cybereason

Lab Analysis

Mac OS X:

Attackers Don't Discriminate

Senior security researcher,
Amit Serper, reveals the latest Mac OS X security threats,
including ransomware, malware and fileless malware.

www.cybereason.com

There's a perception that OS X is impenetrable, especially when compared to Windows. This assumption, however, is wrong. Fewer threats may target OS X, but this doesn't mean Macs are immune to attacks.

Adversaries haven't written many malware programs for OS X since the platform's market share was so low. Compromising Windows machines offered far greater windfalls. But this is changing as more people and companies use Macs. A larger user base provides attackers with an incentive to hack Apple computers. In fact, security research has shown that attackers are directing more of their efforts at compromising OS X as the platform's market share increases.

A Variety of Malware is Targeting Mac OS X

A recent example is Palo Alto Networks' discovery of the first functioning ransomware that attacks Mac computers. Called "KeRanger," the malware infected Transmission, an open-source BitTorrent client, and was programmed to encrypt files on a person's computer three days after the initial infection. To retrieve their files, users have to pay a bitcoin ransom. The BitTorrent client was signed with a digital certificate from a legitimate Apple developer, allowing KeRanger to circumvent Gatekeeper, a tool that's built-in to OS X and prevents unsigned code from running. If the malware had been unsigned, there would have been a few opportunities to prevent it from executing.

Macs can be configured to not run programs without a certificate, a common procedure at many companies. Additionally, if a program lacks a certificate, a message appears alerting users that the application is unsigned and gives them the option not to run it. Having a certificate made the program seem legitimate. Fortunately for Mac users, the fallout from KeRanger appears to be minimal with few users having their files encrypted, according to media reports. However, this doesn't make them safe from future attacks.

Other research has revealed that OS X is vulnerable to dynamic library hijacking. Previously, these types of attacks were believed to only affect Windows. AlienVault

researchers examined a piece of malware called OceanLotus that targeted OS X. The malware, which was discovered by Chinese security company Qihoo 360, was disguised as an application bundle for an Adobe Flash update. Like the ransomware, OceanLotus was signed with a certificate, allowing it to bypass security measures.

AlienVault also noted that the malware's creators designed and programmed it for OS X, meaning, it was not ported from a Windows version. Given the details the attackers included to make the malware seem authentic, users and security analysts probably had no idea that they were installing a bogus program. There are also zero-day attacks that exploit OS X and iOS 7, according to Hacking Team emails that emerged after the company was breached last July. Not to stoke security fears, but there may be other zero-day attacks as well.

Fileless Malware Attacks Turn Scripting Languages into Mac Attack Vectors

But attackers may not need malware to carry out an attack on OS X. They just need an initial penetration vector, like an exploit or a phishing email with a malicious payload, that allows them to run code on the machine. In theory, they can use the programming languages that are built-in to a Mac computer to carry out malicious activities. Python, Perl and Ruby on Rails have access to many internal resources and can perform several functions, including code execution. Even AppleScript has the potential to be used against a Mac computer since it can access resources on virtually any piece of Mac software and, if enabled, run commands on remote machines, like Windows Management Instrumentation (WMI) in Windows.

Adversaries could damage a company without ever dropping a file on a Mac. And they wouldn't have to exert much effort to carry out this type of attack. First, they need to take over a Mac to gain the ability to execute commands. Several vectors are available to attackers looking to infiltrate a machine. Attackers could send out

phishing emails, leverage exploits in other programs, even use lateral movement to compromise other machines assuming they've already taken over another Mac in the organization. Or, in the case of KeRanger, attackers could purchase a developer's certificate and use social engineering to get victims to download the malicious but signed application. Finally, to execute the attack, they just have to write a script in Python and call the Python interpreter with the script as a command line argument.

Since Python is a legitimate scripting language, a program built with it wouldn't look suspicious to security analysts and most antivirus programs probably won't issue an alert. The Mac's task manager would only show that a Python program was running, not that it was being used for malicious purposes. Behavioral analysis would provide companies with context around what that program was doing as well as what other activities were occurring across the organization's entire IT environment.

These types of threats, called fileless malware attacks, are frequently used on Windows machines and typically involve hackers using tools like PowerShell and WMI for malicious activities. In these attacks, which Cybereason's research team has analyzed, hackers essentially turn a company's infrastructure against the organization. And now that Cybereason runs on Macs, we're seeing how frequently these attacks occur on Apple machines.

Deleting Programming Languages Won't Keep Mac OS X Users Safe

Companies can take a few steps to try to protect themselves, but, truthfully, there isn't much they can do to stop motivated attackers. Macs that use Ruby, Perl, AppleScript and Python aren't more vulnerable to attacks and a company isn't less secure. A majority of the time, these languages are used for legitimate activities, like running updating scripts or individual software updates that occur as part of Apple's regular update mechanism.

Keeping this in mind, administrators who think removing programming languages from a user's Mac will solve their security problem should proceed with caution.

They could delete scripting languages from the Macs of employees who don't write code, but this move could have unintended consequences that keep people from doing their jobs, like preventing software from updating because Python is needed.

Having full visibility into an IT environment helps tremendously, but given the complexity of enterprise networks, achieving that perspective is extremely challenging. Reviewing security logs for communications to strange domain names could help analysts spot malicious behavior, but again, this plan is impractical in a company with hundred or thousands of Macs. Analysts don't have the time to review all these logs and analyze the data for abnormalities.

Beware of Flash Updates and Autorun

To guard against malware-based attacks, administrators should instruct their users to consult with them before downloading Flash updates or installing Flash plug-ins. Malware is often concealed as a Flash update or plug-in, as seen with the OceanLotus threat. Users are probably unaware that they could accidentally download malware and don't know how to check to make sure that a program was actually updated. Administrators should also check the autorun functions on a Mac, which are called launch agents, launch daemons, log-in items and startup items. This will ensure that malicious programs are not automatically starting when users boot their machines.

Mac OS X is vulnerable like any other computer system. Attackers don't discriminate against operating systems and fileless malware attacks, traditional malware and other threats pose dangers to both Macs and PCs.

About the Author

Amit Serper

Lead Linux and Mac OS X Security Researcher
Cybereason

Follow Amit on Twitter: @0xAmit

At Cybereason, Amit leads Mac OS X and Linux security research. He specializes in low-level, vulnerability and kernel research, malware analysis and reverse engineering. He also has extensive experience studying attack simulations on large scale networks and researching undocumented OS resources and APIs.

Prior to joining Cybereason, Amit spent nine years leading security projects for the Israeli government, specifically in embedded system security.

cybereason

Cybereason was founded in 2012 by a team of ex-military cyber security experts to revolutionize detection and response to cyber attacks. The Cybereason Malop Hunting Engine identifies signature and non-signature based attacks using big data, behavioral analytics, and machine learning. The Incident Response console provides security teams with an at-your-fingertip view of the complete attack story, including the attack's timeline, root cause, adversarial activity and tools, inbound and outbound communication used by the hackers, as well as affected endpoints and users. This eliminates the need for manual investigation and radically reduces response time for security teams. The platform is available as an on premise solution or a cloud-based service. Cybereason is privately held and headquartered in Boston, MA with offices in Tel Aviv, Israel.