MAC ENDPOINTS MOVE INTO THE ENTERPRISE – AND INTO THE CROSSHAIRS OF HACKERS

Combat the Growing Threat to Macs

After years of believing the Mac® was immune to attack, the world is waking up to the fact that it is indeed vulnerable to malware and exploits. Recent growth in corporate use of Macs has made the platform increasingly interesting to hackers: high-value users (such as executives and road warriors) and high-value content (including designs and engineering specs) are inviting a growing number of hacking attempts. We can't afford to go through the long learning curve we saw with Windows® endpoints, trying a variety of approaches that ultimately fail. Instead, we must take a fresh approach to protecting Macs, and employ better, more effective ways of protecting against both malware and exploits. It's important to understand what a multi-method prevention approach can do for Mac endpoint security. When built on a next-generation security platform, this approach can provide full context and intelligence, enabling the security team to address the unique requirements of the Mac while providing protection for all endpoints.

Trends Causing Security Professionals to Take Notice

For years, the relatively few Mac users in the corporate environment believed themselves immune to cyberattacks, since the Mac was not targeted by viruses. However, viruses are only a fraction of the threats, and today, Mac endpoints are vulnerable to various types of malware and exploits.

Corporate security officers are noticing two trends. The first is the increasing incorporation of Macs into the corporate environment (91 percent of enterprise organizations use Macs, and 2016 saw a 74 percent increase in Mac adoption[1]). The second is the increase in Mac attacks.

Macs make interesting targets. Many hold high-value content, given their use by creative, marketing, engineering and design teams. They're also the platform of choice for many high-value users, such as executives and road warriors. With Macs entering the corporate mainstream, security teams are on alert to reduce the possibility of attacks or breaches. Executive and sales team downtime, not to mention loss of intellectual property, could do serious harm to an enterprise.

No Longer a Safe Haven

The landscape for Mac threats has changed dramatically in recent years. Until 2012, attacks were few and far between, but that changed when Flashback (which exploited a Java® vulnerability) affected up to one million users. The number of attacks has crept up each year, mirroring the increasing prevalence of Macs in the corporate world. We saw more malware attacks in 2015 than every other year since 2010 combined. One study showed 1,400 new malware samples in just 10 weeks.[2] Many were designed to run commands, exfiltrate data and download malware. The number of malware samples from the first quarter of 2017 maintains the pace of acceleration, with as many samples as were found in all of 2016.[3]

High-profile Mac breaches are not only seen in the media – they play an increasing role in the day-to-day work of enterprise security teams. Several troubling examples are:

- **KeRanger –** Ransomware written specifically for the Mac.
- **XAgent –** Downloaded by the Komplex Trojan; a backdoor that can be customized to log passwords, detect system configurations, take screenshots and exfiltrate files.
- **Mac OS Dynamic Linker Exploitation –** Malware that exploits a privilege escalation flaw to infect Macs with adware and junkware.
- **iOS Trifecta–** Tricks the Mac into silently running unauthorized system code to get kernel-level access to the device.

The increasing frequency and destructiveness of the attacks is now on the radars of many enterprise security teams that, in the past, worried less about Macs than other systems.

Stuck in the Past – Why Legacy Approaches Aren't Working

The legacy approach to combating malware has been through antivirus or anti-malware software. Third-party AV vendors have released products targeted at Macs, but with some of the same weaknesses as Windows AV products, along with fewer capabilities that would normally be built up over time.

Legacy AV Weaknesses

AV is signature-based, so it is only effective against a portion of known malware, and ineffective against zero-day threats. Signature-based solutions require constant updates, but hackers can make minor changes that render updates obsolete. AV solutions also create significant drag on system performance. In addition, some security products cause issues in and of themselves, as seen with a recently publicized vulnerability caused by an antivirus vendor. An exploitable vulnerability in one of its libraries allowed remote code execution as root, effectively giving full privileged access to the system.[4]

Gatekeeper Issues

Apple® has its own approach: a security feature of Mac OS called Gatekeeper. This program attempts to stop malware by ensuring every application downloaded has been approved by Apple or comes from a developer with a preapproved developer certificate. The check is done before applications are allowed to run. Unfortunately, Gatekeeper itself has been shown to have weaknesses, including exploitable vulnerabilities. For example, a mechanism in Gatekeeper was discovered last year that allowed hackers to infect software that had previously been approved by Apple, thus bypassing the security controls.

Limited Effectiveness Against Exploits

A further issue with legacy and even modern ("next-gen") AV products on Macs is their limited effectiveness against exploits, ransomware and advanced threats, many of which come from known (and often longstanding, but unpatched) vulnerabilities. In fact, the CVE (Common Vulnerabilities and Exposures) system lists almost 2,000 known Mac vulnerabilities.5 Legacy antivirus and anti-malware products fall short when it comes to protecting against exploits.

Why a Multi-Method Prevention Approach Is Effective for Malware Prevention

It is not enough to simply implement an AV system and expect it to protect against the many types of increasingly sophisticated Mac malware. Some malware has been seen previously, so prevention solutions need to immediately recognize and prevent it. Other malware has not been seen before, so solutions need to quickly determine if it is actually malicious. Still other malware is executed from launching legitimate processes, such as script engines and command shells, but uses these processes to carry out malicious activities.

To effectively prevent malware, any approach must employ multiple methods to maximize protection. It should proactively reduce the attack surface of the endpoint, and accurately protect against malware. This means the approach needs to overcome the deficiencies of AV and built-in security safeguards like Gatekeeper. Additional advantages come when the solution is built on a security platform that brings together disparate silos of information to create a clearer picture of the security landscape.

Integration – The Key to Multi-Method Malware Prevention

Maximizing coverage against known and unknown malware calls for tight integration with threat intelligence to identify and stop known threats such as the XAgent or Komplex malware mentioned above, which relied on code previously deemed malicious. A multi-method prevention approach will rapidly analyze an executable and, if the

executable is found to be malicious, automatically terminate it as well as take other action to prevent future execution. If an executable file is unknown, it can be submitted to the threat intelligence solution for complete inspection and analysis.

A multi-method prevention approach can also enhance Gatekeeper security features by extending its functionality to child processes that can be blocked or selectively allowed, preventing hackers from bypassing the digital signature verification mechanism.

Don't Neglect Backdoors: Multi-Method Exploit Prevention

Many attacks start with an exploit delivered as a file from a website or email. When the recipient opens the file using an application, a vulnerability in the application or operating system is exploited and a set of malicious instructions is carried out. Since this appears, on the surface, to be normal application behavior, an antivirus system will not detect it. The application can also easily bypass whitelists because it is sanctioned.

Most exploits use a known set of techniques that change infrequently. Common techniques include memory corruption, which attempts to manipulate the normal memory management mechanisms for the application opening the file; logic flaws (such as dylib hijacking, which manipulates an application to load dynamic libraries different from those it normally loads); and kernel-level privilege escalation, which affords a process elevated privileges. A multi-method prevention approach will focus on techniques to effectively block exploit-based attacks.

No More Security Silos: Leverage the Power of a Platform

Most organizations employ a variety of products in their security program. However, these products are often implemented in silos and don't communicate effectively, leading to incomplete information and increased risk. Overall security benefits greatly from real-time sharing of information to enrich knowledge and the ability to prevent threats.

A platform approach to Mac endpoint protection will bring together intelligence to automatically block malware first encountered elsewhere, including on firewalls, SaaS applications and endpoints. This enables users to leverage investments in network, cloud and endpoint security.

Palo Alto Networks Traps

Traps™ advanced endpoint protection replaces legacy AV with a multi-method prevention approach that blocks malware and exploits, both known and unknown, before they compromise endpoints such as laptops, desktops and servers. Traps enables you to manage both Windows and Mac endpoints, reducing administrative overhead and maximizing operational efficiency.

Multi-Method Malware Coverage

Specifically designed to maximize coverage against known and unknown malware, Traps is tightly integrated with WildFire™ cloud-based threat analysis service.

- Traps rapidly assesses known malware, such as XAgent and Komplex, and takes action. It can automatically terminate an executable, reprogram itself to prevent future execution of that executable, and optionally quarantine the file.
- For unknown malware, Traps performs local analysis and optionally submits the file to WildFire for complete inspection and analysis. WildFire delivers a verdict, in as few as five minutes, through a combination of dynamic and static analysis, innovative machine learning techniques, and a groundbreaking bare metal analysis environment to detect and prevent even the most evasive threats.
- Traps extends Gatekeeper functionality, allowing customers to block child processes or allow only those with signature levels that match or exceed their parent process.

Multi-method exploit protection

Traps uses multiple methods to detect and deflect Mac exploits. It recognizes privilege techniques, as used in the Mac OS Dynamic Linker Exploitation mentioned above, and blocks attacks targeting the operating system. Similarly, it detects and blocks attempts to silently run unauthorized system code to get kernel-level access, as seen in the iOS Trifectaexploit discussed previously. With exploits such as dylib hijacking, Traps likewise recognizes this technique and prevents it from being carried out.

The Traps approach produces several benefits:

- Protects unpatched applications and operating systems from exploit-based attacks
- Eliminates the urgency to patch applications immediately
- Protects against zero-day exploits

This effectively immunizes endpoints, safeguarding them against exploits that have not even been created yet.

Built on a Platform

Traps is an integral component of the Palo Alto Networks® Next-Generation Security Platform, designed for comprehensive security and information sharing. Even customers who deploy Traps in environments that include no other components of the Next-Generation Security Platform still receive access to threat intelligence collected by WildFire, in part crowdsourced from Palo Alto Networks global community of customers. Traps uses this threat intelligence to automatically prevent malware first encountered elsewhere, including on other customers' firewalls, SaaS applications and endpoints. This effectively enables Traps customers to leverage the investments other customers have made in their network, cloud and endpoint security products from Palo Alto Networks.

Customers who deploy Traps as part of a broader Palo Alto Networks Next-Generation Security Platform see further benefits: in addition to preventing endpoint attacks, Traps provides the ability to upload logs to Panorama™ network security management to correlate endpoint and network security events for increased visibility and automated actions.

Another important benefit is an increase in operational efficiency. Traps presents a single pane of glass through which to manage both Windows and Mac endpoints.

The Big Picture: Traps Delivers Effective Mac Protection

You need to protect your entire organization, and this is best done through a comprehensive approach that protects both Mac and Windows endpoints. Where legacy endpoint security products fall short, Traps was specifically designed to prevent endpoint cyber breaches by preemptively blocking known and unknown threats. Only Traps delivers a multi-method prevention approach, continuously learning, automatically converting threat intelligence into prevention, and providing effective endpoint protection against malware and exploits.

Learn More

Learn how Traps can play an integral role in protecting your environment. Read about Traps online or download the datasheet. For a comprehensive overview of the Traps multi-method approach, watch our lightboard video, request a Traps demo and then take Traps for a test drive.

[1] 2016 Survey: Managing Apple Devices in the Enterprise. JAMF Feb 2017. Retrieved from https://www.jamf.com/resources/2016-survey-managing-apple-devices-in-the-enterprise

[2] Tim Greene. Think Apple OS X is below the malware radar? Think again. Network World, Oct. 2015. Retrieved from http://www.cio.com/article/2993474/security/think-apple-os-x-is-below-the-malware-radar-think-again.html

[3] Jai Vijayan. Ransomware, Mac Malware Dominate Q1 Threat Landscape. Dark Reading, April 2017. Retrieved from http://www.darkreading.com/endpoint/ransomware-mac-malware-dominate-q1-threat-landscape/d/d-id/1328640

[4] Roi Perez. Mac antivirus software from ESET has RCE vulnerability – patch now! SC Magazine, Feb. 2017. Retrieved from https://www.scmagazineuk.com/mac-antivirus-software-from-eset-has-rce-vulnerability--patch-now/article/640675

[5] CVE Details – the ultimate security vulnerability data source. Retrieved from https://www.cvedetails.com/product/156/Apple-Mac-Os-X.html?vendor_id=49

4401 Great America Parkway
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com