IT Security, Assignment 1
Chasing a RAT

DIKU, block 4, April 30 2014

Imagine your an IT security consultant, and that you have been hired to help a company, the ficticious BIOchem, that has been infected with the well-known Poison Ivy RAT. BIOchem is a Danish-based and owned biochemical company with some 200 employees.

1 Initial infection vector

As it turns out Poison Ivy has been detected on a number of the company's Windows-based workstations. By analysing when the Poison Ivy files were created and correlating that with other file system activity, it is suspected that the RAT made its way onto the computers via a JAR file that was downloaded while visiting some compromised external website. A copy of the suspicious JAR file has been obtained from one of the infected computers.

Try to determine as well as you can what the JAR file does and consider what could have prevented it from infecting the workstations in the first place, and what the company should look for in order to find any additional infected systems. (Get the JAR on Absalon.)

Hint: You may want to make extract and inspect the embedded Java class files from the JAR file with a tool such as JD GUI. Also, assume any evaluation of `System.getSecurityManager()==null` always returns `true`.

2 Yet another JAR file (optional)

Another malicious JAR file has been found on a company workstation. If you have time, analyse it and try answer the same types of questions as for the first one. Get the JAR on Absalon.

Assume `System.getSecurityManager()==null` always returns `true` and also that the java version of the computer where the second JAR was found is 1.7.0_21.

Note again, this second JAR analysis is an **optional** part of the assignment. You should solve the other parts of the assignment before this, should you choose to solve it.

3 Lateral movement

Log entries show malware operators connected to their Poison Ivy installations regularly. They typically did so on weekdays during normal business hours. In all occasions a batch script was transferred and executed as one of the the very first steps after the initial connection. One such batch script has been uncovered.

Comment on the purpose of the batch script. Which commands, if any, would you have left out or included in the script—if you were the attacker. (Get the script on Absalon.)

4 Local privilege escalation

While most workstations run Windows at BIOchem, most servers are some UNIX-flavor. Using stolen credentials from the workstations, the attackers logged on to one of the UNIX-based servers. Once here they located an executable file with setuid permissions and exploited coding errors to spawn a root shell. As it turns out, this binary was built in-house so you have access to the source code.

Review the source code to find any codings errors the attackers could have exploited. Suggest ways to fix the issues you find. You do not have to demonstrate the flaws. (Get the code, updatephone.c, on Absalon.)

5 Motives and threat actors

Management is eager to learn who was behind the attack and why. The modus suggests similarities between this and the Nitro attacks, in the opinion of the company's chief security officer. Management would like your take on that hypothesis.

Based on your analysis of the attack, the information given in the assignment text, and any open source information on the Nitro attacks you may wish to consult, what do you think? If it is the Nitro attackers, what recommendations, if any, would you give to BIOchem in order to thwart the attackers?

General requirements

There are 3 assignments during the course, intended to give you hands-on experience in how to analyse information security risks, implement (parts of) security systems, break such systems, analyse attacks and provide recommendations to prevent future similar attacks.

Your solution to each assignment should be documented in a short report. Your report may follow the usual structure for scientific reports, starting with a summary followed by a description of the problem and the solution and finishing with a conclusion and a list of references.

Reports must be submitted in PDF format via Absalon no later than two weeks after the assignment in question is posted. Reports are graded as 'pass' or 'no-pass'. Resubmissions are allowed once per assignment. You must pass all assignments to sit in for the exam.

Limited written feedback is given via Absalon. Additional feedback may be given at exercise classes.

You should keep your hand-in as short and precise as possible. If you are in doubt about the interpretation of some of the requirements, or feel it necessary to make some assumptions, you should explain what you did and why. Be sure to clearly mark work included in your solution that is not your own personal work and make a reference to its source.

You may solve the assignmets in groups of 1-3 students. The first page of your report must contain the assignment number, your name and the name of any other group members.