Solution Guide

Busted: Seven Myths about Advanced Malware

Advanced malware: the catchall term for the most sophisticated, evasive, destructive, and ever-evolving cyber threats. When used in conjunction with one's own security infrastructure, these two words understandably accelerate heartbeats. Fed by this anxiety and sometimes perpetuated by security vendors, a number of misconceptions have arisen concerning this cyber menace. This guide will examine seven common misconceptions and distinguish between myth and reality.

Myth #1: The Primary Challenge is [Still] Identification

Before advanced malware became prevalent, the primary challenge of both the anti-malware vendor and the information security manager was to identify the cyber threat and push out new signatures as fast as possible. By recognizing the protection gap several years ago, before signatures were available for emerging threats, McAfee and others in the industry began to use cloud-based reputational assessments to supplement signatures for faster recognition of emerging threats.

Identifying advanced malware is important, but the real challenge is stopping it and remediating any damage.

Today's malware continues to push the defensive frontier. Though often based on well-known malware with available signatures, advanced malware:

- Has been modified and disguised enough to avoid typical signature-based, pattern-recognition defenses.
- Usually focuses on specific targets, minimizing its footprint on the Internet and the network, thus evading reputation-based defenses.
- Is very patient, able to loiter for a long time and stealthily maneuver until it achieves its objective.

For these reasons, advanced malware is routinely active for days, weeks, or months before it is discovered and shut down. In the meantime, it creates significant risk to systems and organizations as it seeks data or disruption.

Signature-based approaches still have merit (as we will see later on). But, because advanced malware evades such defenses and may be too targeted to trigger a reputation, it requires alternative security approaches for accurate identification.

Two other technologies can now easily supplement signatures and reputation. Both dynamic sandboxing and static code analysis can strip away malware's defenses and disguises to reveal its intent.

Identification has become possible with modern technologies. You *can* detect the threat. The new problem is detecting the threat in time to disrupt the attack and prevent the breach.

The fight against advanced malware only starts with identification. Myth busted.

Myth #2: Sandboxing is Sufficient

Sandboxing is one of the most popular methods for discovering advanced malware. A sandbox is an offline, isolated virtual environment that mirrors a real endpoint environment. The file is executed (or detonated) within this controlled setting, revealing what the file will do. In the sandbox, a suspicious file's behavior can be examined without causing harm to the live system.

The initial success of sandboxing has generated a lot of excitement. People are struck by visibility into activities they couldn't see before. However, although some "heavy lifting" associated with advanced threats is done by sandboxing, it's important to understand what this technology does and does not do. Similar to standard signature-based products, sandboxing is not a panacea.

Sandboxing *does* assist in discovering advanced malware. The very best sandbox technologies use multi-engine behavioral analysis to quickly determine what the exploit is intended to do and where it was targeted to go. However, just as they did with signatures, many malware authors have figured out how to detect and avoid sandboxing defenses. Malware can:

- Detect when it is in a sandbox type of environment and then refrain from executing malicious actions.
- Contain preset delays so that its exploits will not execute until hours or even days after entering—and leaving—the sandbox.
- Execute only in the presence of specific applications or host configurations, so if the sandbox does not mimic these applications or configurations exactly, the malware doesn't activate.

Use of any of these sneaky techniques can cause the sandbox to conclude that the file in question is harmless, which allows the attack to proceed. These limitations are why, according to a leading analyst firm, sandboxing is a feature and not a complete solution.

How do you determine what that code will really do then? A thorough advanced malware solution uses the sandbox as just one form of analysis, making verdicts based on more than one opinion.

One complementary technology is full-fledged static code analysis: exhaustively examining what the code is coded to do.

- If it detects a sandbox, does it stay dormant? That's suspicious.
- Does a portion of the code resemble a known malware family? Since pieces of code are often re-used, a match of even a small percentage of code to a known malware family can convict a malicious file.
- Does it download other code, start or stop processes, or change registry keys? These are typical hallmarks of malicious intent.
- Does the file call an IP address with a risky reputation? In this case, your defense could convict based on external information.

Through innovations such as integrated static analysis, advanced anti-malware can be just as determined as advanced malware.

Sandboxing is a feature, not sufficient for a reliable conviction. Myth busted.

Myth #3: All sandboxes are similar

So if you accept that sandboxing is important, can you assume that any sandbox will suffice? No. Sandboxing options have changed very quickly in recent years, with standalone and centralized options for deployment. Each has different impacts on protection and performance.

One popular design deploys sandboxing standalone. Analysis happens offline, out of band, and disconnected from other analytics or remediation processes, so more files are evaluated than may be strictly necessary (had they been convicted through another form of analysis), and manual communications slow the investigative response. Any impact on time matters because you are hoping to disrupt and contain the attack before data is exposed.

Risk increases because standalone sandbox techniques analyze a *copy* of the suspicious file. While the copy of the file is undergoing complex, often time-consuming analysis in the sandbox, the original file continues on its way with plenty of time to reap havoc on "patient zero." So even if sandboxing reveals that the suspicious file is indeed malicious, it is often too late. By the time the diagnosis is reached, the actual file has very likely already compromised the target.

Rollout can be slow and expensive if a sensor must be deployed for each ingress point and protocol. Until every ingress point and protocol is covered, advanced malware can easily slip into the environment undetected. In the final TCO analysis, managing all those distributed systems can be costly and complex. Actually getting value out of the malware data requires manual and custom integrations that break with each product release.

In addition, many sandbox technologies run generic versions of a given operating system and its applications. Failing to duplicate each end-user's actual operating environment can lead to false assumptions about the behavior of the suspicious file. You may not have tested against the true target of the targeted attack.

Even if it covers all ingress points and uses a mirror image of each actual operating environment, standalone sandboxing still has the shortcoming that it can be evaded (discussed in the previous section), and the challenge that it doesn't operate in real time.

The preferred alternative to standalone sandboxing is centralized sandboxing. Instead of separate systems for web and email, a single system can handle multiple protocols and be placed to receive and evaluate traffic from all ingress points. This greatly reduces cost and deployment time and increases your ability to reliably assess files.

When the centralized system includes sandboxing in a series of filters, it fulfills the expectation of positioning sandboxing as a feature of a complete system. The filters can apply signatures, reputation, and real-time emulation to reduce the number of files to be analyzed in the sandbox and increase the accuracy of the assessment. Filters applied in a gateway layer are not run again, maximizing the resources and speed of the sandbox.

Sandboxing is like any emerging technology—your mileage will vary based on your choices. Myth busted.

Sandboxing options have changed very quickly in recent years, with multiple options for deployment, each with pros and cons.

Myth #4: Endpoint AV is Dead

With the advent of advanced threat defenses, people sometimes assume that traditional signature-based approaches are simply no longer part of the defense equation. With so many other potential bills to pay, should you continue to pay for endpoint antivirus?

Yes. Although signature-based antivirus technologies are only as effective as their last update, there are good reasons to continue using them:

- The most prevalent attacks are still based on known malware, so you can't afford to stop blocking.
- Ruling out known bad files makes it easier to concentrate on files that are suspicious or unknown.
- Endpoint protections operate in real time and can quarantine a suspicious file immediately, before it can do harm.
- Endpoint AV has the capacity to neutralize the threat – it can clean the system if a suspicious file is convicted.

Signature-based, endpoint protection can find and block malware in real time, track files into sandboxes, and increase overall efficiency of advanced malware defenses.

Compared to sandbox technologies, signature-based technologies have little operational overhead and are extremely efficient. They're also very accurate, with typically high hit rates and few false positives. Consequently, they dramatically decrease the load on more advanced malware detection technologies, which is key to maintaining the efficiency and cost control of the overall environment.

While their role in the malware equation may be changing, established endpoint protection approaches are not fading away. They are a critical technology in an integrated advanced malware solution. Signature-based protection can find and block malware in real time, track suspicious or unknown files into advanced threat defense solutions, and clean malware that has been convicted. Signatures reduce the noise and increase the overall efficiency of advanced malware defenses.

Endpoint AV may not be the star of the show anymore, but it is definitely still a supporting player. Myth busted.

Myth #5: Threat Intelligence is Simple

Makers of anti-malware signatures constantly employ thousands of researchers and systems across the globe to augment their respective threat intelligence databases. These databases contain information about malware stretching all the way back to the very earliest variants. Because of this vast history of archived information, many people assume that every security vendor is using the same basic cache of anti-malware information to support its point products.

Not all security vendors have the same threat intelligence or use it the same way.

Not in practice. Although antivirus vendors and researchers may share hash files and other virus information in industry forums, on bulletin boards, and in conferences such as Black Hat, the information each provides is not entirely the same. There is no assurance of accurate or timely data.

New vendors or vendors adding security to another product often just resell another vendor's research or implement publicly available threat data. This "lowest common denominator" protection isn't suited to advanced malware since it isn't optimized to promptly detect subtle and emerging techniques that are the essence of the targeted attack.

Ideally your threat intelligence vendor should be able to apply machine readable threat intelligence beyond signatures—reputation blacklisting and whitelisting, contextual and behavioral analysis, and localized threat intelligence—to detect the stealthy stuff.

But just as signature quality varies from vendor to vendor, other threat intelligence technologies vary, too. While a hash is a fairly definitive way to recognize and convict a file, reputations vary in type (file message, IP address, URL, and certificate), quality, and timeliness. A stale reputation—good or bad—increases risk that something undesirable will happen.

Equally important, the signature and reputation information that is consumed is very different across security vendors. This is because each point solution has its own distinct security architecture and objectives. For instance, endpoints may do elaborate analysis and cloud lookups before rendering judgment, without noticeably affecting the user experience. However, because of the high volume of traffic a next-generation firewall (NGFW) has to process, most will use a simple DAT file lookup filter to make block/allow decisions for files. Some NGFWs and next generation IPS systems, on the other hand, will look at other activities besides signatures or draw upon a different set of signature information, looking at behavior and vulnerability signatures.

Because of these inherent variations in threat intelligence resources and defenses, it's smart security to deploy different types of threat intelligence in different parts of your network. If an attacker can't break in through one door, he'll test a window or try a different room. With the right threat intelligence, your defenses can fend off each attempt. With linked and localized threat intelligence, you can force him to look for an easier target—another, less well defended, enterprise.

Not all security vendors collect the same threat intelligence or use it the same way. Myth busted.

Myth #6: Finding Equals Freezing

Detecting the malware—via signatures, reputation, sandboxing, or static code analysis—is just the first step. Identification is like intrusion detection systems and car alarms. What do you do when the alert goes off? How do you respond? Do you just watch as your car (or sensitive data) disappears?

Ideally, your first sighting occurs as you block a malicious file. If you can't block it, the next challenge is freezing or containment, the process of limiting the file's activities. Take the analogy of a TSA agent checking IDs at the airport:

If you can't block advanced malware, then the next challenge is freezing its activities, called containment.

- Everyday malware can be stopped by the TSA agent (endpoint agent, firewall, or web gateway) because its ID (signature) is known. Advanced malware, on the other hand, may try to get in through a service door with no TSA agent, or use a fake ID in front of a new agent at an especially busy gate, betting the agent will be too pressured to spot subtle differences in height or facial features.
- If the airport is sufficiently staffed, a TSA agent may sense something suspicious. She grabs some frames off the video stream and runs some facial recognition software. Her offline analysis finds that the airport (IT infrastructure) has been infiltrated. The problem, of course, is that the perpetrator is already inside, somewhere, and someone has to decide whether or not it's important enough to go after the culprit. Significantly, the analysis system itself doesn't make that decision; it can only tell her what the culprit looks like.

If you've been able to isolate a copy of a suspicious file, taken the time to analyze it, and correctly identified it as advanced malware, then you're like the TSA agent. You know you have a problem, but you can't stop it without help. The only way to truly stop an advanced malware attack is to immediately propagate information about the malware throughout the network so the file can be *isolated* and *frozen* before spreading to other points.

Finding does not equal freezing. Myth busted.

Myth #7: The Right Point Solution Will Keep You Safe

It is tempting to think if you had the right point solution, your environment would be adequately protected against advanced malware. Unfortunately given the sophisticated zero-day strategies of most advanced malware developers, the ease with which sandboxing can be beaten, the wide variation in point tools, and the necessity to work in concert with earlier antivirus tools integration of your various security solutions is absolutely critical.

No group of point solutions will protect you from all advanced malware. An integrated, layered approach will always be the best defense.

This is a big hurdle today. Effective teamwork is tough in IT. At a people level, administrators for endpoints, data centers, and network infrastructure operate in silos. At the process and technology levels, defenses were patched together from a medley of point products over many years. As a result, information security environments often lack a common vocabulary and dynamic, infrastructure-wide security integration. It's as if the staff in the control room speaks English and uses American standard sized tools, but the guards on the floor all speak different languages and use tools with metric measurements. Every discussion carries extra overhead for communication, data conversion, and comprehension.

In the meantime, the attacker's malware has settled into a host, begun reconnaissance and propagation, and is well on its way to enabling a successful breach.

It's often said that a system is only as good as its weakest link. The inability to isolate an instance of advanced malware and ensure that it won't spread is usually the weak link.

The way to successfully defend against advanced malware is to tie all of your solutions together—firewall, gateways, IPS, endpoints, mobile, virtual environments, and so on—with one cohesive, integrated, and resilient system.

The various technologies in your environment need to work together and share information so that malware that bypasses one solution will be caught by another. Next, the solution that detects the malware needs to share information with the bypassed product so that it can catch similar malware the next time. Shared knowledge helps all products and improves security across the enterprise.

To do this, the entire system must be capable of fully comprehending the urgency and complexity of the threat, and communicating that information intelligently to any point within the environment, including servers, endpoints, and remote operations. This command and control role is increasingly given to a security information and event management (SIEM) system. An integrated, layered security approach that combines real-time identification and blocking with offline analysis can achieve maximum coverage and protection throughout the enterprise environment, from core resources to firewalls, gateways, endpoints, and beyond. A flexible, scalable, and adaptable integrated approach will optimize coverage of network resources, reduce the risk of a crippling intrusion, and optimize the performance and value of security resources.

With advanced malware, the best point solution in the world won't protect you. Myth busted.

Conclusion

No doubt about it, combatting advanced malware is a formidable task that will only continue to grow. The complex nature of advanced malware demands a thoughtful review of your defensive strategy. Point technologies like sandboxing and threat intelligence should be knit into other analytic and response processes to get better results, faster. With sufficient integration, tools, and some luck, you can even disrupt the attacker's kill chain. Here are some key concepts to take away:

- It's not enough to find advanced malware; you have to block and remediate it, too.
- Sandboxing is far from foolproof and significantly hampered by lack of real-time analysis.
- Sandboxing helps you find but not block or remediate advanced malware.
- Signature and reputation tools are still very useful in your advanced malware defense arsenal.
- Security solutions vary substantially, even at the most basic level, so choose wisely.
- Advanced malware defense requires an integrated, layered approach to find, freeze, and fix any compromised systems in a rapid response model.

The best defense against advanced malware is a cohesive, integrated, layered security approach. That's what the Security Connected™ platform is all about. Learn more at **www.mcafee.com/securityconnected**

A key component of this layered security approach is McAfee Advanced Threat Defense. With a unique approach to sandboxing, Advanced Threat Defense finds stealthy malware and tightly integrates with McAfee solutions to freeze malware and initiate the fix for impacted systems. Learn more at **www.mcafee.com/atd**

About McAfee, a Wholly Owned Subsidiary of Intel Corporation

McAfee, part of Intel Security and a wholly owned subsidiary of Intel Corporation (NASDAQ:INTC), empowers businesses, the public sector, and home users to safely experience the benefits of the Internet. The company delivers proactive and proven security solutions and services for systems, networks, and mobile devices around the world. With its Security Connected strategy, innovative approach to hardware-enhanced security, and unique Global Threat Intelligence network, McAfee is relentlessly focused on keeping its customers safe. **www.mcafee.com**

About the McAfee Security Connected Platform

The Security Connected platform from McAfee provides a unified framework for hundreds of products, services, and partners to learn from each other, share context-specific data in real time, and act as a team to keep information and networks safe. Any organization can reduce risk and response time and lower overhead and operational staff costs through the platform's innovative concepts, optimized processes, and practical recommendations.

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