PH1SH1NG

Attn: Sir/Madam

AGENDA

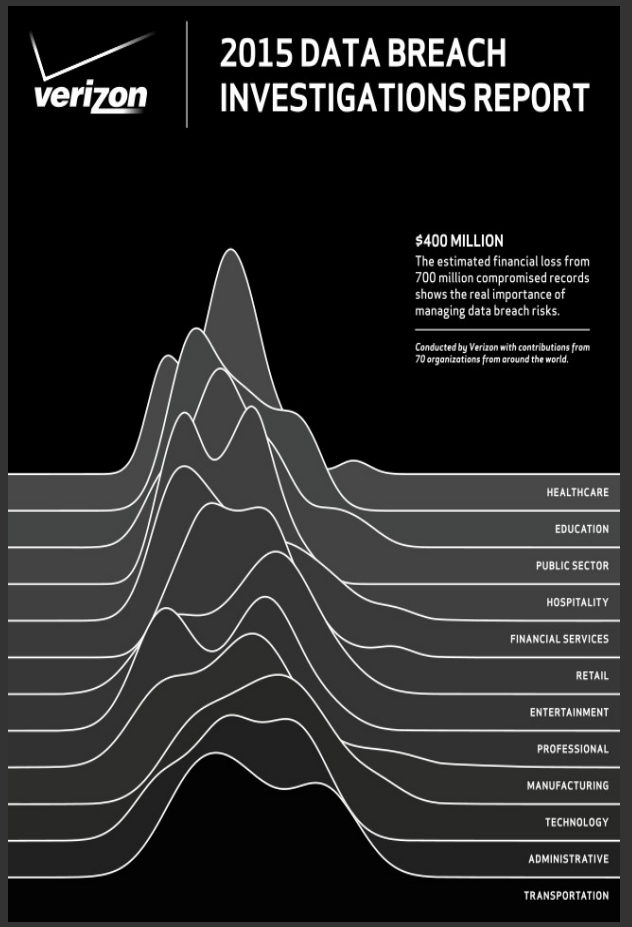
* references
* intro to phishing
* big targets
* typosquatting
* threat mitigation

REFERENCES

VERIZON DBIR (2015)

* 70 contributing organizations
* 79,790 security incidents
* 2,122 confirmed data breaches

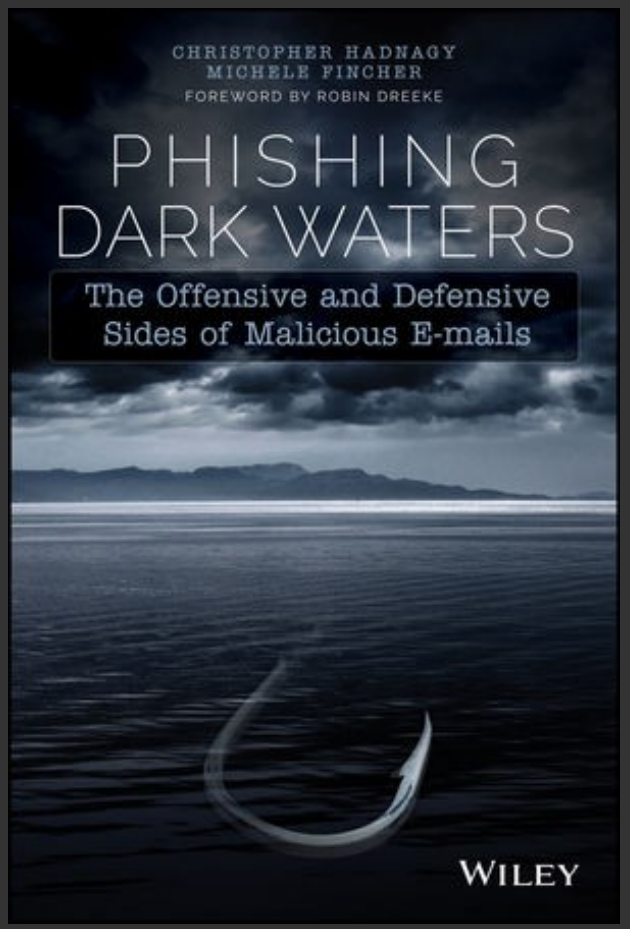
* recommended reading



PHISHING DARK WATERS

* Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails

* go get one or read online



REFERENCES

* www.verizonenterprise.com/DBIR/2015

* www.safaribooksonline.com/library/view/phishing-dark-waters/9781118958483

* www.securityweek.com/manual-account-hijacking-rare-damaging-google

INTRO TO PHISHING

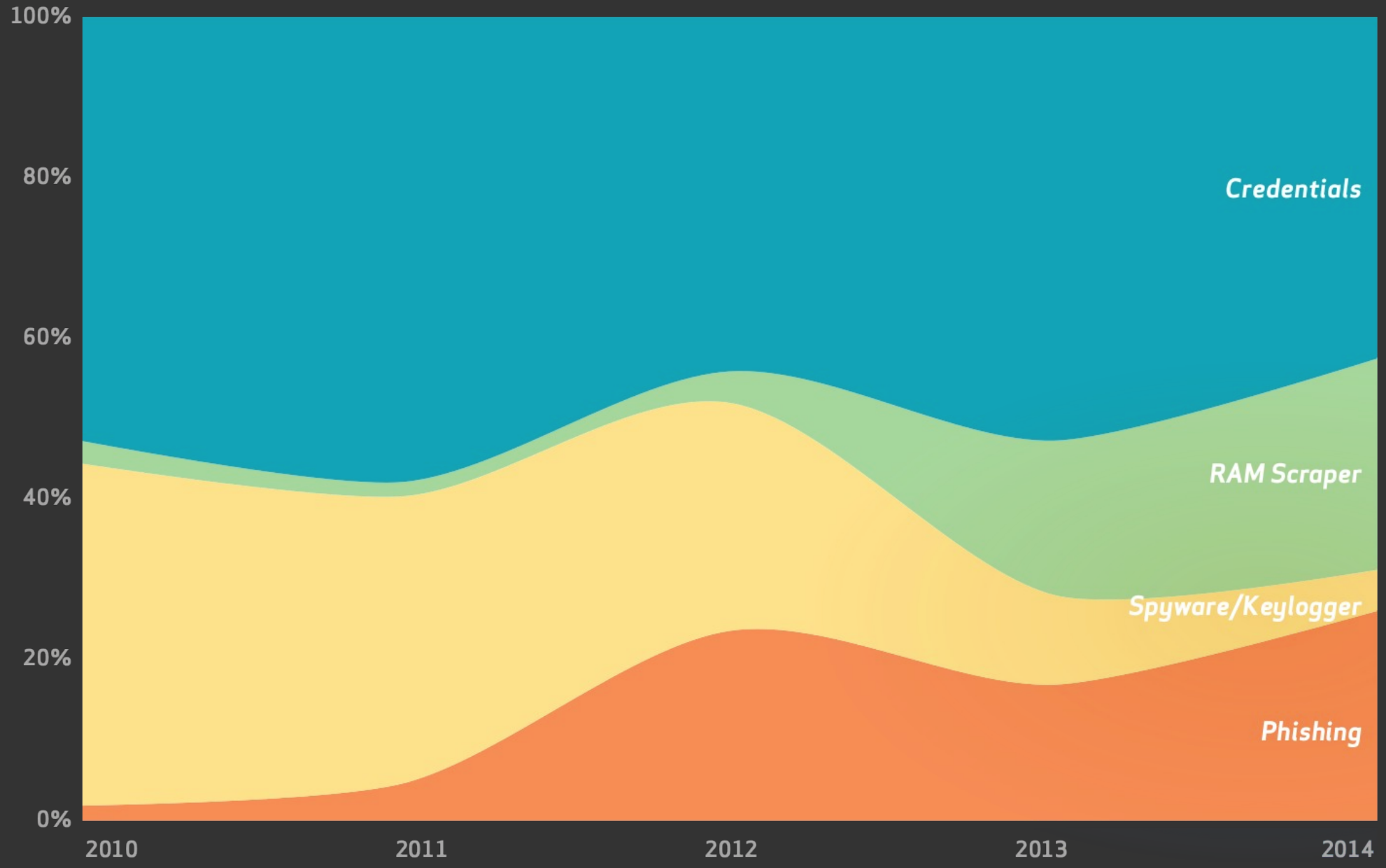
WHAT IS PHISHING?

* attempt to obtain sensitive information such as usernames, passwords, credit card details by spoofing legitimate entity

* email will typically direct user to visit malicious website or encourage to open attached malware

* favorite and reliable tactic of state-sponsored threat actors and criminals with the intent to gain an access to a network

SIGNIFICANT THREAT ACTIONS

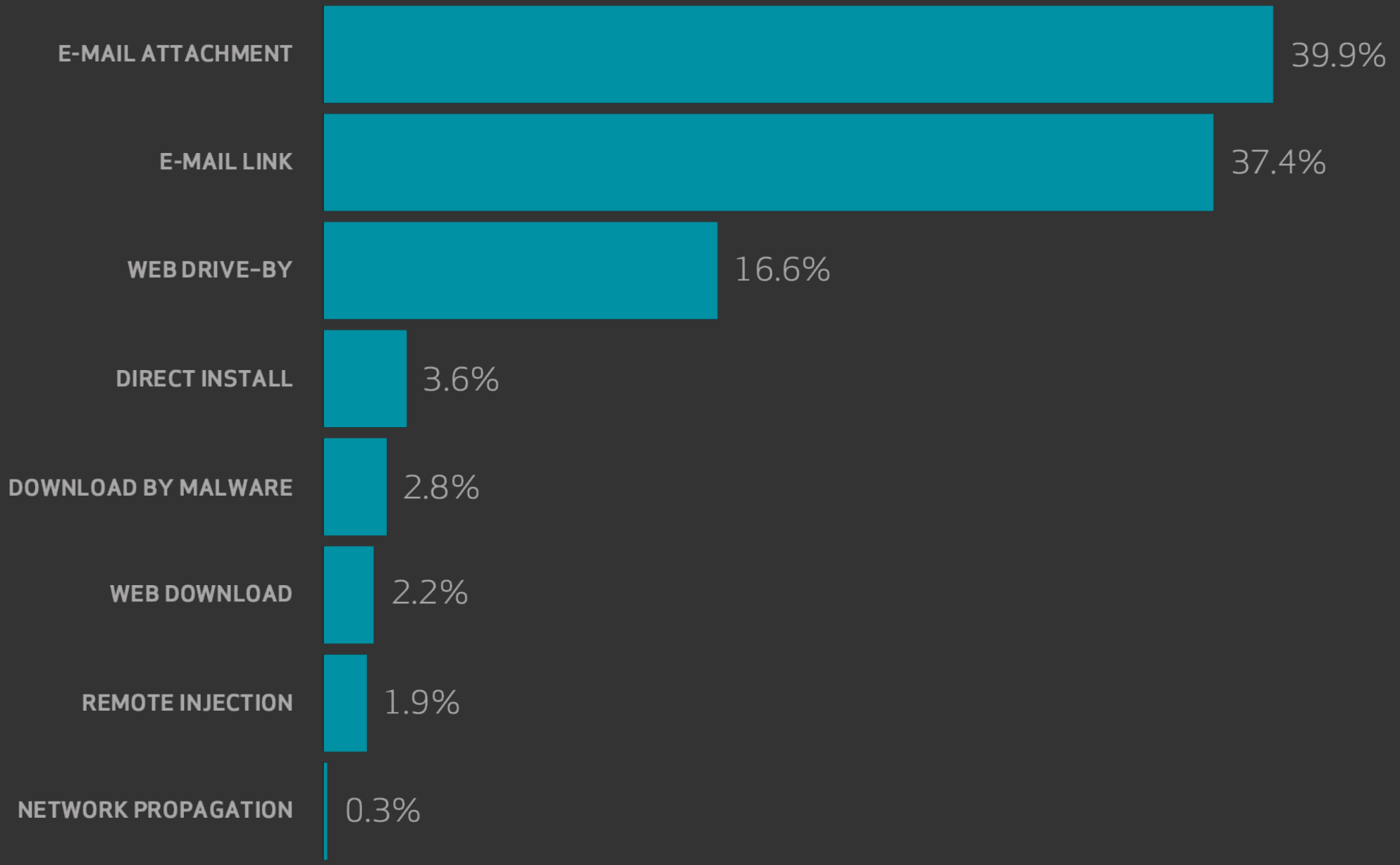


PHISHING ON THE RISE

* 23% of recipients open phishing messages and 11% of recipients click on attachments

* more than 2/3 of incidents classified as cyber-espionage have featured phishing in last 2 years

MALWARE INSTALLATION (CE 2015)



THERE IS MORE

* aggregated the results of over 150k emails sent by infosec partners

* nearly 50% open e-mails and click on links within the first 1 hour

* the median time-to-first-click is 82 seconds across all campaigns

CONCLUSION

* phishing is serious problem

* small, targeted campaigns are guaranteed to work

* there is no time on our side when it comes to detecting and reacting to phishing attacks

BIG TARGETS

GMAIL (2011 - 2014)

* attackers attempted to access 20% of accounts with harvested credentials within 30 minutes and 50% within 7 hours

* attackers spent an average of 3 minutes searching accounts to determine their value (financial data or other credentials)

* contact of a compromised account was 36 times more likely to receive phishing emails

TARGET (2013)

* one of the highest-profile breaches to date
  * affected around 110 million consumers
  * estimated 40 million credit cards
  * 70 million people with stolen PII

* total cost $252 mln ($90 mln covered by insurance)

ASSOCIATED PRESS (2013)

* Twitter account has been temporarily suspended after tweeting:

Breaking: Two Explosions in the White House and Barack Obama is injured.

* Dow Jones Industrial Average dropped 150 points as it was retweeted

OPM (2015)

* 18 mln records and details on federal employees exposed

* malicious domains: opmsecurity.org and opm-learning.org

* OPM sents e-mails to employees to notify them of the breach and encourages to click on link to 3rd party web site to sign up for credit monitoring

TYPOSQUATTING

SLIDE REDACTED

SLIDE REDACTED

How tough are you?

Can I play, Daddy?
Don't hurt me.
Bring 'em on!
I am Death incarnate!

GENERAL ADVICE (NOT SO USEFUL)

* don't open or download attachements
* inspect and don't click on suspicious links
* don't submit personal information
* report phishing to your favourite #security slack channel

THREAT MITIGATION

* better email filtering at the gateway
* security awareness program
* improved detection and response

END OF PART 1