ATIS - Software Reverse Engineering

Prof. Dr. Christian Dietrich
dietrich@internet-sicherheit.de

5 Lab: Dynamic Code Analysis

Aufgabe

Dieses Mal ist die Lage kritisch. Die Hochschule ist offensichtlich Opfer eines Hacker-Angriffs geworden. Mehrere Fachbereiche sind betroffen, im Fachbereich Informatik wurde das Prüfungsamt infiziert und der Server, der alle Klausur- und Prüfungsergebnisse speichert, hat merkwürdige Ausgaben getätigt. Forensiker haben die Ausgaben festhalten können, sie lauten wie folgt:

```
[*] Connecting to server #1
[*] Sending request #1
[*] Successfully reached target environment in Gelsenkirchen.
[*] Sending request to C&C server


[*] System engaged. WIPING WILL BEGIN IN 2 HOURS !!!
```

Es ist wahrscheinlich, dass hier eine Schadsoftware am Werk ist. Die Ausgaben suggerieren, dass jegliche Inhalte auf dem Server in absehbarer Zeit gelöscht werden. Wenn jetzt nicht gehandelt wird, macht hier in diesem Jahr wohl keiner einen Abschluss...

Die Ermittler sind ratlos und trauen sich nicht, den Server auszuschalten, solange nicht geklärt ist, was eine mögliche Schadsoftware macht. Neben den Ausgaben konnte immerhin eine verdächtige Datei sichergestellt werden.

Unterstützen Sie die Ermittler indem Sie versuchen herauszufinden, was diese Datei beinhaltet oder macht. Jegliche Hinweise, die zur Ermittlung oder Ergreifung eines Täters führen sind dienlich. Versuchen Sie Spuren zu finden, zum Beispiel ob Netzwerkkommunikation stattfindet und wenn ja mit welchen Endpunkten und welchem Inhalt. Suchen Sie Hinweise auf Namen möglicher Autoren oder Operatoren. Beschränken Sie sich bei Ihrer Analyse nicht nur auf die Datei, sondern auch um möglicherweise kontaktierte Server.

Eingaben

- Datei mit dem Namen `botclient`

Abzuliefernde Ergebnisse

Beschreiben Sie Ihren Ansatz und fassen Sie die Ergebnisse (auch Zwischenergebnisse, falls Sie Ihrer Meinung nach nicht am Ende sind) zusammen und laden Sie sie als Textdatei hoch.

Hinweise

- Betrachten Sie die zur Verfügung gestellte Datei als bösartig und analysieren Sie sie ausschließlich in einer virtuellen Maschine, die Sie im Notfall zurücksetzen können. Dies gilt insbesondere für den Fall, dass Sie eine dynamische Analyse vornehmen.
- Überlegen Sie sich eine Strategie, wie Sie die zur Verfügung gestellte Datei analysieren wollen. Bilden Sie Teams und diskutieren Sie die Ansätze im Team.

- Möglicherweise ist die Datei obfuskiert. Erinnern Sie sich an die Inhalte der Vorlesung und überlegen Sie, welche Analysetechnik im gegebenen Fall vielversprechend aussieht.