KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | New Lightning Framework malware targets Linux systems

Tracker ID: TN0807 **Date:** 03/Aug/22 **Category:** Malware **Industry:** All **Region**: All

Background

A previously unknown "Lightning Framework" is targeting Linux systems and has subsequently been used to backdoor affected PCs through SSH and install rootkits to obscure the attackers' tracks. The Lightning Framework, popularly known as a "Swiss Army Knife," is a modular malware that can be upgraded using plugins. The framework supports both passive and active communication with the threat actor, as well as the ability to access SSH on an infected system and a polymorphic, configurable command and control configuration. Some of its components have yet to be discovered and evaluated.

The Lightning Framework has a simple design: a downloader component that downloads and installs the malware's numerous modules and plugins, including its core module, on infected Linux systems. The malware exploits typo squatting and masquerades as the Seahorse GNOME password and encryption key manager to prevent detection on infected systems. It retrieves its plugins and core modules after connecting to its command-and-control (C2) server via TCP connections and using C2 information saved in undetectable polymorphic encoded configuration files.

The malware uses the framework's core module (kkdmflush) to take orders from its C2 server and execute its plugins. To operate beneath the radar, the module has numerous capabilities and employs several methods for concealing artifacts. Other methods of concealment include timestamping harmful artifacts and masking its Process ID (PID) or any linked network ports with one of the rootkits it employs. It may also achieve persistence by including an elastic-search script in /etc/rc.d/init.d/ that runs on every system boot to activate the downloader module and reinfect the device.

Finally, this malware installs its SSH-based backdoor by launching an SSH server with one of the provided plugins (Linux.Plugin.Lightning.Sshd). Since this newly disclosed OpenSSH daemon includes hardcoded private and hosts keys, attackers can use their SSH keys to SSH into compromised consoles. "The Lightning Framework is an intriguing piece of malware since it is unusual to see such a massive framework designed for targeting Linux.“

MITRE ATT&CK Tactics

Persistence, Defense Evasion, Discovery, Command and Control.

Indicators of Compromise *

Please refer to the attached sheet for IOCs.

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | New Lightning Framework malware targets Linux systems

Tracker ID: TN0807 **Date:** 03/Aug/22 **Category:** Malware **Industry:** All **Region**: All

Detections **

Utilize the attached Sigma Rules for Lightning Framework Malware Detection in the network.

Recommendations

- Check with your existing AV/EDR vendor to validate the detection scope of identified samples.
- Validate the IOCs attached and implement the detection & prevention accordingly.
- Use reputed anti-virus solutions and internet security software packages on your connected devices, including PCs, laptops, and mobile devices.
- Monitor the beacon on the network level to block data exfiltration by malware or TAs.
- Ensure the vulnerable systems are updated with the latest security releases to safeguard them from threat actors.

References

- Ryan Robinson, Lightning Framework: New Undetected “Swiss Army Knife” Linux Malware, Intezer, 21st July 2022, External Link (www.intezer.com).
- Sergiu Gatlan, New ‘Lightning Framework’ Linux malware installs rootkits, backdoors, BleepingComputer, 21st July 2022, External Link (www.bleepingcomputer.com).

In case of a Security Incident, please report to IN-FM KPMG SOC.

For any query or feedback, feel free to reach us at IN-FM KPMG CTI.

KPMG in India Cyber Response Hotline : +91 9176 471 471

KPMG

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | New Lightning Framework malware targets Linux systems

Tracker ID: TN0807 **Date:** 03/Aug/22 **Category:** Malware **Industry:** All **Region**: All

*

SHA256 Hash
48f9471c20316b295704e6f8feb2196dd619799edec5835734fc24051f45c5b7
fd285c2fb4d42dde23590118dba016bf5b846625da3abdbe48773530a07bcd1e
ad16989a3ebf0b416681f8db31af098e02eabd25452f8d781383547ead395237

**

```
title: Lightning Framework File Path
status: experimental
description: Detects creation of files related to Lightning Framework.
author: Intezer
references:
  - https://www.intezer.com
logsource:
  product: linux
  category: file_create
detection:
  selection1:
    TargetFilename|startswith:
      - '/usr/lib64/seahorses/'
  selection2:
    TargetFilename|contains:
      - 'kbioset'
      - 'cpc'
      - 'kkdmflush'
      - 'soss'
      - 'sshod'
      - 'nethoogs'
      - 'iftoop'
      - 'iptraof'
  condition: selection1 and selection2
falsepositives:
  - Unknown.
```

```
title: Lightning Default C2 Communication
status: experimental
description: Detects communication to default local ip for Lightning Framework
author: Intezer
references:
  - https://intezer.com
logsource:
  category: firewall
detection:
  select_outgoing:
    dst_ip: 10.2.22.67
    dst_port: 33229
  condition: select_outgoing
falsepositives:
  - Unknown.
```