Wirksamer Schutz gegen die Botnets der Zukunft

Der folgende Artikel ist ein Auszug aus dem White Paper *Understanding and Blocking the New Botnets*, recherchiert und verfasst von Scott Pinzon (CISSP) und Corey Nachreiner (CISSP) vom WatchGuard® LiveSecurity® Team; eine faszinierende Abhandlung über Botnets, ihre Entstehung und aktuelle Technologie. Ihr kostenloses Exemplar können Sie unter www.watchguard.com/whitepapers.asp herunterladen.

Botnets sind der perfekte Blended Threat, denn mit ihrem Code lässt sich praktisch jede Form von Malware übertragen, von Spyware über Downloader bis hin zu Rootkits, Spam-Engines und vielem mehr. Obwohl die beste Waffe gegen diese vielschichtige Bedrohung ein mehrschichtiges Verteidigungssystem ist, zeigen sich auch althergebrachte Techniken immer noch erstaunlich effektiv. Nachfolgend finden Sie Empfehlungen, wie Sie das Risiko einer Bot-Infektion Ihres Netzwerks deutlich verringern können.

1. Aktuelle Patches

Bot-Infektionen können über eine Vielfalt an Bedrohungen erfolgen. Die größten und wirksamsten Bots aber greifen Sicherheitslücken an, *für die es bereits sechs bis achtzehn Monate zuvor Patches gab*, in Extremfällen sogar bis zu 4 Jahre. Keiner weiß genau, warum Bots immer noch auf bekannte und völlig veraltete Bedrohungen programmiert werden, obwohl sich ihre Kommunikations- und Backend-Systeme rasend schnell weiterentwickeln. Wir können nur annehmen, dass Botmaster ein Reverse-Engineering neuer Patches durchführen und so Sicherheitslücken finden.

Es ist zu vermuten, dass Botmaster in Zukunft vermehrt aktuelle Patches ins Visier nehmen werden. Bis dahin gilt für Netzwerkadministratoren: Je schneller Sie Patches installieren, desto geringer die Gefahr für Ihr Netzwerk.

2. Blockieren von JavaScript

Ein webbasierter Bot-Angriff auf einen PC geschieht unweigerlich per JavaScript. Die meisten dieser Infektionen können Sie vermeiden, indem Sie die automatische Ausführung solcher Skripts in Ihrem Browser blockieren. Unserer Meinung nach empfiehlt sich dafür am besten Firefox mit dem NoScript Plugin.

3. Port-Überwachung

Diese Empfehlung teilt sich in zwei Bereiche.

1) Auch wenn aktuelle Bots über Ports kommunizieren können, die Administratoren gezwungenermaßen geöffnet lassen müssen, gelangt eine Vielzahl von ihnen immer noch über den IRC- (Port 6667) oder andere Ports mit hohen, ungeraden Nummern (wie 31337 und 54321) ins Netzwerk. Sofern Sie also nicht einen Port oberhalb von 1024 für eine benutzerdefinierte Anwendung oder Ähnliches benötigen, sollten sie dafür allen ein- und abgehenden Verkehr blockieren. Aber auch im anderen Fall können Sie sich schützen, indem Sie z. B. Richtlinien wie „Nur während der Bürozeit öffnen“ oder „Nur Datenverkehr von den vertrauenswürdigen IP-Adressen in dieser Liste zulassen“ definieren. Einfache und langsam reagierende Bots können so von ihrem Command and Control Center (C&C) nicht mit Anweisungen und Updates versorgt werden und lassen sich so praktisch sofort bei Ankunft ausmerzen.

2) Botnet-Verkehr, der über häufig verwendete Ports wie 80 oder 7 weitergeleitet wird, verrät sich nicht selten durch Datenpakete, wo keine sein sollten. Die meisten Botmaster aktualisieren ihre Zombies (infizierte PCs) zu nachtschlafener Zeit zwischen 01.00 und 05.00 Uhr. Prüfen Sie also Ihre Protokolle jeden Morgen auf Webbrowsing-Aktivitäten ohne Benutzeraktivität und Sie werden verdächtige Einträge schnell finden.

Administratoren mit WatchGuard-Firebox®-Modellen werden sich freuen zu hören, dass die Proxys dieser Appliances nicht-standardmäßigen Verkehr über Standardports blockieren. So unterbindet beispielsweise das HTTP-Proxy automatisch vom Spamming-Botnet Mega-D über den HTTP-Port 80 gesendete Daten.

4. Intensiviertes Benutzertraining

Manche Bots führen im Internet Massen-Scans nach anfälligen Rechnern durch und infizieren diese. Weiter verbreitet ist heute jedoch das so genannte „Social Engineering“. Dabei werden arglose Benutzer dazu gebracht,

einen Link oder eine Datei zu öffnen. Diese Bots besitzen dieselben Beschränkungen wie ältere Spyware: sie sind nur dann gefährlich, wenn Sie Ihnen Tür und Tor öffnen.

Diese „Ködermethode" ist mittlerweile zu einem Auslaufmodell geworden, denn die meisten Attacken geschehen heute per Internet. Während E-Mails vor zwei Jahren noch mit bösartigen Anhängen versendet wurden, enthalten sie heute Links zu bösartigen Sites. Oft werden auch harmlose Websites mit dem Exploit-Toolkit Mpack oder einer anderen Malware infiziert, um unvorsichtige Besucher auszuspionieren.

Erklären Sie Ihren Benutzern deshalb so verständlich wie möglich, warum Sie sich vor solcher Malware hüten müssen. Warnen Sie davor, unerwünschte oder unerwartete Anhänge zu öffnen oder Links in E-Mails bzw. andere ungewöhnliche Varianten anzuklicken. Als Hilfe zur Benutzerschulung können wir Ihnen unser Video empfehlen (http://video.google.com/videoplay?docid=-4094518401580008932), in dem die Funktionsweise von Drive-by-Downloads für technische Laien illustriert wird. Durch den gewissenhaften Einsatz der oben angegebenen Vorbeugemaßnahmen bleibt Ihr Netzwerk auf Jahre hinaus vor Bots geschützt.

5. Ständige Wachsamkeit

Diese Empfehlung scheint zwar fast schon selbstverständlich, aber wir haben nicht wenige EDV-Administratoren getroffen, die so sehr mit zahlreichen Sicherheitsproblemen und der Verwaltung eines unterbesetzten Helpdesks beschäftigt sind, dass sie die Prüfung von Systemprotokoll oder Bandbreitennutzung vernachlässigen. Oft wissen sie noch nicht einmal, wer oder welches Gerät Verbindungen über das Netzwerk aufbaut.

Wenn dies alles auf Sie zutrifft, dann haben Sie ein Problem. Denn in diesem Moment kann schon ein Bot in Ihrem Netzwerk aktiv sein. Wenn Sie also Ihre Systemprotokolle nur selten prüfen, müssen Sie das unbedingt heute noch ändern. Sobald Sie einmal wissen, welche Netzwerkaktivitäten „normal" sind, benötigen Sie höchstens 30 Minuten pro Tag, um notwendige Stichproben durchzuführen.

Wenn dies alles auf Sie zutrifft, dann heißt das nicht, dass Sie faul sind, sondern lediglich unter Personal- und Ressourcenmangel zu leiden haben. Erklären Sie Ihren Vorgesetzten das Problem und bitten Sie sie, Ihnen jeden Morgen eine halbe Stunde für die Prüfung des Netzwerkstatus einzuräumen. Von dieser Aufgabe sollten Sie sich auch nicht von Besprechungen, Konferenzgesprächen und anderen Unterbrechungen abhalten lassen. Denken Sie daran: Ein infiziertes Netzwerk kann Sie teuer zu stehen kommen, diese Vorbeugemaßnahme nicht.

Wir glauben, dass die aktuellen, massiven Bot-Attacken nur die Spitze des Eisbergs sind. Nie zuvor in unserer langjährigen Tätigkeit im Bereich Internetsicherheit kamen im Laufe eines Monats so viele völlig neue Bedrohungen in Umlauf, *für die kein Experte eine richtige Erklärung hat*.

Botnets waren schon immer eine Form des Blended Threats, aber bis dato nicht in dieser Perfektion. So ergänzen Botmaster mittlerweile die traditionelle Botnet-Architektur mit Komponenten, die die Automatisierung und Administration verbessern und eine Entdeckung erschweren. Die Ausgereiftheit dieser Technologiekombinationen ist wahrhaft erschreckend. So muss man kein Prophet sein, um vorherzusagen, dass sich dieser Trend nicht nur fortsetzen, sondern noch weiter verstärken wird.

Also werden die Bösewichte siegen? Wohl nicht, denn bis dato mussten wir Internet-Banking und Online-Shopping ja auch nicht aufgeben. Aber die Flut der Bot-Aktivitäten nimmt spürbar zu und wir müssen alles tun, um sie einzudämmen und den Botmastern das Handwerk zu legen. Die beste Strategie ist dabei, dem Bot-Code die Infizierung zu erschweren. WatchGuard Security Appliances verwenden z. B. mehrere Sicherheitsschichten, die intelligent über mehrere Protokolle verteilt und mit einer leistungsstarken Proxy-Technologie ausgestattet sind. Sie prüfen ein- und abgehenden Verkehr effektiv auf Malware und sorgen so für eine optimale Netzwerksicherheit.

Informationen zu WatchGuard Sicherheitslösungen und wie sie gegen Botnets und andere Netzwerkbedrohungen schützen, erhalten Sie unter www.watchguard.de oder von Ihrem Händler.