2016 NSF CyberSecurity Summit For Large Facilities and Cyberinfrastructure Training Day

DEVELOPING CYBERSECURITY PROGRAMS FOR NSF PROJECTS:

REN-ISAC CYBERTHREAT BRIEFING

Kim Milford,
Research & Education Networking Information Sharing & Analysis (REN-ISAC)

Threat Trends

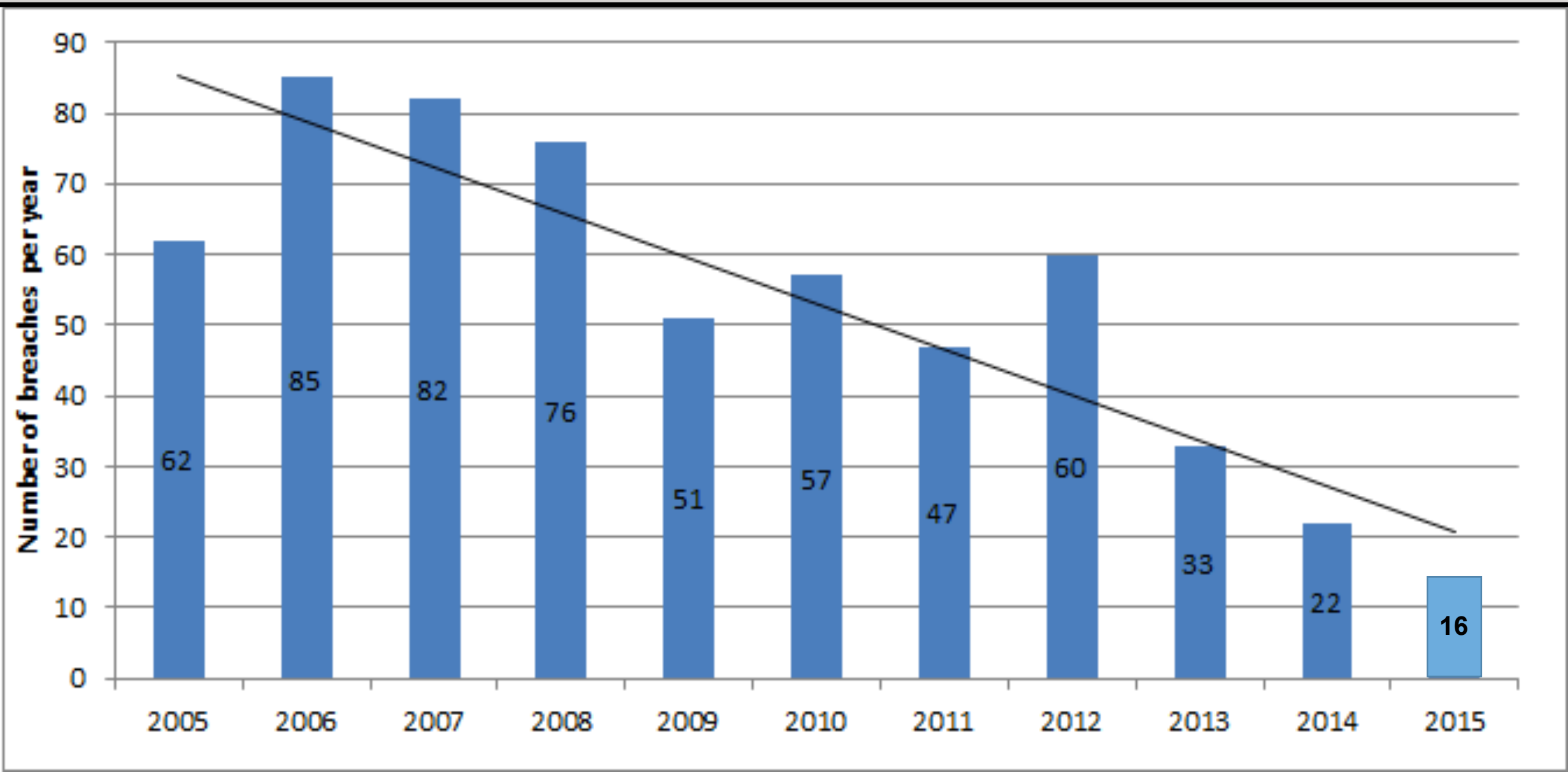
- Motive is espionage or financial 89% of the time
- 80% of the time, the threat actor is external to the organization
- Time to discover (more than 1 day over 68% of the time) is still way behind time to compromise (minutes 82% of the time)
- Mobile is not a big vector in data breaches
- Defense requires vigilance and consistency

Malicious Actors Target US Colleges and Universities

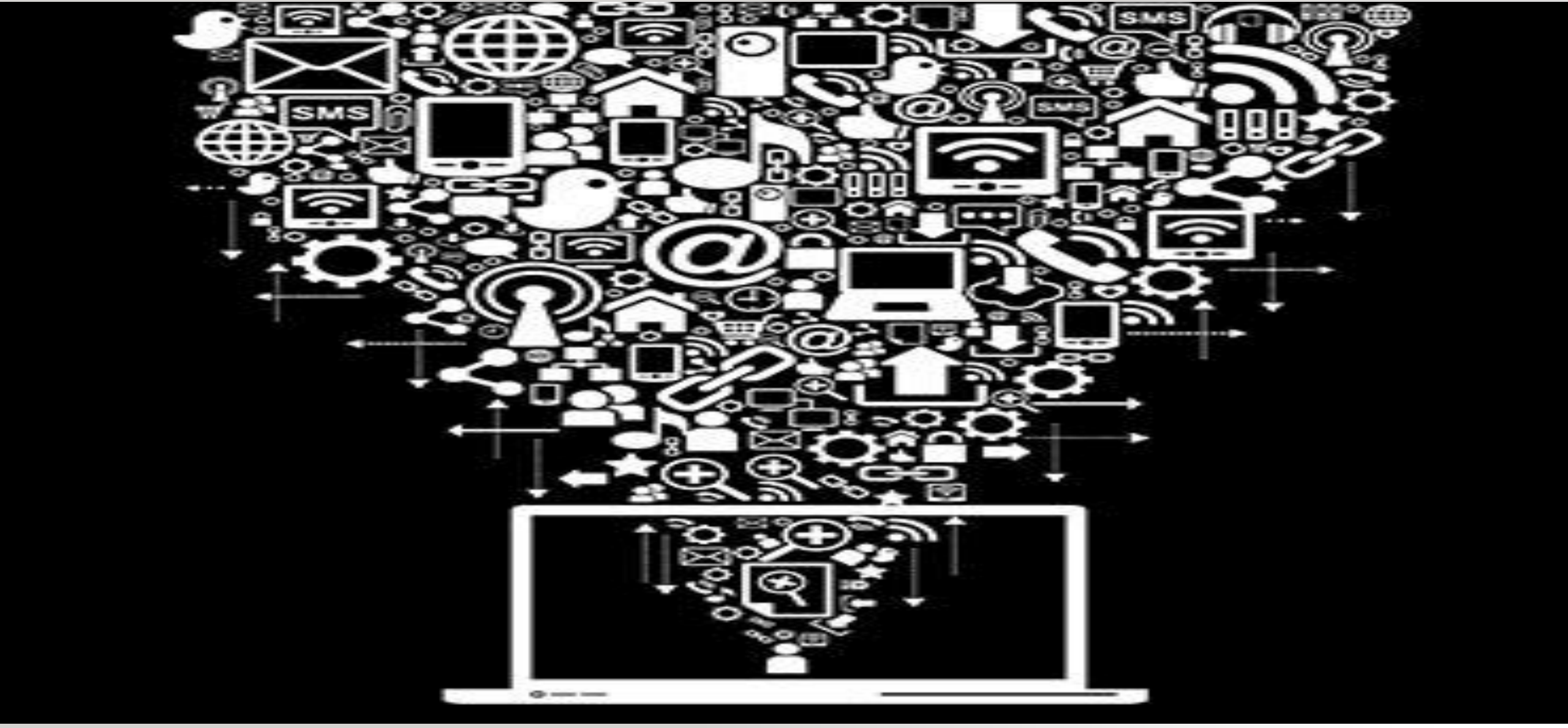
Homeland Security

INTELLIGENCE ASSESSMENT

Data Breaches in Higher Education



Sensitive Data Breaches



2016 Verizon Data Breach Report

Industry	Total	Small	Large	Unknown
Accommodation (72)	362	140	79	143
Administrative (56)	44	6	3	35
Agriculture (11)	4	1	0	3
Construction (23)	9	0	4	5
Educational (61)	254	16	29	209
Entertainment (71)	2,707	18	1	2,688
Finance (52)	1,368	29	131	1,208
Healthcare (62)	166	21	25	120
Information (51)	1,028	18	38	972
Management (55)	1	0	1	0
Manufacturing (31-33)	171	7	61	103
Mining (21)	11	1	7	3
Other Services (81)	17	5	3	9
Professional (54)	916	24	9	883
Public (92)	47,237	6	46,973	258
Real Estate (53)	11	3	4	4
Retail (44-45)	370	109	23	238
Trade (42)	15	3	7	5
Transportation (48-49)	31	1	6	24
Utilities (22)	24	0	3	21
Unknown	9,453	113	1	9,339
Total	64,199	521	47,408	16,270

Table 1.

Number of security incidents by victim industry and organization size, 2015 dataset.

2016 Verizon Data Breach Report

Industry	Total	Small	Large	Unknown
Accommodation (72)	282	136	10	136
Administrative (56)	18	6	2	10
Agriculture (11)	1	0	0	1
Construction (23)	4	0	1	3
Educational (61)	29	3	8	18
Entertainment (71)	38	18	1	19
Finance (52)	795	14	94	687
Healthcare (62)	115	18	20	77
Information (51)	194	12	12	170
Management (55)	0	0	0	0
Manufacturing (31-33)	37	5	11	21
Mining (21)	7	0	6	1
Other Services (81)	11	5	2	4
Professional (54)	53	10	4	39
Public (92)	193	4	122	67
Real Estate (53)	5	3	0	2
Retail (44-45)	182	101	14	67
Trade (42)	4	2	2	0
Transportation (48-49)	15	1	3	11
Utilities (22)	7	0	0	7
Unknown	270	109	0	161
Total	2,260	447	312	1501

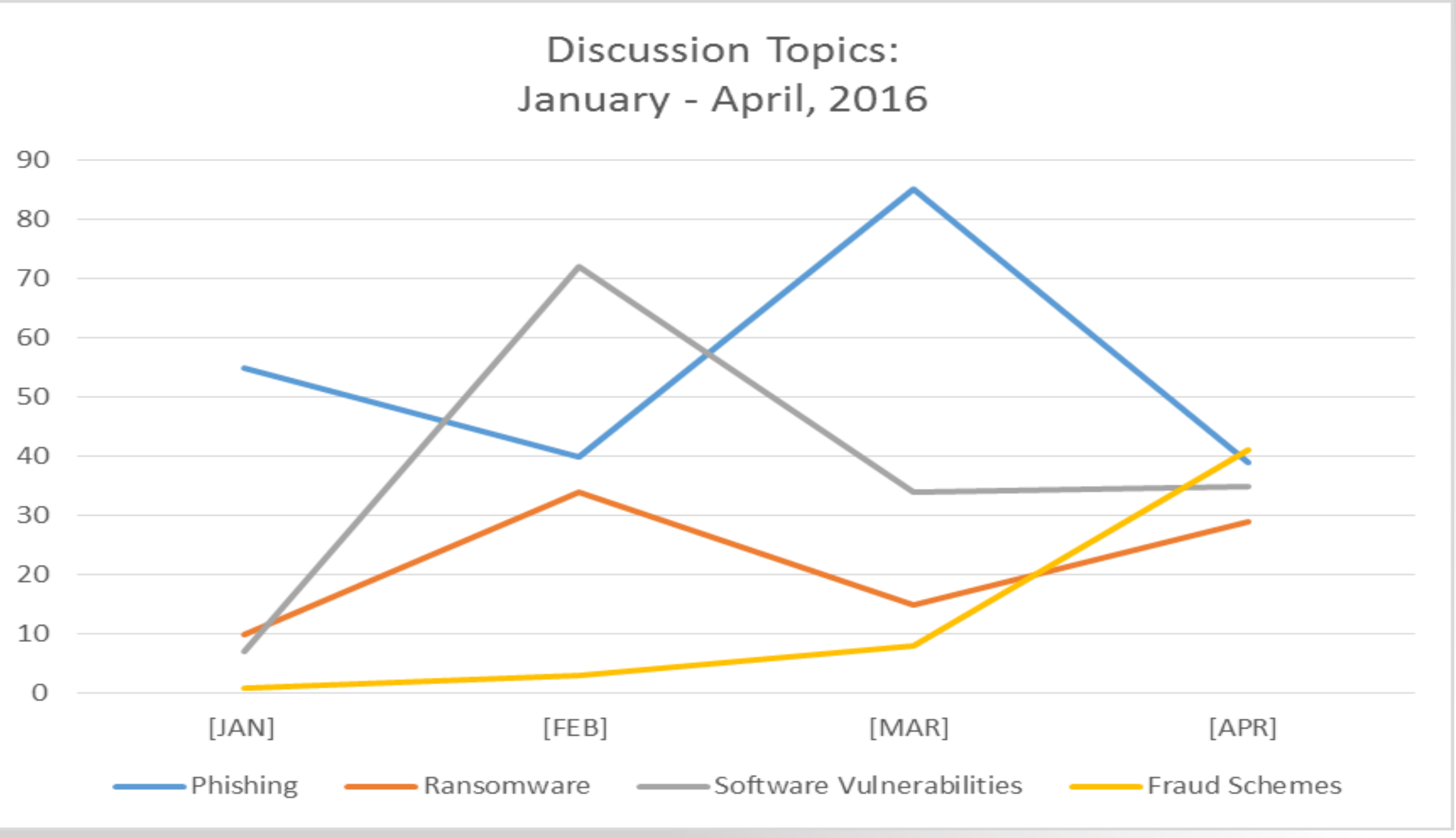
Small = organizations with fewer than 1,000 employees, Large = organizations with 1,001+ employees.

Table 2.

Number of security incidents with confirmed data loss by victim industry and organization size, 2015 dataset.

REN-ISAC CSIRT

Notifications	Jan. 2016	Feb. 2016	March 2016	April 2016	Total
compromised machines	7,885	8,147	7,911	7,742	31,685
compromised credentials	6,889	4,698	1,575	7,267	20,429
spam or phish	42	29	46	29	146
vulnerable machines	-	-	1	1	2
open recursive DNS resolvers	263	168	362	239	1,032
open mail relays	21	17	14	11	63
other	-	-	1	-	1
total notifications:	**15,100**	**13,059**	**9,910**	**15,289**	**53,358**


Discussion Topics:
January - April, 2016
90
80
70
60
50
40
30
20
10
0
[JAN]
[FEB]
[MAR]
[APR]
Phishing
Ransomware
Software Vulnerabilities
Fraud Schemes

Vulnerabilities

Attacks come in millions, exploits are automated

Badlock Bug

On **April 12th, 2016** a crucial security bug in Windows and Samba will be disclosed. We call it: **Badlock**.

Engineers at Microsoft and the Samba Team are working together to get this problem fixed. Patches will be released on April 12th.

Admins and all of you responsible for Windows or Samba server infrastructure: Mark the date. (Again: It's **April 12th, 2016**.)

Please get yourself ready to patch all systems on this day. We are pretty sure that there will be exploits soon after we publish all relevant information.

Vulnerabilities

Reported Malware	Count
Conficker	1861
Bedep	1446
Gozi	816
Ponmocup	668
ZeroAccess	492
Kelihos	432
Fleercivet	265
Pushdo	262
Nivdort	184
Dorkbot	142
Zeus P2P	126
Zeus	124
Nymaim	122
Sality	113
Ramdo	107
Qakbot	90
Virut	72
Tinba	67

Reported Malware	Count
Ramnit	50
Beebone	49
Rovnix	36
Locky	25
Corebot	24
Slenfbot	24
Shiz	22
Murofet	20
Vawtrak	16
Dridex	15
Pykspa	15
ZeroAccess-Supernode	13
Torpig	12
Pony	10
Bamital	6
Vobfus	6
IRC bot	5
scanner	4

U.S. Department of Justice
Federal Bureau of Investigation

Ransomware is a form of malware that targets both human and technical weaknesses in organizations and individual networks in an effort to deny the availability of critical data and systems. Ransomware is frequently delivered through spear phishing e-mails to end users. When the victim organization determines they are no longer able to access their data, the cyber actor demands the payment of a ransom, at which time the actor will purportedly provide an avenue to the victim to regain access to their data. Recent iterations target enterprise end users, making awareness and training a critical preventative measure.

Federal Bureau of Investigation

Cyber Task Forces
www.fbi.gov/contact-us/field

Internet Crime Complaint Center
www.ic3.gov

Ransomware

Key areas to focus on with ransomware are prevention, business continuity, and remediation. As ransomware techniques continue to evolve and become more sophisticated, even with the most robust prevention controls in place, there is no guarantee against exploitation. This makes contingency and remediation planning crucial to business recovery and continuity.

Prevention Considerations

- Implement an awareness and training program. Because end users are targeted, employees and individuals should be made aware of the threat of ransomware and how it is delivered.
- Patch operating systems, software, and firmware on devices, which may be made easier through a centralized patch management system.
- Ensure anti-virus and anti-malware solutions are set to automatically update and that regular scans are conducted.
- Manage the use of privileged accounts. Implement the principle of least privilege: no users should be assigned administrative access unless absolutely needed; those with a need for administrator accounts should only use them when necessary.
- Configure access controls, including file, directory, and network share permissions, with least privilege in mind. If a user only needs to read specific files, they should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via e-mail. Consider using Office Viewer software to open Microsoft Office files transmitted via e-mail instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

Business Continuity Considerations

- Back up data regularly, and regularly verify the integrity of those backups.
- Secure your backups. Ensure backups are not connected to the computers and networks they are backing up. Examples might be securing backups in the cloud or physically storing offline. Some instances of ransomware have the capability to lock cloud-based backups when systems continuously back up in real time, also known as persistent synchronization. Backups are critical in ransomware; if you are infected, this may be the best way to recover your critical data.

Other Considerations

- Implement application whitelisting; only allow systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value, and implement physical/logical separation of networks and data for different organizational units.

The Ransom

The FBI does not support paying a ransom to the adversary. Paying a ransom does not guarantee an organization will regain access to their data; in fact, some individuals or organizations were never provided with decryption keys after having paid a ransom. Paying a ransom emboldens the adversary to target other organizations for profit, and provides for a lucrative environment for other criminals to become involved. While the FBI does not support paying a ransom, there is an understanding that when businesses are faced with an inability to function, executives will evaluate all options to protect their shareholders, employees, and customers.

In all cases the FBI encourages organizations to contact a local FBI field office immediately to report a ransomware event and request assistance. Victims are also encouraged to report cyber incidents to the FBI's Internet Crime Complaint Center (www.ic3.gov).

Ransomware

Your files were encrypted and locked with a RSA4096 key

To decrypt your files:
Download the Tor browser here and go tc [redacted] within the browser.
Follow the instructions and you will receive the decrypter within 12 hours.
You have ten days to obtain the decrypter before the private key is deleted from our server - leaving your files irrevocably broken.
Your ID is 7385827

Guaranteed recovery is provided before scheduled deletion on 05/30/2014 04:59:35

Friday Pulse Survey: Ransomware

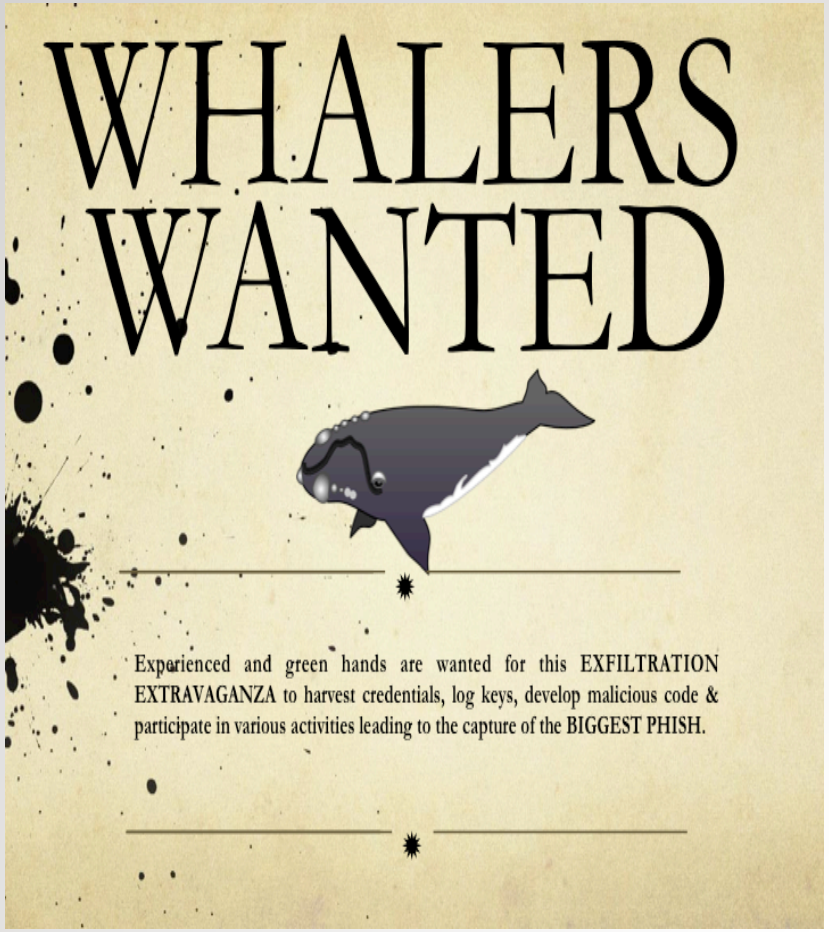
With regard to ransomware, how has the amount of time spent on incident response changed in the last 3 months?	
Increasing	4
Decreasing	3
About the same	18

What are you doing to mitigate the risk of Ransomware?	
Increasing employee education and awareness efforts	19
Tightening spam filters on email systems	11
Accelerating the institution's move to cloud storage	1
Reminding system administrators to verify/test backups, check schedules	9
Updating institutional policies / standards	2

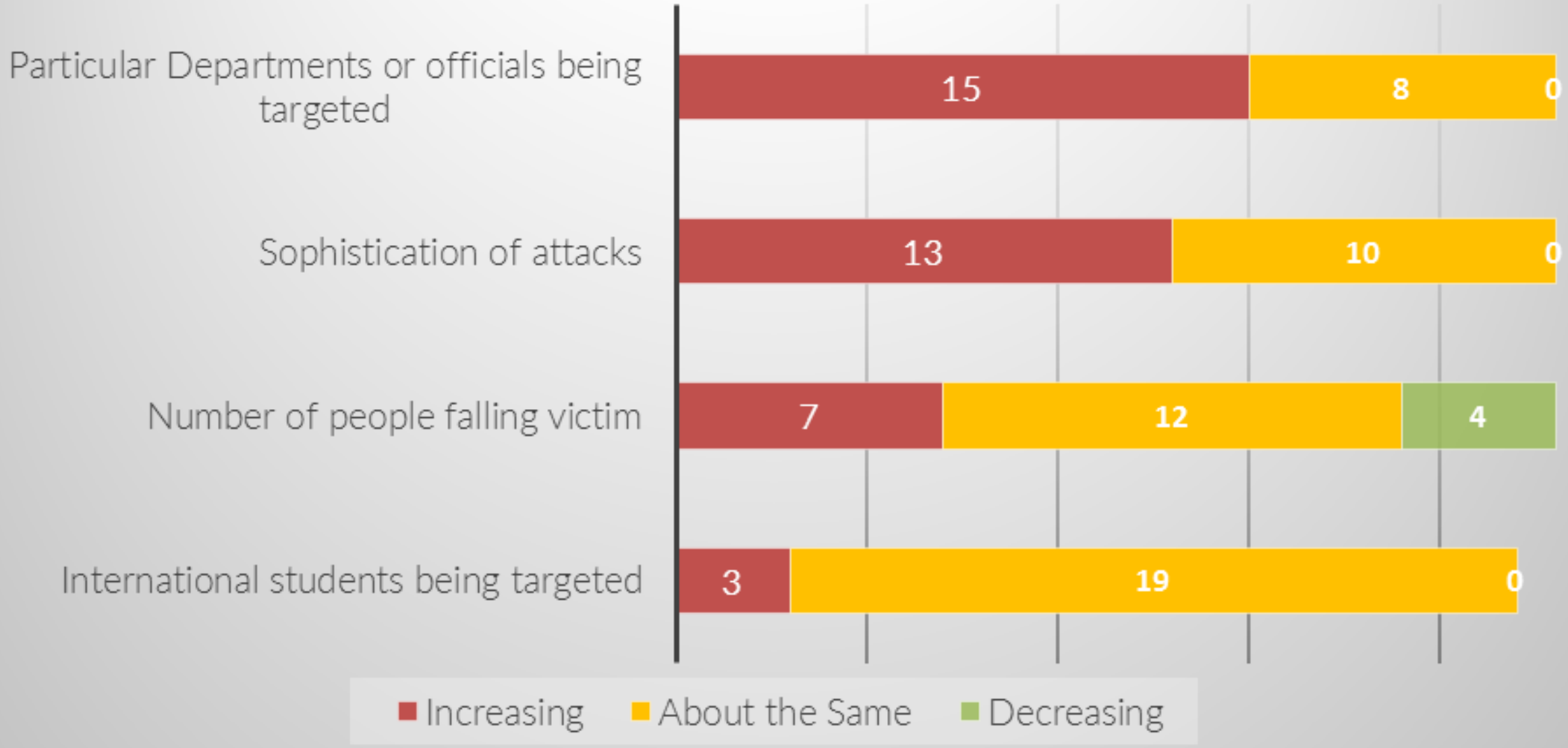

THE INSIDERS

Phishing, Spear-phishing, Whaling & Poison Harpooning

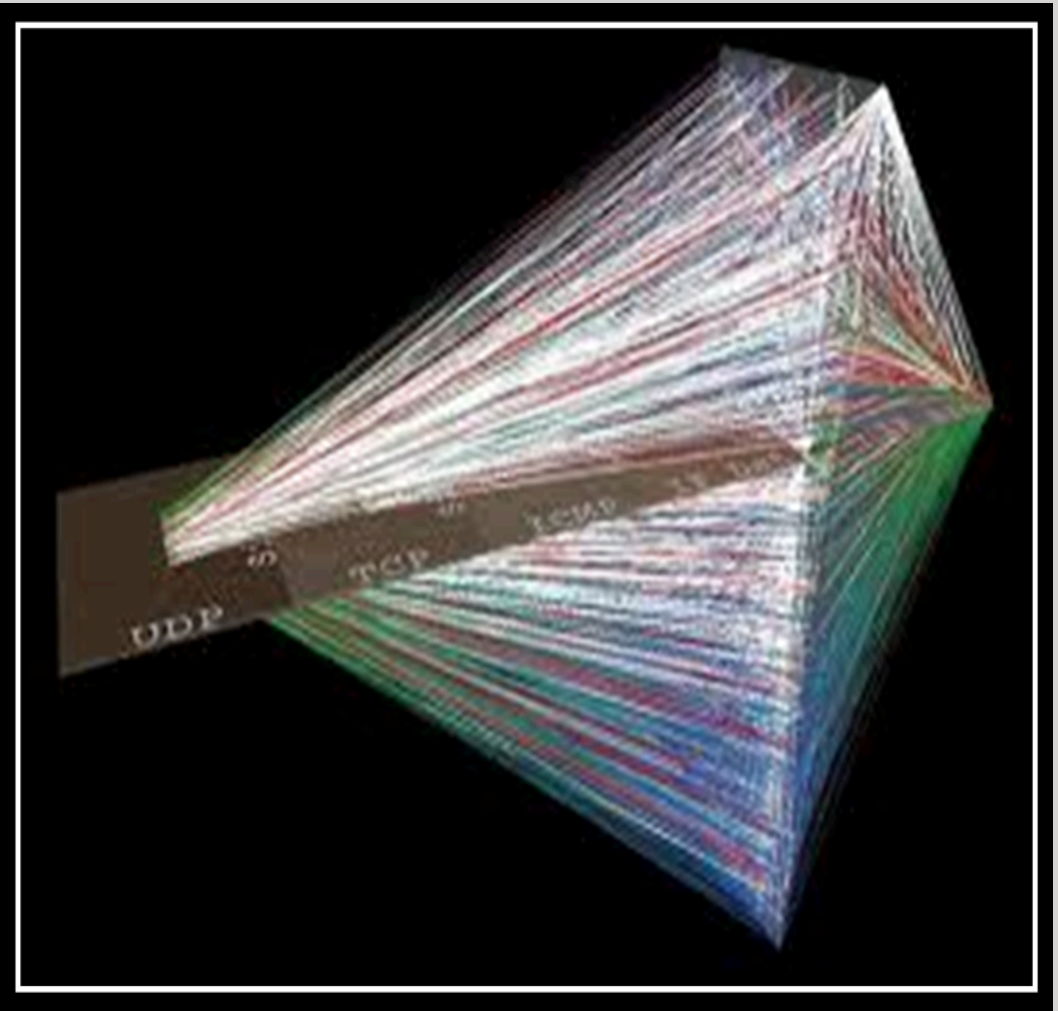
- Nearly 50% of users open phishing email and click on the links within the first hour after they receive
- Phishing is now the established initial attack vector for online crime



Drill-down on Phishing: Trends



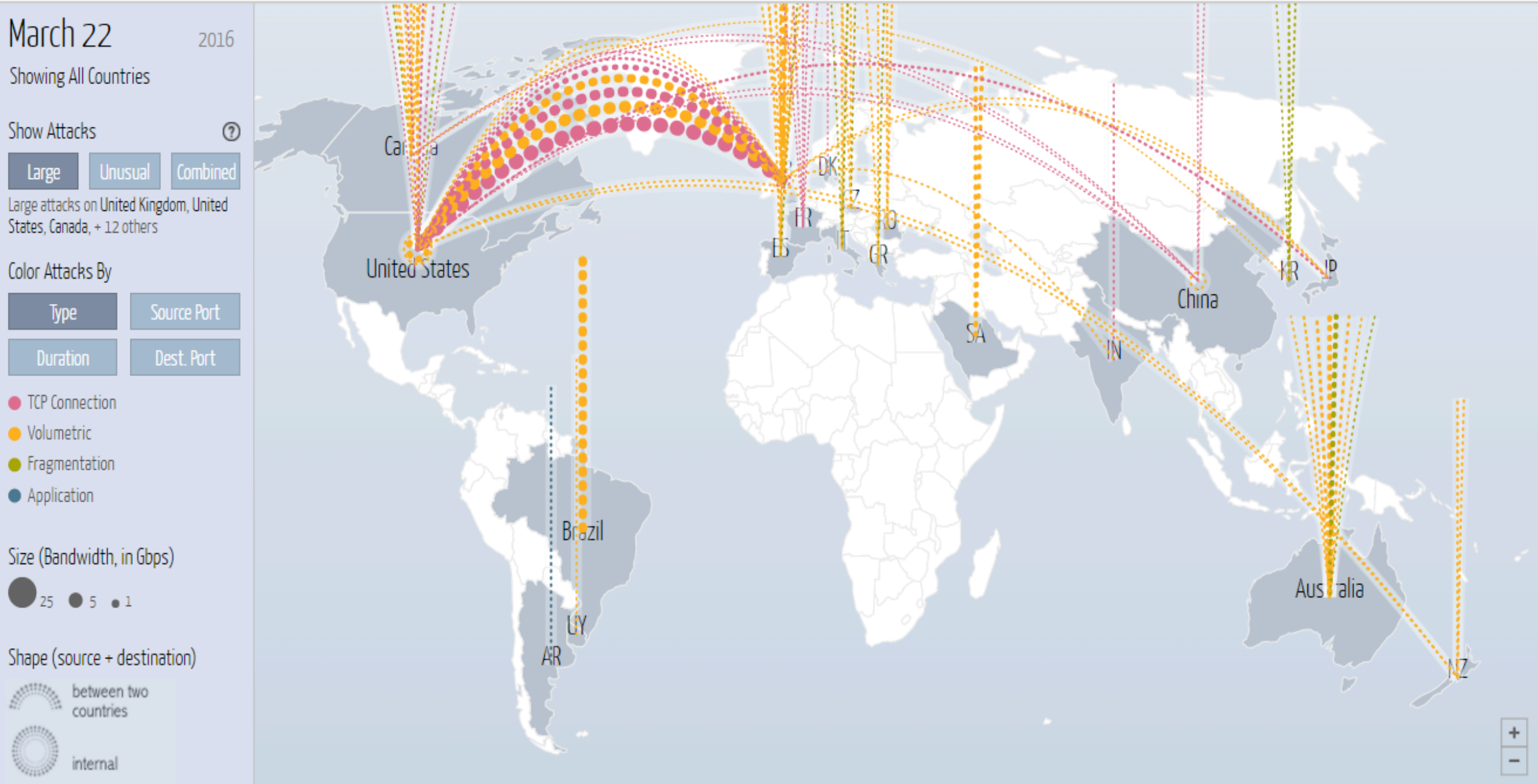
Denial of Service Attacks



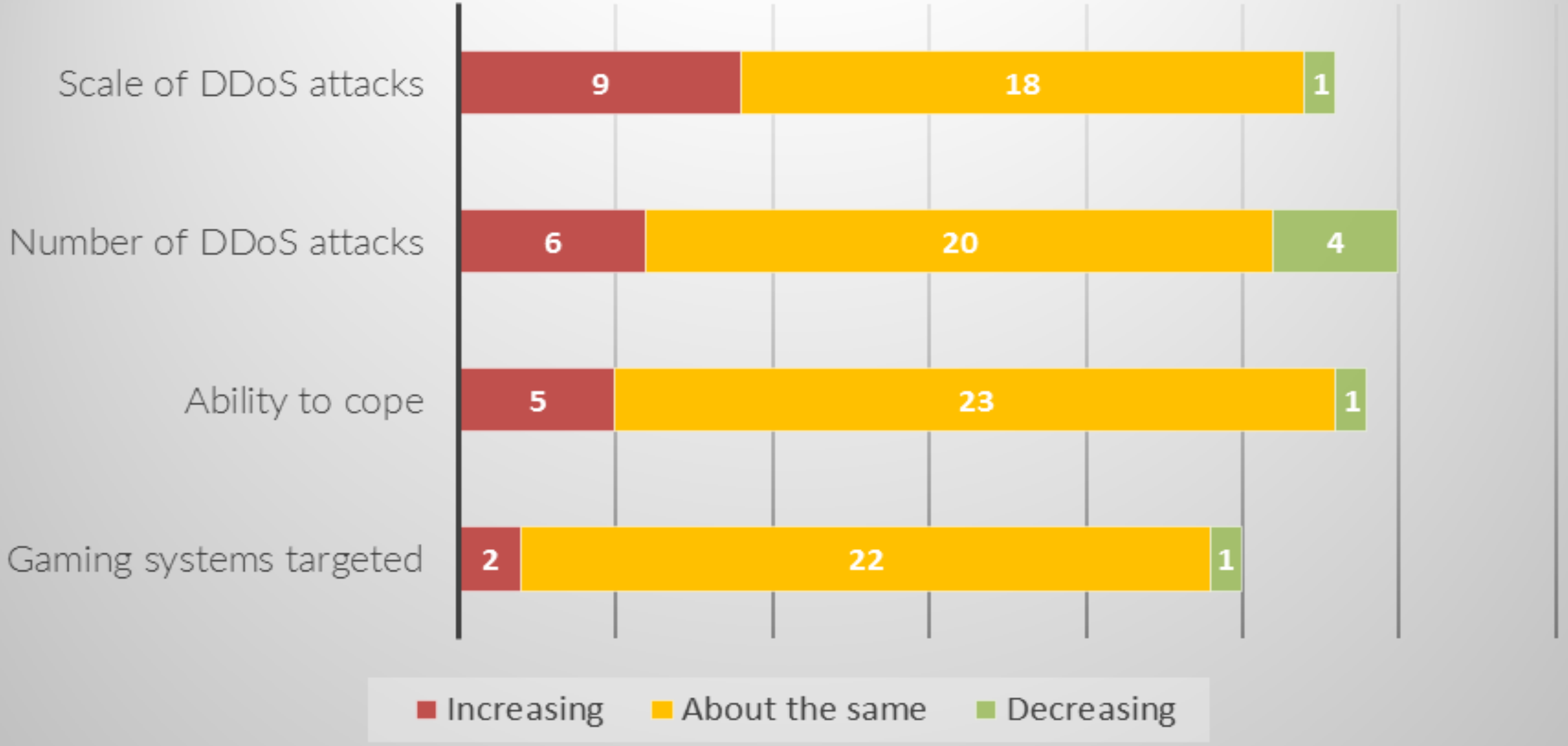
- Amplification via vulnerable protocols, e.g. NTP
- Increasing use of powerful cloud infrastructure, e.g., AWS

Digital Attack Map

Top daily DDoS attacks worldwide



Drill-down on DDoS Attacks



Compromised Credentials

DEVELOPING CYBERSECURITY PROGRAMS FOR NSF PROJECTS:

REN-ISAC CYBERTHREAT BRIEFING

Kim Milford
Research & Education Networking
Information Sharing & Analysis
(REN-ISAC)