McAfee
An Intel Company

COUNTER STEALTH MALWARE

Solution Guide

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.

"Rootkits are one of the fastest growing types of malware, with more than 200,000 new rootkits identified each quarter (2012). The number of total stealthy kernel threats has tripled since early 2010."

—McAfee Labs™

Unmask Stealthy Villains

Challenges

The most menacing type of cyberattack is invisible. It may be a targeted attack that uses sophisticated stealth techniques, such as hiding outside the operating system (OS), or a banking Trojan that dynamically moves across endpoints and compromised servers globally.

A stealthy attack operates quietly, hiding evidence of an attacker's actions. In Operation High Roller, malware scripts adjusted the bank statements a victim could view, presenting a false balance and eliminating indications of the criminal's fraudulent transaction. By concealing proof of the transaction, the criminal had time to cash out.

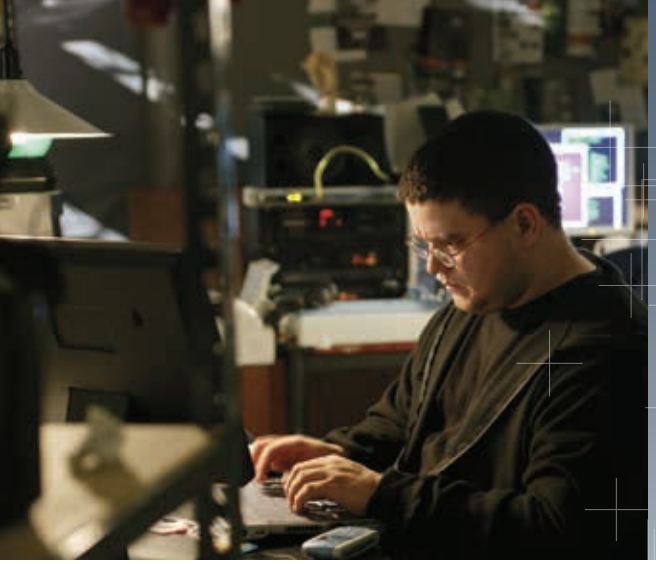
Many criminals do "just enough" to stay ahead of traditional security tools. However, advanced cybercriminals invest extra time and ingenuity in stealth tactics to get the highest ROI— vital data or sabotage. Attackers behind these threats are well funded, with clandestine supply chains with access to evolving stealth malware toolkits.

Stealth attacks may include any the following:

- *Evasion*—Malware goes unseen by traditional anti-malware and intrusion prevention systems (IPS) that rely on signatures. It often lurks outside the OS and disguises its presence, disabling scanners. It may move from system to system without generating the network traffic usually seen when malware propagates. Attackers will also move command and control centers, frequently among bots that are not known to be malicious hosts.
- *Targeting*—Malware may be compiled for a unique organization or industry, as was the case with AntiCNN.exe and Stuxnet/Duqu
- *Dormancy*—Attackers may plant malware throughout an environment and leave it inactive for a long time, waiting for conditions to be ripe for the next phase. They use rootkits to hide the malware.
- *Complex phases*—Attack sequences employ a mix of tactics, vectors, and malware to navigate around point security solutions designed to address a particular crime of opportunity and attack vector
- *Determination*—Attackers will take their time to get their reward. The longest attack duration discovered in McAfee Shady RAT analysis was 28 months, while the average of the more than 70 companies identified was 8.75 months.

For years, security experts have urged layers of security controls across endpoints, networks, and cloud, supported by multivector threat intelligence. This reduces the attack surface and the "noise" that hinders detection. But many companies have not yet achieved this level of protection. Most have porous networks with many Internet-connected entry points from which to launch an attack.

Since they do not see the threat, administrators often believe they don't have a problem. Without something to "fix," cost justifying these systems has seemed difficult and unnecessary—until the company falls victim to an attack or data loss.



Stealthology 101

Professional hackers learn early on to cover their tracks. Rootkits are one of the preferred tools, since rootkits can target any system, from database servers to point-of-sale terminals, from mobile phones to automobile electronics. Because rootkits can operate within and below the OS, they can disguise or conceal the files, processes, and registry keys touched by other malware. These traits make rootkits a vital component of multistage threat operations.

—Dave Marcus and Thom Sawicki,
The New Reality of Stealth Crimeware.[1]

Solutions

Detecting the presence and actions of stealthy malware and attackers requires investment in tools that provide broad and deep visibility integrated with protection and response systems. The strategy applies technical controls across the phases and vectors of stealthy attacks.

Since no environment is 100 percent clean of malware and compromised systems, the controls work together to block the activities of each phase. Business needs must still be taken into account to guide sensitivities and determine what to investigate.

First contact

The best and most cost-effective time to block a stealthy attack is before the attacker gets into a host or network. Although perimeters are now very porous, inline network security systems can inspect inbound traffic and block known and suspected attacks entering through web, email, and network protocols. These network protections can be separate systems, or "next-generation" systems that integrate multiple inspections.

To protect endpoints—both fixed and mobile—robust security suites should mirror network protections, encrypt sensitive data, and include device controls that restrict use of unapproved USB devices or portable storage. Both endpoint and network systems should use real-time and reputation-based intelligence to block communications with dynamic malicious addresses, undesirable messages, and files.

Local execution

Vulnerability assessment tools can help you discover and audit systems on your network in real time to keep software patches up to date and check for malware and misconfigurations. Best practice is to lock down high-risk and shared systems, including fixed-function devices and printers, against unapproved system and application changes. Anything with an IP address can be a launch pad for attackers.

Establish presence

Attackers use techniques such as rootkits to embed and conceal software and await the right moment to trigger the next phase of the attack. Because some rootkits load before the OS, they load before traditional security measures that protect at the OS level, including antivirus. To counter this stealth move, your system protections should be enhanced with real-time hardware-assisted software that prevents installation of malware outside the OS.

It's also important to be sure your network security prevents propagation of malware within the network and outbound communications by compromised hosts, such as beacon messages out to a command and control center.

Malicious activity

The final phase of the attack delivers the payoff, destroying data, brands, systems, or productivity. Ideally, the other layers of controls have reduced the attack surface and attack activities. What's left is to monitor traffic and analyze data flows for irregularities. It helps to begin with a baseline of "normal."

Because of the diverse types of attack activities and threat vectors, it is important to aggregate and correlate data across protection systems—the faster, the better. This data collection can quickly turn into "Big Security Data." You capture a range of data from the network, correlate it, add context, and analyze it to surface suspicious events like bot activities, reconnaissance, exfiltration of data or credentials, malware propagation, and tampering.

Threat analytic tools correlate internal and external events, threat feeds, and actors to detect patterns, interactions, and telltale signs of attack elements, building profiles of attacks and drawing attention to the most critical events. Through this continuous feedback loop, your defenses get smarter and more attuned to your business risks and threat patterns.

Best Practice Considerations

- Choose solutions that include real-time prevention and disruption of threats to stop stealth techniques automatically before they have a chance to take hold
- Deploy solutions that protect at multiple threat points, including network, endpoint, web, and email security to stop all stealthy attack vectors
- Layer defenses to provide reinforcing protections that halt attacks in process
- Ensure endpoint security has visibility beyond the operating system to detect dormant and low-level malware
- Leverage hardware features enabling enhanced and accelerated security

Value Drivers

- Create a central command and control platform to minimize manual correlation, response time, and human resource requirements
- Facilitate increasingly rapid threat detection and assessment, reducing the threat window and incident impact
- Generate contextually relevant alerts to provide more exact and timely incident response
- Minimize false positives and correctly prioritize critical events to focus time and resources more accurately
- Reduce remediation, forensic, and legal costs
- Stop stealthy threats in real time before they have a chance to conceal their presence

Related Material from the Security Connected Reference Architecture

Level II—Solution Guides

- Operationalize Intelligence-Driven Response
- Control and Monitor Change

Level III—Technology Blueprints

- Achieve Situational Awareness
- Assess Vulnerabilities
- Essential Protection for PCs
- Fight Rootkits
- Investigate Data Breaches
- Look Inside Network Traffic
- Protect Your Databases
- Protect the Network Perimeter
- Secure and Control Laptops
- Scan Anytime Using Intel AMT

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

About the Author

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.

McAfee
An Intel Company

[1] Source: http://www.mcafee.com/us/resources/reports/rp-cylab-mobile-security.pdf

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

60562sg_stealth-malware-L2_0913_kg