McAfee®
An Intel Company

NEUTRALIZE ADVANCED MALWARE

Solution Guide

Malware infiltration and data exfiltration almost always occur over a network. Installation of malware by a remote attacker after system access was the infection vector 95% of the time.

—2012 Verizon Data Breach Investigations Report [2]

Security Connected

The Security Connected framework from McAfee enables integration of multiple products, services, and partnerships for centralized, efficient, and effective risk mitigation. Built on more than two decades of proven security practices, the Security Connected approach helps organizations of all sizes and segments—across all geographies—improve security postures, optimize security for greater cost effectiveness, and align security strategically with business initiatives. The Security Connected Reference Architecture provides a concrete path from ideas to implementation. Use it to adapt the Security Connected concepts to your unique risks, infrastructure, and business objectives. McAfee is relentlessly focused on finding new ways to keep our customers safe.

"Within the hacker underground, there are services cybercriminals use to have thousands of malware checked at one time against all the available AV software to determine which crimeware is undetectable. Some services also offer to fix detectable malware."[1]

Adapt Layered Defenses for Comprehensive Malware Protection

Challenges

Each month brings a new example of a targeted attack against a business, government, or critical infrastructure operator previously considered "invulnerable." At the same time, "money-driven crooks continue to focus more on opportunistic attacks against weaker targets," according to the 2012 Verizon Data Breach Investigations Report. In the Verizon study, 69 percent of events involved malware, and 61 percent involved both malware and hacking techniques.

As more organizations encounter the cost, disruption, and public humiliation of malware-enabled events, more CIOs are asking IT teams to reassess their current and future risks from malware and evaluate their defenses. Today's malware is a malleable tool in the hands of a clever cybercriminal. Malicious code is disguised to look innocent. Code can attack through vulnerabilities and vectors that standard antivirus doesn't monitor or is not designed to catch. Malware adapts to evade static tools and active defenses, varying its timing and execution paths depending on the host.

Commercial malware toolkits have made it simple for these techniques to be part of opportunistic phishing, spam, and bot networks. When the rewards are high enough, the tactics are woven into custom, targeted attacks. Once established within an organization, both generic and custom malware spreads, reaches out to its command and control centers, exfiltrates data, and, in the hands of cyberactivists, looks for ways to disrupt or damage operations. Each hour, day, and month before malware is mitigated is an hour, day, or month that the malware can propagate, evolve, and conceal itself on another host.

Why is malware still affecting users?

Most companies depend heavily on two or three layers to defend against malware: an initial line of defense at the Internet gateway, plus a second layer on each desktop or server. Each of these layers must be as sophisticated as the malware. Look for the unexpected—unusual behavior and malicious designs in unknown code.

While inline systems will detect the bulk of malware, it's inevitable that some nasty code will slip through. Few companies have had the resources to deploy specialized monitoring tools and hire malware forensics experts to capture and analyze anomalous code. Typically, nothing happens until a breach or attack is identified—often well after the event through a third party—and specialists are called in to determine what happened where and define a remediation and recovery plan.

Solutions

Today's layered defense strategy must match the sophistication of modern threats. No individual antimalware product can block all malware infiltration and subsequent activity. Comprehensive malware protection requires enough of the right layers within each asset and within your infrastructure. Just as importantly, these layers must be knit together into a system of systems, sharing data through dynamic processes that work to highlight key events and expedite identification, containment, and remediation.

Reduce vulnerability to opportunistic attacks

First, organizations should reduce the attack surface for opportunistic malware by upgrading antimalware in endpoints and network gateways.

Going beyond signatures, effective antimalware technologies should hunt for known and emerging threats using dynamic detection heuristics and referrals to cloud-based services that constantly correlate breaking threat intelligence from multiple types of sensors and sources. Ideally, endpoint tools will apply context to make a blocking decision: unusual application behavior, activity below the OS layer, or a real-time comparison of a suspicious file to a database that reflects multiple reputation attributes (file, sender/destination IP address). In addition to these techniques, some of today's advanced content gateways and network intrusion prevention systems (IPS) have the processing power and antimalware engines to perform real-time static analysis as well as emulation.

Add layers of scalable forensic analysis

Any remaining unusual code detected by antimalware should be referred to a dedicated forensic appliance that can perform high-speed analysis and detect subtle malware using both static and dynamic techniques. Forensic appliances can incorporate the static analysis used in advanced content gateways or next-gen IPS systems, and also apply dynamic analysis—sometimes called sandboxing—which runs the code in a safe environment to see what it tries to do. The combination will reveal malicious intent and behavior to quickly confirm a threat.

Use automation to speed response

If malicious code is confirmed, then the analysis system should tell your other security tools to detect and block that code in the future. The same fingerprint can also be used to track down compromised systems throughout your network for remediation. This is typically a manual process today. However, if you are able to integrate malware response data and processes with system security and network security, you can use automated management workflows to quickly quarantine and remediate compromised hosts.

Add additional lines of defense

Malware (and the hackers using it) will look for vulnerabilities in laptops, tablets, mobile devices, applications, file servers, and databases. You can reinforce the antimalware on these systems with controls that prevent system exploitation, creation of back doors, rootkit installation, and malware execution if the code is able to install. Common tools include host IPS, application control, vulnerability scanning, real-time kernel protection, and change management monitoring. Add database activity monitoring to protect critical assets in the data center. Integrate these systems together to create a manageable mesh of defenses that improve your resistance to multi-pronged attacks.

Assume some malware has or will get onto your network

These technical endpoint and network controls should reduce the chance that malware will get in or infect your assets. However, today's best practice is to assume that there are already compromised systems within your network. You must enhance your ability to detect, dissect, and disrupt the actions enabled by this malware by ensuring your security operations center can monitor your environment for malware activity, data exfiltration, and suspicious user behavior.

Given the volume of network traffic, comprehensive malware protection also requires a "Big Data" class security and information event monitoring (SIEM) system that can aggregate, correlate, and mine data from multiple sources: endpoint system logs, network gateways, user directories, inventories of devices entering and leaving the network, and more. With end-to-end visibility, humans can look at patterns and higher-level threat trends while automated systems tackle the tactical defenses.

Best Practice Considerations

- Protect at multiple threat points, including network, endpoint, web, and email, to close all malware attack vectors
- Incorporate diverse static and dynamic analysis techniques to detect malware using advanced and evasive tactics
- Layer defenses to provide reinforcing protections that can prevent system compromise and remote access and halt attacks in process
- Ensure communication and integration between network protection and endpoint protection to enable fast detection and remediation
- Fuse real-time intelligence into designs to minimize false positives, detect emerging threats, and allow the system of systems to make context-aware decisions
- Centralize management and monitoring across all protection technologies to lower costs and improve visibility, response, and decision-making

Value Drivers

- Close coverage gaps to prevent malware-enabled loss of sensitive data such as intellectual property and regulated data
- Reduce disruption to users and the network by preventing infections and malicious traffic
- Improve resilience through an organizational ability to detect, validate, classify, and contain targeted attacks before damage is done
- Automate manual tasks and workflows to lower the event-to-incident confirmation time
- Reduce remediation, consulting, forensic, disclosure, and legal costs
- Prioritize critical events to focus time and resources more accurately and increase incident handling capacity
- Improve situational awareness through real-time visibility into changing risk and threat events
- Enable agility through modular and open architecture and integration with legacy and third-party systems

Related Material from the Security Connected Reference Architecture

Level II—Solution Guides

- Counter Stealth Attacks
- Operationalize Intelligence Driven Response
- Control and Monitor Change
- Protect Your Information

Level III—Technology Blueprints

- Protect the Data Center
- Essential Protection for PCs
- Fighting Rootkits
- Investigate Data Breaches
- Look Inside Network Traffic
- Protect Databases
- Protect the Network Perimeter
- Secure and Control Laptops

For more information about the Security Connected Reference Architecture, visit: www.mcafee.com/securityconnected.

About the Authors

Ed Metcalf is director of product and solution marketing at McAfee. He has been with McAfee for nearly nine years and is responsible for developing strategic go-to-market plans for a number of McAfee products, including the joint McAfee and Intel solutions of McAfee DeepSAFE™ technology platform, McAfee Deep Defender, and McAfee ePO™ Deep Command. Ed has nearly two decades of experience in security and technology product marketing, product management, and sales management. Before McAfee, Ed worked for Hewlett Packard, Tripwire, and various technology startups.

Rick Simon is a senior group marketing manager in the Network Security Business Unit at McAfee. Rick develops and markets integrated solutions that enable enterprises to solve key security problems. Prior to joining McAfee, Rick worked for Cisco and led marketing at several startups and held roles in product management, product marketing, and strategic alliances at Hewlett-Packard, Oracle, and Cisco. Rick holds a BSEE from The University of Michigan and an MBA from The University of Chicago Booth School of Business.

[1] http://www.csoonline.com/article/708790/virtual-analysis-misses-a-third-of-malware
[2] http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

McAfee
An Intel Company

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

60087sg_advanced-malware-L2_0213_wh