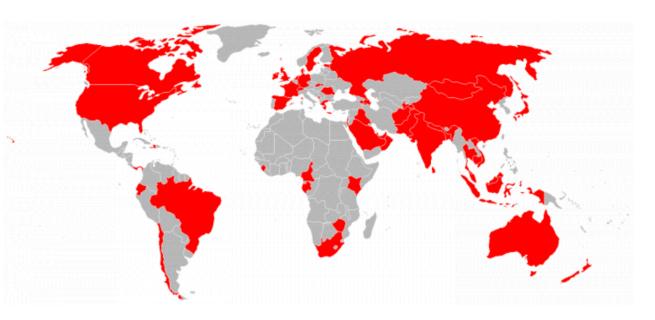


#### **2019 Verizon Data Breach Investigations Report** Suzanne Widup



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.

#### Demographics



73 CONTRIBUTING ORGANIZATIONS

41,686

SECURITY INCIDENTS

2,013

CONFIRMED DATA BREACHES

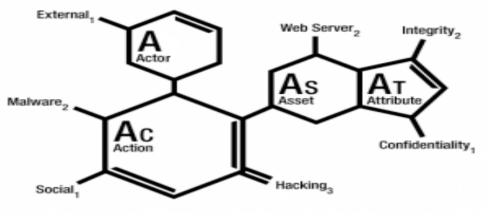
**86** COUNTRIES REPRESENTED



# **The VERIS Framework**

Vocabulary for Event **Recording and Incident** Sharing (VERIS) is an open framework designed to provide a common language for describing security incidents (or threats) in a structured and repeatable manner.

http://www.veriscommunity.net



Actor – Who did it?

Action – How'd they do it?

Asset - What was affected?

Attribute – How was it affected??



### **VERIS in Action**

#### MALWARE

Malware is any **mal**icious soft**ware**, script, or code run on a device that alters its state or function without the owner's informed consent. Examples include viruses, worms, spyware, keyloggers, backdoors, etc.

#### VARIETY

Question Text: What varieties or functions of malware were involved?

User notes: N/A

Question type: enumerated list (multi-select)

Variable name: action.malware.variety (string)

**Purpose:** In the short term, variety is necessary to adequately describe the incident and its ramifications. In the long term, it gives insight into the evolving nature of malware and how criminals use it.

**Developer notes: N/A** 

Miscellaneous: N/A

#### VECTOR

Question Text: What were the vectors or paths of infection?

<> Code	() Issues 5,000+	1) Pull requests 5	Projects 0	💷 Wiki	III Insights	🗘 Sett	inas	
	0 100000		- 10,0000		in insights	in Oct	1195	
Filters -	Q is:issue is:open		S Labels	il 🛉 Mile	estones 1			
	<b>5,859 Open →</b> 6,561 C	Closed	Author -	Labels 🗸	Projects 🗸	Milestones	s <del>v</del> As	signee
l	SkyMed Medical Eva PHIDBR2019 113470 opened 5 days ago I	cuation Membership	Service Expose	ed Data of 1	37k Members	Breach	rror	
	<b>s a Desert Valley Dei Needs Details</b> 113469 opened 5 days ago I	ntal breach ongoing?	? And did OCR o	order them t	to notify patie	nts? <mark>Brea</mark>	ch	
	Charles River Labora 13468 opened 5 days ago	tories discloses a bro	each, but detail	s are lackin	ig <mark>Breach Hack</mark>	ing		
#	Government in email 13467 opened 5 days ago I	privacy blunder Brea by swidup	Error					

#### https://github.com/vz-risk/VCDB/issues

#### verizon /

# **DBIR Overview**



### **Incidents vs Breaches**

### What influences

#### these numbers?

- Regulatory
   requirements
- Partner visibility
- Breach trends

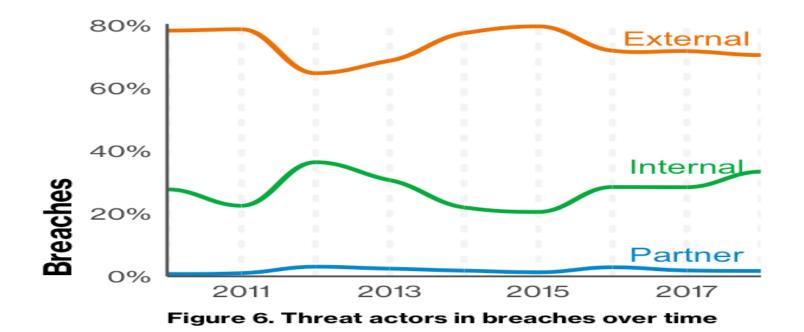
Incidents:	Total	Small	Large	Unknown	Breaches: Total	Small	Large	Unknown
Accommodation (72)	87	38	9	40	61	34	7	20
Administrative (56)	90	13	23	54	17	6	6	5
Agriculture (11)	4	2	0	2	2	2	0	0
Construction (23)	31	11	13	7	11	7	3	1
Education (61)	382	24	11	347	99	14	8	77
Entertainment (71)	6,299	6	6	6,287	10	2	3	5
Finance (52)	927	50	64	813	207	26	19	162
Healthcare (62)	466	45	40	381	304	29	25	250
Information (51)	1,094	30	37	1,027	155	20	18	117
Management (55)	4	1	3	0	2	1	1	0
Manufacturing (31-33)	352	27	220	105	87	10	22	55
Mining (21)	28	3	6	19	15	2	5	8
Other Services (81)	78	14	5	59	54	6	5	43
Professional (54)	670	54	17	599	157	34	10	113
Public (92)	23,399	30	22,930	439	330	17	83	230
Real Estate (53)	22	9	5	8	14	6	3	5
Retail (44-45)	234	58	31	145	139	46	19	74
<b>Trade</b> (42)	34	5	16	13	16	4	8	4
Transportation (48-49)	112	6	23	83	36	3	9	24
Utilities (22)	23	3	7	13	8	2	0	6
Unknown	7,350	0	3,558	3,792	289	0	109	180
Total	41,686	429	27,024	14,233	2,013	271	363	1,379

#### Table 2

Number of security incidents by victim industry and organization size



#### **Threat Actors**



**verizon**<sup>√</sup>

#### **Actor Motives**

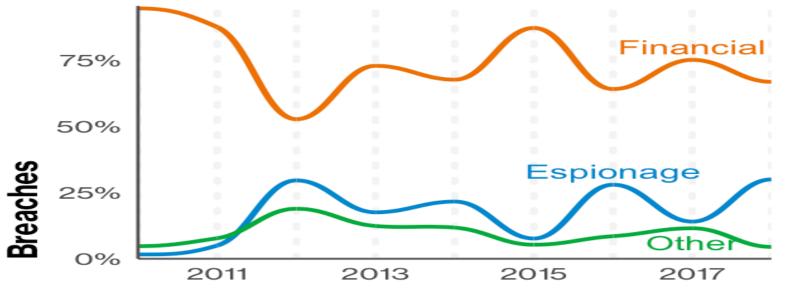


Figure 7. Threat actor motives in breaches over time



#### **Actor Varieties**

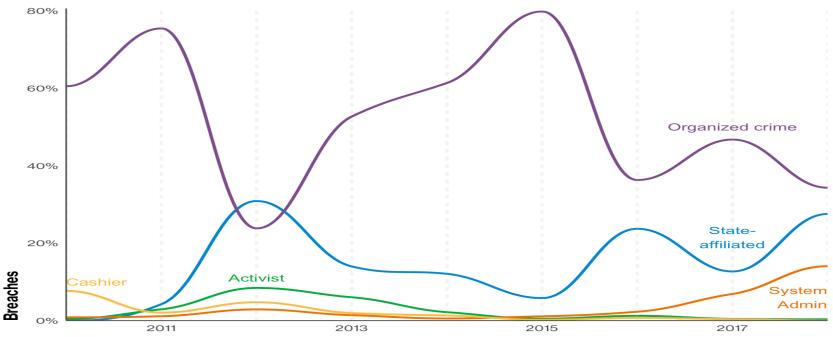
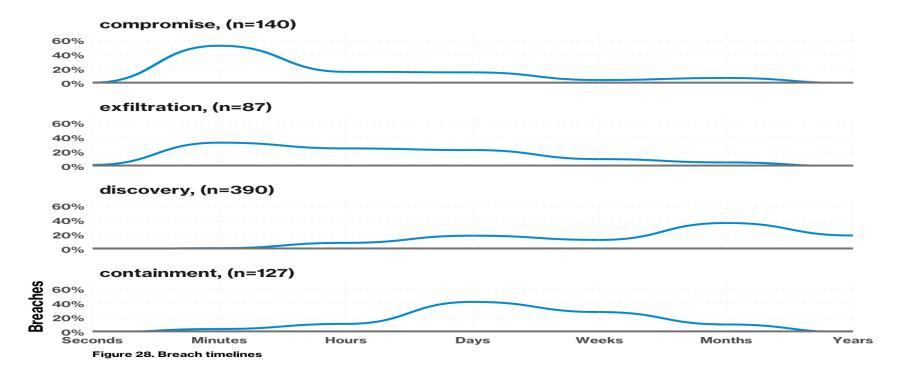


Figure 8. Select threat actors in breaches over time

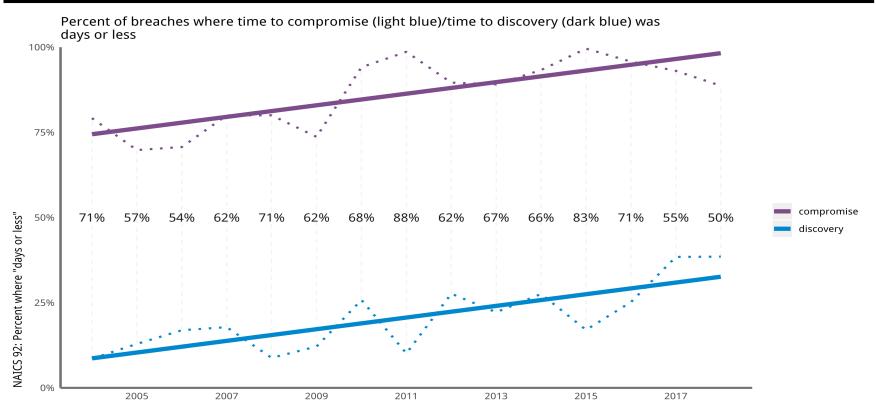


#### **Discovery Timeline**



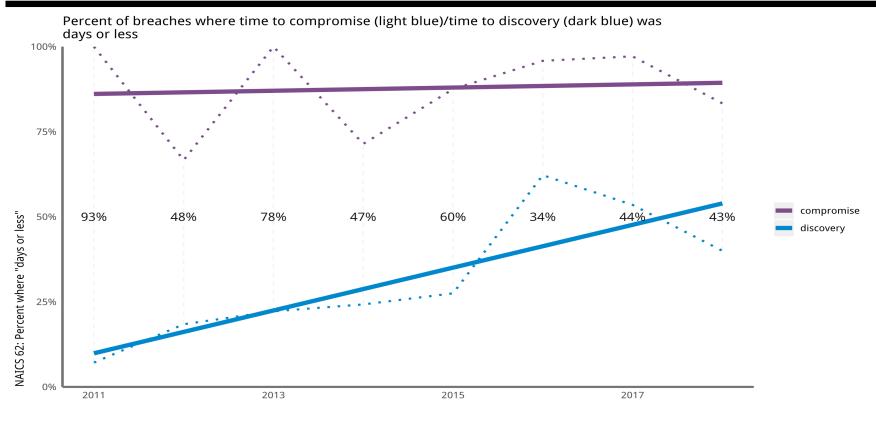


### **The Detection Deficit**





#### The Healthcare Detection Deficit (2011-2018)





# Industries



#### **The Nefarious Nine Patterns**

Privilege Misuse	
	Web Applications
Denial of Service	•
•	Miscellaneous Errors
Crimeware	
•	Privilege Misuse
Lost and Stolen Assets	
	Cyber-Espionage
Web Applications	
	Everything Else
Miscellaneous Errors	Crimeware
Everything Else	Lost and Stolen Assets
Cyber-Espionage	Point of Sale
Point of Sale	Payment Card Skimmers
•	
Payment Card Skimmers	Denial of Service
	•
0% 20% 40% 60% 80% 100% Incidents	0% 20% 40% 60% 80% 100% Breaches
Figure 35. Incidents per pattern (n=41,686)	Figure 36. Breaches per pattern (n=2,013)



### **Industry Comparison**

					Inc	iden	Its							Br	each	es			
		Accommodation (72)	Education (61)	Finance (52)	Healthcare (62)	Information (51)	Manufacturing (31-33)	Professional (54)	Public (92)	Retail (44-45)	(72)	Education (61)	Finance (52)	Healthcare (62)	Information (51)	Manufacturing (31-33)	Professional (54)	Public (92)	Retail (44-45)
	Crimeware	17	31	52	76	206	58	60	4,758	21	3	З	7	1	З	5	8	8	3
	Web Applications	14	30	76	71	75	40	79	93	92	14	24	70	65	45	36	73	33	88
	Privilege Misuse	1	19	100	110	14	36	13	13,021	16	1	9	45	85	7	14	10	40	14
	Everything Else	7	24	29	39	23	23	59	61	14	3	20	12	27	17	8	26	37	8
ern	Denial of Service		226	575	3	684	163	408	992	54							1		
Pattern	Cyber-Espionage	1	6	32	3	22	16	9	143	2	1	5	22	2	20	13	8	140	2
	Miscellaneous Errors	5	37	36	104	69	14	30	1,515	12	2	35	34	97	65	12	28	58	11
	Lost and Stolen Assets	4	9	9	62	4	5	14	2,820	7	1	3	2	28	1	2	5	16	3
	Point of Sale	40			2					10	38			2					9
	Payment Card Skimmers			21		1				10			18		1				4



#### **Healthcare Errors**

	Misdelivery					
	59					
	Publishing error					
	14					
	Disposal error					
	12					
	Loss					
	12					
	Misconfiguration					
Breaches	8					
С	0%	20%	40%	60%	80%	100%
	Error breach varieties					



#### **Healthcare Misuse Actor Varieties**

End-user					
134					
Other					
48					
Doctor or nurse					
25					
Finance					
15					
Manager					
7					
Executive					
6					
System admin 3					
Call center					
Cashier					
1					
Human resources					
1					
Unknown					
0%	20%	40%	60%	80%	100%
Actor Varieties in Misus	se				
- /					

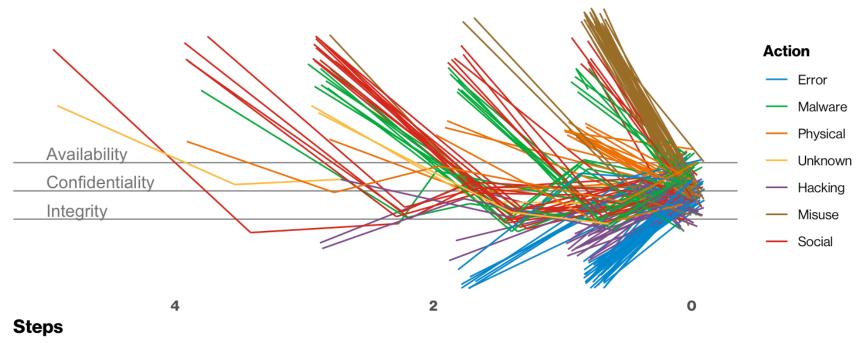


#### **Healthcare Misuse Motivations**

Financial					
136					
Fun					
109					
Convenience					
23					
Grudge					
14					
Espionage					
13					
NA					
10					
Other					
3					
Ideology					
1					
Unknown					
0% Actor Varieties in Misus	20%	40%	60%	80%	100%
Actor varieties in Misus					



#### **Healthcare**



Attack chains in Healthcare incidents

#### verizon

# I Click, Therefore I am



### **Types of Social Attacks**

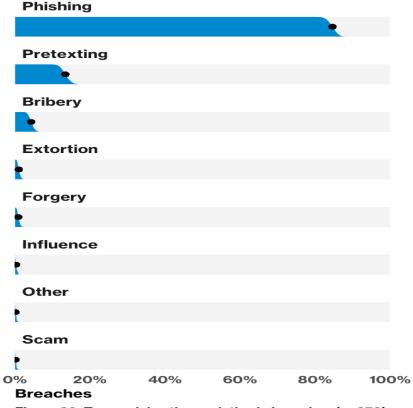




Figure 20. Top social action varieties in breaches (n=670)

#### **Progress**

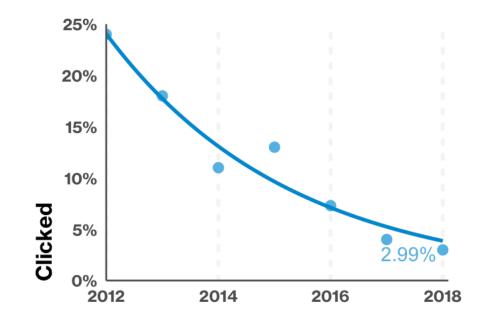
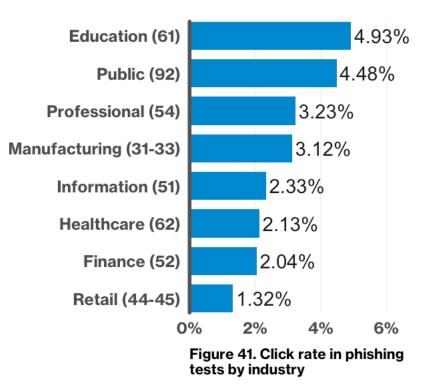


Figure 21. Click rates over time in sanctioned phishing exercises



### By Industry





### **Financially-motivated Social Engineering**

Professional (54)
•
Healthcare (62)
•
Finance (52)
Manufacturing (31-33)
Education (61)
Public (92)
Information (51)
Accommodation (72)
Retail (44-45)
0% 20% 40% 60% 80% 100%
Incidents Figure 40. FMSE incidents by industry (n=370)



# Malware



### **Choose the Form of the Destructor**

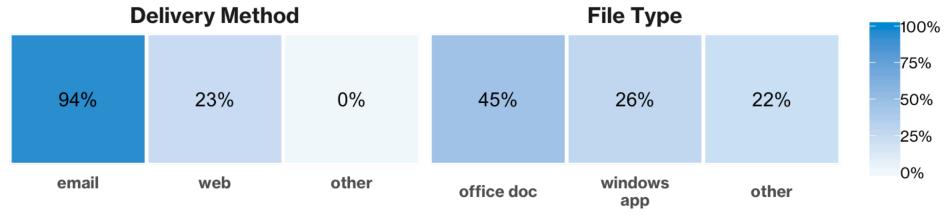


Figure 19. Malware types and delivery methods



#### **Vectors and Varieties**

Backdoor	Email attachment
•	•
C2	Direct install
	•
Spyware/Keylogger	Email unknown
•	•
Capture app data	Web drive-by
Adminware	Download by malware
Downloader	Remote injection
Capture stored data	Email link
Password dumper	Network propagation
Ram scraper	Other
Ransomware	Web download
0% 20% 40% 60% 80% 100% Breaches	0% 20% 40% 60% 80% 100% Incidents
Figure 17. Top malware action varieties in breaches (n=500)	Figure 18. Top malware action vectors in incidents (n=795)



### **Denial of Service Attacks**

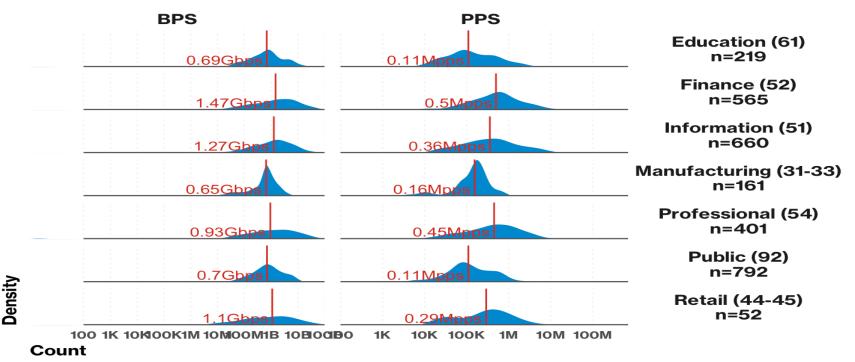


Figure 42. DDoS attack bandwidth and packet counts by industry



# **Unbroken Chains**



#### **Steps to Success**

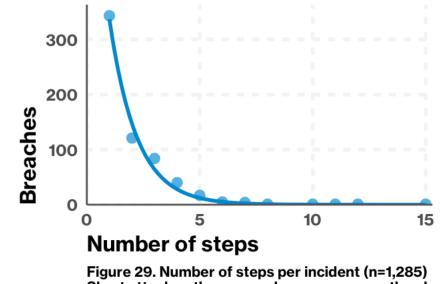
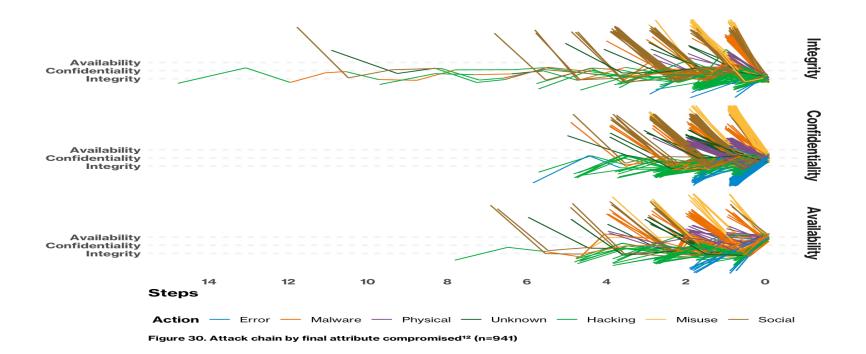


Figure 29. Number of steps per incident (n=1,285) Short attack paths are much more common than long attack paths.

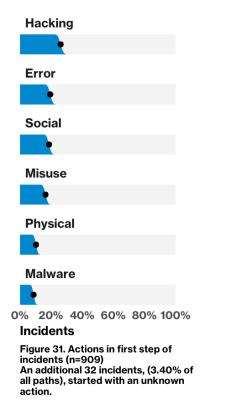


#### Paths

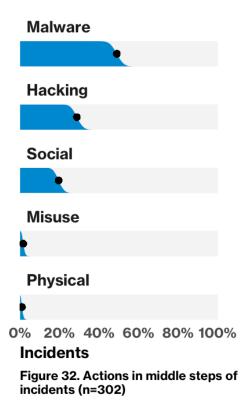


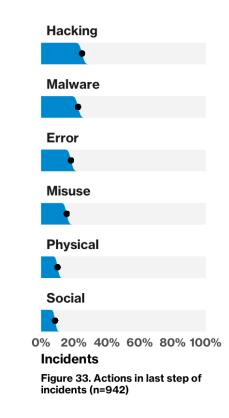


# **Beginning, Middle and End**

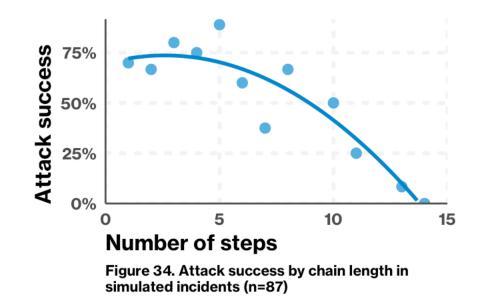








### **Simulation**





### **More Information**

Download the DBIR	http://www.verizonenterprise.com/verizon- insights-lab/dbir/
Grab the DBIR Graphics	<u>https://</u> github.com/vz-risk/dbir/tree/gh- pages/2019
Learn about VERIS	www.veriscommunity.net and
	http://github.com/vz-risk/veris
<b>Explore the VERIS</b>	http://www.vcdb.org and
Community Database	https://github.com/vz-risk/VCDB/issues
Ask a Question	DBIR@verizon.com
Follow Us	@vzdbir and hashtag #dbir



# Thank you.

# Twitter: @SuzanneWidup <u>suzanne.widup@verizon.com</u> and @VERISDB for data breach feed



Verizon confidential and proprietary. Unauthorized disclosure, reproduction or other use prohibited.