Palo Alto Networks Uncovers Backdoor In Android Devices Sold by Coolpad

December 17, 2014

"CoolReaper" potentially affects 24 Android phone models and over 10 million users

SANTA CLARA, Calif., Dec. 17, 2014 /PRNewswire/ -- Palo Alto Networks® (NYSE: PANW), the leader in enterprise security, today revealed details of a backdoor contained in millions of Android-based mobile devices sold by Coolpad, one of the world's largest smartphone manufacturers based in China. The backdoor, named "CoolReaper," exposes users to potential malicious activity and appears to have been installed and maintained by Coolpad despite objections from customers.

It is common for device manufacturers to install software on top of Google's Android mobile operating system to provide additional functionality and customization to Android devices, and some mobile carriers install applications that gather data on device performance. Following detailed analysis by Unit 42, the Palo Alto Networks threat intelligence team, CoolReaper appears to operate well beyond the collection of basic usage data, acting as a true backdoor into Coolpad devices. Coolpad also appears to have modified a version of the Android OS to make it much more difficult for antivirus programs to detect the backdoor.

CoolReaper, which was discovered by Palo Alto Networks researcher Claud Xiao, has been identified on 24 phone models sold by Coolpad, meaning a potential impact to over 10 million users based on publicly-obtainable Coolpad sales information.

QUOTE:

- "We expect Android manufacturers to pre-install software onto devices that provide features and keep their applications up to date. But the CoolReaper backdoor detailed in this report goes well beyond what users might expect, giving Coolpad complete control over the affected devices, hiding the software from antivirus programs, and leaving users unprotected from malicious attackers. We urge the millions of Coolpad users who may be impacted by CoolReaper to inspect their devices for presence of the backdoor and to take measures to protect their data."
  – Ryan Olson, Intelligence Director, Unit 42, Palo Alto Networks

Background and effects of CoolReaper
The full findings related to CoolReaper were published today in "CoolReaper: The Coolpad Backdoor," a new report from Unit 42 written by Claud Xiao and Ryan Olson. In the report, Palo Alto Networks has also published a list of files to check for in Coolpad devices that may indicate the presence of the CoolReaper backdoor.

As observed by researchers, CoolReaper can perform each of the following tasks, any of which might put sensitive user or corporate data at risk. In addition, malicious attackers could exploit a vulnerability found in CoolReaper's back-end control system.

CoolReaper can:

- Download, install, or activate any Android application without user consent or notification.
- Clear user data, uninstall existing applications, or disable system applications.
- Notify users of a fake over-the-air (OTA) update that doesn't update the device, but installs unwanted applications.
- Send or insert arbitrary SMS or MMS messages into the phone.
- Dial arbitrary phone numbers.
- Upload information about the device, its location, application usage, calling and SMS history to a Coolpad server.

Coolpad acknowledgment
Unit 42 began observing what came to be known as CoolReaper following numerous complaints from Coolpad customers in China posted to Internet message boards. In November, a researcher working with Wooyun.org identified a vulnerability in the back-end control system for CoolReaper, which made clear how Coolpad itself controls the backdoor in the software. In addition, a Chinese news site, Aqniu.com, reported some details of the backdoor's existence and its abuses in an article published November 20, 2014.

As of December 17, 2014, Coolpad did not respond to multiple requests for assistance by Palo Alto Networks. Google's Android Security Team also has been provided with the data contained in the report.

Protecting users
All known samples of CoolReaper have been marked as malicious in WildFire™, a key component of the Palo Alto Networks Threat Intelligence Cloud that helps identify threats from applications by executing them in a virtual environment, and automatically sharing them with Palo Alto Networks GlobalProtect to identify affected devices.

In addition, all known Command & Control URLs used by CoolReaper are identified as malicious in Palo Alto Networks Threat Prevention products, allowing customers to prevent data exfiltration, even if the Command & Control servers or URLs change.

Palo Alto Networks has also made signatures available to detect and block malicious CoolReaper Command & Control traffic, which are effective even if the Command & Control server changes to a new location.

The CoolReaper findings further reinforce the need for comprehensive mobile security using a combination of traffic inspection along with threat intelligence for both the detection and prevention of dangerous applications. GlobalProtect from Palo Alto Networks provides organizations with protection against advanced cyber threats, including the ability to continuously analyze mobile content for covert or malicious activity.

To learn more

- **Download CoolReaper: The Coolpad Backdoor: https://www.paloaltonetworks.com/resources/research/cool-reaper.html**
- **Visit the Unit 42 Research Center for new research, updates and confirmed speaking appearances: https://www.paloaltonetworks.com/threat-research.html**
- **Subscribe to regular research and analysis from the Unit 42 blog: http://researchcenter.paloaltonetworks.com/unit42/**
- **Learn more about Palo Alto Networks enterprise security platform and how it provides protections for CoolReaper: https://www.paloaltonetworks.com/products/platforms.html**
- **Meet Unit 42 team leads at Ignite 2015, where your toughest security challenges get solved. Register now to join Palo Alto Networks in Las Vegas, March 30-April 1, 2015.**

About Unit 42
Unit 42, the Palo Alto Networks threat intelligence team, is made up of accomplished cybersecurity researchers and industry experts. Unit 42 gathers, researches and analyzes up-to-the-minute threat intelligence, sharing insights with Palo Alto Networks customers, partners and the broader community to better protect organizations. Unit 42 team leads regularly appear at industry conferences throughout the world.

About Palo Alto Networks
Palo Alto Networks is leading a new era in cybersecurity by protecting thousands of enterprise, government, and service provider networks from cyber threats. Unlike fragmented legacy products, our security platform safely enables business operations and delivers protection based on what matters most in today's dynamic computing environments: applications, users, and content. Find out more at www.paloaltonetworks.com.

Logo - http://photos.prnewswire.com/prnh/20130508/SF04701LOGO

To view the original version on PR Newswire, visit:http://www.prnewswire.com/news-releases/palo-alto-networks-uncovers-backdoor-in-android-devices-sold-by-coolpad-300010972.html

SOURCE Palo Alto Networks

Jennifer Jasper-Smith, Head of Corporate Communications, Palo Alto Networks, 408-638-3280, jjsmith@paloaltonetworks.com; or Tim Whitman, Voce Communications, 617-721-5994, twhitman@vocecomm.com