DOCUMENTATION FOR THE ISOT CLOUD INTRUSION DETECTION BENCHMARK DATASET(ISOT-CID)

Abdulaziz Aldribi, Issa Traore, Paulo Gustavo Quinan, Onyekachi Nwamuo

Table of Contents

1 Citations

To reference this dataset use:

1 Aldribi A., Traore I., Moa B. (2018). “Data Sources and Datasets for Cloud Intrusion Detection Modeling and Evaluation”. Mishra B., Das H., Dehuri S., Jagadev A. Cloud Computing for Optimization: Foundations, Applications, and Challenges. Studies in Big Data. (39): 333-366. Springer.

2 Aldribi A., Traore I., Quinan P. G., Nwamuo O., “Documentation for the ISOT Cloud Intrusion Detection Dataset”, Technical Report # ECE-2020-10-10, University of Victoria, ECE Department

3 Abdulaziz Aldribi, Issa Traore, Belaid Moa, Onyekachi Nwamuo, “Hypervisor-Based Cloud Intrusion Detection through Online Multivariate Statistical Change Tracking”, *Computers & Security (2019)*, Elsevier, doi: https://doi.org/10.1016/j.cose.2019.101646

2 Overview

Cloud computing is susceptible to traditional IT attacks because it leverages the existing IT infrastructure, operating systems (OSs), and applications. In addition to the conventional threats, cloud computing environments face new security issues as these involve many new technologies that could lead to new forms of exploitation.

Developing cloud-based IDS that can capture suspicious activities or threats and prevent attacks and data leakage from both inside and outside the cloud environment is paramount. Developing such systems, however, is very challenging as cloud IDS researchers are faced with one of the greatest hurdles: the lack of publicly available datasets collected from a real cloud computing environment, which is a big hindrance for developing and testing realistic detection models.

We introduce the first public dataset of its kind collected from a production cloud environment, named ISOT Cloud Intrusion Dataset (ISOT-CID), as an initial response toward addressing such need and paving the way for cloud security communities for more research and findings. The dataset consists of over 2.5 terabytes of data, involving normal activities and a wide variety of attack vectors, collected in two phases (phase 1 in December 2016 and phase 2 in February 2018) and over several months for the VM instances, and several days and time slots for the Hypervisors. The benign/normal data are from web applications and administrative activities ranging from maintaining the status of VMs, rebooting, updating, creating files, SSHing to the machines, and logging in a remote server. The web traffic was generated by more than 160 legitimate visitors, including more than 60 human users and genuine traffic generated by 100 robots, performing tasks such as account registration, reading/posting and commenting on blogs, browsing various pages, and so on. One of the web applications consists of a password management service for registered users.

The ISOT-CID is an aggregation of different data gathered from a variety of cloud layers, including guest hosts, hypervisors and networks, and it comprises data with different formats and from multiple data sources, including memory dumps, resource (e.g., CPU) utilization logs, system call traces, system logs, and network traffic. It is large and diverse enough to accommodate various intrusion data models, feature sets and analysis models. The purpose of ISOT-CID is the embodiment of a real cloud dataset, it is essentially raw and has not been transformed, manipulated or altered. This is important for the industry and academia towards developing and evaluating realistic intrusion models for cloud computing.

The current documentation describes and explains the dataset metadata files and how they are structured and stored in the repository hosted on ISOT public repository to ensure an unambiguous meaning of the data. Moreover, it provides details on the attack scenarios and the network statistics. In particular, the network traffic of ISOT-CID, is described in much more details.

3 Getting Started with the ISOT-CID dataset

3.1 ISOT-CID Environment

The ISOT-CID environment consists of 3 hypervisor nodes and 10 virtual machines.

The hypervisor nodes are named A, B and C, with each one hosting a different number of VMs as shown by Table 1. Only hypervisors A and B are involved in the attacks which means only their data and data from their VMs were captured and given a capture label.

Table 1: Hypervisor details

Node	VMs hosted	Capture label
A	5	poseidon0050
B	4	poseidon0049
C	1	–

The VMs are identified by a unique ID from 1 to 10 and a unique hostname. They have different operating systems and each one of them has an external and an internal IP, except for VMs 2 and 5 which only have internal IPs. Tables 2 and 3 contains the VM details.

Table 2: ISOT-CID VM OS details

Node	ID	Hostname	Operating System
C	1	isotvm-1	Centos
A	2	isotvm-2	Centos
	3	hpisot-dj	Debian
	4	ohp-win12	Windows Server 12

	5	isotvm-in1	Ubuntu
	6	hpisot-centos7	Centos
B	7	hpisot-ubuntu	Ubuntu
	8	ohp-ubuntu	Ubuntu
	9	hpisot-winserve	Windows Server 12
	10	2hpisot-centos7	Centos

Table 3: ISOT-CID VMs network details

Node	ID	Internal IP Address	External IP Address	Capture Label
C	1	172.16.1.10	206.12.59.162	–
A	2	172.16.1.28	–	tap697d1afd-ba
	3	172.16.1.23	206.12.96.142	tape7fbbb33-8d
	4	172.16.1.26	206.12.96.149	tapab39f95e-60
	5	192.168.0.10	–	tap9ffd61d3-f2
	6	172.16.1.19	206.12.96.240	tap3178ed86-a9
B	7	172.16.1.20	206.12.96.239	tap5f861c6c-ec
	8	172.16.1.24	206.12.96.143	tapf11051e8-cb
	9	172.16.1.21	206.12.96.141	tapbbf98dae-e9
	10	172.16.1.27	206.12.96.150	tap70a780f3-34

3.2 Collection Days

The dataset was collected in two phases. Phase 1 was collected in December 2016. It contains 4 rounds of executed attack scenarios spread over 4 days (days 1 to 4) between December 9 and December 16, 2016. Moreover, one extra day (day 0 – December 8) of data is provided which can serve as a baseline in comparison against the executed attack days as it only contains data generated from administrative tasks and unsolicited internet traffic.

Phase 2 was collected in February 2018. It contains 5 rounds of executed attack scenarios spread over 5 days (days 1 to 5) between February 16 and February 23, 2018. As with phase 1, it contains one extra day (day 0 – February 15) of data generated from administrative tasks and unsolicited Internet traffic which can serve as a baseline in comparison with the other attack days.

3.2.1 Additional Syslog Data

In phase 1, in addition to the data collected through the primary data collection process, extra syslog data were collected from December 1 to 19 outside the collection windows. The data consist of the following:

- **Dec 1:** logs from 1 Windows machine;
- **Dec 2:** logs from the 2 Windows machines;
- **Dec 3 to 7:** logs from 8 machines;
- **Dec 8 to 19:** logs for from 10 machines.

3.3 Data Sampling

For storage, performance and practical reasons, most of the data in the dataset was sampled or snapshotted in repeating intervals.

The network traffic data in phase 1, for instance, were collected in bursts of random durations ranging from 2 to 12 seconds and repeating every 80 seconds on average while memory dumps were collected by taking snapshots of the memory of each VM every 5 to 8 minutes. Other intervals were used for other non-stream data like *ps* and *of*.

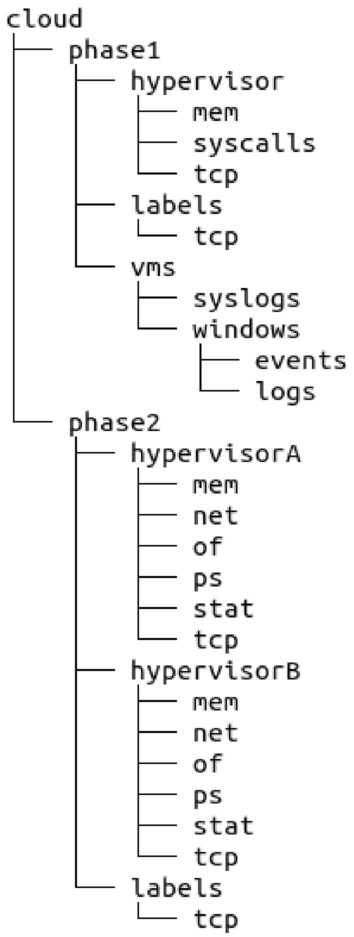
On the other hand, the network traffic data in phase 2 were collected without any sampling.

3.4 File Structure

ISOT-CID is organized under two main directories, one for each of the two collection phases. Figure 1 shows the high-level directory structure of the dataset.

Phase 1 data is divided into three directories, two for data, being one for data collected in the hypervisor, comprising of memory dumps, syscalls traces and network traffic dumps, and one for data collected in the VMs, comprising of syslogs from the Linux VMs and Windows logs from the Windows VMs, with the third directory, called *labels*, containing the label files of this phase as described in section 3.5. Data of each of the data types are placed inside their respective directories under either of the two data directories and are further divided into subdirectories according to attack day.

In this phase, files collected in the hypervisor level are named according to the following pattern: The time of the snapshot or of the start of the collection burst (as explained in section 3.3) in ISO-8601 date time format (YYYY-MM-DDTHH:mm:ssZ) followed by the hypervisor capture label and either the VM capture label for network trace files or the VM hostname for the rest, followed by the extension. Some files are stored in a compressed format and therefore need to be uncompressed in order to access the content.



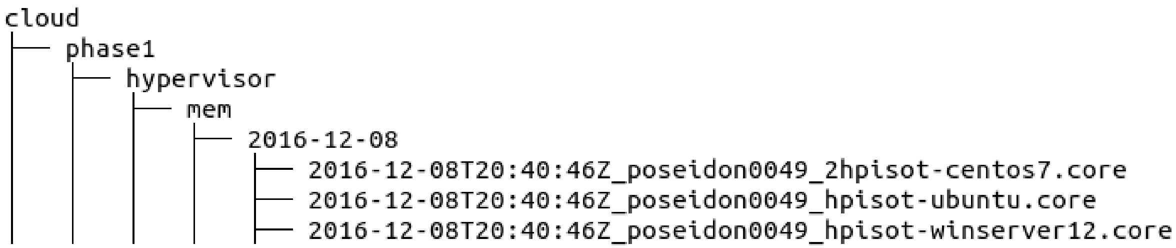
```
cloud
├── phase1
│   ├── hypervisor
│   │   ├── mem
│   │   ├── syscalls
│   │   └── tcp
│   ├── labels
│   │   └── tcp
│   └── vms
│       ├── syslogs
│       └── windows
│           ├── events
│           └── logs
└── phase2
    ├── hypervisorA
    │   ├── mem
    │   ├── net
    │   ├── of
    │   ├── ps
    │   ├── stat
    │   └── tcp
    ├── hypervisorB
    │   ├── mem
    │   ├── net
    │   ├── of
    │   ├── ps
    │   ├── stat
    │   └── tcp
    └── labels
        └── tcp
```

Figure 1: Dataset Directory Structure

For instance, the network trace file *phase1/hypervisor/tcp/2016-12-09/2016-12-09T19:42:24Z_poseidon0050.wgcloud.uvic.ca_tape7fbbb33-8d.dump* contains the network packets of VM 3 (which is hosted by hypervisor A, aka, poseidon0050) captured on December 09 2016 around 19:42:24 UTC.

On the other hand, files collected on the VM level are named simply based on the hostname with a type prefix for the Windows logs.

Figure 2 shows a sample of the filenames of phase 1 hypervisor files.



```
cloud
├── phase1
│   ├── hypervisor
│   │   ├── mem
│   │   │   ├── 2016-12-08
│   │   │   │   ├── 2016-12-08T20:40:46Z_poseidon0049_2hpisot-centos7.core
│   │   │   │   ├── 2016-12-08T20:40:46Z_poseidon0049_hpisot-ubuntu.core
│   │   │   │   ├── 2016-12-08T20:40:46Z_poseidon0049_hpisot-winserver12.core
```

Figure 2: Phase 1 hypervisor filename sample

Phase 2 data has no VM level data and its hypervisor level data are organized into separate directories for each hypervisor with subdirectories for each type of log collected. Filenames in this phase are simply based on the attack day, except for network traffic files which are named based on the attack day and on the capture label of the VM.

For instance, the network trace file p*hase2/hypervisorA/tcp/2018-02-15_tap3178ed86-a9.dump* contains the network packets of VM 6 (which is hosted by hypervisor A) captured on February 15, 2018 during the whole collection window.

As with phase 1, the *labels* directory contains the label files of this phase.

3.5 Data Labelling

Labelling is provided only for network traffic data in the form of CSV files where each row contains the header data (for identification) and the classification of a single packet. Each file contains all packets of the day specified by its name.

Labelling process works as such: Hosts (specifically IP addresses) are labelled as either benign or malicious with packets between benign hosts labelled as benign and packets to and from malicious hosts considered malicious.

Most hosts keep their classification throughout the whole collection phase, with the exception of internal hosts compromised as part of an attack. In those cases, the host's data starts out as benign but is considered malicious once the host is compromised.

Tables 4 and 5 lists the IP addresses belonging to hosts whose data are initially labelled as benign in phase 1 and 2, respectively. In practice these hosts are: (a) internal hosts, that is, those inside the virtual local network; (b) external hosts which generate benign traffic or are part of the administrative infrastructure and (c) broadcast addresses observed in the network traffic data.

Table 4: Phase 1 benign IP addresses

134.87.154.134	134.87.157.129	142.104.6.1	142.104.64.196	142.104.80.2
142.104.191.194	172.16.1.10	172.16.1.16	172.16.1.17	172.16.1.19
172.16.1.20	172.16.1.21	172.16.1.23	172.16.1.24	172.16.1.26
172.16.1.27	172.16.1.28	172.16.1.254	172.16.1.255	192.168.0.8
192.168.0.9	192.168.0.10	206.12.48.43	206.12.48.115	206.12.59.162
206.12.96.141	206.12.96.142	206.12.96.143	206.12.96.149	206.12.96.150
206.12.96.239	206.12.96.240	255.255.255.255		

Table 5: Phase 2 benign IP addresses

2.89.202.164	5.41.6.52	5.41.55.201	5.108.143.27	5.156.23.30
5.156.104.155	5.156.239.222	5.246.50.54	24.108.16.189	24.108.17.78

24.244.32.170	24.244.32.247	37.104.156.213	37.104.183.171	37.104.214.214
37.105.194.65	51.36.19.37	51.36.31.176	51.36.39.186	51.36.52.127
51.36.89.58	51.36.98.236	51.36.198.76	51.36.217.50	51.36.227.160
51.39.8.69	51.39.153.205	51.39.162.99	51.39.202.109	51.218.220.231
51.218.248.166	51.218.252.241	51.218.252.241	51.255.40.63	62.120.22.18
62.120.25.143	78.95.44.45	78.95.126.150	90.148.165.218	93.168.52.172
93.168.61.191	93.168.64.12	93.168.90.82	93.168.144.25	93.169.29.93
93.169.127.140	94.48.53.155	94.98.250.78	95.184.33.34	95.184.34.83
95.184.83.170	95.185.185.142	95.186.3.107	95.186.76.167	95.186.109.44
95.187.159.184	129.208.0.104	129.208.99.140	129.208.142.220	129.237.123.95
134.87.154.71	134.87.154.134	134.87.157.129	134.87.157.231	134.87.164.132
142.104.6.1	142.104.64.196	142.104.64.201	142.104.64.202	142.104.80.2
142.104.96.25	142.104.191.194	147.143.196.4	147.143.196.5	147.143.196.33
147.143.196.39	147.143.196.44	151.254.22.168	151.254.68.156	151.255.78.159
172.16.1.10	172.16.1.16	172.16.1.17	172.16.1.19	172.16.1.20
172.16.1.21	172.16.1.24	172.16.1.26	172.16.1.27	172.16.1.28
172.16.1.254	172.16.1.255	176.45.160.91	176.47.6.105	176.47.78.249
184.66.35.39	184.66.37.31	184.66.39.200	184.66.46.31	184.151.231.50
188.48.138.54	188.49.40.63	188.49.132.63	188.49.184.140	188.50.228.245
188.55.218.54	188.248.25.40	188.248.33.172	192.168.0.8	192.168.0.9
192.168.0.10	206.12.48.43	206.12.48.115	206.12.59.162	206.12.96.141
206.12.96.142	206.12.96.143	206.12.96.149	206.12.96.150	206.12.96.239
206.12.96.240	206.87.164.188	206.87.190.30	220.54.25.114	255.255.255.255

Hosts that are not part of the benign list are considered malicious along with any data related to them. In practice these hosts are: (a) hosts used as part of the executed attacks; and (b) sources of unsolicited traffic, mostly probing and password guessing attacks.

Specifically, for phase 1, a special consideration must be given to IP address **142.104.64.196** which was used as a log server during the attacks of this phase, generating a large amount of traffic (around 15% of the total of the phase). Traffic between this host and an internal machine compromised during an attack is considered malicious given that it originates from a compromised machine but it can also be filtered out given the oversized contribution it has to the collected data in this phase.

Finally, although not provided here, it is possible to at least partially label logs and other data based on the host and packet classification at each given point in time in cases where it is possible to link said host or packet (or stream of packets) to said log event or other data point.

3.6 Network Traffic

In a cloud computing infrastructure such as OpenStack, the network traffic travels through different network points. In our case, the outside traffic first arrives via the entry and top-rack switches to dedicated network nodes, called neutron nodes, and then travels to the hypervisor on the compute nodes passing through our internal physical switches. Finally, the hypervisor delivers the traffic to the designated instance.

With this OpenStack networking configuration, there are three different network flows: external, internal and local traffic. The external traffic is between the virtual machine and an outside machine (an "instance-outside" traffic). The internal traffic is between the compute node and another compute node ("hypervisor-hypervisor" traffic). The local traffic is between two instances on the same Compute node ("instance-instance" traffic).

In ISOT-CID, we were able to collect all of these three different types of traffic from both hypervisors and instances. By setting the network interface into promiscuous mode, we were able to collect all the network traffic that passes through all the network interfaces on the hypervisors and instances (except for the special network interfaces not involved in our network traffic collection) in both directions.

The utility TCPdump was used to capture the network traffic on *nix OSs and Netsh on Windows, and store it in packet capture (pcap) format. We performed two kinds of network traffic data collections: the network traffic without payload on both hypervisors and instances, and the full network traffic on the hypervisors only.

In phase 1, the network traffic data consists of a total of 24,519,987 network packets, of which 15,306,027 are labelled as benign/normal, and 9,213,960 are labelled as malicious. Table 6 details the phase 1 traffic breakdown per day. In phase 2, the network traffic data contains a total of 12,418,998 network packets, of which 9,770,676 are labelled as benign/normal, and 2,648,322 are labelled as malicious. Table 7 details the phase 2 traffic breakdown per day.

Table 6: Phase 1 network traffic data breakdown per day (packets)

Date	Benign	Malicious	Total
Day 0 2016-12-08	2,097,939 (99.92%)	1,585 (0.08%)	2,099,524
Day 1 2016-12-09	3,112,457 (49.46%)	3,180,869 (50.54%)	6,293,326
Day 2 2016-12-15	7,157,658 (61.90%)	4,404,874 (38.10%)	11,562,532
Day 3 2016-12-16	1,355,938 (65.29%)	720,814 (34.71%)	2,076,752
Day 4 2016-12-19	1,582,035 (63.59%)	905,818 (36.41%)	2,487,853
Total	15,306,027 (62.42%)	9,213,960 (37.58%)	24,519,987

Table 7: Phase 2 network traffic data breakdown per day (packets)

Date	Benign	Malicious	Total
Day 0 2018-02-15	936,813 (97.39%)	25,122 (2.61%)	961,935
Day 1 2018-02-16	2,594,752 (90.37%)	276,427 (9.63%)	2,871,179
Day 2 2018-02-19	704,226 (69.88%)	303,529 (30.12%)	1,007,755
Day 3 2018-02-20	1,670,428 (94.98%)	88,322 (5.02%)	1,758,750
Day 4 2018-02-21	1,806,839 (96.99%)	56,109 (3.01%)	1,862,948
Day 5 2018-02-23	2,057,618 (52.01%)	1,898,813 (47.99%)	3,956,431

Total	9,770,676 (78.68%)	2,648,322 (21.32%)	12,418,998

The packets can be analyzed both at packet-level and flow-level using tools such as tcpflow, netflow, tranalyzer, Scapy etc. However, note that phase 1 data might require some amount of pre-processing given the nature of the sampling performed.

4 Attack Scenarios

The ISOT-CID contains both application and network layer attacks. The attacks are also divided according to where they originate, specifically, either from inside or outside the ISOT-cloud environment.

The external attacks are defined as attacks from the outside world that target the ISOT-cloud environment while the internal attacks originate from a compromised instance inside the ISOT-cloud environment network and target either the internal cloud infrastructure or the outside world.

The types of inside attack performed is as followed:

- **Application Layer:**
  - Web Vulnerabilities Scanning
  - Dictionary/Brute Force login attacks
  - Directory/Path Traversal
  - Cross-site Scripting (XSS)
  - SQL Injection
  - Fuzzers
  - HTTP Flood DOS
- **Network Layer:**
  - Unauthorized Cryptomining (download/install/run crytpo-miner)
  - Dictionary/Brute Force login attacks
  - DNS Amplification DOS
  - Network Scanning
  - Dictionary/Brute Force login attacks
  - Synflood DOS

- UDP Flood DOS
- Trojan Horse
- Backdoor (reverse shell)
- Stepping Stone Attack
- Unclassified (unsolicited traffic)

More details are provided in subsequent subsections.

4.1 Phase One Attack Scenarios

The attack scenarios in this phase involve different attack times and distinct attacker's geographical locations. The attacks were divided into 4 rounds lasting 1 hour each on average spread over 4 different days. Moreover, the attackers performed and completed the attack scenarios from different continents, e.g., Europe and North America. Data were collected from all previously mentioned data sources according to the described protocols.

Different attacks were carried out such as Remote-to-Local (R2L), DOS, probing, information disclosure, input validation, authentication breach, and backdoors. In addition to that, the dataset also contains data from unsolicited traffic which normally consists of probing and password guessing attacks.

The following tables describe the attack scenarios performed. Each table contains a list of attacks or actions performed by the attacker in the order they were performed. It contains the type of attack or action, the source and destination IP addresses, the time of the event as available in the dataset (either packet or syslog) and a column (called "Packets") specifying the number of packets related to that attack or action that were collected (as described in Section 3.3).

4.1.1 Day 1, 2016-12-09

Seq	Attack	Source	Destination	Time	Packets
1	Password Guessing: SSH	Attacker IP 1: 213.41.131.165	VM 8: 172.16.1.24	**From:** 17:41:27 **To:** 17:41:42	0
2	Successful Password Guess: SSH (Unauthorized Login)	Attacker IP 1: 213.41.131.165	VM 8: 172.16.1.24	**From:** 17:41:40 **To:** 17:41:40	0
3	Unauthorized Login: SSH	Attacker IP 1: 213.41.131.165	VM 8: 172.16.1.24	**From:** 17:43:02 **To:** 17:49:22	0
4	Internal Port Scanning	VM 8: 172.16.1.24	172.16.1.0/24	**From:** 17:45:51 **To:** 17:45:53	0

5	Unauthorized Login: SSH	Attacker IP 2: 62.212.117.210	VM 8: 172.16.1.24	**From:** 17:55:05 **To:** 19:55:53	16
6	Unauthorized Login: SSH	Attacker IP 1: 213.41.131.165	VM 8: 172.16.1.24	**From:** 17:59:01 **To:** 20:01:06	7
7	Unauthorized Login: SSH	Attacker IP 1: 213.41.131.165	VM 8: 172.16.1.24	**From:** 18:06:55 **To:** 18:06:57	1
8	Unauthorized Login: SSH	Attacker IP 2: 62.212.117.210	VM 8: 172.16.1.24	**From:** 18:09:19 **To:** 18:13:39	0
9	Unauthorized Login: SSH	Attacker IP 1: 213.41.131.165	VM 8: 172.16.1.24	**From:** 18:27:13 **To:** 18:28:05	0
10	Unauthorized Login: SSH	Attacker IP 1: 213.41.131.165	VM 8: 172.16.1.24	**From:** 18:28:51 **To:** 18:28:52	0
11	Unauthorized Login: SSH	Attacker IP 1: 213.41.131.165	VM 8: 172.16.1.24	**From:** 18:29:13 **To:** 18:41:34	44
12	Download and install Hydra (apt)	VM 8: 172.16.1.24	archive.ubuntu.com	**From:** 18:31:16 **To:** 18:42:04+	0
13	Internal Port Scanning	VM 8: 172.16.1.24	192.168.0.1-10	**From:** 18:34:25 **To:** 18:34:28+	0
14	Password Guessing: SSH	VM 8: 172.16.1.24	VM 5: 192.168.0.10	**From:** 18:36:11 **To:** 18:41:30+	271
15	Unauthorized Login: SSH	Attacker IP 1: 213.41.131.165	VM 8: 172.16.1.24	**From:** 18:42:47 **To:** 20:49:31	0
16	Unauthorized Login: SSH	VM 8: 172.16.1.24	VM 5: 192.168.0.10	**From:** 18:45:28 **To:** 19:39:06	498,521
17	Self ping to external IP	VM 8: 172.16.1.24	VM 8: 172.16.1.24 (206.12.96.143)	**From:** 18:46:48 **To:** 18:46:48	0
18	Download and install hping3 (apt)	VM 8: 172.16.1.24	archive.ubuntu.com	**From:** 18:48:08 **To:** 18:49:17+	0
19	Port Scanning	Attacker IP 1: 213.41.131.165	VM 4: 172.16.1.26	**From:** 18:52:11 **To:** 18:52:13+	7

20	Unauthorized Login: SSH	Attacker IP 1: 213.41.131.165	VM 8: 172.16.1.24	**From:** 18:57:21 **To:** 19:00:59	0
21	Unauthorized Login: SSH	Attacker IP 1: 213.41.131.165	VM 8: 172.16.1.24	**From:** 19:03:41 **To:** 19:04:10	1
22	Ping	VM 8: 172.16.1.24	VM 4: 172.16.1.26 (206.12.96.149)	**From:** 19:04:00 **To:** 19:04:01+	1

4.1.2 Day 2, 2016-12-15

Seq	Attack	Source	Destination	Time	Packets
1	Port Scanning	Attacker IP: 184.69.179.82	VM 8: 172.16.1.24	**From:** 17:18:46 **To:** 17:29:10+	71
2	Password Guessing: SSH	Attacker IP: 184.69.179.82	VM 8: 172.16.1.24	**From:** 17:29:48 **To:** 17:38:55	0
3	Successful Password Guess: SSH (Unauthorized Login)	Attacker IP: 184.69.179.82	VM 8: 172.16.1.24	**From:** 17:38:53 **To:** 17:38:53	0
4	Unauthorized Login: SSH	Attacker IP: 184.69.179.82	VM 8: 172.16.1.24	**From:** 17:43:40 **To:** 18:29:48	0
5	Unauthorized Login: SSH	Attacker IP: 184.69.179.82	VM 8: 172.16.1.24	**From:** 18:18:10 **To:** 18:18:11	0
6	Failed Login Attempt: SSH (using Metasploit ssh pubkey module)	Attacker IP: 184.69.179.82	VM 8: 172.16.1.24	**From:** 18:21:46 **To:** 18:21:46	0
7	Password Guessing: SSH	Attacker IP: 184.69.179.82	VM 8: 172.16.1.24	**From:** 18:28:03 **To:** 18:28:19	117
8	Unauthorized Login: SSH	Attacker IP: 184.69.179.82	VM 8: 172.16.1.24	**From:** 18:28:19 **To:** 18:29:44	0

4.1.3 Day 3, 2016-12-16

Seq	Attack	Source	Destination	Time	Packets
1	Port Scanning	Attacker IP: 64.180.188.173	VM 4: 172.16.1.26	**From:** 17:09:45 **To:** 17:12:13	44
2	Port Scanning	Attacker IP: 64.180.188.173	VM 8: 172.16.1.24	**From:** 17:16:15 **To:** 17:16:42	0
3	Password Guessing: SSH	Attacker IP: 64.180.188.173	VM 8: 172.16.1.24	**From:** 17:19:44 **To:** 17:23:59	265
4	Unauthorized Login: SSH	Attacker IP: 64.180.188.173	VM 8: 172.16.1.24	**From:** 17:23:59 **To:** 18:16:45	0
5	Unauthorized Login: SSH	Attacker IP: 64.180.188.173	VM 8: 172.16.1.24	**From:** 17:26:31 **To:** 17:53:25	0
6	Download and install netcat (apt)	VM 8: 172.16.1.24	archive.ubuntu.com	**From:** 17:32:22 **To:** 17:33:06+	0
7	Start backdoor using netcat	VM 8: 172.16.1.24	N/A	17:36:26	–
8	Reverse Shell Open	VM 8: 172.16.1.24	Attacker IP: 64.180.188.173	**From:** 17:47:07 **To:** 17:52:26+	0

4.1.4 Day 4, 2016-12-19

Seq	Attack	Source	Destination	Time	Packets
1	Unauthorized Login: SSH	Attacker IP: 64.180.188.173	VM 8: 172.16.1.24	**From:** 17:33:27 **To:** 18:01:24	74
2	Ping	VM 8: 172.16.1.24	142.104.64.202	**From:** 17:34:36 **To:** 17:34:53+	0
3	Port Scanning	VM 8: 172.16.1.24	142.104.64.202	**From:** 17:36:18 **To:** 17:36:18	0
4	Failed to connect to backdoor using ncat	VM 8: 172.16.1.24	142.104.64.202	**From:** ~17:57 **To:** ~18:00	0

5	Unauthorized Login: SSH	Attacker IP: 64.180.188.173	VM 8: 172.16.1.24	**From:** 18:06:22 **To:** 18:18:09	231

4.2 Phase Two Attack Scenarios

The attacks in ISOT-CID phase two were divided into 6 rounds lasting 2 hours each on average spread over 6 different days. Moreover, the attackers performed and completed the attack scenarios independently. Data from all other previously mentioned data sources except memory dumps and syslogs were collected but with lightweight agents only.

In this phase, the attacks consist of layer 7 attacks against a web application that attempt to exploit input validation vulnerabilities, including cross-site scripting (XSS), SQL injection and path/directory traversal, as well as network layer DoS attacks launched remotely against the cloud infrastructure.

4.2.1 Day 1, 2018-02-16

Seq	Attack	Source	Destination	Time	Packets
1	Access Website	Attacker IP: 23.16.123.57	VM 10: 172.16.1.27	**From:** 17:24:03 **To:** 17:25:18	28
2	Web Scanning	Attacker IP: 23.16.123.57	VM 10: 172.16.1.27	**From:** 17:27:53 **To:** 17:56:39	183,717
3	Directory Traversal	Attacker IP: 23.16.123.57	VM 10: 172.16.1.27	**From:** 18:17:13 **To:** 18:42:16	258
4	Download Web App configuration file	Attacker IP: 23.16.123.57	VM 10: 172.16.1.27	**From:** 18:50:10 **To:** 18:51:10	12
5	Download SSH key (dhub.pem)	Attacker IP: 23.16.123.57	VM 10: 172.16.1.27	**From:** 18:59:26 **To:** 19:01:25	21

4.2.2 Day 2, 2018-02-19

Seq	Attack	Source	Destination	Time	Packets
1	Network Scanning	Attacker IP 1: 142.104.79.224	VM 10: 172.16.1.27	**From:** 18:26:33 **To:** 18:27:54	723
2	Network Scanning	Attacker IP 1: 142.104.79.224	VM 7: 172.16.1.20	**From:** 18:30:09 **To:** 18:30:33	241

3	Failed Login Attempt: SSH (using credentials stolen in day 1)	Attacker IP 1: 142.104.79.224	VM 7 & 10: 172.16.1.20 & 172.16.1.27	**From:** 18:39:04 **To:** 18:42:56	64
4	Unauthorized Login: SSH	Attacker IP 2: 103.60.13.34	VM 6: 172.16.1.19	**From:** 18:47:13 **To:** 18:47:13	3
5	Network Scanning	Attacker IP 3: 120.63.209.69	VM 8: 172.16.1.24	**From:** 19:12:40 **To:** 19:12:40	2

4.2.3 Day 3, 2018-02-20

Two independent attacks were performed in this day.

Attack Scenario A:

Seq	**Attack**	**Source**	**Destination**	**Time**	**Packets**
1	Web Application Vulnerability Scanning using ZAP (XSS, SQL Injection, Directory Traversal etc.)	Attacker IP 1: 185.210.218.98	VM 10: 172.16.1.27	**From:** 17:30:00 **To:** 18:15:01	10,115
2	Manual Directory Traversal (downloaded shadow file but failed to replace SSH authorized keys file)	Attacker IP 1: 185.210.218.98	VM 10: 172.16.1.27	**From:** 18:10:58 **To:** 18:22:18	66
3	Failed Login Attempt: SSH (using credentials from replacement keys file from step 2)	Attacker IP 1: 185.210.218.98	VM 10: 172.16.1.27	**From:** 18:22:38 **To:** 18:22:43	12
4	Manual XSS	Attacker IP 1: 185.210.218.98	VM 10: 172.16.1.27	**From:** 18:24:01 **To:** 18:47:12	9,840
5	Directory Traversal (downloaded logs and config files containing DB password)	Attacker IP 1: 185.210.218.98	VM 10: 172.16.1.27	**From:** 18:46:11 **To:** 19:01:31	648

6	Failed Login Attempt: MySQL (failed because of host restriction)	Attacker IP 1: 185.210.218.98	VM 8: 172.16.1.24	**From:** 18:55:08 **To:** 18:55:09	12
7	Fuzzing	Attacker IP 1: 185.210.218.98	VM 10: 172.16.1.27	**From:** 19:06:24 **To:** 19:08:32	3,613

Attack Scenario B:

Seq	Attack	Source	Destination	Time	Packets
1	Failed Login Attempt: SSH (using credentials stolen in day 1)	Attacker IP: 23.16.123.57	VM 10: 172.16.1.27	**From:** 17:20:37 **To:** 17:20:38	25
2	Unauthorized Login: SSH (using credentials stolen in day 1)	Attacker IP: 23.16.123.57	VM 7: 172.16.1.20	**From:** 17:25:32 **To:** 17:45:58	475
3	Denial of Service using Slowloris	Attacker IP: 23.16.123.57	VM 10: 172.16.1.27	**From:** 19:00:19 **To:** 19:05:29	19,928

4.2.4 Day 4, 2018-02-21

Seq	Attack	Source	Destination	Time	Packets
1	Password Guessing: Web App (failed)	Attacker IP: 142.104.79.224	VM 10: 172.16.1.27	**From:** 18:55:57 **To:** 19:16:47	2,152

4.2.5 Day 5, 2018-02-23

Two independent attacks were performed in this day.

Attack Scenario A:

Seq	Attack	Source	Destination	Time	Packets
1	Unauthorized Login: SSH (using credentials stolen in day 1)	Attacker IP: 185.210.218.98	VM 7: 172.16.1.20	**From:** 17:46:50 **To:** 17:53:10	1,072

2	Download and install cryptominer	VM 7: 172.16.1.20	(download.)cryptogate.com: (88.99.142.163, 176.9.8.174, 94.130.143.162, 136.243.102.154, 136.243.102.167)	**From:** 17:47:43 **To:** 17:50:55	9,713
3	Run cryptominer	VM 7: 172.16.1.20	176.9.0.89	**From:** 17:50:45 **To:** 19:43:50	2,635

Attack Scenario B:

Seq	Attack	Source	Destination	Time	Packets
1	Access Website	Attacker IP: 23.16.123.57	VM 10: 172.16.1.27	**From:** 17:19:47 **To:** 17:20:52	394
2	Failed Login Attempt: SSH	Attacker IP: 23.16.123.57	VM 7: 172.16.1.20	**From:** 17:23:45 **To:** 17:23:46	29
3	Failed Login Attempt: SSH	Attacker IP: 23.16.123.57	VM 7: 172.16.1.20	**From:** 17:28:50 **To:** 17:28:51	26
4	Failed Login Attempt: SSH	Attacker IP: 23.16.123.57	VM 7: 172.16.1.20	**From:** 17:42:58 **To:** 17:42:58	26
5	HTTP Flood against Web App	Attacker IP: 23.16.123.57	VM 7: 172.16.1.20	**From:** 18:19:09 **To:** 18:45:44	1,811,914