SECURONIX™

**Securonix Threat Research:**

# Detecting Persistent Cloud Infrastructure/ Hadoop/YARN Attacks Using Security Analytics: Moanacroner, XBash, and Others

**Oleg Kolesnikov and Harshvardhan Parashar**
Securonix Threat Research Team

Last Updated: January 15, 2019

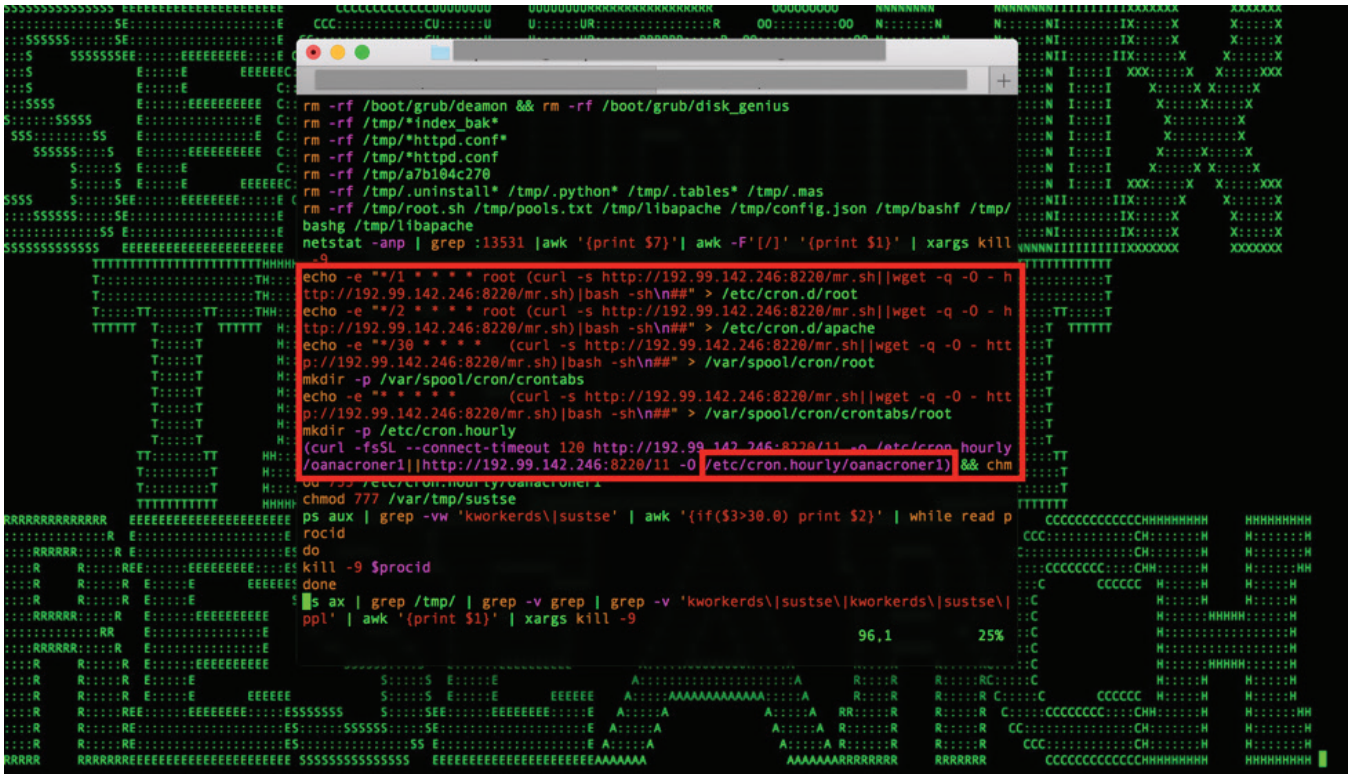


Figure 1: Moanacroner Establishes Persistence After Initial Cloud YARN/Hadoop Infection Using Crontabs

## Introduction

In recent months, we have been observing an increase in the number of automated attacks targeting exposed cloud infrastructure/Hadoop/YARN instances. Some of the attacks we have been seeing – for example, Moanacroner (a variant of Sustes [11]) – are fairly trivial, targeted single-vector/single-platform attacks where the focus is mainly on cryptomining.

Some attacks, however, are multi-vector/multi-platform threats where multiple functionalities – including cryptomining, ransomware, and botnet/worms for both Linux and Windows – are combined as part of the same malicious threat (for example, XBash).

The Securonix Threat Research Team has been actively investigating and closely monitoring these persistent malicious attacks impacting exposed cloud infrastructure in order to help our customers prevent, detect, and mitigate/respond to the attacks. Below is a summary of what we currently know, and our recommendations for possible mitigations and Securonix predictive indicators that can be used to detect such attacks.


Figure 2: Cloud Infrastructure Hadoop/YARN Logs Containing the Initial Infection/Malicious Commands Launched by Various Malicious Threat Actors

## Summary

Here is a summary of some of the key details about some of the persistent cloud infrastructure/Hadoop/YARN attacks we have been observing.

### Impact

In most cases, the focus of the attacks is on installing a second-stage payload for cryptomining and/or remote access. In other cases, the malware propagates and infects the exposed services, removes data, and installs second-stage cryptomining and ransomware payloads. For example, in the case of Xbash (which was reported a few months ago), the malware deletes the databases instead of encrypting them, and does not have any functionality to backup/recover the files.

### Infiltration Vector(s)

Some of the key vectors we have been observing in these attacks involve the use of Hadoop unauthenticated command execution [2] and Redis remote command execution [3]. There have also been other vectors used, including ActiveMQ (Arbitrary File Execution) [4].

### Command and Control (C2)

There are a number of different C2 servers observed, and the hop points change continuously. Some malware fetches a hardcoded list of C2 server domain names from a pastebin webpage. C2 servers are then used to collect the target IP addresses and domains, download additional malicious scripts to perform cryptojacking, fetch additional username/password lists to be used for brute-force attacks, and report the results.

### Persistence

Most of the malicious implants observed maintain persistence by creating a cronjob entry, usually by leveraging different files (for example, on Linux: /etc/crontab, /etc/cron.d/root, /etc/cron.d/apache, /var/spool/cron/root, etc.), or by creating a malicious startup item if running on Windows, in order to download additional malicious stagers from a C2 server.

## Observed Artifacts

### Hash Values

7a18c7bdf0c504832c8552766dcfe0ba33dd5493daa3d9dbe9c985c1ce36e5aa
0b9c54692d25f68ede1de47d4206ec3cd2e5836e368794eccb3daa632334c641
dbc380cbfb1536dfb24ef460ce18bccdae549b4585ba713b5228c23924385e54
5b790f02bdb26b6b6b270a5669311b4f231d17872aafb237b7e87b6bbb57426d
e59be6eec9629d376a8a4a70fe9f8f3eec7b0919019f819d44b9bdd1c429277c
f808a42b10cf55603389945a549ce45edc6a04562196d14f7489af04688f12bc
dcd37e5b266cc0cd3fab73caa63b218f5b92e9bd5b25cf1cacf1afdb0d8e76ff
de63ce4a42f06a5903b9daa62b67fcfbdeca05beb574f966370a6ae7fd21190d
09968c4573580398b3269577ced28090eae4a7c326c1a0ec546761c623625885
a27acc07844bb751ac33f5df569fd949d8b61dba26eb5447482d90243fc739af
f888dda9ca1876eba12ffb55a7a993bd1f5a622a30045a675da4955ede3e4cb8
31155bf8c85c6c6193842b8d09bda88990d710db9f70efe85c421f1484f0ee78
725efd0f5310763bc5375e7b72dbb2e883ad90ec32d6177c578a1c04c1b62054
d7fbd2a4db44d86b4cf5fa4202203dacfefd6ffca6a0615dca5bc2a200ad56b6
ece3cfdb75aaabc570bf38af6f4653f73101c1641ce78a4bb146e62d9ac0cd50
2103af76b361efbebca8bb59f94ee4b3
38699519eb6197359f89bcc38c7266f1

## C2 IP/Stager Addresses

167.99.166.61
192.99.142.246
202.144.193.110
213.32.29.143
37.44.212.223
142.44.215.177
144.217.61.147
104.24.107.22
104.24.106.22
104.18.63.34
104.18.62.34
45.63.17.78
104.24.99.120
104.24.98.120
104.27.137.249
104.27.136.249
195.22.26.248

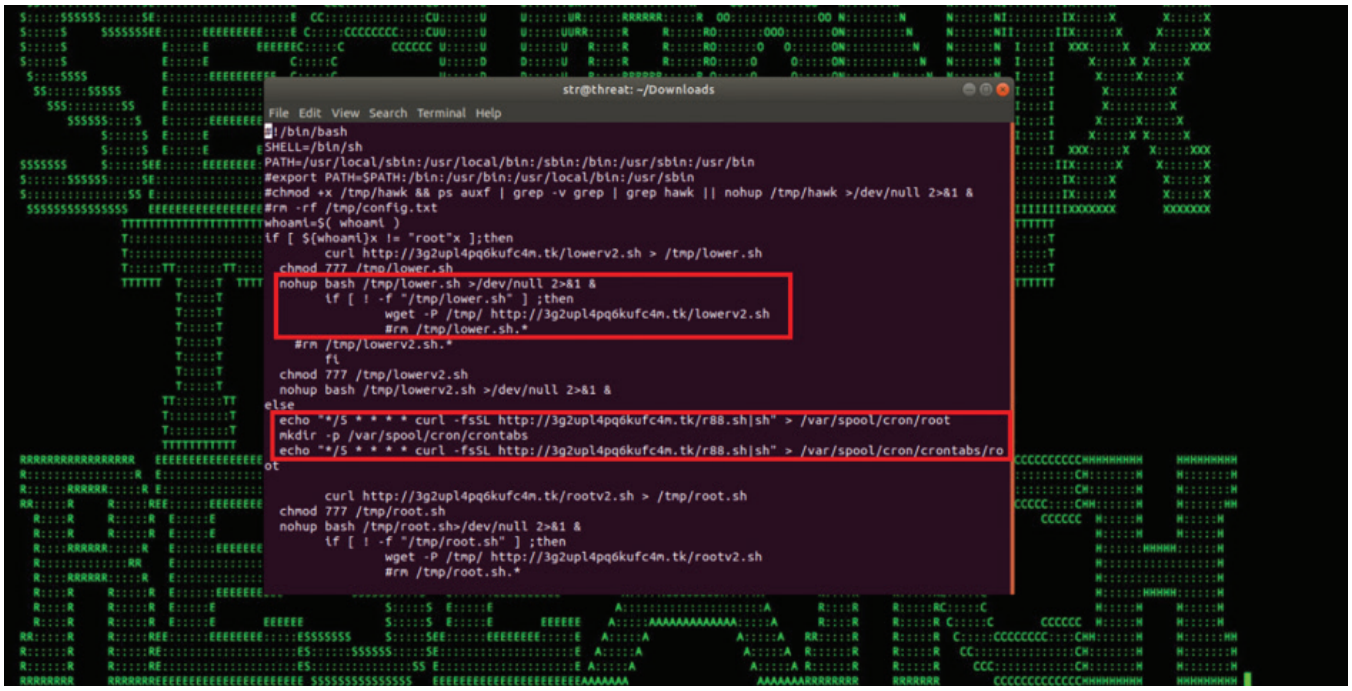


Figure 3: Xbash Maintains Persistence by Setting Up Cronjobs to Download Additional Malicious Scripts

## Some Relevant Behaviors - Highlights

There are many common behaviors shared by the malicious threat actors we've been observing, including the infection vectors mentioned above, the persistence mechanisms, and some of the actions on objectives, including cryptomining payloads. XBash is a good example of a more advanced threat actor leveraging many of these common behaviors, so below we will provide some highlights of some of the relevant behaviors used by Xbash from a detection perspective.

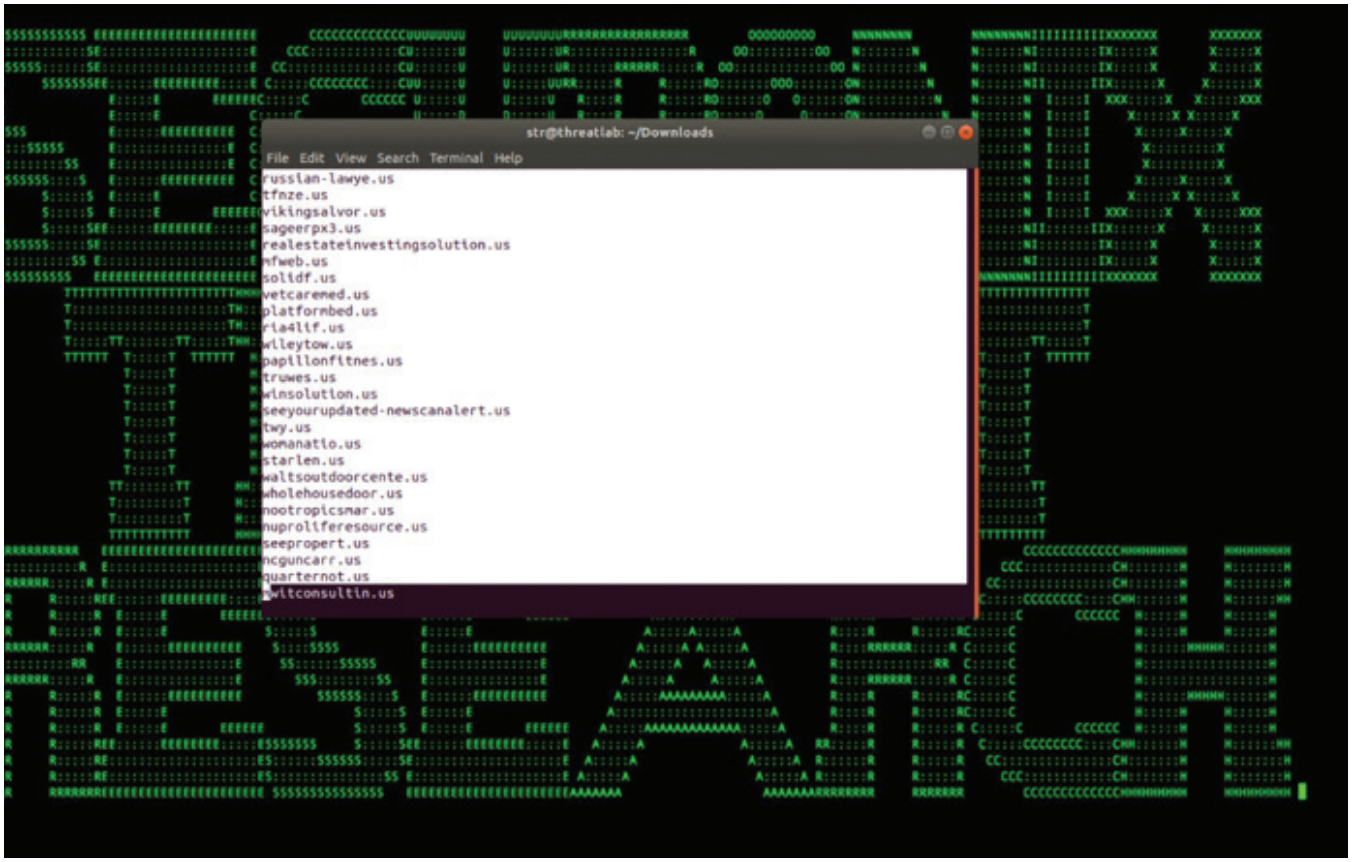


Figure 4: Target Domain List Fetched by Xbash from One of the C2s

The Xbash botnet has been active since May 2018 and has shown a distinguishing combination of cryptojacking, cybersabotage, and multi-platform characteristics. Xbash malware infects Linux and Windows systems with the aim of deleting critical databases, installing cryptojacking scripts, and asking for ransoms by impersonating a ransomware attack. The Xbash botnet has been scanning the target domains and IP addresses specified by the C2 for multiple services running on different ports including [1]:

HTTP: 80, 8080, 8888, 8000, 8001, 8088
MySQL/MariaDB: 3309, 3308,3360 3306, 3307, 9806, 1433
MySQL: 3306
Memcached: 11211
RDP: 3389
VNC: 5900, 5901, 5902, 5903
FTP: 21
MongoDB: 27017
PostgreSQL: 5432
Telnet: 23, 2323
SNMP: 161
Oracle Database: 1521
NTP: 123
CouchDB: 5984
Rexec: 512
Redis: 6379, 2379
ElasticSearch: 9200
UPnP/SSDP: 1900
DNS: 53
LDAP: 389
Rlogin: 513
Rsh: 514
Rsync: 873

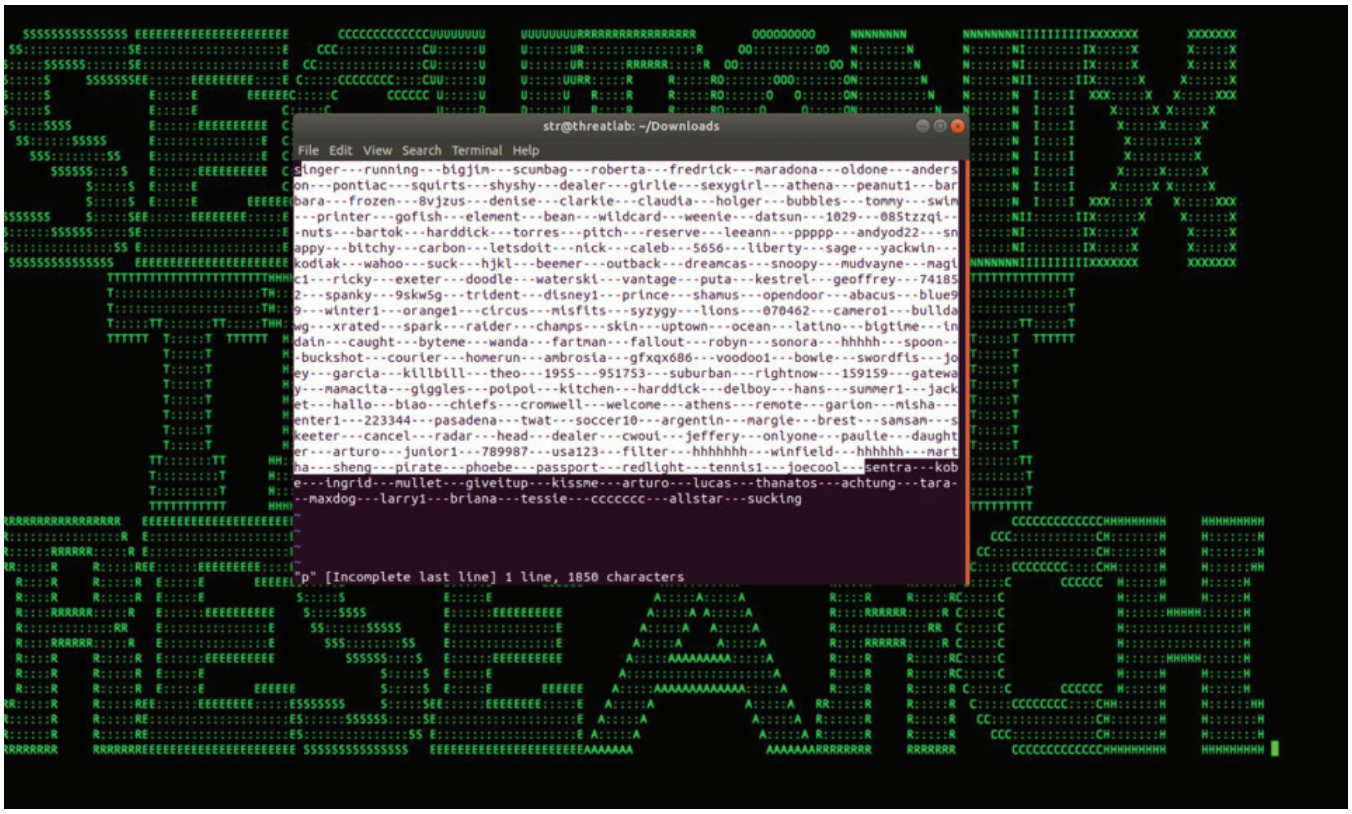


Figure 5: Password Dictionary Fetched from One of the C2s for Brute-Force Attacks

The malware infiltrates and spreads by brute-forcing the weak passwords configured on the above services, or by exploiting one of three vulnerabilities found on Hadoop YARN Resource Manager, Redis, and ActiveMQ.

Once the malware is successfully able to log into the database services (MYSQL, PostgreSQL, MongoDB, or phpMyAdmin) it deletes the existing databases stored on the server and creates a database with a ransom note specifying the amount and the bitcoin wallet.

While infecting a vulnerable Redis service Xbash determines if the server is installed on Windows or Linux by identifying the location of the installation from the config. If the Redis is installed on Windows, the malware creates a startup item for persistence and downloads additional scripts and executables to perform cryptojacking or install ransomware [1].

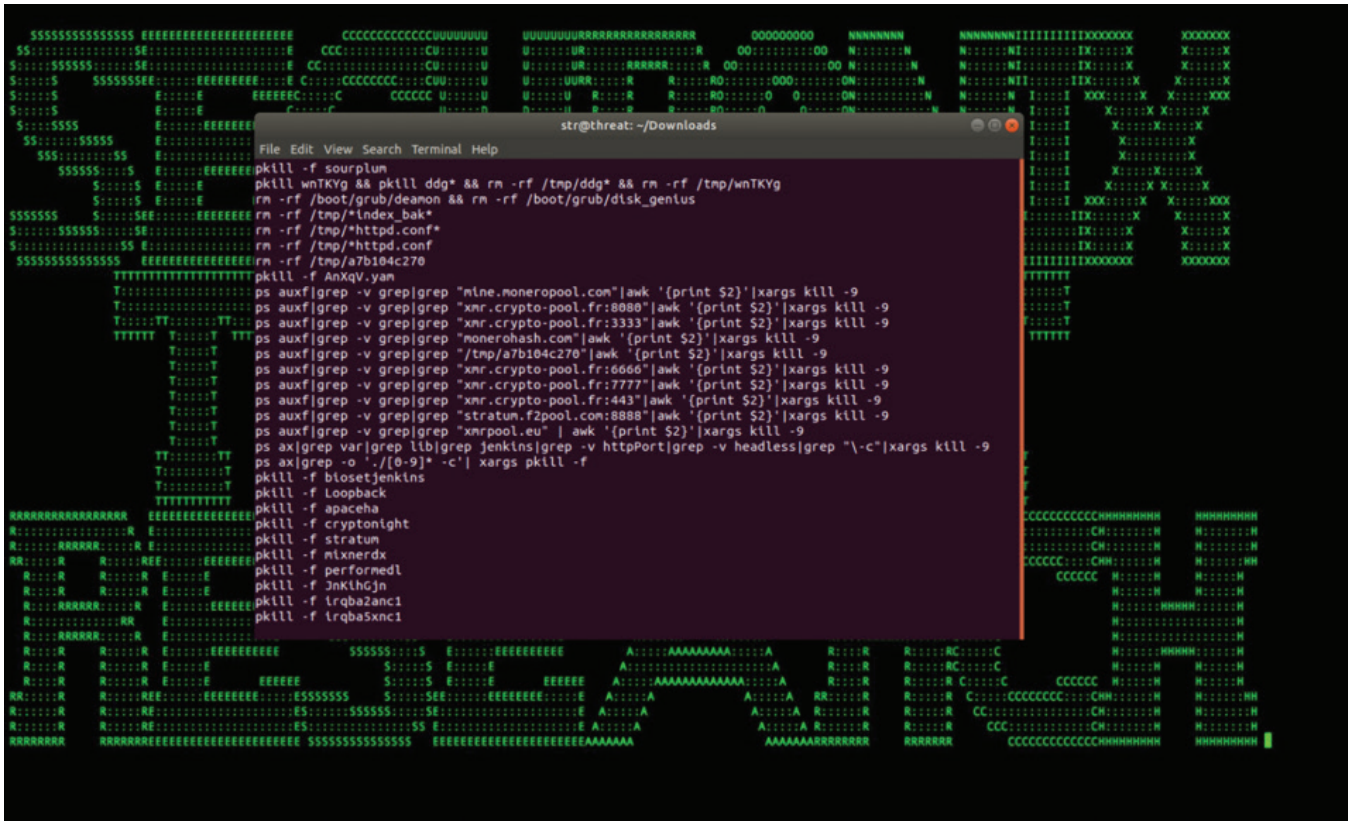


Figure 6: Malicious Script Kills Any Other Cryptomining Services Found Running

## Detection - Sample Securonix Spotter Search Queries

Some sample Securonix Spotter search queries to assist with the detection of existing infections.

## ETDR Process Monitoring (Process Hash Conditions)

(rg_category contains “Endpoint” OR rg_category contains “ips” OR rg_category contains “ids”) AND (customstring3=7a18c7bdf0c504832c8552766dcfe0ba33dd5493daa3d9dbe9c985c1ce36e5aa or customstring3=0b9c54692d25f68ede1de47d4206ec3cd2e5836e368794eccb3daa632334c641 or customstring3=dbc380cbfb1536dfb24ef460ce18bccdae549b4585ba713b5228c23924385e54 or customstring3=5b790f02bdb26b6b6b270a5669311b4f231d17872aafb237b7e87b6bbb57426d or customstring3=e59be6eec9629d376a8a4a70fe9f8f3eec7b0919019f819d44b9bdd1c429277c or customstring3=f808a42b10cf55603389945a549ce45edc6a04562196d14f7489af04688f12bc or customstring3=dcd37e5b266cc0cd3fab73caa63b218f5b92e9bd5b25cf1cacf1afdb0d8e76ff or customstring3=de63ce4a42f06a5903b9daa62b67fcfbdeca05beb574f966370a6ae7fd21190d or customstring3=09968c4573580398b3269577ced28090eae4a7c326c1a0ec546761c623625885 or customstring3=a27acc07844bb751ac33f5df569fd949d8b61dba26eb5447482d90243fc739af or customstring3=f888dda9ca1876eba12ffb55a7a993bd1f5a622a30045a675da4955ede3e4cb8 or customstring3=31155bf8c85c6c6193842b8d09bda88990d710db9f70efe85c421f1484f0ee78 or customstring3=725efd0f5310763bc5375e7b72dbb2e883ad90ec32d6177c578a1c04c1b62054 or customstring3=d7fbd2a4db44d86b4cf5fa4202203dacfefd6ffca6a0615dca5bc2a200ad56b6 or customstring3=ece3cfdb75aaabc570bf38af6f4653f73101c1641ce78a4bb146e62d9ac0cd50 or customstring3=2103af76b361efbebca8bb59f94ee4b3 or customstring3=38699519eb6197359f89bcc38c7266f1)

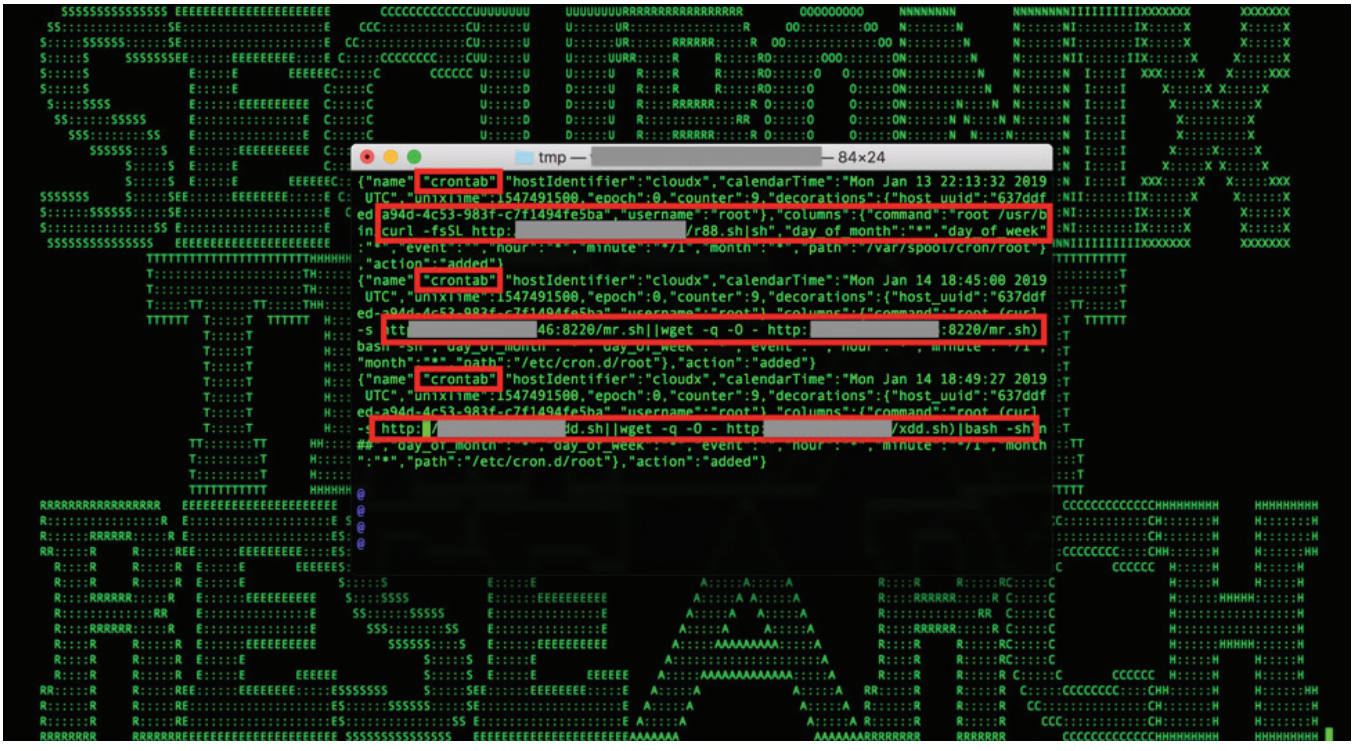


Figure 7: Examples of Changes to Crontab Made by Malicious Implants in FIM Logs

### Network Monitoring (Network Traffic to C2/Stagers)

rg_category contains “Firewall” OR rg_category contains “proxy”) AND (destinationaddress IN “167.99.166.61”,“192.99.142.246”,“202.144.193.110”,“213.32.29.143”,“37.44.212.223”,“142.44.215.177”, “144.217.61.147”, “104.24.107.22”, “104.24.106.22”, “104.18.63.34”, “104.18.62.34”, “45.63.17.78”, “104.24.99.120”, “104.24.98.120”, “104.27.137.249”, “104.27.136.249”, “195.22.26.248”)

## Securonix Detection

### Some Relevant Log/Data Source Examples

VPC EDR logs (sysmon, osquery, Bit9/Carbonblack, etc.)
Cloud infrastructure application/database/webserver/Hadoop/YARN logs
VPC flow logs, etc.
Windows Event Logs

### Some Examples of Securonix Predictive Indicators

Below is a summary of some of the relevant Securonix predictive indicators to increase the chances of early detection of this, and potentially other future variants of the threats mentioned above, in your cloud infrastructure. Figure 8 shows a practical example of detection of the malicious threats impacting cloud infrastructure described above using Securonix.

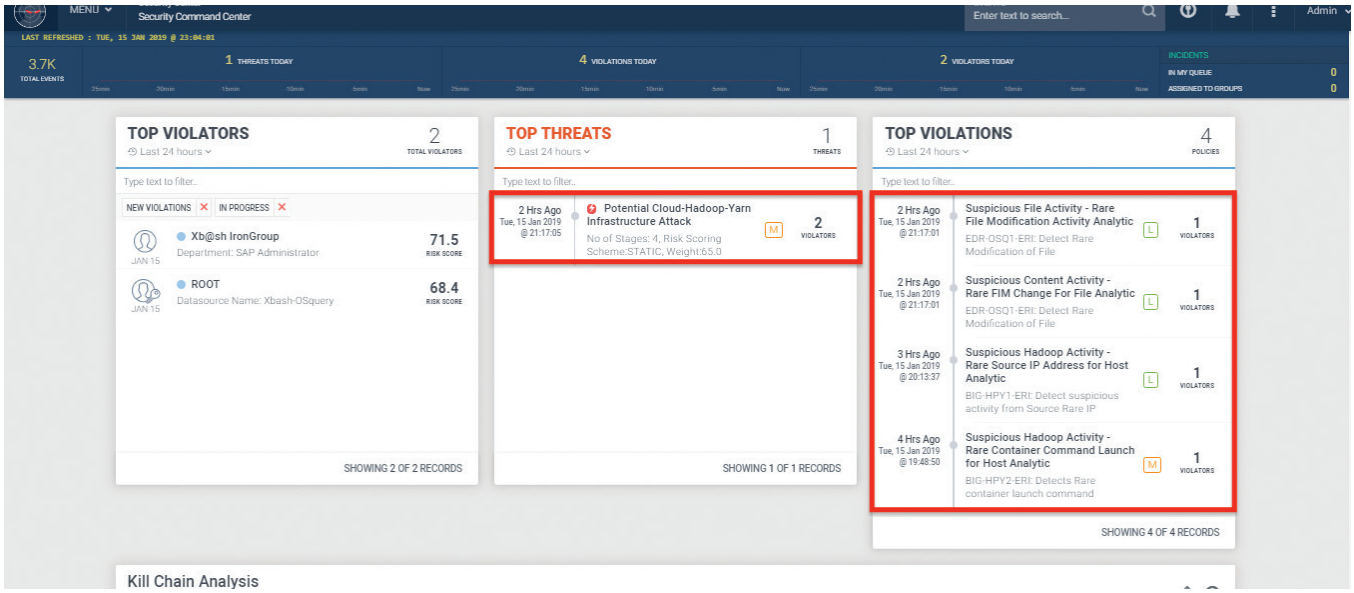


Figure 8: Practical Example of Detection Using Securonix

- Suspicious Filesystem Activity - Unusual FIM Change For File Analytic
  - + One possible example is an unusual change to one of the crontab files (see Figure 7).
- Suspicious Process Activity - Unusual Parent-Child Relationship For Host Analytic
  - + One possible example is an unusual parent process for wget or curl execution that is commonly used by malicious threat actors as part of staging the attacks.
- Suspicious Hadoop Activity - Unusual Container Command Launch for Host Analytic
  - + One possible example is running unexpected commands as part of YARN manager activity (see Figure 2).
- Suspicious Network Activity - Unusual Outbound Connection For Container Analytic
- Suspicious Windows Activity - Unusual CPU Utilization Amount For Host Analytic
- Suspicious Database Activity - Unusual Source IP Address for User Analytic

and a number of other Securonix behavioral analytics/predictive indicators including EDR-SYM19-ERI, EDR-SYM2-ERI, PXY-PAN5-TAN, WEL-WOT1-BPI, WEL-TAN2-BPI, WEL-SCH2-RUN, EDR-SYM12-RUN, and others.

## Mitigation and Prevention - Securonix Recommendations

Here are some of the Securonix recommendations to help customers prevent and/or mitigate the attack:

1. Continuously review your cloud infrastructure services' exposure to the internet, including Hadoop/YARN, Redis, and ActiveMQ, and restrict access whenever possible to reduce the potential attack surface (see http://activemq.apache.org/security-advisories.data/CVE-2016-3088-announcement.txt, http://antirez.com/news/96, https://fortiguard.com/encyclopedia/ips/46466). Also, consider leveraging a centralized patch management system.
2. Consider implementing Redis in protected mode (see http://antirez.com/news/96).
3. Implement strong password policies for your services mentioned above as some of the malicious threat actors described, such as Xbash, use password brute-force to propagate.

## References

[1] Claud Xiao, Cong Zheng and Xingyu Jin. Xbash Combines Botnet, Ransomware, Coinmining in Worm that Targets Linux and Windows. Unit 42. September 17, 2018. https://researchcenter.paloaltonetworks.com/2018/09/unit42-xbash-combines-botnet-ransomware-coinmining-worm-targets-linux-windows/.Last accessed: 01-14-2019.

[2] Rapid7. Hadoop YARN ResourceManager Unauthenticated Command Execution. Rapid7. March 23, 2018. https://www.rapid7.com/db/modules/exploit/linux/http/hadoop_unauth_exec. Last accessed: 01-14-2019.

[3] Antirez. Redis Remote Command Execution Redis Remote Command Execution. Packet Storm. Nov 3, 2015. https://packetstormsecurity.com/files/134200/Redis-Remote-Command-Execution.html. Last accessed: 01-14-2019.

[4] NVD. CVE-2016-3088 Detail. National Vulnerability Database. June 01, 2016. https://nvd.nist.gov/vuln/detail/CVE-2016-3088. Last accessed: 01-14-2019.

[5] Omri Ben Bassat. Iron Cybercrime Group Under The Scope. Intezer. May 29, 2018. https://www.intezer.com/iron-cybercrime-group-under-the-scope-2/. Last accessed: 01-14-2019.

[6] Blockchain. Bitcoin Address. September 26, 2018. https://www.blockchain.com/btc/address/1Kss6v4eSUgP4WrYtfYGZGDoRsf74M7CMr. Last accessed: 01-14-2019.

[7] Blockchain. Bitcoin Address. October 02, 2018. https://www.blockchain.com/btc/address/1jqpmcLygJdH8fN7BCk2cwwNBRWqMZqL1. Last accessed: 01-14-2019.

[8] Antirez. A few things about Redis security. November 3, 2015. http://antirez.com/news/96. Last accessed: 01-14-2019.

[9] Green-m. hadoop_unauth_exec.rb. October 19, 2016. https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/linux/http/hadoop_unauth_exec.rb. Last accessed: 01-14-2019.

[10] FortiGuard Labs. Apache.Hadoop.YARN.ResourceManager.Command.Execution. Fortinet. https://fortiguard.com/encyclopedia/ips/46466. Last accessed: 01-14-2019.

[11] Marco Ramilli. Sustes Malware: CPU for Monero. https://marcoramilli.com/2018/09/20/sustes-malware-cpu-for-monero/. Last accessed: 01-14-2019.

## ABOUT SECURONIX

Securonix is radically transforming all areas of data security with actionable security intelligence. Our purpose-built, advanced security analytics technology mines, enriches, analyzes, scores and visualizes customer data into actionable intelligence on the highest risk threats from within and outside their environment. Using signature-less anomaly detection techniques that track users, account and system behavior, Securonix is able to detect the most advanced insider threats, data security and fraud attacks automatically and accurately.

## CONTACT SECURONIX

**www.securonix.com**
info@securonix.com | (310) 641-1000

0119


SECURONIX™