Palo Alto Networks reveals discovery of unprecedented iOS and OS X malware

recognition|pr

Research spotlights new malware family distributed through trojanised and repackaged Apple OS applications

Palo Alto Networks® (NYSE: PANW), the leader in enterprise security, has announced discovery of a new family of Apple OS X and iOS malware exhibiting characteristics unseen in any previously documented threats targeting Apple platforms. This new family, dubbed WireLurker, marks a new era in malware across Apple's desktop and mobile platforms, representing a potential threat to businesses, governments and Apple customers worldwide.

Among its defining characteristics, WireLurker represents:

- the first known malware family that can infect installed iOS applications similar to how a traditional virus would
- the first in-the-wild malware family that can install third-party applications on non-jailbroken iOS devices through enterprise provisioning
- only the second known malware family that attacks iOS devices through OS X via USB
- the first malware family to automate generation of malicious iOS applications through binary file replacement.

WireLurker malware was discovered by Claud Xiao of Unit 42, the Palo Alto Networks threat intelligence team, and detailed in a report, "WireLurker: A New Era in OS X and iOS Malware."

Following its initial observation in the wild in June by a developer at Tencent, Palo Alto Networks researchers have determined WireLurker's potential impact, assessed the methods available to prevent, detect, contain and remediate the threat, and detailed the protections available for Palo Alto Networks customers.

Palo Alto Networks has released signatures to detect all WireLurker Command & Control communication traffic. It is recommended that customers using OS X or iOS devices deploy a strict policy for blocking WireLurker traffic using the Palo Alto Networks enterprise security platform. A full list of system recommendations, remediation techniques and best practices is included in the WireLurker report.

QUOTE

- "WireLurker is unlike anything we've ever seen in terms of Apple iOS and OS X malware. The techniques in use suggest that bad actors are getting more sophisticated when it comes to exploiting some of the world's best-known desktop and mobile platforms. As such we have provided full protection to Palo Alto Networks customers and published a detailed report so others can assess the risk and take appropriate measures to protect themselves."

– Ryan Olson, Intelligence Director, Unit 42, Palo Alto Networks

To learn more

- Download WireLurker: A New Era in OS X and iOS Malware
- Visit Unit 42, the Palo Alto Networks threat intelligence team, for new research, updates and confirmed speaking appearances
- Read regular research and analysis on the Unit 42 blog

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.