Doing Battle with Advanced Malware

How enterprises are tackling a new generation of insidious and potentially costly threats.

February 2014

Sponsored by: McAfee, an Intel Company

---

1. Introduction and Background: A New Kind of Threat

Advanced malware has arrived. A sly form of network breach, advanced malware creeps onto your network and parks itself, biding its time, usually with the intent to steal data or sabotage part or all of your business. Advanced malware attacks are most often unknown and can't be detected or stopped by traditional, signature-based defense tools.

Before panicking, note that most threats coming your way don't constitute advanced malware. That means you can continue to thwart the majority of threats using the defenses already in place: firewalls, intrusion prevention systems (IPSs), and Web and email gateways, for example. These tools remain critical, because the arrival of advanced malware doesn't mean that more easily identifiable attacks have gone away. Quite the contrary: they are now arriving every second instead of every hour, according to some reports.

But you do need to stay on top of the advanced malware situation. It's here, and you'll most likely have to deal with it sooner than you'd hoped.

To gauge enterprise awareness and activity level in battling today's security challenges, we surveyed the Webtorials subscriber base in September 2013. We found a surprising and refreshingly respectable level of awareness of advanced malware and its security challenges. We also learned that measures to defend against it need some beefing up in terms of investments in tools that not only detect advanced malware but halt it, so it can do no more damage, and also repair any damage that's already been done.

Our research findings represent 168 IT professionals in the Webtorials community who said they were a "involved in some aspect of installing, operating, planning and/or designing an enterprise communications network."

2. Key Findings

Our study determined that enterprises were fairly well aware of the new type of threat called advanced malware. Most find it quite worrisome but not yet rampant.

Here is a summary of our key findings:

- ***A good portion of enterprises are aware of advanced malware and consider it a "huge" or "significant" concern.***
- ***While enterprises don't seem to experience a massive volume of advanced malware incidents each week, they do spend a substantial amount of time resolving the few that they do get.***
- ***Organizations are ramping up their arsenals to do battle with advanced malware, though most current investments are weighted heavily toward detection-only tools.***
- ***Most respondents are familiar with a defense called sandboxing to fight malware but acknowledged that, alone, sandboxing is insufficient for conquering advanced malware.***

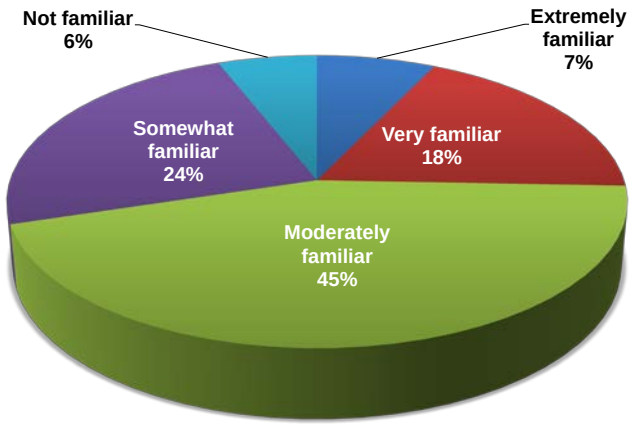
Let's take a brief look at each data point.

3. Enterprise Awareness and Concern

Most of the Webtorials response base (94%) indicated some level of awareness of advanced malware, and nearly three fourths (73%) reported that advanced malware represented a huge or significant concern to them (see **Figure 1** and **Figure 2**).

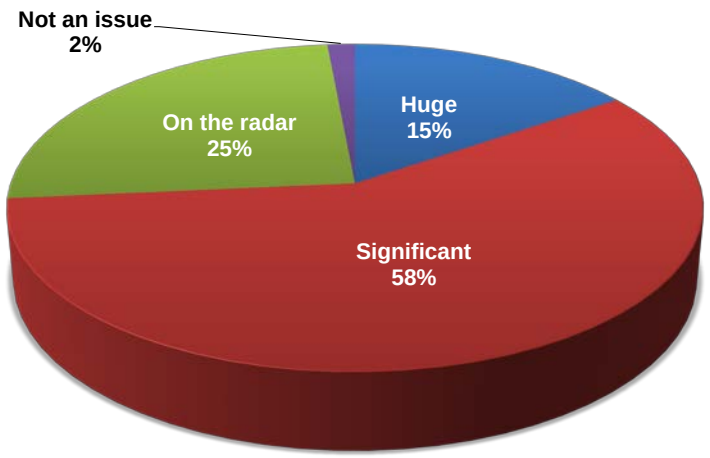
Armed with this knowledge and awareness, about a third (31%) were already using tools to combat them, while another 52% said they did not use any specifically for advanced malware, but were investigating doing so (see **Figure 3**).

Figure 1: Advanced Malware Awareness



How familiar are you with advanced malware threats and defenses?

Figure 2: Advanced Malware Concern Levels



How big of a concern is advanced malware at your organization?

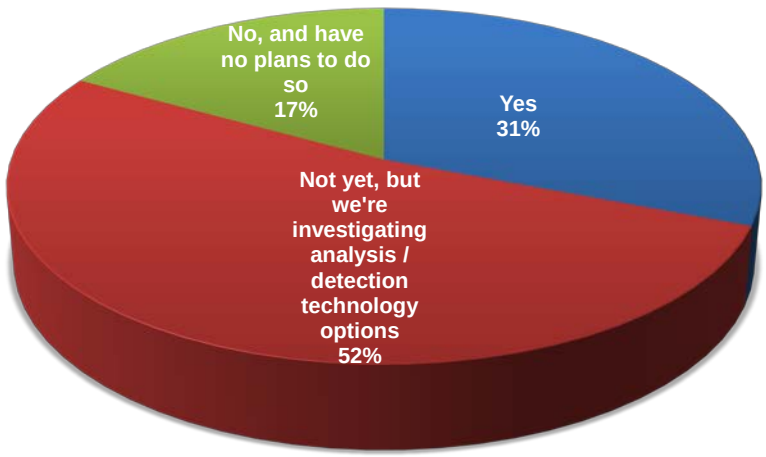
One respondent, Robert Frailey, who is the IS manager of Utah Medical, for example, said his company uses a well-known packet analysis and accounting tool to monitor activity on packet streams originating in the United States. These transmissions can then can be tracked back to the user and dealt with at the user or law enforcement level.

There's a problem with this approach, however, Frailey notes. "We can't do anything outside the U.S." with the tool, he acknowledged, because of different and stricter privacy regulations abroad.

4. Threat Volumes and Time Expended

The good news is that respondents perceive a low number of advanced malware incidents, relatively speaking. However, it appears that each consumes a substantial amount of time to detect and remediate. More than half of respondents (57%) said they experience fewer than five advanced malware incidents per week (see **Figure 4**), yet nearly a quarter (24%) said they spend upwards of 10 hours per week battling them (see **Figure 5**).

Figure 3: Are You Using Advanced Tools?

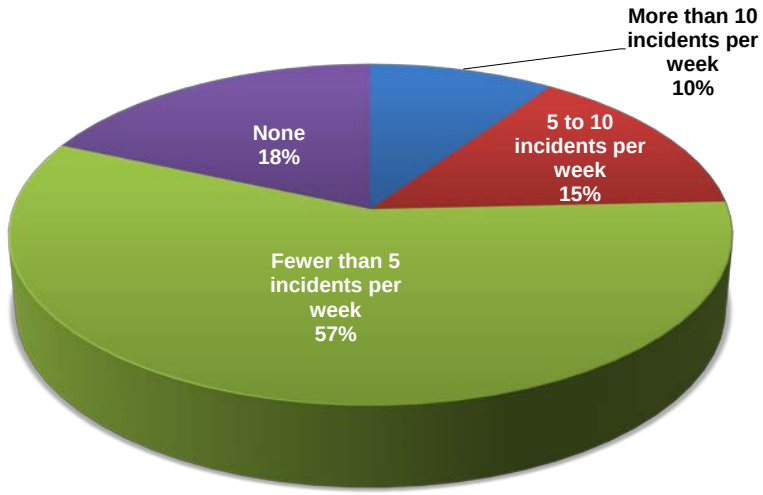


Does your organization use any technologies specifically for advanced malware defense?

A subsequent question supports the trend toward a low number of advanced incidents occurring that nonetheless require significant amounts of time to address them. Respondents were asked to rate how challenging advanced malware management tasks were, and the highest scorers were

"detection" (3.72 on a scale of 1 to 4) and "damage repair/ eradication," which earned a 3.53 ranking. Slightly less difficult, according to Webtorials respondents, were chasing false positives detected by their defense tools (2.86), blocking problems once they were found (3.16) and the timely notification of security incidents (3.37).

Figure 4: Advanced Malware Incidents

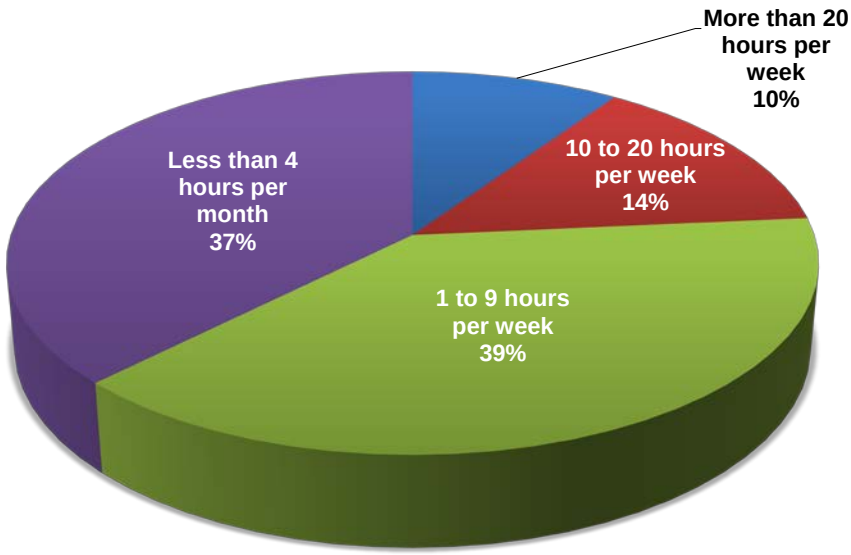


About how many malware incidents do you encounter at your organization?

5. Enterprise Investments: Slightly Lopsided

Most investments being made in the advanced malware area are those aimed at finding/ identifying it. Thirty percent (30%) of respondents said they had made no advanced malware security tools investments or had invested in detection tools only, leaving the follow-up blocking and fixing functions completely unaddressed.

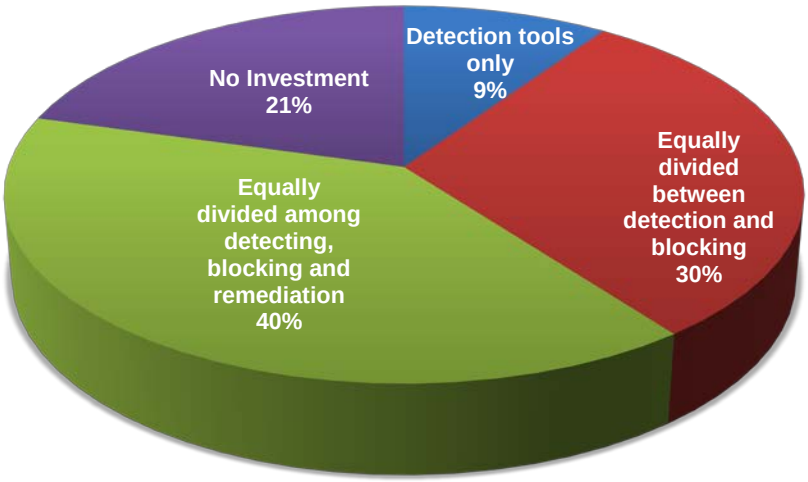
Figure 5: Advanced Malware Incidents



About how many malware incidents do you encounter at your organization?

Still, 40% said that they had purchased tools not only for detecting, but also for blocking and remediating advanced malware (see **Figure 6**), indicating a stronger balance across toolsets than Webtorials suspected before conducting the study. Fewer respondents (30%) have addressed detection and blocking but not remediation, as also shown.

Figure 6: Investment Distribution



How are your investments in tools to fight advanced malware currently divided up?

6. State of Sandboxing

Sandboxing is a function whereby questionable packets are sent into a virtual environment for analysis and inspection. Sandboxing is perceived as a useful security defense among the Webtorials community. Alone, though, it is considered insufficient for fighting the varied types of attacks that constitute advanced malware, which, by definition, is malware that is unknown. Where sandboxing tends to fall short is that the function is resource-intensive and, as such, does not always operate in real time. So enterprises can't count on this function to immediately detect and filter "bad" packets. While the sandbox is running its analysis to determine whether packets are good or bad, damage to the network and business can already be in progress.

In addition, malware writers at this point have become familiar with sandboxing and have begun to build in attributes to evade detection. To continue to be effective, sandboxes need to augment execution observation with thorough code analysis to determine when a piece of code is trying to outsmart them.

Nearly three quarters (74%) of Webtorials respondents agreed that sandboxing alone was insufficient for conquering advanced malware, though 57% said that sandboxing was the most effective defense available. The latter number indicates that additional tools are needed to address the real-time (and often one-time) nature of insidious, sophisticated attacks that are unknown and, as yet, unrecognizable.

7. How Can You Defend Your Network?

The best defense today is a layered approach that includes both signature-based and real-time, signature-less identification and blocking along with off-line analysis such as sandboxing. A layered approach provides the best protection and performance combination.

This layered approach can include numerous security products, both old and new. The key to success is tight integration between products so that you have a consistent, system-wide security solution. Integration enables security products to quickly communicate potential breaches and take action such as blocking additional entry attempts as well as identifying compromised machines and initiating clean-up.

There are some signature-less tools that can be used against advanced malware that operate in real time. Among those that have been around for a while are network behavior analysis (NBA), behavior heuristics, and emulation. However, these tools tend to focus on detection only and do not address blocking and remediation. So if a clever attack circumvents these detection tools, the tools cannot be relied upon to find and stop the attack or clean up any damage already done.

But these existing tools can be combined with others that address blocking and remediation into a security engine that's holistic and comprehensive. The more advanced malware management functions you can integrate to see all aspects of your security environment, the more likely you are to be able to detect something unusual and stop creative malware in its tracks. Just as next-generation firewalls at one point moved from being a single-function, grant/deny access-control box to containing a number of defense capabilities, the security landscape is now again at a point where it needs to aggregate functions.

"Integration enables security products to quickly communicate potential breaches and take action."

This aggregation includes endpoint and IPS tools with emulation of your environment. Covering all the bases in an integrated fashion allows you to be predictive as to what the outcome of certain types of breaches might be. And once the new attack type is identified as malicious, steps can be taken network-wide to initiate cleaning and remediation. The information can also be sent into cloud-based threat-intelligence databases so that it can be recognized by all future security products globally across enterprises to stop future instances of the malware.

8. Summary and Recommendations

Enterprises are aware of advanced malware and have taken early steps to prepare for defending against it. Much of the investments made to date have been in non-real-time, detection-only tools, leaving any mischief caused by the malicious code that has evaded the tools free to wreak havoc on the network. Advanced malware is hard to detect, stop and remediate. It is unknown and often is a one-time attack, making it difficult for signature-based defenses to recognize (as it's never been seen before) and thus hard to find. Sandboxing is the tool most used to identify this malware, but alone, it is inadequate, because it tends not to work in real-time

Enterprises are advised to balance security tools investment across all threat vectors – detection of the breach first, then a tool with which to halt its operation, then a tool with which to clean up any damage the infection may have done when on the network. Then integrate more traditional network security solutions with newer, dedicated malware analysis and remediation solutions. Portfolios of tools working in tandem to handle all these threats, not just point products to tackle select types of breaches and aspects of those breaches, make sense for use so as to create a holistic, comprehensive approach to information security. ♦

About McAfee

McAfee, 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.

For more information, visit http://www.mcafee.com/us/.

About the Webtorials® Editorial/Analyst Division

The Webtorials® Editorial/Analyst Division, a joint venture of industry veterans Steven Taylor and Jim Metzler, is devoted to performing in-depth analysis and research in focused areas such as Metro Ethernet and MPLS, as well as in areas that cross the traditional functional boundaries of IT, such as Unified Communications and Application Delivery. The Editorial/Analyst Division's focus is on providing actionable insight through custom research with a forward looking viewpoint. Through reports that examine industry dynamics from both a demand and a supply perspective, the firm educates the marketplace both on emerging trends and the role that IT products, services and processes play in responding to those trends.

For more information and for additional Webtorials® Editorial/Analyst Division products, please contact Jim Metzler at jim@webtorials.com or Steven Taylor at taylor@webtorials.com.

The primary author of this study was Joanie Wexler.

Published by Webtorials Editorial/Analyst Division
www.Webtorials.com

Division Cofounders:
Jim Metzler
jim@webtorials.com
Steven Taylor
taylor@webtorials.com

Professional Opinions Disclaimer
All information presented and opinions expressed in this publication represent the current opinions of the author(s) based on professional judgment and best available information at the time of the presentation. Consequently, the information is subject to change, and no liability for advice presented is assumed. Ultimate responsibility for choice of appropriate solutions remains with the reader.