**VAST 2012 Mini-Challenge 2 Solution Description for Reviewers and Committee**

**Updated 7/2/2012**

## Introduction

The 2012 VAST Challenge consists of two Mini-Challenges that concern a fictitious world called BankWorld and a fictitious international bank called Bank of Money (BOM). Mini-Challenge 2 focuses on issues involving operational concerns for the BOM enterprise. Contestants are provided with background information that provides the setting and context for the problem and solution, three questions that they must answer in their submission concerning the scenario, two datasets, and a standard answer form. The Challenge descriptions provided to contestants can be found at the VA Community Wiki Site, under “[VAST Challenge 2012: Challenge Descriptions](http://www.vacommunity.org/tiki-index.php?page=VAST%20Challenge%202012%3A%20Challenge%20Descriptions)”. Before reviewing solution packets, reviewers may want to familiarize themselves with the BankWorld and Bank of Money background material. Specific information about the geography of BankWorld and the physical environment for the Bank of Money enterprise can be found in the [information packet](http://www.vacommunity.org/tiki-index.php?page=VAST%20Challenge%202012%3A%20Submission%20Instructions%20and%20Downloads) provided with the Mini-Challenge2 materials.

The primary goal of the contestants is stated in the Challenge Descriptions. To wit:

During a time period that is NOT overlapping with MC 1, a Region within the Bank of Money is experiencing operational difficulties. This becomes a challenge for the operations staff, particularly as they attempt to deploy their limited number of skilled administrators to address issues occurring in the enterprise.

You will be provided with Firewall and IDS logs from one of the BOM networks of approximately 5000 machines. These are very similar to the Firewall and IDS logs you worked on during the VAST 2011 MC 2, and so the tools you used there will come in handy for this mini-challenge (and reuse is encouraged). You will also be provided with a description of the network to guide your investigation.

So, although this mini-challenge has a forensics theme, it is still concerned with situation awareness.

The three questions to be answered for Mini-Challenge 2 are:

MC 2.1 Using your visual analytics tools, can you identify what noteworthy events took place for the time period covered in the firewall and IDS logs? Provide screen shots of your visual analytics tools that highlight the five most noteworthy events of security concern, along with explanations of each event.

MC 2.2 What security trend is apparent in the firewall and IDS logs over the course of the two days included here? Illustrate the identified trend with an informative and innovative visualization.

MC 2.3 What do you suspect is (are) the root cause(s) of the events identified in MC 2.1? Understanding that you cannot shut down the corporate network or disconnect it from the internet, what actions should the network administrators take to mitigate the root cause problem(s)?

## Data Characteristics

Reviewers should read the Mini-Challenge 2 Information Sheet provided to the contestants for specific information on the network and the data provided.

The data reflects a situation where a botnet was introduced to the network and was able to spread and exfiltrate data to external machines. In MC2, we provide a firewall log and an IDS log which allows contestants to detect botnet activity by picking up on behavior patterns the botnet exhibits. The behavior of how the simulated botnet operates is described below:

Botnet Command and Control Server Behavior

1. Ten Command and Control servers, also known as C&C servers, are brought online to communicate with the botnet clients. They are dormant until a client connection is made from a workstation infected with the botnet.
2. When a client connection is made the C&C server instructs the botnet to determine what type of computer it has infected by querying the computer’s hardware.
3. If a server is detected by the botnet client additional instructions are sent to the client by the C&C to look for sensitive data.
4. If sensitive data is detected on the server, the C&C server instructs the client to attempt exfiltration of the data using FTP or SSH protocols.
5. If a workstation is detected by the botnet client, the C&C server instructs the client to attempt to replicate by port scanning other computers on the network which are vulnerable to a particular vulnerability.

Botnet Client Behavior

1. After the botnet client is installed on a target workstation, it attempts to contact one of ten of the Command and Control servers.
2. If a connection is successful it asks the C&C server for its first instruction.
3. The first instruction received from the C&C server is to determine what type of computer it has infected. Based on what type of computer is detected, the client sends this information to the C&C server.
4. If a server is detected by the botnet client, it is instructed by the C&C server to look for sensitive data such as a database or shared network drive.
5. If a database is detected for which it can read records, or a shared drive contains sensitive information, the client sends the details it found to the C&C server.
6. If the C&C server likes the files detected by the botnet client, it instructs it to exfiltrate the data to one of the other C&C servers via FTP.
7. If the FTP connection fails the client waits for a random duration and then attempts to send it by SSH.
8. If a workstation is detected by the botnet client, it is instructed by the C&C server to find other computers on the network to infect.

The evolving botnet situation can be followed with this timeline:

## MC2 Timeline

|  |  |
| --- | --- |
| Time | Event |
| 04/05/2012 17:51 | The scenario begins and normal traffic is seen on the network. The normal traffic includes regional headquarters computers communicating with the corporate headquarters financial server, user web browsing, and IRC. |
| 04/05/2012 20:25 | A cleaning crew inserts a USB key into a loan officer’s workstation which infects the computer with a botnet (not visible in the data). The botnet attempts to replicate itself to other machines on the network. Some of the botnets port scan the network to detect vulnerabilities. The botnet then communicates with one of ten command and control servers on the virtual internet. |
| 04/05/2012 20:26 | The botnet infects additional computers and locates sensitive data. It attempts to exfiltrate the data using FTP. |
| 04/05/2012 22:16 | The infected botnets begins to receive a payload from the C&C servers which will display ads on the infected computers. |
| 04/05/2012 22:21 | The botnet’s FTP traffic is blocked by an access list on the firewall. Numerous deny events are created and sent to the Log Server. |
|  | The botnets which have data to exfiltrate are instructed by the Botnet control server to attempt to exfiltrate using SSH instead of FTP. It works and the data is sent out of the network. |
| 04/05/2012 22:40 | The IT department is alerted by a large amount of failed FTP connections on the Log Server and start to troubleshoot the problem (not directly detectable in the data). Some infected workstations are patched and rebooted to attempt to get rid of the botnet. Some of the botnet traffic is no longer visible, but the majority of the traffic is still present. |
| 04/05/2012 22:41 | Due to all the botnet traffic the network starts to slow down and users start to notice their workstations are running slower than usual (user behavior not detectable in the data). |
| 04/06/2012 17:21 | End of File 1 |
| 04/06/2012 17:40 | Start of File 2 |
| 04/06/2012 17:41 | By this time, 10% of machines are infected. 5% of infected machines are communicating to adware servers, and the computers reboot multiple times. The data shows some drop in the exfiltration, but it doesn’t stop. |
|  | The Bank of Money IT Department is informed by an employee at the Regional headquarters that their machine is showing an excessive amount of popups which contain ads. The employee notes this didn’t occur the day prior. The employee informs the IT department that they first tried rebooting their machine several times before calling. The IT department was unaware the botnet has spread this fast and continues to look into the issue. (Not detectable in the data – scenario explanation) |
| 4/6/2012 18:11 | By this time, 15% of machines are infected and exfiltration is continuing. The new botnets attempt to exfiltrate by FTP. |

## Detecting the botnet behavior in the firewall and IDS log files

The IDS server is configured with a rule set to detect certain types of activity on the network. One of the rule sets it can detect is if a computer is port scanning the network. The IDS doesn’t contain a rule which is capable of detecting a botnet, but it is capable of detecting the unexpected behavior the botnet produces. The IDS will log an alert if:

1. A computer is port scanning the network.
2. An FTP session is started.
3. An IRC session is started.

The firewall will log traffic that passes from the outside interface to the inside interface or that passes from the inside interface to the outside interface. Examples of this include browsing websites, updating financial records on the corporate headquarters server, botnet activity, or IRC chat.

The firewall will not log traffic between two or more devices on the same interface. Examples of this include a server inside the regional headquarters office talking to a workstation in the regional headquarters office. Both of these devices reside on the internal network and the traffic does not traverse the outside interface.

## Answers to Specific Mini-Challenge Questions

MC2.1: Noteworthy events can be mapped into the VAST MC2 Syslog Answer Key that calls out the traffic events related to the scenario. Visualizations should present this information in a much improved format over a spreadsheet.

MC2.2: The trends that could be detected are indicated in the timeline above. These relate to the spread of the infections, “ad displays”, and attempts at exfiltration.

MC2.3: The root cause is, of course, the botnet, however other reasonably described explanations could also be presented by contestants.

## Dataset Content

There are (essentially) three datasets provided to contestants for Mini-Challenge 2.

* a description of the challenge: “VAST-MC2-generalinformation.zip” that includes the standard answer sheet.
* a firewall log, provided in “Firewall-04062012.csv” and “Firewall-04072012.csv” in CSV format. This data is also provided as “Firewall-part1.txt” through “Firewall-part4.txt” in its raw captured form.
* an IDS log, provided in “IDS-0406.csv” and “IDS-0407.csv” in CSV format. This data is also provided as “IDSlog.04062012” and “IDSlog.04072012” in its raw captured format.

Contestants may use either the CSV or raw formats in their analyses.