Project Plan
Detecting State Sponsored Computer Security Terrorists
The Capstone Experience
Team Proofpoint
Chris Maidlow
John Crawford
Zhehan Wu
Nick Jones
Josue Kpodo

Department of Computer Science and Engineering
Michigan State University
Fall 2019
Functional Specifications

• Adds an important tool to the arsenal of those combating cyberterrorism through novel approaches in monitoring, luring and the data collection of bad actors

• Uses reproducible methods to generate believable and attractive content desirable by bad actors

• Leverages multiple existing technologies to collect meaningful data upon accessing lures

• Gathers and organizes acquired data in a purposeful and intuitive matter

• Protects companies from future attacks by identifying common attack patterns
Design Specifications

• Lures
  ▪ Generating convincing collateral
  ▪ Cloned websites tailored to each lure
  ▪ Dissemination of lures

• Web Application
  ▪ Data analysis of attackers and their attack pattern displayed on homepage
  ▪ “Roll-up” individual actor’s methodology into an incident design allows intuitive
Screen Mockup: Content Generation

Use standard file APIs to check for files with this prefix.
Model prompt >>> Hackers with a certain degree of technical strength know to destroy the traces of hidden invasion and sniffing to cover up themselves.

If even the slightest traces of the spyware infection (which could give a clue as to the identity of the hacker) and the hacking techniques used to control the network are left exposed, the hacker could be identified and punished accordingly. This is precisely what happened during the recent attacks of Russian hackers against the Ukrainian leadership.

The Ukrainian hacker group (who were known as “Hackers.ATL” since last February) released a video about their hack against Ukraine’s power sector, which was a full compromise of the system of Ukraine’s state-owned power company (PUK) and even its internal networks.

“We do not only want to bring down all these networks and install our own malware and Trojan to compromise the whole power sector. We also do not only want to infect the whole system with our Trojan, we also want to use the malware to infiltrate the systems of the political opposition. We only want to cause as much damage to the power systems of Ukraine as possible, as it is not possible to prevent such a hack and we expect maximum damage.” – Ukrainian hacker group (Hackers.ATL).

If this is not enough, the hackers have decided to use the cyber security tools that they developed themselves and the most sophisticated techniques that can be found on the cyber security market to bring down power networks and even steal electrical power supplies. As a result, the Ukrainian power company which was once one of the most powerful electric grids in the world has failed to provide electricity to the whole of its territory and has even started evacuating customers as a result of the cyber attack.

Russian hackers will do their utmost to find the hackers who are responsible and expose them by disclosing the details of their secret plan in the most efficient way possible. It is not surprising to see such an organization as Hacking Team – one of the world’s largest and most widely used security companies – who provides the government and the security agencies with an extremely secure and effective security solution for sensitive information and data breaches.
Fake Person

Fake Person is a professor of the Department of Biomedical Research. His research interests lie in the intersection of various biomedical topics and their impacts on possible aging. Currently, he is researching the impacts of intermittent fasting on various anti-aging processes. He also co-coordinates with Dr. Aseem Bikhil to formulate clinical trials to see what effects intermittent fasting and other low-calorie/restricting meals has on the human body.

He has a background in the field of epidemiological research and has done his clinical work in the field of nutrition and physical activity. His research activities over the last several years has focused on the impact of intermittent fasting on other anti-aging processes as well as the impact on general health and function.

His main research field involves the impact of dietary restriction and fasting on the function of the body and the human metabolism. For the past three years, he has been conducting his research in the field on anti-aging and low-calorie intermittent exercise by studying subjects with various forms of diabetes as well as healthy.

Research

- Fake research #1
- Fake research #2
- Fake research #3
- Fake research #4
- Fake research #5
- Fake research #6
Screen Mockup: Web App Homepage

Dashboard

Dashboard for the application. Short description of what the web app allows you to do. Information available. Dashboard will have basic overview stats. Tabs on top of the page to navigate throughout the web app. Most importantly the home "dashboard" with a basic overview of the week along with an incident tab that allows you to view specific incidents and more in-depth information on them. Possibly add more tabs.

Brief description of most recent and largest attacks received this week. Various infographics below to offer an overview on various attacks across multiple lures from the past week.

Types of attacks received

Number of distinct IP addresses that have visited

Number of files dropped

Lures visited

Days: Sun, Mon, Tue, Wed, Thu, Fri, Sat
Screen Mockup: Web App Lure Page

Lure #1
Open the lure
Specific information on this lure. Type of lure, recent events, order of said events, files dropped. Performance compared to other lures, most common attacks received.

This lure is meant to replicate a Nuclear Physics based research NGO. Fake research documents are available to entice attackers. Currently, 12 attackers have visited this site, making this lure the most attractive lure.

Number of files dropped

Types of files dropped

<table>
<thead>
<tr>
<th>Type</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>exe</td>
<td>27.8%</td>
</tr>
<tr>
<td>pdf</td>
<td>33.7%</td>
</tr>
<tr>
<td>doc</td>
<td>11.1%</td>
</tr>
<tr>
<td>jpg</td>
<td>5.6%</td>
</tr>
<tr>
<td>rar</td>
<td>22.2%</td>
</tr>
</tbody>
</table>
Technical Specifications

• HTTrack to clone websites
• GPT-2 ML model to generate documents
• Suricata IDS, tcpdump and drill for network analysis
• Flask and React to develop website, RESTful APIs for data transfer
System Architecture

- **Lure Development**
  - HTTrack
  - GPT-2
  - Websites
  - PDF

- **Lure Deployment**
  - APT / Cyber Terrorist
  - WikiLeaks
  - Non-Indexed Websites

- **Backend / Server**
  - Proofpoint
  - Tunnel Server
  - Network Monitoring Tools
    - SURICATA
    - TCPDUMP
    - Drill
  - Capstone Server

- **Monitoring Dashboard**
  - Front End
  - Back End
    - Flask
    - plotly
    - PostgreSQL
System Components

• Hardware Platforms
  ▪ Proofpoint VMWare ESXi Server
  ▪ FreeNAS CIFS Server backend

• Software Platforms / Technologies
  ▪ HTTrack
  ▪ GPT-2 Model
  ▪ Canary
  ▪ Flask/React
Risks

- **Failure to lure professional State Sponsored cyber criminals**
  - Cannot catch our targets if they have different motives (Broad)
  - Target ‘The Silent Librarian’ – an APT targeting MSU (Specific)

- **Intangible content generation**
  - Possible grammatical/date errors in ML-generated content/articles
  - Automate autocorrection with Python and/or correct manually

- **Inefficiency in managing multiple Honeypots**
  - Create and Monitor many Honeypots (FTP, SMTP) scattered on the Internet
  - Use alternative to Honeypots: Canary tokens

- **Familiarity of our techniques by professional attackers**
  - Very hard to lure professionals since they are familiar with the technology.
  - Attempting to identify our lures will trigger an alert (when using canary tokens)
Questions?