**Final Project**

**and**

**Report**

**The Big Bang**

**Prepared by Coby Flannery**

**UID: U99342804**

Table of Contents

[Abstract 3](#_Toc133268127)

[Scenario Introduction 3](#_Toc133268128)

[Threat Actor 3](#_Toc133268129)

[Target 3](#_Toc133268130)

[Campaign 3](#_Toc133268131)

[The Exploit 4](#_Toc133268132)

[Stages of the Attack 4](#_Toc133268133)

[Reconnaissance 4](#_Toc133268134)

[Weaponizing 4](#_Toc133268135)

[Delivery 4](#_Toc133268136)

[Exploit 4](#_Toc133268137)

[Stix Viz Representation 5](#_Toc133268138)

[Soltra/Edge Representation 5](#_Toc133268139)

[Install 7](#_Toc133268140)

[Command and Control 8](#_Toc133268141)

[Actions on Objectives 8](#_Toc133268142)

[**Incident Handling Process** 8](#_Toc133268143)

[Identification Phase 8](#_Toc133268144)

[Eradication and Recovery Phase 8](#_Toc133268145)

[Lessons Learned Phase 8](#_Toc133268146)

[References 9](#_Toc133268147)

# Abstract

The article will address the phases of an attack directly reflecting the agenda of the “Big Bang” attack. This attack was used by a hacker group named the Gaza hackers who posed as the Palestinian Political and National Guidance Commission. This attack starts with the use of a phishing email including an attachment of a self-extracting archive having a standard doc file and a malicious executable. When the document is double clicked, the standard doc file is opened and displayed as normal, but while the target is preoccupied with the document, the executable is opened behind decoy document. Big Bang has multiple protocols including taking a screenshot of the targeted user’s machine and sending it to the C&C server, sending a list of documents with file extensions including .doc, .odt, .xls, .ppt, .pdf, etc., logging system details, rebooting the user’s machine, and then self-destructing the executable. This attack can be qualified as a surveillance attack due to its ability to stay completely unknown and discrete while it obtains information and monitors the target.

# Scenario Introduction

Threat Actor

For this scenario, a fake actor named Craig will be using this attack to obtain confidential government information by targeting government officials’ emails in order to gain access to documents and files regarding government plans and motives.

Target

The target will be the emails of the government officials who are most likely to possess highly confidential information and hold the most valuable documents for his plans. The end target will be the actual information/documents that are obtained from this attack.

Campaign

For this scenario Craig will research a group of targets for his attack that will satisfy his end goal of obtaining confidential government plans. Craig will create an email posing as an important Florida government affiliate who has a change in plans in accordance with a previously proposed bill. The email will be regarding the solution to the concurring issue of the lake Okeechobee water levels. An attachment of the “changes” stated in the email will be included in the email.

The Exploit

Criag knows that the water levels of lake Okeechobee is a current even and that solutions are being discussed between Florida government officials. The subject of this fake email will draw attention to government officials because of how it is relevant and that the targeted Florida government officials will have a hard time differentiating this fake email from a real one. Due to the low security of the email systems that these affiliates are using and their inability to flag suspicious activity, a phishing tactic will be the most effective in this situation.

# Stages of the Attack

## Reconnaissance

In the reconnaissance phase, Craig finds information about the government agency's network architecture from his friend who works in IT for the agency. Craig uses this information to learn about systems and applications that can be manipulated. Craig then reviews the agency's websites and social media accounts to obtain information regarding their employees and the connection that the employees have along with the relationships between the employees. This allows Craig to make a list of potential targets for the attack that he is preparing.

## Weaponizing

After Craig identifies the vulnerabilities and weaknesses in the agency's network and devises a plan to exploit them, Criag creates his fake email by ensuring that is follows the protocols of a real government document and ensures that the name or extension of the document does not get flagged by the government emailing system. After the document is created, Craig embeds the malicious executable within the metadata of the fake document so that it stays undetected by the target. Once this is set up, he is ready to send the email to his list of targets.

## Delivery

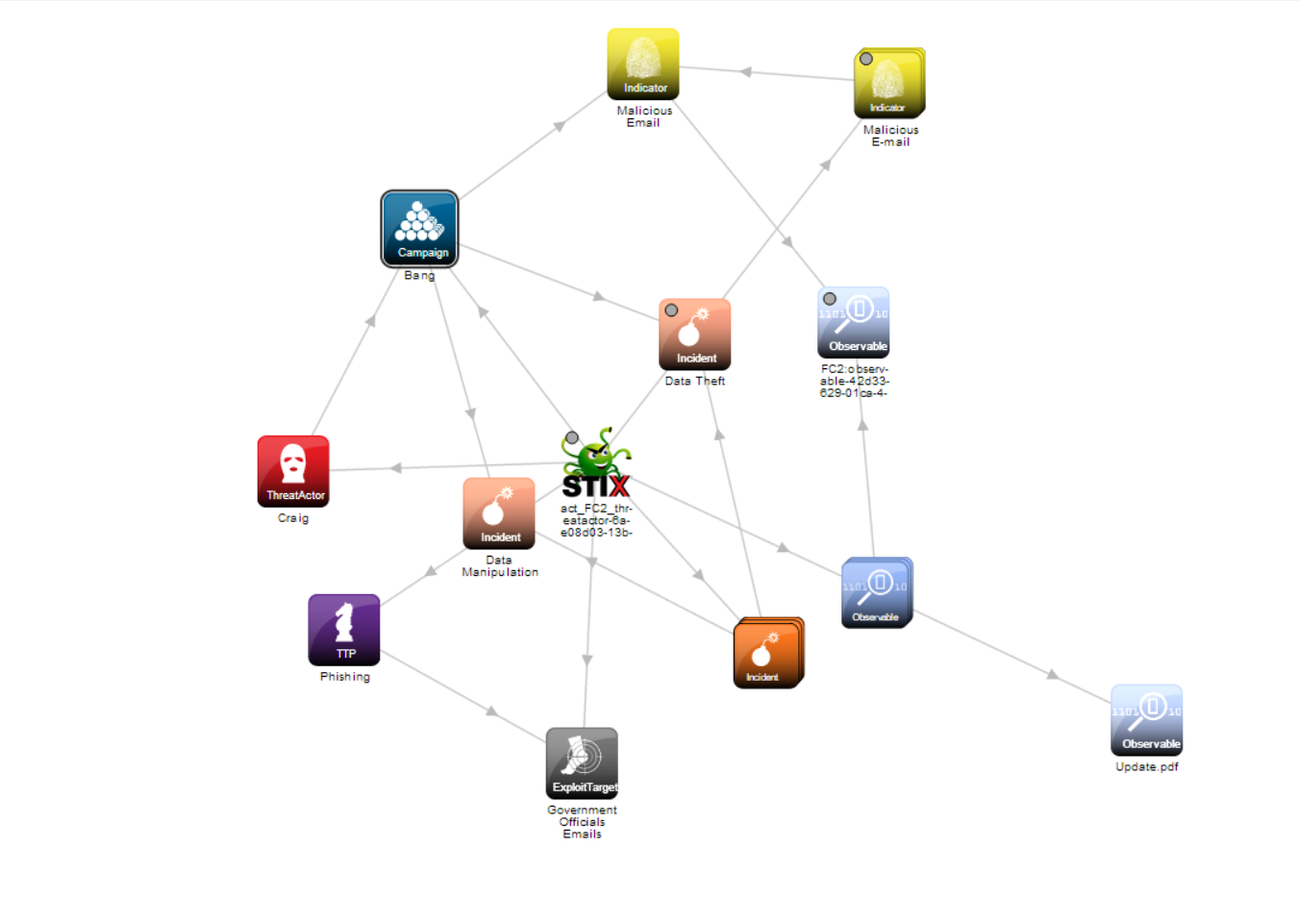
To execute his plan, Criag proceeds to sending the emails to his list of targets. The executable in the archive is called “DriverInstallerU.exe” but the metadata remains to display that its name is “Internet Assistant.exe”. Once the executable is ran by the government officials, the malware is copied to the program data dir., and adds scheduled tasks/processes for pulling files with specific extensions. In order to remain unidentifiable by the target, the tasks must pull information gradually and not all at once so that the user does not notice an increase of CPU stress on their system.

## Exploit

The user who double clicks the pdf will view the fake document and begin reading it. As the user reads the document, it will distract them from the executable which is archived with the fake document installed in the background. Once the previously mentioned .exe file is secured, it communicates with a C&C website. The APT actors hardcode a backup C&C website in case the malware does not communicate with the first website.

### Stix Viz Representation

The Big Bang in Stix Viz image below:



Soltra/Edge Representation

The Big Bang in Soltra/Edge image below:

Graphical user interface, text, application

Description automatically generated

Graphical user interface

Description automatically generated

## Install

Once the user has downloaded the pdf, the executable sets a mutex (“InterenetAssistantN”), which copies itself to “ProgramData” directory. Then, the malware talks with a primary hardcoded command and control website. A backup C&C website is communicated with in case the original website fails to connect. Below is the hardcoded 2 command and the control websites.

Text

Description automatically generated

As soon as the sample makes contact with the C&C server, it “fingerprints” the system which gathers OS version, user and PC names, and Anti-Virus engines. Then it proceeds with withdrawing the information gathered. Below is the initial beacon.

Text, letter

Description automatically generated

After Gathering information, a POST request is scheduled to send periodically to the C&C server resulting in the functionality of the malware going into effect.

## Command and Control

Craig will use the functionality of the C&C server in order to collect the necessary data that he desires from the target’s machine. Craig can use different commands with the malware such as “Penny” which takes a screenshot of the user’s computer, or Hofstadter, which terminates a process by name. He can collect this data without getting caught because the C&C server will collect it periodically and little by little to stay unrecognizable by the user.

## Actions on Objectives

When Craig is done collecting his desired information from the government affiliates, he runs a few commands incorporated into the malware in order to not get caught or to leave any traces of information theft. First, he runs the command “Hofstadter” on any applications that can trace the execution of the malware he has placed on the computer. Then in order to stop the data collection from payload in the startup folder of the government affiliate’s machine, he uses the command “Parsons\_Sheldon”. Then, Craig will run “Bialik\_Gokhan” to reboot the machine.

# **Incident Handling Process**

## Identification Phase

There are several ways of identifying a C&C attack like the “big bang”. Checking DNS log files can provide valuable information regarding who is accessing the device. Many C&C attacks use DNS servers, but in the case that the attack does not, DNS log files cannot trace the attack. Other similar methods that can be used in case DNS log files are no use are Firewall logs and Proxy log files. Many organizations use these methods to tighten the security of data.

## Eradication and Recovery Phase

In order protect and mitigate from cyber threats such as phishing attacks and C&C attacks, there many process that an organization/individual can take such as:

* Employee training and self-awareness to unknown sources – Make sure that employees of an organization are aware of phishing emails and any other cyber threats.
* Multi-Factor Authentication – make passwords require more than one way of identifying the user.
* Anti-virus/Anti-malware software – Install relevant antivirus software that can conduct searches for unknown and suspicious activity.
* Network Segmentation – Create isolated zones for sensitive data.

## Lessons Learned Phase

All it takes for someone’s data to be completely conceived and held against them is the simple click of an email and the download of an attachment. Remaining aware of the damages that the attacks discussed in the report is crucial to the confidentiality of someone’s personal data or even an entire organization’s data. Regularly performing security scanning with personal antivirus software or even being attentive to the monitoring software that operating systems such as windows has like task manager is beneficial to the security of data.

Craig was able to easily manipulate the data contained on the government affiliates device with a simple phishing method that became much more dangerous as a C&C attack. If the government worker had ensured that their email system was more secure to avoiding malicious emails, had been educated on different kind of cyber-attacks, and had a proper antivirus software, the data compromise could have been completely avoided.

# References

1. Canvas – “APT Attack In the Middle East: The Big Bang”
2. “The Big Bang attack campaign: Gaza hackers suspected of targeting Middle Eastern victims” URL: <https://cyware.com/news/the-big-bang-attack-campaign-gaza-hackers-suspected-of-targeting-middle-eastern-victims-642585f4>