Second Annual State of Ransomware Report: Survey Results for Australia

An Osterman Research Survey Report

Published July 2017

Sponsored by Malwarebytes
# TABLE OF CONTENTS

**Executive Summary** ............................................................................................................. 1  
  - The Aftermath of Ransomware .......................................................................................... 1  
  - Attitudes About Paying Ransomware ............................................................................. 1  
  - Ransomware Technology Trends .................................................................................... 2  
  - About This Survey Audience .......................................................................................... 2  

**Ransomware is a Critical Problem** ....................................................................................... 3  
  - Ransomware in the Context of Other Security Threats .................................................. 3  
  - How Common are Ransomware and Other Threats? ...................................................... 4  
  - Confidence in Addressing the Ransomware Problem .................................................... 5  

**How Organizations Respond to Ransomware and How They’re Impacted** ....................... 6  
  - The Impacts of Ransomware Can be Devastating .......................................................... 6  
  - How Does Ransomware Enter an Organization? ............................................................. 10  
  - How Does IT Respond to Ransomware? ......................................................................... 11  
  - Amounts That Cyber Criminals Have Demanded and Responses to These Demands .... 12  
  - Should Organizations Pay Ransomware Demands? ...................................................... 15  

**The Importance of Addressing the Ransomware Problem** .................................................. 17  
  - The Need to Solve the Ransomware Problem ................................................................. 17  
  - Is Solving Ransomware a Human or Technology Issue? .............................................. 18  
  - The Role of Security Awareness Training .................................................................... 19  
  - Technologies/Processes in Place to Address Ransomware .......................................... 20  

**About Malwarebytes** .......................................................................................................... 21
EXECUTIVE SUMMARY

This survey report presents the results of a survey undertaken in Australia as part of a larger survey of organizations in five additional geographies – the United States, the United Kingdom, France, Germany, and Singapore – on ransomware and other critical security issues. The survey was conducted with small- to mid-sized businesses during June 2017 with 179 organizations in the United States and 175 in each of the other five nations. In order to qualify for participation in the survey, respondents had to be a) responsible and/or knowledgeable about cybersecurity issues within their organization, and b) the organizations surveyed could have no more than 1,000 employees. A total of 22 questions were included in the survey. Results from the other surveys are available in separate national and regional survey reports.

THE AFTERMATH OF RANSOMWARE

- **The impact of ransomware on small to mid-sized businesses can be very damaging**
  Among small to mid-sized Australian organizations that have experienced a successful infiltration of the corporate network by ransomware, 22 percent reported that they had to cease business operations immediately (identical to the global average), and 18 percent lost revenue (higher than the global average).

- **Ransom demands aren’t the biggest problem with ransomware – it’s downtime**
  We found that for more than four in five of the Australian organizations that were infected with ransomware, the ransom demanded was $1,000 or less. In fact, only four percent of ransom demands were in excess of $10,000 and none were for more than $50,000. However, our research also found that for 24 percent of impacted organizations, a ransomware infection caused 25 or more hours of downtime, with some organizations reporting that it caused systems to be down for more than 100 hours. The amount of high levels of ransomware-induced downtime for Australian organizations was higher than the global average of 17 percent.

- **For many, the source of ransomware is not known**
  Nearly one-third (31 percent) of the Australian organizations we surveyed did not know the cause of their most severe ransomware infection. Among those that could identify the source of the infection, it was most often a malicious link in an email (22 percent) or a malicious email attachment (18 percent).

- **Ransomware infections often spread to other endpoints once they take hold**
  Our research found that in many ransomware attacks the infection is not limited to a single endpoint, but can spread to others, as well. In fact, in some cases the infection spread to every endpoint on the network. Organizations in Australia were much more likely than the global average to see ransomware infections spread to more than just the initial endpoint that was infected, but not every endpoint; whereas these organizations were just as likely as the global average to experience every endpoint on the network become infected.

ATTITUDES ABOUT PAYING RANSOMWARE

- **Most small to mid-sized businesses do not believe in paying ransomware demands**
  We found that a sizeable majority of respondents believe that ransomware demands should never be paid, while most of the remaining organization believe they should be paid if the encrypted data is of value to the organization. Only a tiny minority believe that ransom demands should always be paid.

- **Not paying ransom often results in lost files**
  We found that among Australian organizations that did not pay the ransom that was demanded of them, 40 percent lost files, significantly higher than the global average.

- **Most organizations make addressing ransomware a high priority, but they don’t have the confidence that their defenses are adequate**
  Most Australian organizations give a high or very high priority to addressing the ransomware problem, but they view it less seriously than is the case globally. For example, 61 percent of the Australian organizations surveyed versus 75 percent globally view addressing ransomware this seriously. Australian organizations are willing to invest in resources, technology and funding to address the problem, but only 54 percent compared to 67 percent globally consider it to be a high or very high priority. Moreover, many Australian organizations are willing to invest in
education and training about ransomware for end users, but only 47 percent are making it a
higher or very high priority compared to 53 percent globally.

Despite these investments, nearly three in five of the Australian organizations surveyed
expressed little to only moderate confidence in their ability to stop a ransomware attack. In fact,
only eight percent of organizations surveyed felt “very confident” in their ability to thwart
ransomware attacks, lower than the global average of 10 percent.

RANSOMWARE TECHNOLOGY TRENDS

- Small to mid-sized businesses believe fighting ransomware is more about technology
  than user training
  When asked if ransomware should be addressed only through technology or only through
  training, more Australian organizations believe the former will be more effective in addressing
  the ransomware problem, which is consistent with the global view that technology is more
effective. Although the remaining 83 percent of survey respondents believe that a mix of
technology and training are necessary, Australian organizations tilt decidedly toward technology-
based approaches as the more effective method of dealing with ransomware.

- Current anti-ransomware technology does not seem to be enough
  Our research found that organizations have implemented a variety of solutions to address their
  ransomware concerns, either before or after the fact. These include traditional email security
  solutions, regular backups to be able to restore to a known good state, network segmentation,
  and ransomware-specific solutions, either on-premises and/or in the cloud. However, having
  these defenses in place does not seem to be enough. While more than one-third of small to mid-
sized businesses in Australia claim to be running anti-ransomware technologies (higher than the
  global average for both on-premises and cloud-based solutions), 31 percent of businesses
  surveyed still experienced a ransomware attack.

ABOUT THIS SURVEY AUDIENCE
The distribution of industries surveyed in Australia is shown in Figure 1. These organizations had a
mean of 401 employees and 269 email users.

<table>
<thead>
<tr>
<th>Industry</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturing</td>
<td>14%</td>
</tr>
<tr>
<td>Engineering/Construction</td>
<td>12%</td>
</tr>
<tr>
<td>Retail/E-commerce</td>
<td>11%</td>
</tr>
<tr>
<td>High tech</td>
<td>9%</td>
</tr>
<tr>
<td>Education</td>
<td>7%</td>
</tr>
<tr>
<td>Food/Agriculture</td>
<td>7%</td>
</tr>
<tr>
<td>Transportation</td>
<td>7%</td>
</tr>
<tr>
<td>Financial services/Banking/Insurance</td>
<td>6%</td>
</tr>
<tr>
<td>Healthcare</td>
<td>6%</td>
</tr>
<tr>
<td>Government</td>
<td>4%</td>
</tr>
<tr>
<td>Hospitality</td>
<td>3%</td>
</tr>
<tr>
<td>Pharmaceutical</td>
<td>3%</td>
</tr>
<tr>
<td>Law enforcement</td>
<td>1%</td>
</tr>
<tr>
<td>Other</td>
<td>11%</td>
</tr>
</tbody>
</table>

Source: Osterman Research, Inc.
A U S T R A L I A

RANSOMWARE IS A CRITICAL PROBLEM

RANSOMWARE IN THE CONTEXT OF OTHER SECURITY THREATS

Ransomware is an increasingly serious issue, and the problem is getting worse over time. As shown in Figure 2, ransomware is a "top four" problem for organizations in Australia, cited by 58 percent of those surveyed as a problem about which they are "concerned" or "extremely concerned" (significantly lower than the global average of 69 percent). Our research found that the average level of concern about the issues shown in Figure 2 (those indicating that they are "concerned" or "extremely concerned") was within a fairly tight band across all of the geographies we surveyed, ranging from a low of 51.9 percent in Germany to a high of 58.5 percent in the United States. However, the range for the concern over ransomware varied more significantly, from a low of 57.7 percent in Australia to a high of 78.9 percent in France.

Figure 2
Concern About Various Security Threats
Percentage Responding Concerned or Extremely Concerned

<table>
<thead>
<tr>
<th>Security Threat</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware infiltration through email</td>
<td>79%</td>
</tr>
<tr>
<td>Malware infiltration via web browsing</td>
<td>73%</td>
</tr>
<tr>
<td>Phishing through email</td>
<td>70%</td>
</tr>
<tr>
<td>Ransomware</td>
<td>58%</td>
</tr>
<tr>
<td>Phishing through social media</td>
<td>44%</td>
</tr>
<tr>
<td>Insider theft of data</td>
<td>41%</td>
</tr>
<tr>
<td>Physical theft of laptops and mobile devices</td>
<td>20%</td>
</tr>
</tbody>
</table>

Source: Osterman Research, Inc.
HOW COMMON ARE RANSOMWARE AND OTHER THREATS?
As shown in Figure 3, most organizations in Australia have experienced various types of security attacks and data breaches over the past year, with many organizations experiencing some type of security-related incident on a more than monthly basis. Also of note is that 31 percent of organizations have experienced a ransomware attack during the last 12 months, with most of those having been victimized seeing anywhere from one to five such attacks during the past year. The Australian companies we surveyed actually rank a bit better globally, with 31 percent of Australian companies victimized versus 35 percent globally.

Figure 3
Attacks, Breaches and Ransomware Infiltrations During the Previous 12 Months

Source: Osterman Research, Inc.
CONFIDENCE IN ADDRESSING THE RANSOMWARE PROBLEM

Organization confidence among decision-makers about their ability to stop a ransomware attack is not very high. As shown in Figure 4, 15 percent of organizations has little confidence that they can stop a ransomware attack that has infiltrated their network, and another 44 percent are only “somewhat” confident in their ability to stop such attacks. Only 41 percent of organizations are “fairly” or “very” confident that they can thwart a ransomware attack. Compared to the global results, Australian companies are less confident: 15 percent of Australian companies with no confidence versus 11 percent globally, and 44 percent somewhat confident versus 35 percent.

Figure 4
Level of Confidence That a Ransomware Attack Can be Stopped

Source: Osterman Research, Inc.
HOW ORGANIZATIONS RESPOND TO RANSOMWARE AND HOW THEY’RE IMPACTED

THE IMPACTS OF RANSOMWARE CAN BE DEVASTATING

The impact of ransomware can be damaging to an organization. As shown in Figure 5, our research found that while most of the ransomware incidents that have been experienced involved just the endpoint, more than 47 percent of these infections spread to other devices, and for two percent of organizations the ransomware infection impacted every device on the network. The spread of ransomware was higher among Australian companies than across many of the other six geographies we surveyed. For example, while the spread of ransomware to every device on the network in Australia was equal to the global average of two percent, “only” 35 percent of organizations globally experienced a spread of ransomware beyond the original entry point versus 47 percent in Australia.

The survey found some level of variability in the proportion of endpoints that were infected by the most serious ransomware infection that had impacted organizations. For example, organizations in Germany and the United States experienced the greatest proportion of network/every endpoint-wide infections at 5.0 percent and 4.3 percent, while no organizations surveyed in France or Singapore reported ransomware infections that impacted every device on the network. By contrast, 68.3 percent of French organizations reported that only a single endpoint was infected by the most severe ransomware infection they had experienced, whereas this figure was only 50.7 percent for Australian organizations.

Source: Osterman Research, Inc.
Infections from ransomware attacks create a wide range of consequences. As shown in Figure 6, individuals whose computers were infected (or who suffered the follow-on impacts of a co-worker or colleague being infected) felt the impact of ransomware by losing access to their files, which happened to nearly two-fifths of the companies infected with ransomware. However, for 22 percent of organizations, their business stopped immediately, either because they had to deal with the infection and/or because they lost access to critical files needed to keep the business operational. Other impacts from ransomware included lost revenue, employees using personally owned devices like smartphones and tablets instead of corporate systems and, in extreme cases, lives were endangered from the ransomware infection.

Figure 6
Impact of the Most Serious Ransomware Attack That Has Been Experienced

<table>
<thead>
<tr>
<th>Impact Description</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>People were personally impacted (customers, students, vendors, staff, etc.)</td>
<td>39%</td>
</tr>
<tr>
<td>It stopped business immediately</td>
<td>22%</td>
</tr>
<tr>
<td>We lost revenue</td>
<td>18%</td>
</tr>
<tr>
<td>Employees used personally owned smartphones, tablets or laptops because corporate systems were down</td>
<td>14%</td>
</tr>
<tr>
<td>Lives were endangered</td>
<td>2%</td>
</tr>
</tbody>
</table>

Source: Osterman Research, Inc.

The impact of ransomware was on par with the global average in Australia in the context of things like stopping business immediately, but slightly higher in terms of the personal impact it had on lost revenue (18 percent in Australia versus 15 percent globally) and ransomware victims (39 percent in Australia versus 37 percent globally).
AUSTRALIA

As shown in Figure 7, about one-fifth of organizations in Australia that fell victim to ransomware had fewer than one percent of their endpoints infected, while over half had up to 25 percent infected. However, the remaining one-quarter had more than 25 percent of their endpoints infected. The situation in Australia was similar to the global outcome: 26 percent of Australian and global organizations had more than one-quarter of their endpoints infected in their most serious ransomware attacks.

Figure 7
Proportion of Endpoints Infected in the Most Serious Ransomware Attack That Has Been Experienced

<table>
<thead>
<tr>
<th>Proportion</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1%</td>
<td>20%</td>
</tr>
<tr>
<td>1% to 25%</td>
<td>55%</td>
</tr>
<tr>
<td>26% to 50%</td>
<td>15%</td>
</tr>
<tr>
<td>51% to 75%</td>
<td>7%</td>
</tr>
<tr>
<td>76% to 99%</td>
<td>4%</td>
</tr>
<tr>
<td>100%</td>
<td>0%</td>
</tr>
</tbody>
</table>

Source: Osterman Research, Inc.
Ransomware-induced downtime is a major consequence for many ransomware infections because an infected endpoint becomes immediately unavailable. A rapid restoration of an infected endpoint can minimize downtime, but as shown in Figure 8, fast recovery from ransomware is not common, with most experiencing anywhere from one day to almost two weeks of downtime from a ransomware attack.

Our research found that only 13 percent of organizations had minimal downtime resulting from ransomware, but more than one-sixth of organizations experienced anywhere from one to eight hours of downtime. However, it gets much worse: 71 percent of organizations infected by ransomware experienced nine or more hours of downtime, with four percent of organizations finding that they were down more than 100 hours because of the infection, which was twice the global average.

Source: Osterman Research, Inc.
**AUSTRALIA**

**HOW DOES RANSOMWARE ENTER AN ORGANIZATION?**

The most commonly cited source of a ransomware infection was unknown, followed by a malicious link in an email. As shown in Figure 9, nearly one in five organizations could trace their ransomware infection to an email attachment. Other sources included a business application, malicious web site or web application, a social media tool or a USB stick.

**Figure 9**
Manner by Which Malware Entered in the Most Serious Ransomware Attack That Has Been Experienced

<table>
<thead>
<tr>
<th>Source</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>We don't know</td>
<td>31%</td>
</tr>
<tr>
<td>Link in an email</td>
<td>22%</td>
</tr>
<tr>
<td>Email attachment</td>
<td>18%</td>
</tr>
<tr>
<td>Business application</td>
<td>11%</td>
</tr>
<tr>
<td>A Web site or Web application other than email or social media</td>
<td>11%</td>
</tr>
<tr>
<td>Social media</td>
<td>5%</td>
</tr>
<tr>
<td>USB stick</td>
<td>2%</td>
</tr>
</tbody>
</table>

*Source: Osterman Research, Inc.*
HOW DOES IT RESPOND TO RANSOMWARE?

The length of time that elapses between the initial ransomware infection and its detection is critical to stopping the spread of the infection. As shown in Figure 10, only seven percent of Australian organizations could detect a ransomware infection in five minutes or less. Another 35 percent could do so more in no more than one hour after an endpoint was infected, but more than 58 percent of the organizations surveyed in Australia required many hours or even a full day before they detected the problem. The results we discovered among organizations in Australia was slightly worse than the overall global results, but not by much.

Figure 10
Time Elapsed Before Detection in the Most Serious Ransomware Attack That Has Been Experienced

Source: Osterman Research, Inc.
Most ransom demands from cyber criminals are fairly small: as shown in Figure 11, about 81 percent of these demands of small to mid-sized businesses ask for less than $1,000. However, some cyber criminals ask for much larger sums, with 19 percent asking for more than $1,000 and four percent demanding up to $50,000. The results we found for organizations in Australia were moderately different than those we discovered in the other geographies, in that ransom quantities over $50,000 were not reported.

Source: Osterman Research, Inc.
Among organizations that were infected with ransomware, only about 45 percent opted to pay the ransomware demands, as shown in Figure 12. However, we found significant variability between the geographies that we surveyed. For example, only 16 percent of French and 17 percent of German organizations opted to pay the ransom demanded after their most severe ransomware infection, but 21 percent of American and 43 percent of British organizations opted to do so. Companies in the Australia were significantly more likely to pay ransomware demands than the global average (45 percent versus 28 percent).

Figure 12
Was Ransom Paid in the Most Serious Ransomware Attack That Has Been Experienced?

Source: Osterman Research, Inc.
Among Australian-based organizations that chose not to pay cyber criminals’ ransom demands, about two-fifths lost files as a result of their decision not to pay, as shown in Figure 13. Here, too, we found significant variability among the organizations based on geography. For example, British and Australian organizations experienced the greatest degree of file loss from their decision not to pay – 46 percent and 40 percent, respectively. Organizations in Germany and France were the least likely to lose files from their decision not to pay ransom demands. American organizations’ experience in losing or not losing files after not paying the ransom exactly matched the global average.

**Figure 13**
Were Files Lost in the Most Serious Ransomware Attack That Has Been Experienced Among Organizations That Did Not Pay the Ransom?

Source: Osterman Research, Inc.
SHOULD ORGANIZATIONS PAY RANSOMWARE DEMANDS?
When infected by ransomware, decision makers face a difficult decision: should they pay the ransomware to recover their files and potentially increase their chances of being infected again by demonstrating a willingness to pay, or should they refuse to pay and suffer the consequences? As shown in Figure 14, the majority of organizations in Australia believe, at least in general, that organizations should not pay ransomware demands, and a small proportion believe this occurs each and every time they are infected. Organizations in Australia are on par with the global average in believing that organizations should always pay ransom demands.

Figure 14
Belief That Companies Should Pay Ransom Demands if They Are Hit With Ransomware

- 58%: No, never
- 40%: Yes, but it depends on what is encrypted and its value to the company
- 2%: Yes, always

Source: Osterman Research, Inc.
We also asked survey respondents to personalize the decision of whether or not to pay ransom demands. As shown in Figure 15, the results were largely the same about the decision to pay a ransom whether or not respondents were answering about organizations in general or their own organization. Organizations in Australia were less likely to tell us that they should always pay ransom demands (two percent versus three percent globally) and much more likely to consider whether payment should be evaluated on a case-by-case basis (46 percent versus 37 percent globally).

Figure 15
Do You Believe That Your Company Should Pay Ransom Demands If You Are Hit With Ransomware?

Source: Osterman Research, Inc.
THE IMPORTANCE OF ADDRESSING THE RANSOMWARE PROBLEM

THE NEED TO SOLVE THE RANSOMWARE PROBLEM

Decision makers are mostly in agreement that the ransomware problem needs to be solved and they are addressing it as a high priority. As shown in Figure 16, 61 percent of survey respondents give a "high" or "very high" priority to addressing the ransomware problem (lower than the global average of 75 percent); 54 percent give investing in resources, technology and funding to address ransomware as a "high" priority (versus 67 percent globally); and 47 percent consider that investing in user education and training about ransomware needs to be a "high" or "very high" priority (versus 53 percent globally).

Figure 16
Priorities for Addressing Various Aspects of the Ransomware Problem
Percentage Responding a High or Very High Priority

<table>
<thead>
<tr>
<th>Priority</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Addressing the ransomware problem</td>
<td>61%</td>
</tr>
<tr>
<td>Investing in resources, technology and funding to address</td>
<td>54%</td>
</tr>
<tr>
<td>ransomware</td>
<td></td>
</tr>
<tr>
<td>Investing in education and training about ransomware for your</td>
<td>47%</td>
</tr>
<tr>
<td>end users</td>
<td></td>
</tr>
</tbody>
</table>

Source: Osterman Research, Inc.
IS SOLVING RANSOMWARE A HUMAN OR TECHNOLOGY ISSUE?

The debate about how best to solve the ransomware problem is an ongoing issue: should the primary or only focus be on user training, or should the focus be primarily exclusively on a technology-oriented approach? As shown in Figure 17, the majority believe that training and technology are equally important factors in solving the ransomware problem. Another 12 percent of the organizations surveyed believe ransomware can be addressed properly only through a technology-focused approach, while another 30 percent believe that the problem is best addressed mostly using anti-ransomware technology. By contrast, 21 percent of respondents believe that the primary focus of anti-ransomware approaches should be directed toward training users.

Organizations in Australia are significantly more focused on technology than organizations globally. For example, while 39 percent of organizations globally believe that addressing ransomware is primarily a technology-focused issue versus 42 percent in Australia. The opposite is true with regard to security awareness training: 21 percent of Australian organizations believe in a primarily training-based approach to deal with ransomware versus 30 percent globally.

Figure 17
Extent to Which Organizations Believe That Solving the Ransomware Problem is a Human vs. Technology Issue

- We can only solve the ransomware problem through technology: 12%
- It’s mostly about technology, but training can help mitigate human-error: 30%
- Training and technology are equally important: 37%
- People are the weakest link in the security chain, but technology can help: 16%
- People are the weakest link in the security chain and good end-user training can solve the problem completely by eliminating human-error: 5%

Source: Osterman Research, Inc.
THE ROLE OF SECURITY AWARENESS TRAINING

As shown in Figure 18, seven percent of organizations in Australia do not conduct security awareness training that specifically addresses ransomware. Among the 93 percent of Australian organizations that conduct some form of training, most conducted ransomware-related security awareness training multiple times per year, with 27 percent of organizations offering this training at least two to three times per year. Despite the greater focus of organizations in Australia on security awareness training to deal with ransomware relative to the global results, slightly fewer organizations actually conduct this type of training today.

Figure 18
Do Employees Go Through Security Awareness Training that Specifically Mentions Ransomware and Frequency of This Training

Source: Osterman Research, Inc.
Most of the Australian-based organizations we surveyed have deployed email security to address ransomware and have implemented regular, on-premises backup of data so that they can restore ransomware-infected machines to a known good state as quickly as possible, as shown in Figure 19. Many organizations also have implemented network segmentation, on-premises ransomware-detection solutions, regular, cloud-based backup capabilities, the use of outsourced security providers, and cloud-based ransomware detection.

### Figure 19
Technologies and Processes in Place to Address Ransomware

<table>
<thead>
<tr>
<th>Technology</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email security that is installed on our servers,</td>
<td>85%</td>
</tr>
<tr>
<td>computers, etc.</td>
<td></td>
</tr>
<tr>
<td>Regular on-premises data backup to restore to</td>
<td>65%</td>
</tr>
<tr>
<td>a known good state</td>
<td></td>
</tr>
<tr>
<td>Network segmentation</td>
<td>62%</td>
</tr>
<tr>
<td>Ransomware-detection solutions on-premises</td>
<td>43%</td>
</tr>
<tr>
<td>Regular cloud-based backup to restore to a</td>
<td>41%</td>
</tr>
<tr>
<td>known good state</td>
<td></td>
</tr>
<tr>
<td>Outsourced service provider for security</td>
<td>35%</td>
</tr>
<tr>
<td>Ransomware-detection solutions in the cloud</td>
<td>25%</td>
</tr>
</tbody>
</table>

*Source: Osterman Research, Inc.*
ABOUT MALWAREBYTES

Malwarebytes is the next-gen cybersecurity company that millions worldwide trust. Malwarebytes proactively protects people and businesses against dangerous threats such as malware, ransomware, and exploits that escape detection by traditional antivirus solutions. The company’s flagship product combines advanced heuristic threat detection with signature-less technologies to detect and stop a cyberattack before damage occurs. More than 10,000 businesses worldwide use, trust, and recommend Malwarebytes. Founded in 2008, the company is headquartered in California, with offices in Europe and Asia, and a global team of threat researchers and security experts. For more information, please visit us at http://www.malwarebytes.com/.

Malwarebytes founder and CEO Marcin Kleczynski started the company to create the best disinfection and protection solutions to combat the world’s most harmful Internet threats. Marcin was recently named “CEO of the Year” in the Global Excellence awards and has been named to the Forbes 30 Under 30 Rising Stars of Enterprise Technology list and the Silicon Valley Business Journal’s 40 Under 40 award, adding those to an Ernst & Young Entrepreneur of the Year Award.