IT Security

Aktuelle Verfahren zur IRC und P2P Botnetzerkennung und -bekämpfung

IRC: Bernhard Waldecker

P2P: Wolfgang Reidlinger

Agenda

- Einleitung/Erklärung
- Hostbasierte Erkennungsverfahren
- Netzwerkbasierte Erkennungserfahren: IRC
- Spezielle Eigenschaften von P2P Botnetzen
- Botnetzabwehr
- P2P Botnet Tracking
- Botnetze und deren Schwachstellen
- Aktuelle Produkte zur Botnetzerkennung

Einleitung

Einleitung

- Probleme die verursacht werden durch Botnetze:
  - Spam E-Mails
  - Distributed Denial-of-Service (DDOS) Angriffe
  - Identitätsdiebstähle
  - Usw.
- Größe der Botnetze hat sich verringert, Anzahl der kleinen Botnetze ist gestiegen (8)
- Kleinere Botnetze sind schwieriger zu detektieren

Einleitung

- Kommunikationsarchitektur spielt eine wichtige Rolle, 3 Arten (7):
  - Zentral: Internet Relay Chat (IRC)
  - Zentral: Hypertext Transfer Protokoll (HTTP)
  - Dezentral: Peer-to-Peer (P2P)
- Infizierung des Systems:
  1. Botmaster identifiziert neues mögliches Opfer
  2. Angriff auf Opfer wird gestartet
  3. Nach einem erfolgreichen Angriff, lädt der neue Bot die entsprechenden Binaries von einem zugehörigen Botnetzserver und installiert diese
  4. Weitere Schritte sind Abhängig von der Architektur

Botnetzerkennung

- Hostbasierte Verfahren
- Netzwerkbasierende Verfahren
- Kombinierte Verfahren

Hostbasierte Verfahren

Hostbasierte Verfahren

- Erkennung von möglichen Anomalien oder Änderungen am Filesystem des jeweiligen Hosts
- AntiViren Software
  - (für jede Schadsoftware) Signatur notwendig
  - Reaktive Maßnahme
  - Schwäche: Abänderung des Quellcodes, somit müssen Signatur nicht mehr zutreffen (2)
  - Schwäche: je geringer die Verbreitung, desto niedriger die Wahrscheinlichkeit einer Signatur (1)
  - Lösung: Software auf Verhalten mit bisher bekannter Malware untersuchen (2)

Hostbasierte Verfahren

- Auffindung von
  - ungewollten Files
  - neuen bzw. modifizierten Files
  - gelöschten Files
- Sammlung und Analyse von Malware Binaries mittels Honeypots (3)
  - Extrahieren von zB IRC relevanten Daten wie Username, Kanalname, DNS oder IP

Netzwerkbasierende Verfahren

IRC: Netzwerkbasierende Verfahren

Allgemeines

- Untersuchung des Netzwerkverkehrs auf
  - Anomalien
  - Protokoll spezifische Eigenheiten
  - relevante Pakete: IRC und TCP
- Vertical Correlation (2)
  - Erkennung einzelner bzw. individueller infizierter Systeme
  - Schwäche: wie bei AntiViren Software
- Horizontal Correlation (2)
  - Detektion von zwei oder mehreren infizierten Systemen anhand der Ähnlichkeit des Netzwerkverkehrs
  - Schwäche: einzelner oder unterschiedliche Bots können nicht erkannt werden

IRC: Netzwerkbasierende Verfahren

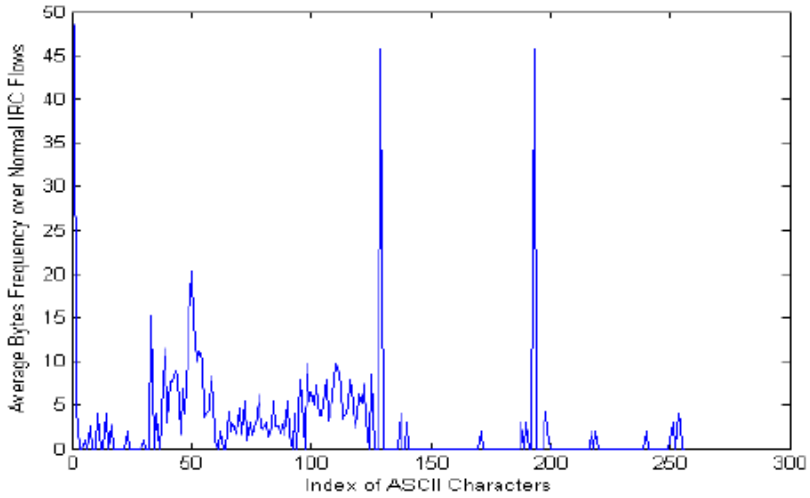
Erkennungsverfahren: Anomalien

- Anomalie = Abweichung oder eine besondere Auffälligkeit zum üblichen Netzwerkverkehr
- 1. Methode (4)
  - Hohe Netzwerklast, verursacht durch
    - Netzwerkscans
    - Mangel an Servern
    - P2P Applikationen
  - Beispiel: Spambot
    - Gegenüberstellung der gesendeten und empfangen E-Mails

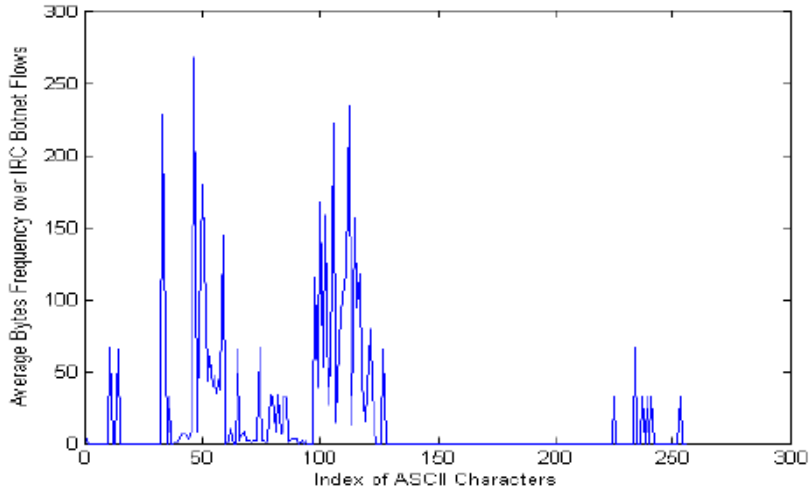
IRC: Netzwerkbasierende Verfahren

Erkennungsverfahren: Anomalien

- 2. Methode (5)
  - Kürzere Antwortzeit des IRC Clients zum Command & Controll Server



Average byte frequency over 256 ASCIIs for normale IRC florws (5)



Average byte frequency over 256 ASCIIs for botnet IRC florws (5)

IRC: Netzwerkbasierende Verfahren

Erkennungsverfahren: IRC spezifische Eigenheiten

- Möglich durch die Standardisierung des IRC Protokolls
  - RFC 2810, RFC 1459 uvm.
- Beispiele für Kommunikationskommandos
  - NICK, JOIN, USER, QUIT, MODE
- Nicknamen müssen pro Kanal ein Unikat sein (6)
  - Botmaster erstellen die Usernamen aus einem konstanten zB Name des Trojaners oder Name des Landes und einem variablen Teil zB Zufallszahl
- Methoden zur Detektion häufig automatisiert zB Rishi oder IDS/IPS Snort

IRC: Netzwerkbasierende Verfahren

Erkennungsverfahren: IRC spezifische Eigenheiten Beispiel Rishi (6)

- Früheste mögliche Erkennung von der Kommunikation: Kontakt mit C&C nach Infizierung
- TCP Pakte werden auf standardisierte Kommandos untersucht
- Im Erfolgsfall werden folgende Parameter extrahiert und in „connection object“ gespeichert:
  - Timestamp
  - Quell IP und Port des Clients
  - Ziel IP und Port des Servers
  - Gewählter Kanal
  - Nicknamen
- Analyse der Nicknamen
  - Merkmale zB Sonderzeichen, Nummernfolgen
  - 52 Regular Expressions
  - Punktevergabe: 0 bis 15 Punkte, ab 10 Punkten möglicher Bot

IRC: Netzwerkbasierende Verfahren

Erkennungsverfahren: IRC spezifische Eigenheiten Beispiel Rishi (6)

ID	Nickname	AV-scanner output
1	[00|DEU|172507]	Worm/Aimbot.AE.6
2	|DEU|2K|92193	not found
3	[XP]|6454734036	Worm/Rbot.171008.6
4	DEU|245500	Worm/Rbot.166912.5
5	LL-9985168738	Worm/Rbot.146432.10
6	ZX-44697595408	Worm/Rbot.166912.7
7	ASN-649955079	Worm/Rbot.90112.46
8	ZD-91817267335	Worm/Rbot.91136.62
9	[RAPEDv2]775571	Worm/Rbot.455680
10	{ripper}-310167	Worm/SdBot.56924.A
11	[SOUL]983586	Worm/SdBo.100864.22
12	[FUCK]-56507	Worm/Rbot.are
13	vjlr_13	W32/Parite
14	ezbxtju_12	Worm/Korgo.I
15	jeck-1_8887_1350	Trojan.Zlob.Gen

IRC: Netzwerkbasierende Verfahren

Erkennungsverfahren: IRC spezifische Eigenheiten Beispiel Rishi (6)

- White- und Blacklist
  - statische und dynamische Einträge
  - Whitelist: dynamische Einträge für „0“ Punkte
  - Blacklist: dynamische Einträge ab „10“ Punkten
- Schwächen
  - wenn Bots verwenden „reguläre“ Nicknamen verwenden
  - IRC Protokollabhängikeiten, d.h., keine Abänderung von zB den Kommandos
  - Hardware Limitierung: bei zu vielen Paketen können IRC Pakte übersehen werden

Quellen:

(1) Deutsches Bundesamt fuer Sicherheit in der Informationstechnik (BSI) (2009). BSI-Lagebericht IT-Sicherheit 2009

(2) Wurzinger, P. / Bilge, L. / Holz, T. / Goebel, J. / Kruegel, C. / Kirda, E. (2009). Automatically Generating Models for Botnet Detection TR-iSecLab-0609-001

(3) Zhuge, J. / Holz, T. / Han, X. / Guo, J. / Zou, W. (2007). Characterizing the IRC-based Botnet Phenomenon

(4) Binkley, J. R. / Singh, S. (2006). An Algorithm for Anomaly-based Botnet Detection. In: Proceedings of USENIX Steps to Reducing Unwanted Traffic on the Internet Workshop (SRUTI), S. 43–48

(5) Lu, W. / Tavallaee, M. / Rammidi, G. / Ghorbani, A. A. (2009). BotCop: An Online Botnet Traffic Classifier. In: CNSR '09: Proceedings of the 2009 Seventh Annual Communication Networks and Services Research Conference, S. 70–77, Washington, DC, USA. IEEE Computer Society.

(6) Goebel, J. / Holz, T. (2007). Rishi: Identify Bot Contaminated Hosts by IRC Nickname Evaluation. In: HotBots'07: Proceedings of the first conference on First Workshop on Hot Topics in Understanding Botnets, Berkeley, CA, USA. USENIX Association

(7) Holz, T. (2009). Tracking and Mitigation of Malicious Remote Control Networks. PhD thesis, Universitaet Mannheim

(8) Deutsches Bundesamt fuer Sicherheit in der Informationstechnik (BSI) (2007). BSI-Lagebericht IT-Sicherheit 2007

Spezielle Eigenschaften von P2P Botnetzen

- Benötigen keinen zentralen C&C Server
- Unempfindlicher auf Störungen von Außen
- Jeder Bot ist Client und Server zugleich
- Äußerst stabile Kommunikationsstruktur

Botnetzabwehr

- Keine Symptombehandlung
  - DDoS Attacken, Spam Attacken sonstige Attacken
- Organisatorische Maßnahmen
  - Patchlevel der Systeme
  - Aktuelle Virensignaturen der AVs
  - Blacklists für bekannte C&C Server
  - DEP Aktivieren
- Warum so schwere?
  - Infektionsvektor bei neuen Bots meist unbekannt (Applikation, Service)
  - Schadcode wird durch Code Morphing verändert
  - Zero Day Exploits

P2P Botnet Tracking

Aufspüren, analysieren und infiltrieren, abschwächen

- Bootstrapping Process
  - Bot- / Malware Sample
  - infection vector ermitteln
  - vulnerable applications simulieren
  - virtuelle Umgebung | Honeybot mit Bot infizieren
  - alle Aktivitäten am Netz und System aufzeichnen und analysieren
- Infiltration and Analysis
  - Entwicklung eines speziell angepassten P2P-Clients
  - Verbindung zum Botnetz (Botmaster)
  - Kommandos aufzeichnen und analysieren
- Mitigation
  - Größe des Botnetzes ermitteln
  - Störung der Kontrollinfrastruktur (Kommunikationsprotokoll oder Server)

Botnetze und deren Schwachstellen

Schwachstellen sowie deren Gegenmaßnahmen

- Unverschlüsselte Übertragung von Kommandos
  - Implementierung von Public Key Cryptography
- Kommunikation über wenige zentrale Server
  - Antwort waren P2P Botnetze
- Authentifizierung der Bots am Botnetz
  - Implementierung von Authentifizierungsmethoden

Aktuelle Produkte zur Botnetzerkennung

- BotHunter
  - Entwicklung von College of Computing | Georgia Institute of Technologie und SRI International
  - Verfahren wurde zum Patent angemeldet
  - erhältlich für Linux, Windows, Mac OS X und FreeBSD
  - Hauptsponsor ist das US-Army Research Office (ARO)
  - www.bothunter.org

- BotSniffer
  - Entwickelt am College of Computing | Georgia Institute of Technologie
  - benötigt keine Kenntnis von Bot Signaturen
  - beschränkt auf Bots mit IRC und HTTP Kommunikation
  - http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.110.8092&rep=rep1&type=pdf

Aktuelle Produkte zur Botnetzerkennung

- BotProbe
  - Entwicklung von Texas A&M University, SRI International und Georgia Institute of Technology
  - Erkennt speziell verschleierte und selten stattfindende C&C Kommunikation
  - Erkennt IRC Bots, P2P sowie HTTP Funktionalität ist in Planung
  - Unterscheidet C&C von Mensch-zu-Mensch Kommunikation
  - http://faculty.cs.tamu.edu/guofei/paper/botProbe_acsac09_slides.pdf

- BotMiner
  - Benötigt kein Bot Signaturen
  - Erkennt IRC, HTTP und P2P Bot Kommunikation
  - http://faculty.cs.tamu.edu/guofei/paper/botMiner-Security08-slides.pdf

Vielen Dank für Ihre Aufmerksamkeit.

Fragen im Anschluss, oder E-Mail an:

Wolfgang Reidlinger: is081021@fhstp.ac.at

Bernhard Waldecker: is081031@fhstp.ac.at