CARBON
BLACK

Carbon Black Threat Report

Non-Malware Attacks and Ransomware Take Center Stage in 2016

SUMMARY

According to Carbon Black data, attackers are holding data for ransom at an alarming rate and are continuing to deploy attacks across every industry. In conjunction with the rise of ransomware and the continued ubiquity of mass malware, attackers are increasingly utilizing non-malware attacks in an attempt to remain undetected and persistent on organizations' enterprises.

These non-malware attacks are capable of gaining control of computers without downloading any files and are using trusted, native operating system tools (such as PowerShell) and exploiting running applications (such as web browsers and Office applications) to conduct malicious behavior.

Some leading attack campaigns in 2016, including PowerWare and the alleged hack against the Democratic National Committee (DNC) leveraged non-malware attack mechanisms to carry out nefarious actions.

As organizations plan to defend their enterprises against ransomware and non-malware attacks in 2017, it's critical to understand the scope of the problem. In this report, Carbon Black researchers reveal some of the key attack trends of 2016, and predict what to look out for in 2017.

AS WE HEAD INTO 2017, **MOTIVATED ATTACKERS** ARE NOT SLOWING DOWN.

HIGHLIGHTS

Virtually every organization included in this research was targeted by a non-malware attack in 2016.

Instances of severe non-malware attacks grew throughout 2016. Over a 90-day period, about one-third of organizations are likely to encounter at least one severe, non-malware attack.

Instances of non-malware attacks leveraging PowerShell and Windows Management Instrumentation (WMI) grew throughout 2016. Such attacks spiked by more than 90% in the second quarter of this year (+93.2%) and have stayed at escalated levels since.

In 2016, ransomware instances grew by more than 50% over 2015.

Ransomware has emerged as the fastest-growing malware across all industries in 2016, with major percentage increases seen at technology companies, energy/utility companies and banking organizations when compared to 2015.

“Locky” emerged as the go-to ransomware family of 2016, used in 1 out of every 4 ransomware-based attacks.

The top five ransomware families seen in 2016 were Locky, CryptoWall, CryptXXX, Bitman and Onion (CTB Locker).

Overall, malware continues to target virtually every industry with manufacturing companies, non-profit organizations and utility/energy companies seeing the highest percentages of total malware in 2016.

NON-MALWARE ATTACKS ARE ON THE RISE

In the battle between attackers and security defenders, much is being discussed about attacks that rely on little or no malware. These 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.

Deployment of non-malware attacks in the wild has moved, with regularity, into attack campaigns. For example, earlier this year, Carbon Black discovered the first known instance of PowerShell being used in a ransomware attack with PowerWare. By using PowerShell, PowerWare avoids writing new files to disk and tries to blend in with more legitimate computer activity.

For the research included in this report, Carbon Black analyzed more than a thousand customers (representing more than 2.5 million endpoints) to understand the prevalence and growth of attacks.

For the purposes of investigating non-malware attacks, Carbon Black focused on instances of PowerShell and WMI used for malicious intent.

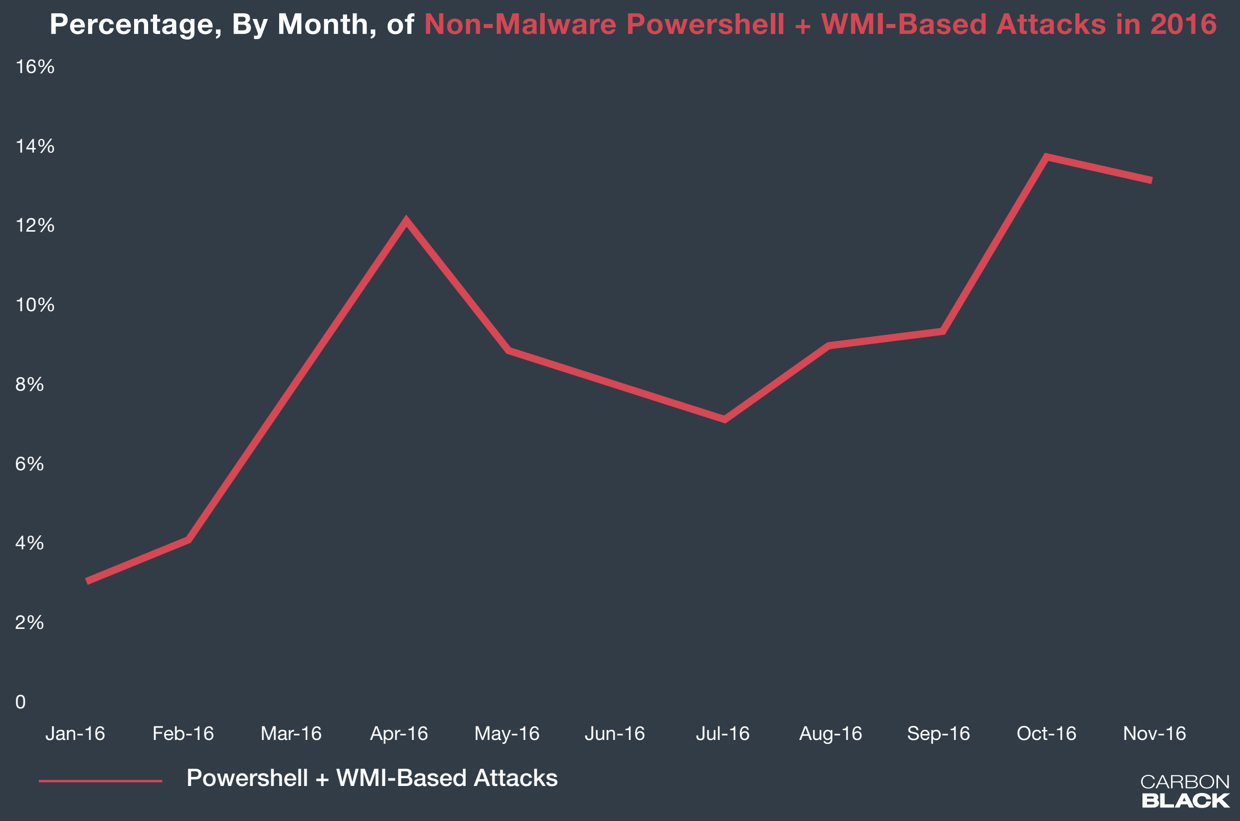
NON-MALWARE ATTACKS USE **TRUSTED PROGRAMS**, NATIVE TO OPERATING SYSTEMS, TO GAIN CONTROL OF COMPUTERS.

GROWTH OF NON-MALWARE ATTACKS IN 2016

Virtually every organization included in Carbon Black's research was targeted by a non-malware attack in 2016.

Instances of non-malware **attacks leveraging PowerShell and Windows Management Instrumentation (WMI) spiked by more than 90% in the second quarter of this year (+93.2%)** and, after a brief reprieve, have grown to the **highest levels we've seen** in 2016 as we close out the year.

The alleged hack against the Democratic National Committee (DNC) earlier this year was reported to have leveraged both PowerShell and WMI in order for attackers to move laterally and remain undetected.



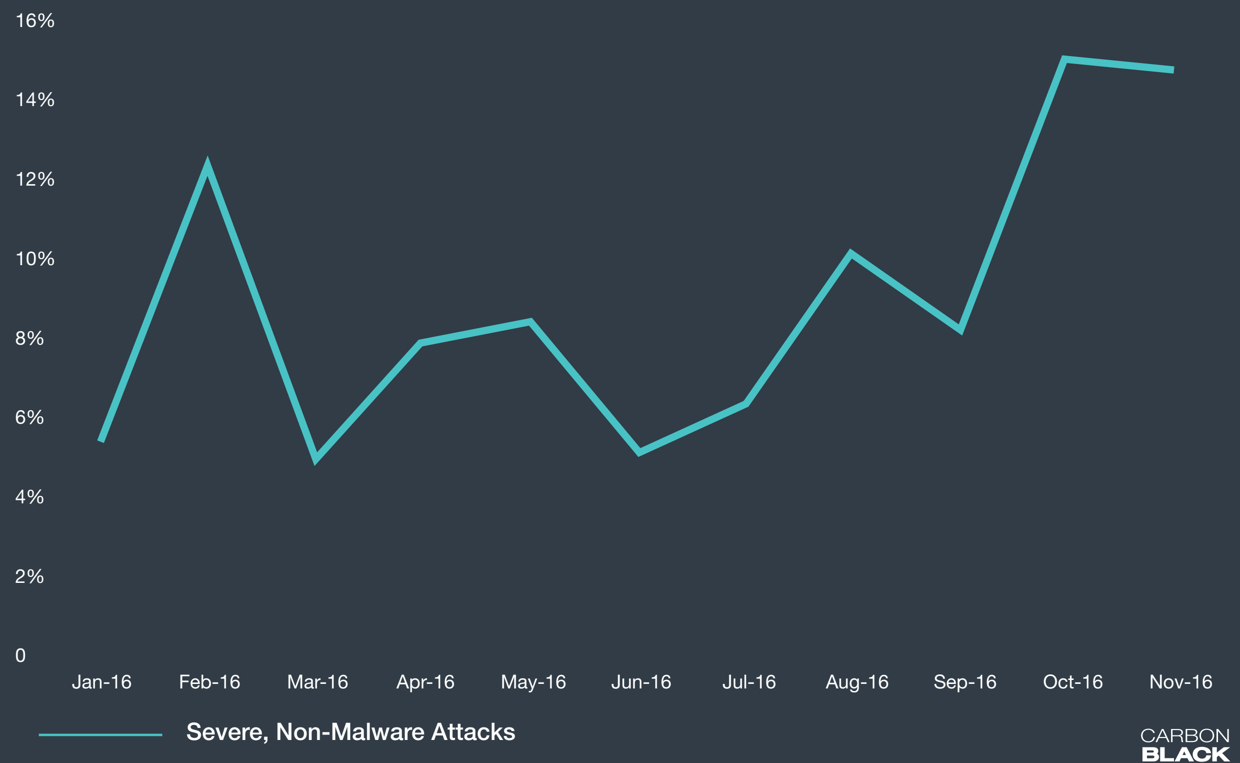
Additionally, “severe” non-malware attacks are on the rise 2016. In **Q4 of 2016, Carbon Black customers saw 33% more severe non-malware attacks than they did in Q1 of 2016.**

The number of **severe non-malware attacks has been steadily growing** since Q2 of this year, jumping 16.4% from Q2 to Q3 and 21.4% from Q3 to Q4.

A severe, non-malware attack is classified as an attack that often includes suspicious command lines, delivering executable code directly to PowerShell and exhibits some type of additional malicious techniques during execution (such as executing dynamically delivered shellcode, reading memory of other processes, or injecting into other running processes.)

OVER A 90-DAY PERIOD, ABOUT **ONE-THIRD OF ORGANIZATIONS** ARE LIKELY TO ENCOUNTER AT LEAST ONE, SEVERE, NON-MALWARE ATTACK.

Percentage, By Month, of Severe Non-Malware Attacks in 2016

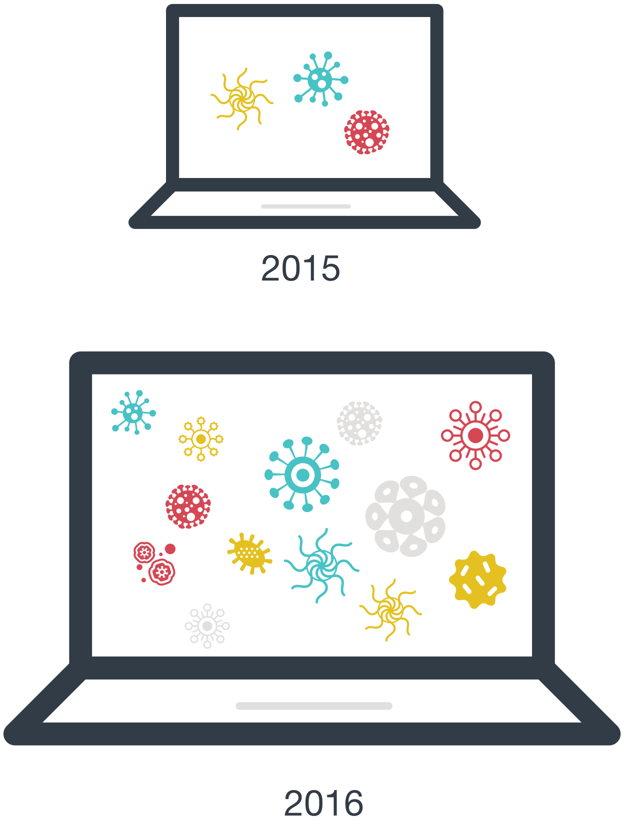


THE RISE AND GROWTH OF RANSOMWARE

RANSOMWARE INSTANCES GREW BY MORE THAN 50% IN 2016 WHEN COMPARED TO 2015.

While ransomware is more than 30-years-old, it experienced a renaissance of sorts for attackers in 2016. According to Carbon Black data, the number of ransomware instances grew by more than 50% in 2016 when compared to 2015.

Ransomware grew by more than 50% from 2015 to 2016



CARBON
BLACK

$ $ $

RANSOMWARE IS ON TRACK TO BE AN

$850 MILLION

CRIME IN 2016

Attackers' motivation for utilizing ransomware is clear. It's on track to be an $850 million crime in 2016, according to FBI data. That's a substantial increase from 2015, when ransomware was a "mere" $24 million crime.

Total Ransom Money Paid to Attackers by Businesses

$24 Million

2015

$850 Million

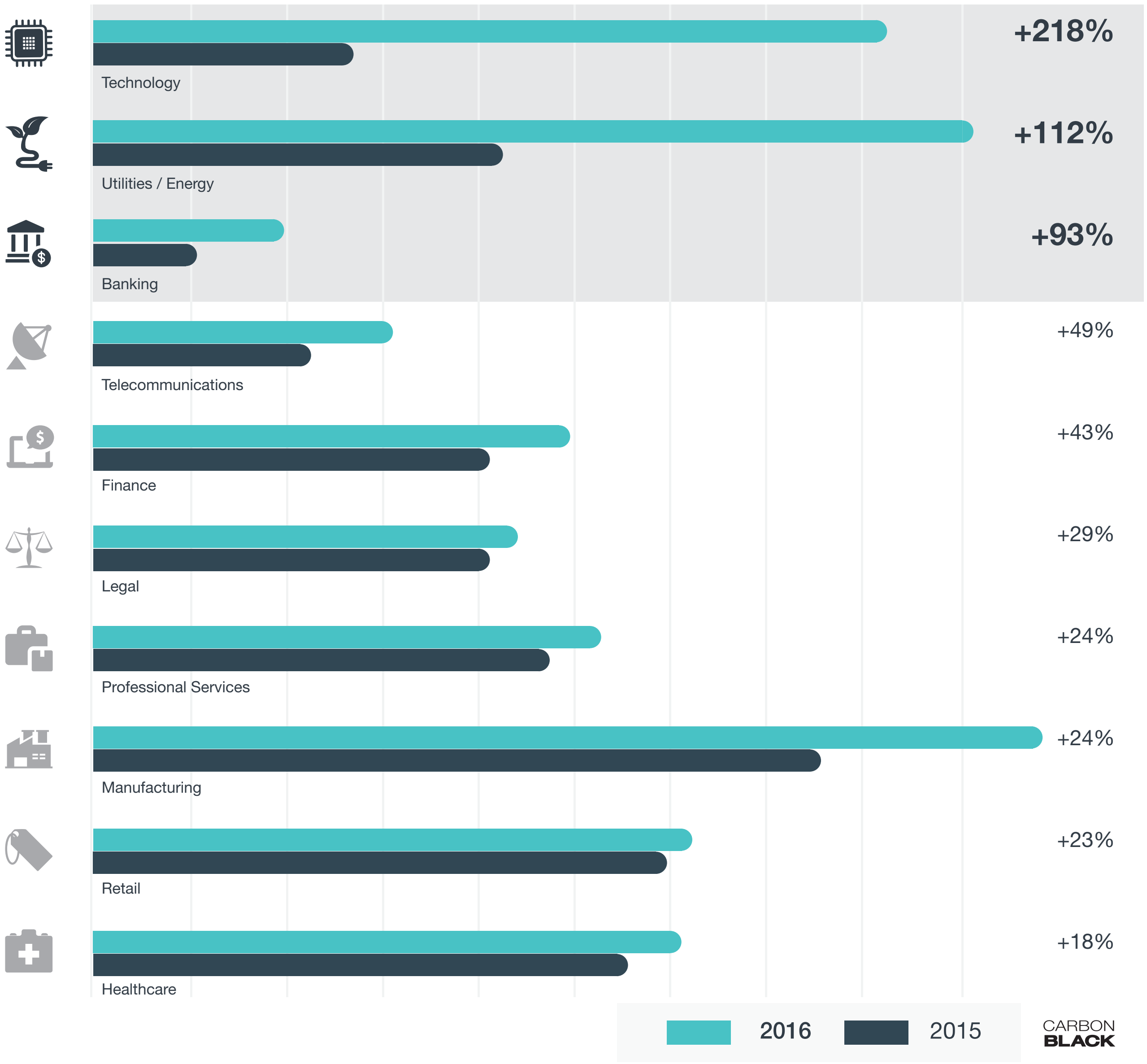
2016

CARBON BLACK

Ransomware has emerged as the fastest-growing malware category across all industries in 2016, with major **increases seen at technology companies, energy/utility companies and financial organizations** since 2015.

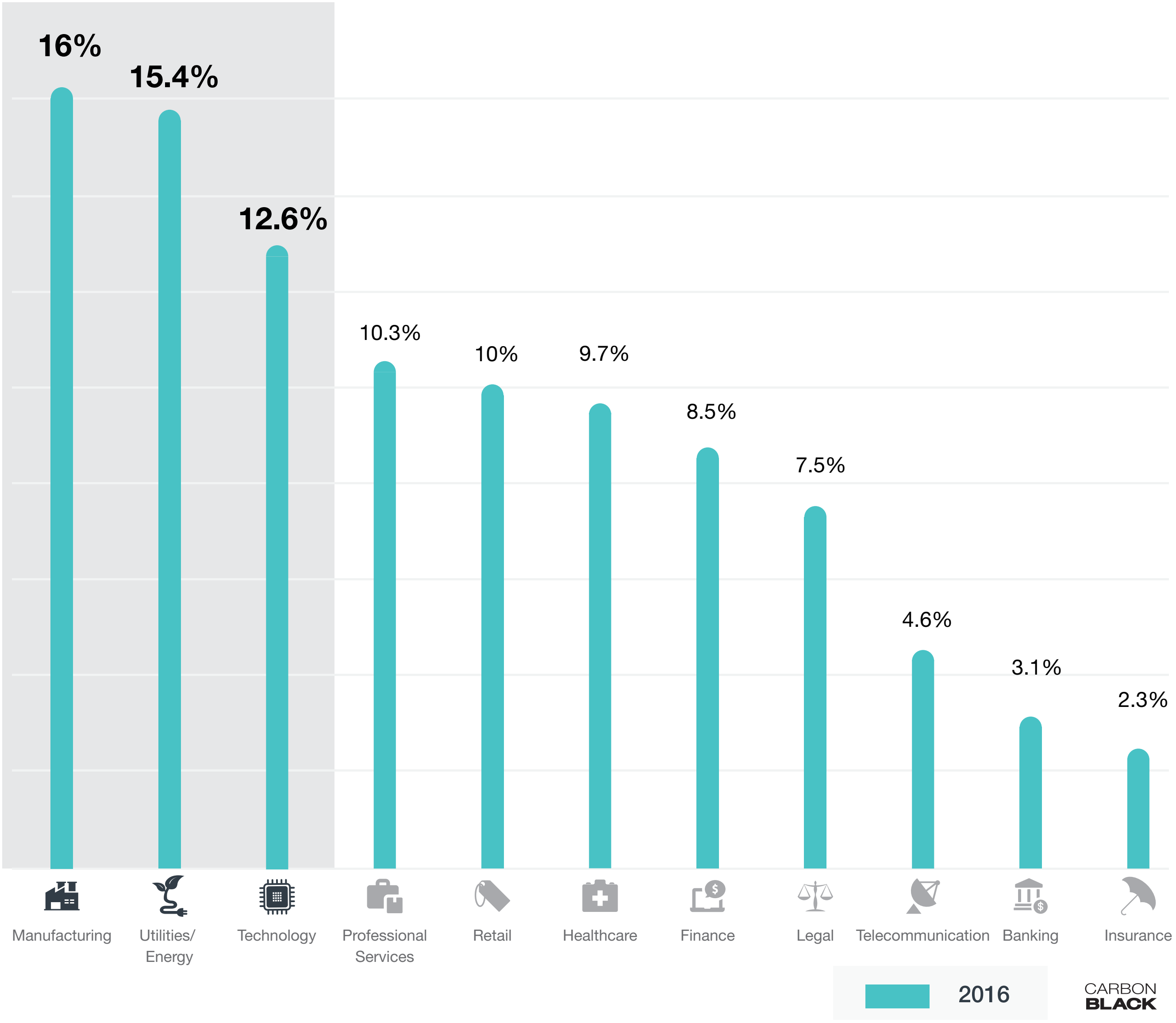
Ransomware is quickly evolving in sophistication as well. Payloads are increasingly infecting hundreds of machines at once, as occurred during the attack against the San Francisco Municipal Transport Agency, where more than 2,000 systems were locked down.

Year-over-Year Ransomware Growth by Industry in 2016



When considering the total amount of ransomware seen this year, **manufacturing companies** (16% of total ransomware instances), **utility/energy companies** (15.4% of all ransomware instances) and **technology companies** (12.6% of all ransomware instances) led the way.

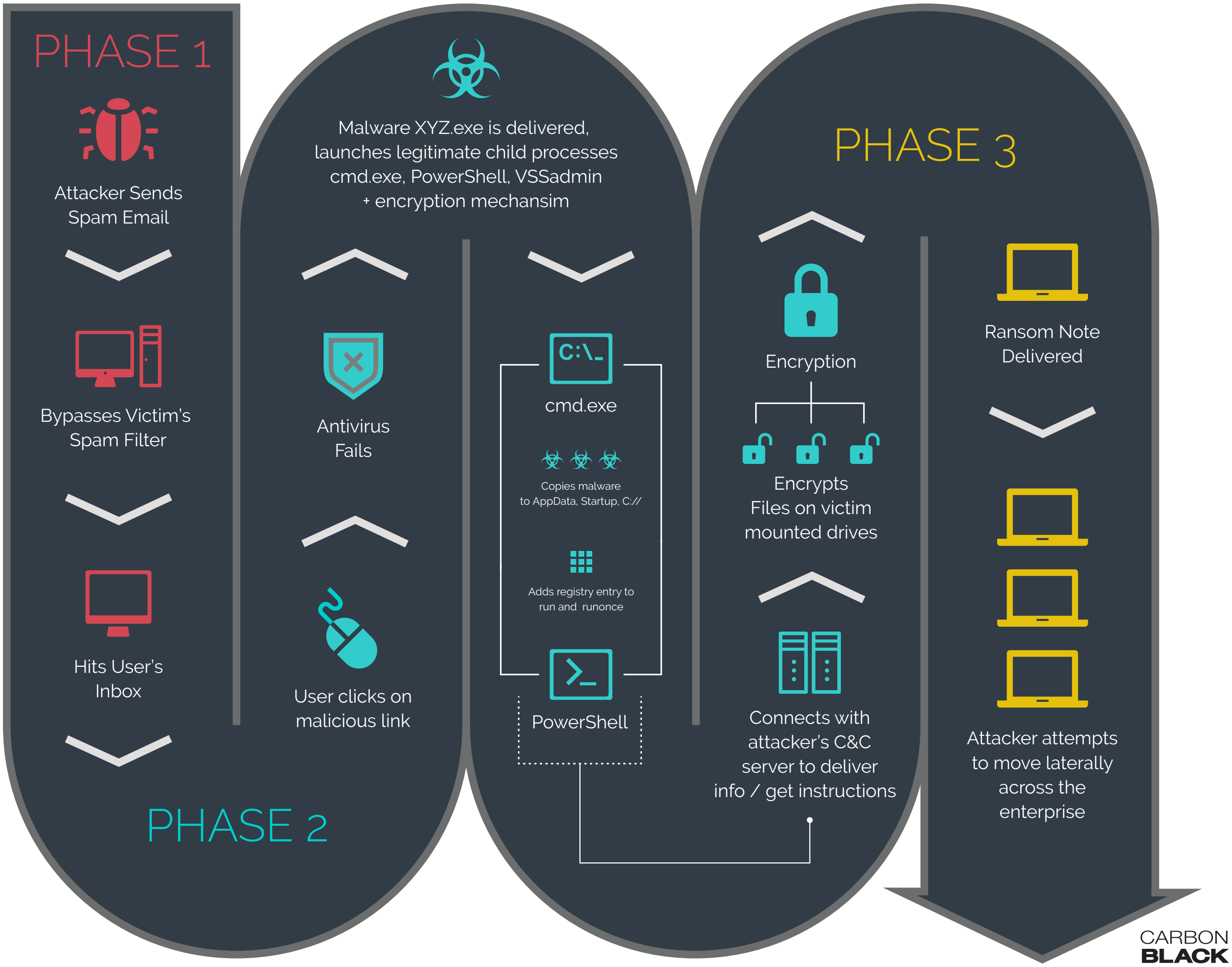
Percentage of Total Ransomware by Industry in 2016



Locky emerged as the go-to ransomware family for attackers in 2016, used in 1 out of every 4 ransomware-based attacks.

Released in 2016, Locky ransomware is typically delivered via a phishing email that prompts a targeted victim to enable malicious macros via Microsoft Word. These macros then run a file that delivers an encryption trojan, which prevents the victim from accessing their files. Following the file encryption, the victim receives a message with instructions on how to pay a Bitcoin ransom to decrypt the files.

HERE'S HOW A TYPICAL RANSOMWARE ATTACK WORKS:


PHASE 1
Attacker Sends Spam Email
Bypasses Victim's Spam Filter
Hits User's Inbox
PHASE 2
User clicks on malicious link
Antivirus Fails
Malware XYZ.exe is delivered, launches legitimate child processes cmd.exe, PowerShell, VSSadmin + encryption mechansim
C:_
cmd.exe
Copies malware to AppData, Startup, C://
Adds registry entry to run and runonce
PowerShell
PHASE 3
Encryption
Encrypts Files on victim mounted drives
Connects with attacker's C&C server to deliver info / get instructions
Ransom Note Delivered
Attacker attempts to move laterally across the enterprise
CARBON BLACK

Locky gained notoriety in February 2016, when the Hollywood Presbyterian Medical Center was hit with a Locky attack and then paid an alleged $17,000 Bitcoin ransom to decrypt patient data.

Locky has evolved several times in since February in an effort to further deceive targeted victims. Most recently, attackers have been using Facebook instant messaging to spread Locky ransomware.

LOCKY EMERGED AS THE GO-TO RANSOMWARE FAMILY FOR ATTACKERS IN 2016, USED IN 1 OUT OF EVERY 4 RANSOMWARE-BASED ATTACKS.

TOP 5 RANSOMWARE FAMILIES SEEN IN 2016

1 - LOCKY

2 - CRYPTOWALL

3 - CRYPTXXX

4 - BITMAN

5 - ONION (CTB LOCKER)

TOP 5 RANSOMWARE FAMILIES SEEN IN 2015

1 - CRYPTOWALL

2 - BLOCKER

3 - ONION (CTB LOCKER)

4 - SNOCRY

5 - BITMAN

SECURITY RECOMMENDATIONS FOR RANSOMWARE

Ransomware infections can be devastating and recovery efforts threaten to financially cripple an organization. Prevention is the most effective defense. Here are 14 additional best practices recommended by the U.S. government and other experts to combat ransomware:

1. **Back up data regularly.** Verify the integrity of those backups and test the restoration process to ensure it's working.

2. **Secure your offline backups.** Backups are essential. If you're infected, a backup may be the only way to recover your data. Ensure backups are not connected permanently to the computers and networks they are backing up.

3. **Configure firewalls** to block access to known malicious IP addresses.

4. **Logically separate networks.** This will help prevent the spread of malware. If every user and server is on the same network, newer variants can spread.

5. **Patch operating systems, software, and firmware on devices.** Consider using a centralized patch-management system.

6. **Implement an awareness and training program.** End users are targets, so everyone in your organization needs to be aware of the threat of ransomware and how it's delivered.

7. **Scan all incoming and outgoing emails** to detect threats and filter executable files from reaching end users.

8. **Enable strong spam filters to prevent phishing emails** from reaching end users and authenticate inbound email using technologies such as Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent spoofing.

9. **Block ads.** Ransomware is often distributed through malicious ads served when visiting certain sites. Blocking ads or preventing users from accessing certain sites can reduce that risk.

10. **Use the principle of "least privilege" to manage accounts.** No users should be assigned administrative access unless absolutely needed. If a user only needs to read specific files, the user should not have write access to them.

11. **Leverage next-generation anti-virus technology** to inspect files and identify malicious behavior to block malware and malware-less attacks that exploit memory and scripting languages like PowerShell.

12. **Use application whitelisting,** which only allows systems to execute programs known and permitted by security policy.

13. **Categorize data based on organizational value** and implement physical and logical separation of networks and data for different organizational units.

14. **Conduct an annual penetration test** and vulnerability assessment.

RANSOMWARE STILL JUST A PIECE OF THE MALWARE PICTURE

While ransomware continues to generate headlines, it is still only a piece of the overall malware scope. Even with its rapid growth, ransomware still only accounts for 2% of total malware seen in 2016. In the graphic below, Locky, which was the most prevalent ransomware family seen in 2016 according to Carbon Black data, ranks 13th when stacked against other types of malware.

Percentage of Malware by Family in 2016

13.4%	Kazy
13.1%	Razy
11.4%	Graftor
11.17	Generic Injector/ downloader
10.56	Zegost
10.11	Symmi
8.92	Kovter
6.85	Zusy
3.62	Strictor
2.94	BitCoinMiner
2.90	Kryptik
2.77	Yakes
2.17	Locky

EVEN WITH ITS RAPID GROWTH, RANSOMWARE STILL ONLY ACCOUNTS FOR **2% OF TOTAL MALWARE** SEEN IN 2016.

PERCENTAGE OF TOTAL MALWARE SEEN BY INDUSTRY IN 2016

Overall, malware continues to target every industry with **manufacturing** companies (21.8% of total malware), **non-profit** organizations (16.4% of total malware), and **utility/energy** companies (15.6% of total malware) leading the way in 2016.

NON-MALWARE ATTACKS ARE AT THE **HIGHEST LEVELS** WE'VE SEEN AND SHOULD BE A **MAJOR FOCUS FOR SECURITY** DEFENDERS DURING THE COMING YEAR.

Manufacturing	**21.8%**
Non-Profit	**16.4%**
Utilities/Energy	**15.6%**
Telecommunications	10.1%
Technology	8.6%
Retail	8.1%
Healthcare	5.8%
Finance	5.0%
Business Products & Services	4.6%
Legal	3.9%

CARBON BLACK

PREDICTIONS FOR 2017

NON-MALWARE ATTACKS WILL CONTINUE TO RISE AND BECOME MORE SEVERE.

The trend in our graphs detailing non-malware attack instances in 2016 offer cause for concern. After seeing an initial spike in Q2 of this year, we began to see non-malware attack instances trending downward. This brief trend was reversed in July and we haven't looked back since. As we turn the calendar to 2017, non-malware attacks are at the highest levels we've seen and should be a major focus for security defenders during the coming year.

THE RANSOMWARE BLITZ WILL CONTINUE.

While mass malware still accounts for the majority of total malware, ransomware is stealing the headlines. Unfortunately, that's because it works and has resulted in major paydays for attackers. In 2015, ransomware was a $24 million crime. As we close out 2016, businesses from all industries have lost more than $850 million to ransomware. Organizations looking to defend against ransomware in 2017 should be well versed in the ransomware cheat sheet presented earlier in this document to defend against the expected continuation of ransomware attacks in 2017.

CYBER-SECURITY INVESTMENTS WILL RISE ON A NATIONAL AND GLOBAL SCALE.

Organizations are quickly coming to the realization that traditional antivirus does very little to stop modern attacks. The proliferation of non-malware attacks has only accentuated this issue. Major global hacks against SWIFT and the Ukraine power grid, among others, have served as clarion calls that critical infrastructure and worldwide financial systems will continue to be targeted. In the U.S., alleged attacks against voter databases and the election process have placed a renewed emphasis on cyber security as an issue of national security. As a result, we will see a significant shift away from traditional antivirus solutions around the globe in 2017 as private organizations and worldwide governing bodies effort to curb the growing trend of attacks seen this year.

METHODOLOGY

For this report, Carbon Black analyzed data from more than 1,000 customers of Cb Protection and Cb Defense (totaling more than 2.5 million endpoints) to determine the prevalence of malware, ransomware and non-malware attacks in 2016. For non-malware attacks, nefarious usage of both PowerShell and WMI were considered. “Severe” non-malware attacks meant attacks included suspicious command lines, delivering executable code directly to PowerShell, and exhibited some type of additional malicious techniques during execution (such as executing dynamically delivered shellcode, reading memory of other processes, or injecting into other running processes.)

To learn more on how to defend against non-malware attacks, register for the upcoming webinar: **“The Rise of Malware-Less Attacks: How Can Endpoint Security Keep Up?”**

CARBON
BLACK

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

www.carbonblack.com

ABOUT CARBON BLACK

Carbon Black is the leading provider of a next-generation endpoint-security platform designed to enable organizations to stop the most attacks, see every threat, close security gaps, and evolve their defenses. The Cb Endpoint Security Platform helps organizations of all sizes replace legacy antivirus technology, lock down systems, and arm incident response teams with advanced tools to proactively hunt down threats. Today, Carbon Black has approximately 2,000 worldwide customers, including 25 of the Fortune 100 and more than 650 employees. Carbon Black was voted Best Endpoint Protection by security professionals in the SANS Institute’s Best of 2015 Awards.