BEWARE THE

BEASTLY THREATS

OF IT SECURITY

TABLE OF CONTENTS

An ominous headline in the *L.A. Times* proclaims, “2016 is shaping up as the year of ransomware—and the FBI isn’t helping.”[1]

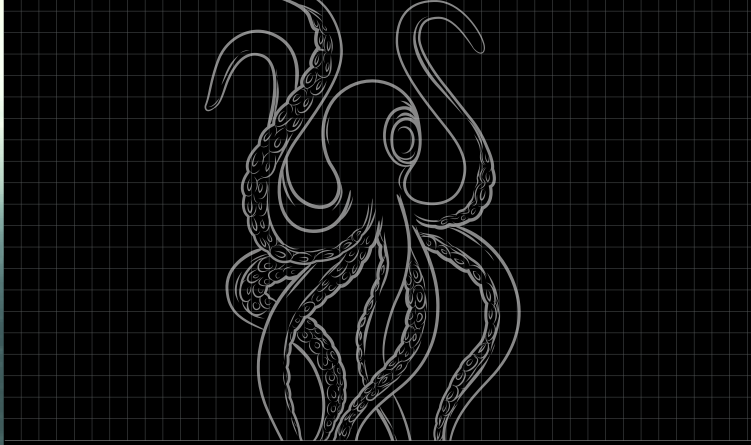
INTRODUCTION

An ominous headline in the *L.A. Times* proclaims, “2016 is shaping up as the year of ransomware—and the FBI isn’t helping.”[1] This was written days after the U.S. Internal Revenue Service warned payroll and HR professionals about the growing trend of Business Email Compromise attacks targeting tax-related data.[2]

And these are just two of the beastly threats stalking the internet, trying to steal your company’s data, money and peace of mind.

With one billion users, the internet offers a vast hunting ground for these attacks. In 2014, about 84 million new strains of malware were created—230,000 new viruses each day.[3] Large businesses and websites of all types were attacked or had client data stolen, affecting millions of users across the world.

And it’s only going to get worse, as cyber-criminals find new ways to smash through security software. This eBook explores the beastly threats scratching at the perimeter of your company’s computers and IT networks, and where these threats are trending.



Security Beast:

DEVICE THEFT/LOSS

Primary Attack Method:

"Sneak and grab"

Too often, device thieves gain easy access to onboard data with the press of a button or swipe of a finger

Characteristics:

Overlooked

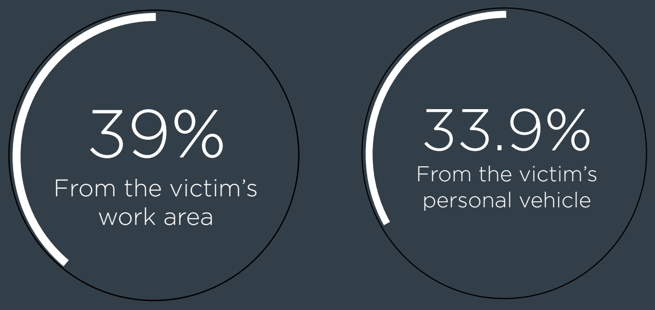
Unlocked

Unreported

In many cases, the most beastly IT threat of them all is a lost or stolen device. First of all, devices are too often left up for grabs from the desks on which they reside. In addition, a lack of encryption on desktop PCs, laptops, tablets and even phones leaves the data exposed on these devices. In 2014 alone, a quarter of companies experienced theft of a mobile device, continuing an upward trend.[4] In the healthcare sector alone, 68% of data breaches since 2010 have been due to device theft or loss, according to one report.[5]

Another issue? End users aren't so great about passwords. Only 58% of device users protect all their devices with passwords—and 16% don't password-protect any. The same goes for tablets, with 39% of tablet users failing to use passwords.[4]

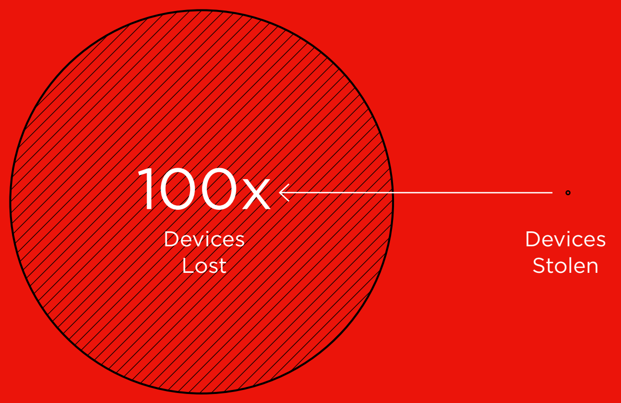
THEFT MOST OFTEN OCCURS:[6]



39% From the victim's work area

33.9% From the victim's personal vehicle

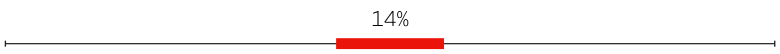
A DEVICE IS LOST >100X MORE FREQUENTLY THAN IT'S STOLEN.[6]



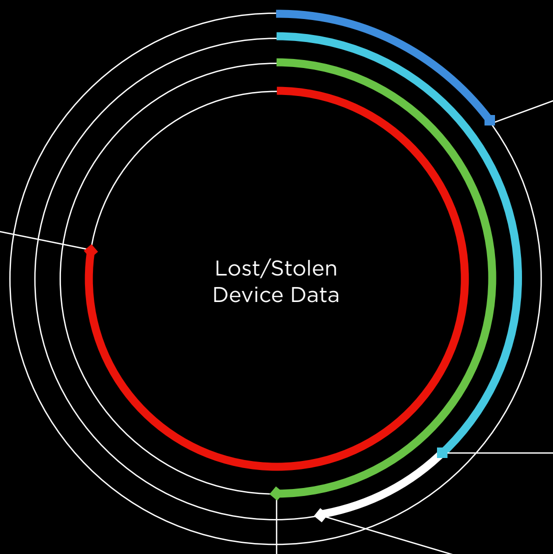
100x Devices Lost

Devices Stolen

LOST/STOLEN DEVICE DATA



In one year, 14% of respondents in a Kaspersky Lab study had lost a connected device or had it stolen. The study also found:[7]



Lost/Stolen Device Data

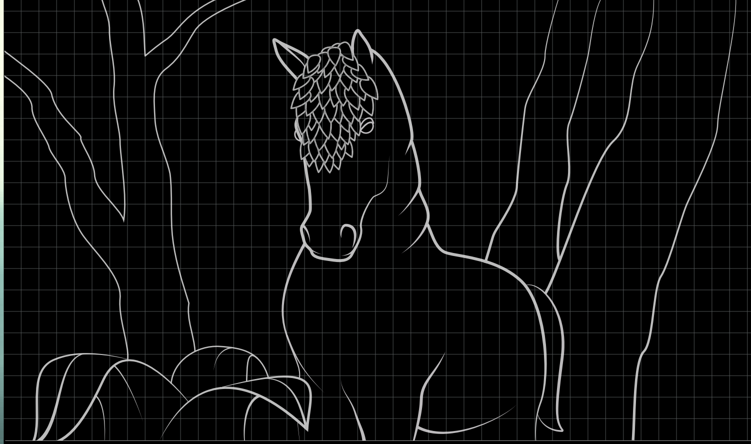
15% of lost data was never recovered.

For 77% of respondents, the loss or theft of a device had far-reaching consequences.

38% took up to two days to notify their employers

9% waited between three and five days.

Only 50% of employees reported a stolen device on the same day the incident occurred.



Security Beast:

TROJAN HORSE

Primary Attack Method:

Sneaking in the door

Providing unauthorized, remote access to the computer, allowing viruses to invade

Characteristics:

Data loss

Systems hijacked

Viruses intruding

Then, there are the IT threats that hide in plain sight. With their legendary sneakiness, Trojan horses again topped the list of new malware created in 2015, comprising more than 50% of all new malware.[8] Trojans are a very big reason that nearly one-third of computers worldwide have been struck by malicious software in one form or another.[9]

For example, after takedown operations against Zeus (aka Trojan.Zbot) and the Dyre group in 2015, the number of Trojan infections dropped by 73%. But 547 institutions in 49 countries were still targeted by at least 656 financial Trojans last year.[11]

FINANCIAL TARGETS

The two most targeted banks were located in the U.S. and were attacked by 78.2% and 77.9% of all analyzed Trojans.

78.2%

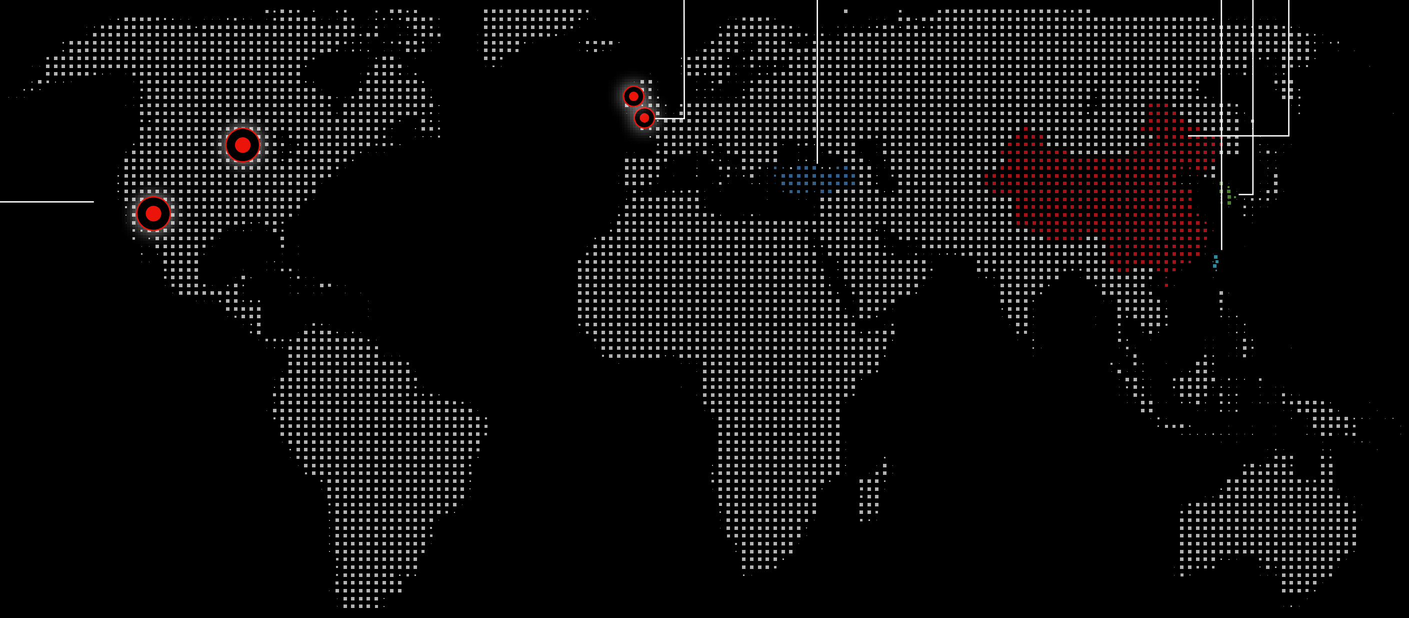
77.9%

Next were two banks in the U.K., with 69.36% each.[11]

69.36%

COUNTRIES MOST AFFECTED BY MALWARE:[9]

China	56% 🟥
South Korea	51% 🟩
Taiwan	44% 🟦
Turkey	43% 🟦

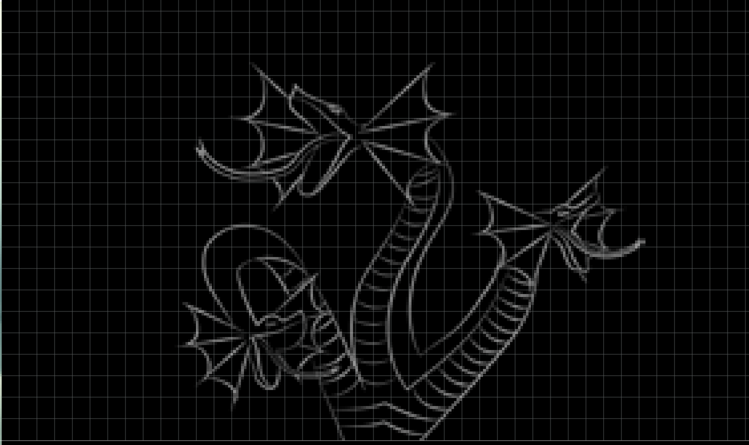


In 2014, 9 of the most common and sophisticated financial Trojans:

compromised **4.1 million** user's computers

&

targeted the customers of **1,467** institutions.[10]



Security Beast:

RANSOMWARE

Primary Attack Method:

Extortion

Encrypting sensitive data, then demanding a sum of money to decrypt it

Characteristics:

Infiltration

Restriction

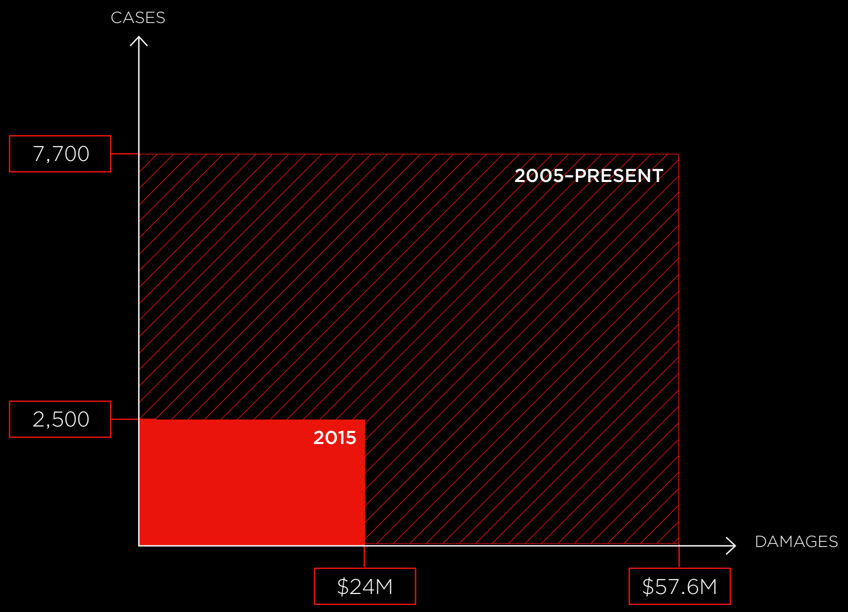
Demands

More and more cybercriminals are launching venomous attacks through ransomware. Unfortunately, these ransomware attacks are predicted to become even more common in the future—targeting more platforms and demanding bigger payouts. Kaspersky Lab researchers have called ransomware the biggest cybersecurity threat.[12]

While currently not the most common malware, ransomware infections in April 2016 more than doubled the total amount from March 2016. And ransomware made up a larger percentage of overall infections in April than in any other month in the last three years.[15]

PUBLIC COMPLAINTS HAVE INCREASED SHARPLY

Ransoms paid were generally $200 to $10,000.[3]



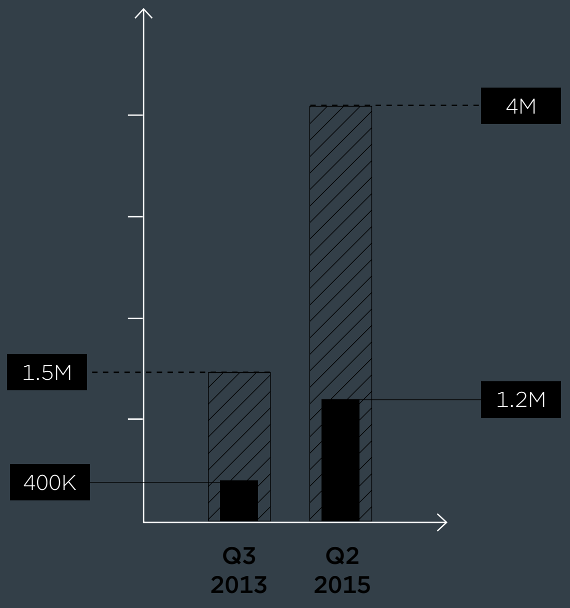
▨ 2005–Present

Since 2005, the Internet Crime Complaint Center has received nearly 7,700 public complaints about ransomware, totaling $57.6M in damages, including costs incurred in dealing with the attack and estimated value of data lost.[13]

🟥 2015

In 2015 alone, victims paid >$24M across nearly 2,500 cases reported.[13]

RANSOMWARE SAMPLES HAVE TRIPLED



TOTAL SAMPLES ▨

NEW SAMPLES ■

McAfee Labs saw more than 4M samples of ransomware in Q2 2015, including 1.2M new ones, and expect instances to grow in 2016.

That compares to <1.5M total samples in Q3 2013, when <400,000 were new.[14]

Security Beast:

PHISHING

Primary Attack Method:

Backstabbing

Acquiring sensitive info by masquerading as a trustworthy entity (e.g., website)

Characteristics:

Sneaky

Stealthy

? Misleading

With a perfectly innocent disguise, phishing threats are making a dramatic impact. In February 2016, there were 293,747 phishing sites on the internet, an increase of over 150% from just seven months earlier.[16] Phishing costs large companies on average $3.7 million a year, a Ponemon study revealed.[17] The SANS Institute, a leading provider of cyber-security training, found that 95% of all attacks on enterprise networks gained access via a spear-phishing attack.[18]

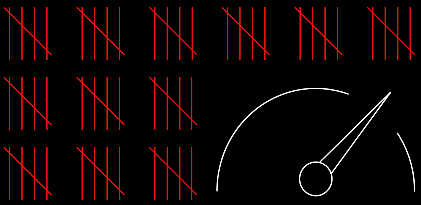
Spear phishing is the primary initial attack vector used by advanced persistent threats (APTs). In addition, 22% of spear-phishing attacks analyzed in 2015 were motivated by financial fraud or related crimes.[19]

SOCIAL MEDIA

is a primary promotion and distribution channel for consumer-focused phishing kits and related goods or services.[19]

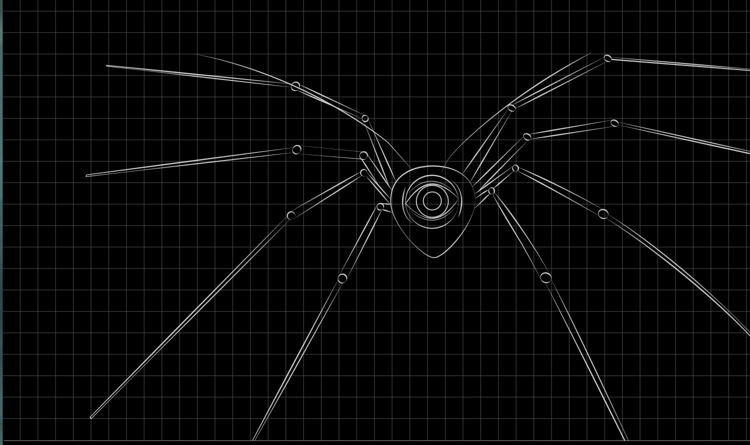
Top targets for most consumer-phishing attacks:[9]

- financial institutions
- cloud storage/file hosting sites
- webmail and online services
- ecommerce sites
- payment services



60 days:

The fastest average response after compromise notification, in the past year[16]



Security Beast:

SPYWARE

Primary Attack Method:

Watching and learning

Obtaining covert information about computer activities by transmitting hard drive data

Characteristics:

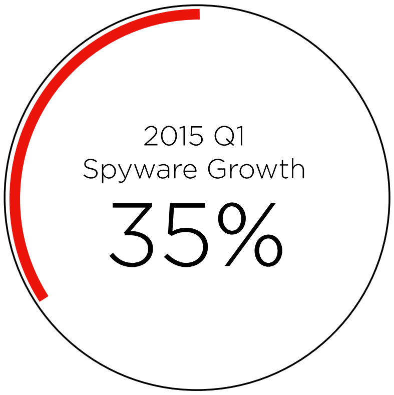
Watchful

Silent

Hidden

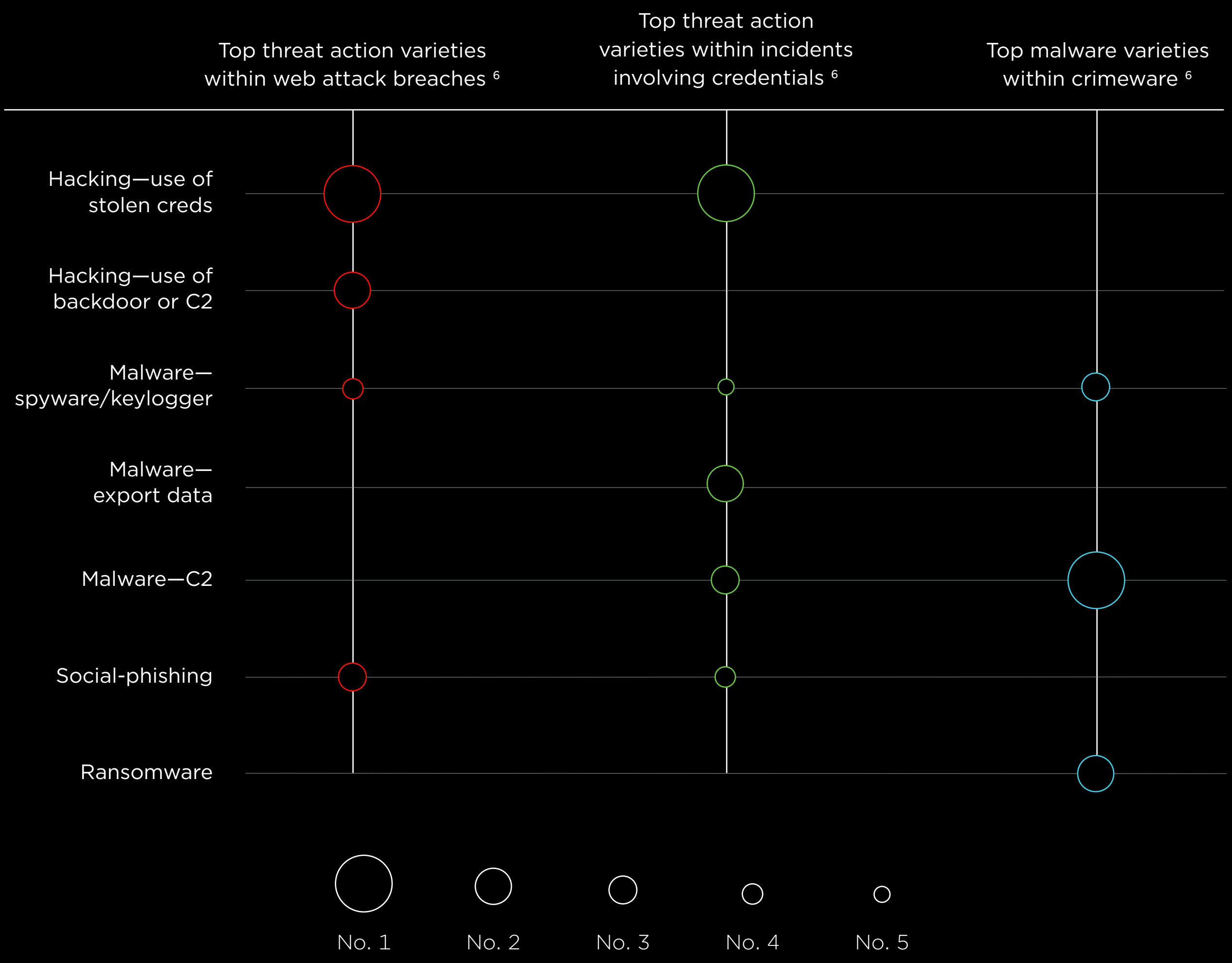
The threat of spyware looms virtually everywhere. While its watchful eye often affects personal-use computers—one source says 8 million U.S. households had spyware problems in a six-month period in 2014[20]—this threat has devastating effects on business, as well. Cybercriminals use spyware to collect—and exploit— valuable customer account data, medical records and other proprietary information.

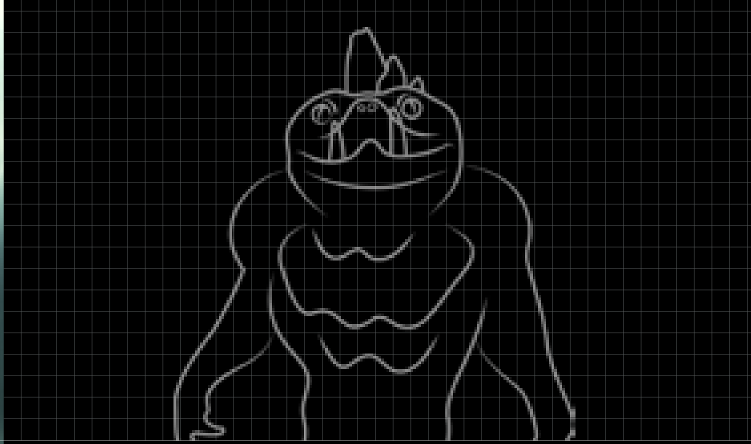
Two-thirds of U.K. big business firms had a cyber breach in 2015, and spyware was among the most common type of breach they experienced.[21]



The number of spyware programs captured by Kaspersky Lab products grew by 35% in Q1 2015.[12]

TOP THREAT RANKINGS





Security Beast:

DDoS

Primary Attack Method:

Denial of service

Using multiple compromised systems to target a single system and either flood or crash services

Characteristics:

Exploitation

Targeted

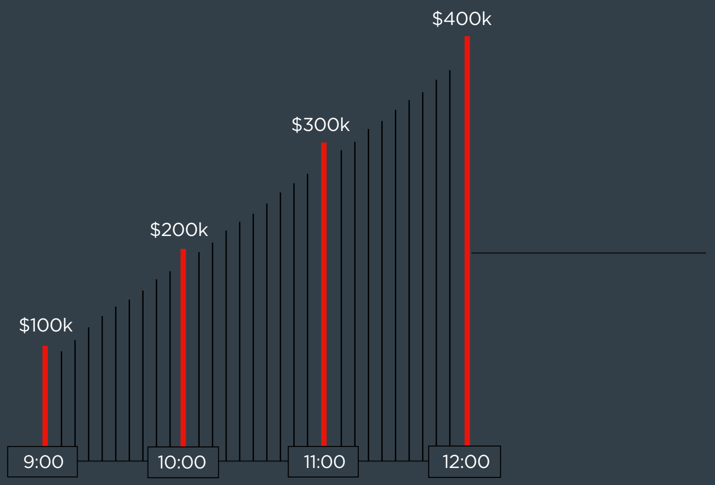
Team Player

Distributed denial-of-service (DDoS) attacks are growing in size and strength. In fact, these brute-force threats are increasingly crippling organizations with a flood of requests. Between 2013 and 2015, average peak bandwidth of DDoS doubled, according to one report.[22] And DDoS attacks targeted half of U.S.-based companies in 2014 and 2015.[23]

According to the United States Computer Emergency Readiness Team (US-CERT), symptoms of DDoS attacks include:[27]

- Unusually slow network performance
- Unavailability of website(s)
- Dramatic increase in spam received
- Disconnection of internet
- Long-term inability to access the web or any internet services

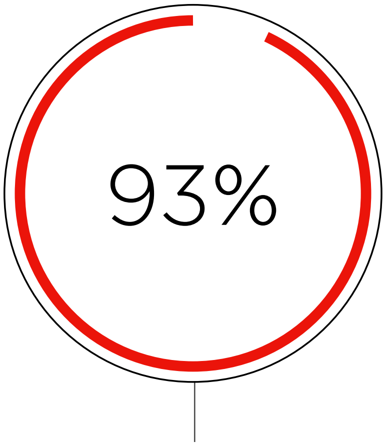
COST PER HOUR OF DOWNTIME



41%

$100,000+

Amount DDoS attacks cost 41% of businesses for every hour of downtime.[24]



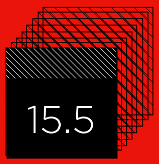
93% of survey respondents reported application-layer DDoS attacks—most commonly, DNS services[25]

DDoS ATTACKS

34% saw outbound DDoS attacks from servers within their network

33% saw DDoS attacks targeting cloud-based services

51% saw DDoS attacks saturate their internet connectivity



Length of longest DDoS attack detected and analyzed by Kaspersky Lab in 2015.[26]

15.5 days (371 hours)

FIGHTING OFF THESE THREATS ISN'T EASY.

It's essential that IT professionals have the right tools to build bulwarks against them. Battling threats is more critical for organizations than ever—in dollars and in brand reputation. It's time for a new hero—or a company that sets you up as the hero.

THE LENOVO THINKPAD X1 FAMILY HELPS KEEP YOU SAFE

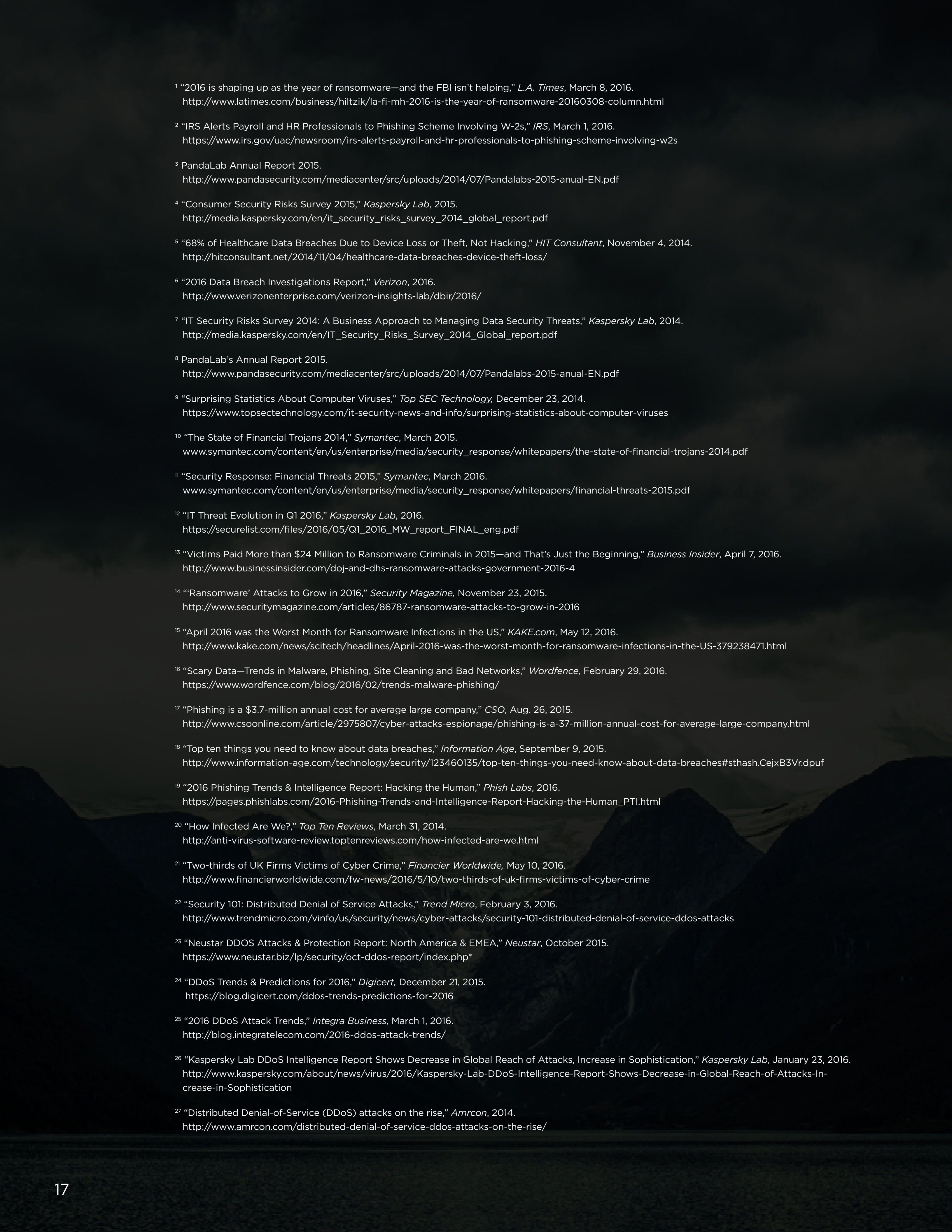
Lenovo gives you the awareness and the technology you need to address these threats, with products designed to secure your valuable data from loss, theft and all types of malware. The Lenovo ThinkPad X1 family is intelligently designed with advanced security features—from fingerprint readers to Trusted Platform Modules (TPMs) and Kensington locks—to help you save your organization from common security beasts.

LEARN MORE

Lenovo™

ThinkPad X1 YOGA

Featuring Intel® Core™ Processors.
Intel® Inside. Powerful Productivity Outside.



[1] “2016 is shaping up as the year of ransomware—and the FBI isn’t helping,” *L.A. Times*, March 8, 2016.
http://www.latimes.com/business/hiltzik/la-fi-mh-2016-is-the-year-of-ransomware-20160308-column.html

[2] “IRS Alerts Payroll and HR Professionals to Phishing Scheme Involving W-2s,” *IRS*, March 1, 2016.
https://www.irs.gov/uac/newsroom/irs-alerts-payroll-and-hr-professionals-to-phishing-scheme-involving-w2s

[3] PandaLab Annual Report 2015.
http://www.pandasecurity.com/mediacenter/src/uploads/2014/07/Pandalabs-2015-anual-EN.pdf

[4] “Consumer Security Risks Survey 2015,” *Kaspersky Lab*, 2015.
http://media.kaspersky.com/en/it_security_risks_survey_2014_global_report.pdf

[5] “68% of Healthcare Data Breaches Due to Device Loss or Theft, Not Hacking,” *HIT Consultant*, November 4, 2014.
http://hitconsultant.net/2014/11/04/healthcare-data-breaches-device-theft-loss/

[6] “2016 Data Breach Investigations Report,” *Verizon*, 2016.
http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

[7] “IT Security Risks Survey 2014: A Business Approach to Managing Data Security Threats,” *Kaspersky Lab*, 2014.
http://media.kaspersky.com/en/IT_Security_Risks_Survey_2014_Global_report.pdf

[8] PandaLab’s Annual Report 2015.
http://www.pandasecurity.com/mediacenter/src/uploads/2014/07/Pandalabs-2015-anual-EN.pdf

[9] “Surprising Statistics About Computer Viruses,” *Top SEC Technology,* December 23, 2014.
https://www.topsectechnology.com/it-security-news-and-info/surprising-statistics-about-computer-viruses

[10] “The State of Financial Trojans 2014,” *Symantec*, March 2015.
www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-state-of-financial-trojans-2014.pdf

[11] “Security Response: Financial Threats 2015,” *Symantec*, March 2016.
www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/financial-threats-2015.pdf

[12] “IT Threat Evolution in Q1 2016,” *Kaspersky Lab*, 2016.
https://securelist.com/files/2016/05/Q1_2016_MW_report_FINAL_eng.pdf

[13] “Victims Paid More than $24 Million to Ransomware Criminals in 2015—and That’s Just the Beginning,” *Business Insider*, April 7, 2016.
http://www.businessinsider.com/doj-and-dhs-ransomware-attacks-government-2016-4

[14] “‘Ransomware’ Attacks to Grow in 2016,” *Security Magazine,* November 23, 2015.
http://www.securitymagazine.com/articles/86787-ransomware-attacks-to-grow-in-2016

[15] “April 2016 was the Worst Month for Ransomware Infections in the US,” *KAKE.com*, May 12, 2016.
http://www.kake.com/news/scitech/headlines/April-2016-was-the-worst-month-for-ransomware-infections-in-the-US-379238471.html

[16] “Scary Data—Trends in Malware, Phishing, Site Cleaning and Bad Networks,” *Wordfence*, February 29, 2016.
https://www.wordfence.com/blog/2016/02/trends-malware-phishing/

[17] “Phishing is a $3.7-million annual cost for average large company,” *CSO*, Aug. 26, 2015.
http://www.csoonline.com/article/2975807/cyber-attacks-espionage/phishing-is-a-37-million-annual-cost-for-average-large-company.html

[18] “Top ten things you need to know about data breaches,” *Information Age*, September 9, 2015.
http://www.information-age.com/technology/security/123460135/top-ten-things-you-need-know-about-data-breaches#sthash.CejxB3Vr.dpuf

[19] “2016 Phishing Trends & Intelligence Report: Hacking the Human,” *Phish Labs*, 2016.
https://pages.phishlabs.com/2016-Phishing-Trends-and-Intelligence-Report-Hacking-the-Human_PTI.html

[20] “How Infected Are We?,” *Top Ten Reviews*, March 31, 2014.
http://anti-virus-software-review.toptenreviews.com/how-infected-are-we.html

[21] “Two-thirds of UK Firms Victims of Cyber Crime,” *Financier Worldwide,* May 10, 2016.
http://www.financierworldwide.com/fw-news/2016/5/10/two-thirds-of-uk-firms-victims-of-cyber-crime

[22] “Security 101: Distributed Denial of Service Attacks,” *Trend Micro*, February 3, 2016.
http://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/security-101-distributed-denial-of-service-ddos-attacks

[23] “Neustar DDOS Attacks & Protection Report: North America & EMEA,” *Neustar*, October 2015.
https://www.neustar.biz/lp/security/oct-ddos-report/index.php*

[24] “DDoS Trends & Predictions for 2016,” *Digicert,* December 21, 2015.
https://blog.digicert.com/ddos-trends-predictions-for-2016

[25] “2016 DDoS Attack Trends,” *Integra Business*, March 1, 2016.
http://blog.integratelecom.com/2016-ddos-attack-trends/

[26] “Kaspersky Lab DDoS Intelligence Report Shows Decrease in Global Reach of Attacks, Increase in Sophistication,” *Kaspersky Lab*, January 23, 2016.
http://www.kaspersky.com/about/news/virus/2016/Kaspersky-Lab-DDoS-Intelligence-Report-Shows-Decrease-in-Global-Reach-of-Attacks-Increase-in-Sophistication

[27] “Distributed Denial-of-Service (DDoS) attacks on the rise,” *Amrcon*, 2014.
http://www.amrcon.com/distributed-denial-of-service-ddos-attacks-on-the-rise/

Insight®

Work smarter.

At Insight, we'll help you solve challenges and improve performance with Intelligent Technology Solutions™.

Learn more