MIS|TI™ PRESENTS

InfoSec World

Conference & Expo 2018

THE FOUR PITFALLS OF PRIVILEGE: DEFEND CRITICAL ACCOUNTS & SYSTEMS AGAINST CYBERCRIME

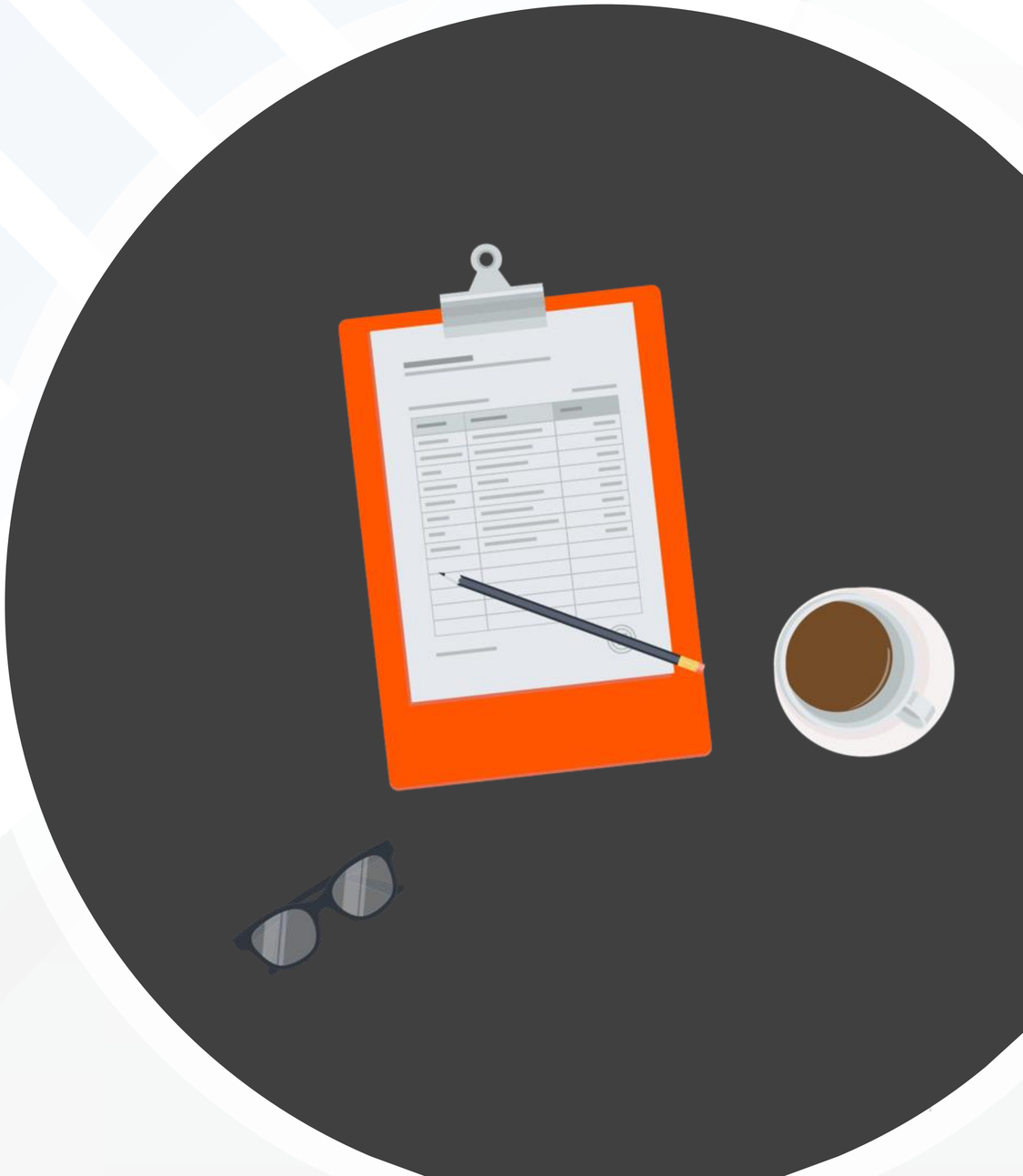
Sam Elliott

Director of Security Product Management / Bomgar

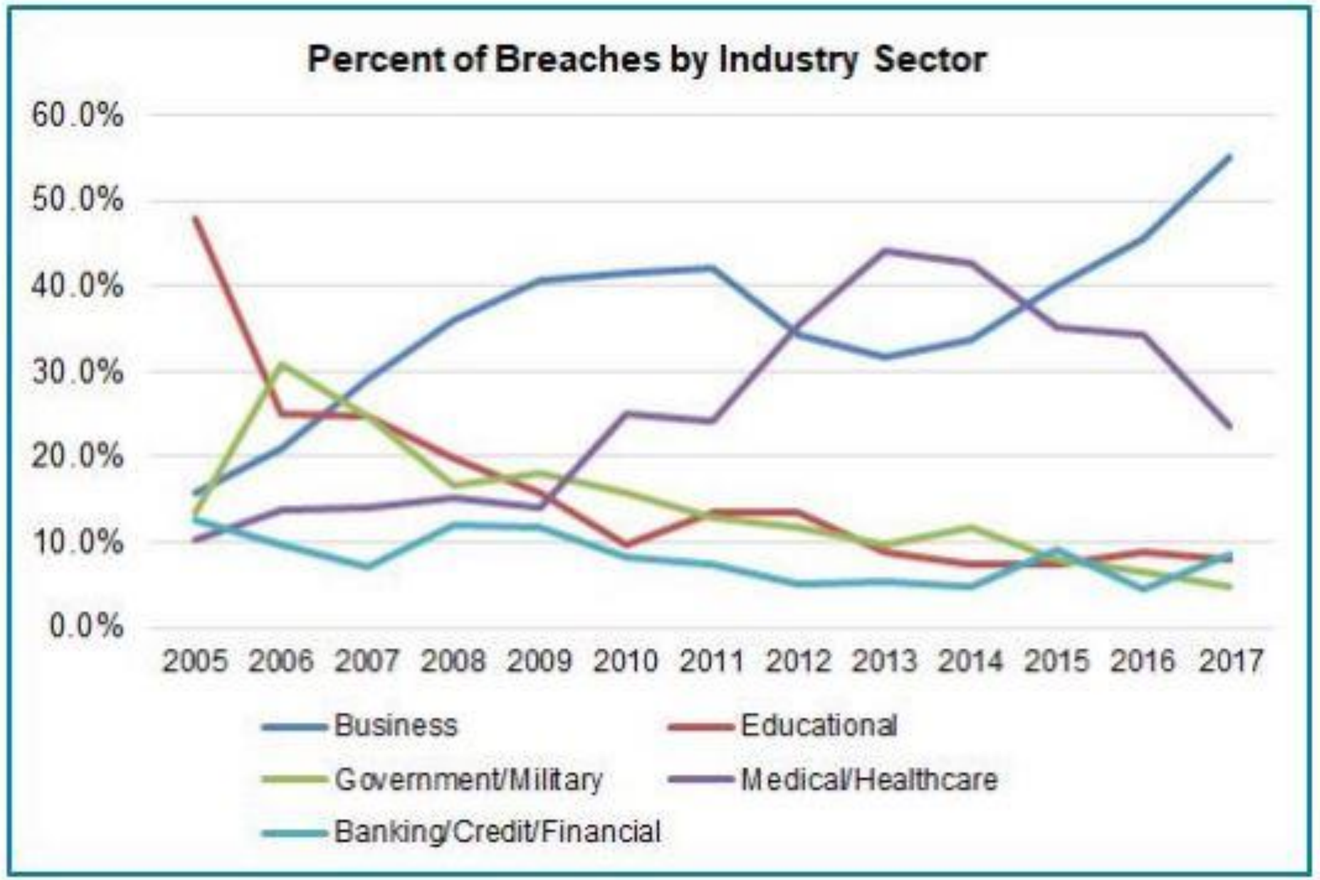
@samelliott / @bomgar

AGENDA

- Security Realization
- Gaps left by traditional approaches to privileged access
- Common “Pitfalls of Privilege”
- How to avoid the pitfalls
- Q&A

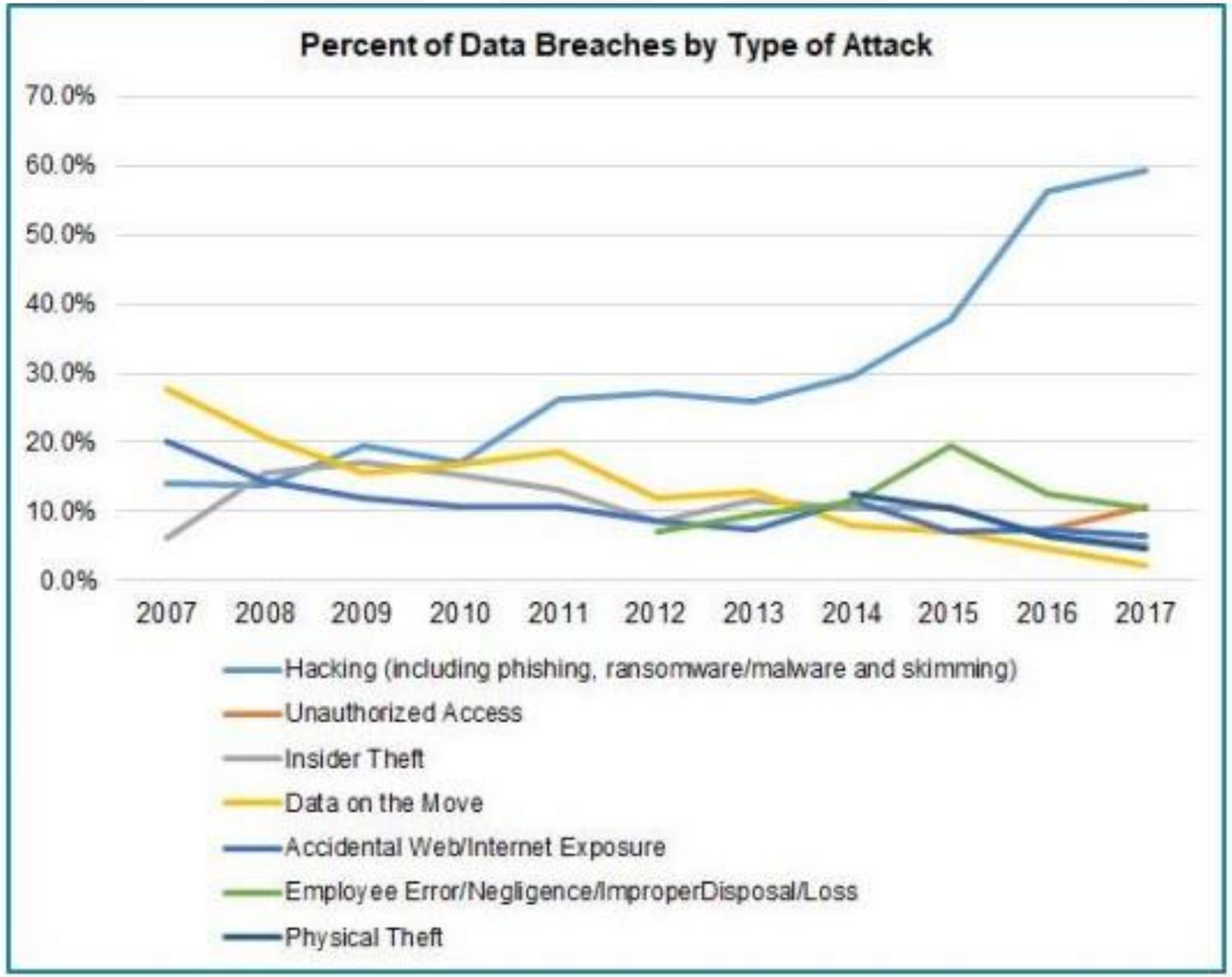


2017 = THE RISE OF THE DATA BREACH

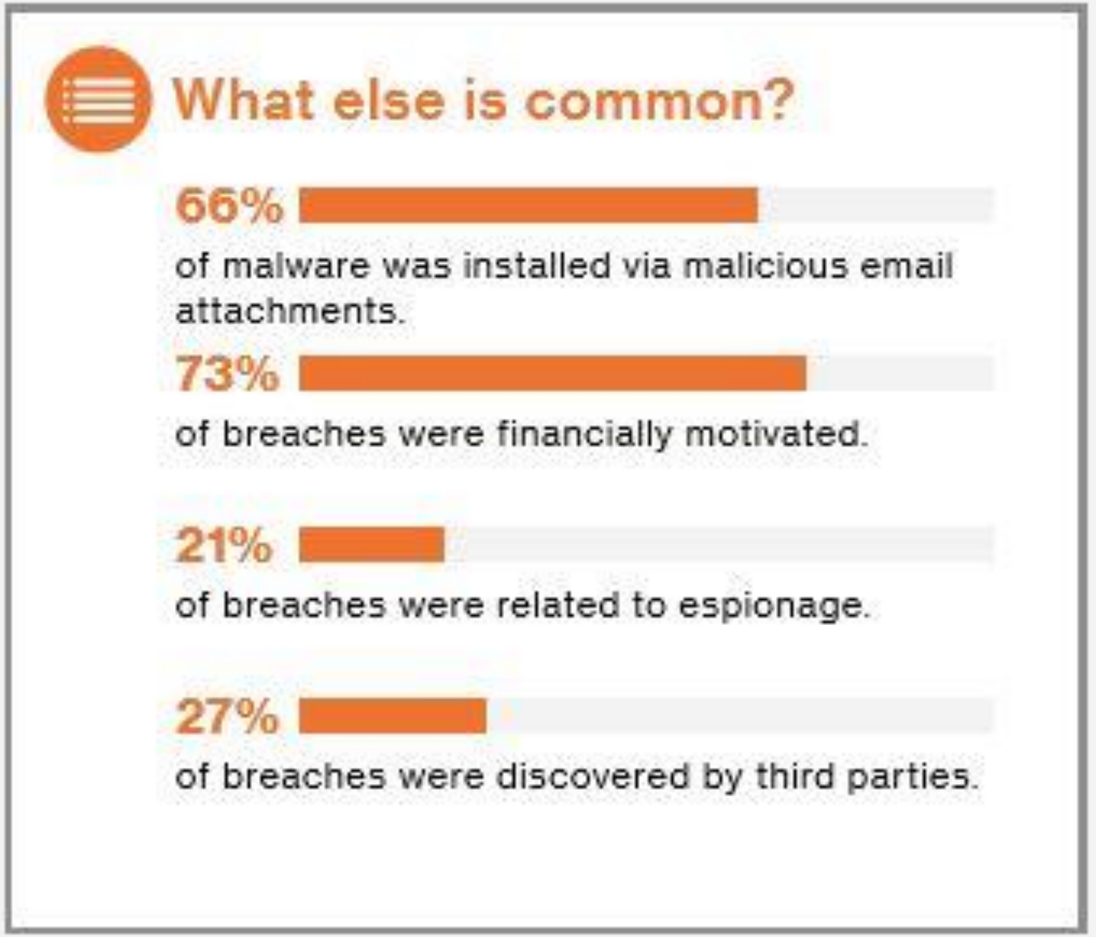


HACKING LEADS THE WAY…

- Phishing
- Ransomware
- Malware
- Skimming



RANSOMWARE ON THE RISE



2017 Data Breach Investigations Report (Verizon)

RANSOMWARE ON THE RISE

What tactics do they use?

62%
of breaches featured hacking.

51%
over half of breaches included malware.

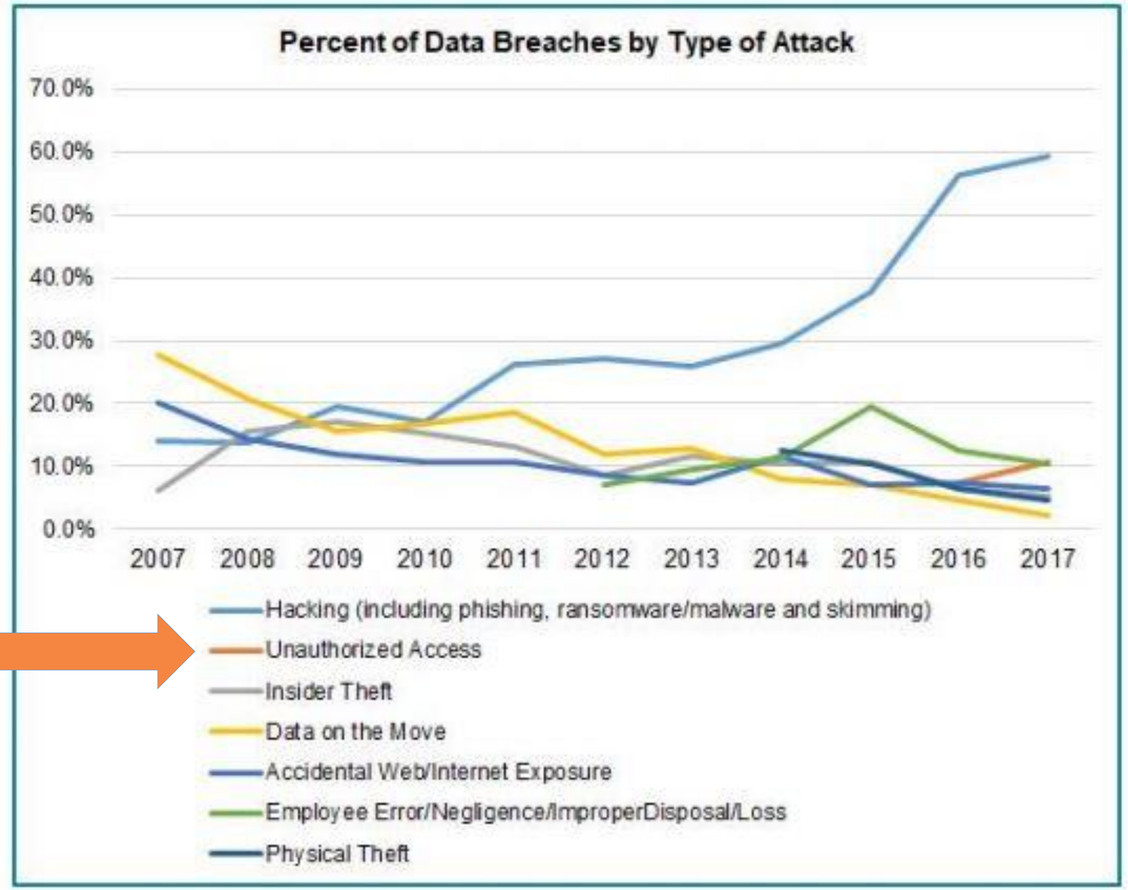
81%
of hacking-related breaches leveraged either stolen and/or weak passwords.

43%
were social attacks.

14%
Errors were causal events in 14% of breaches. The same proportion involved privilege misuse.

8%
Physical actions were present in 8% of breaches.

2017 Data Breach Investigations Report (Verizon)



2017 Annual Data Breach Year-End Review (Identity Theft Resource Center)

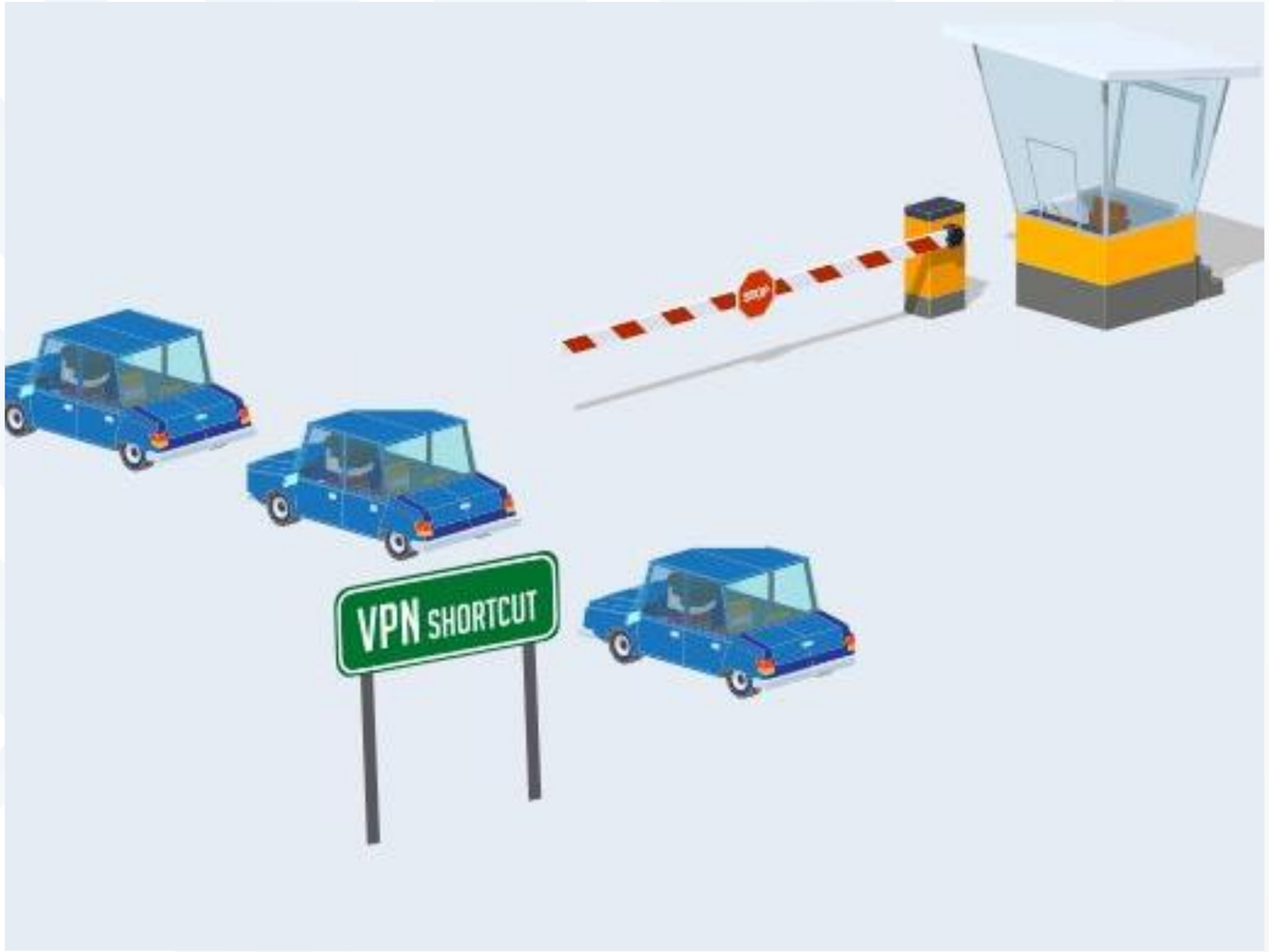
- Entry point – conference room window
- Easily navigate from the conference room, to the lobby
- From the lobby, you can now go anywhere in the bank (other conferences rooms, offices, filing rooms, etc.)
- Jump over the teller wall

- Entry point – compromised credentials
- Navigate from one system (room) to another
- All or nothing network access
- Leaving behind devices (malware) in drawers and cabinets behind the teller desks
- When the next business day comes around, your devices are at work gathering information needed to crack the vault

COMMON CHALLENGES THAT CAN CREATE “PRIVILEGE PITFALLS”

PITFALL #1: PROTECTING ONLY PASSWORDS

- Focus solely on privileged credentials or identities
- Unsecured pathways/access
- Included other solutions integrated with an enterprise password vault for a true defense-in-depth strategy



TOTAL RESULTS

1,978,134

TOP COUNTRIES

United States	485,779
China	424,781
Germany	84,958
Brazil	74,719
France	60,811

TOP SERVICES

RDP	1,950,547
RDP (3388)	26,993
SMB	284
Citrix	241
HTTP	25

TOP ORGANIZATIONS

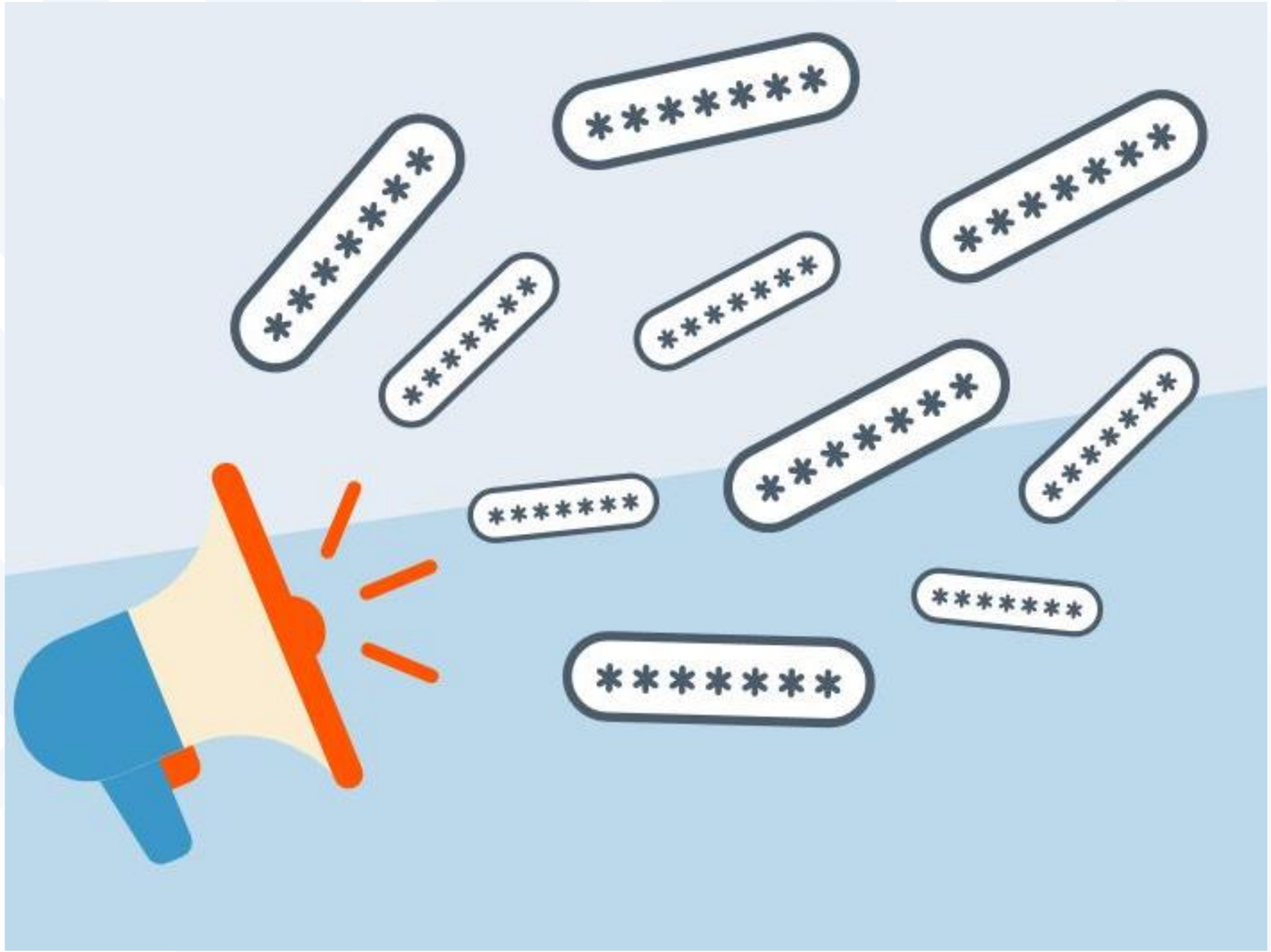
Amazon.com	119,494
Hangzhou Alibaba Advertising Co....	116,214
Tencent cloud computing	81,201
Korea Telecom	30,804
Comcast Business	29,704

PITFALL #2: PARTNERS WITH PRIVILEGES

- Focus on just employees
- Failure to consider outside vendors or contractors
- Unfettered VPN access allowed to the network

PITFALL #3: PRIVILEGE SPRAWL

- Failure to secure all non-traditional privileged accounts
- Cloud migration struggles



“Out of all the incident response engagements that we conducted; 100% of them involved the threat actor compromising valid credentials during the attack.”

SOURCE:

HTTPS://WWW.FIREEYE.COM/BLOG/PRODUCTS-AND-SERVICES/2015/08/MALWARE_LATERAL_MOVE.HTML

PITFALL #4: PRIORITIZING ONLY PEOPLE

- What about the machines?
- Securing privileged ‘app-to-app’ credentials or service accounts often get ignored


IT ORCHESTRATES
ON MY MACHINE

MAKE LEAST PRIVILEGE PRODUCTIVE

- Our goal is to prevent the initial compromise and to prevent data exfiltration
- Even if we fail to prevent the initial compromise, we can prevent useful lateral movement

Bomgar Privileged Access Management

- Eliminate a cybersecurity threat vector
- Meet privileged access compliance requirements
- Give them a privileged access solution they'll love
- Secure the access, defend the credential

MIS|TI™ PRESENTS

InfoSec World

Conference & Expo 2018

THANK YOU

PLEASE FILL OUT YOUR EVALUATIONS!

Sam Elliott

Director of Security Product Management / Bomgar

@samelliott / @bomgar