Lacework™

Lacework 2021 Cloud Threat Report

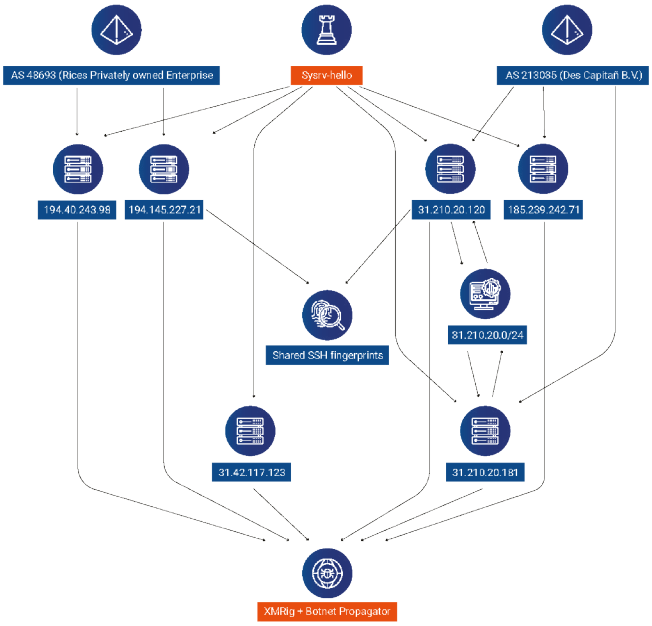
Volume 1

Lacework Labs Research

The Lacework Labs team continually conducts security research focused on risks and threats relevant to cloud services, containers and container orchestration systems, and new attack surfaces that the public cloud exposes through additional services or deployment methods. This quarter the team has researched a variety of new Linux malware families, and shared multiple analyst techniques on improved investigation quality.

Sysrv-Hello Expands Infrastructure

This blog is an analysis of Sysrv-hello. Sysrv-hello is a multi-architecture Cryptojacking botnet that first emerged in late 2020, and employs Golang malware compiled into both Linux and Windows payloads. The malware is equal parts XMRig crypto miner and aggressive botnet-propagator. The propagator leverages MySQL and Tomcat brute forcing along with a suite of exploits including those for Atlassian and Apache. The malware also leverages several "No CVE" command execution techniques including those for Jupyter notebook and Tomcat Manager.



Resolving Embedded Files at Runtime via strace

This blog is a tutorial on resolving embedded files at runtime via strace. Modern Linux malware binaries are being shipped with one or more embedded files. Often, the first stage binary is simply a dropper for the real payload. Prior to the "real payload" being dropped, it's common to see checks for the host's CPU architecture, Linux distribution or a series of other factors that influence which embedded payload is used on the victim host. When you add in the complexities of obfuscation, encryption and decompilation of modern languages (Golang/Rust), identifying said embedded resources and manually extracting them through static reversing engineering techniques is often quite the time sink.

Carbine Loader Cryptojacking Campaign

Lacework Labs recently came across an interesting shell script that's part of an opportunistic Cryptojacking campaign. This campaign operated through the remote code execution of public facing Nagios XI applications. In this blog, Lacework Labs has dubbed the loader script "Carbine Loader" during our research and clustering process.

Groundhog Botnet Rapidly Infecting Cloud

This blog is an analysis of the "Groundhog" DDoS botnet. As early as 2015, the Groundhog botnet began proliferating via SSH brute force attacks. The botnet is believed to have a China nexus and has been active since its inception.

In early December 2020, Lacework Labs started monitoring activity along with botnet traffic from a sinkhole operation.

Our analysis revealed the botnet is rapidly expanding by hundreds of new infections daily and has to date infected at least 26K servers.

LD_PRELOAD processes hiding technique

In this video micro-lesson, we describe how attackers can hide processes from common Linux monitoring tools by using LD_PRELOAD and Shared Objects to overwrite common functions. We see this technique used frequently by attackers targeting cloud workloads.

Threat Landscape Events

Lacework Labs closely monitors and reacts to activity in the global threat landscape. In this section, we aim to share some of the more interesting and noteworthy events which we've been involved with.

Supply Chain Threats

Over the recent years supply chain attacks have become more common due to their astonishing effectiveness at completing an adversaries mission. Supply chain attacks are one of the most concerning threats for the Lacework Labs team. In this quarter, multiple were discovered and publicly reported, including Codecov.

Codecov, a popular code coverage tool, was compromised for over two months allowing attackers to steal victim credentials. The attack occurred through a single-line modification to their bash uploader, essentially automating the process for all Codecov used to run malicious code to collect and exfiltrate machine credentials. Codecov has a customer base of more than 29,000 enterprises, so the enormous impact can closely be compared to the recent Solar Winds supply chain attack.

Upon news of the attack happening, Lacework Labs went to work on tracking down the redacted technical IOCs (indicators of compromise) through open-source intelligence and further internal research. Once we collected and verified malicious files and attacker IP addresses, we scanned internal customer telemetry to proactively identify and alert all impacted customers.

Tactics, Techniques, and Procedures

Lacework Labs designs, builds, and tracks threat activity in a methodology based around the MITRE ATT&CK® techniques on top of our own expertise of adversary activity. This section details the quarters most noteworthy Tactics, Techniques, and Procedures (TTPs).

Permission Groups Discovery: Cloud Groups [T1069]

Permission groups discovery [T1069] is when adversaries attempt to find cloud groups and permission settings, often to determine the particular roles of users and groups to use maliciously. When an AWS user or role is compromised by an attacker we typically see them first query the IAM service to check for permissions. Commonly this is IAM list-users, list-policies, and get-account-authorization-details.

Many opportunistic threats automate the collection of valid accounts for lateral movement, as **we've written about in Carbine Loader and Sysrv.**

Valid Accounts: Cloud Accounts [T1078]

Lacework Labs has observed many cases in which an attacker seeks to obtain and abuse credentials of a cloud account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion [T1078]. Many opportunistic threats automate the collection of valid accounts for lateral movement, as we've written about in Carbine Loader and Sysrv. We've also observed attackers obtaining AWS credentials and using them to hijack resources in their victim's accounts.

Cloud Infrastructure Discovery [T1580]

Cloud infrastructure discovery [T1580] is when an adversary may attempt to discover resources that are available within an infrastructure-as-a-service (IaaS) environment. Lacework Labs observes this technique quite often in most cloud-capable threats. In addition to the permission enumeration techniques described above, we typically observe attackers use the S3 and EC2 service upon initial access. Most commonly are the calls S3 list-buckets and EC2 describe-instances.

Threat Intelligence Highlight

Each quarter Lacework Labs will share a deeper highlight of a single threat we actively track, hunt for, and take a particular interest in. The threat for this report is the adversary group most commonly known as TeamTNT.

Lacework Labs News

For a closing section to this quarterly report, let's review some recent news about the Lacework Labs team itself.

Social Media Presence

As you can read in our team's mission statement, we aim to be a true contributing force to the security community at large. As a step in that direction the Lacework Labs team continues to build and expand our online presence. Below are areas you can find and follow us delivering excellence in efficacy and innovative threat research. **Click below!**

TeamTNT

Name	•	**TeamTNT / Hilde**
Originating	•	**Germany**
Type	•	**Opportunistic**
Target Location	•	**Global**

Cryptojacking · **Botnet** · **Financial**

Motivation and Objetives

TeamTNT is overall motivated by public notoriety. Attack objectives are primarily focused on financial gain. This is achieved through commodity malware used in cryptojacking and botnet campaigns.

Observed Toolkit

- Diamorphine Open Source Rootkit
- Black-T Backdoor
- Tsunami IRC Backdoor / DDoS bot
- AWS credential stealing worm
- Cetus - Cryptojacking Worm
- Shell Scripts with unique features
- Mirai botnet, batik variant
- Weave Scope
- XMRig Miner, monero
- Libprocesshider
- Ziggystartux
- MimiPenguin
- Docker-escape
- Massscan / Priscan

Targeted Services

- Linux OS
- AWS Overall
- Openstack
- Docker
- SSH
- VNC
- Nahios
- Django
- Oracle
- applmgr
- Git
- ansible
- mysql
- Postgresql
- Hadoop
- elastic
- Redis
- Jenkins
- nexus
- FTP (Various)
- Jboss
- tomcat
- Busy box
- Gin
- zabbix

Attack Techniques

Initial Access
T1190 - Exploit Public-Facing Application
T1133 - External Remote Services

Execution
T1059 - Command and Scripting Interpreter

Persistence
T1525 - Implant Container Image
T1574 - Hijack Execution Flow

Credential Access
T1070 - Indicator Removal on Host

Defence Evasion
T1003 - OS Credential Dumping

Discovery
T1046 - Network Service Scanning

Lateral Movement
T1021 - Remote Services
T1021.004 - SSH

Collection
T1119 - Automated Collection

Exfiltration
T1020 - Automated Exfiltration

Impact
T1496 - Resource Hijacking

Social Media

Contributing to MITRE ATT&CK

> We're excited to announce that Lacework Labs is officially a contributing member of MITRE ATT&CK®! For anyone not familiar - "ATT&CK is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community."

In the Media

Some of the research the team has published this quarter was written about by third parties, such as news sources, and referenced/recommended by other security vendors.

- **Bleeping Computer** - "New cryptomining malware builds an army of Windows, Linux bots".
- **The Record** - "Sysrv: A new crypto-mining botnet is silently growing in the shadows".
- **The CyberWire Newsletter** - "SolarWinds campaign infrastructure. ToxicEye RAT abuses Telegram. Mount Locker shifts tactics. New cryptojacking botnet."
- **AT&T Cybersecurity, Open Threat Exchange:**
  - Sysrv-Hello Cryptominer Botnet
  - Carbine Loader
  - Groundhog Botnet
- **RiskIQ Threat Intel Portal**
  - Sysrv-Hello Expands Infrastructure
  - Carbine Loader Cryptojacking Campaign