Februar 2013

Der Kampf gegen Botnetze

Die wichtigsten Punkte im Überblick

- Botnetze sind vernetzte infizierte Rechner, die von externen Kriminellen gesteuert werden. Sie führen, meistens ohne Wissen des Eigentümers, illegale Aktionen aus. Hierzu gehören der Versand von unerwünschten E-Mails genauso wie Betrugsversuche oder Attacken auf andere Rechner.

- Für Unternehmen und Regierungen stellen Botnetze eine enorme Bedrohung dar, weil sie sehr viele Rechner für gezielte gemeinsame Attacken auf IT-Infrastrukturen verwenden. Durch den gemeinsam mit IT-Unternehmen geführten Kampf gegen Botnetze und durch die Umsetzung ausgefeilter Regularien und Gesetze schützen Regierungen ihre Systeme und Bürger besser vor Botnetzen und damit verteilter Malware.

- Microsoft bekämpft Botnetze sehr aggressiv und in enger Zusammenarbeit mit Regierungen und Unternehmen. Wir stellen hierfür Sicherheitswerkzeuge zur Verfügung und unterstützen Unternehmen, Regierungen und Anwender.

HINTERGRUND

Ein Botnetz besteht aus vielen infizierten, mit dem Internet verbundenen Rechnern. Kriminelle Anwender steuern diese illegal und unbemerkt von den Eigentümern und nutzen sie für ungesetzliche Aktionen. Die Rechner in einem Botnetz werden auch Knoten, Bots, Robots oder Zombies genannt. Es handelt sich meistens um Rechner, die Anwender privat oder am Arbeitsplatz nutzen. Ein Rechner wird dann zu einem Knoten in einem Botnetz, wenn es einem Angreifer gelingt, Schadsoftware darauf zu installieren. Dies geschieht oft mit einem sogenannten Social-Engineering-Angriff, der die menschliche Schwäche eines Anwenders ausnutzt und ihn mit einem Trick zur Installation der Schadsoftware verleitet.

Die Eigentümer und Anwender bemerken es normalerweise nicht, wenn ein so infizierter Rechner für verbrecherische Zwecke genutzt wird. Ist ein Rechner von einer Botnetz-Malware infiziert, verbindet der Botnetz-Betreiber den Rechner unbemerkt mit dem Botnetz. Er versendet mit dem Rechner dann unerwünschte E-Mail-Werbung, hostet und verteilt damit Malware oder andere illegale Dateien oder attackiert damit andere Rechner.

Botnetze stellen für IT-Umgebungen von Unternehmen und Regierungen eine weitaus größere Gefahr dar als beispielsweise individuelle Hacker. Denn sie sind in der Lage, sehr viele Rechner für gezielte Angriffe zu koordinieren. Diese kombinierte Leistung blockiert mühelos nicht nur größte Websites und E-Mail-Server, sondern auch wichtige Kommunikations-, Datenverarbeitungs- und andere Elektroniksysteme.

Zudem bedrohen Botnetze auch IT-Wertschöpfungsketten.
Nach einer Microsoft-Untersuchung aus dem Jahr 2012 gelang es Cyber-Kriminellen, nicht ausreichend geschützte Wertschöpfungsketten mit dem Nitol-Botnetz zu infizieren. Dabei wurden auf Rechnern, noch vor deren Verkauf, unbemerkt mit Malware verseuchte Raubkopien installiert. Botnetze lassen sich zudem vollkommen anonym von Kriminellen – oft auch Botherders genannt – betreiben, weil sie den Ursprung einer Attacke hinter einem weit verzweigten Netz mit vielen Rechnern verbergen.

DER MICROSOFT-ANSATZ

- Wir bekämpfen Cyber-Verbrechen mit innovativen Technologien, gerichtlichen Schritten und Aufklärung der Anwender.
- Wir unterstützen Regierungen und gesetzgebende Organe mit technischen Trainings sowie bei kriminaltechnischen Ermittlungen und Untersuchungen. Zudem entwickeln wir kontinuierlich neue Werkzeuge für den Kampf gegen Cyber-Kriminalität.
- Mit der Initiative Microsoft Active Response for Security (MARS) vereinen wir rechtliches und technisches Fachwissen, um kriminelle Infrastrukturen aktiv zu vernichten. Dazu gehören zivilrechtlich eingeleitete Verfahren, aber auch technische Untersuchungen, mit denen wir Botnetze zerstören, sowie die Beschlagnahmung von Infrastrukturen und Domänen, mit denen Cyber-Kriminelle Botnetze kontrollieren. Mit den dabei gewonnenen Informationen erhöhen wir den Schutz aller Internet-Nutzer.

  MARS ist eine gemeinsame Initiative der Microsoft Digital Crimes Unit, des Microsoft Malware Protection Center, der Customer Support Services und von Trustworthy Computing. Einige Beispiele für den Erfolg der MARS-Initiative sind die kürzlich zerstörten Botnetze Waledac, Rustock, Kelihos, Zeus, Nitol und Bamital.

STRATEGISCHE ÜBERLEGUNGEN

- **Öffentlich-private Partnerschaften**. Wir freuen uns über die Unterstützung von Regierungen und gesetzgebenden Organen im Kampf gegen Botnetze. Die Kooperation mit Behörden ist unserer Meinung nach ein wesentliches Mittel, um Cyber-Bedrohungen effizient zu reduzieren, weil dabei auch entsprechende Gesetze und Regularien zum Einsatz kommen. Dazu gehören Initiativen wie der Anti-Bot-Verhaltenskodex für Internet Service Provider, den die U.S. Federal Communications Commission empfiehlt. Wir sind zudem überzeugt davon, dass eine Lockerung bestimmter Restriktionen in vielen Unternehmen zu mehr Innovationen und mehr Flexibilität im Kampf gegen Cyber-Kriminalität führen würde.
- **Internationale Kooperationen**. Wir fordern, wie viele andere Unternehmen auch, Staaten auf, das Übereinkommen über Computerkriminalität des Europarats zu übernehmen und zu ratifizieren. Die Unterzeichner verpflichten sich damit, die eigenen Gesetze und Prozeduren so anzupassen, dass sie dem Übereinkommen entsprechen und mit dessen Zielen übereinstimmen.
- **Kompromissloses Durchsetzen und ausgewogene Regularien**. Wir unterstützen eine kompromisslose Gesetzgebung, die rigorose Anwendung der Gesetze im Kampf gegen Botnetze und Cyber-Kriminelle unnachgiebig anklagt und verurteilt. Gleichzeitig ist es wichtig, dass diese Gesetze nicht nur Innovationen ermöglichen, sondern auch neue Technologien unverzüglich verwenden.

Hilfreiche Ressourcen

Das Microsoft Safety and Security Center hilft Ihnen mit Informationen über Sicherheitsthemen
www.microsoft.com/security

Die Microsoft Digital Crimes Unit
www.microsoft.com/dcu