ESG Brief

Malware and the State of Enterprise Security

Date: July 2013 **Author:** Jon Oltsik, Senior Principal Analyst

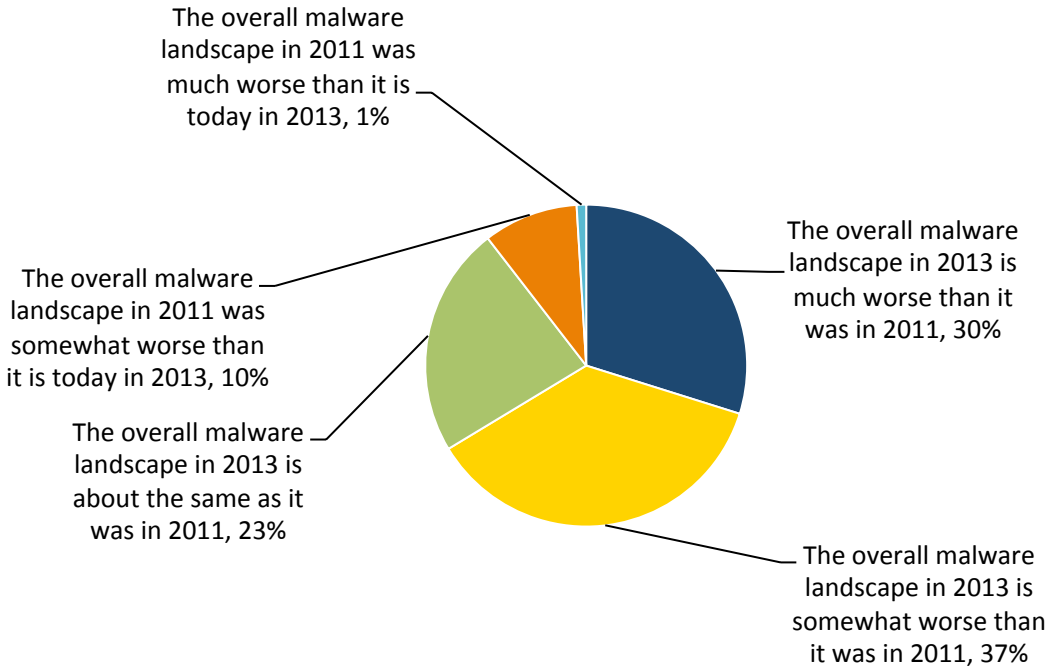
Abstract: *The malware threat landscape is getting worse and many large organizations continue to suffer security breaches as a result. Why? Enterprises often lack the right security skills and their current defenses and security analytics are no match for increasingly sophisticated and stealthy targeted attacks. Fortunately, large organizations recognize these gaps and are increasing security budgets to bolster malware prevention, detection, and response. To benefit from these investments as soon as possible, CISOs should improve malware knowledge, invest in security analytics, and deploy modern anti-malware technologies on networks and hosts.*

Overview

In May 2013, ESG surveyed 315 security professionals working at North American-based enterprise organizations (i.e., more than 1,000 employees) and asked them various questions about their malware knowledge, experience, challenges, and security strategies. The research reveals that 30% of security professionals believe that the overall malware landscape is much worse today than it was in 2011, while another 37% claim that the overall malware landscape in 2013 is somewhat worse than it was two years ago (see Figure 1).[1]

Figure 1. Advanced Malware Landscape Sentiment

In your opinion, how would you compare the overall malware landscape (i.e., volume, sophistication, sources, etc. of malware) in 2013 with the overall malware landscape in 2011? (Percent of respondents, N=315)



Source: Enterprise Strategy Group, 2013.

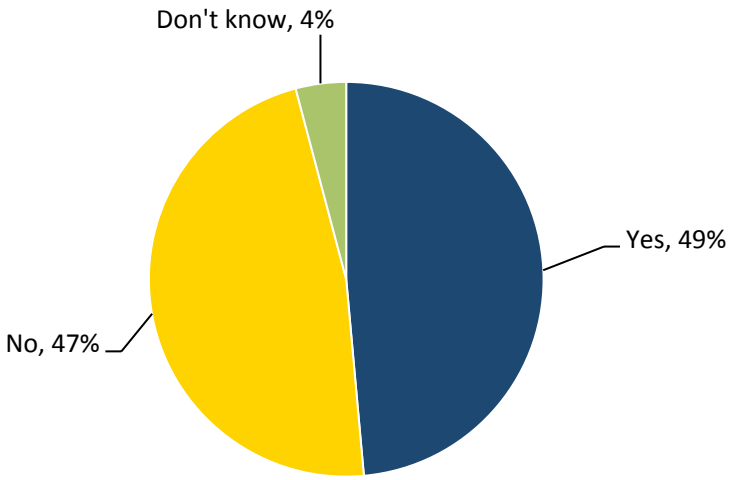
[1] Source: ESG Research Report, *Advanced Malware Detection and Prevention*, to be published August 2013. All ESG research references and charts in this brief have been taken from this research report.

Why do two-thirds of respondent organizations believe the malware landscape is getting worse? More than half (55%) claim that malware has grown more sophisticated, 47% believe that malware attacks have grown more frequent, and 43% say that malware is more stealthy today than it was in 2011.

Security professionals often base their opinions on personal experience and that seems to be the case in the ESG research. Nearly half (49%) of enterprises surveyed suffered a successful malware attack over the past 24 months (see Figure 2). For the purposes of this project, the term "successful malware attack" was defined as a malware attack that bypassed security defenses, compromised IT assets, altered IT assets' functionality in some way, and led to some type of unwanted outcome (i.e., system damage, data theft, unplanned remediation activities, etc.). It should be noted that 22% of organizations claim they suffered 26 or more successful malware attacks in the last 24 months.

Figure 2. Have Organizations Suffered a Successful Malware Attack in the Last 24 Months?

Has your organization suffered a successful malware attack in the last 24 months? (Percent of respondents, N=315)



Source: Enterprise Strategy Group, 2013.

Why Do Enterprises Continue to Struggle with Malware?

Large organizations have been dealing with malware like the Melissa virus (1999), SQL slammer worm (2003), and Zeus Trojan (2007) for years. Based upon this experience, it would be safe to assume that companies have become more adept with malware defenses, but the ESG data seems to indicate just the opposite. Yes, attacks have grown more targeted than in the past, but why are enterprises still having so much trouble with malware prevention, detection, and remediation? Because:

- **End-users open the door to malware too often.** As the old security adage states, "People are the weakest link of the information security chain." Clearly, security professionals believe this axiom is as true as ever: When asked to identify the factors most responsible for successful malware attacks, 58% of organizations point to lack of user knowledge about cybersecurity risks. This data certainly calls out the need for more end-user cybersecurity training, but CISOs must also always assume that in spite of any knowledge transfer, non-technical users will continue to be extremely vulnerable to social engineering and sophisticated attacks. Smart CISOs will supplement user training with more comprehensive and layered security controls as well as increased proactive monitoring.
- **Most organizations lack the right level of malware knowledge.** While security professionals understand the basic concepts about malware, the ESG research indicates that a large number are unfamiliar with advanced malware properties. For example, 40% of surveyed security professionals claim they are not very familiar or not at all familiar with polymorphic malware, 41% are not very familiar or not at all familiar with malware

packing techniques, and 50% are not very familiar or not at all familiar with malware command and control (C&C) techniques. To use another maxim, "You can't see what you are not looking for." Evidently when it comes to malware detection and remediation, many enterprises don't know what to look for.

- **Internet security defenses can't block or detect many forms of modern malware**. Enterprises have invested millions of dollars in security technologies, yet modern malware seems to have no problem circumventing technologies like firewalls, IDS/IPS, and security analytics tools. Security professionals are particularly critical about the efficacy of endpoint security software. Sixty-two percent of security professionals strongly agreed or agreed with the statement that host-based security software is effective at detecting/blocking older types of malware but it is not effective for blocking/detection zero day and/or polymorphic malware commonly used for targeted attacks today. If this is the case, endpoints remain extremely vulnerable and need to add new layers of security to all exposed hosts.

CISOs Are Taking Action

The malware situation does not paint a pretty picture; too often, cyber adversaries are gaining the upper hand in this persistent cat-and-mouse game. Enterprise organizations recognize this situation and are addressing the growing malware vulnerability gap. ESG research indicates that many enterprise CISOs are:

- **Increasing anti-malware spending.** Nearly three-quarters (74%) of respondent organizations say that security budgets are increasing significantly or somewhat in reaction to APTs, advanced malware, and sophisticated attacks. In most cases, these budget increases are used to add security headcount, purchase security technologies, or contract security services specifically intended for anti-malware activities.
- **Making organizational changes.** Many CISOs realize that the existing security organization lacks the right skills and structure to address modern malware threats. As a result, 39% of organizations created a specific group of security analysts dedicated to malware intelligence and analysis, 31% invested in incident detection services to support the IT team in the event of a malware attack, and 31% are actively recruiting security professionals and adding headcount in 2013. ESG believes that it is also worthwhile to invest in advanced education on malware techniques and tactics so analysts have a better perspective on what to look for as they monitor the network.
- **Bolstering defenses.** About 42% of organizations are conducting proof-of-concept testing or have already implemented anti-malware network gateways capable of executing and inspecting malware with virtual "sandboxing" technology. While network gateways are often added as an additional layer of defense, many organizations are moving on with other defenses. For example, 51% of enterprises will add new layers of endpoint security software to detect/block zero day threats and polymorphic malware moving forward. This is an area where advanced malware detection/prevention (AMD/P) tools such as Malwarebytes Anti-Malware Enterprise Edition can add immediate value.
- **Improving security analytics.** Nearly half (49%) of organizations plan to collect and analyze more security data to better detect and respond to malware attacks. This is another data point indicating a trend toward big data security analytics in the enterprise market.

The Bigger Truth

The ESG malware research indicates an alarming situation: Many large organizations are unprepared for the increasingly dangerous malware threat landscape. CISOs should certainly move quickly, but ESG believes it is worthwhile to take a step back and look at the big picture rather than jump into impetuous actions. For example, many organizations lack the right staff size or skills necessary to address malware threats, but given their current workload and the information security skills shortage, it is unlikely they can fill this void quickly.

Moving forward, most organizations would be well served by pursuing an anti-malware strategy focused on:

- **Common malware behavior knowledge.** APTs follow a general lifecycle that includes external reconnaissance, initial compromise, gaining foothold, escalating privileges, internal reconnaissance, lateral movement, and data exfiltration. Security professionals should become intimately familiar with each of

these phases so they can implement appropriate security controls for each phase and recognize anomalous behavior that may be associated with one or many phases of an attack.

- **Increasingly sophisticated security analytics.** Once security organizations understand what to look for, the next step is to ensure that they are collecting and analyzing the right data that can provide these critical indicators of compromise. It should be noted that many organizations find themselves overwhelmed by security data with no clue about how to derive meaning from it. To avoid this "garbage-in, garbage-out" situation, it is worthwhile to invest in analyst training, work with services experts, and plan to implement big data security analytics in phases over time.
- **Specific anti-malware defenses on networks and endpoints.** This guideline seems intuitive because many organizations are already proceeding down this path. In order to "stop the bleeding," enterprises need modern anti-malware defenses that include network gateways and modern anti-malware detection/prevention engines like Malwarebytes on endpoints and servers. These investments should produce near-term ROI benefits as they can be implemented quickly to immediately increase protection.

Smart CISOs will weigh all new security technologies against available resources for testing, implementation, and ongoing operations. The best technologies will address anti-malware requirements with highly tuned intelligence, algorithms, and automation.