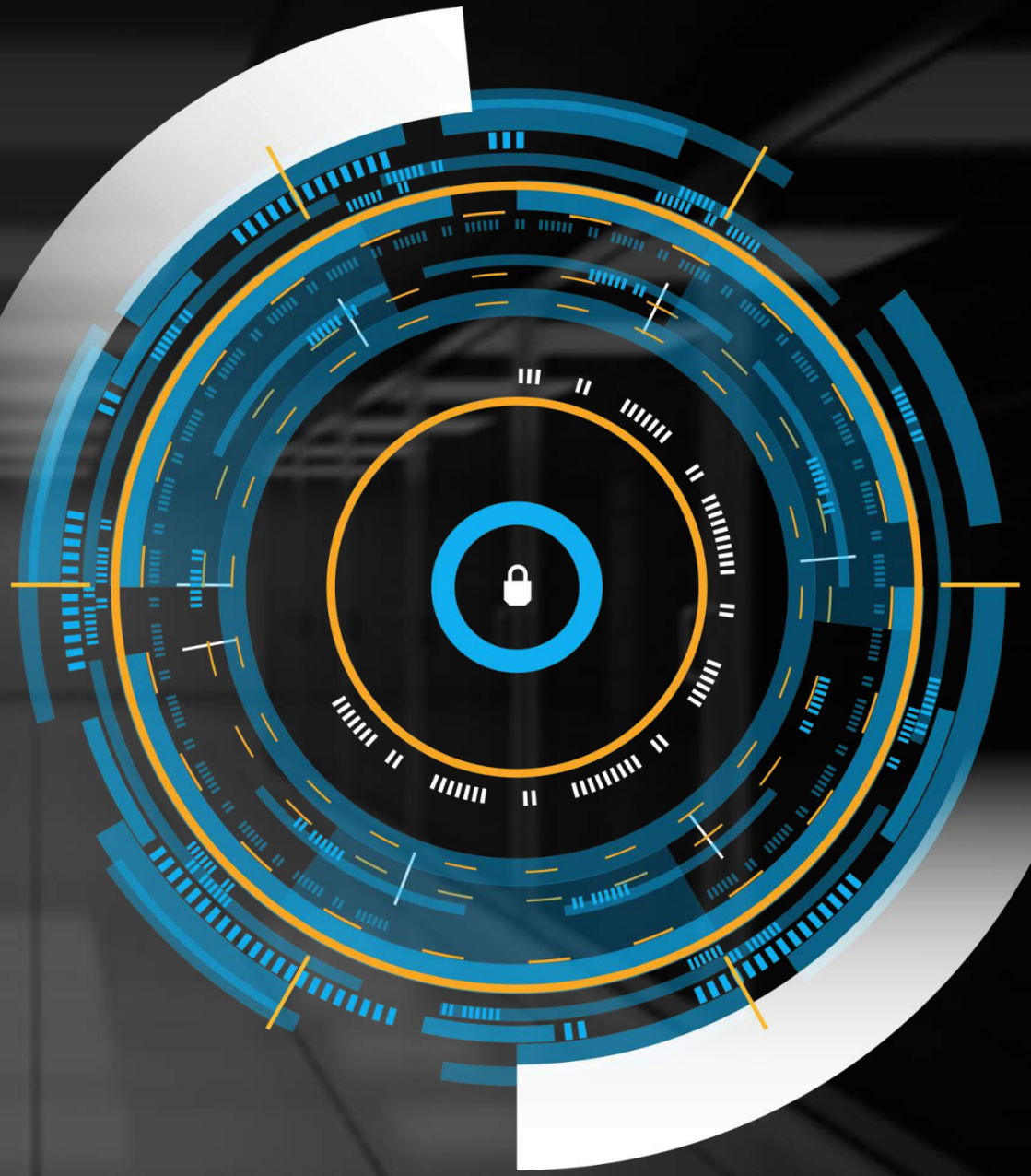
Symantec

ISTR

Internet Security Threat Report



Insert Name Here
Insert Title Here

In 2009 there were

2,361,414

new piece of malware created.

In 2015 that number was

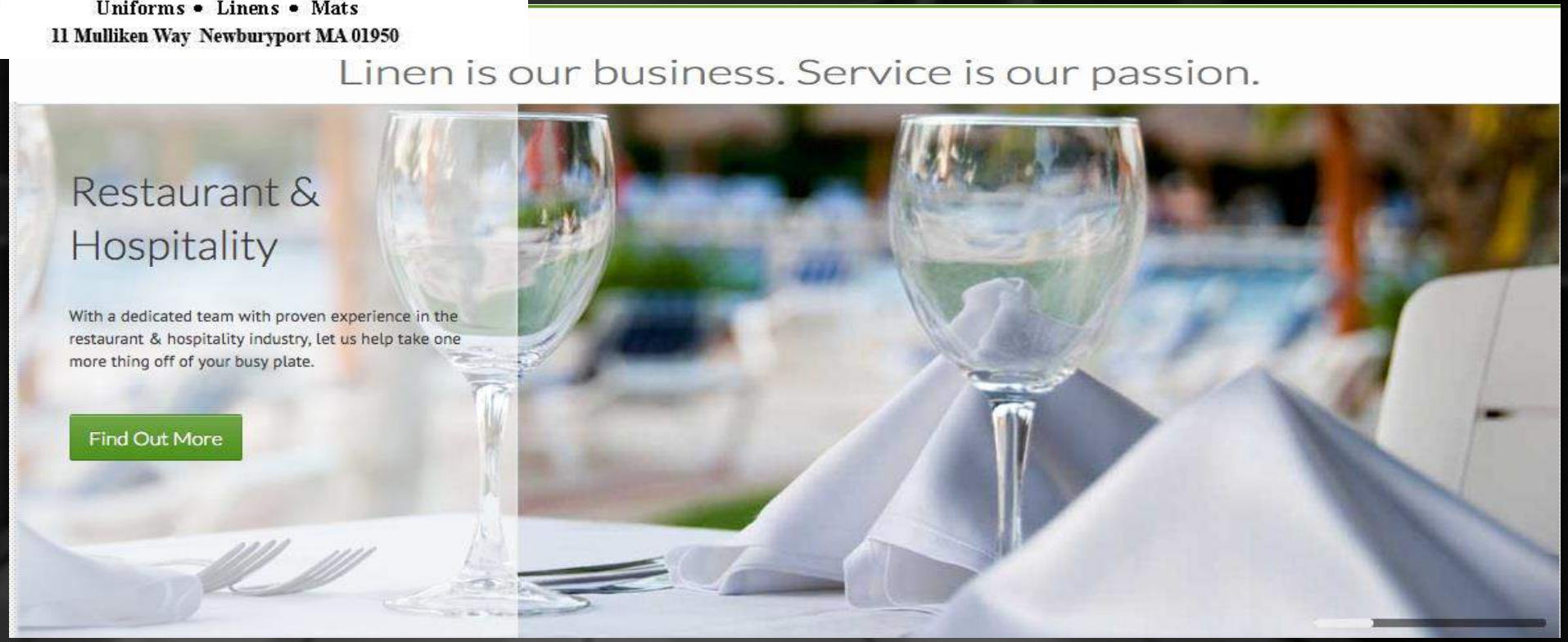
430,555,582

That's

1 Million 179 Thousand

a day.

Founded: 1933
1 location
35 employees



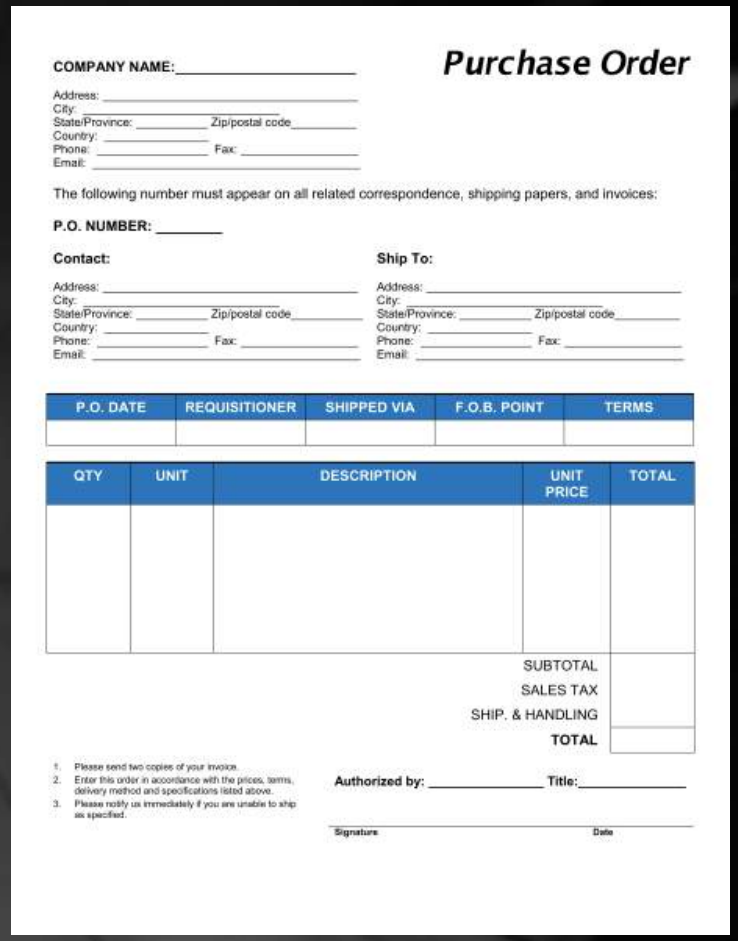
Victim

Founded: 1933
1 location
35 employees

Attacker

Founded: 1938
5 location
285 employees

- In the network for two years
- Access data 157 times



COMPANY NAME:_____

Purchase Order

Address: _____
City: _____
State/Province: _____ Zip/postal code_____
Country: _____
Phone: _____ Fax: _____
Email: _____

The following number must appear on all related correspondence, shipping papers, and invoices:

P.O. NUMBER: _____

Contact:

Address: _____
City: _____
State/Province: _____ Zip/postal code_____
Country: _____
Phone: _____ Fax: _____
Email: _____

Ship To:

Address: _____
City: _____
State/Province: _____ Zip/postal code_____
Country: _____
Phone: _____ Fax: _____
Email: _____

P.O. DATE	REQUISITIONER	SHIPPED VIA	F.O.B. POINT	TERMS

QTY	UNIT	DESCRIPTION	UNIT PRICE	TOTAL
			SUBTOTAL	
			SALES TAX	
			SHIP. & HANDLING	
			TOTAL	

1. Please send two copies of your invoice.
2. Enter this order in accordance with the prices, terms, delivery method and specifications listed above.
3. Please notify us immediately if you are unable to ship as specified.

Authorized by: _____ **Title:**_____

Signature Date

New Hampshire Company Pleads Guilty to Hacking Into a Competitor's Computer System for Commercial Advantage

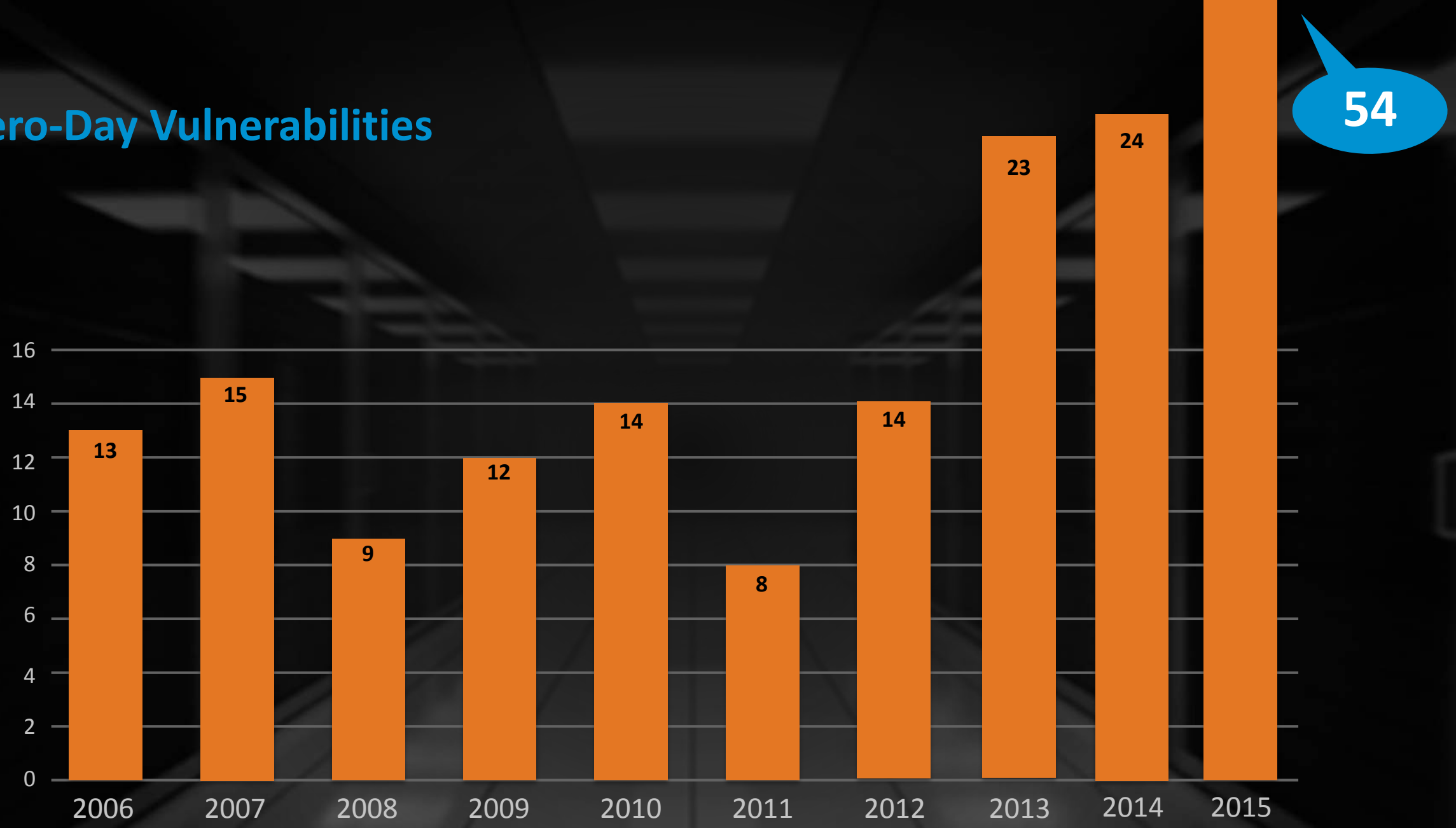
U.S. Attorney's Office — **District of New Hampshire**

December 03, 2015 — (603) 225-1552

CONCORD, NH—Acting United States Attorney Donald Feith, and FBI Special Agent in Charge, Harold H. Shaw, announced today that General Linen Services, LLC of Somersworth, New Hampshire, formerly known as General Linen Service Co., Inc. (General Linen Somersworth) pled guilty to computer hacking in violation of Title 18, United States Code, Sections 1030(a)(2)(C) & (c)(2)(B)(i). Earlier this month, charges were filed alleging that between September 2009 and April 8, 2010 the company "intentionally accesses a computer without authorization, and thereby obtained information from a protected computer," a computer used in interstate commerce, "and the offense was committed for purposes of commercial advantage and private financial gain ... ."

Zero-Days

Zero-Day Vulnerabilities



Hackers Unleash Trove of Data from Hacking Team

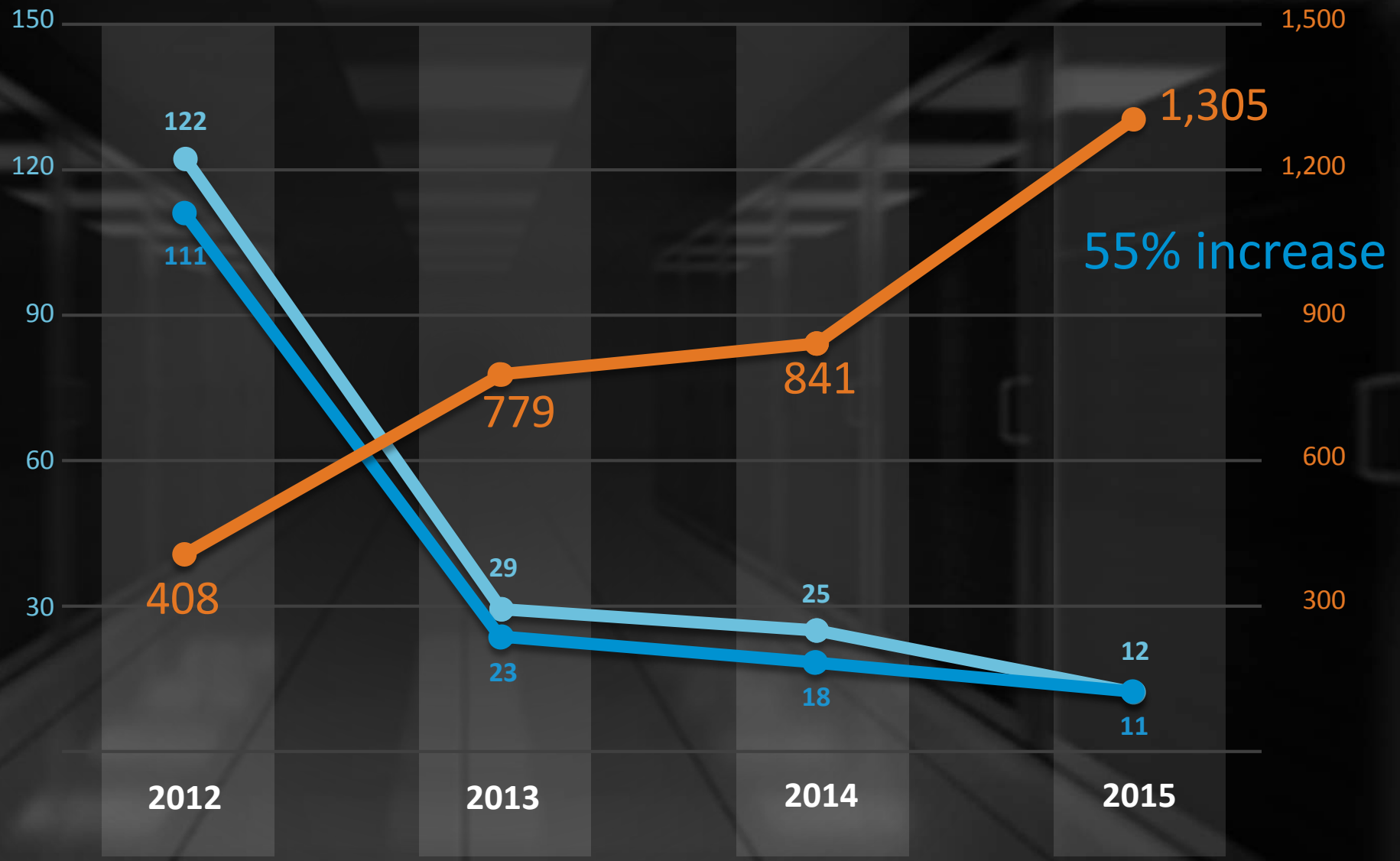
- HackingTeam (HT) had zero days in Adobe Flash, Internet Explorer and Microsoft Windows

CVE	Affected Product	First Notice	Patch Date
CVE-2015-5119	Adobe Flash	July 7	July 8
CVE-2015-5122	Adobe Flash	July 10	July 14
CVE-2015-5123	Adobe Flash	July 10	July 14
CVE-2015-2425	Internet Explorer	July 14	July 14
CVE-2015-2426	Microsoft Windows	July 20	July 20
CVE-2015-2387	Microsoft Windows	July 8	July 14

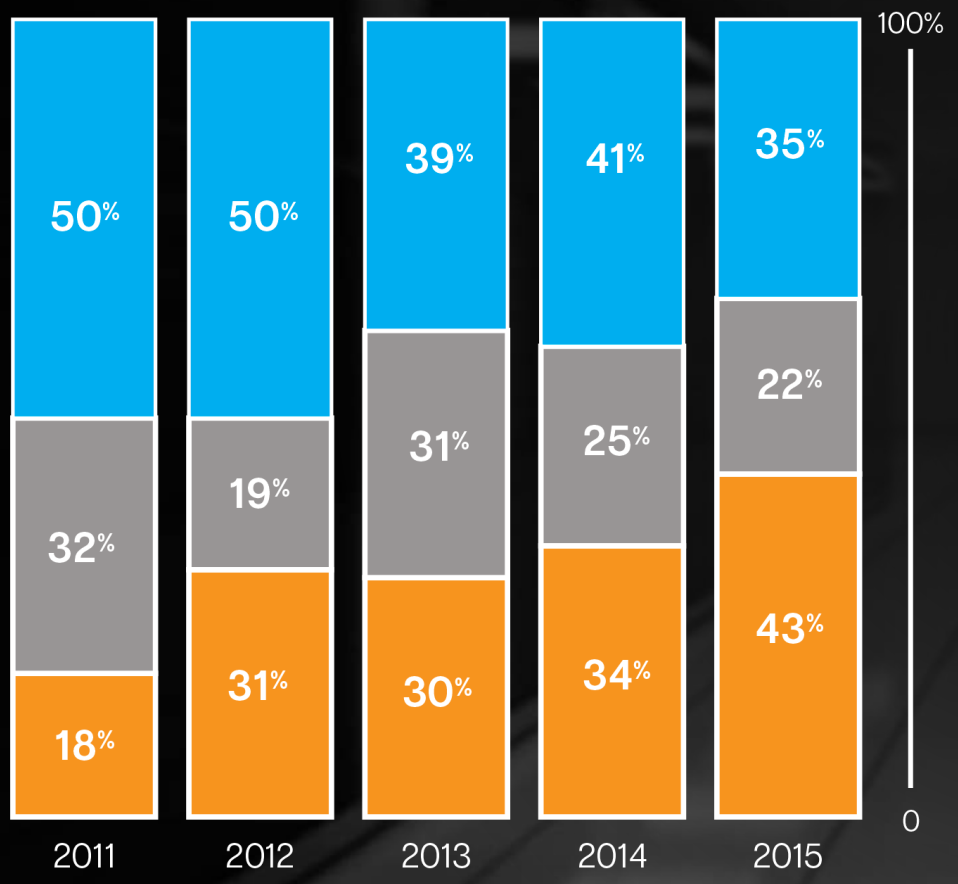
Targeted Attacks

Targeted Attack Campaigns

- Average Number of Email Attacks Per Campaign
- Recipients per Campaign
- Campaigns



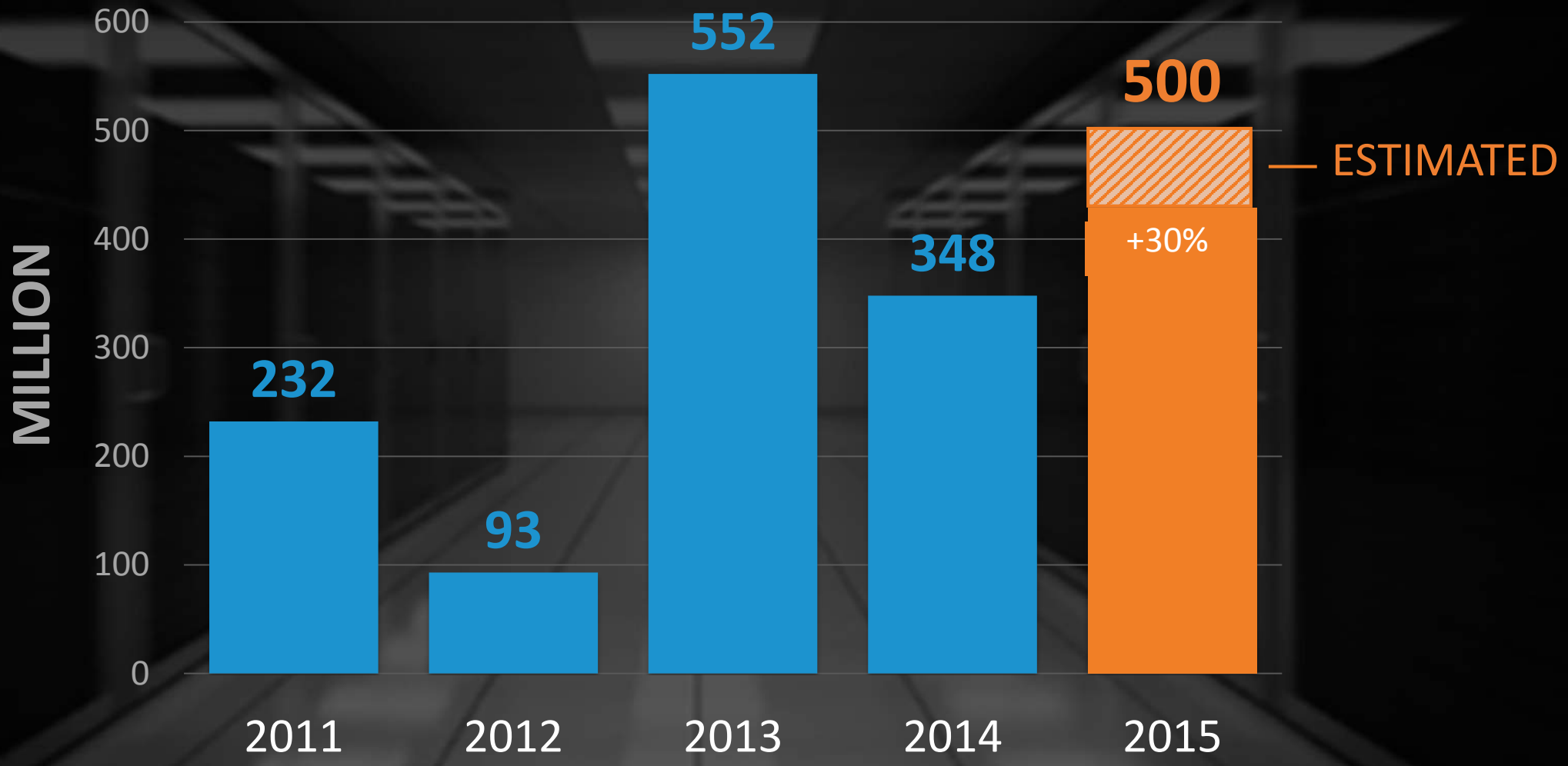
Spear-Phishing Attacks by Size of Targeted Organization



Org Size	2015 Risk Ratio	2015 Risk Ratio as Percentage	Attacks per Org
Large Enterprises **2,500+** Employees	1 in 2.7	38%	3.6
Medium Business **251–2,500** Employees	1 in 6.8	15%	2.2
Small Business (SMB) **1–250** Employees	1 in 40.5	3%	2.1

Breaches

Total Identities Exposed



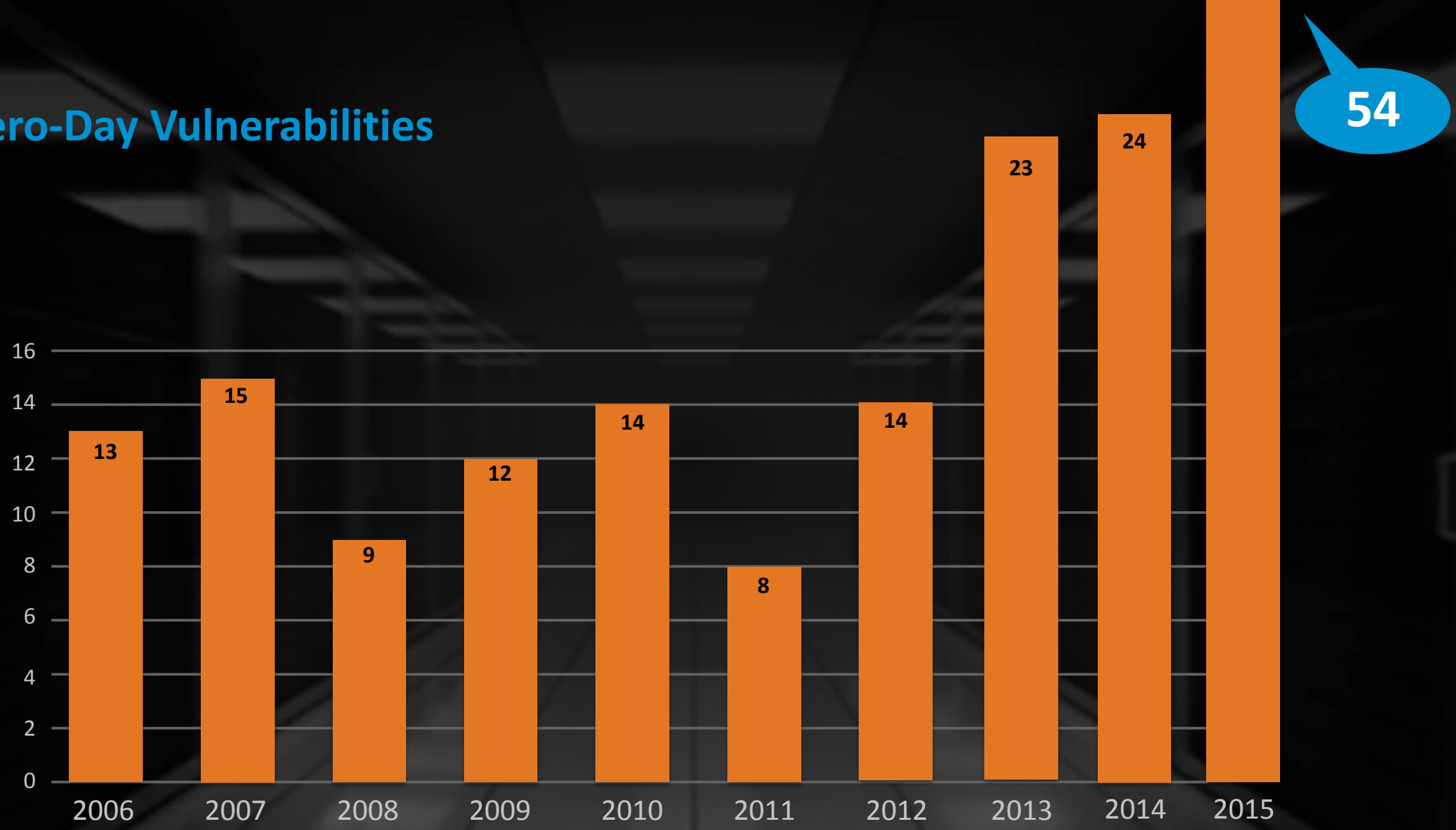
Mega Breaches 2015

Breaches With More Than 10 Million Identities Exposed

2013	2014	2015
8	4	9
–	-50%	+125%

Vulnerabilities

Zero-Day Vulnerabilities



Top 5 most Frequently Exploited Zero-Day Vulnerabilities

Rank	Name	2015 Percentage
1	Adobe Flash Player CVE-2015-0313	81%
2	Adobe Flash Player CVE-2015-5119	14%
3	Adobe Flash Player CVE-2015-5122	5%
4	Heap-Based Buffer Overflow aka 'Ghost' CVE-2015-0235	<1%
5	Adobe Flash Player CVE-2015-3113	<1%

Adobe Releases Out-of-Band Patch For Flash Vulnerability

- On June 23, Adobe released an out-of-band patch for a critical zero day vulnerability, designated CVE-2015-3113
- Within a week, five of the most well known exploit kits had integrated this vulnerability into their platforms

Exploit Kit	First Seen
Magnitude	June 27, 2015
Angler	June 29, 2015
Nuclear	July 1, 2015
RIG	July 1, 2015
Neutrino	July 1, 2015

Scanned Websites with Vulnerabilities ...

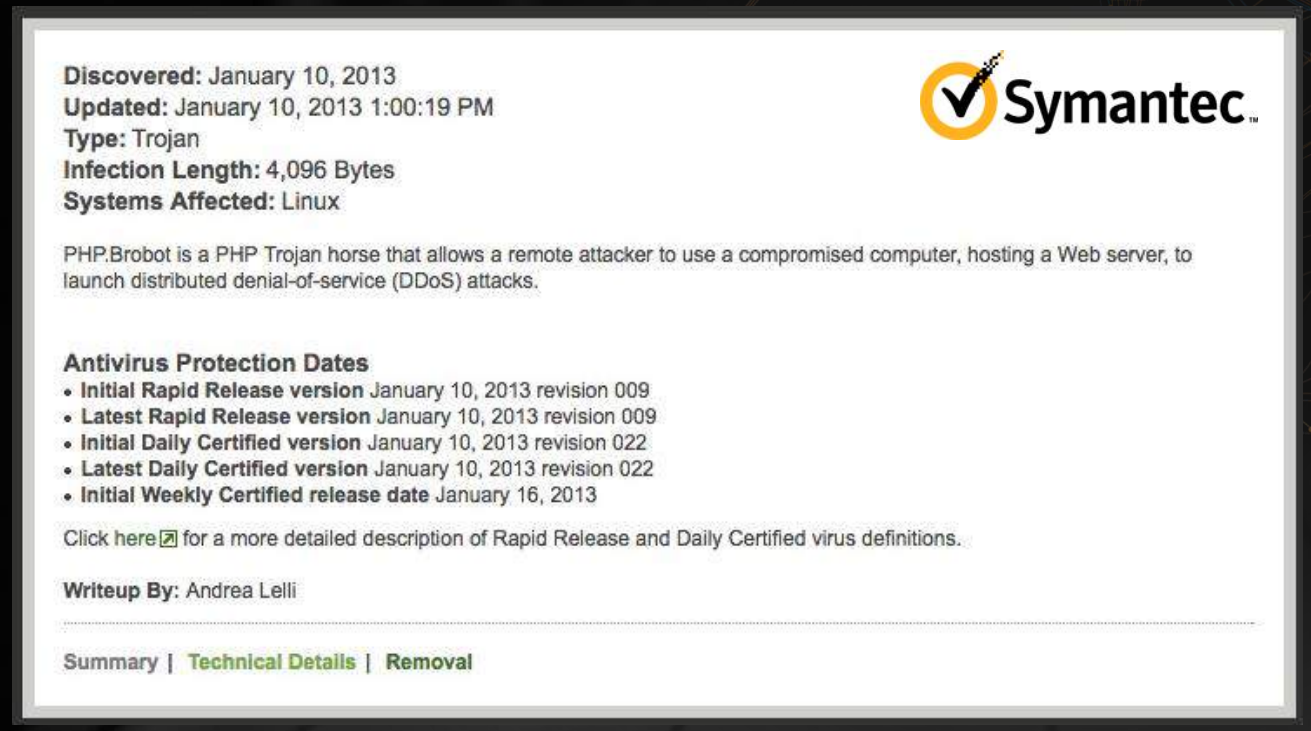
2013	2014	2015	
77%	**76%**	**78%**	
–	-1% pts	+2% pts	

... Percentage of Which Were Critical

2013	2014	2015	
16%	**20%**	**15%**	
–	+4% pts	-5% pts	

The Alleged Attackers Used DDoS Attacks

"The accused men are alleged to have built the botnet by scanning the internet for servers running older versions of a "popular website content management software" that had not been updated to patch known vulnerabilities. These vulnerabilities allow them to install the Brobot malware on affected servers."



Discovered: January 10, 2013
Updated: January 10, 2013 1:00:19 PM
Type: Trojan
Infection Length: 4,096 Bytes
Systems Affected: Linux

PHP.Brobot is a PHP Trojan horse that allows a remote attacker to use a compromised computer, hosting a Web server, to launch distributed denial-of-service (DDoS) attacks.

Antivirus Protection Dates

- **Initial Rapid Release version** January 10, 2013 revision 009
- **Latest Rapid Release version** January 10, 2013 revision 009
- **Initial Daily Certified version** January 10, 2013 revision 022
- **Latest Daily Certified version** January 10, 2013 revision 022
- **Initial Weekly Certified release date** January 16, 2013

Click here for a more detailed description of Rapid Release and Daily Certified virus definitions.

Writeup By: Andrea Lelli

Summary | Technical Details | Removal

Ransomware

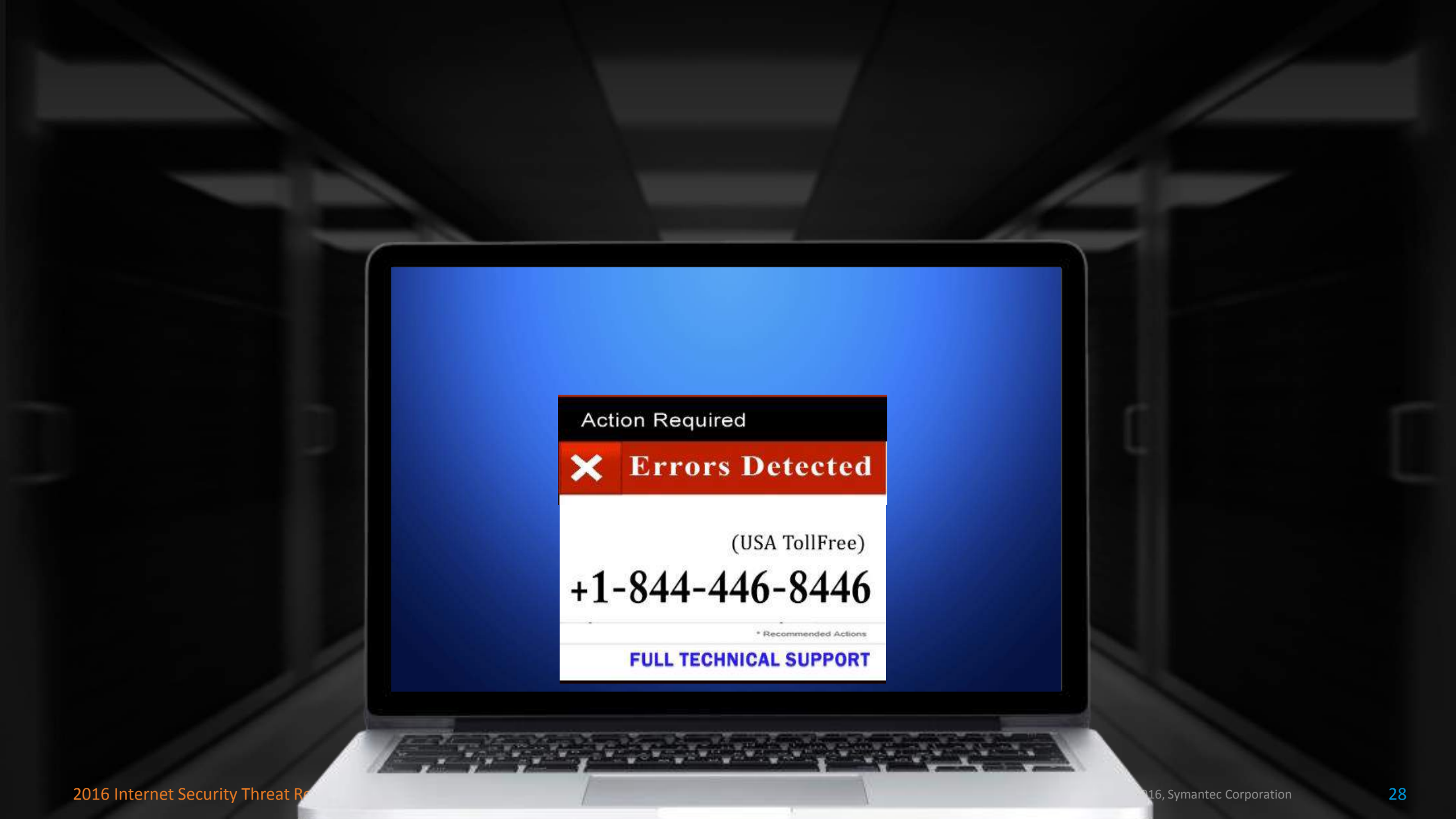
Ransomware Families

- Android
- Linux
- OSX

35% Increase in Crypto-Ransomware Attacks

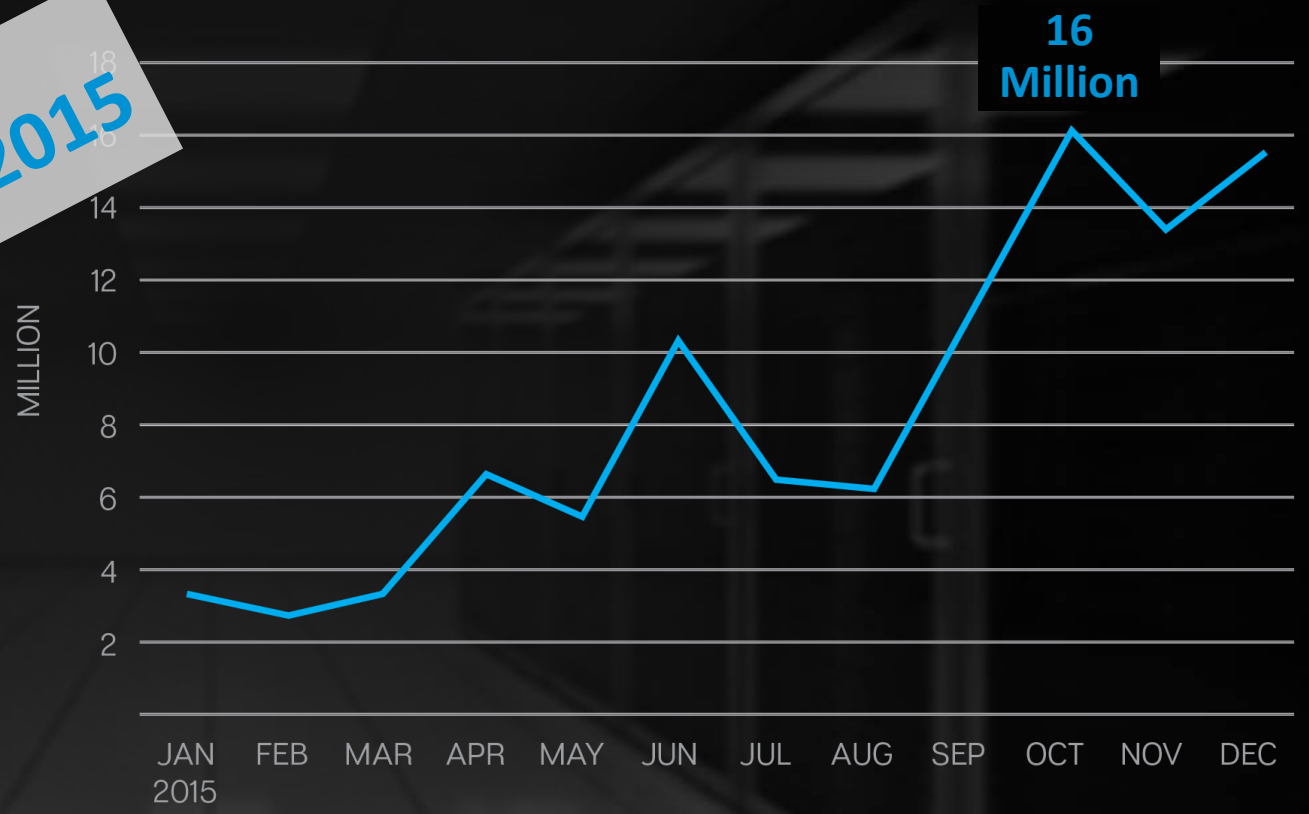
Crypto-Ransomware Total	
2014	2015
269K	362K
–	+35%
Average Per Day	Average Per Day
737	992

Consumer Scams


Action Required
Errors Detected
(USA TollFree)
+1-844-446-8446
* Recommended Actions
FULL TECHNICAL SUPPORT

Blocked Tech Support Scams

100 MILLION BLOCKED in 2015



Professionalization of Cyber Crime

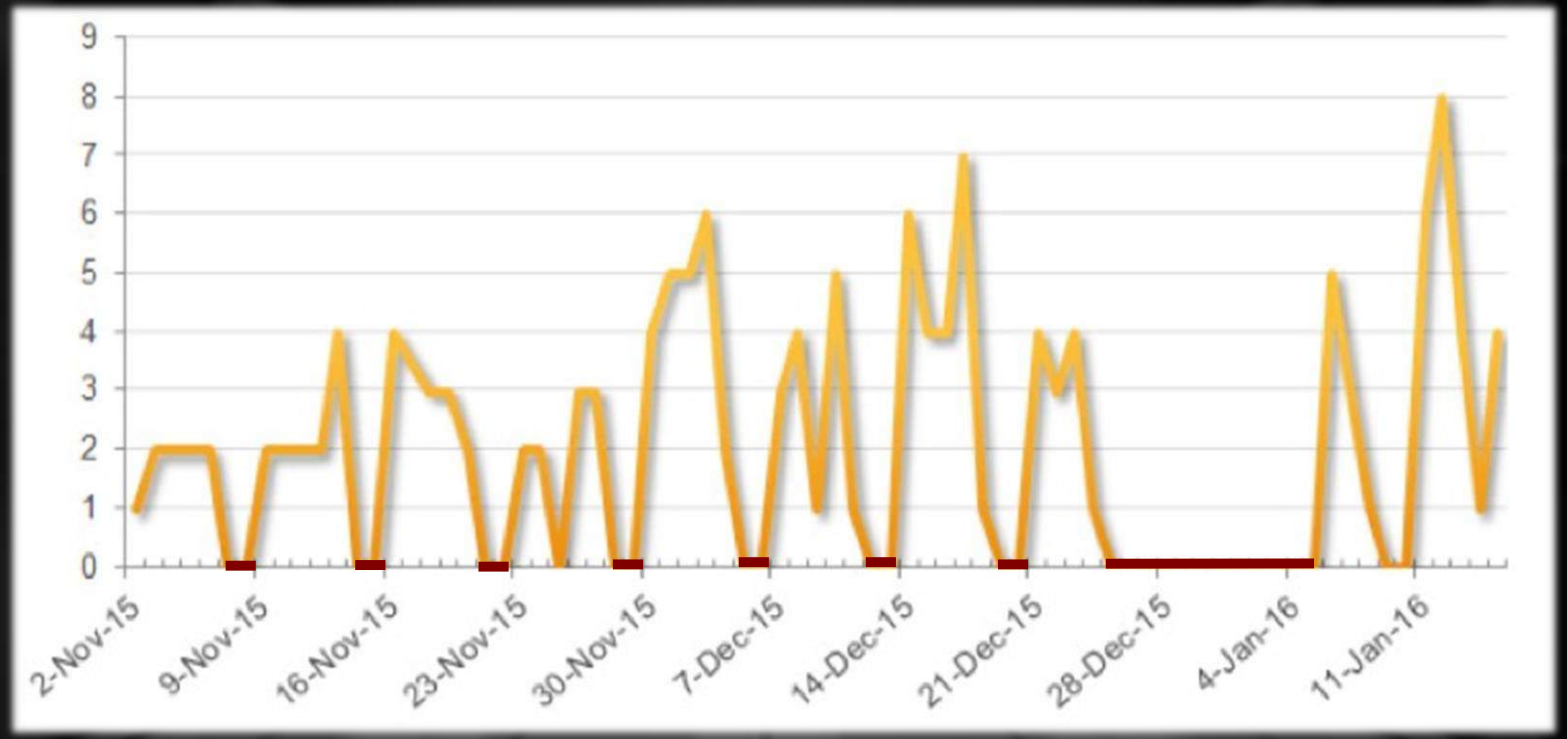
TeslaCrypt Ransomware – Technical Support Available

Hacktool.MultiPurpose

```
General options
---------------
 --install: install server on local host and load it
 --host <host>: hostname or IP (local host if not set)
 --password <password>: server password connection (mandatory)
 --forceload: load server on local host without test

Server options
--------------
 --cmd: server command:
    dump: dump stuffz
      --sam: fetch LM/NTLM hashes
      --machines: fetch machines hashes
      --history: fetch history for LM/NTLM hashes
      --sh: fetch logon sessions hashes
      --sp: fetch security packages cleartext passwords
      --accounts: <account list>: with --sam, specify accounts to dump
(comma separated)
      --lsa: fetch LSA secrets
```

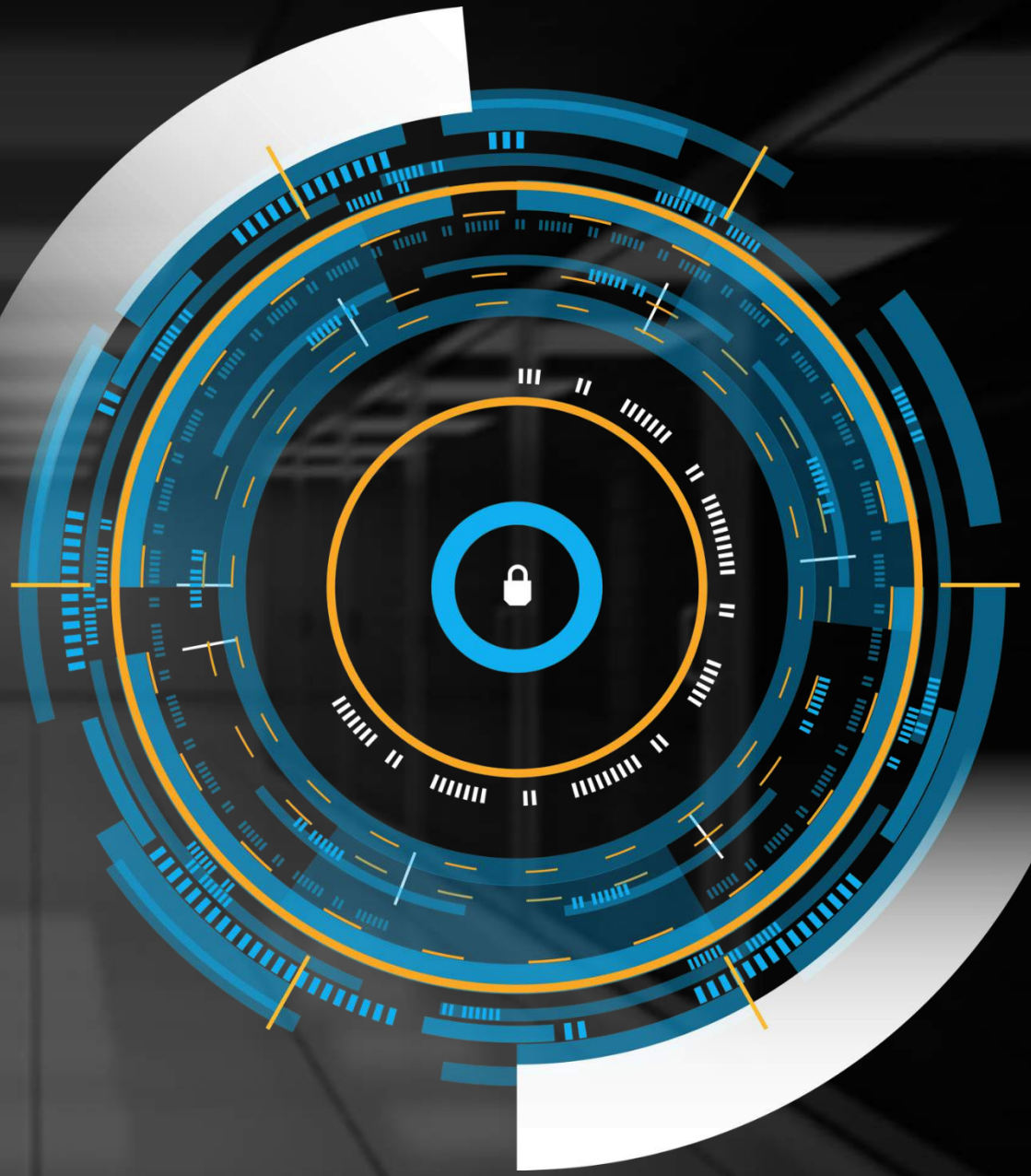
Dridex Gang - Number of Known Spam Runs Per Day



Symantec

ISTR

Internet Security Threat Report



Best Practices & Solutions

ISTR 21: Best Practices

Don't get caught flat-footed	• Use advanced threat and adversary intelligence solutions to help you track indicators of compromise and more quickly identify and respond to attacks
Employ a strong security posture	• Implement multi-layered endpoint security, network security, encryption, strong authentication and reputation-based technologies. • Partner with a managed security service provider to extend your IT and security teams for 24x7 SOC services.
Prepare for the worst	• Incident management ensures your security framework is optimized, measureable and repeatable, and that lessons learned improve your security posture. • Consider adding an Incident Response retainer with a third-party expert to help manage crises.
Provide ongoing education & training	• Establish a program to develop cybersecurity skills for technical and non-technical teams as well as guidelines and procedures for protecting sensitive data on personal and corporate devices. • Regularly assess internal response and investigation teams—and run practice drills—to ensure you address skills gaps to effectively combat cyber threats.

What You're Faced With Today

It's hard to achieve a higher level of security

I'M NOT READY FOR TOMORROW'S THREATS

- Advanced attacks are lost in a mass of less important alerts
- Average attack goes undetected for 170 days
- Just 31% of breaches are found by the victim organization – the rest are found by a third party, law enforcement, etc.

MY DATA IS MOBILE AND MOVING TO THE CLOUD

- With 65% of workloads in the cloud (Amazon Web Services, Salesforce, Box, Office 365), more of your data is at risk
- Data is increasingly accessed from outside your firewall

I NEED TO REASSURE MY ONLINE CUSTOMERS

- My customers don't know if they can trust my website
- I don't have visibility into attacks on my brand

I NEVER HAVE ENOUGH TIME OR RESOURCES

- Organizations don't know how they are doing or where to focus – 96% of alerts never reviewed
- It's hard to hire the right security talent

How Can We Help?

Achieve a higher level of security from endpoint to the cloud

STAY AHEAD OF TOMORROW'S THREATS

THREAT PROTECTION

Block, detect and quickly respond to the most advanced threats.

PROTECT YOUR CRITICAL DATA WHEREVER IT LIVES

INFORMATION PROTECTION

Keep your customer's information protected while keeping their employees productive.

TAKE ONLINE TRUST TO A WHOLE NEW LEVEL

WEBSITE SECURITY

Deploy comprehensive website security for your customer's ecommerce properties.

RELY ON EXPERTS TO WATCH OVER YOUR SECURITY

CYBER SECURITY SERVICES

Stay ahead of emerging threats by extending your team with the help of our team, around the clock, around the world.

Help stay ahead of tomorrow's threats

Our Threat Protection solutions provide complete security from endpoints to the cloud

Advanced Threat Protection

Uncover, prioritize, and remediate advanced threats

- Protect against advanced attacks across endpoints, networks, and email, all from a single console

Endpoint Protection

Protect and manage your endpoints and devices

- Unrivaled protection, blazing performance, and smarter management
- Proactively block known and unknown threats

Data Center Security

Secure your physical, virtual, private cloud and public cloud workloads

- Protect your servers, protect your data repositories, and ensure compliance

Email Security.cloud

Protect against email-based attacks

- Always-on, inbound and outbound email security, with protection against targeted attacks, spear phishing, advanced malware, spam and bulk mail- on premise or in cloud

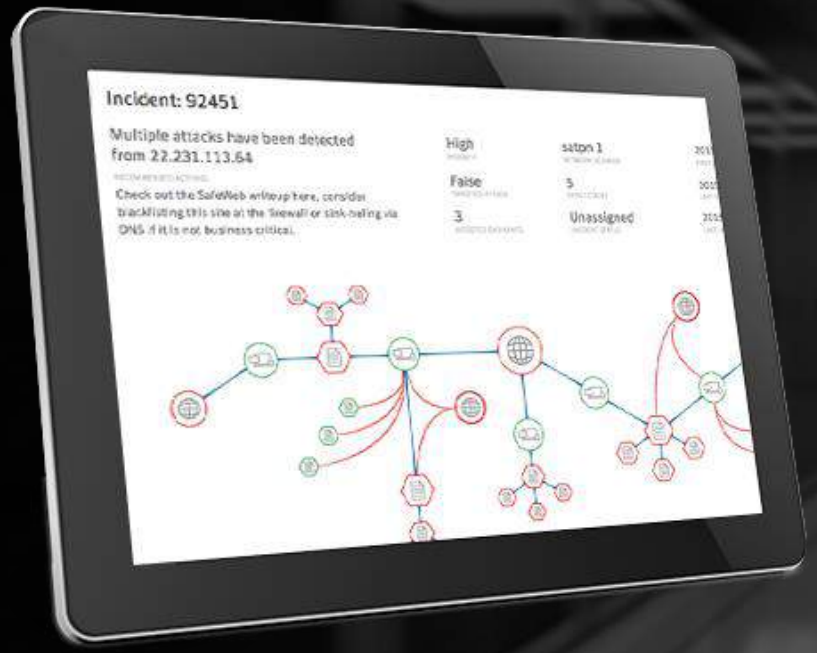
Web Security

Stop web-based threats

- Leverage our cloud-based or on-premise web security solutions to stop today's most complex, web-based attacks

Symantec Advanced Threat Protection

Uncover, Prioritize, and Remediate today's most advanced threats



Uncover advanced threats across endpoints, networks and email gateways, all from a single console

- Combines global telemetry with local customer context to uncover attacks that would otherwise evade detection
- Search for any attack artifact across your infrastructure, with the single click of a button

Prioritize what matters most

- Aggregates intelligence across control points to identify and prioritize systems that remain compromised and require immediate attention
- Powered by new Cynic cloud-based sandboxing service that finds and prioritizes the most stealthy and persistent threats

Remediate fast

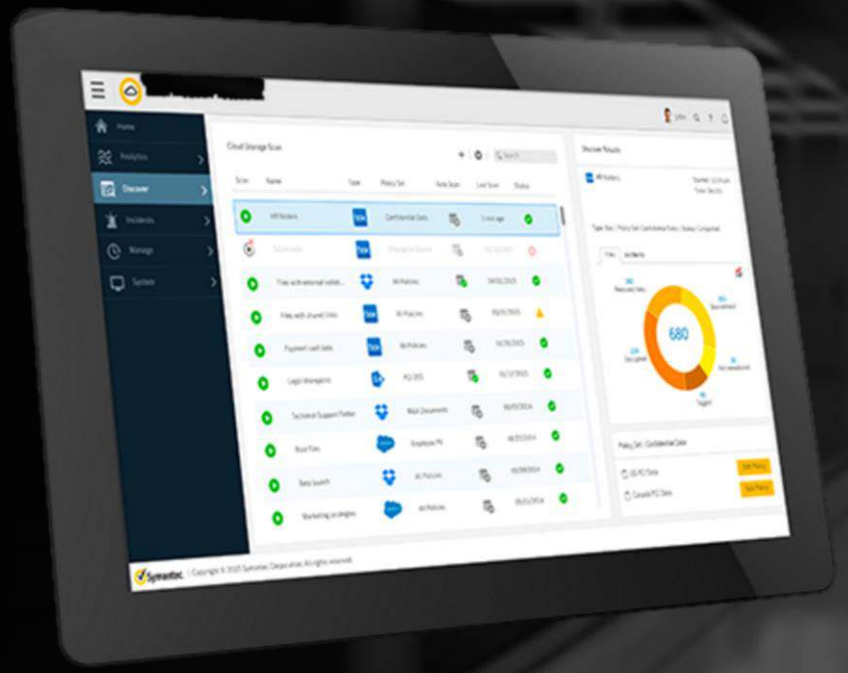
- Provides all data a customer needs to know about an attack, in one place
- Click once to remediate across endpoint, networks and email

Leverage existing Symantec Investments

- Leverages Symantec Endpoint Security and Email Security .cloud investments, requires no new endpoint agents
- Monitor Symantec ATP with Symantec Managed Security Services

Protect your customer's data wherever it lives

Our Information Protection portfolio keeps data protected while keeping employees productive



Data Loss Prevention

Track and secure confidential data

- Discover, monitor, and protect your customer's confidential information wherever it's stored and however it's used—on mobile devices, within a data center, or in the cloud

Encryption

Encrypt data in case it falls into the wrong hands

- Full-disk and removable media encryption for endpoints, email encryption secures sensitive communications, and file share encryption protects files on shared network drives and in the cloud

Identity Access Manager

Give access only to users who need it

- Single Sign-on (SSO) with strong authentication, access control, and user management, so you can help your customer's control who accesses internal and 3rd-party cloud-based applications

Validation and ID Protection (VIP)

Strong authentication made easy

- Two-factor and risk-based tokenless authentication prevents unauthorized access to your sensitive networks and applications

Take online confidence to a whole new level

Protect your online business - always

Secure your websites

- Protect your brand and prevent financial losses resulting from exploitation of vulnerabilities and DDoS attacks

Maintain business and operational continuity – 24/7

- Eliminate downtime due to expired or non-compliant SSL/TLS certificates

Ensure safe application/code publications

- Minimize risks of malware propagation from stolen or misused code signing keys.

Increase customer confidence with the Norton Shopping Guarantee

- Increase online sales and customer engagement

Let our experts help you watch over your customer's security

You can rely on our 1,000+ Cyber Warriors, around the clock, around the world

Threat Intelligence Services

Arm your team with actionable insights

- Receive proactive notifications of evolving attack vectors and techniques
- DeepSight Intelligence keeps your teams informed of vulnerabilities and threats to your organization

Managed Security Services

Extend your customer's team with our experts

- 24/7 monitoring of your entire security infrastructure
- Monitors every major security product on the market

Incident Response

Respond with speed and precision

- Readiness Services help you and your customer's assess, test, and refine their response program
- Incident Response Services provides remote and on-site investigation to help you contain attacks, understand their full scope, and ensure that all components have been eradicated

Cyber Skills Development

Prepare your customer's for what's next

- Strengthen employee cyber-readiness through security education and simulation exercises
- Identify key risks employees are facing and build a comprehensive program to assess and improve security awareness

Leader in Gartner Magic Quadrant for Managed Security Services*

ISTR

Internet Security Threat Report

Thank you!

go.symantec.com/ISTR