Analysis of Malware Trends for Small and Medium Businesses

Q1 2017

Malwarebytes

TABLE OF CONTENTS

Introduction

Even before the ransomware known as WannaCry or WannaCrypt0r made headlines, ransomware had been growing exponentially and victimizing businesses of all sizes. Small-to-medium sized businesses (SMBs) are acutely impacted by these types of attacks, as many do not have a dedicated IT team, let alone an IT security team. And just one breach could cost them their entire business.

The findings in this report quantify the rate of increase and geographic spread of ransomware among businesses over the last year and shed light on how rapidly new malware families are impacting SMBs in 2017. All businesses studied in the report, over 90 percent of which are officially categorized as SMBs, experienced an increased number of malware detections in Q1 2017 over Q1 2016. Businesses in 10 states experienced a 500 percent increase in ransomware in March 2017 alone.

Methodology

Data was collected from telemetry feeds of malware detections across millions of computer endpoints in small-to-medium sized companies (SMB) protected by Malwarebytes business products. For the purposes of this report, SMB is defined as all companies with fewer than 1,000 seats of Malwarebytes business products installed. Only four malware family types are included in the data below: adware, botnets, ~~ransomware~~ and spyware. Other threat types were not included in this assessment.

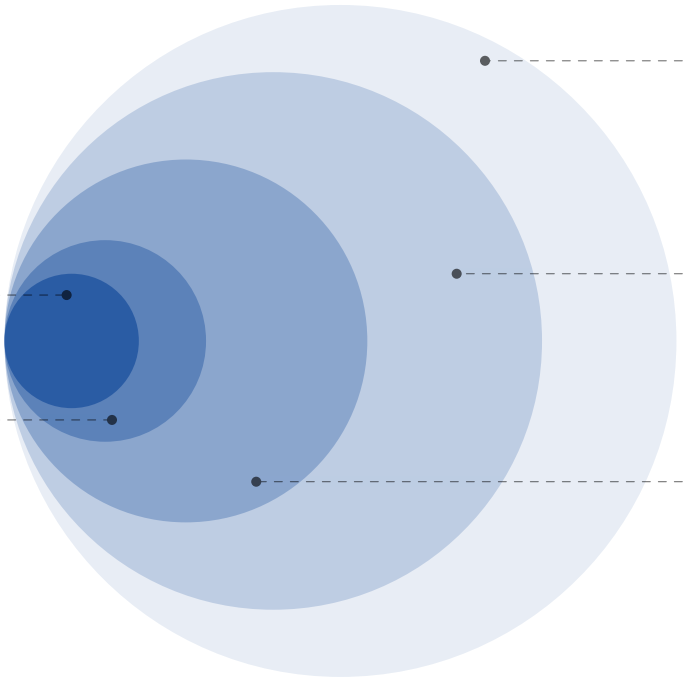
All data in this report was collected in the United States and represents malware encounters and remediation from January 1, 2016 to March 31, 2017.

- Q1, 2016 is defined as January 1 to March 31, 2016
- Q1, 2017 is defined as January 1 to March 31, 2017
- When noted as YoY, figures compare Q1 2017 v. Q1 2016

Findings

Businesses are experiencing far more threats in 2017: In the first quarter of 2017, businesses encountered far more malware than they experienced in Q1 2016.

In Q1 2017, overall malware detections increased more than 165 percent over Q1 2016.



All **50 states** had an increased number of malware detections.

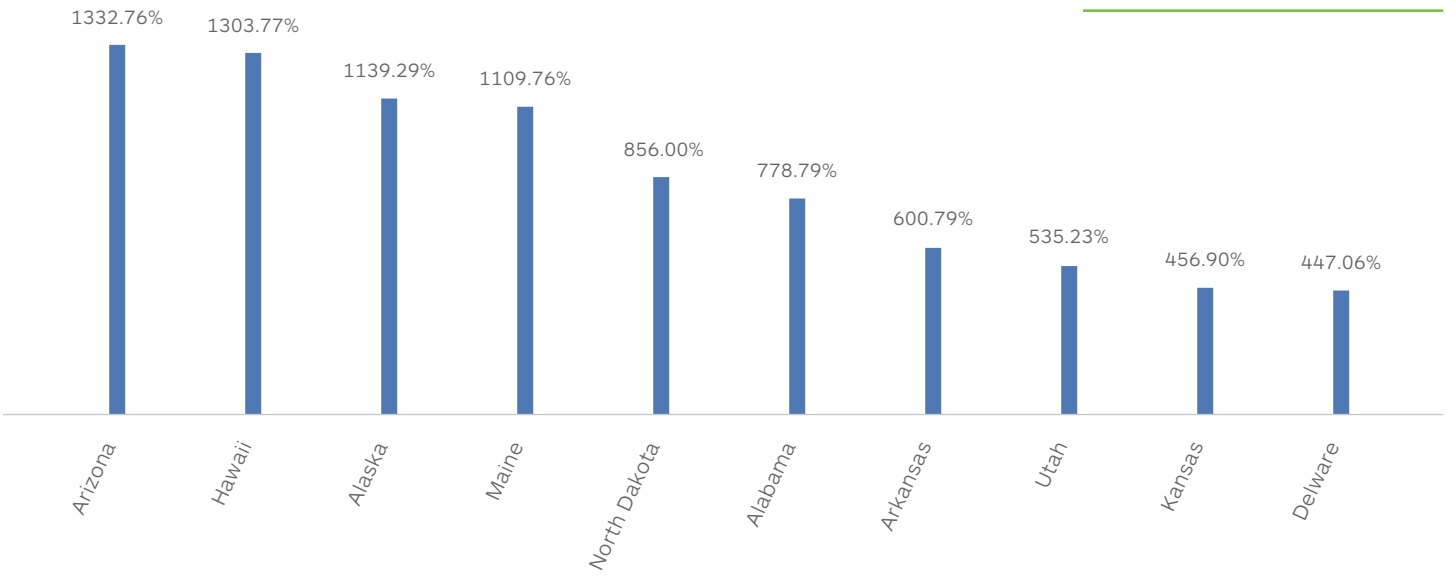
In **40 states,** total malware incidents more than doubled.

In **ten states**, malware incidents increased by 500 percent or more, YoY.

15 states had their total number of malware incidents quadruple.

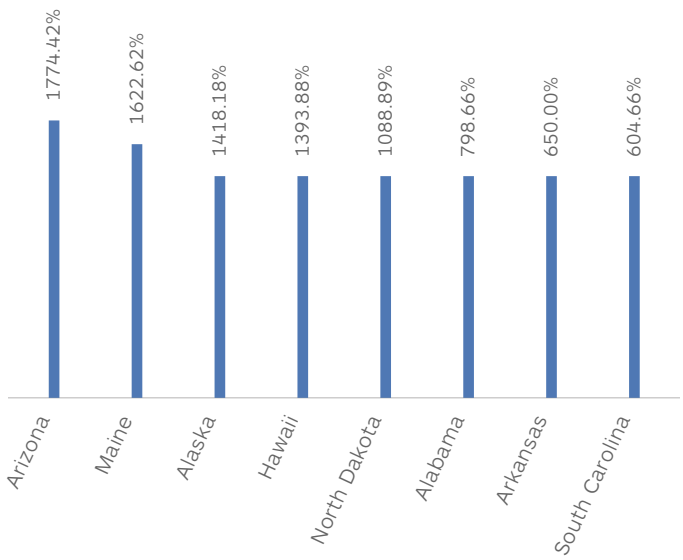
27 states more than tripled their total number of malware ~~incidents, YoY.~~

Ten ~~States~~ with the highest increases in total volume of malware incidents YoY:



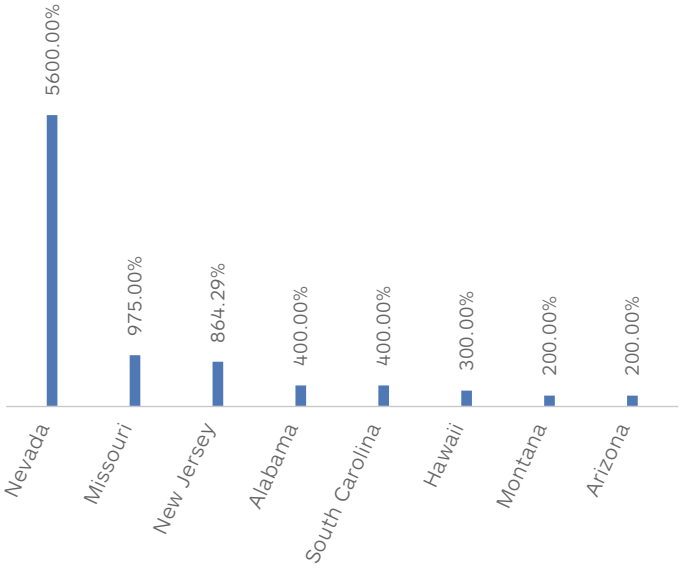
ADWARE IN Q1 2017

- Adware incidents increased in all 50 states, with total detections up 200 percent
- States with highest increase in adware incidents YoY:



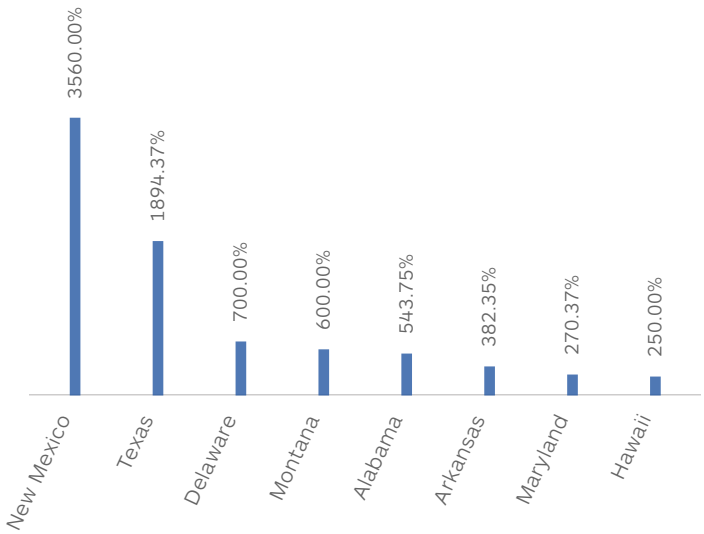
BOTNETS IN Q1 2017

- 31 states had increased YoY botnet activity
- States with highest increase in botnet incidents YoY:



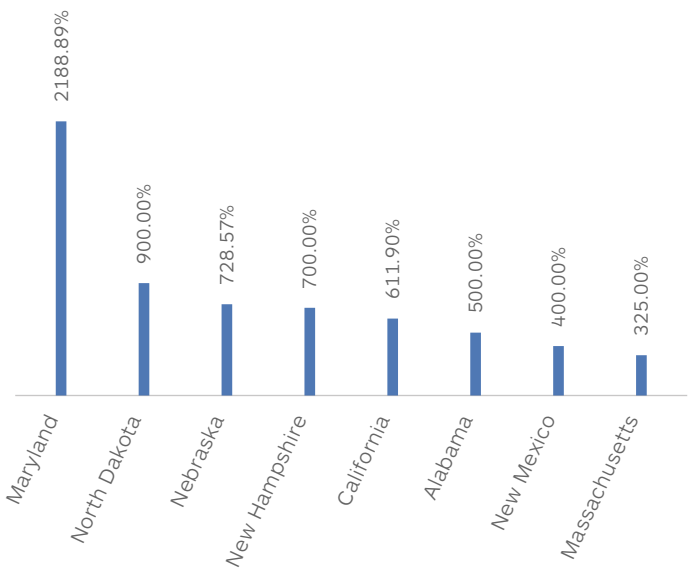
RANSONWARE IN Q1 2017

- 49 states had increased YoY ransomware activity
- Only one state (Vermont) experienced a decrease in ransomware in 2017
- States with highest YoY increase in ransomware incidents YoY:



SPYWARE IN Q1 2017

- 46 states had increased YoY ransomware activity
- Spyware incidents increased 231 percent over Q1 2016
- States with highest increase in spyware incidents YoY:



Businesses in certain states experienced much higher increases in malware encounters, likely due to the primary industries and types of businesses within those states

THREATS BY GEOGRAPHY

- States with highest incidents of malware (per 100 endpoints):

1. Maine
2. Arizona
3. Hawaii
4. Alaska
5. New Mexico
6. West Virginia
7. New Jersey
8. Texas
9. Alabama
10. South Carolina

- Most of these states have heavy involvement in some of the industries with high rates of malware encounters, including:
  - Aerospace
  - Automotive
  - Chemicals
  - Education
  - Healthcare
  - Hospitality
  - Manufacturing
  - Mining
  - Oil and Gas (Energy)
  - Retail
  - Technology
  - Tourism

- If malware incidents were evenly distributed to all endpoints:
  - Business endpoints in Hawaii, Alaska, New Mexico, West Virginia, New Jersey, Texas, and Alabama all experienced between 150 percent average detections per endpoint (Alabama) to 303 percent average detections per endpoint (Hawaii).
    - Aerospace, Automotive, Chemicals, Oil and Gas (Energy) and Technology are among the top industries/employers in ~~Alabama~~.
    - Alabama also was among the top 10 states with the highest increases in adware, botnets, ransomware, and spyware encounters.
      - It was the only state to be in the top 10 in rate of increase for each category of malware.
  - Small business endpoints in Arizona saw 4X the average detections per endpoint.
    - Arizona also was among the top 10 states with the highest increases in adware and botnet detections.
    - Manufacturing, Mining and Tourism are among the top industries/employers in Arizona.
  - Maine would have experienced 5X the average incident rate
    - Education, Healthcare, Retail, Tourism are among the top industries/employers in Maine.

- However, everything is bigger in Texas:
    - Texas was the state with the highest total number of overall malware incidents detected by Malwarebytes, with one of every five threats detected. This shifted from New Jersey as the state with the most overall threat detections in 2016.
        - Education, Hospitality, Manufacturing, Oil and Gas (Energy) and Technology are among the top industries/employers in Texas.
    - With the combination of large population base and highly-targeted industries and number of malware incidents, Texas is a primary hotbed for malware activity.
        - Highest in adware volume: Texas (11.47 percent of all incidents)
        - Highest in botnets volume: Texas (50 percent of all incidents)
        - Highest in ransomware volume: Texas (61 percent of all incidents)
        - Highest in spyware volume: Texas (55 percent of all incidents)

Businesses experienced a massive surge of new malware in March ~~2017.~~ Even with increases over 2016, we haven't seen anything yet, if the malware surge of March 2017 is any indication.

RANSONWARE RISES

- Total ransomware incidents increased 231 percent in Q1 2017 vs. Q1 ~~2016~~
- This occurred even with Locky (our most detected variant of 2016) essentially falling off the map during the first few months of 2017.
    - In fact, many states experienced fewer ransomware incidents in January and February.
- However, during March 2017, ransomware surged:
    - 10,100 percent in Massachusetts
    - ~~a~~ whopping 5038 percent in Texas and is up more than 500 percent for the quarter
    - 1,400 percent in Montana
    - 1,140 percent in Maryland
    - Nearly 1,000 percent in Pennsylvania
    - 10 states experienced more than 500 percent more ransomware in March 2017
    - 14 additional states experienced between 200 and 500 percent more ransomware incidents in March
    - In all, 33 states experienced an increase in ransomware in March 2017

- Over the full first quarter of 2017, the ten states with the largest increase in ransomware incidents include:

1. New Mexico
2. Texas
3. Montana
4. Delaware
5. Maryland
6. Alaska
7. New Jersey
8. North Dakota
9. Arizona
10. Rhode Island

- Ransomware increased 747 percent in New Mexico over the first three months of 2017

SPYWARE SURGES

- Spyware leaped more than 2,500 percent in Texas and Kentucky in March
- Spyware increases were driven by gains of more than 400 percent in at least five known variants
    - Spyware.Imminent increased more than 9766.67 percent over the quarter
    - Spyware.LokiBot increased more than 4150 percent over the quarter

ADWARE ADVANCES

- Adware continued to be the most prolific malware encountered, with 33 adware variants increasing their incident rate by more than 100 percent or more for the quarter
    - Arizona and Maine saw adware incidents rise nearly 300 percent in Q1 2017
    - Q1 adware trends indicate ongoing flux and shifts in the landscape, with nine of the top ten adware variants of 2016 changing.
        - Only Adware.MoboGenie remains from the 2016 top ten list

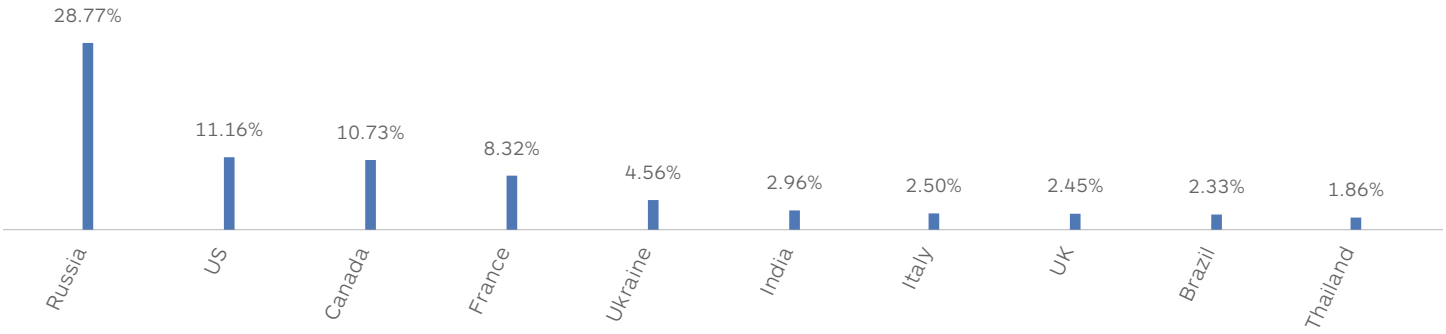
WannaCry ransomware in-depth

As this report was being prepared, the ransomware known as WannaCry or WannaCrypt0r spread globally. Among all of endpoints protected by Malwarebytes, we have detected more than 150,000 incidents/detections/infection attempts by WannaCry in more than 130 countries.

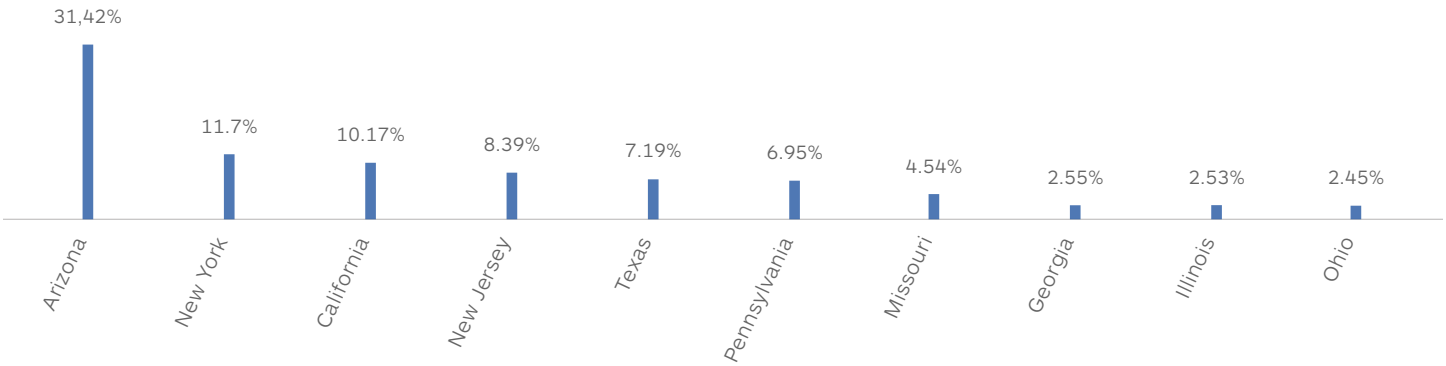
Among those countries:

- Russia is by ~~few~~ with nearly 29 percent of global detections.
- Another Eastern European country, Ukraine, is fifth with nearly five percent of global detections.
- Other top five countries are:
    - the US (second, 11 percent of incidents),
    - Canada (third, with 11 percent of detections)
    - and France (fourth, comprising 8 percent of incidents).
- Despite infections in the UK making the headlines (and the compromise of certain ~~NHS~~ computers), the country was only eighth on our detection list, with approximately 2.5 percent of global detections.

Top 10 countries for WannaCry detections globally:



Within the US, the top 10 states for WannaCry detections are:



Conclusion

The findings in this report demonstrate that the frequency of cyberattacks impacting ~~small~~ and mid-sized businesses has reached a level we have never seen before. Many of these businesses cannot afford the impact of one breach, and have limited internal IT staff to help manage their security programs.

Malwarebytes recently announced the release of its new single-agent cloud platform for businesses featuring Malwarebytes Incident Response ~~(IR)~~ and Malwarebytes Endpoint Protection ~~(EP)~~. The cloud platform leverages Malwarebytes' new seven-layered approach to security to offer a more robust response to the rapidly evolving threat landscape. For more information, visit malwarebytes.com/business.

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.

 Santa Clara, CA

 malwarebytes.com

 corporate-sales@malwarebytes.com

 1.800.520.2796