E-Guide

Proactive security measures: How to prevent malware attacks
One constant that all IT departments can always count on is a new type of threat entering their industry. With the current use of mobile devices, social media and cloud services, malware is finding new ways to enter and threaten companies in a completely different way. This expert E-Guide discusses how to proactively secure your enterprise and the necessity to improve and update your antimalware strategy.

New Malware threats require new antimalware protection strategy

By Lisa Phifer

While IT continues to fight increasingly clever attacks against on-site enterprise infrastructure, new malware is taking aim at lower-hanging fruit: under-secured smartphones, mobile applications, social media, and other cloud services. As workers make more extensive use of such perimeter-less platforms, they create rich targets that require new antimalware protection strategies to mitigate these multifaceted new malware threats.

Enterprises can defend themselves by understanding these new malware vectors, enforcing application policies, implementing new device resident and cloud-based antimalware techniques, and leveraging other security tools.

Following the money

Far more than fame or hacktivism, the malware industry is driven by financial gain and drawn to low-cost, high-profit attacks. This has been repeatedly proven, as malware migrated from floppy to USB drives, email to Web, browser to PDF, abandoning old haunts to seek out more vulnerable monocultures.

“As technology trends such as Web and mobile come to the forefront, that’s where malware refocuses,” says Intrepidus Group Principal Consultant Zach Lanier. “Mobile convergence creates an interesting opportunity: one device that delivers [non-stop] network, Web, media, and application access.”
Because there are only so many players -- Apple, Google, the WebKit browser engine -- a single bug can be leveraged to attack millions of users."

And criminals needn’t look far to find beefy targets. Google activates 700,000 new Android smartphones and tablets per day. According to Flurry Analytics, 6.8 million Apple (iOS) and Android devices were enabled on Christmas Day alone. Facebook now reaches over 800 million users, half-active on any given day. Popular Web 2.0 sites like YouTube, Twitter, and WordPress average 450, 200, and 100 million visitors per day, respectively. Google Apps has 40 million accounts, including 4 million businesses.

In fact, cloud services like Google Apps "are a very large data repository for a wide range of companies and people," Cisco Senior Threat Researcher Mary Landesman says. “Rather than trying to penetrate one [business] at a time, cloud is an avenue of attack to penetrate many. Increased return on investment means making money with less effort – cloud attacks are a natural progression of that."

**Looking for loopholes: Mobile malware and social media**

But size and popularity are not the only draws. Co-mingled personal and business use, real-time communication, bring-your-own consumerization, and little or no IT control combine to make any discovered vulnerabilities more readily exploitable.

Lookout Principal Engineer Tim Wyatt has examined thousands of mobile applications from Apple’s AppStore, Google’s Android Market, and unofficial markets. "We’re still seeing the start-up phase of smartphone malware development. Attackers are experimenting with what they can do, inside and outside the enterprise. We haven’t yet seen massive self-replicating mobile malware, but we think that’s mostly because nobody has hit on a business model for untargeted attacks, beyond toll fraud," he says.

Symantec tracked mobile malware monetization, including premium-rate SMS trojans, tracking spyware, search engine poisoning, pay-per-install/click schemes, repackaged adware, and identity theft. According to Product Manager John Engels, "We used to see these for Symbian. When iOS
changed the landscape, Apple did a good job of building in [malware deterrents] such as sandboxing and AppStore review. Now Android is picking up where Symbian left off because it’s open, with alternative distribution paths that are a recipe for more challenging malware.”

Similar trends have been seen in malicious activity on social networks such as Facebook. “[Social media] malware tends to be user-focused: looking to gain access to the user’s account or credentials,” Cisco’s Landesman says. “Today’s biggest enterprise threats don’t evolve from social networks, but at some point, those could morph into more targeted attacks.”

For now, social media attacks tend to be untargeted. M86 Security Labs reports that Facebook scams surged during the first half of 2011 as attackers searched for new ways to convince thousands to click on malicious links. From “like-jacking” and “comment-jacking” to photo tagging and rogue applications, social engineering tricks snared users into pay-per-click or pay-per-install scams -- some leading to malware like the Koobface botnet Trojan. Facebook itself scans over a trillion clicks per day, blocking more than 200 million posts and messages carrying malicious links.

Social media security risks
For IT groups scrambling to stop malware on so many different fronts, deciding which threats to tackle can be a challenge. The best place to begin is by understanding emerging malware: targeted platforms, exploited vulnerabilities, and jeopardized business assets.

“Recently, the biggest threats have not attacked computers -- they’ve attacked people,” says Symantec Security Response Director Kevin Haley. “We’re seeing [email] spam drop as attackers move to social media. Factors include shutdown of major botnets, growing ineffectiveness of spam, and natural migration to new vectors. Technology itself hasn’t changed that much; social engineering got better and toolkits made malware easier.”

To date, social media malware has gotten the biggest bang by aiming at Facebook, Twitter, and YouTube. For example, Twitter’s brevity, anonymity, and real-time communication have fostered many hacks since 2007 -- some
involving account compromise, others malware dissemination. The two are intertwined, as legitimate and fraudulent top-followed accounts are used to phish thousands of victims. Shortened links, trend tags, and direct messaging further increase the odds of following tweets to malware.

As more businesses use Twitter to track industry news and communicate with customers, associated risk is growing. Not only do less than one-quarter of enterprises block Twitter, but “companies cannot assume they don’t have a social networking presence,” Cisco’s Landesman says. “Nothing from a technology standpoint will solve this. You’re better off having practices in place to determine what’s being said about your company and your tone and action plan should a social networking crisis develop” Such practices might involve rapidly detecting and reporting tweets that reference your brand but carry links leading to malware.

Facebook too has been plagued by phishing attacks. However, Facebook tends to be more personal, resulting in individual rather than business risk. But millenials expect to use Facebook and other social networks 24/7: Over half of surveyed college students said they would not even consider taking a job with an employer that banned access. Rampant password reuse and bring-your-own devices also mean credentials gleaned by Facebook malware could well play a role in corporate account break-ins.

**Workforce and malware mobility**

In fact, consumer mobile network attach rates are skyrocketing, driven largely by bring-your-own devices. According McAfee Senior Architect Igor Muttik, these unmanaged smartphones and tablets pose real enterprise risk.

“Mobile devices are no longer just phones; they are now full computing devices. For example, they can record audio and video for blackmail or industrial espionage,” he says. “If somebody brings their device into the office, IT has no idea what’s on it. A blanket ban on personal devices isn’t going to succeed, so measurement of security is essential before allowing devices in or rejecting them.”
According to Muttik, market-leading devices -- iPhones, iPads, and their Android counterparts -- have similar OS security models. The latest incarnations of each deter malware through sandboxing, code signing, permissions, and hardware encryption. The biggest difference in malware risk, he says, lies in software sourcing.

"Apple has done a better job. Non-jailbroken iPhones have been pretty safe -- to date we've seen only proof-of-concept malware in the AppStore -- but it will not stay clean forever," says Muttik. "The fact that Apple devices can be jail-broken illustrates there are vulnerabilities. Wherever you have both a browser and a kernel exploit, you can remotely own the device."

Unfortunately, Android has not been so fortunate; in-the-wild malware spiked last year. By December 2011, Lookout had identified over 1,000 Android malware applications, doubling since July. The firm now pegs annual risk of an Android user encountering malware at four percent, compared to risk of clicking on a phishing link at 36 percent.

Kaspersky Researcher Tim Armstrong believes a tipping point has been reached for Android malware. "We're still seeing SMS as a vector, but we've seen rapid growth in sophistication since FakePlayer [the first Android SMS Trojan in late 2009]. We're seeing malware like DroidDream exploit phones to gain [root] permissions, and Trojans like GGTracker download code," he says.

**Deterring malware through governance**

CheckPoint Researcher Tomer Teller attributes this surge to unwise app downloads. "We can clearly see a big mobile malware shift from the Web to apps, using markets to bypass review, get distributed, and [solicit] installation through social engineering," he says.

"The app review process is what makes Android less secure. There is no validation of the person distributing apps through the market. Open policies are good for developers, but a bad thing for users. Enterprises need to get involved with their [device] manufacturers and carriers to understand these threats, vulnerabilities, and risks," Teller says.
While many would like Google to tighten Android Market policies, others see a need for IT to step in. "If enterprises can control apps, they can control their malware exposure," Kaspersky's Armstrong says. "Application management has potential to stop a lot of mobile malware from entering networks."

Symantec's Engels suggests using mobile device management (MDM) to enforce whitelists and control mobile apps in some use cases, for example iPads used for retail, logistics or health care. But Teller says whitelisting is problematic for BYO devices. "Enterprises don’t have time to review [public] apps published on a daily basis. I think we’ll see [list providers] emerge to do second tier review and certification, helping enterprises [use blacklists] to make sure user-downloaded apps don’t have malware."

Enterprises must rely on carriers to patch vulnerabilities exploited by malware. But Lookout's Wyatt suggests auditing installed apps, correlated to known vulnerabilities. For enterprise-developed mobile apps, Wyatt recommends code review. "We often encounter apps that do not leverage OS security, send identities in the clear, or expose vulnerabilities in back-end apps. [Looking for these mistakes] would eliminate fundamental problems that we see [exploited] time and again," he says.

**Rolling out new antimalware protection**

Additional strategies likely are needed to mitigate business-affecting malware delivered and executed outside corporate networks. New device-resident and in-the-cloud antimalware approaches can complement existing defenses.

"Even with bring-your-own devices, some policies are still applicable if not directly, then from a practices standpoint," Lookout's Wyatt says. "With the emergence of native and third-party MDM solutions, there are now enterprise-friendly ways to bolt security onto mobile devices that don’t have antimalware baked in."

Specifically, MDM can not only mandate passwords and invoke remote wipe; it can also remotely install (or direct users to) mobile antimalware apps. Such scanners are readily available for Android, but not effective on iPhones or iPads due to OS restrictions.
Ultimately, many antimalware vendors recommend embedding antimalware “in the cloud.” For example, some carriers already deploy anti-malware to deliver SMS filters and anti-phishing to subscribers. A growing number of Software as a Service providers apply internal antimalware measures like email attachment virus scanning, phishing URL filters and domain reputation systems, blocking malicious content before it can be delivered. Enterprises can follow suit by embedding in-the-cloud antimalware as they deploy private clouds.

Beyond in-the-cloud antimalware, cloud threat intelligence services can help to rapidly update malware signatures and deliver real-time threat analysis, detecting links that lead to social media malware and malicious applications, thereby reducing enterprise dependence on inevitably diverse website or market governance.

For example, McAfee analyzes events gathered from all over the Internet at over 100 million endpoints (including mobile devices) and 60 million gateways. According to CTO for Public Sector Phyllis Schneck, McAfee uses these events to create a real-time reputation weather map that shows storms forming on the Internet. Reputation data can then be delivered to human network operators and fed back into reputation-aware systems (e.g., secure Web gateways).

“This global threat intelligence enables the network to respond automatically, stopping attacks never seen before,” Schneck says. “If ISPs can use this to filter out a lot of [malicious] traffic before it reaches the enterprise, we can lower the profit model for botnets. The same methodology applies to cloud services -- the cloud just changes where the bits and bytes are processed.”

**Stopping malware inside the corporate network**

Even experts with vested interest in new antimalware approaches recommend leveraging other types of security tools to battle malware, such as next-generation firewalls, secure Web gateways, data loss prevention and network behavior analysis. This strategy may not stop external infection, but it can reduce business impact, especially if platforms are reputation-aware.
Proactive security measures: How to prevent malware attacks

By Chenxi Wang, Forrester Research

Malware problems are a widespread issue for both consumers and business. In 2010 alone, we saw Operation Aurora, Zeus, Stuxnet and many other significant malware instances. To enhance the enterprise's malware-defense capability, security professionals need to stop chasing the malware flavor of the month, and instead develop proactive security measures that strengthen...
the enterprise’s fundamental defense DNA. If you have not made “defense against malware” a top priority, it’s high time you do so.

One of the reasons malware defense should be an IT priority is that the incumbent technologies are only effective to a degree against modern malware. Additionally, the growing adoption of social media, both within the enterprise and the consumer market, provides a convenient malware distribution channel, as well as an information reconnaissance platform.

For businesses that conduct transactions over the Web via consumer-facing applications, man-in-the-browser (MITB) malware, such as the Zeus Trojan, which aims to steal a user’s banking credentials by intercepting online banking sessions, is of special concern. If MITB malware exists on a customer’s desktop, the business can’t trust anything sent via the user’s browser, not even when SSL is used. This presents a major challenge for consumer-facing businesses, because it’s impossible for them to exert client-side controls on the consumer’s endpoint. In order to understand how to prevent malware attacks of this sort and protect the integrity of your consumer transactions, there are a few things to consider:

- **For B2B transactions, implement dual approval.** This process stipulates that, for every transaction initiated by a user, a separate approval step involving a different user in the same organization (presumably on a different machine), must take place before the transaction can proceed. The assumption is it’s unlikely that two users’ machines would be compromised simultaneously.

- **For B2C transactions, implement second-channel verification.** For this type of verification, the second channel must be distinct from HTTP, and the server can only execute a transaction after it has been verified via the second channel. For example, if a consumer requests a fund transfer over the Web, he or she will get an SMS message verifying this transaction. The transaction will only proceed if the consumer consents to the transaction via SMS.
• **Strengthen server-side fraud detection.** By looking for anomalous patterns, such as unusual location and usual spending patterns, server-side fraud detection is a good defense-in-depth principle, even with second-channel verification or dual approval procedures.

For business-facing malware, the variants today are stealthy, polymorphic, targeted and agile --and typically exploit several types of vulnerabilities. Client-side vulnerabilities are a major vector by which malware infiltrates businesses. In order to detect malware penetrating the work environment, security professionals should consider the following:

• **Offline malware and threat detection.** Inline technologies, such as IPS and secure Web gateways, need to keep up with line speed, and therefore are limited in the amount of analysis they can perform. But, offline detection capabilities in products provided by vendors such as FireEye Inc., Damballa Inc. and NetWitness Corp. can conduct much deeper analysis and may catch malware others have missed.

• **Whitelisting whenever possible.** In a highly controlled environment, whitelisting can be a powerful tool against anomalies, including malware. It can be applied to Web accesses, software installed on servers and endpoints, and server-to-server communication. Organizations using whitelisting, however, must have a fast response capability to handle exceptions and rare cases.

• **Browser security.** Since many malware problems spread via the Web and exploit browser vulnerabilities, a hardened browser environment should eliminate this major threat vector. With new technologies, such as those provided by products from vendors Invincea Inc. and Quaresso Software Technologies Inc., browser security is almost fully attainable.

While malware defense is and should be an ongoing effort, security professionals don't have to perpetually play catch-up with the ever-changing malware industry. Rather than buying into the threat du jour marketing hype, organizations can become more threat tolerant by creating and promoting a
How antivirus software works: Virus detection techniques
By Lenny Zeltser

An antivirus tool is an essential component of most antimalware suites. It must identify known and previously unseen malicious files with the goal of blocking them before they can cause damage. Though tools differ in the implementation of malware-detection mechanisms, they tend to incorporate the same virus detection techniques. Familiarity with these techniques can help you understand how antivirus software works.

Virus detection techniques can be classified as follows:

- **Signature-based detection** uses key aspects of an examined file to create a static fingerprint of known malware. The signature could represent a series of bytes in the file. It could also be a cryptographic hash of the file or its sections. This method of detecting malware has been an essential aspect of antivirus tools since their inception; it remains a part of many tools to date, though its importance is diminishing. A major limitation of signature-based detection is that, by itself, this method is unable to flag malicious files for which signatures have not yet been developed. With this in mind, modern attackers frequently mutate their creations to retain malicious functionality by changing the file’s signature.

- **Heuristics-based detection** aims at generically detecting new malware by statically examining files for suspicious characteristics without an exact signature match. For instance, an antivirus tool might look for the presence of rare instructions or junk code in the examined file. The tool might also emulate running the file to see what it would do if executed, attempting to do this without noticeably slowing down the system. A single suspicious attribute might not be enough to flag the file as malicious. However, several such
characteristics might exceed the expected risk threshold, leading the tool to classify the file as malware. The biggest downside of heuristics is it can inadvertently flag legitimate files as malicious.

- **Behavioral detection** observes how the program executes, rather than merely emulating its execution. This approach attempts to identify malware by looking for suspicious behaviors, such as unpacking of malcode, modifying the hosts file or observing keystrokes. Noticing such actions allows an antivirus tool to detect the presence of previously unseen malware on the protected system. As with heuristics, each of these actions by itself might not be sufficient to classify the program as malware. However, taken together, they could be indicative of a malicious program. The use of behavioral techniques brings antivirus tools closer to the category of host intrusion prevention systems (HIPS), which have traditionally existed as a separate product category.

- **Cloud-based detection** identifies malware by collecting data from protected computers while analyzing it on the provider’s infrastructure, instead of performing the analysis locally. This is usually done by capturing the relevant details about the file and the context of its execution on the endpoint, and providing them to the cloud engine for processing. The local antivirus agent only needs to perform minimal processing. Moreover, the vendor’s cloud engine can derive patterns related to malware characteristics and behavior by correlating data from multiple systems. In contrast, other antivirus components base decisions mostly on locally observed attributes and behaviors. A cloud-based engine allows individual users of the antivirus tool to benefit from the experiences of other members of the community.

Though the approaches above are listed under individual headings, the distinctions between various techniques are often blurred. For instance, the terms "heuristics-based" and "behavioral detection" are often used interchangeably. In addition, these methods -- as well as signature detection -- tend to play an active role when the tool incorporates cloud-based
capabilities. To keep up with the intensifying flow of malware samples, antivirus vendors have to incorporate multiple layers into their tools; relying on a single approach is no longer a viable option.

Contents

New Malware threats require new antimalware protection strategy

Proactive security measures: How to prevent malware attacks

How antivirus software works: Virus detection techniques
Free resources for technology professionals
TechTarget publishes targeted technology media that address your need for information and resources for researching products, developing strategy and making cost-effective purchase decisions. Our network of technology-specific Web sites gives you access to industry experts, independent content and analysis and the Web’s largest library of vendor-provided white papers, webcasts, podcasts, videos, virtual trade shows, research reports and more—drawing on the rich R&D resources of technology providers to address market trends, challenges and solutions. Our live events and virtual seminars give you access to vendor neutral, expert commentary and advice on the issues and challenges you face daily. Our social community IT Knowledge Exchange allows you to share real world information in real time with peers and experts.

What makes TechTarget unique?
TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals and management. We leverage the immediacy of the Web, the networking and face-to-face opportunities of events and virtual events, and the ability to interact with peers—all to create compelling and actionable information for enterprise IT professionals across all industries and markets.

Related TechTarget Websites
➤ SearchCloudSecurity
➤ SearchFinancialSecurity
➤ SearchSecurityChannel