ThreatTrack Security

Malware Analysts Have the Tools to Defend Against Cyber-Attacks, But Challenges Remain

Summary

While many malware analysts said they have all the tools they need to properly protect their companies against cyber-attacks, a disturbing number of internal challenges prohibit those analysts from completely defending their networks from malware and other sophisticated threats.

Malware analysts believe they have the right tools to defend against cyber-attacks, and protecting against those threats is easier than compared with a year ago, but they sometimes still face internal challenges that hinder efforts to keep their company networks clean.

Among the issues that malware analysts face: more than half said they've had to remove malware from the device of a member of senior leadership because the executive clicked on a malicious link in a phishing e-mail, while nearly 40% had to remove malware after a senior executive visited an infected pornographic website.

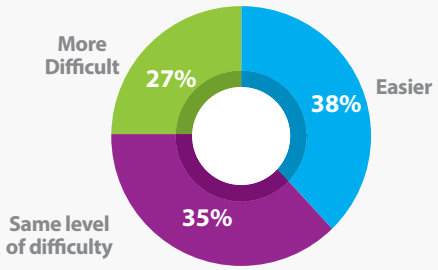
A ThreatTrack Security study of malware analysts from U.S. enterprises in October 2013 also reveals that more than half of the malware analysts surveyed said they have investigated or addressed a data breach that the company did not disclose to customers, partners or other stakeholders.

The findings highlight some behind-the-scenes struggles that many malware analysts still face. It's hard enough trying to protect against threats coming from outside the company's walls, but when senior executives hinder those efforts or don't communicate data breaches publicly, it makes it even more difficult.

It's Gotten Better

It's not all bad news, however. In fact, malware analysts said their ability to defend against malware and other cyber threats has actually improved over the past year. About 38% of malware analysts said it's gotten easier to defend their company's network from cyber-attacks compared to only 27% who said it has become more difficult, according to the study. Another 35% said their capability to defend against cyber-attacks has stayed about the same.

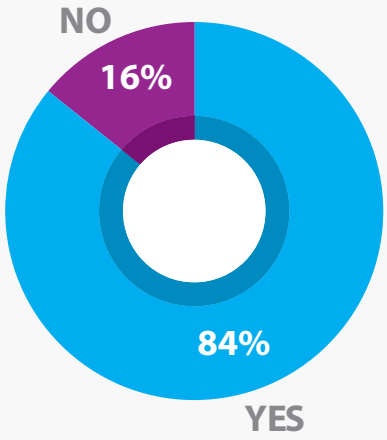
HOW HAS MALWARE DEFENSE CHANGED IN LAST YEAR?



It's become easier for malware analysts to defend their organization against malware attacks compared to last year.

One reason malware analysts might be better at stopping cyber-attacks is because they have the solutions necessary to become aware of incoming threats. Almost 84% of respondents believe they have the tools to properly defend their organization from an advanced malware attack.

HAVE THE TOOLS TO FIGHT MALWARE?



Malware analysts believe they have the tools they need to fight cyber threats.

One such weapon that the malware analysts are using to their advantage is an Incident Response Team (IRT). In the study, 86.5% of the analysts work for a company that has an IRT in place to identify, react to and remediate cyber-attacks launched against their network, including Advanced Persistent Threats (APTs), Zero-day attacks and other sophisticated malware.

As you might expect, larger companies are more likely to have an IRT in place, with 92% of malware analysts with companies with more than 500 employees having a dedicated team, according to the study. In the same vein, companies with higher IT security budgets were more likely to be able to invest in an IRT. About 98% of malware analysts with enterprises with IT security budgets of at least $200,000 have a response team to activate in the event of a potential threat.

Phishing, Families & Porn

While it's great news that malware analysts feel they have the tools needed to defend against cyber-threats, sometimes those teams might be put to work because their own senior executives' PCs get avoidable malware infections.

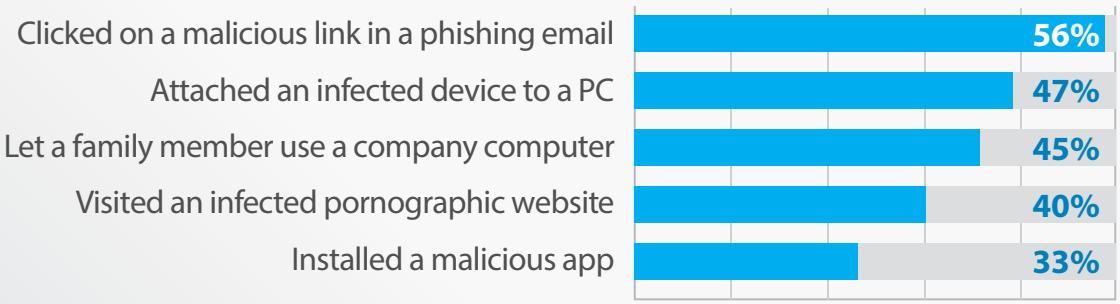
According to the study, 56% of the malware analysts have had to remove malware from their companies' senior leaders' PCs after those leaders infected their own devices by clicking on a malicious link in a phishing email.

Another 47% said they have removed malware from a PC because of an infected USB drive or a smartphone that a senior executive attached to the PC, and 45% of the malware analysts said senior execs have let family members use company-owned devices that led to malware infection.

And then there's the porn. Almost 40% of malware analysts said they've removed malware from senior executives' devices after those leaders visited an infected pornographic website.

Only 14% said they've never been asked to remove malware from an executive's computer or mobile device.

REMOVING MALWARE FROM SENIOR LEADERSHIP'S PC OR MOBILE DEVICES

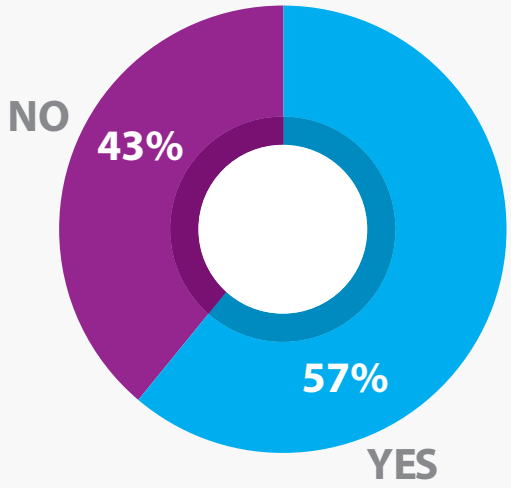


Senior leadership can't seem to keep their devices clean from malware, whether it's because of phishing emails or visiting porn sites.

Hiding The Truth?

While it may be interesting—and perhaps amusing—that malware analysts admit to cleaning their bosses' machines for things the bosses should know better not to do, it's a much more serious finding that 57% of the analysts said they've investigated or addressed a data breach that the company ultimately did not disclose to customers, partners or other stakeholders.

NOT DISCLOSED A DATA BREACH?



More than half of malware analysts say their organizations have not disclosed data breaches to customers, partners or other stakeholders.

While the European Union has stringent requirements about reporting data breaches, the United States laws are not as strong, often depending on the state, industry and other factors. The number of data breaches in the U.S. might be vastly underreported if companies aren't as forthcoming as they could or perhaps should be.

In the study, malware analysts from large enterprises said their orginization did not disclose a data breach to customers than analysts from smaller companies. Nearly two-thirds (66%) of analysts from organizations with more than 500 employees didn't disclose a data breach, compared to 18% of malware analysts from companies with less than 50 employees. Of course, larger companies pose a bigger target to malware creators than do smaller companies because of their larger presence in the market and more information they possess.

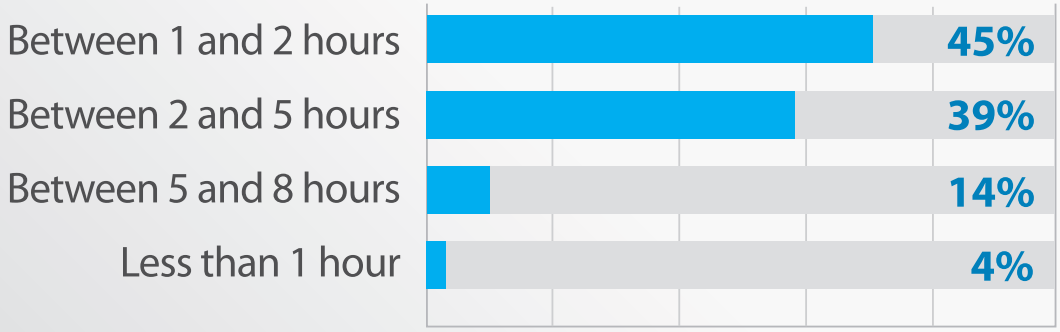
Among industries, manufacturing and utility companies were the industries most likely not to disclose a breach, with 79% of respondents admitted to not telling customers, partners or other stakeholders about a compromise. Other industries in which more than half of respondents did not disclose data breaches include IT and Telecom (57%) and healthcare (56%).

The findings also varied dramatically by size of IT security budget. About 76% of companies that spend between $500,000 and $10 million on IT security said they haven't disclosed data breaches to customers. Less than 30% of companies with IT security budgets under $500,000 failed to disclose breaches, while 37.5% of companies with IT budgets of more than $10 million didn't close breaches.

Analyzing Malware

Meanwhile, when malware analysts do get a sample to analyze, almost 45% cited an analysis time between one and two hours, while another 39% said analyzing malware samples takes between two and five hours. Another 14% said analysis takes between five and eight hours, while only 4% said it takes less than one hour.

HOW LONG TO ANAYLZE A MALWARE SAMPLE?



Only 4% of malware analysts said they can analyze a sample in under an hour.

The study highlights the need for more automated malware analysis tools, such as sandboxes, in the market. Analysis of a malware sample can be completed in a matter of minutes with an automated malware analysis sandbox. On the other hand, it can take days to investigate especially complex samples for malware analysts who have to analyze samples manually.

The lack of an automated malware analysis tool was cited as a pain point by 35% of respondents, with regards to defending their organization from sophisticated threats.

The most difficult aspects of defending an organization from advanced malware are the complexity of the malware (chosen by 67% of respondents) and the volume of malware attacks (67%), according to the study.

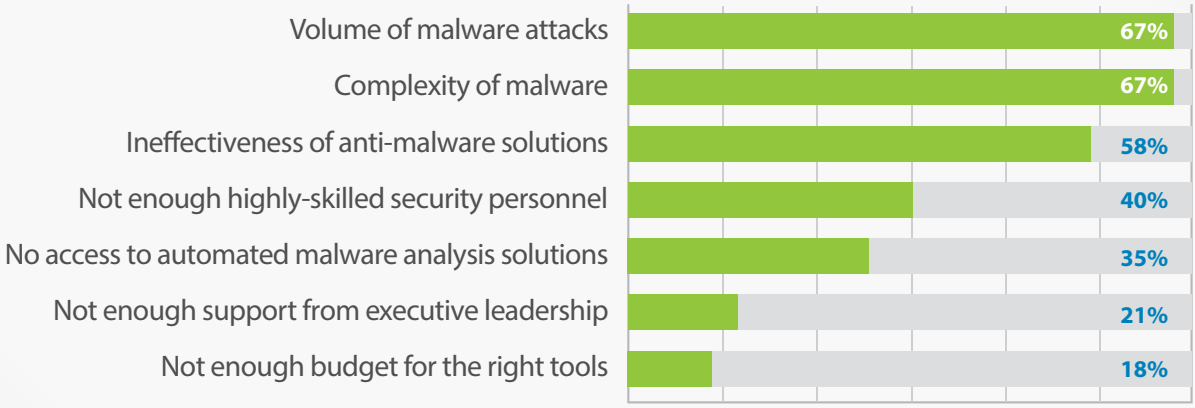
what's happening, with senior executives who let family members use corporate PCs and can't keep away from pornographic websites.

And then there are the undisclosed data breaches. Not only are unreported compromises doing a disservice to customers, they may even be inhibiting proper attention that needs to be placed on the cybersecurity industry in general. If it were mandated that all breaches be reported, you might see more notice—and more funding—be given to advanced malware protection solutions.

Study Methodology

This independent, blind survey of 200 malware analysts at U.S.-based enterprises by Opinion Matters on behalf of ThreatTrack Security in October 2013.

COMPLEXITY, VOLUME OF MALWARE ATTACKS ARE MOST DIFFICULT



The volume and complexity of malware are the most difficult aspects of defending an organization against malware, while finding executive support and budget for the right tools are not big problems.

Meanwhile, 58% of malware analysts said the ineffectiveness of anti-malware solutions inhibited their ability to defend their organization, and 40% said they just don't have enough highly-skilled personnel on staff to effectively combat cyber-attacks.

Only 21% cited that they don't get enough support from executive leadership to fight malware, and only 18% said they don't have enough budget to do so.

Conclusion

Malware analysts and CISOs face enough challenges trying to protect their companies' networks from external threats. They certainly don't need internal forces hindering those efforts. Yet that seems to be

About ThreatTrack Security

ThreatTrack Security Inc. specializes in helping organizations identify and stop Advanced Persistent Threats (APTs), targeted attacks, Zero-day threats and other sophisticated malware designed to evade the traditional cyber-defenses deployed by enterprises around the world.

ThreatAnalyzer, ThreatTrack Security's malware analysis sandbox, is used by government security, defense and intelligence agencies, making it an integral component of the U.S. cybersecurity infrastructure.

More information on ThreatTrack Security can be found at www.ThreatTrackSecurity.com.