener Informationen erst so richtig in Gang kommt, wenn die Daten über mehrere Zwischenhändler gegangen sind. Dazu entsprechende Tagebucheinträge:

1. Spear Phishing funktioniert. Es ist der erfolgreichste Angriffsvektor überhaupt und versieht den Angreifer mit Privilegien
2. Alle Arten von Daten sind begehrenswert
3. Angreifer werden unterschiedlich motiviert. Bei Shady RAT stand die finanzielle und politische Motivation im Vordergrund
4. Gestohlene Daten haben Petabyte-Größe erreicht
5. Es ist nicht bekannt, wohin die erbeuteten Informationen gingen, wer darauf Zugriff hat und was mit ihnen geschieht
6. Alle Regionen sind betroffen
7. Alle Organisations-Arten (öffentliche Einrichtungen, private Unternehmen, Regierungen) sind betroffen
8. Jede Unternehmensgröße ist betroffen
9. Die Attacken sind langlebig und ausdauernd: Die längste Attacke von Shady RAT dauerte 28 Monate (durchschnittliche Dauer 8,75 Monate)
10. Die führenden Unternehmen der Welt können in zwei Kategorien unterteilt werden: Erstens diejenigen, die angegriffen wurden und davon wussten, und zweitens die, die angegriffen wurden und immer noch keine Ahnung davon haben.

Sogenannte „APTs“, Advanced Persistent Threats, die im Falle von Operation Shady RAT zum Einsatz kamen, verstecken sich nicht und sind dennoch schwer auffindbar. Sie entziehen sich der Entdeckung, indem sie zum Beispiel gängige Network Ports ausnutzen. APTs steuern generell nur Netzwerkverbindungen nach außen an. Sollte also ein Unternehmensnetzwerk nicht speziell auch ausgehenden Netzwerkverkehr auf APT-bezogenen Anomalien beobachten, wird diese Art von Malware nicht identifiziert. Abschließend einige interessante Angaben zu APTs:

- Die durchschnittliche File-Größe liegt bei 121.85 kB

Werden Sie nicht zum Opfer

Nachfolgend sind fünf Schritte aufgelistet, die dabei helfen, Unternehmen zu schützen – egal, ob man schon angegriffen wurde oder noch nicht.

1. Stoppen Sie ungewünschte Infiltration

a. E-Mail-Sicherheitslösungen helfen, Spear-Phishing-Nachrichten abzufangen, bevor sie in die Inbox eines Anwenders gelangen
b. Web-Sicherheitslösungen helfen bei der Entdeckung und hindern Anwender daran, auf korrumpierte oder infizierte URLs zu gehen
c. Umfassender Schutz am Endpunkt hilft gegen den Download bösartiger Programme
d. Firewalls und Intrusion-Prevention-Systeme blockieren den Download von Malware und verhindern den unautorisierten Zugriff von „Command & Control“-Servern

2. Stoppen Sie nicht autorisierte Änderungen

a. „Application WhiteListing“ verhindert nicht genehmigte Änderungen
b. Das Monitoring von Datenbank-Aktivitäten verhindert den nicht genehmigten Zugriff auf geschäftskritische Daten in Datenbanken

3. Verhindern Sie, dass vertrauliche Daten ausgelesen werden können

a. Datenverschlüsselung verhindert, dass Daten gelesen werden können, auch wenn sie gestohlen werden
b. Data Loss Prevention identifiziert sensible Daten und kontrolliert deren Bewegung im Netz

4. Wissen, was sich im Netzwerk tut

a. Netzwerk-Verhaltensanalyse kann kompromittierte Systeme aufgrund von Traffic-Anomalien identifizieren und melden
b. Zentrale Verwaltung und Vulnerability-Einschätzung erlauben es, angreifbare Systeme in akzeptabler Zeit zu patchen

5. Globale Perspektive

a. Nur das eigene Netzwerk zu kennen, reicht mittlerweile nicht mehr aus. Man braucht praktisch ein globales Verständnis, um die Gefahren einschätzen zu können

- Die am meisten genutzten APT-Filenamen sind: svchost.ext, lexplore.exe, lprinp.dll und Wiinzf21.dll
- Sie unterbinden ihre Entdeckung zum Beispiel durch nach außen gehende http-Verbindungen
- 100 Prozent der APT-Backdoor-Trojaner nutzen nur ausgehende Verbindungen, 83 Prozent nutzen die TCP-Ports 80 und 443, die restlichen 17 Prozent einen anderen Port

nahmen einzurichten und vor allem nicht zu unterschätzen, dass sich Daten – auch wenn sie scheinbar vollkommen unbedeutend sind – in den Händen unautorisierter Personen zu einer Ware entwickeln können. In Zeiten der Globalisierung, in denen schon kleine Details einem Wettbewerber Vorsprünge verschaffen können, sind solche Angriffe also durchaus ernst zu nehmen.

Fazit

Shady RAT ist nur ein Beispiel für die weite Vielfalt von Angriffen auf Unternehmen. Die Operation hatte allerdings Signalwirkung, denn die Attacken waren gezielt auf namhafte Organisationen gerichtet und liefen über eine sehr lange Zeit, ohne dass manche Opfer davon Kenntnis hatten. Solche Angriffe werden in Zukunft keine Seltenheit bleiben, und man kann Unternehmen und Einrichtungen aller Größe und Coleur nur raten, wachsam zu sein, entsprechende Schutzmaß-

Isabell Unseld
McAfee GmbH
isabell_unseld@mcafee.com

Newsticker

Oracle stellt VM 3.0 vor

Die neue VM 3.0 umfasst neue regelbasierte Verwaltungsmöglichkeiten, innovatives Storage-Management über die Oracle VM Storage Connect Plug-in-API, zentrale Verwaltung der Netzwerk-Konfiguration, verbesserte Bedienbarkeit und Unterstützung für Open Virtualization Format (OVF). Oracle VM 3.0 bietet eine zentrale Management-Konsole für Virtuelle Maschinen, das Storage-Management und die Netzwerk-Konfiguration. So können Administratoren die Bereitstellung virtueller Maschinen automatisieren und rationalisieren. Zum automatisierten Ausrollen von Unternehmens-Software stehen mehr als neunzig VM Templates für Oracle Applications, Middleware und Datenbanken bereit. Die neue Version von Oracle VM unterstützt bis zu 128 virtuelle Prozessoren pro virtueller Maschine. Auf Oracle Sun Fire X4800 M2 Servern kann VM 3.0 sogar 160 physische Prozessor-Threads und 2 TB Speicher unterstützen.