Carbon Black.

DECEMBER 2017

Carbon Black 2017 Threat Report

Non-Malware Attacks and Ransomware Continu e to Own the Spotlight

Executive Summary

As the calendar shifted from December 2016 to January 2017, the prospect of a large-scale cyberattack loomed. Questions over the possible hacking of the 2016 U.S. presidential election swirled and businesses faced a growing attack vector in ransomware. In 2016, ransomware was estimated to be an $850 million crime.

As we shift to 2018, questions still exist regarding the politics and possibility of a hacked democracy, but one thing is abundantly clear—2017 saw several large-scale cyberattacks including WannaCry, NotPetya, and BadRabbit demonstrating that ransomware is not going anywhere. **Ransomware is now estimated to be a $5 billion crime,** according to research from Cybersecurity Ventures.

Ransomware, combined with the continued ubiquity of mass malware and non-malware attacks, is creating a vast attack surface for cyberattackers, who are getting more creative and persistent.

To better understand the evolving attack landscape as we head into 2018, the Carbon Black Threat Analysis Unit (TAU) researched the current state of ransomware, malware, and non-malware attacks. In particular we looked at how, and how frequently, Carbon Black customers have been targeted. In this report the TAU also provides some predictions for 2018.

RANSOMWARE, COMBINED WITH THE CONTINUED UBIQUITY OF MASS MALWARE AND NON-MALWARE ATTACKS, IS CREATING A VAST ATTACK SURFACE FOR CYBERATTACKERS, WHO ARE GETTING MORE CREATIVE AND PERSISTENT.

Carbon Black.

Research Highlights

In 2017, ransomware is estimated to be a **$5 billion crime**, according to research from Cybersecurity Ventures. In 2016, the estimate was $850 million. In 2015, the estimate was a mere $24 million.

As we close out 2017, every computer protected by Carbon Black is being **targeted by an attack an average of 3x per month**. At the beginning of 2017, this number was **less than one attack per month on average (0.7)**, a growth rate of 328%.

Throughout 2017, there was, on average, a **13% increase per month** in attacks targeting endpoints protected by Carbon Black.

52% of all attacks seen in 2017 were non-malware attacks. Malware-based attacks account for the remaining **48% of attacks**.

Non-malware attacks are increasing at a rate of **6.8% per month**.

Ransomware most often targeted **technology** companies, **government/non-profit** organizations, and **legal** firms in 2017.

The most common ransomware variants seen in 2017 were: **Spora, CryptXXX/Exxroute, Locky, Cerber,** and **Genasom**.

Financial organizations, **healthcare** providers, and **retail** stores were the top three verticals targeted by cyberattacks leveraging malware in 2017.

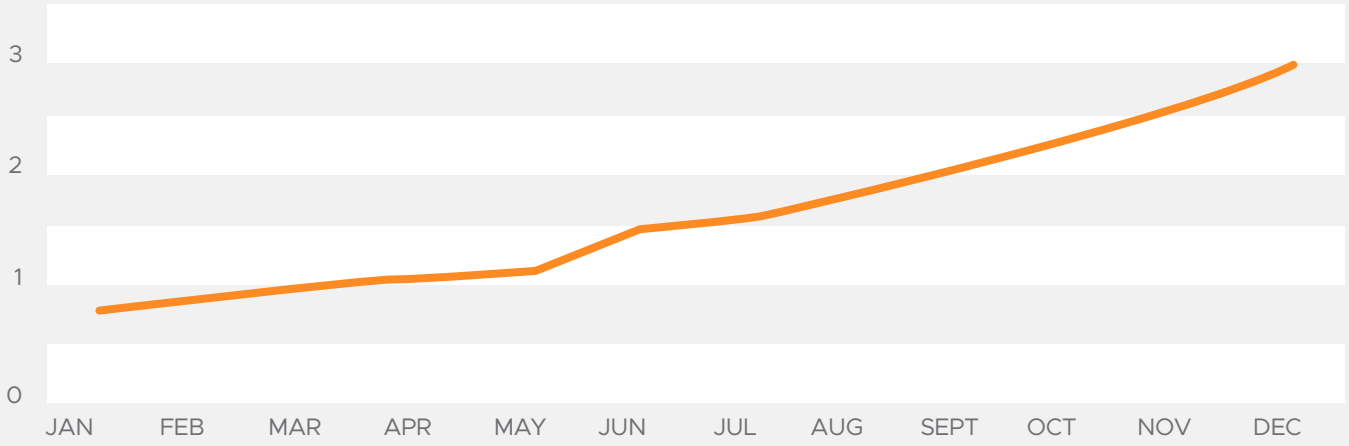
The top five most seen malware families in 2017 were: **Kryptik, Strictor, Nemucod, Emotet,** and **Skeeyah**.

Cyberattacks Continued to Grow

At the start of 2017, the average computer protected by Carbon Black was targeted by an attack 0.7 times per month. As of December 2018, that number has jumped 328% to three attacks on average, per computer, per month. That means an organization with 10,000 endpoints is seeing approximately 1,000 attacks per day.

Overall, we're seeing a **13% monthly growth rate for attacks per month targeting Carbon Black protected endpoints**.

AVERAGE NUMBER OF ATTACKS PER ENDPOINT IN 2017



Carbon Black.

AN ORGANIZATION WITH 10,000 ENDPOINTS IS SEEING APPROXIMATELY 1,000 ATTACKS PER DAY.

Carbon Black.

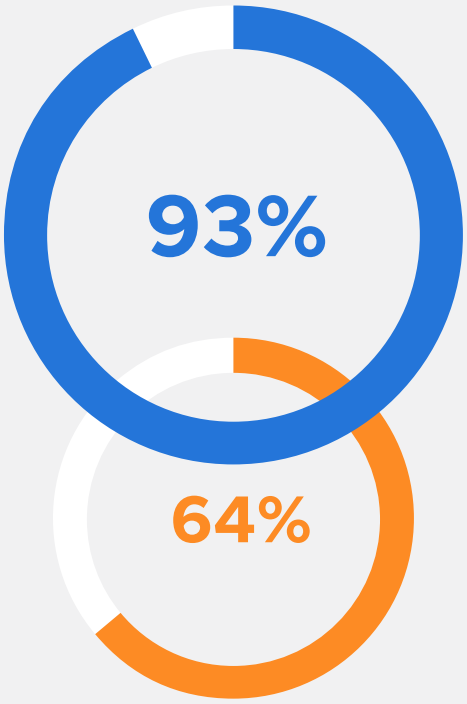
Non-Malware Attacks

Non-malware attacks (fileless attack) experienced a bit of a renaissance last year with virtually every organization in our 2016 research targeted by such an attack. The trend is continuing.

Non-malware attacks use trusted programs, native to operating systems, to gain control of computers. Non-malware attacks typically do not require downloading additional malicious files and are capable of conducting extremely nefarious activities such as stealing data, stealing credentials, and spying on IT environments.

Native operating system tools regularly used in non-malware attacks include PowerShell and Windows Management Instrumentation (WMI), tools typically reserved for IT admins. Non-malware attacks also exploit in-memory access and running applications, such as web browsers and Office applications to conduct malicious behavior.

In a Carbon Black survey, the **vast majority of security researchers (93%) said non-malware attacks pose more of a business risk than commodity malware attacks**.



93% of security researchers say non-malware attacks pose more of a

BUSINESS RISK

than commodity malware attacks

64% of security researchers say they have seen an increase in non-malware

ATTACKS

Carbon Black.

Source: 2017 Beyond the Hype: Artificial Intelligence, Machine Learning and Non-Malware Attacks Report

Deployment of non-malware attacks in the wild has moved with regularity into attack campaigns. For the purposes of investigating non-malware attacks for this report, Carbon Black focused on instances of PowerShell and WMI used for malicious intent.

52%
non-malware attacks

48%
malware-based attacks

Carbon Black.

We found that **more than half (52%) of all cyberattacks in 2017 leveraged non-malware tactics**. It's interesting to note this number aligns almost precisely with industry data suggesting that 53% of all successful data breaches are caused by non-malware attacks.

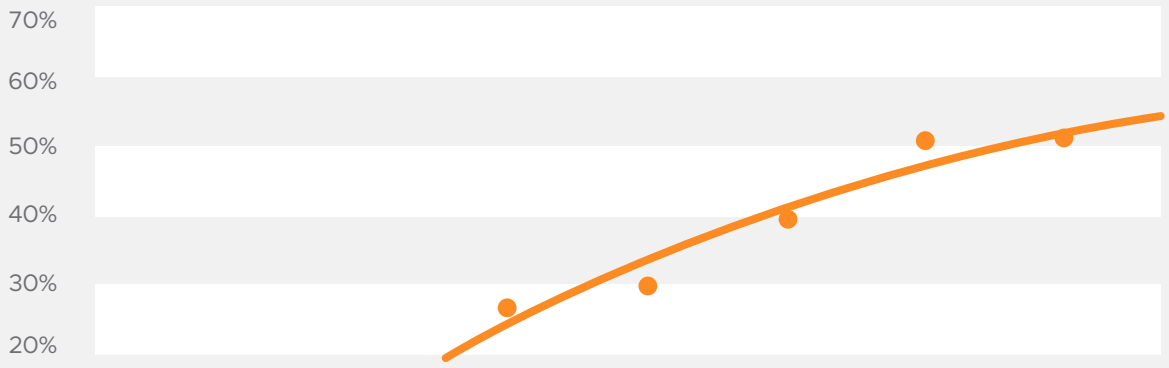
MORE THAN HALF OF ALL CYBERATTACKS (52%) IN 2017 LEVERAGED NON-MALWARE TACTICS.

Carbon Black.

Non-Malware Attacks Trending Upward

A noticeable uptick in non-malware attacks evolved over 2017. **We're seeing a monthly average growth rate of 6.8% for non-malware attacks.**

SNAPSHOT - LINEAR GROWTH IN NON-MALWARE ATTACKS

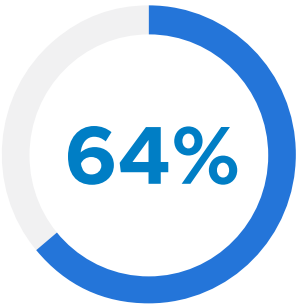


Carbon Black.

In our survey, **64% of security researchers noted seeing an increase in non-malware attacks**.

Almost all of the researchers **(96%) said being able to prevent non-malware attacks would improve their organization's security posture**.

Among these researchers, confidence is waning that legacy antivirus (AV) can protect an organization against these attacks. **Two-thirds of security researchers said they were not confident legacy AV could protect an organization from non-malware attacks**.



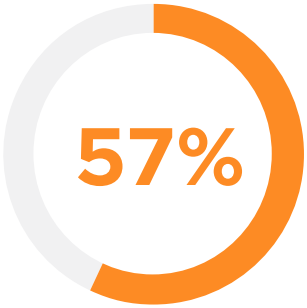
NOTED SEEING AN INCREASE IN NON-MALWARE ATTACKS

Carbon Black.

Ransomware in 2017

The global WannaCry and NotPetya attacks from earlier this year thrust ransomware into the public's consciousness like never before. As the attacks unfolded, more than 300,000 computers across 150 countries around the world were held hostage. News reports helped explain to the world how ransomware works.

According to Carbon Black research, **WannaCry was the first exposure to the intricacies of ransomware** for more than half of the population.



WERE FIRST EXPOSED TO
THE INTRICACIES OF RANSOMWARE
FOLLOWING THE
WANNACRY ATTACKS

Carbon Black.

This increased awareness may ultimately affect businesses that are breached. According to our research, about **70% of consumers said they would consider leaving a business affected by ransomware**.

Carbon Black.

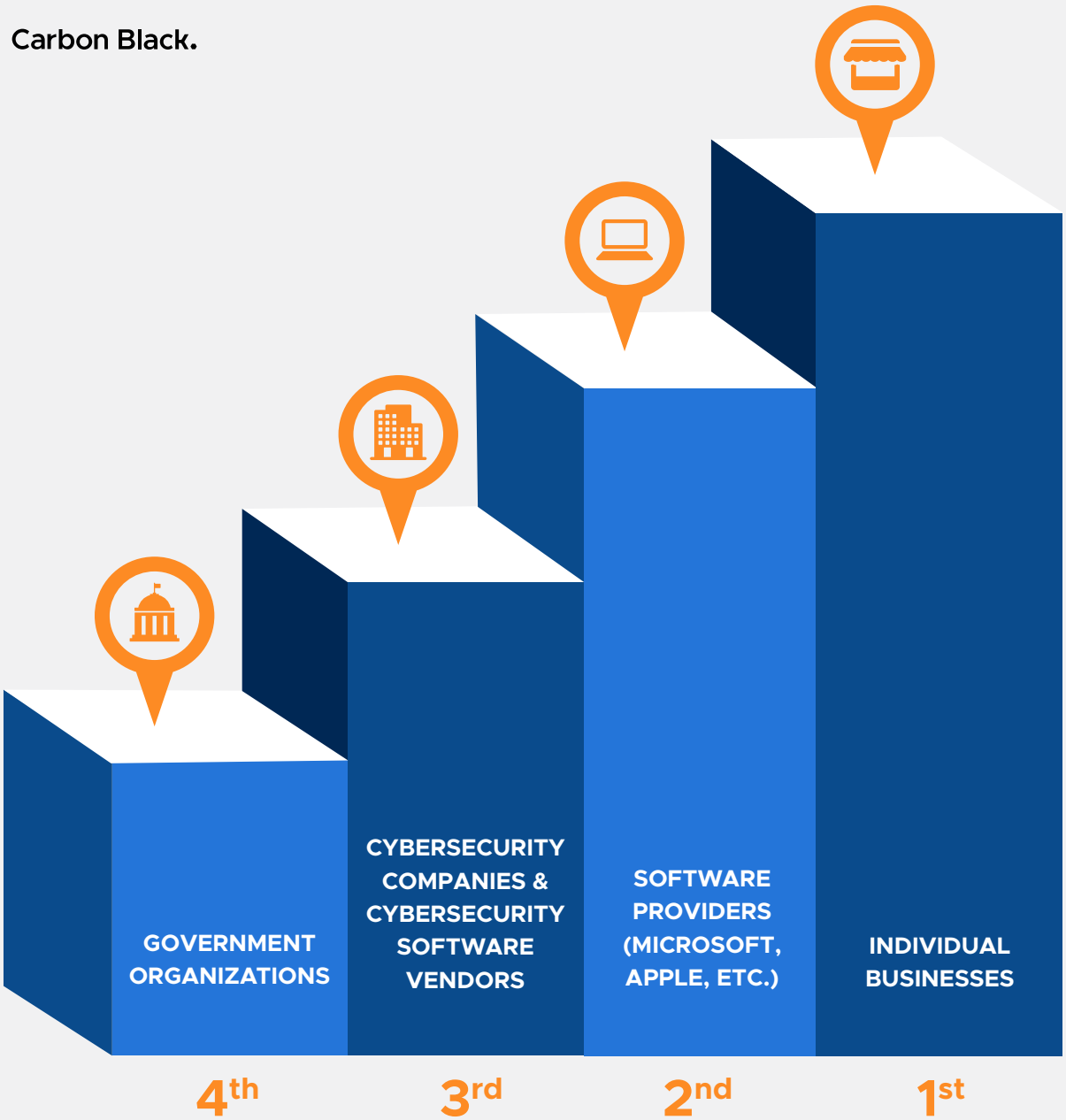
% OF CONSUMERS WHO SAID THEY WOULD CONSIDER LEAVING
A BUSINESS THAT WAS HIT BY RANSOMWARE

72% would consider leaving their financial institution

68% would consider leaving their healthcare provider

70% would consider leaving their retailer

As our data noted, consumers believe the largest onus of responsibility to protect against ransomware attacks lies with the individual businesses.



$$$

ACCORDING TO RESEARCH FROM CYBERSECURITY VENTURES, RANSOMWARE IS NOW ESTIMATED TO BE A

$5B

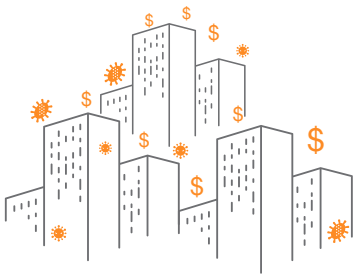
CRIME

The Ransomware Economy

Ransomware is now estimated to be a $5 billion crime. In 2016, the estimate was $850 million. In 2015, the estimate was a mere $24 million, marking a stark growth rate in just three years, according to research from Cybersecurity Ventures. Given the recent price of bitcoin, the 2017 figure may actually be larger. Read more here.

ESTIMATED RANSOM MONEY BUSINESSES PAID TO ATTACKERS

$24 MILLION
2015



$850 MILLION
2016

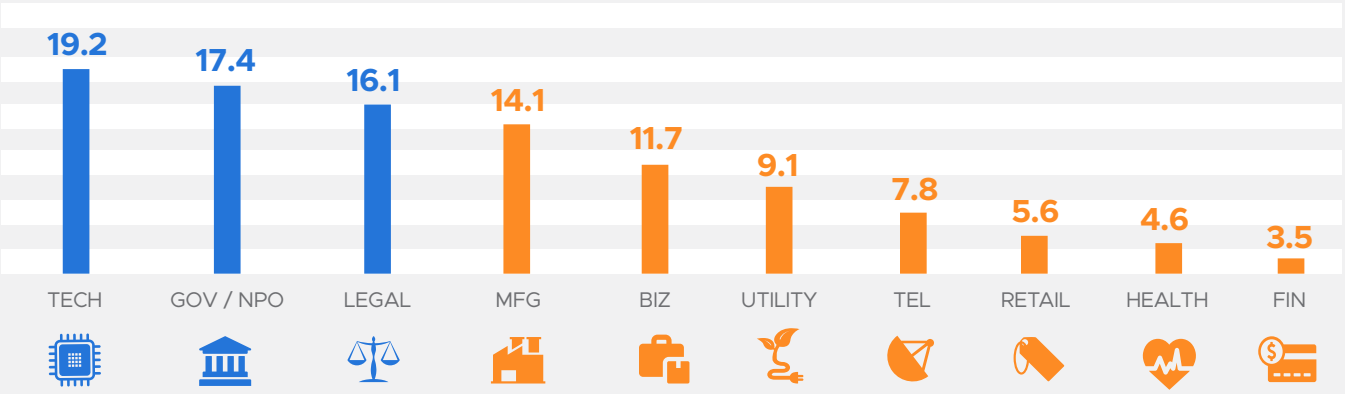
$5 BILLION
2017

Source: Cybersecurity Ventures

No industry was immune and the industries most targeted by ransomware this year were **technology, government/nonprofit,** and **legal**.

Carbon Black.

INDUSTRIES MOST TARGETED BY RANSOMWARE IN 2017



Spora emerged as the go-to ransomware variant for 2017, used in 1 out of every 5 attacks. The most common ransomware variants seen in 2017 were: **Spora, CryptXXX/Exxroute, Locky, Cerber,** and **Genasom**.

2017
TOP 5 RANSOMWARE

1 - Spora
2 - CryptXXX/Exxroute
3 - Locky
4 - Cerber
5 - Genasom

2016
TOP 5 RANSOMWARE

1 - Locky
2 - CryptoWall
3 - CryptXXX
4 - Bitman
5 - Onion

2015
TOP 5 RANSOMWARE

1 - CryptoWall
2 - Blocker
3 - Onion
4 - Snocry
5 - Bitman

2018 Ransomware Predictions

1. Based on the direction ransomware is trending, we believe **ransomware will increasingly target Linux systems** in an effort to further extort larger enterprises. We have already observed attacks hitting MongoDB earlier this year which provide an excellent foreshadowing.

2. **Ransomware will become more targeted** by looking for certain file types and targeting specific companies such as legal, healthcare, and tax preparers rather than "spray and pray" attacks we largely see now. There is already ransomware that targets databases, preying on businesses, and small tweaks to their code can target critical, proprietary files such as AutoCAD designs.

3. While most ransomware samples we analyzed simply encrypt files in place and transmit encryption keys for the purpose of decryption, **there will be ransomware samples that will take the extra step of exfiltrating data prior to encryption**. Not only would such an evolution put stress on companies to restore their data but also incorporate the loss of proprietary data that could be sold on the black market.

4. **Ransomware will increasingly be used as a smokescreen**. For example, in the past, Zeus botnet operators hit victims with DDoS attacks after an infection to take investigators off the trail. A similar trend is emerging with ransomware attacks where the encryption of files could take place after more damning actions are taken by adversaries. Using already existing techniques of deleting Volume Shadow Copies, which deletes potential file backups, and the deletion of Windows event logs, adversaries can thwart many incident response efforts by forcing responders to focus on decrypting files instead of investigating data and credentials exfiltrated.

5. Ransomware will emerge as a secondary method when initial forms of attack fail. **Adversaries that rely upon more crafted and targeted attacks may use ransomware as an attack of last resort**.

6. **Ransomware will be used more commonly as a false flag, as seen with NotPetya**. Solely from dynamic analysis it was perceived to be Petya, when more detailed analysis showed it wasn't. Such quick analysis also insinuated it to be obvious ransomware, but a greater depth of disassembly showed that data was not held at ransom; it was simply destroyed.

7. **Ransomware will increasingly leverage social media to spread either intentionally or unintentionally**. Similar to malware such as Koobface, maliciously shared content on sites such as Facebook could lead victims to click enticing links. Intentionally shared ransomware, seen in prior concepts, such as Popcorn Time where victims could share to reduce or eliminate their ransom, could see larger-scale use.

Malware-Based Attacks in 2017

With all the attention given to non-malware attacks and ransomware, it's important to consider the profound influence malware-based attacks still have. **Malware-based attacks still account for 48% of cyberattacks, according to Carbon Black data, and 47% of successful breaches, according to industry data.**

When it comes to malware-based attacks, the most commonly **targeted verticals in 2017 were finance, healthcare, and retail**.

Carbon Black.

VERTICALS MOST TARGETED BY MALWARE IN 2017

1. **FINANCE**
2. **HEALTHCARE**
3. **RETAIL**
4. LEGAL
5. TELECOMMUNICATIONS / ENTERTAINMENT
6. UTILITIES
7. MANUFACTURING
8. GOVERNMENT / NONPROFIT
9. TECHNOLOGY
10. BUSINESS PRODUCTS & SERVICES

The top-10 most seen malware families in 2017 were: **Kryptik** (15.7%), **Strictor** (14.7%), **Nemucod** (12.4%), **Emotet** (10%), **Skeeyah** (7.3%), **Zapchast** (4.9%), **Sality** (4.7%), **Zusy** (4.6%), **Zbot** (4.2%), and **CoinMiner** (4.1%).

Carbon Black.

PERCENTAGE OF MALWARE BY FAMILY IN 2017

15.7%
Kryptik

14.7%
Strictor

12.4%
Nemucod

10%
Emotet

7.3%
Skeeyah

4.9%
Zapchast

4.7%
Sality

4.6%
Zusy

4.2%
Zbot

4.1%
CoinMiner

MALWARE-BASED ATTACKS STILL ACCOUNT FOR 48% OF CYBERATTACKS

Carbon Black.

2018 Outlook & Predictions

Targeted attacks are on the rise, and the dark web isn't helping curb that trend. To compound this, the recent revelations on Shadow Brokers and CIA Vault 7, as well as burgeoning nation-state cyber capabilities aren't helping either. It's only a matter of time before more attack methods are developed using these highly advanced tools.

THE 2018 U.S. MIDTERM ELECTIONS WILL BE A TARGET FOR CYBERATTACKS

Next year is another election year in the United States. It is likely that Russia will engage in more cyber electioneering following their efforts in 2016. Data from Carbon Black research suggests that one in four voters, amounting to 58.8 million people, may not vote in the upcoming 2018 U.S. midterm elections due to cybersecurity fears. In this regard, our U.S. democracy is at risk.

1 in 4 voters said they will consider not voting in future elections over cybersecurity fears

Carbon Black.

NATION-STATE ACTORS WILL LOOK TO TARGET CRITICAL INFRASTRUCTURE

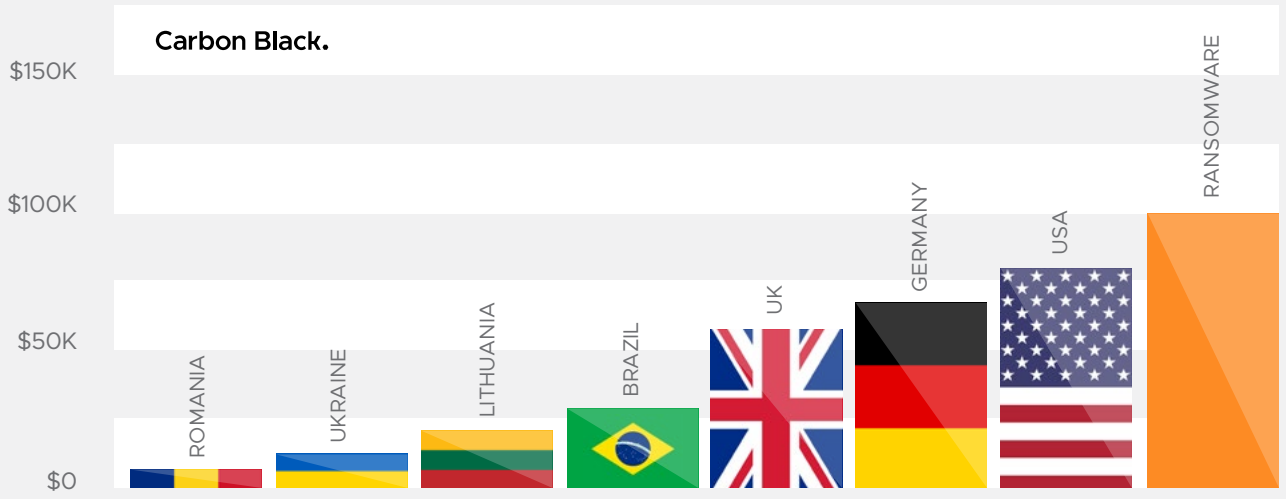
Malign nation-state actors, including Iran and North Korea, are likely to increase cyberattacks following increased pressure from the United States. It's further likely these and other nation-state actors become emboldened following the non-response from the United States.

Global critical infrastructure will also be a key focus in 2018. To date, we have only scratched the surface when it comes to a real-world effect from cyberattacks.

THE RANSOMWARE ECONOMY WILL CONTINUE TO GROW

With ransomware on the rise, the economy is looking especially positive for would-be cybercriminals. The dark web remains a veritable treasure trove for buyers and sellers. According to Carbon Black research, the dark web economy for ransomware is growing at a rate of 2,502% per year. Some sellers of ransomware are making more than $100,000 per year simply retailing ransomware. The ransomware economy is alive and well.

SOFTWARE DEVELOPER SALARIES BY REGION IN 2017



INCREASE IN SECURITY SPENDING & AWARENESS EXPECTED IN CONJUNCTION WITH CLOUD MIGRATION AND PROLIFERATION OF DEVICES

With the attack landscape growing at an alarming rate, we're hopeful to see a marked increase in security awareness training and overall cybersecurity spending in 2018. This should happen as organizations continue to transition to the cloud and threats evolve to target traditional endpoints, mobile devices, IoT devices, transportation mechanisms, critical infrastructure, and more.

According to SANS data, 90% of organizations are now investing more in cybersecurity than during the previous 12 months. This approach is carrying over to multiple sectors. That is encouraging. Concerning, though, is that organizations are still battling a lack of skills and a lack of cybersecurity staffing. About half of organizations (47%) perceive this as a significant problem. And 48% of organizations say they lack the resources to execute cybersecurity improvements in key areas. It appears we're continuing to play a game of catch-up but the trend may be reversing. We're hopeful 2018 will mark the turning point.

METHODOLOGY

For this report, Carbon Black analyzed 2017 customer data to determine the prevalence of ransomware, malware, and non-malware attacks. For non-malware attacks, nefarious usage of both PowerShell and WMI were considered.

ABOUT CARBON BLACK

Carbon Black is the leading provider of next-generation endpoint security. Carbon Black's Predictive Security Cloud provides advanced protection for more than 14 million endpoints across more than 3,300 customers, including 31 of the Fortune 100. These customers use Carbon Black to replace legacy antivirus, lock down critical systems, hunt threats, and protect their endpoints from the most advanced cyberattacks, including non-malware attacks.

For more information, please visit carbonblack.com or follow us on Twitter at @CarbonBlack_Inc.

Carbon Black.

1100 Winter Street
Waltham, MA 02451
P: 617.393.7400
F: 617.393.7499

carbonblack.com