



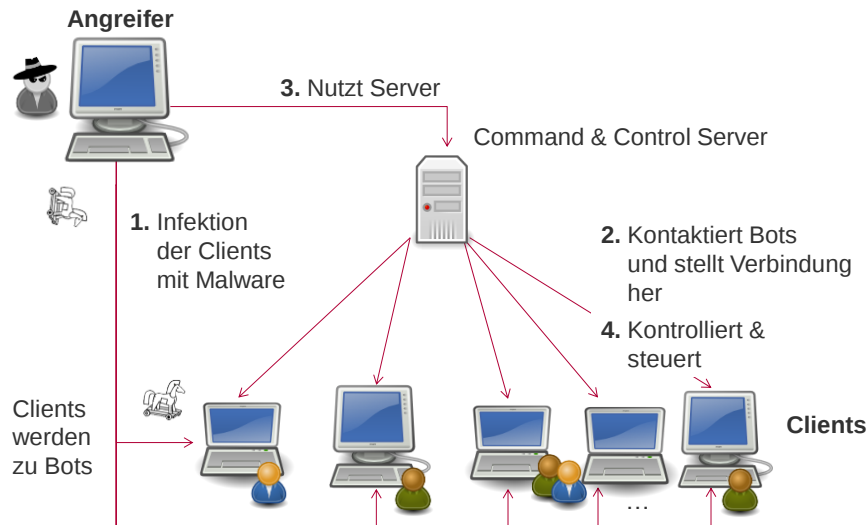
openHPI – Sicherheit im Internet
Malware: Botnets

Prof. Dr. Christoph Meinel
Hasso-Plattner-Institut, Potsdam

Botnets

Erste Beschreibung

- Ferngesteuerter Zusammenschluss (vieler) verschiedener Computer - **Bots** -, der typischerweise ohne Wissen der jeweiligen Computerbesitzer durch Malware hergestellt wird
- (Zentraler) „**Command and Control Server**“ – **C&C Server** –
– in den Händen eines Angreifers verwaltet, koordiniert und steuert die (zahlreichen) Bots
- C&C Server übernimmt Fernsteuerung und Kontrolle über die Bots und schickt Handlungsanweisungen, die diese dann selbstständig ausführen
- Durch den Zusammenschluss zahlreicher Bots kann eine Vielzahl von Angriffen mit hoher Rechenkraft erfolgen



- Angreifer infiziert viele Clients mit Malware
 - meist kommen Trojaner zum Einsatz, um wirkliche Funktion zu verschleiern
 - aber auch Würmer ermöglichen schnelle automatische Verbreitung
 - schließlich dienen Schwachstellen im Web-Browser als Einfallstor
- Malware ermöglicht Kommunikation mit dem C&C Server
- Clients, die zu „Bots“ geworden sind, können anschließend die Befehle des C&C Servers empfangen und ausführen
 - Angreifer kann seine Befehle über C&C Server an die Bots versenden
 - Bots führen Befehle daraufhin selbstständig aus

Cyberkriminelle nutzen Botnets zum

- Durchführen von verteilten Denial of Service Angriffen – DDoS
- Versand von Spam-E-mails
- Verschleierung von Absenderadressen des Angreifers
- Ausführung von Klickbetrug
- Auslesen sensibler Daten der Bots, z.B. Passwörter,...
- Bereitstellung von illegalen Informationen und Ressourcen (Speichermedium / Serviceanbieter)
- Berechnung / Schöpfung von Kryptowährung (Bitcoin Mining)
- Einsatz von Ransomware, z.B. zur Erpressung durch Verschlüsseln persönlicher Daten und Angebot zur kostenpflichtigen Freigabe des Schlüssels

Zeus

- Geschätzte Größe: 3.600.000 Bots
- Entdeckt: 2007

Conficker

- Geschätzte Größe: 9.000.000 Bots
- Entdeckt: 2008

Bredolab

- Geschätzte Größe: 30.000.000 Bots,
- Entdeckt: 2009

ZeroAccess

- Geschätzte Größe: 9.000.000 Bots
- Entdeckt: 2011

Beispiel für Botnet-Angriff: Bitcoin Mining

Botnets sind dank ihrer riesigen Zahl an Bots sehr gut geeignet, Aufgaben zu erfüllen, die extrem hohe, aber leicht zu verteilende Rechenleistung erfordern, z.B. Bitcoin Mining

- Bitcoin Mining verbraucht sehr viel Rechenleistung, lässt sich aber leicht verteilen
- Einzelner PC ist dazu kaum in der Lage, aber wenn viele PCs zusammengeschaltet werden, können brauchbare Resultate erzeugt werden
- Erste „Prototypen“ entstanden in Universitäten, in denen Studenten oder Angestellte Arbeitsrechner zum „Minen“ nutzten
- Im Dezember 2013 wurden zwei deutsche Hacker verhaftet, die einen Trojaner zum „Minen“ modifiziert und damit Bitcoins im Gegenwert von 950.000 US\$ generiert hatten ...

„Storm“ Botnet (1/2)

„**Storm**“ Botnet wurde erstmals 2007 entdeckt wegen einer starken Verbreitung des Storm-Worms

- Verbreitung via Spam-E-mails und anschließende Infektion von Windows Systemen
- Geschätzte Größe: 1-50 Millionen Bot-PCs
- Betreiber blieben bisher unentdeckt
 - Sicherheitsexperten / Forscher wurden massiv angegriffen, sobald Nachforschungen angestellt wurden
- Antivirus-Programme als Gegenmaßnahmen wurden aus der Ferne ausgeschaltet, dem Nutzer aber vorgegaukelt, sie wären in Funktion
- War stark genug, um ganze Länder vom Internet zu trennen
- Teilweise sogar leistungsfähiger als Supercomputer ...

„Storm“ Botnet (2/2)

- Ende 2007 begannen die Betreiber des „Storm“ Botnets ihre Organisation aufzuteilen, womöglich um Teile des Botnets zu verkaufen
- Datenverkehr zur Kommunikation mit dem Botnet war verschlüsselt
- Architektur sehr komplex mit ganz verschiedenen Bestandteilen:
 - (1) Backdoor bzw. Downloader Malware
 - (2) SMTP Relay Server, um Emails zu verschicken
 - (3) Angriffssoftware zum Stehlen von Email-Adressen
 - (4) Angriffssoftware zur Verbreitung der Malware via Emails
 - (5) DDoS Angriffssoftware, um verteilte Angriffe auszuführen
 - (6) Aktualisierte Version von Malware-Installationsprogrammen

„Storm“ Botnet: Stormfucker

Vorgestellt auf dem Chaos Communication Congress (2008, Berlin)

- Eigenständiger Wurm, der nur Systeme infiziert, die bereits mit dem Storm-Wurm infiziert sind. Entfernt Storm-Malware über Update-Mechanismus
- Erlaubt Säuberung / Übernahme von Teilen des „Storm“ Botnets
 - Möglich, da in „Storm“ Botnets Identifikation des C&C Servern nur unzureichend durchgeführt wird
 - Verifikationsmechanismus konnte durch Brute-Force Angriffe geknackt und eigene Kommandos an C&C Server gesendet werden (Übernahme des C&C Server)
 - Aufforderung zum Updaten der Storm-Anwendung
 - Ersetzen durch gefälschte Anwendung
- Bots empfangen Kommandos nicht mehr vom ursprünglichen, sondern vom neuen C&C Server

Zeus (1/3)

Erstmals 2007 entdeckt

- Zielt auf Windows Systeme ab
- Trojaner enthält zusätzliche Software zum
 - Ausspähen persönlicher Daten im Web-Browser, z.B. Logins für soziale Netzwerke oder Online-Banking
 - Verschlüsselung sensibler Daten und anschließende Erpressung zur kostenpflichtige Herausgabe des Schlüssels
- Erfasste Daten von über 74.000 Nutzerkonten von Firmen wie: NASA, Bank of America, Oracle, Amazon, Cisco,...
- Durch Verschleiерungsmechanismen nur sehr schwer zu identifizieren
- Verbreitet sich durch Phishing und versteckte Downloads
 - Allein in den USA 3.600.000 infizierte Systeme

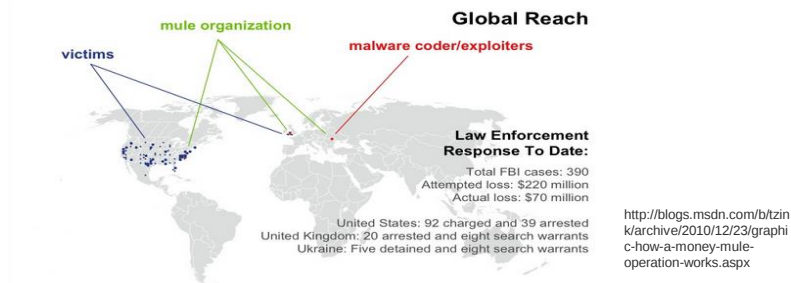
Zeus (2/3)

Betreiber von Zeus können fein granular auswählen, an welchen Informationen sie interessiert sind, z.B. Zugangsdaten zu bestimmten Diensten, Sozialen Netzwerken, Online-Banking, ...

- FBI informierte im Oktober 2010, dass es osteuropäischen Hackern gelungen war, weltweit Systeme mit Zeus-Malware zu infizieren
 - Es konnten Onlinekonten bei Banken übernommen und mehrere tausend Dollar zu Mittelsmännern transferiert werden
 - Mittelsmänner hatten zuvor Konten mit gefälschten Identitäten eröffnet und überwiesen das erbeutete Geld weiter oder schmuggelten es außer Landes
- Verursachter Gesamtschaden von ca. 70 Millionen US\$. Es wurden mehr als 100 Personen festgenommen

Phänomenal war hierbei die globale Organisation der Kriminellen

- Insgesamt wollten Cyberkriminelle 220 Millionen US\$ stehlen
- FBI registrierte 390 Betrugsfälle
- Die Hacker stammten aus Osteuropa, die Mittelsmänner aus Amerika, Großbritannien und Osteuropa und die Opfer weitgehend aus den USA



Zeus – Gameover ZeuS

Ende 2013 wurde Abwandlung „**Gameover ZeuS**“ entdeckt

- Ist Botnet, das ebenfalls für Bankbetrug und verbrecherische Verschlüsselung persönlicher Daten verwendet wird
- Im Gegensatz zu älterer Version wird Verbindung zum C&C Server verschlüsselt
- Generiert tausende Domänen-Namen, die zur Kommunikation dienen und nur einen Tag gültig sind
- Eine Variante zielt ab auf Systeme in der Ukraine und Weißrussland, eine andere auf Computer in den USA
- Im Juni 2014 gelang es einer internationalen Organisation „Operation Torvar“, die Verbindung zwischen C&C Server und Bots temporär zu trennen