Advanced Malware: Protecting Federal Agencies with a Layered Defense Strategy

by Pat Calhoun, SVP and GM, Network Security Solutions, McAfee

Federal mandates and regulations—including FISMA/CAESARS, FDCC/USGCB, NERC-CIP, HIPAA, and the DHS CDM program—all specifically call out the requirements for monitoring, analyzing, and mitigating increasingly sophisticated advanced malware threats and attacks.

"In 2012, US Computer Emergency Readiness Team processed approximately 190,000 cyber incidents involving Federal agencies, critical infrastructure, and the Department's industry partners. This represents a 68% increase from 2011."

—Assistant Secretary Roberta Stempfley and Director Lawrence Zelvin, Department of Homeland Security, May 16, 2013

"While we previously watched, collected information, and added to our understanding of our nation-state adversaries' intentions, we are now looking to disrupt and deter the individuals behind the keyboard who have made it their mission to attack, steal, spy, and commit terrorist attacks against our nation and its citizens."

—Richard A. McFeely, Executive Assistant Director, FBI June 12, 2013

Determined cyberattackers are striking US federal agencies with malware that is both more malicious and smarter than ever before. This malware is targeted, stealthy, evasive, and adaptive—enabling these characteristics in advanced persistent threats. Sure, known threats are still with us, but lurking in their midst are complex zero-day attacks that elude traditional defenses such as signatures. We are faced with designer rootkits and Trojans that can hide and move around US government networks, go unnoticed for long periods of time as they do their dirty work, infiltrating those networks and systems to steal vital government and citizen data assets. It's a big and continually evolving problem that must be foremost in the minds of those entrusted to secure our government's most sensitive and vital information and communication assets.

Agencies Attract Attacks

Attacks targeting government agencies are increasing in both number and potency. In 2013, a department of energy facility was singled out by cyberhackers, compromising several hundred employees' personal information for possible future exploits on sensitive and/or classified information. A recent high-profile attack against the Federal Reserve demonstrated that new vulnerabilities can now be exploited within an hour or two of discovery—the "zero-day" threat has shrunk to "zero hour."

With nation-states involved in—or providing sponsorship for—more and more of these attacks, the threat landscape is becoming increasingly dangerous for US federal information systems.

Urgent Need, Concerted Response

There's widespread recognition and general consensus regarding the rapidly expanding nature of these threats and attacks, and the urgent need for the US to effectively respond to them.

As they move to adopt more effective protections, US federal agencies and organizations associated with critical infrastructure are beginning to realize that traditional single-tier security solutions can't keep up with these insidious threats. What's needed is a more sophisticated, intelligent, and all-encompassing advanced malware solution that addresses detection, protection, and remediation.

The most successful way to address the advanced malware quandary is through a layered solution that integrates multiple technologies to quickly attack the problem from beginning to end. That's where the concept of comprehensive threat protection comes in—a big idea that really works to round out and bolster your defense strategy at every angle.

Think Beyond the Sandbox

Lately, there's been a lot of excitement and buzz about technologies such as sandboxing, which isolates suspicious files in a safe environment to help identify new threats when they appear. But identification is only part of the problem, and malware designers have gotten better at writing malware that avoids detection in a sandbox. Furthermore, it doesn't stop malware from infiltrating your network, nor does it repair the damage done. For a more complete solution, complex government environments need much more than just a sandboxing tool. As with other security technologies, sandboxing can have immense value, but it's only one piece of the larger puzzle.

In recognition and support of this new cybersecurity reality, the National Institute of Standards and Technology (NIST) recently released an update to one of its core federal cybersecurity documents, SP800-53. The primary driver for this critical revision was clearly stated upfront:

"This update was motivated principally by the expanding threat space—characterized by the increasing sophistication of cyberattacks and the operations tempo of adversaries (for example, the frequency of such attacks, the professionalism of the attackers, and the persistence of targeting by the attackers). State-of-the-practice security controls and control enhancements have been developed and integrated into the catalog addressing such areas as: Mobile and cloud computing, applications security, trustworthiness, assurance, and resiliency of information systems; insider threat, supply chain security, and the advanced persistent threat."

—Excerpt from opening paragraph, Special Publication (SP) 800-53, Revision 4 *Security and Privacy Controls for Federal Information Systems and Organizations*

We believe that in-depth analysis technologies integrated with reputation services and other anti-malware, network, and endpoint solutions provide a layered approach that covers all of the requirements of a comprehensive threat protection strategy: Identification and analysis, protection, and remediation. These critical defenses build on one another and support each other in important ways.

For example, highly cost-effective and efficient signatures and reputation services work hard day-in and day-out to catch a high volume of threats. Why not leverage a global reputation database to avoid malware that other entities have already seen? Plus, signatures and reputation help lighten the load on advanced malware appliances and technologies like static analysis and sandboxing, so that they can tackle the difficult cases. Static code analysis reverse-engineers code, analyzing all attributes and instruction sets to determine intended behaviors, including those that may not execute immediately.

Sandboxing, or dynamic analysis, on the other hand, allows suspicious code to run in a controlled, isolated environment as a way of understanding its behavior. It's a great way to recognize a well-choreographed attack sequence. A combination of signatures/reputation, thorough static analysis, and sandboxing is the ideal way to protect your organization against malware of all types.

Plan Your Defense Against Advanced Malware

Let's take a look at how a comprehensive threat-protection strategy works, why it works, and why you need it:

- *Analysis and conviction*—Innovative analysis technologies, including static code analysis and sandboxing, work together to provide the most accurate detection and classification of sophisticated malware threats across multiple protocols. Additionally, signatures and behavioral analysis do a lot of discovery work on the front end, minimizing the volume of suspicious files that require the heavy lifting involved in sandbox analysis down the line. Unlike generic sandboxing environments, which can be evaded by situationally aware malware or can incorrectly trigger malware alerts on safe files, a better approach would be to analyze threats in the environment that matches the targeted system. You get more accurate results faster, which is exactly what you need.
- *Protection*—Integrated network security products, such as intrusion prevention systems and web and email gateways, instantly stop additional infiltration attempts and contain infected endpoints, preventing malware from spreading. A comprehensive threat protection strategy shares what it knows about identified malware immediately with global threat intelligence reputation services. This means that protection against these newly detected threats is distributed across multiple products, including endpoint and network solutions, worldwide.
- *Remediation*—Integration of endpoint defenses streamlines the process of investigation across all endpoints and delivers swift, selective, and effective remediation, significantly reducing your operational costs while improving efficacy.

Stand up to Malware with an Arsenal of Defenses

The challenges presented by advanced malware to US federal agencies and critical infrastructure owners and operators are formidable and continually evolving. Clearly, big ideas are needed to conquer this big problem. Dropping another box on a network does not solve the problem. A truly effective solution requires deep integration with other security technologies and products—like the comprehensive threat-protection strategy from McAfee.

Advanced malware is simply no match for our unique threat-detection technology, which combines deep, comprehensive static code analysis and sandboxing integrated with our systematic arsenal of layered defenses that meet the expanding capabilities of advanced malware attacks head-on. Find out just how prolific advanced malware has become by reviewing the findings in the *McAfee® Threat Report: Second Quarter 2013*: http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q2-2013.pdf.

And for much more information on how McAfee is helping to address these challenges, please visit the McAfee Public Sector and Critical Infrastructure websites:

- http://www.mcafee.com/us/industry/public-sector/index.aspx
- http://www.mcafee.com/us/solutions/critical-infrastructure/critical-infrastructure.aspx

About the Author

Pat Calhoun is senior vice president and general manager responsible for defining and executing the strategic direction for McAfee Network Security solutions, which include network intrusion prevention systems, enterprise firewall, web protection, email security, data loss prevention, and identity management. Calhoun leads the engineering, marketing, and sales functions that drive worldwide growth for this area of the business.

McAfee
An Intel Company

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

60546brf_atd-fed_1013_fnl_ETMG