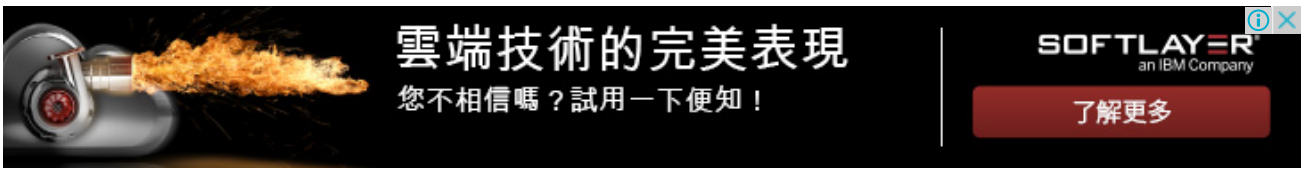


Mac OS X Malware at All-Time High, Research Shows

By GlobeNewswire • on October 14, 2015 10:03 am • in Technology

WALTHAM, Mass., Oct. 14, 2015 (GLOBE NEWSWIRE) — Mac OS X malware is at an all-time high, according to a new report from the Bit9® + Carbon Black® Threat Research Team.

A 10-week analysis conducted by Bit9 + Carbon Black demonstrated the unprecedented growth in OS X malware. In 2015 alone, the number of OS X malware samples has been five times greater than in 2010, 2011, 2012, 2013 and 2014 combined, the research found.

The Bit9 + Carbon Black Threat Research Team collected more than 1,400 unique OS X malware samples. The samples were aggregated from the team's independent research efforts, open sources, experience from incident response engagements involving OS X, peer research, black lists, and a contagio malware dump, among other sources.

"Macs have been largely ignored by malware, until recently," said Mike Sconzo, Bit9 + Carbon Black's senior threat researcher. "Evidence of a more malicious OS X marketplace is clearly compounding and we

confidently expect Mac OS X malware attacks to accelerate in the coming months."

For its analysis, the Bit9 + Carbon Black Threat Research Team utilized a custom-built sandbox to quickly identify common actions performed by malware, such as file creations and network communications. This enabled the team to look at command-and-control infrastructure as well as artifacts left as part of the malware execution.

As the team tracked the malware, it found some interesting behavior. Most notably:

- Typical UNIX persistence mechanisms were not frequently seen in the OS X malware analyzed. For example, the team's analysis found that mechanisms such as adding cron jobs and "trojaning" startup locations such as rc.common weren't typically used; instead, malware authors are choosing to use Mac OS X-specific mechanisms.
- Malware authors are seizing the opportunity to strike on the OS X platform, meaning there's more malware out there but the result of this transition has been "less sophistication" in the malware.
- The Bit9 + Carbon Black Threat Research Team identified that the vast majority of OS X malware leveraged one of just seven persistence techniques to remain active on a system.

The report presented several detection mechanisms that both enterprise users and consumers can use to better understand OS X malware and its behavior. Download the full report here.

"Assuming their machines were 'safe' from malware and cyber attacks, many enterprises and consumers have failed to implement the same safeguards and controls on OS X devices as they have for Windows machines," Sconzo said. "As threats against OS X have increased, this security gap has left many organizations and consumers exposed and unable to identify or stop infections."

About Bit9 + Carbon Black

Bit9 + Carbon Black is the market leader in Next-Generation Endpoint

The ValueWalk Investor Series

Get all 5 of ValueWalk's Famous investor profiles for free: Buffett, Munger, Schloss, Klarman and Dalio.

GET ALL 5 EBOOKS FREE

Send us your tips at tips(at)valuewalk.com

VectorVest Click Here

VectorVest Click Here

VectorVest Click Here

VectorVest Click Here

Are you Vanguarding® your clients' portfolios?

Start Vanguarding now

© 2015 The Vanguard Group, Inc. All rights reserved. U.S. Patent Nos. 6,879,964; 7,337,138; 7,720,749; 7,925,573; 8,090,646; and 8,417,623. Vanguard Marketing Corporation, Distributor. Obtain prospectus

Van

Security. We have sold more licenses, have more experience, and more customers than any other NGES company because our solution is the most effective way to prevent, detect and respond to advanced threats that target users, servers, and fixed-function devices. That's why more than 60 MSSP and IR leaders, including Dell SecureWorks, EY, Optiv and Solutionary, have chosen our technology as a key component of their security offerings, and 25 of the Fortune 100 rely on us as a critical element of their advanced threat defense and compliance strategies. By the end of 2015, we expect to achieve $70M+ in annual revenue, 70 percent growth, 7 million+ software licenses sold, and almost 2,000 customers worldwide. We were voted Best Endpoint Protection by security professionals in the SANS Institute's Best of 2014 Awards, and a 2015 SANS survey found that 68 percent of IR professionals are using or evaluating Carbon Black.

Bit9 and Carbon Black are registered trademarks of Bit9, Inc. All other company or product names may be the trademarks of their respective owners.

CONTACT: Kevin Flanagan
Bit9 + Carbon Black
+1 781-856-2589
kflanagan@bit9.com

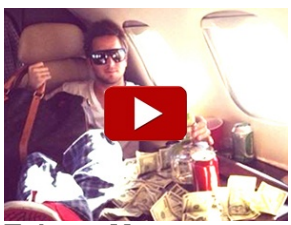
Tags: Max OS X

Written by **GlobeNewswire**

GlobeNewswire, a NASDAQ OMX company, is one of the world's largest newswire distribution networks, specializing in the delivery of corporate press releases financial disclosures and multimedia content to the media, investment community, individual investors and the general public.

Ads by Adblade

More offers and articles



Taiwan Man Exposes A Secret To Earn TWD 138,200/Week From Home

Can you have 20/20 Vision again without surgery?

These are the most toxic places on earth. You'll never believe #5!

Man Makes TWD 27,850/Day at Home! Find Out How!

These 12 super foods speed up your weight loss and can potentially help melt fat!

Single Mom Earns TWD 410,500/Month From Her Laptop. Find Out How

A Seduction Technique Women Can't Resist

Weight Loss System Melts Fat Like Butter

The Way To Capture His Heart And Keep Him

The Simplest Way To Back Up Your Computer

Natural Trick For Restoring Hair Color

'Fat Hormone' Stops Women From Losing Weight

3 Simple Steps To Get Any Woman To Obsess Over You

She Can't Resist A Man Who Does This 1 Thing...

0 Comments ValueWalk 1 Login

Recommend Share Sort by Newest

Start the discussion…

Be the first to comment.

Subscribe Add Disqus to your site Privacy DISQUS

Copyright © 2015 ValueWalk - Privacy Policy Developed by ValueWalk Team