Presseinformation

Zehn Tipps für eine effektive Bot-Abwehr

Westcon Security unterstützt den Channel bei der Bekämpfung von Botnetzen

Paderborn, 29.05. 2013 – Westcon Security, ein Geschäftsbereich der Westcon Group, unterstützt Systemhäuser und Integratoren bei der Planung und Umsetzung ganzheitlicher Bot-Abwehrstrategien. Aufsetzend auf ein breites Portfolio marktführender Produkte und eigener Professional Services hat der VAD einen Best-Practice-Leitfaden entwickelt, der Systemhäusern hilft, Unternehmensnetze zuverlässig vor Bot-Infektionen zu schützen und infizierte Systeme zeitnah zu erkennen und zu isolieren.

Botnetze haben sich auf Grund ihres immensen Leistungspotenzials binnen weniger Jahre zu einer der gefährlichsten Waffen im Arsenal der Cyberkriminellen entwickelt. Als ‚Dark Clouds' bündeln sie die Speicher- und Rechenleistung von Millionen verteilter PCs und bieten Hackern zahllose lukrative Einsatzmöglichkeiten – von der Vermietung an Spam-Versender oder als Speicherplatz für illegale Inhalte über den Einsatz für verheerende DDoS-Angriffe bis hin zum Click-Jacking.

Bei der Abwehr der Botnetze können Unternehmen auf eine breite Palette von Best-Practice-Ansätzen zugreifen, die sie zuverlässig vor Infektionen schützen und Schäden durch infizierte Systeme verhindern. Die Westcon-Experten raten, bei der Absicherung der Netzwerke folgende zehn Regeln zu beachten:

1. **Aktueller Desktop-AV ist Pflicht:** Ein zuverlässiger Desktop-AV ist das A und O beim effektiven Schutz vor Bot-Infektionen. Achten Sie bei der Produktauswahl darauf, dass die Lösung neben E-Mails und Attachements auch Downloads scannen und dafür klassische Pattern- und Signatur-Filter sowie Reputationsanalysen unterstützen.
2. **Ergänzen Sie den Desktop-AV um ein Mail-Gateway:** Ein Secure-Mail-Gateway stoppt infizierte E-Mails vor dem Netzwerk und senkt so nachhaltig das Risiko einer Bot-Infektion. Im Idealfall sollten Mail-Gateway und Desktop-AV dabei von verschiedenen Herstellern stammen, um auch dann optimalen Schutz zu garantieren, wenn ein Produkt für ein Pattern länger braucht.
3. **Stoppen Sie Malware aus dem Internet mit einem Web-Gateway:** Die häufigste Ursache für Bot-Infektionen ist das Surfen auf infizierten Web-Seiten. Schutz bietet ein Web-Gateway, das über URL- und Kategorie-Filter Zugriffe auf kompromittierte Seiten stoppt. Die Lösung sollte reputations- und patternbasierte Filter kombinieren und auch den SSL-Traffic scannen. Das Gateway macht sich doppelt bezahlt: Es schiebt Online-Infektionen einen Riegel vor und verhindert, dass infizierte PCs Kontakt zum Command & Control-Server (C&C) aufnehmen.
4. **Konfigurieren Sie Ihre Firewall restriktiv:** Bots kontaktieren ihren C&C über unterschiedlichste Kanäle: ältere kommunizieren über IRC, neuere in der Regel über HTTP. Besonders beliebt sind aktuell Bots, die ihre Anfragen im SSL-Traffic an der Firewall vorbeischleusen oder in Tweets und Facebook-Apps verstecken. Schutz bietet nur eine restriktiv konfigurierte Firewall, die lediglich tatsächlich benötigte Ports und Protokolle zulässt.
5. **Überwachen Sie auch die Anwendungsebene:** Selbst die zuverlässigsten Firewalls und Web-Gateways können Kommandos in Tweets und Facebook-Apps nicht immer entdecken – daher

sollten Sie diese Kommunikationskanäle mithilfe einer Next Generation Firewall oder einer dedizierten App Control-Lösung im Auge behalten.

6. **Bei kritischen Web-Anwendungen lohnt sich eine WAF:** Unternehmen, die viele oder geschäftskritische Web-Anwendungen betreiben, sollten die Investition in eine dedizierte Web Application Firewall prüfen. Als lernendes System überwacht die WAF das Verhalten von Anwendern und Anwendungen und stoppt gängige Angriffsmuster wie SQL-Injections oder Cross-Site-Scripting.
7. **Ein IDP garantiert höchste Transparenz:** Mit IDP-Lösungen lässt sich der gesamte Datenstrom feingranular nach Kontaktaufnahmen zum C&C oder nach dessen Kommandos durchsuchen. Die IDP-Implementierung ist in der Praxis meist nicht so aufwändig wie im Vorfeld befürchtet: Für die meisten IDP-Lösungen sind getestete, vorkonfigurierte Regelwerke erhältlich, die vom ersten Tag an zuverlässig vor Schäden durch Bots schützen.
8. **Behalten Sie die Mobilgeräte im Blick:** Smartphones und Tablets stellen ein Haupteinfallstor für Viren dar. Installieren Sie eine unternehmensweite Mobile-Security-Suite, die zumindest eine Personal Firewall, Mobile AV, sicheren Remote Access und zentralisierte Management-Features umfasst. Noch besser ist, wenn auch starke Client-Encryption enthalten ist.
9. **Halten Sie sich über neue Produkte auf dem Laufenden:** Gerade im Bereich Bot-Abwehr kommen aktuell immer wieder innovative Produkte auf den Markt – etwa die intelligente, auf Honey-Pots basierende Intrusion-Deception-Lösung Mykonos von Juniper Networks oder das Antibot-Software Blade von Check Point. Stoßen Sie auf eine interessante neue Technologie, unterstützt Sie Westcon gerne bei der Teststellung.
10. **Schulen Sie Ihre Mitarbeiter:** Ein gut informierter Anwender ist und bleibt der beste Schutz. Durch Security-Awareness-Workshops werden Ihre Mitarbeiter für das Thema Bot-Detection und unterschiedlichste Angriffe sensibilisiert.

Für Unternehmen, die sich vertieft in das Thema Bot-Abwehr einlesen möchten, hat Westcon Security die achtseitige Best Practice-Broschüre „Botnetze. So schützen Sie Ihr Netzwerk“ veröffentlicht. Das Dokument kann per E-Mail an marketing@westconsecurity.de kostenfrei angefordert werden.

Mehr Informationen
In mehr als 25 Jahren hat sich Westcon einen Ruf als marktführender Anbieter von IT Sicherheits-Technologien erarbeitet. Durch seine hervorragenden Beziehungen zu den strategisch wichtigsten Akteuren auf dem Markt – und unübertroffene Erfahrungen im Umgang mit der gesamten Bandbreite an Lösungen – stellt Westcon Services und Support bereit, mit denen Reseller neue Geschäftsmöglichkeiten nutzen können, die sich aus dem marktführenden Security-Portfolio ergeben. Aktuelle Diskussionen über Westcon finden Sie in der XING Gruppe von Westcon Security unter https://www.xing.com/net/westconsecurity.

Über die Westcon Group
Die Westcon Group Inc. ist ein Value Added Distributor von führenden Unified Communications-, Infrastruktur-, Data Center- und Security-Lösungen mit einem weltweiten Netzwerk von spezialisierten Wiederverkäufern. Die Westcon Teams erstellen einzigartige Programme, und bieten außergewöhnliche Services, welche es unseren globalen Partnern ermöglichen, ihre Umsätze zu steigern. Eine starke Beziehung zu jedem Bereich der Westcon Group Organisation ermöglicht es Partnern, einen auf die

Bedürfnisse maßgeschneiderten Support zu erhalten. Von weltweiten Logistik-Services und flexiblen, den Bedürfnissen angepassten Finanzierungslösungen bis hin zu Presales-Unterstützung, Entwicklungsunterstützung und technischer Unterstützung, arbeitet das Unternehmen mit Partnern sehr agil und schnell auf sich ändernde Marktgegebenheiten reagierend, um diese noch schneller erfolgreich zu machen. Das Portfolio an marktführenden Herstellern der Westcon Group umfasst unter anderem: Check Point, Avaya, Juniper Networks, F5, Cisco, Polycom, and Blue Coat. Um mehr zu erfahren besuchen Sie bitte: www.westcongroup.com.

Mehr Info Westcon Security:
Westcon Group European Operations Ltd.
Christian Jantoß
Heidturmweg 64–66
33100 Paderborn
Tel. 0 52 51 / 14 56-286
Fax 0 52 51 / 14 56-100
E-Mail: christian.jantoss@westconsecurity.de
Internet: http://www.westconsecurity.de

Abdruck frei. Beleg bitte an:
H zwo B Kommunikations GmbH
Michal Vitkovsky
Am Anger 2
91052 Erlangen
Tel. +49 (0) 91 31 812 81 25
Fax +49 (0) 91 31 812 81 28
E-Mail: michal.vitkovsky@h-zwo-b.de
Internet: http://www.h-zwo-b.de