XAVIER BECERRA
Attorney General

State of California
DEPARTMENT OF JUSTICE

1300 I STREET, SUITE 125
P.O. BOX 944255
SACRAMENTO, CA 94244-2550

Public: (916) 445-9555
Telephone: (916) 210-7251
Facsimile: (916) 322-2368
E-Mail: Robert.Morgester@doj.ca.gov

May 3, 2018

Dear Custodian of Records:

The California Attorney General's Office, working with the California CyberSecurity Integration Center, is conducting an ongoing criminal investigation that involves one or more subscribers or other entities that is using your service.

As part of this investigation we are requesting the identity of the subscriber or other entity that is associated with the use of the attached Internet Protocol (IP) Address(es) on March 13, 2018, during the time period of 6:00AM - 12:00PM.

This preservation is requested pursuant to 18 U.S.C. § 2703(f) that the subscriber or entity identification associated with the use of the listed IP address(es) be preserved pending the issuance of a search warrant or other legal process seeking disclosure of such information.

What happened?

The listed IP addresses were logged as part of a Distributed Denial of Service (DDoS) attack. We believe the devices connected to the listed IP address(es) are infected by malicious software (malware) causing them to collectively receive and obey commands from a common command and control infrastructure. This activity suggests they are most likely part of a botnet. We also believe the subscriber or other entities associated with these devices were likely unaware of the activities that their devices were undertaking.

Subscriber notification is encouraged

You are encouraged to notify the subscriber or other entity that is associated with the use of the listed IP address(es). Notification, permitted pursuant to California Penal Code § 1546.2(d), is intended to reduce exposure to further malicious activity. If notification is not made and no remediation actions taken, the service users will most likely never know they are infected and their devices will continue to participate in DDoS attacks or other malicious activities.

Your notification to the subscriber or other entity of the suspected malware may also eliminate the need for our requested disclosures. Notification and remediation are the primary reasons for seeking the requested subscriber identification.

If you control one of the listed devices

The device will most likely contain malware. Our researchers would like to obtain copies of the malware used. Please contact [redacted]@doj.ca.gov for further information on the identification, preservation, and delivery of the malware. Your assistance will help in improving our abilities to deactivate botnets to reduce damage.

Device remediation

Removing a computer virus or spyware can be difficult without the help of malicious software removal tools. Some computer viruses and other unwanted software reinstall themselves after the viruses and spyware are detected and removed. For additional information please see:

> Security Tip (ST13-003) - Handling Destructive Malware
> https://www.us-cert.gov/ncas/tips/ST13-003

The California Attorney General's Office and the California CyberSecurity Integration Center are committed to containing the spread, operation, and impact of botnets while preserving California internet users' privacy.

If you have any questions concerning this request, please contact our office at [redacted]@doj.ca.gov or Michelle Williams at [redacted].

You may also contact the California Cybersecurity Integration Center directly at CalCSIC@caloes.ca.gov or telephone 1-833-REPORT1.

Thank you for your assistance in this matter.

Sincerely,

Robert Morgester
Senior Assistant Attorney General - eCrime Unit
Office of the Attorney General

For XAVIER BECERRA
Attorney General

enclosures
RM/tjy