INTEZER

Detection & Response to IPStorm

Storm Alert: **IPStorm** is the latest Windows malware to go multi-platform. New Linux variants of the malware uncovered by **Intezer** target various Linux architectures (ARM, AMD64, Intel 80386) and platforms (servers, Android, IoT) and share code with IPStorm Windows samples first reported by researchers at **Anomali** in 2019. This resource provides practical advice on how to mitigate this emerging threat, including:

- How to detect if your system is compromised by IPStorm.
- How to clean an infected machine. If you are infected, use this **dedicated script** to kill any IPStorm process on your machine.
- What you can do to proactively steer clear of this threat.

Compromise System Detection

Take the following steps to check if your system has been attacked by the IPStorm Linux malware.

1. Check if the IPStorm process is running on your system.

Run: pstree | grep storm

```
roota@ubuntu:~$ pstree | grep storm
        |-storm---6*[{storm}]
        |         |-storm---7*[{storm}]
```

IPStorm will usually run with multiple threads.

2. Check if any IPStorm files exist in your system.

Run: sudo find / -name “storm*” -type f

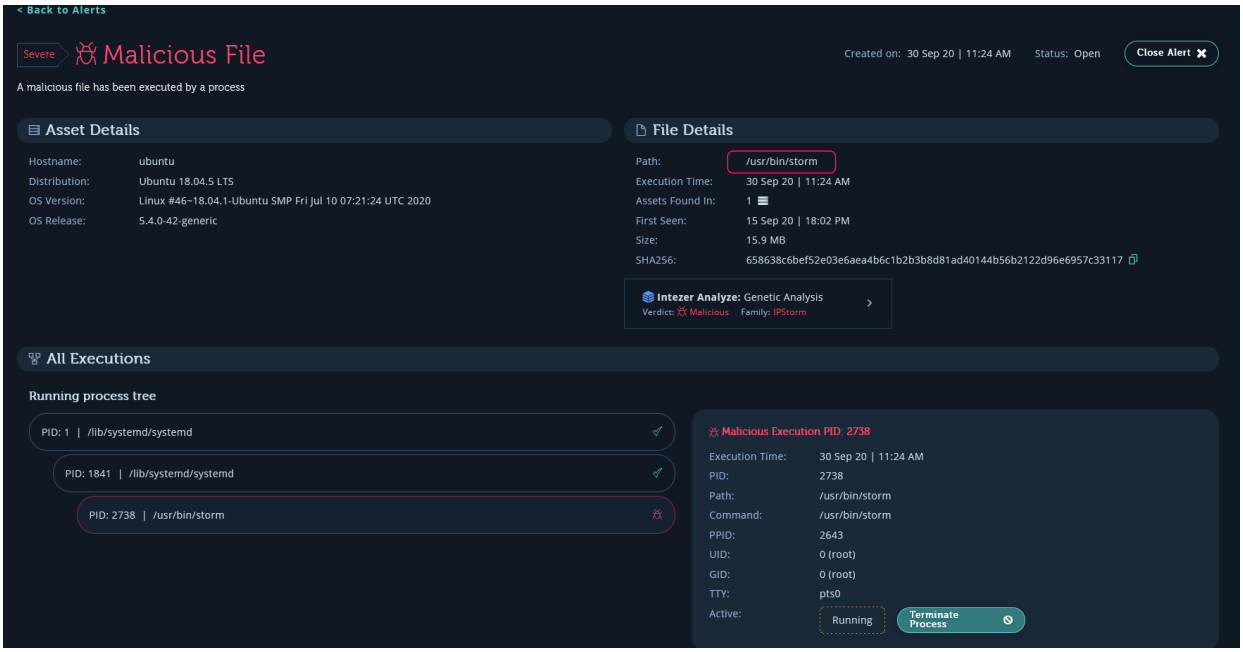
```
roota@ubuntu:~$ sudo find / -name "storm*" -type f
/etc/storm.key
/etc/systemd/system/storm.service
/usr/bin/storm
```

3. Check all open ports on your system and the processes associated with them.

Run: sudo ss -tulpn | grep storm

```
tcp    LISTEN   0        128              0.0.0.0:45671          0.0.0.0:*      users:(("storm",pid=16639,fd=9))
tcp    LISTEN   0        128                  *:46313              *:*        users:(("storm",pid=16639,fd=23))
```

4. The **Intezer Protect Community Edition** continuously monitors all processes running on your system. The screen capture below is taken from an alert following the execution of IPStorm on a server. The alert provides further context about the suspicious activity including malware family, full executable path, process ID, execution time, and the Genetic Analysis where you can see code reuse between this threat and other malware samples. Most importantly, you can quickly terminate the running process.



How to Terminate IPStorm on a Compromised System

You may take the following steps, or alternatively, just run **this script** on your infected machine.

- If the malware runs as a service you should immediately stop the service by executing this command:

  sudo systemctl stop storm.service

- Delete all files that are related to IPStorm. Most importantly, delete the binary itself which will be located at /tmp/storm or /usr/bin/storm.
- Kill the process by running:

  sudo pkill -9 storm

Incident Response

This **YARA rule** is intended to be run against in-memory artifacts in order to detect any IPStorm implants that have been injected into memory.

System Security Hardening

- Make sure your SSH connection is secured. Use a key instead of a password or use multi-factor authentication. **Browse here** for more tips about SSH hardening.
- Make sure your system is updated to the latest software and aligned with most recent security best practices.
- Runtime cloud workload protection solutions like **Intezer Protect** provide full visibility over the code in your system and alert on any suspicious or unauthorized code that deviates from the secure baseline.