Lacework™

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.

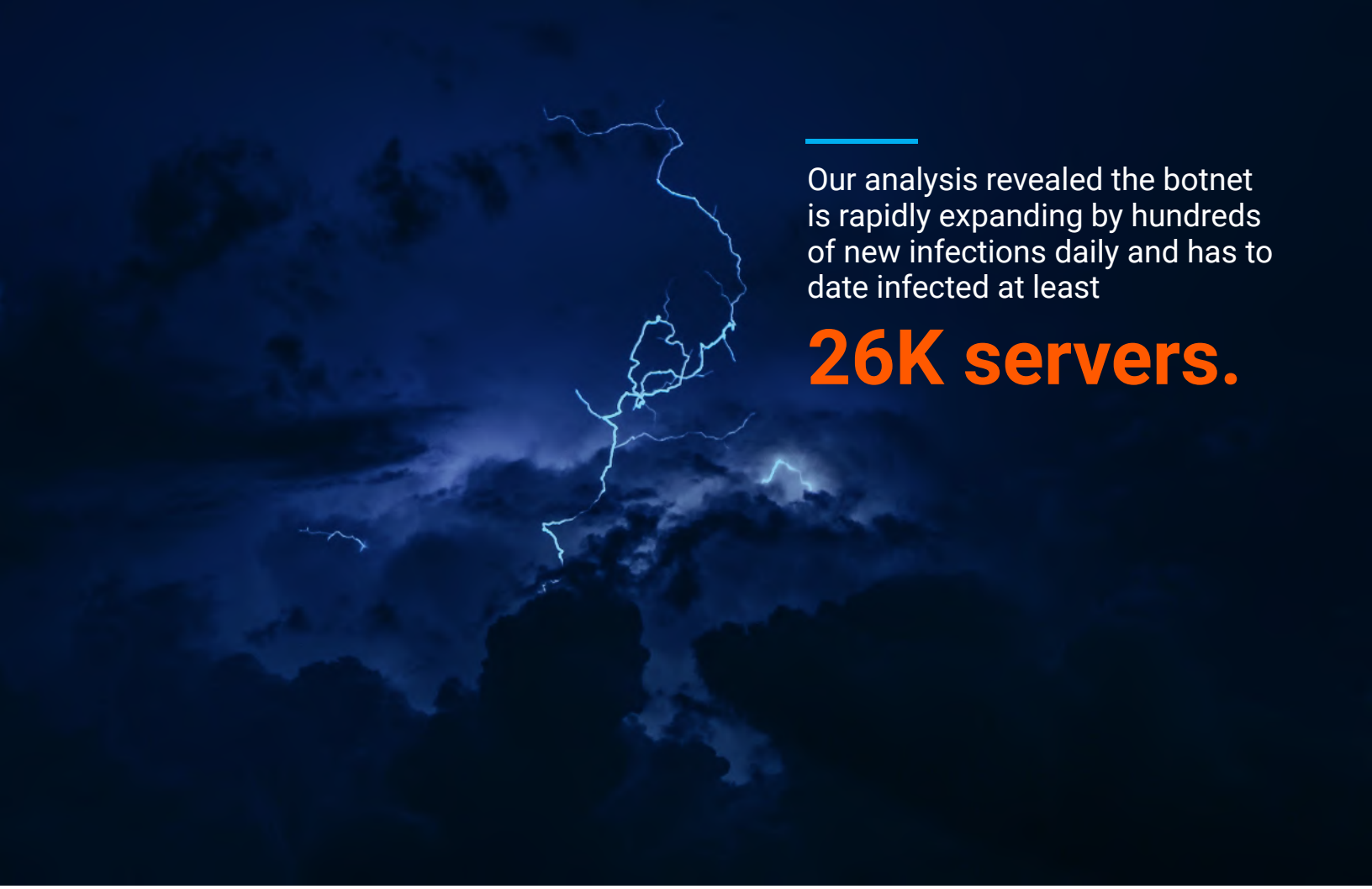
Sysrv-hello is a multi-architecture **Cryptojacking botnet that first emerged in late 2020**, and employs Golang malware compiled into both Linux and Windows payloads.

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.

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.



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

26K servers.

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.