Anatomy of Data-Stealing Malware:

A Study of Enterprise Security & IT Security Practitioners

Sponsored by Trend Micro

Conducted by Ponemon Institute LLC

October 15, 2009

Anatomy of Data-Stealing Malware

Ponemon Institute, October 15, 2009

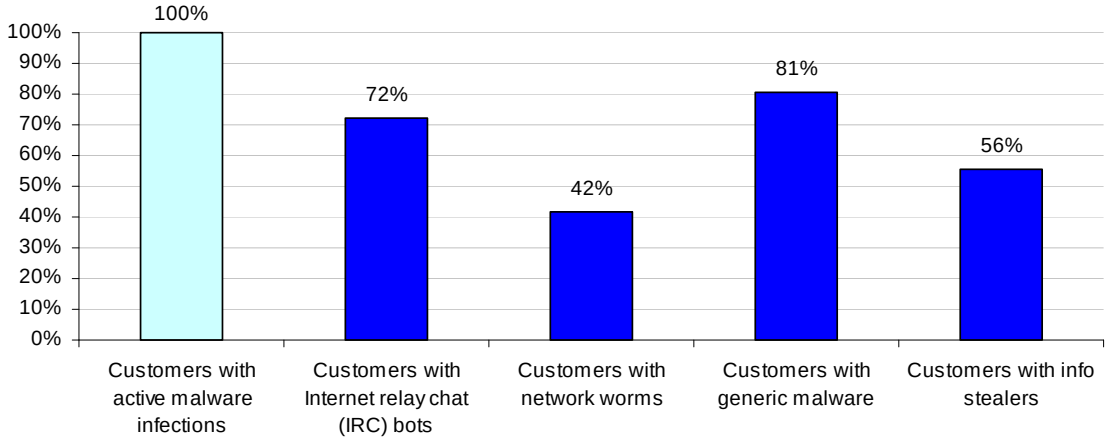
Executive Summary

We are pleased to present *The Anatomy of Data-Stealing Malware* study conducted by Ponemon Institute and sponsored by Trend Micro. The purpose of the study is to gauge the views of enterprise security practitioners[1] about the inherent risks posed by malware. Specifically, we contrast these views with actual, rigorously compiled security assessment results. In the context of this study, malware is defined as software designed to infiltrate a computer or network to damage computer systems or steal information without the owner's knowledge or informed consent.

About assessments: Trend Micro conducted onsite security assessments for 130 enterprise organizations throughout the world. Ponemon Institute independently analyzed these assessments to determine the types and frequency of malware residing within corporate systems.[2] An objective of these assessments was to learn if security practitioners' perceptions of the malware threat reflect the reality of active malware infections actually present in corporate networks.

The security assessment uses on-site technology to monitor corporate network traffic for the presence of active malware that is attempting to contact external parties or propagate within the network. Bar Chart 1 summarizes the results. As can be seen, all assessed organizations had one or more active malware infections that had evaded detection. While generic malware was the most frequent type of infection, more serious threats – including IRC bots (72 percent), Info stealing malware (56 percent) and network worms (42%) – were present in large numbers. These assessment results suggest that most organizations worldwide have active malware infections that may not be readily detected.

Bar Chart 1
Summary of security assessments



About the survey: The 754 IT security respondents who participated in our survey are all from organizations that experienced one or more malware infections in the past year. Our sample of

[1] Our survey sample involved both IT and IT security practitioners. For brevity, we refer to this group as security practitioner or respondent interchangeably.
[2] The assessments conducted by Trend Micro used Trend Micro Threat Management Services technology and threat analysts to evaluate the extent to which corporate networks and systems were infected with active malware that had thus far evaded detection.

respondents is bifurcated into two subgroups – namely, 631 who reported their organizations had experienced only ordinary or non-data-stealing malware (a.k.a. the generic malware group) and 123 whose organizations had experienced data-stealing malware infections (a.k.a. the data-stealing malware group).

The survey addressed the following topics:

- The difference in perceptions among respondents whose organization experienced a malware-caused data loss and those organizations that believed they had only generic malware infections.
- The seriousness of malware infections to organizations' sensitive and confidential data.
- The number of infected endpoints that constitute a serious threat.
- The impact of a malware attack on an organization's data.
- Detection and remediation of a malware infection.

Following are the 10 most salient findings from our research.

1. **Security assessments provide compelling evidence that data-stealing malware is a persistent threat in many organizations globally**. Assessments show the rate of seriously infected endpoints in organizations is much higher than is estimated by security practitioners who participated in the survey. All assessed companies had active resident malware. And, a majority of these networks hosted one or more data stealers.

2. **Respondents underestimate the frequency of data-stealing malware infections within their own organizations**. Assessment data shows that 56 percent of participating organizations had one or more data-stealing malware infections. However, only 11 percent of individuals in the survey were aware of experiencing a data-stealing malware infiltration in their own companies.

3. **Respondents recognize that even a small number of infected endpoints can pose a very significant security threat**. While judging their own endpoint infection rate to be approximately 10 percent, the majority of security practitioners believe that a 5 percent endpoint infection rate creates opportunities for serious data loss or theft. Fifty-six percent of the data-stealing malware group believes that even a one percent infection rate poses a serious risk of data loss.

4. **Despite concerns about data-stealing malware, a large number of respondents are uncertain about how their organizations' networks were infiltrated.** Over 42 percent of respondents who experienced data-stealing malware are not confident of their organization's ability to determine the root cause of a specific infection. Twenty-five percent of these individuals say their organizations cannot determine when a specific infection happened.

5. **Respondents who experienced a data-stealing malware incident say that their organizations sensitive or confidential information was at risk**. More than 66 percent say customer or consumer information was exposed by a malware bot attack. Forty-one percent say non-financial confidential business data was lost or stolen by malware.

6. **Despite uncertainty about the frequency of data-stealing malware, respondents see it as a significant threat that is not diminishing over time.** This is especially true for those in the data-stealing malware group. Over 65 percent of this group reports that an incident posed a serious or very serious threat to their organizations.

7. **Overall, there are significant differences in perceptions among respondents who experienced data-stealing malware from those who only experienced generic malware**. Overall survey results suggest that respondents who experienced data stealers (31 percent) are much more likely to see malware as a very significant threat to their organizations than

those who only experienced generic or ordinary malware (19 percent).

8. **Respondents recognize that their organizations can do a better job in preventing malware infections.** Specifically, 81 percent of security practitioners that experienced data-stealing malware say their organizations' security protections against future infection is either inadequate or can be improved.

9. **Respondents generally agree that additional tools are needed to detect and quickly remediate serious malware threats such as data stealers**. Over 58 percent of security practitioners who experienced data stealing malware say it is important or very important to have leading-edge software tools to help detect and prevent continuing infections.

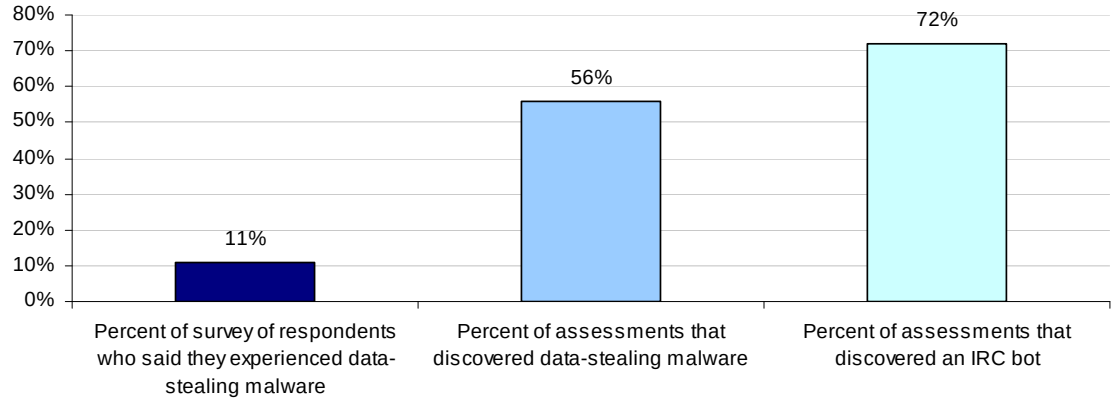
10. **Respondents see cyber criminals or negligent employees as the two greatest sources of malware infections in their organizations**. According to 52 percent of security practitioners, the agent most likely to infect an organization's network is a malicious outsider (a.k.a. cyber criminal). Thirty-nine percent of respondents say the most likely sources of infection are employees who unknowingly introduce malware into networks and systems either through infected endpoints (such as PCs and other mobile data-bearing devices) or insecure Internet or email activities.

Our findings are organized into four parts: Part 1 is about awareness of the malware risk, Part 2 is the anatomy of a malware infection, Part 3 compares the data-stealing malware group to the malware group and Part 4 summarizes the assessment results. Please note that most of the results are displayed in chart or table format.

Part 1: Awareness of the malware risk

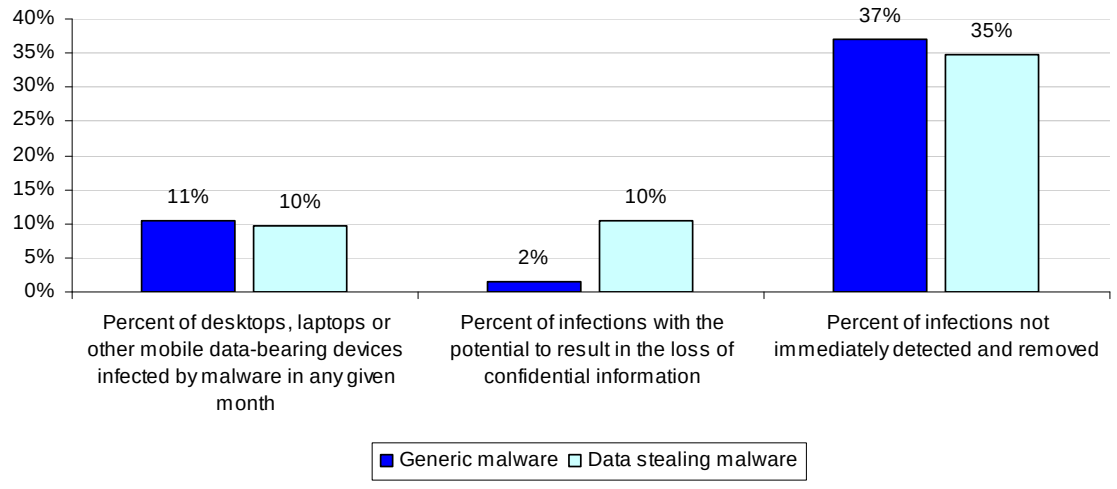
The risk posed by malware is underestimated by security practitioners in our study. Only a small number of companies responding to our survey (11 percent) believe they have experienced a data-stealing malware infection. However, as shown in Bar Chart 2, more than 56 percent of assessed corporate systems had one or more active data-stealing malware infections. In addition, 72 percent of assessed corporate systems experienced one or more IRC (Internet Relay Chat) bots. These IRC bots are also very dangerous because they operate in stealth and are often used to seize and send confidential information to malicious outsiders.

Bar Chart 2
Comparison of survey to assessment results on the frequency of data-stealing malware



Bar Chart 3 shows the respondents' experience with malware infections. As reported, both groups say that the percentage of infected endpoints within their organizations at any one time is about 10 or 11 percent. Of these in infected endpoints, only 2 percent are believed to be data-stealing malware, according to respondents in the generic malware group. Respondents in the data-stealing malware group are five times more likely (10 percent) to see a given infection as data-stealing. These findings suggest that practitioners experienced with data-stealing malware are more cognizant of the possibility that any given malware infection can result in data loss.

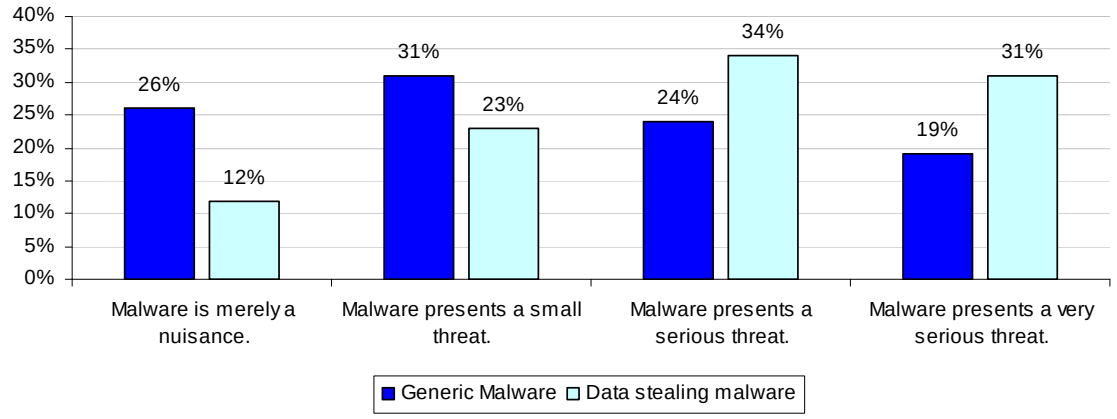
Bar Chart 3
Experience with malware infections



As shown in the above bar chart, 37 percent of the generic malware group and 35 percent of the data-stealing malware group believe that these infections are not immediately detected and removed – thus increasing potential exposure to their organizations.

Malware is considered a serious or very serious threat that is not diminishing in most companies. Bar Chart 4 reports that 65 percent of the data-stealing malware group and 43 percent of the generic malware group believe malware represents a serious or very serious threat to their organizations. In contrast, 57 percent of the generic malware group sees malware as merely a nuisance or a small threat as compared to 35 percent of the data-stealing malware group.

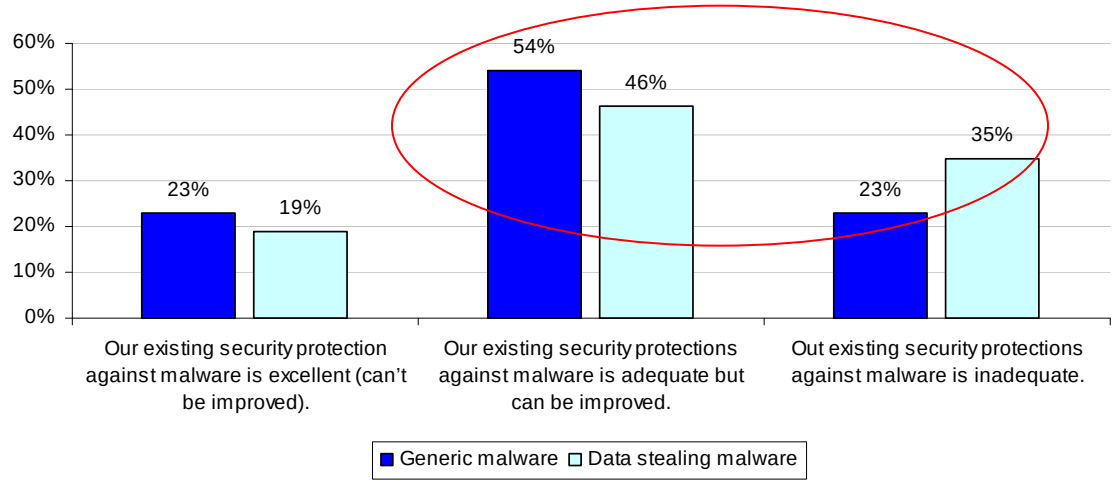
Bar Chart 4
Perceived seriousness of the malware threat



Consistent with the above findings, practitioners in the data-stealing malware group appear to be more sensitive to the risks posed by malware infections.

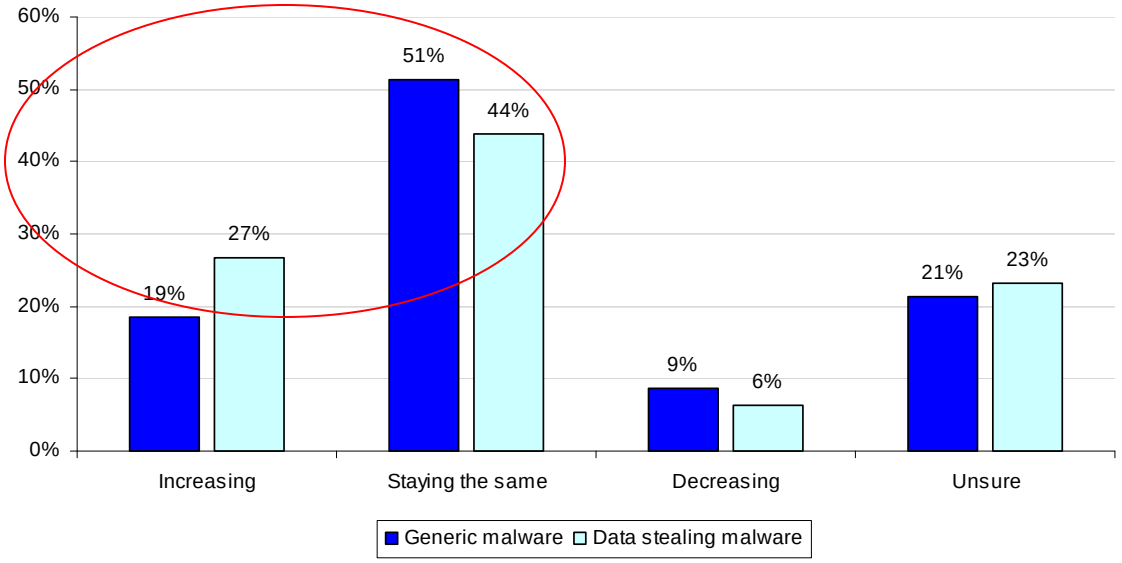
According to Bar Chart 5, 81 percent of the data-stealing malware group and 77 percent of the generic malware group believe security protections against malware infections are either inadequate or can be improved.

Bar Chart 5
Adequacy of existing security protections against malware



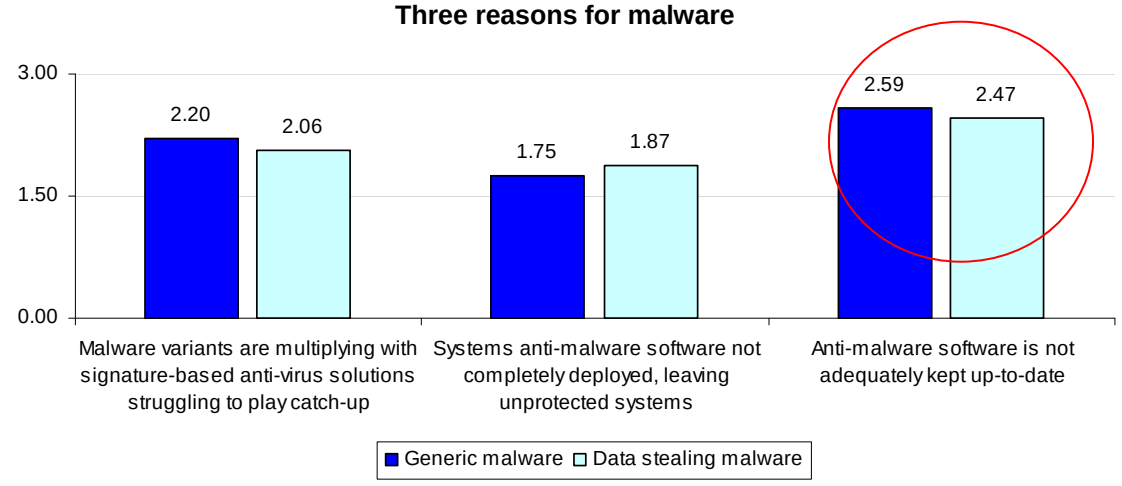
Despite the plethora of anti-malware solutions, Bar Chart 6 reports 71 percent of the data-stealing malware group and 70 percent of the generic malware group believe the malware threat is either increasing or staying the same (stable) over time.

Bar Chart 6
The malware threat changes over time



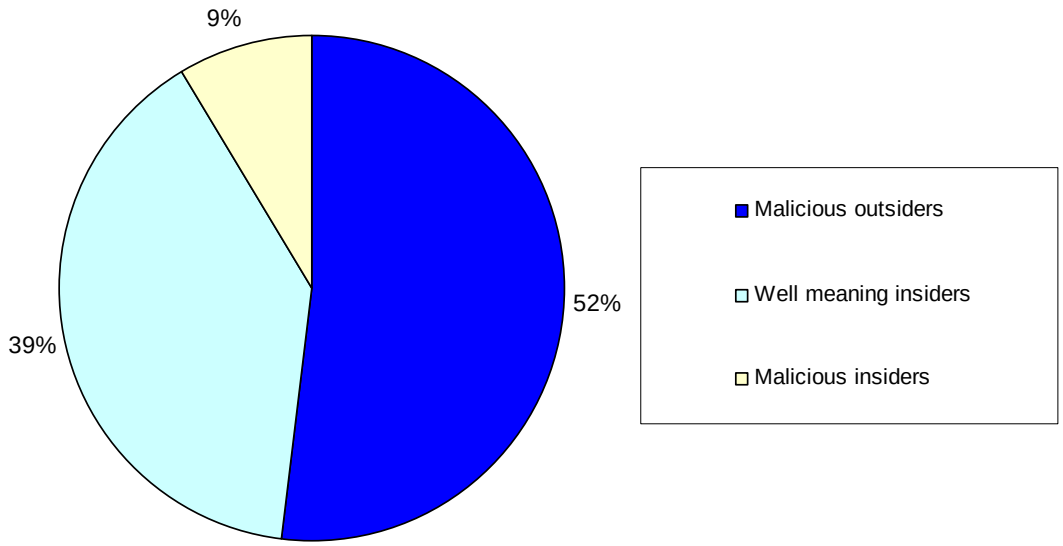
Bar Chart 7 shows how respondents rank three reasons for malware infections (where highest rank is three). As can be seen, "anti-malware software that is not adequately kept up-to-date" has the highest rank – 2.59 for generic and 2.47 for the data-stealing malware groups, respectively.

Bar Chart 7
Three reasons for malware



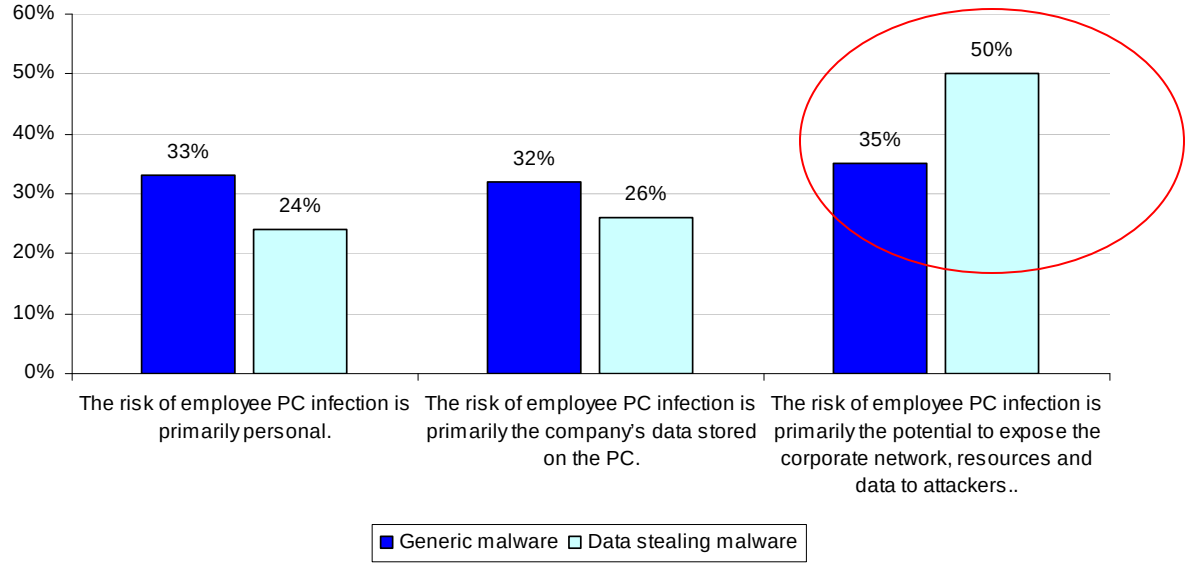
Cyber criminals and negligent employees pose the greatest risk. According to 52 percent of the data-stealing malware group, the agent most likely to infect an organization's network with malware is the malicious outsider directly hacking into systems, followed by well meaning but negligent insiders (39 percent) who unknowingly introduce malware through insecure Internet applications or email attachments. These results are summarized in Pie Chart 1.

Pie Chart 1
Most likely to infect your organization's network or enterprise system



Bar Chart 8 shows 50 percent of the data-stealing malware group is most concerned that an employee's PC infection has the potential to expose the corporate network, resources and data to hackers. In contrast, only 35 percent of the generic malware group shares this concern. Twenty-six percent of the data-stealing malware group and 32 percent of the generic malware group believe employee-infected PCs only put the data stored on the PC at risk (i.e., no network penetration).

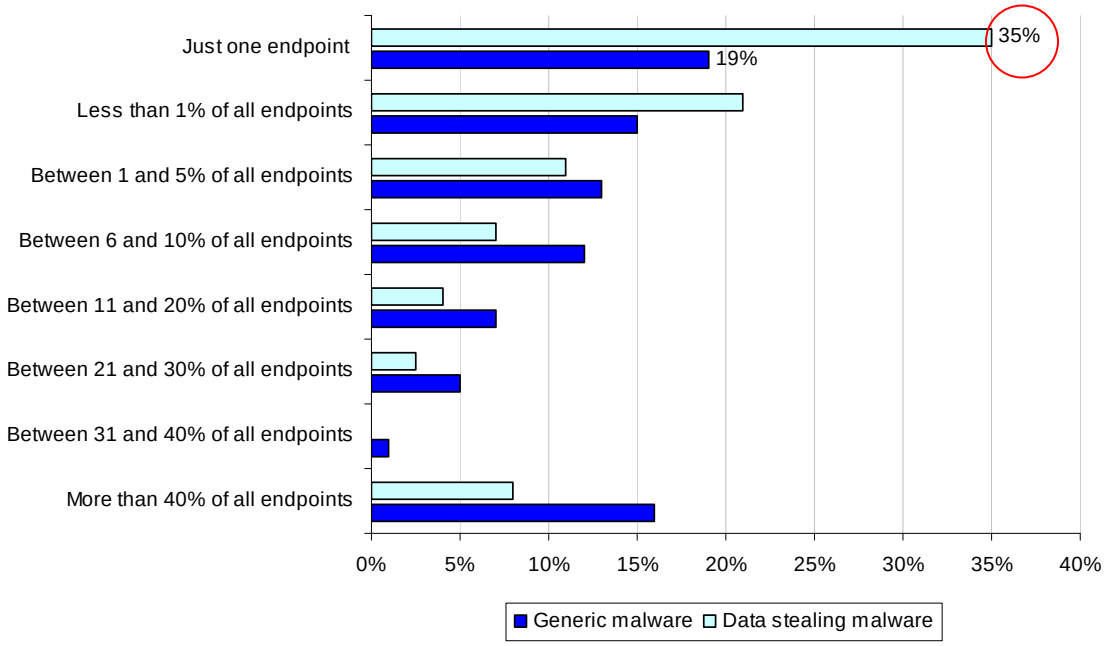
Bar Chart 8
Risk of a malware infection



Even a small number of infected endpoints can bring about very significant data security consequences for organizations. As noted in Bar Chart 9, respondents acknowledge that a very small percentage of infected desktops, laptops or other mobile data-bearing devices create

an opportunity for data loss or theft. Thirty-five percent of respondents in the data-stealing malware group believe that if even one endpoint contained malware infections, there could be a high likelihood that data loss or theft will occur.

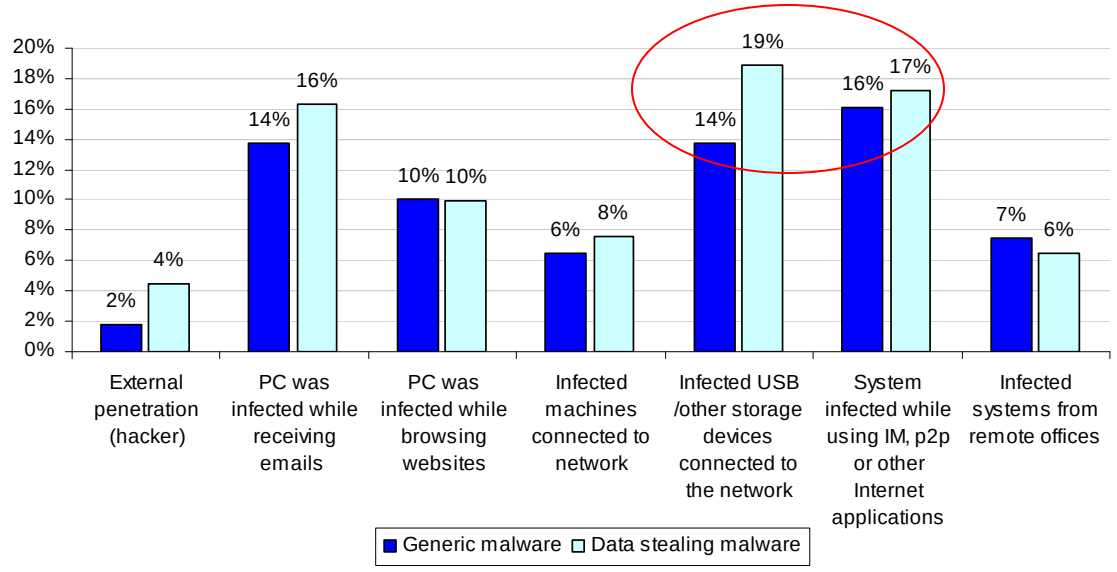
Bar Chart 9
Minimum infected endpoints deemed significant



Part 2: Anatomy of data-stealing malware

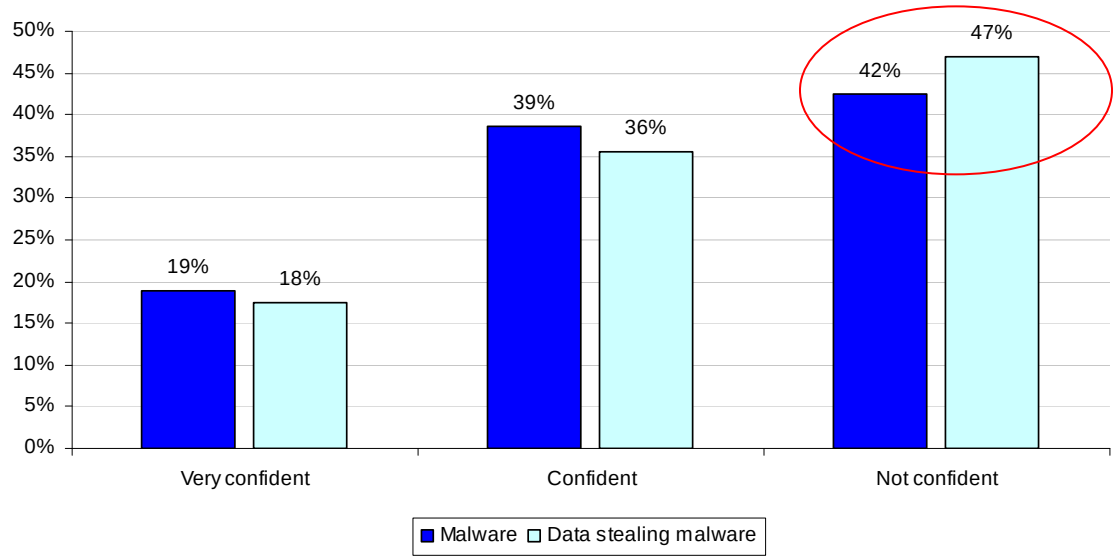
There is uncertainty about the root cause of malware attacks. Bar Chart 10 reports the scenarios that cause malware infections that ultimately penetrate corporate networks. As can bee seen, 19 percent of the data-stealing malware group sees the use of infected USB-connected devices as the most likely cause of network infiltration. For the generic malware group, 16 percent see the most likely cause of malware infiltration as insecure Internet applications such as instant messaging and peer-to-peer software.

Bar Chart 10
Root causes of the malware attack



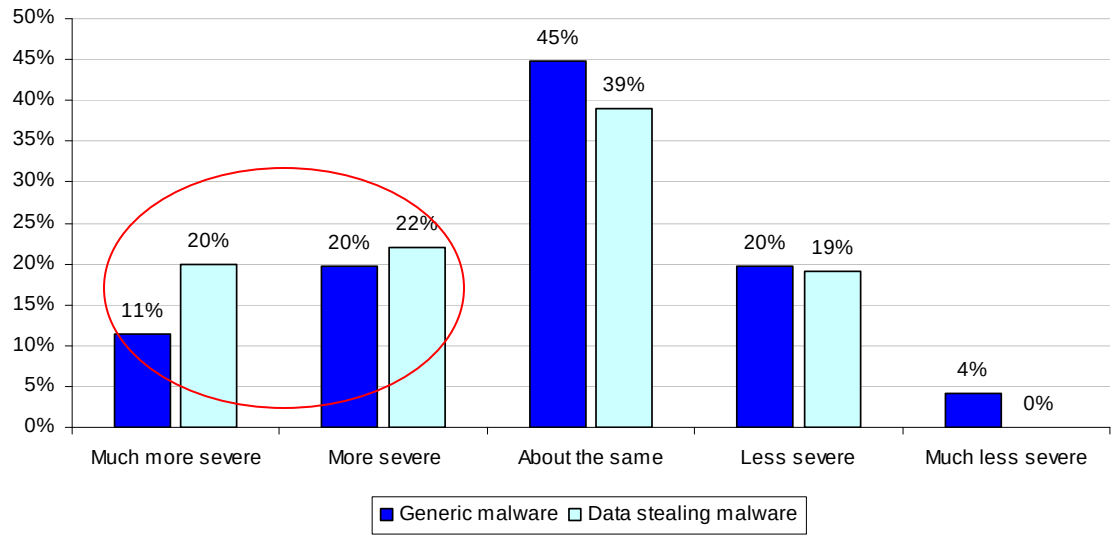
As shown in Bar Chart 11, 47 percent of the data-stealing malware group and 42 percent of the generic malware group are <u>not</u> confident about the source or root of malware infiltrations.

Bar Chart 11
Confidence level about knowing the source of malware attacks



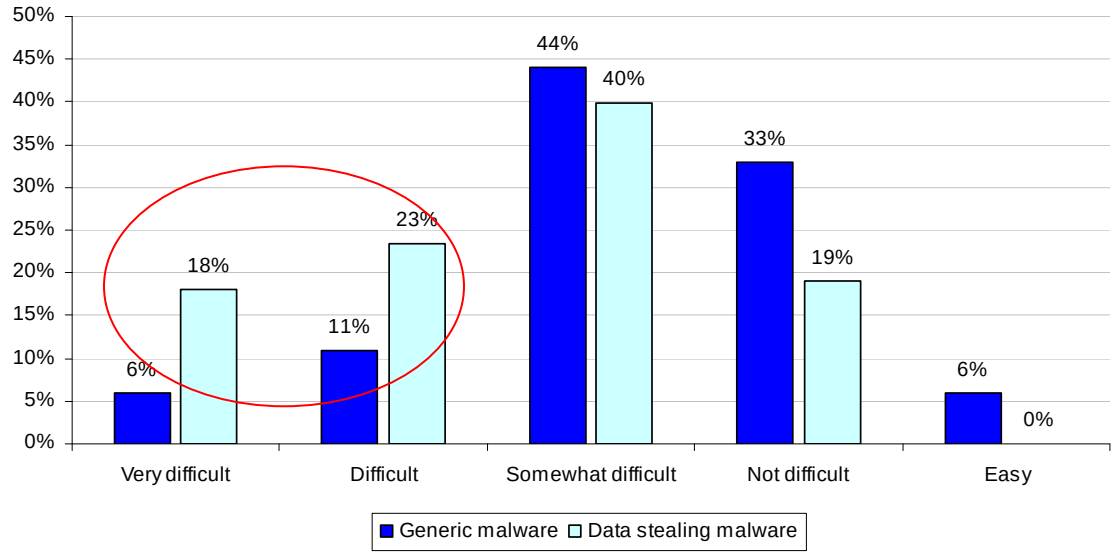
When asked to rate the severity of malware infections their organization experienced in the past year, 42 percent of the data-stealing malware group and 31 percent of the generic malware group say it was more severe or much more severe than other security threats experienced by them.

Bar Chart 12
Severity of the malware attack



Detection is after the fact and difficult. Bar Chart 13 shows 41 percent of the data-stealing malware group says malware was difficult or very difficult to detect. Only 6 percent of the generic malware group and none in the data-stealing malware group say detection was easy.

Bar Chart 13
Difficulty of detection

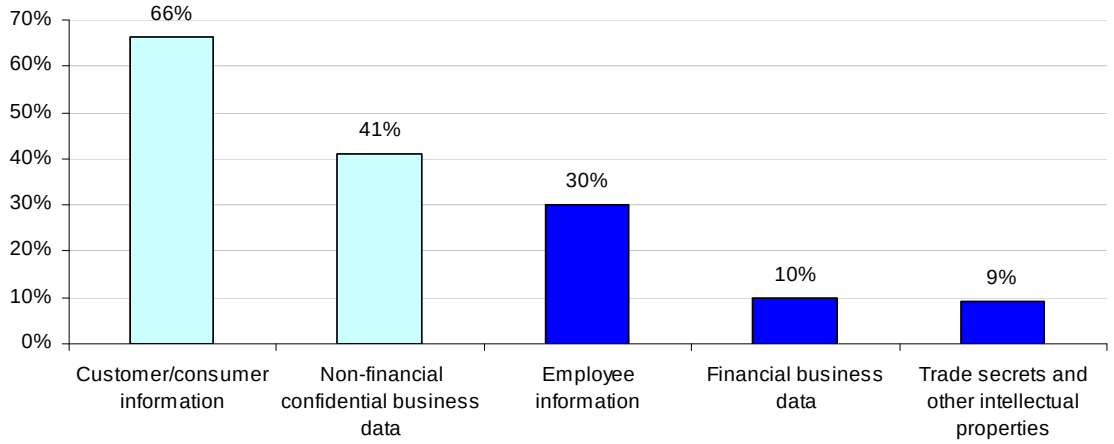


While not shown in the above bar chart, 16 percent of the malware group and 24 percent of the data-stealing malware group say they could not get rid of the infection completely. The largest percentage of respondents in both groups (33 percent in the generic malware group and 36

percent in the data-stealing malware group) learned about the attack after the infection had occurred.

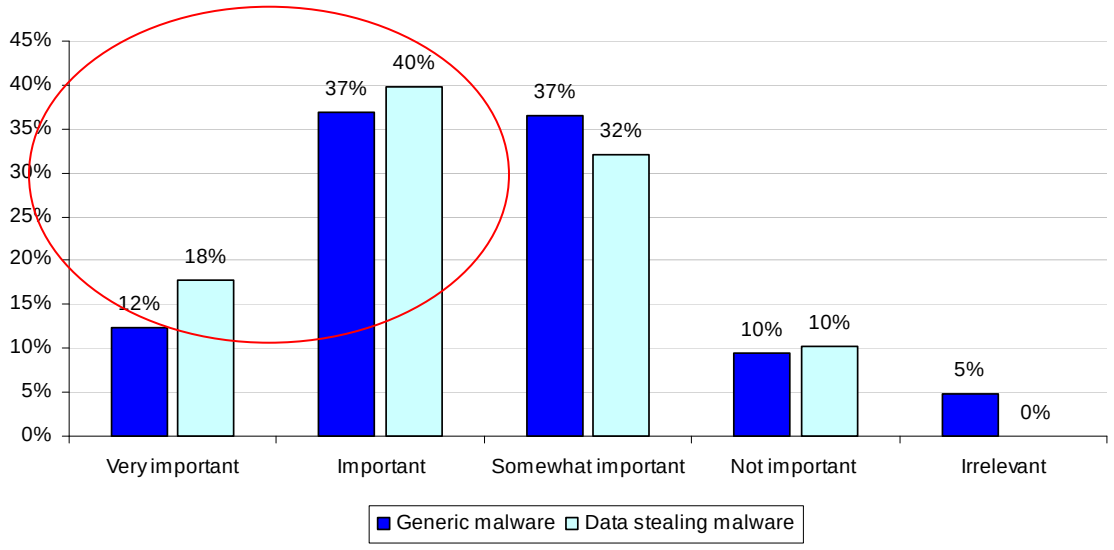
What information is most at risk? As reported in Bar Chart 14, data-stealing malware targets a wide array of sensitive or confidential business information, especially customer and consumer information (66 percent) and non-financial confidential business data (41 percent).

Bar Chart 14
Data compromised by malware



Additional tools and services are needed to detect and remediate serious malware threats. As shown in Bar Chart 15, 58 percent of the data-stealing malware group and 49 percent of the malware group believe it would be important or very important to manage malware threats with advanced tools that help diagnosis malware threats real-time.

Bar Chart 15
Are additional software tools important?



While not shown in a chart, 63 percent of the data-stealing malware group and 51 percent of the generic malware group would like to have a tool that reported the percentage frequency and source of malware infections experienced by their organization in a clear, consistent and comprehensive way.

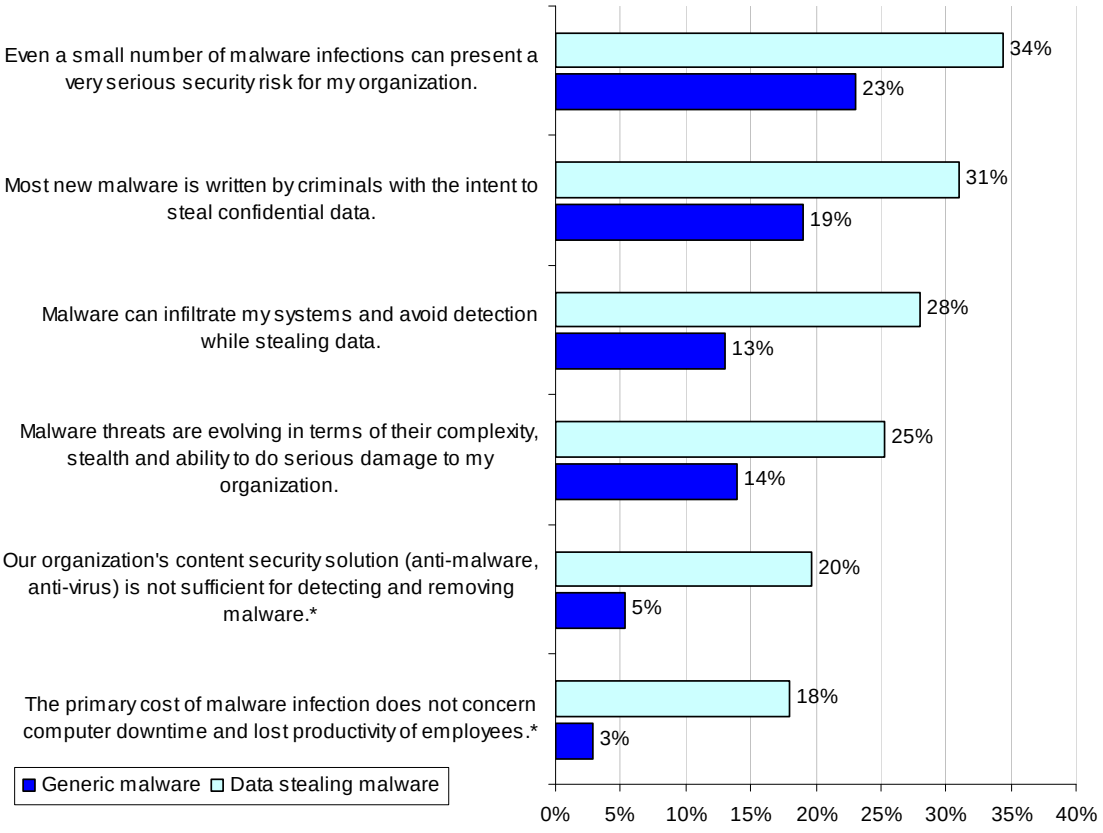
Part 3: Attributions about the data-stealing malware and the generic malware groups

The data-stealing malware group is more likely to see malware as a threat. Bar Chart 16 reports the strongly agree response to seven attributions about the risks caused by malware infections. As can be seen, there are significant differences between these two groups.

Specifically, 41 percent of the generic malware group versus 30 percent of the data-stealing malware group believe the primary cost of a malware infection concerns downtime and lost productivity. Forty percent of the generic malware group versus 27 percent of the data-stealing malware group believes that their organization's content security solution (anti-malware software) is sufficient for detecting and removing malware.

In contrast, 34 percent of the data stealing malware group versus 23 percent of the generic malware group believe that even a small number of malware infections can present a very serious security risk. More than 31 percent of the data-stealing malware group versus 19 percent of the generic malware group believes that new malware is written by criminals with the intent to steal confidential data.

Bar Chart 16
Differences between generic malware and data-stealing malware group
Each bar reflects the percentage strongly agree* to each attribution



*Attribution is reversed scored (where strongly disagree = strongly agree).

Bar Chart 16 reports six attributions concerning the negative impact of malware infections on organizations. As can be seen, respondents in the data-stealing malware group are more likely to "strongly agree" with each statement than respondents in the generic malware group. Specifically, members of the data-stealing malware group are more likely to see even a small number of malware infections as a serious risk. They are also more likely to believe new malware

threats concern cyber criminals intending to steal confidential data. Similarly, they see malware threats as evolving in terms of complexity, stealth and the ability to do serious damage to their organization. Finally, the data-stealing malware group is less likely to believe their organization's existing anti-malware solutions adequately detect or remove malware infections.

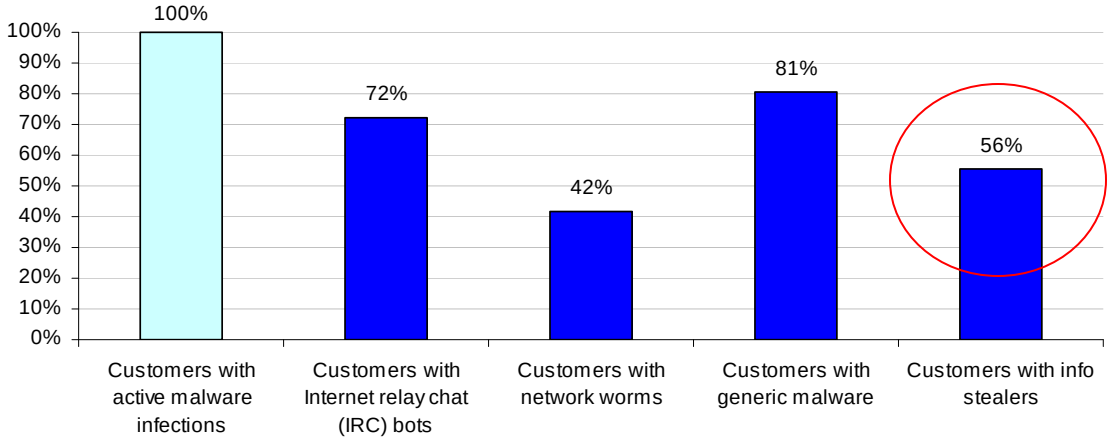
Part 4: Analysis of assessments for Trend Micro

The Trend Micro security threat assessments used Trend Micro Threat Management Services technology and threat analysts to evaluate the extent to which corporate networks and systems were infected with active malware that had thus far evaded detection. The data is based on 130 enterprise organizations worldwide, averaging over 7,000 employees.

Ponemon Institute's independent analysis of Trend Micro's assessment of malware infections supports the findings from this research. As revealed in the assessment, all 130 enterprise organizations have malware infections – that is, a 100 percent infection rate.[3]

As previously reported, Bar Chart 17 shows 56 percent of infected endpoints contain an info stealer (a.k.a. data-stealing malware). Hence, the data-stealing malware group is correct in their perceptions that infection will most likely lead to the loss of sensitive data. Following are additional statistics from the security assessments conducted by Trend Micro.

Bar Chart 17
Summary of security assessments



Certain industries and regions had higher occurrences of malware downloads, data-stealing malware and IRC bots. Table 1 summarizes the industry assessment findings.[4]

Table 1 **Assessments by industry**	Rate of infected endpoints	Rate of IRC bots	Rate of network worms	Rate of generic malware	Rate of Info stealer
Communications	100%	100%	100%	0%	0%
Education	100%	89%	28%	78%	67%
Entertainment	100%	100%	0%	100%	50%
Financial services	100%	64%	27%	64%	36%
Government	100%	85%	37%	78%	52%
Healthcare	100%	40%	80%	90%	50%
Manufacturing	100%	66%	48%	97%	72%
Other	100%	71%	29%	71%	29%
Retail	100%	64%	45%	82%	55%
Services	100%	57%	57%	71%	57%
Transportation	100%	80%	20%	80%	60%

[3] An infection occurs whenever one or more endpoints contain malware.
[4] Please note that the sub-sample sizes of industry segments are too small to render statistical inferences.

The highest rates of malware downloads occur in services, education and manufacturing. The highest rates of data-stealing malware occur in manufacturing, education and transportation. The highest rates of IRC bots occur in communications, entertainment, education and government.

Table 2 **Assessments by global region**	Rate of infected endpoints	Rate of IRC bots	Rate of network worms	Rate of generic malware	Rate of Info stealer
North America	100%	72%	20%	76%	48%
Japan	100%	64%	27%	82%	27%
Asia-Pacific	100%	64%	48%	89%	67%
Latin America	100%	93%	54%	68%	54%
EMEA	100%	67%	33%	67%	0%

Table 2 shows the rate of infections in different global regions. Albeit a small sub-sample, the highest rate of malware downloads occurs in EMEA, North America and Asia-Pacific. The highest rates of data-stealing malware occur in Asia-Pacific, Latin America and North America. The highest rates of IRC bots occur in Latin America, North America and EMEA.

Conclusion & recommendations

Malware is at the heart of serious threats to the security of sensitive data. It is encouraging that 81 percent of the data-stealing malware group and 80 percent of the malware group believe malware ranks at least the same in severity as other threats, or is more severe or much more severe.

Although awareness about the risk of malware seems to be growing, the pervasiveness of the threat is underestimated. This is revealed in the gap between the existing infections in 130 companies and the perceptions respondents have about the extent of infections in their organizations.

As was revealed in our study, employee ignorance or negligence can cause serious malware threats to the organization. In fact, the most likely scenario, according to respondents, is malware downloaded from an employee's web browsing or company email. Hackers are also considered a major reason for malware infections.

The following are recommendations for addressing the malware threat:

- Organizations need a discovery and remediation service to augment their existing security measures. Sixty-three percent of the data-stealing malware group and 51 percent of the malware group would like to have a tool that reported the percentage frequency and source of malware infections experienced by their organization in a clear, consistent and comprehensive way.

- Organizations need to conduct a malware assessment as part of their data protection strategy. Active malware can penetrate even the most secure environments.

- Organizations need to conduct enterprise-wide training on the threat of malware. Awareness should focus on the risks identified as most likely to cause an infection: malware downloaded from an employee's web browsing or company/private email or downloaded from an insecure USB or other mobile devices.

- According to respondents, there is a great deal of uncertainty about the ability to detect an infection and to identify its root cause or source. For this reason, we believe it is critical for every organization to conduct an enterprise assessment. As also revealed, respondents were not confident that they were able to completely eliminate the infection. Understanding first where the infections are located and the source of the infections will help protect your organization from a data-stealing malware infection.

As Ponemon Institute research has shown, a data breach can be costly to an organization as well as damaging to its reputation. A serious risk to organizations' sensitive and confidential data is malware. The recommendations described above, can help organizations address this threat and protect one of its most valuable assets—customer and business confidential information.

Method

A random sampling frame of 17,495 adult-aged individuals who reside within the United States was used to recruit participants to this survey. Our randomly selected sampling frame was selected from national lists of security practitioners. A bifurcated sampling plan was used to compare two sub-samples: respondents who have experienced data-stealing malware and those who have only experienced generic malware.

A two-step discovery sampling procedure was employed to ensure an adequate sample size for respondents who stated they had experienced data-stealing malware.[5] Accordingly, the generic malware sub-sample was captured over a four day period, while the data-stealing malware sub-sample was collected over 10 days.

In total, 845 respondents completed the survey. Of the returned instruments, 91 surveys failed reliability checks. A total of 754 surveys were used as our final sample, of which 631 were in the generic malware group and 123 was in the data-stealing malware group. This combined sample represents a 4.3 percent net response rate.

Table 3 **Sampling response**	Freq.
Sampling frame	17495
Total sample (before reliability)	845
Response rate (before reliability)	4.8%
Total sample (final)	754
Response rate (final)	4.3%
Generic malware sub-sample (group)	631
Data-stealing malware sub-sample (group)	123

Screening questions were used to ensure a high sample quality. The sample size after screening questions was 579 respondents in the generic malware group and 109 respondents in the data-stealing malware group.

Ninety-five percent of respondents completed all survey items within 20 minutes. Table 4 reports the respondent's organizational level. As can be seen, a majority of respondents are at or above the supervisory level. The average experience for respondents in the generic malware and data-stealing malware groups is 9.4 years and 9.8 years, respectively.

Table 4 **Organizational level**	Generic Malware	Data-stealing malware
Senior Executive	0%	0%
Vice President	2%	0%
Director	14%	16%
Manager	23%	24%
Supervisor	20%	19%
Associate/Staff	16%	17%
Technician	23%	24%
Other	2%	1%
Total	100%	100%

[5] We anticipated that the data-stealing malware group would be much smaller. After four days, the total number of respondents who stated they experienced data-stealing malware was about 11% of the total sample results collected of this time period.

Table 5 reports the respondents' primary reporting channels. As can be seen, a large number of respondents report through the IT organization (CIO or CTO) rather than compliance, security or risk management.

Table 5 **Primary reporting channel**	Malware	Data-stealing malware
Chief Information Officer (CIO)	55%	54%
Chief Technology Officer (CTO)	17%	18%
Chief Security Officer	15%	19%
Chief Risk Officer	5%	4%
Compliance Officer	4%	7%
Chief Financial Officer	2%	0%
Human Resources VP	1%	0%
Other	1%	0%
Total	100%	100%

Table 6 reports the respondent organization's headcount. As shown, a majority of respondents work within companies with more than 5,000 employees.

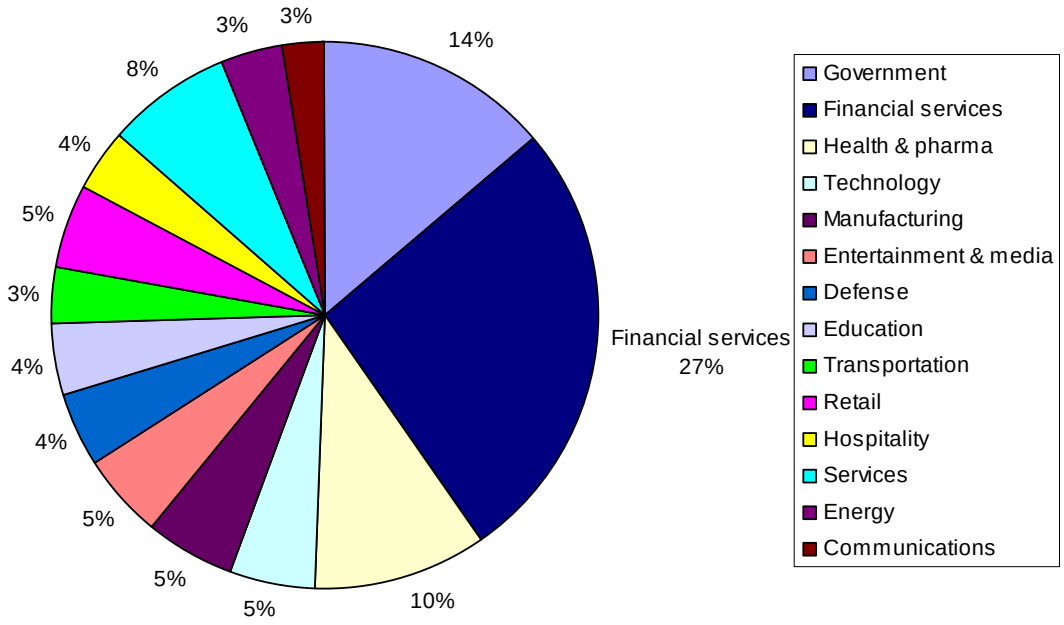
Table 6 **Respondents' organization headcount**	Malware	Data stealing malware
Less than 500	12%	10%
501 to 1,000	8%	8%
1,001 to 5,000	16%	15%
5,001 to 10,000	24%	23%
10,001 to 25,000	22%	23%
25,001 to 75,000	17%	16%
More than 75,000	3%	4%
Total	100%	100%

In total, 34 percent of respondents are female and 66 percent male. Table 7 reports the location of respondents according to six U.S. regions.

Table 7 **Regional location of respondents**	Malware	Data stealing malware
Northeast	20%	19%
Mid-Atlantic	19%	18%
Midwest	16%	17%
Southeast	14%	15%
Southwest	12%	12%
Pacific	19%	19%
Total	100%	100%

Pie Chart 2 reports the percentage distribution of respondents by major industry sector. As shown below, 27 percent of respondents work for financial service companies such as banks, insurance, credit card, brokerage, and others. Over 14 percent of respondents are employed in federal, state, or local governmental organizations. Another 10 percent are employed in healthcare and pharmaceutical companies.

Pie Chart 2
Industry distribution of the combined sample



Caveats to this study

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

- Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.
- Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are IT or IT security practitioners. We also acknowledge that the results may be biased by external events such as media coverage. We also acknowledge bias caused by compensating subjects to complete this research within a holdout period. Finally, because we used a web-based collection method, it is possible that non-web responses by mailed survey or telephone call would result in a different pattern of findings.
- Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide a truthful response.

Please contact research@ponemon.org or call us at 800.877.3118 if you have any questions.

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the **Council of American Survey Research Organizations (CASRO),** we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.