FALL 2016

Ransomware detections soar in the United States

Malwarebytes

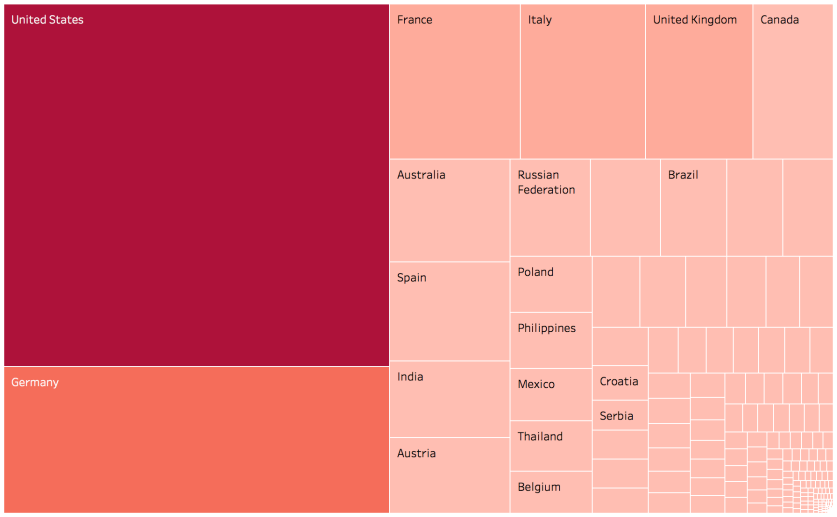
Ransomware a problem for the US

Ransomware rates have been on the rise over the last year throughout the world. However, new data uncovered by Malwarebytes shows that the dangerous malware has been particularly threatening to those in the United States. And it isn't just businesses being targeted. Cybercriminal gangs (primarily based in Eastern and Central Europe) are consistently attacking and victimizing both American businesses and home users with ransomware.

Methodology

- All metrics are from data collected from July 1 to October 15, 2016.
- Malwarebytes reviewed hundreds of thousands of ransomware detections from Malwarebytes software deployed on nearly 50 million endpoints.
- In this time period, Malwarebytes detected ransomware incidents in more than 200 countries.
- The US ranked the highest of all countries for ransomware incidents, with 26 percent of the global total.
    - This is 200 percent more ransomware detected than the number two country, Germany, and approximately 550 percent more than the number three country, France.

Ransomware detections by country



- Las Vegas/Henderson leads in the number of overall ransomware detections, most detections per individual machine, and most detections per population.
- Las Vegas/Henderson had over 300 times more detections than Fort Wayne, number 10 on our list, and had 500 times the average detection levels of the top 40 on our list.

Top three ransomware variants detected and percentage of global detections

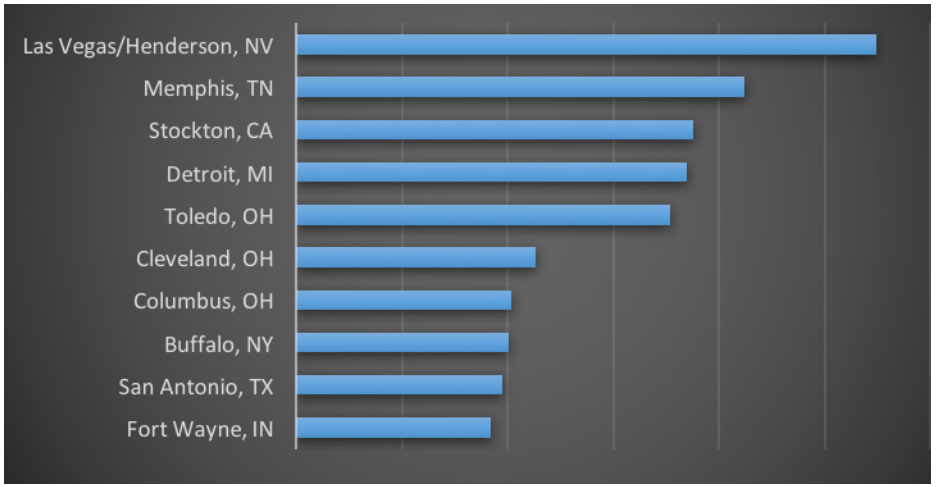
1. Cerber 38%
2. Locky 14%*
3. CryptoWall 4%

Top 10 US cities for ransomware detections

1. Las Vegas/Henderson, Nevada
2. Memphis, Tennessee
3. Stockton, California
4. Detroit, Michigan
5. Toledo, Ohio
6. Cleveland, Ohio
7. Columbus, Ohio
8. Buffalo, New York
9. San Antonio, Texas
10. Fort Wayne, Indiana

*From the time that this data was reviewed to the present day, Locky has since overtaken Cerber as the single largest ransomware family.

Comparing ransomware detections



Top three ransomware variants detected and percentage of all US detections

1. Cerber	38%
2. Locky	10%*
3. CryptoWall	3%

* From the time that this data was reviewed to the present day, Locky has since overtaken Cerber as the single largest ransomware family.

Ransomware distribution in the US

Ransomware is a problem for all Americans, no matter where you live. Ransomware distribution seems to be both geographically consistent and consistent per capita. This results in smaller cities and towns (with fewer than 250,000 residents) experiencing a large percentage of ransomware detections. The lone exception to this even distribution is in the American Rust Belt, which experienced higher incidents of ransomware than other areas of the country. Six of the top 10 cities are located in the Rust Belt.

- Six of the top 10 cities with the highest rates of ransomware incidents (detection per machine) are in the Northeastern region of the US.
- This region straddles the upper Northeastern United States, the Great Lakes, and the Midwest States, and is often characterized by economic decline, population loss, and urban decay due to the shrinking of its once-powerful industrial sector.
- Outside of these outliers, ransomware is evenly dispersed geographically across America.
- While the rates in top 10 cities were more than 1000 percent the average in other cities, the rates of detections per machine in all other cities remained relatively consistent.
  - 86 percent of ransomware detections occurred in cities with fewer than 250,000 residents.
  - However, these cities, towns, and unincorporated areas contain 82 percent of the US population according to the US census[1].
  - Ransomware is equally opportunistic in its victimology and fairly consistent in per capita distribution across the US.

[1]https://www.census.gov/content/dam/Census/library/publications/2015/demo/p25-1142.pdf

Evolving ransomware tactics

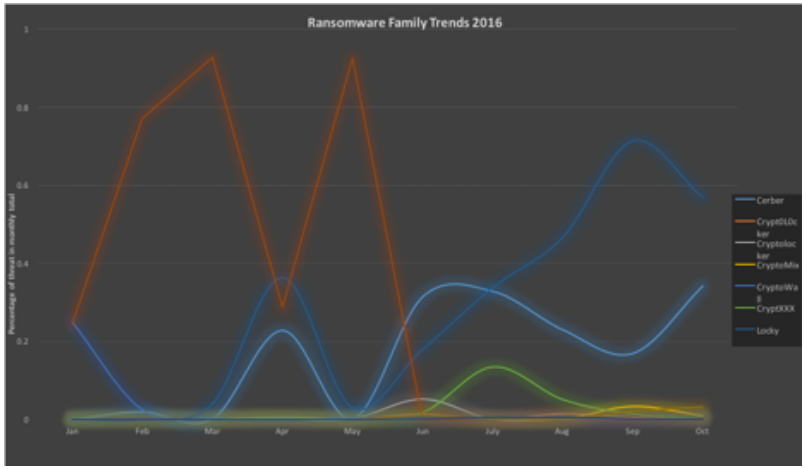
Although cybercriminal gangs have already saturated both the rural and urban US populace with ransomware, they are constantly improving their tactics, execution, and business model to evade detection by current solutions.

- Ransomware as a business is flourishing.
- Organized cybercriminal gangs are continuing to update their business processes, technical support, distribution methodology, and their technical prowess.
- Ransomware distribution is still primarily through spam email campaigns and exploit kits.
- Targeted ransomware (attacking specific industries) has not become the status quo, as spamming techniques and exploit kit integration continue to be profitable.
- New variants are appearing quarterly, and quickly surpass the number of infections/compromises/incidents of previous ransomware families.
- The evolution of ransomware has seen multiple improvements designed to evade detection by current antivirus solutions.
- Internecine battles between gangs appear to be escalating, as code stealing and making public the private encryption keys of competing variants become more frequent.
- The top ransomware encountered in this study, Cerber, provides a perfect microcosm of how these gangs operate and how they continue to target all Americans.
- Locky, the second-largest family of ransomware found by this study, has risen to become one of the most prolific ransomware attacks of the year.

Top ransomware families in top five cities

1. Las Vegas/Henderson, Nevada
    1. Cerber
    2. TeslaCrypt*
    3. Locky
    4. Cryptowall
2. Memphis, Tennessee
    1. Cerber
    2. CryptoWall
    3. Locky
    4. CryptXXX
3. Stockton, California
    1. Cerber
    2. Locky
    3. Crysis
4. Detroit, Michigan
    1. Cerber
    2. CryptoWall
    3. Locky
    4. FileLocke
5. Toledo, Ohio
    1. Cerber
    2. TeslaCrypt
    3. Locky
    4.CryptoWall

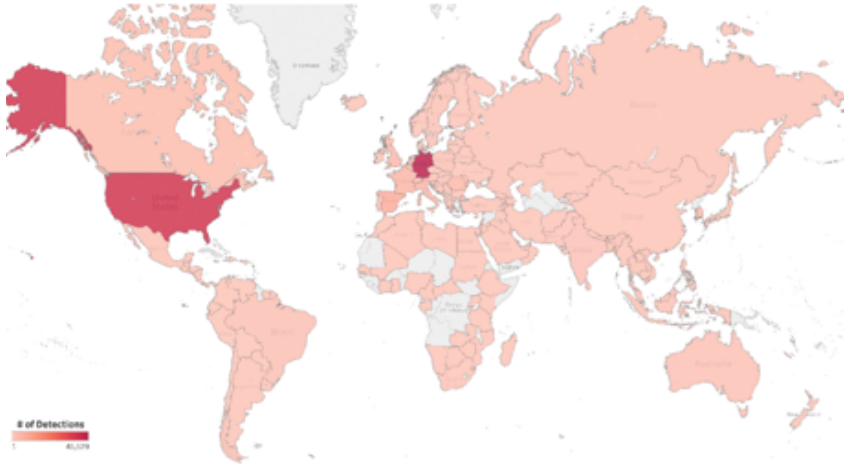
Top ransomware families



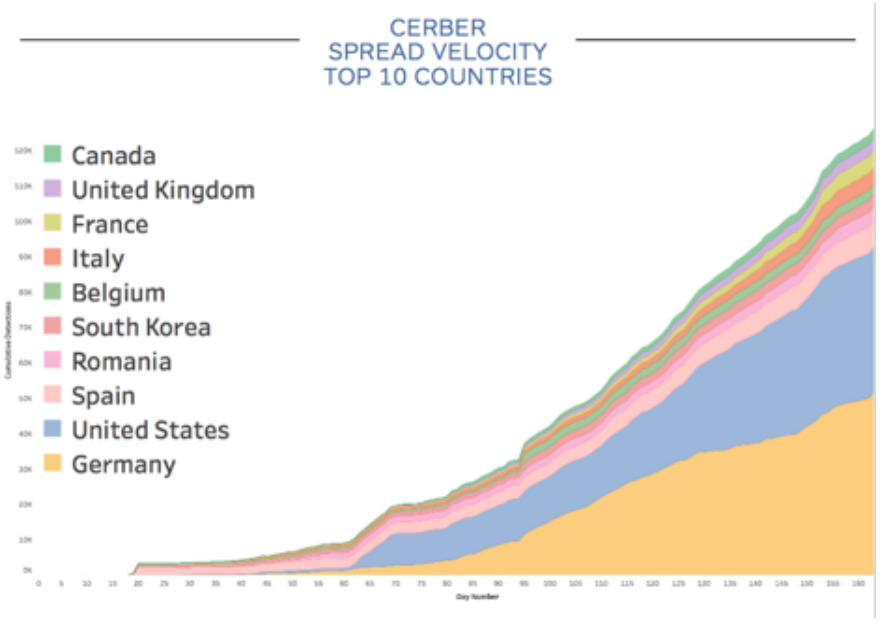
1. Cerber	38%
2. Locky	10%
3. CryptoWall	3%

Cerber consistently high in all cities

CERBER
SPREAD MAP



CERBER
SPREAD VELOCITY
TOP 10 COUNTRIES



- Cerber ransomware was released in early March 2016.
- Despite its relative newness, Malwarebytes Labs describes Cerber as a "powerful ransomware written with attention to detail."
- Cerber is commonly distributed using exploit kits and email campaigns, often through Microsoft Office files like Word documents.
- When victims are infected, their files are encrypted and they are informed that they need to pay a ransom of 1-2 bitcoins to have their files decrypted. The ransom doubles if the victim does not pay within seven days.

More Russian ties?

- When Cerber first runs, it first determines which country the victim is in. If the victim is from Russia or other former Soviet Republics, it will terminate itself and not encrypt the computer.

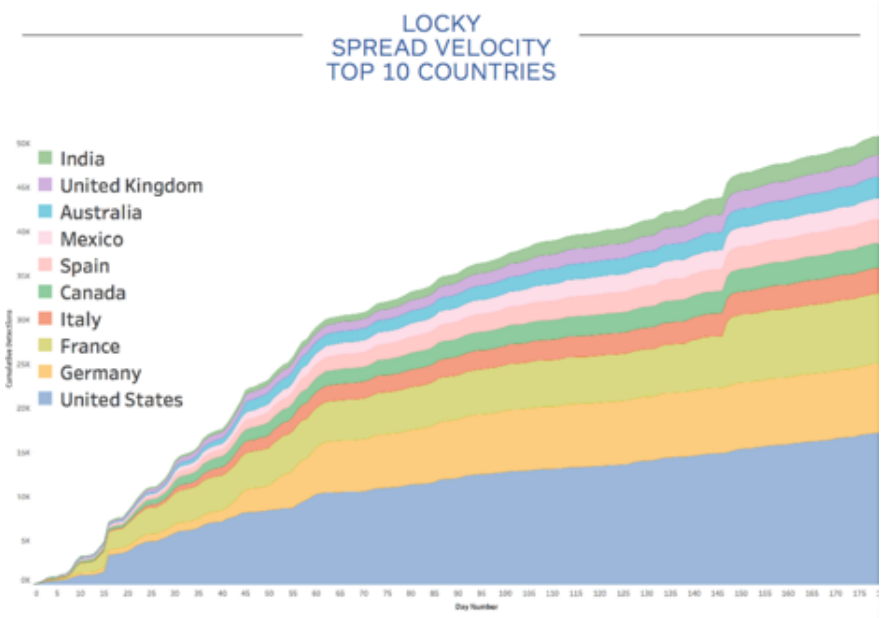
Business model

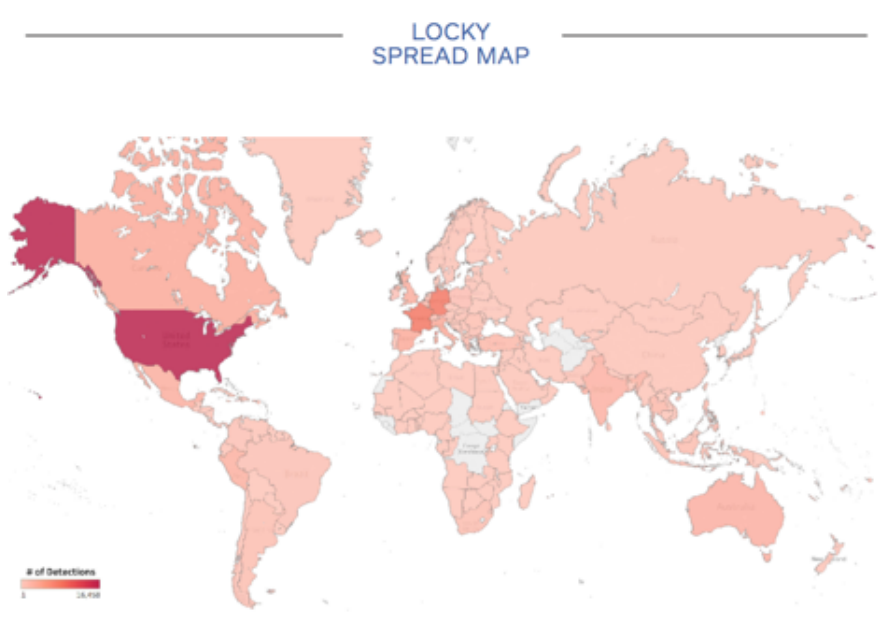
- Cerber's unique use of a ransomware-as-a-service business model has helped it proliferate. The ransomware developer recruits affiliates that spread the ransomware, most often through spam email campaigns, in exchange for a 60 percent cut of the profits and 5 percent for recruiting a new member.
- This amounts to Cerber's creators making an annual profit of about $1 million on about $2.5 million in revenue.
- Cerber offers its affiliates a simple web interface to control their campaigns, allowing nearly anyone to conduct a ransomware campaign, even those with a non-technical background.

Evading and optimizing

- Cerber's authors have also developed new methods to help Cerber evade detection. A new Cerber variant uses a unique trick to avoid signature-based anti-malware solutions by using a hash factory attack that morphs the Cerber payload and generates unique hashes as often as every 15 seconds.
- Versions of Cerber have also been used to conduct DDoS (distributed denial of service) attacks on other victims while the victim is unable to access their system.

Locky is on the rise and is overtaking Cerber





- Locky ransomware was released in February 2016. Locky was originally deployed using a downloader in a Microsoft Office document or JavaScript email attachment in a spam campaign. Most often, it used Microsoft Word documents containing macro scripts to download the ransomware.
- Locky will encrypt any files that it can find, except for essential Windows files. Each file is encrypted using a 128-bit AES key and then renamed with a ".locky" extension.
- The decryption price generally starts at half a bitcoin but can increase to 1 bitcoin depending on the number of files encrypted.

Big shoes

- The size of Locky's geographic footprint so soon after it was released is truly astounding.
  - By day three, Locky had been detected in 85 countries.
  - By the end of week one, it was detected in 109 total countries.
  - Some security companies have suggested that Locky spam accounted for 97 percent of all spam campaigns spreading malicious email attachments.

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