Schadsoftware mit Honeypots fangen und analysieren

Stefan Schumacher

sicherheitsforschung-magdeburg.de
stefan.schumacher@sicherheitsforschung-magdeburg.de

Leipzig
GUUG FFG 2018



Über Mich



Über Mich

- Geek, Nerd, Hacker seit knapp 20 Jahren
- exNetBSD-Entwickler
- Bildungswissenschaft/Psychologie
- Berater für Finanzinstitute, Regierungen, Sicherheitsbehörden
- Direktor des Magdeburger Instituts für Sicherheitsforschung
  Forschungsprogramme zur Unternehmenssicherheit
- Herausgeber des Magdeburger Journals zur Sicherheitsforschung
- `www.Sicherheitsforschung-Magdeburg.de`
- 300. Vortrag seit dem CCC-Camp 2003 :-)



Forschungsprogramme des MIS

- Psychologie der Sicherheit
  - Social Engineering
  - Security Awareness, Sicherheit in Organisationen
  - Didaktik der Sicherheit
  - Didaktik der Kryptographie
- Lehrerfortbildung
  - Lernfelder: Fachinformatiker IT-Sicherheit
  - Lernfelder: IT-Sicherheit für Kaufleute
  - Lernfelder: IT-Sicherheit für Elektroberufe
- IT-Sicherheit in KMU
  - empirische Grundlagenforschung
  - didaktische Aufbereitung
  - Schulungen



Honeypot

- Honigtopf um Bären anzulocken und abzulenken
- Programm oder Server welcher das Verhalten eines Rechners, Netzes oder Anwenders simuliert
- Alle Interaktionen werden protokolliert und analysiert
- bessere SNR als IDS
- neue IDS-Regeln können generiert werden
- löst ggf Alarm aus (Einbruchserkennung)
- berechtigte Nutzer kontaktieren den Honeypot nicht, nur Einbrecher ohne Kenntnisse der Netztopologie
- Innentäter!
- Simulieren den Fingerabdruck des Betriebssystems (IP Stack)
- Skripte simulieren Dienste (sshd, httpd) und deren I/O-Verhalten



Honeypot

Interaktion, Aufwand, Risiko

- niedrige Interaktionsstufe: emuliert ein/mehrere Netzwerkdienste, niedriges Risiko, wenig Datensammlung (Zeit, IP und Port)
- mittlere Interaktionsstufe: Netzwerkdienste reagieren auf Angreifer (Fake-SSH oder FTP), kann Verwundbarkeiten in Diensten emulieren und Schadsoftware fangen, mittleres Risiko, gute Datensammlung
- hohe Interaktionsstufe: echtes OS als Bauernopfer, volle Kontrolle für Angreifer möglich, sehr hohes Risiko, sehr gute Daten, sehr gute Isolation nötig



- direkt im Internet (vor der Firewall): sofort angreifbar, ideal für Forschungssysteme, öffentliche IP benötigt
- im privaten Netz (hinter der Firewall): Frühwarnungssystem, zeigt wenn Außensicherung gebrochen wurde, Portforwarding benötigt, hohe Interaktionsstufe stark gefährdet und benötigt zusätzliche Absicherung
- in der DMZ (zwischen den Firewalls): beste Plazierung, Honeypot und andere DMZ-Server im selben Subnet!, können echte Systeme spiegeln und frühwarnen



Honeypot

- Cowrie: SSH (vormals Kippo)
- ConPot: SCADA
- GasPot: Veeder Root Guardian AST
- Dionaea: Malware
- Glastopf: Web-Application
- HoneyDrive VM (OVA)



SCHADSOFTWARE

- Software die nicht intendierte Dinge tut
- Software die böse Dinge tut
- Viren, Würmer, Trojaner, Rootkits, Spyware
- *nicht:* schadhafte Software



- Schadensabschätzung
- Angriffsvektoren identifizieren
- Sicherheitslücken aufdecken
- weitere Hinweise auf Kompromittierungen finden
- Schöpfungshöhe feststellen
- Angreifer identifizieren oder einschätzen (Cybern uns die Russen oder Chinesen?)



1. Welche (strategischen) Ziele verfolgt die Schadsoftware?
2. Welche Angriffsvektoren wurden ausgenutzt?
3. Wie kann ich die Schadsoftware loswerden?
4. Welche Daten wurden abgeschöpft und/oder manipuliert?
5. Wer greift uns an?
6. Welche Handlungskompetenz hat der Angreifer
7. Wie lange sind die Systeme schon kompromitiert?
8. Wie verbreitet sich die Schadsoftware weiter?
9. Sind andere Systeme infiziert
10. Wie verhindere ich weitere/zukünftige Infektionen?



Anaylse

Tips

- Dateinamen durch Hash ersetzen
- Ausführbare Dateien nicht ausführbar machen (NOEXEC, X-Bit bzw. exe_)
- Beim Versand in passwortgeschützte ZIP packen (`infected`)
- Wenn online VPN/Tor nutzen um eigene IP zu verschleieren - Achtung: unterschiedliches Verhalten nach Land
- VM zur Analyse nutzen oder dedizierte Maschine (Snapshots)
- anderes Betriebssystem und/oder Architektur nutzen (PowerBook G4 mit NetBSD)
- Images auf FTP-Server in isoliertem Netz ablegen mit G4U



Analyse

nach Hause telefonieren

- vereinfacht Analyse
- Netzwerkverkehr kann überwacht und analysiert werden
- Verhalten der Schadsoftware abhängig von Netzwerkverbindung
- Duell mit echten Menschen?
- eigene Maschine als Infektionsherd
- VM kann detektiert werden (*Malicious Hypervisor Threat – Phase Two: How to Catch the Hypervisor by Mikhail Utin, PhD*)
- 0Day?



Analyse

1. Virenscanner (offline / online)
2. statische Analyse: Datei wird nicht ausgeführt, Metadaten, theoretisch komplette Analyse möglich aber sehr aufwändig
3. dynamische Analyse: extraktion von Informationen während des Ausführens der Datei, Was macht die Schadsoftware wichtiger als wie macht sie es



- offline: ClamAV, F-Prot, Sophos
- Online-Analyse bei VirusTotal
- `https://www.virustotal.com/de/`
- scannt Datei oder URL mit 70 verschiedenen Virenscannern
- identifiziert Dateien über Prüfsummen
- registrierte Nutzer können Kommentare hinterlassen
- Identifikation über Prüfsummen (googlen)



- ExifTool: Perl-Programm, ursprünglich für Exif-Daten in Fotos, liest Metadaten aus
- strings(1): zeigt eingebette Strings an, können falsche Fährte legen nach auffälligen Strings googlen, könnte uU auch Alarm auslösen
- automatisierte Disassembler: `objdump(1)`, IDA Pro, AnalyzePE.py



- sichere Analyseumgebung notwendig, Snapshots, traue keinem Speicher
- Ziele: Aktivitäten der Schadsoftware (IO, IPC)
- strace, ltrace
- angr: angr is a platform-agnostic binary analysis framework developed by the Computer Security Lab at UC Santa Barbara and their associated CTF team, Shellphish.
- Cuckoo Sandbox: traced API calls, untersucht Netzwerkverkehr, untersucht Speicher des infizierten Systems
- Limon - Sandbox for Analyzing Linux Malwares



Visualisierung

ELK-Stack

- ElasticSearch
- Logstash
- Kibana

Wichtig für Geschäftsführung und/oder Sensibilisierung



- sicherheitsforschung-magdeburg.de
- stefan.schumacher@sicherheitsforschung-magdeburg.de
- sicherheitsforschung-magdeburg.de/publikationen/journal.html



- youtube.de/Sicherheitsforschung
- Twitter: 0xKaishakunin
- Xing: Stefan Schumacher