The Malware Threat Businesses are Ignoring and How Damballa Failsafe Fits In

by Kevin Beaver, CISSP

Malware is no doubt one of the most misunderstood threats to business. Perhaps it's related to the fact that – like the human virus counterpart – malicious code is out of sight and therefore out of mind. In many respects, telling management that something needs to be done about malware on the network is like telling a toddler to keep his hands out of his mouth while shopping at the mall. They can't *see* the infection, but they also can't comprehend the consequences. They simply don't get it.

The Malware Reality

Contrary to popular perception, a "preventative" approach isn't always what's needed to keep malware at bay, especially zero-day exploits. In many instances, malware has already taken a foothold so it's a matter of responding in a mature and methodical fashion in order to get things back in order. The difference between initial intrusion and all out compromise is in the timing. According to Trustwave's *2011 Global Security Report*, it takes an average of 156 days before security breaches are detected! I see these lengthy delays in my work as well and I suspect that many organizations *never* know their systems have been compromised. Combine this with the fact that many businesses I've come across – both large and small – have no semblance of a security incident response plan and it's the perfect scenario for a malware disaster.

Having worked on projects involving command and control malware that had infected thousands of computers in a targeted attack, I've seen how ugly things can get when malware goes undetected and is improperly handled in the enterprise. The reality is that you can implement what would otherwise be considered "solid" security controls all day long and your network will still not be impervious to command and control, advanced persistent threat (APT) types of attacks using zero-day malware. This is especially true given how simple it is to trick users into clicking malicious links and opening infected files.

We often have a general false sense of security because our traditional security controls are reporting that all's well. Log monitoring and event correlation can't put all the pieces together. Patch management, strong passwords and security awareness training aren't enough by themselves either. Perhaps most importantly, traditional anti-virus and anti-spyware are often not enough to protect the enterprise from advanced malware threats.

Damballa's Solution

Enter Atlanta, Georgia-based Damballa. Having been around since 2006 – a time before command-and-control malware was cool and APTs weren't even being discussed – Damballa has been fine-tuning the Damballa Failsafe product to address this problem. An appliance-based solution, Damballa Failsafe uses sensors to monitor network traffic for anomalies and infections which, in turn, report back to a management console for visibility, control and termination of advanced malware as it propagates.

Don't think this malware affects the average business? According to Verizon's *2011 Data Breach Investigations Report*, 73% of all breaches were the result of the exploitation of a backdoor or command and control channel. I'd argue it's something we certainly shouldn't be ignoring. Damballa Failsafe does this by going beyond traditional prevention-only anti-virus solutions and assisting with the response side of command and control malware as well.

Damballa Failsafe looks across the entire malware/APT infection cycle as follows:

1. The initial dropper being downloaded via a malicious Web link or email attachment
2. The updater and download process reaching out to grab the actual malware
3. The communication of installation status and sensitive information off the victim system
4. The ongoing command and control communication process that can last indefinitely

Damballa Failsafe correlates deep packet inspection of all Internet traffic across egress points, proxies and DNS looking for suspicious behaviors that indicate advanced malware infections. Specifically, the technology determines if the traffic is suspicious, the destination is shady or the behavior is automated – three things that can indicate systems infected with known or zero day malware. Since it monitors network traffic rather than specific endpoints, Damballa Failsafe can detect infected systems across the board from Windows to Mac OS to iPads and smartphones. That is a big advantage over endpoint-centric controls. Because, if you're not protecting *every* type of system then you have some residual – and unnecessary – risks that need to be addressed.

The big new feature of Damballa's recently-released Failsafe 5.0 is its cloud-based malware analysis. Suspicious Windows executables and PDF files are picked off the wire and then sent to Damballa Labs for dynamic analysis. Rather than just alerting to potential infections, all of this information is analyzed automatically so you don't have to correlate log events and determine infections manually. Assets and victim systems are then given "Risk Factor" and "Threat Conviction Scores" that prioritize the systems requiring attention. Instead of producing reactive alerts to problem areas, Damballa Failsafe provides actionable intelligence on how to best respond.

Why do Binary Analysis in the Cloud?

There are many benefits to analyzing malware in the cloud. First – and arguably most importantly – it gets the malware away from your network. Even if it's sandboxed or virtualized, do you really want malicious code executing on your network and communicating via your Internet connection? Also, savvy malware may detect that it's running in a contained environment and not execute like it normally would in an unprotected lab environment. Cloud analysis is much more scalable and requires no system updates on your part.

I've been skeptical of the cloud given that third-parties have their hands in the mix. Cloud services can certainly create accountability issues if they're done poorly. The good thing about Damballa Failsafe is that it lets you decide when and how to send files out to the cloud for analysis. Suspicious files are flagged and analyzed at your direction. Plus they're transmitted via SSL. Not that this makes it right, but if you look at your existing malware protection – or really any other security control on your network – odds are good that you're already sending files and data back to your vendors for analysis anyway.

As with any security product, there are some considerations to make with the Damballa Failsafe appliance. It requires a dedicated management console as well as 1U worth of rack space in your data center. It doesn't currently support IPv6. You'll also need to spend some time up front finding the ideal tap or span port location on your network as the product runs "out of band" and monitors egress, proxy and DNS traffic. Those are certainly not show-stoppers though.

Moving Forward in the Malware Battle

One of Damballa's catchphrases is "A breach *can* be detected, *if* you know where to look." I agree. Acquiring good information on malware infections is more than half the battle. Based on what I'm seeing in my work, responding to outbreaks can prove futile if you don't have the proper tools and processes in place to facilitate good decision making. Simply bringing in specialized expertise for incident handling or forensics analysis is going to take time and it isn't going to be cheap either.

I'm a big believer in doing what you do well with information security and then leaving the rest up to the vendors with specialized technologies, expertise and threat intelligence you're not going to be able to acquire on your own. It's important that you step back and think about this advanced malware problem and what it means for your business. Even if management subscribes to the notion of "Our business is not a target," odds are your business is a target and will get hit at some point. As Ayn Rand said, "We can evade reality but we cannot evade the consequences of evading reality."

Left ignored, the malware problem can grow from a mere "viral infection" to a cancer on your network that you can't ignore. Don't wait until it's too late. One vendor's technology – Damballa or otherwise – isn't the silver bullet for managing all of your information risks but it's certainly a critical piece of the puzzle to help fight this threat that we can't seem to get our arms around. Damballa's technology is certainly worth checking out. Damballa Failsafe or not, just do *something*. This issue isn't going away.

About the Author

Kevin Beaver, CISSP, is an independent information security consultant, author, expert witness and professional speaker with Principle Logic, LLC. He has over two decades of experience in IT and specializes in performing information security assessments revolving around minimizing business risks. Kevin has authored/co-authored 10 books including one of the all-time best-selling information security books Hacking For Dummies (Wiley) as well as Implementation Strategies for Fulfilling and Maintaining IT Compliance (Realtimepublishers.com) and The Practical Guide to HIPAA Privacy and Security Compliance (Auerbach). He is also the creator and producer of the Security On Wheels audio programs providing security learning for IT professionals on the go (securityonwheels.com). Kevin can be reached at his website www.principlelogic.com and you can follow him on Twitter at @kevinbeaver.