Lehrstuhl für Systemsicherheit
Prof. Dr. Thorsten Holz
Andre Pawlowski

Vorlesung Betriebssystemsicherheit
Wintersemester 2014/2015
Ruhr-Universität Bochum

5. Übung

12. Januar 2015
Abgabe der Hausaufgaben: per Moodle bis zum 19. Januar 2015, 16:00 Uhr
Bei Fragen und Problemen können Sie sich per E-Mail/Moodle an die Betreuer wenden.

Aufgabe 1 (PCAP-Analyse) (3 Punkte)

Als Analyst erhalten Sie den Auftrag, eine Netzwerkdump-Datei (`dump.pcap`) von einem Kunden zu untersuchen. Der Rechner, von dem der Dump stammt, wurde von einem Bot infiziert und es gibt Grund zur Annahme, dass der Bot aktiv Befehle von einem C&C-Server erhalten hat. Der Benutzer hat währenddessen weiter an seinem Rechner gearbeitet, weshalb auch eine Reihe von normalen Verbindungen im Dump zu finden sind.

Untersuchen sie den Netzwerkdump (am besten mit *Wireshark* oder einem ähnlichen Tool) und identifizieren sie die Verbindungen, die von dem Bot stammen. Dazu gehören alle C&C-Verbindungen sowie Netzwerktraffic, der in Folge von erteilten Befehlen entstanden ist. Schreiben Sie in Moodle eine kurze Zusammenfassung aller Verbindungen, die Sie gefunden haben und erklären Sie kurz, was genau passiert ist.

Aufgabe 2 (Bot-Analyse) (3 Punkte)

In dieser Aufgabe besteht Ihre Aufgabe darin, einen Bot (`bot.exe`) genauer zu analysieren. Der Bot versucht, sich zu einem bestimmten IRC-Server zu verbinden, um dort anschließend Befehle zu empfangen. Analysieren Sie den Bot und beantworten Sie folgenden Fragen:

1. Zu Beginn des Programm kopiert sich der Bot an eine bestimmte Stelle in das System. Wie lautet der Dateiname dieser Kopie?
2. Wie lautet der Hostname des C&C-Servers, auf den sich der Bot verbindet? Welchen IRC-Channel betritt der Bot?
3. Welche Aktion führt der Bot aus, wenn er das Kommando `something` erhält?

Der Bot sollte ausschließlich in einer virtuellen Maschine untersucht werden, da es sich um einen *echten*, potentiell bösartigen Bot handelt. Entsprechende Funktionalität wurde zwar deaktiviert, es ist aber trotzdem ratsam, eine VM zu verwenden (z.B. indem Sie eine Windows-VM mittels der MSDNAA-Lizenz aufsetzen). Zur Analyse können Sie die *Sysinternals Tools*, einen Debugger/Disassembler oder beliebige andere Tools verwenden. Eventuell ist es hilfreich, einen eigenen IRC-Server aufzusetzen und den Bot zu diesem Server verbinden zu lassen.

Geben Sie Ihre Antworten auf die Fragen im Moodle-Textfeld ab.