IDC ANALYST CONNECTION

Robert Westervelt
Research Manager, Security Products

Stop Malware, Stop Breaches? How to Add Value Through Malware Analysis

May 2015

The shortage of qualified security personnel, increases in the costs for safeguarding networks, and the exponential increase in Web-based attacks dictate a shift in the ways malware defense must be organized and then carefully administered.

The following questions were posed by ThreatTrack to Robert Westervelt, research manager for IDC's Security Products program, on behalf of ThreatTrack's customers.

Q. There are so many data security threats organizations face, and one of the longest standing has been malware. However, the problems with malicious code seem to be more serious than ever. How has the malware threat evolved?

A. The simple answer is that malware is now the key tool of organized criminal operations that are motivated by financial gain. Organized criminals have developed automated attack tools to carry out their financially motivated attacks. Those toolkits are sophisticated, enabling attackers to create targeted campaigns with malware they easily craft to bypass traditional networking and endpoint security defenses. Simply using signature-based antivirus as protection is no longer adequate to keep up with modern malware techniques that use metamorphic and polymorphic tactics to change the iteration of the malware in an effort to evade detection.

Metamorphic malware is on the rise and designed to subtly change over time to obscure functions and defeat signature-based approaches. It's considered to be a more difficult tactic for malware writers to code, but automated tools are reducing the challenges. Polymorphic malware is an older approach but is also designed to make subtle code changes typically to a single malware component. Polymorphic malware strains are easier to detect, but the sheer volume of them in the wild is overwhelming standard signature-based defenses. The crime syndicates actually test their malware against the most popular antivirus software to ensure that it cannot be discovered. They also have designed the custom malware so that they can easily modify it and maintain their edge against standard signature-based antivirus.

The final piece of the malware problem is that attackers understand it doesn't take a high level of sophistication to gain an initial foothold in an endpoint system. Most attacks continue to target known vulnerabilities on endpoint systems, but organized criminal elements have been investing heavily in discovering or buying unknown vulnerabilities in order to create zero-day malware designed to exploit previously unknown weaknesses and other advanced techniques. Although the vast majority of malware will exploit known vulnerabilities, zero-day malware is reserved for use against extremely high-value targets.

Q. It appears that in today's malware environment, discovery isn't enough. There is a growing need for malware analysis. Could you explain the benefits in using malware analysis tools?

A. It is no longer enough to simply detect, quarantine, and remove a threat from an infected system. Forward-thinking organizations have developed and honed incident response processes and remediation measures to address the underlying weaknesses that caused the infection in the first place and to provide protection across the entire corporate environment, including branch offices and remote employees.

Emulated environments, known as sandboxes, enable malware analysts to create a mirror image of a system to detonate a suspicious file and safely monitor its behavior. The various routines associated with the malware are examined and documented and the nature of an attack and the intent of an attacker may become clear. The identified threat indicators can be used to feed additional protection into other security systems. The contextual information can also be used to provide the security team with suggested changes in the environment to reduce the attack surface associated with the sensitive resources being sought.

Security vendors can also use virtual emulation environments, offering the suspicious file analysis capabilities to bolster an organization's current security investments. This kind of cloud-based sandboxing improves detection by detonating and examining suspicious files in milliseconds and determining an object's risk to the corporate network.

As mentioned, malware writers test their code against signature-based antivirus so that they can avoid detection. Performing forensic analysis on a piece of malware helps organizations understand what the evasion techniques are, and in turn they can build defenses that recognize when those techniques are used. Additionally, the malware forensics can see URLs or IP addresses that correspond to command and control or a location where stolen data is to be delivered. This information is again something that can be utilized by intelligence security systems to prevent communications to those sites.

Q. Writing malware and discovering the malicious code would appear to be something that takes a certain set of skills. What types of skills are required? Is there a "skills gap" in malware analysis, and how can organizations find or train the people they need?

A. IDC has posed this question to organizations with mature security programs and incident response teams. The common answer is that hiring and retaining skilled analysts may be a challenge, but skilled personnel are essential to identifying anomalous activity that may signify a significant threat. To meet this challenge, many organizations that lack a mature IT security team consider outsourcing the process to managed security services providers that have the talent to conduct proactive monitoring and assist in identifying potential threats and prioritizing alerts through customized risk scoring.

While outsourced security services is an option, another option is to use automated tools that allow you to do much of the work yourself. There are tools that allow an organization to investigate, in an automated manner, the real threats to your specific environment. That last item is the key in why you would want to perform the malware analysis yourself. By keeping the analysis in-house, you can test the suspected malware against your entire application stack to observe how it will behave in your environment, with your system configurations. Using a malware analysis tool provides you unique insight, which can be quickly turned into response to prevent infection. Because you have a good understanding of your environment, utilizing an automated malware analysis tool allows you to quickly adjust the analysis to any changes in your environment or even to allow some testing of how proposed changes could expose you to malware.

Malware analysis tools are important in automating the forensic process, but they are only tools, and the people using them need some skills. However, those skills are easier to obtain than the highly technical knowledge embedded in malware analysis software.
Malware analysts need to be able to interpret behavioral patterns provided by sandboxing environments — an understanding of attacks that stem from payloads with multiple components used in multistaged attacks. These components include malicious code designed to crash or cripple systems, steal and upload data, or simply log a victim's keystrokes. In addition to understanding payloads, malware analysts must understand common attack vectors, intrusion techniques, and propagation methods when attackers attempt to move laterally within a corporate network.

Successful malware analysts need to be familiar with the overall IT environment, understand the software development process, and be familiar with network protocols. They also must have strong written and verbal communication skills as well as listening skills so that they can clearly articulate the information to the rest of the IT organization and potentially to management. Character is also an important consideration. Analysts should be able to follow policies and procedures and work in a team environment, and they should be trustworthy enough to handle sensitive information.

Q. With the proliferation of advanced, sophisticated, and targeted attacks, what should organizations be looking for from their antimalware tools to ensure that they can defend against modern malware?

A. Emerging vendors are coming to market with threat detection technologies that have automated response capabilities for containment and removal. Early adopters continue to take a hands-on approach, manually addressing remediation with support of automated tools. Threat intelligence feeds are increasingly becoming more customizable to specific industry verticals and unique environments. These threat intelligence feeds should be scrutinized not on the amount of information but on how much actionable threat information they provide.
As mentioned previously, cloud-based and on-premises sandboxing platforms can augment current security investments by inspecting suspicious files that aren't captured by signature-based technologies.

Digital forensics tools, IT management platforms, and integrated security systems that span the endpoint, application, and network layers are critical to addressing advanced attacks that may leverage multiple systems as temporary staging grounds. Organizations need to identify tools that members of the incident response team are comfortable using and don't require extensive training.

Q. With antimalware becoming a critical component of the overall IT security portfolio, what actions can organizations take that will elevate their malware defenses to the next level?

A. Organizations should undergo a thorough assessment of their security infrastructure to identify not only whether systems are properly configured and maintained but also whether systems can interoperate to share threat indicators and provide rapid protection to other parts of the environment. In addition, organizations should find solutions that bridge communications gaps and provide additional contextual information to aid correlation engines to bolster detection capabilities and rapid response.

ABOUT THIS ANALYST

Robert Westervelt is a research manager within IDC's Security Products group. He provides insight and thought leadership in the areas of cloud security, mobile security, and security related to the Internet of Things (IoT). Rob is also responsible for research and analysis around a wide range of evolving security markets, including endpoint security, security and vulnerability management (SVM), and identity and access management (IAM).

ABOUT THIS PUBLICATION

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

COPYRIGHT AND RESTRICTIONS

For more information on IDC, visit www.idc.com. For more information on IDC Custom Solutions, visit http://www.idc.com/prodserv/custom_solutions/index.jsp.

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com