MIS|TI™ PRESENTS

InfoSecWorld

Conference & Expo 2018

AUTOMATED CYBER DEFENSE:

LEVERAGING IDENTITY MANAGEMENT TO GET TO ACCEPTABLE LOSS

Sam Elliott

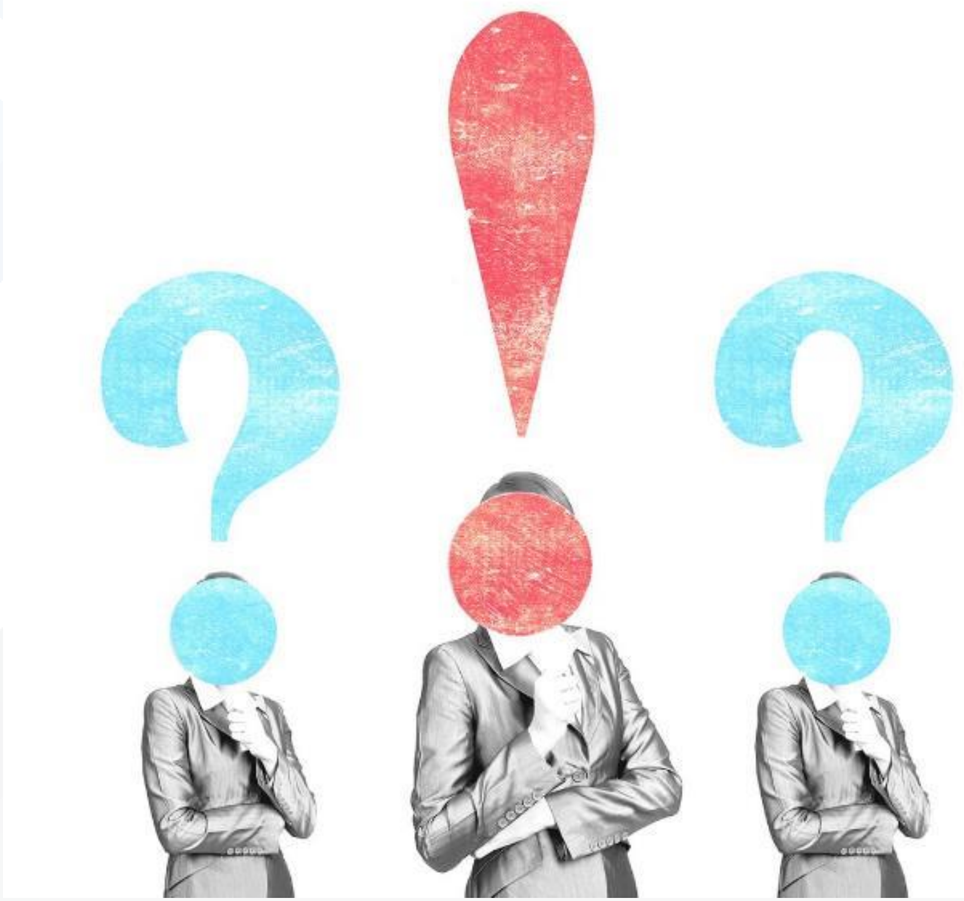
Director of Security Product Management / Bomgar

@samelliott / @bomgar

A breach is a matter of **if**, not **when**

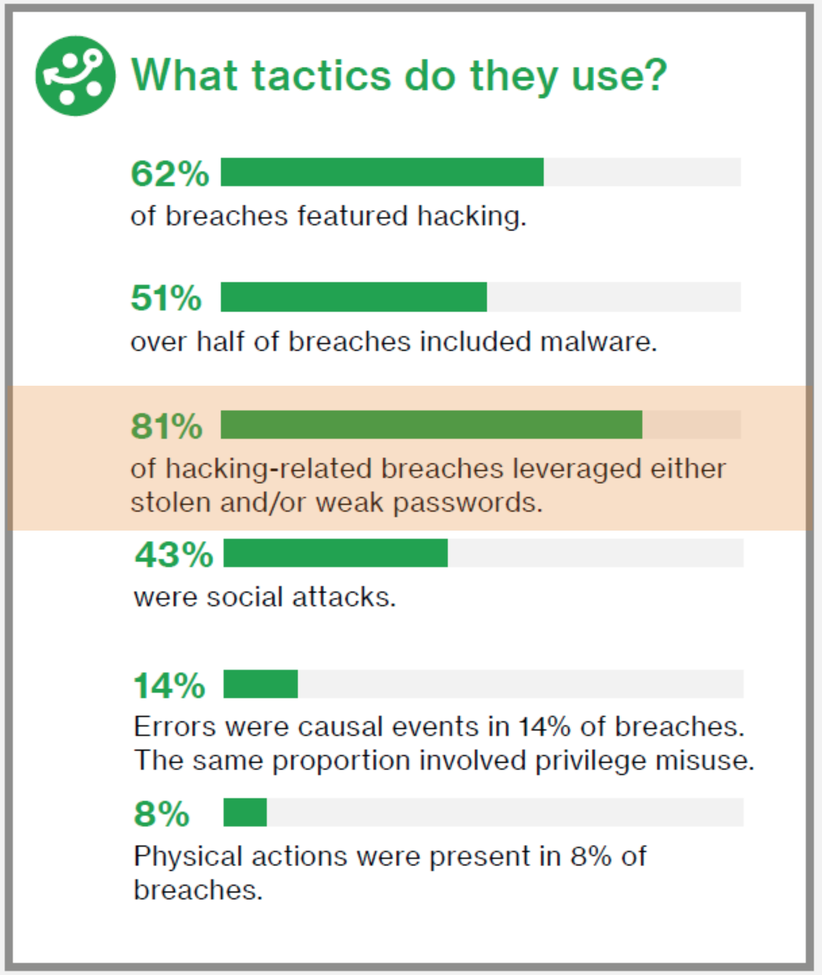
Goal should be to contain breaches to a level of **acceptable loss**

Automating **privileged identity & access** management can help mitigate threats



81% OF HACKING-RELATED BREACHES LEVERAGE STOLEN AND/OR WEAK PASSWORDS

- Privileged credentials are highly targeted “keys to the kingdom”.
- Passwords and privileges are often long-lived and never changed.
- Admin passwords are often shared across teams.



verizon 2017 Data Breach Investigations Report

MORE AND MORE PEOPLE AND SYSTEMS ARE GAINING PRIVILEGES

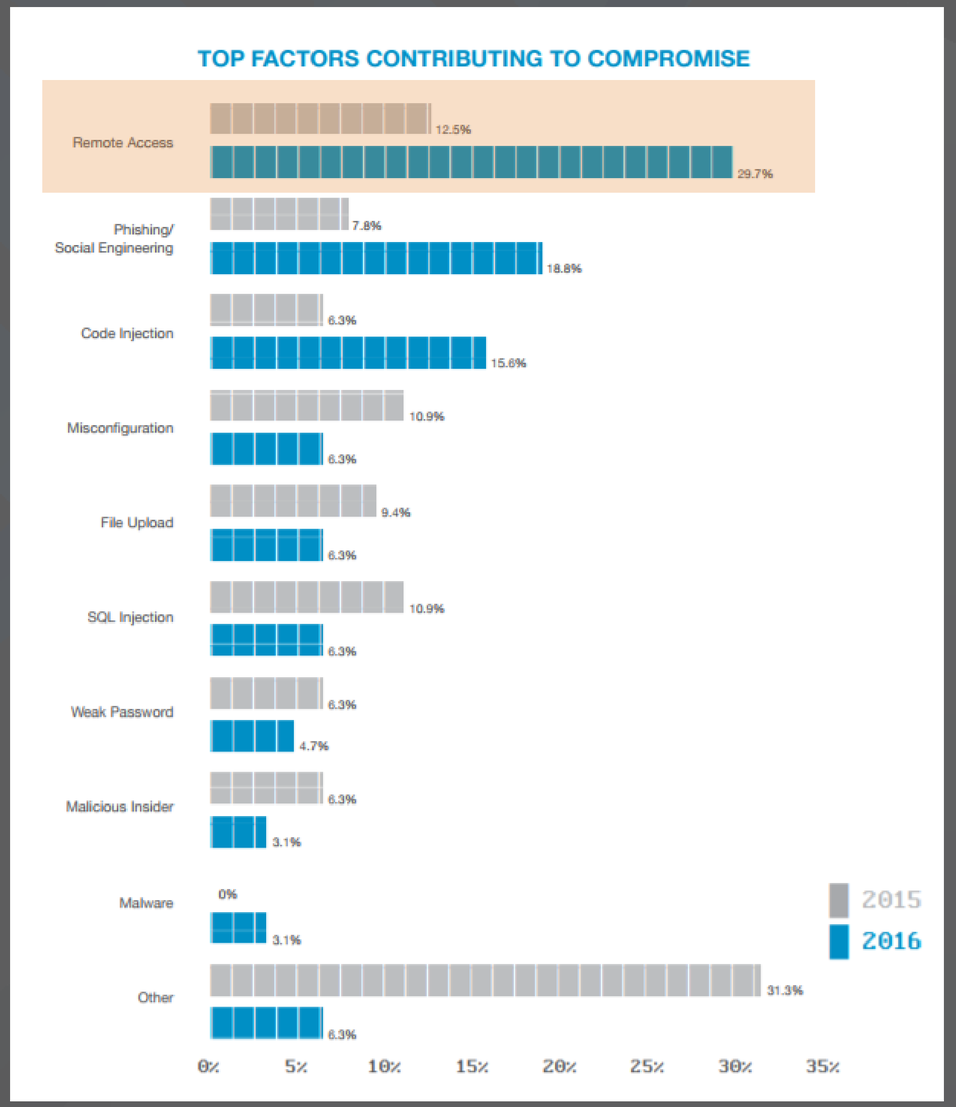
- Privileges are easy to give, but difficult to retract.
- Failure to secure credentials used by non-standard users: service desks, service accounts, app to app, third-party vendors, etc.
- Limited visibility into all privileged accounts across an enterprise.

EVERYTHING-CONNECTED NETWORKS ARE CREATING EASY ENTRY POINTS FOR ATTACKERS

- Gartner forecasts that the number of connected things in use worldwide will reach 20.4 billion by 2020.
- Interconnected networks and IoT are widening the attack surface for our privileged systems and data.
- Making it easier for lateral movement.

REMOTE ACCESS IS #1 METHOD OF COMPROMISE

- Extremely easy for threat actors to find unsecured remote access pathways.
- Most security organizations don’t have visibility into all of the remote access pathways into their networks.
- Different teams & external vendors using their preferred tools.
- No centralized monitoring or auditing.



Trustwave® 2017 Global Security Report

InfoSecWorld Conference & Expo 2018

●●○○○ Verizon VPN 9:21 AM 77%

igyifrhnvxq33sy5.onion

Logout

Browse by category
- Digital Goods 41815
- Fraud Related 5253
  - Accounts 2573
  - Bank Logins 492
  - Other 681
  - Paypal 567
- Digital Goods 41815
- Drugs 47435
- Drugs Paraphernalia 293
- Services 4052
- Other 3387

Onion mirrors

Links
- Forum
- Help
- Conferences
- Vendor application
- Earn money

Exchange

BTC	1.0
mBTC	1000.0
USD	6386.2
EUR	5479.9
GBP	4805.9
CAD	8203.5
AUD	8285.7
SEK	53523.0
NOK	51906.4
DKK	40776.6
TRY	24369.5
CNH	42091.8
HKD	49835.0
RUB	371707.7
INR	411497.9
JPY	727397.4

News
- Downtime & Recovery
- Deposit delays
- Forum under maintainance
- Earn money by finding bugs
- Forum Relaunched

Hint: Javascript enabled

★RDP login★ hacked

Vendor Johnbronz (2000) (4.59 ★) (109/5/6)

Price ฿0.000939 ($6)
Ships to Worldwide, Worldwide
Ships from Worldwide
Escrow Yes

Product description

available countries:

Argentina
Bahrain
Bangladesh
Brazil
Bulgaria
Cambodia
Chile
China
Costa Rica
Egypt
Ghana
India
Indonesia
Iran
Jordan
Kenya
Korea
Kuweit
Latvia
Lebanon
Malaysia
Mauritius
namibia
Nepal
Nigeria
Pakistan
Papua New Guinea
Philippines
Russian Federation
Rwanda
Singapore
South Africa
Taiwan
Thailand
Turkey
Uganda
Vanuatu

$6

●●○○○ Verizon VPN 9:24 AM 76%

igyifrhnvxq33sy5.onion

Browse by category
- Digital Goods 41815
  - Data 1394
  - Drugs 446
  - E-Books 12504
  - Erotica 2951
  - Fraud 2793
  - Fraud Related 5253
  - Hacking 1509
  - Information 11507
  - Other 583
  - Security 388
  - Software 1094
- Digital Goods 41815
- Drugs 47435
- Drugs Paraphernalia 293
- Services 4052
- Other 3387

Onion mirrors

Links
- Forum
- Help
- Conferences
- Vendor application
- Earn money

Exchange

BTC	1.0
mBTC	1000.0
USD	6386.2
EUR	5479.9
GBP	4805.9
CAD	8203.5
AUD	8285.7
SEK	53523.0
NOK	51906.4
DKK	40776.6
TRY	24369.5
CNH	42091.8
HKD	49835.0
RUB	371707.7
INR	411497.9
JPY	727397.4

News
- Downtime & Recovery
- Deposit delays
- Forum under maintainance
- Earn money by finding bugs
- Forum Relaunched

Hint: Javascript enabled

NON-Hacked VPS/RDP Service

Vendor ultimatum2016 (840) (4.82 ★)
(26/1/1) (100~200, 4.97/5)

Price ฿0.0001565 ($1)
Ships to Worldwide, Worldwide
Ships from Worldwide
Escrow Yes

Product description

SPECIAL REQUESTS VIA PM

Windows Desktop VPS with
2.40 GHz Intel Xeon

****
Ram: 1 GB DDR3 with Unlimited Bandwidth: 25 USD Month
Ram: 2 GB DDR3 with Unlimited Bandwidth: 40 USD Month
Ram: 4 GB DDR3 with Unlimited Bandwidth: 50 USD Month
Ram: 8 GB DDR3 with Unlimited Bandwidth: 60 USD Month

****
Storage Capacity: 100GB SSD,
10 GBPs Network Port
****

I am selling RDP access (windows Server/Windows7).

DON'T ASK FOR RDP'S FROM ZIPCODES I JUST HAVE WHAT YOU SEE IN THIS LISTING

Lasts at least 30 days (if you need more time, i can help you with that)
Strong, fast,
Reliable
just what you need to card / Paypal / Amazon /
No ip Logs
Uptime of 99.99%
IP available in US, UK, Europe, Asia

Terms and conditions of ultimatum2016

Hello Ladies and Gents!

FOR A FASTER RESPONSE PLEASE DON'T ENCRYPT ALL MESSAGES. ONLY ENCRYPT IF YOU ARE SHARING PERSONAL INFO.

$1

●●○○○ Verizon VPN 9:19 AM 78%

igyifrhnvxq33sy5.onion

Browse by category
- Digital Goods 41815
- Fraud Related 5253
  - Accounts 2573
  - CC &CVV 1297
  - Documents &Data 821
- Digital Goods 41815
- Drugs 47435
- Drugs Paraphernalia 293
- Services 4052
- Other 3387

Onion mirrors

Links
- Forum
- Help
- Conferences
- Vendor application
- Earn money

Exchange

BTC	1.0
mBTC	1000.0
USD	6386.2
EUR	5479.9
GBP	4805.9
CAD	8203.5
AUD	8285.7
SEK	53523.0
NOK	51906.4
DKK	40776.6
TRY	24369.5
CNH	42091.8
HKD	49835.0
RUB	371707.7
INR	411497.9
JPY	727397.4

News
- Downtime & Recovery
- Deposit delays
- Forum under maintainance
- Earn money by finding bugs
- Forum Relaunched

Hint: Javascript enabled

Hacked Rdp/Vps Service (2 Week replacment)

Vendor ultimatum2016 (840) (4.82 ★)
(26/1/1) (100~200, 4.97/5)

Price ฿0.00704 ($45)
Ships to Worldwide, Worldwide
Ships from Worldwide
Escrow Yes

Product description

Product Description

Hello everybody!
We are selling [illegible] RDP servers for unlimited amount of time!!

1. Hacked RDP Server
2. Good speed
3. No blacklist / Proxyscore = 0
4. E3 1230v2 /L5520 2Processors
6. Unlimited Bandwidth
7. 1GBPS Network Port
8. DDR3 RAM
9. Windows 7/8/10/2008/2012 R2
10. Set-up time: 1 - 12 Hours
11. Admin access (check options)
12. Whitelisted IP
13. for browsing Mail Cracker/AMS Not Allowed
**14. If your RDP dies I will provide a replacement.

If your RDP dies within 2 weeks of delivery, provide previous info at time of purchase and I will offer you a replacement .

You are NOT allowed to change the password of the RDP at any time

Write in buyer notes from what region/country you would like to get RDP !!!!! or we will send you random

Terms and conditions of ultimatum2016

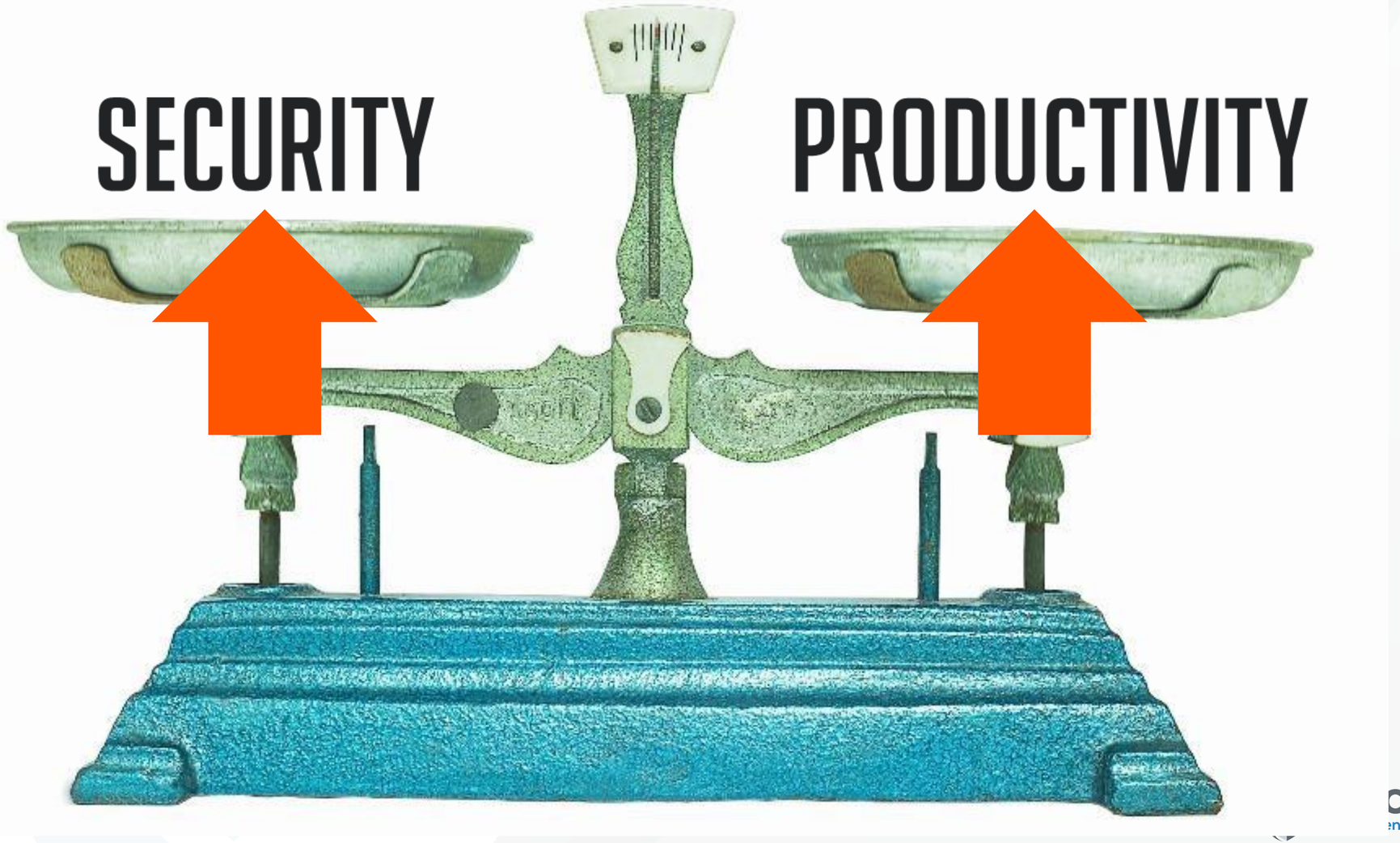
Hello Ladies and Gents!

FOR A FASTER RESPONSE PLEASE DON'T ENCRYPT ALL MESSAGES. ONLY ENCRYPT IF YOU ARE SHARING PERSONAL INFO.

NO AMAZON REFUNDS FOR NOW!!!

$45

Use Automation and Technology to make Least Privilege Productive




Access
Accounts

6 STEPS TO SECURE ACCESS

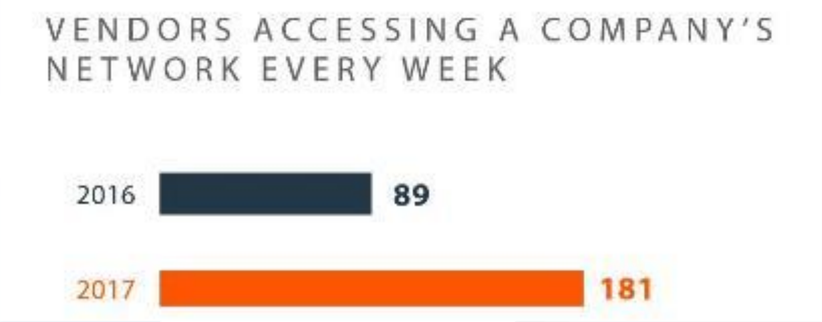
Secure the CONNECTION

Defend the CREDENTIAL

1. SECURE VENDOR ACCESS
2. SECURE INSIDER ACCESS
3. DISCOVER & SAFELY STORE PASSWORDS
4. ROTATE & RANDOMIZE PRIVILEGED CREDENTIALS
5. PROTECT SERVICE ACCOUNTS
6. FORTIFY APP TO APP SECURITY

1. SECURE VENDOR ACCESS

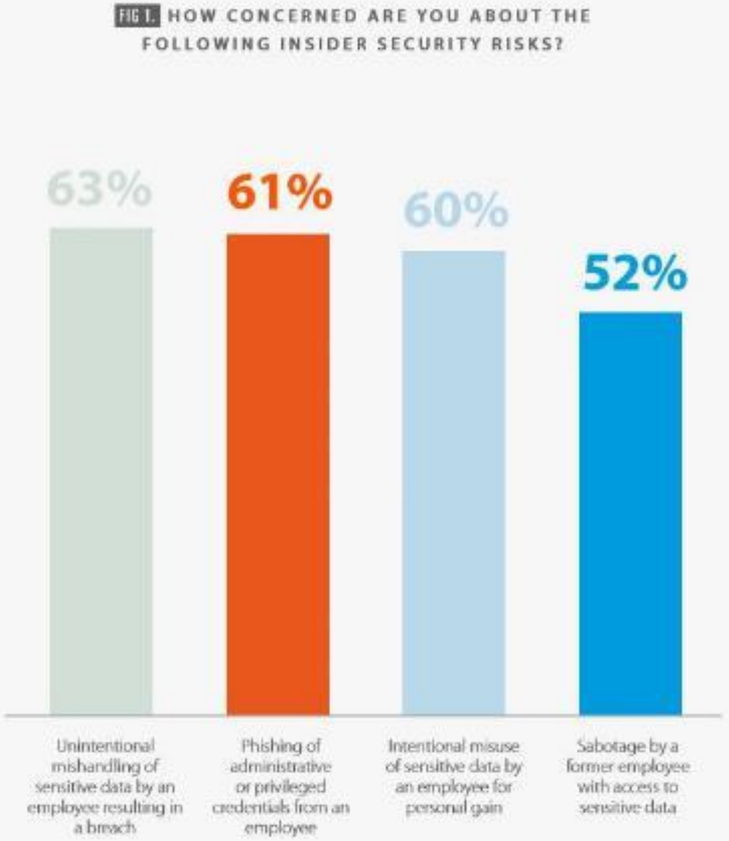
- External vendors are “low hanging fruit” because they have to adhere to your policies.
- Number of third-parties connecting to company networks is rapidly increasing.
- Eliminate VPNs for vendors to improve security and access management.



BOMGAR™ 2017 Secure Access Threat Report

2. SECURE INSIDER ACCESS

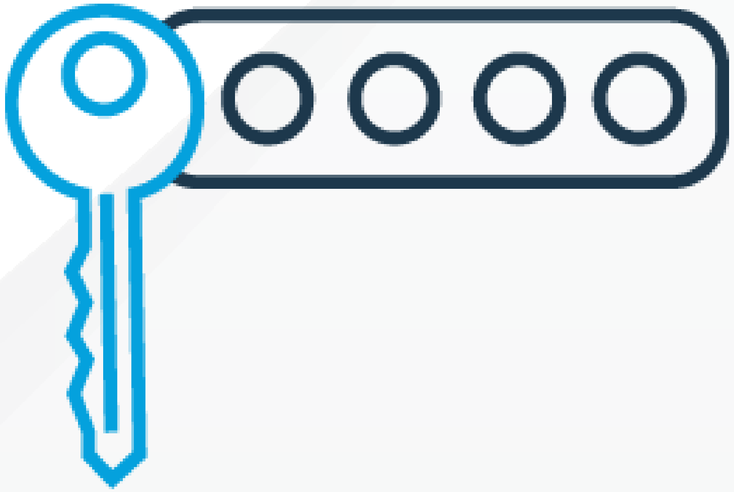
- Any employee who has privileged access:
  - IT Admins
  - IT Operations
  - Operational Technologists
  - Service Desks
- Only 41% of security professionals trust employees with privilege access completely

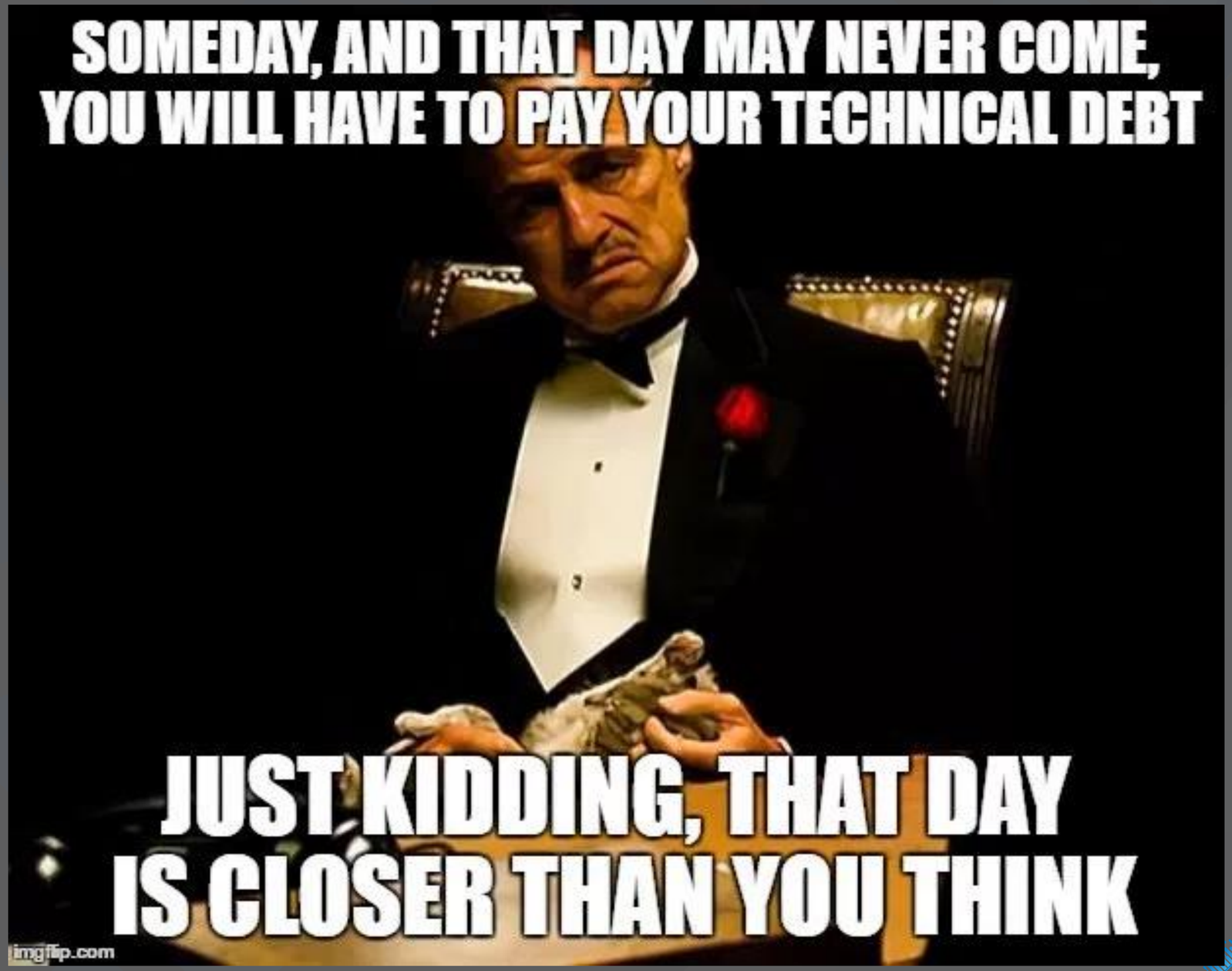


BOMGAR™ 2017 Secure Access Threat Report

3. DISCOVER AND SAFELY STORE PASSWORDS

- Leverage an automated discovery tool to continuously find privileged accounts on your network.
- Secure and manage credentials in an enterprise identity management solution.
- Increase productivity by eliminating check-in/check-out and automatically injecting credentials into a session.
- Eliminating their visibility to the credential reduces threat of being phished or used through another pathway.




SOMEDAY, AND THAT DAY MAY NEVER COME,
YOU WILL HAVE TO PAY YOUR TECHNICAL DEBT
JUST KIDDING, THAT DAY
IS CLOSER THAN YOU THINK
imgflip.com

THE BIRTH OF A NEW SECURITY HOLE

SYSADMIN comments

481

Rant The same old story. Witness the birth of a new security hole. Every time I have to do this, my soul dies a little.

submitted 1 month ago * by lunarhex

I got a rando email asking for some "firewall changes", and of course as the senior network architect, and only cyber security architect, I wasn't involved in the project at all until someone needed something looked at because things don't work. As it turns out we're just swapping in new server hardware for a 3rd party server that's been here for ages, the new server gets the same IP and all. Here's the email chain I just participated in:

> [Coworker Guy],
>
> It looks like the server is up. I can access it through HTTP.
>
> We will need RDP (TCP 3389) enabled from the following IPs: 123.123.123.123 ..... I will also need SNMP (UDP Port 161) and TCP 5666 enabled for the following IP: 123.123.123.123. So we can monitor the server remotely for any hardware issues. Thanks.
>
> Thanks, [3rd Party Guy]

They need this in addition to the SSH and VNC they already have open from anywhere in the world, at least we can lock it down to specific IPs this time

> [Security Guy], Can you accomplish his request for these IP addresses and information listed below regarding Stuff Server?
>
> Thanks, [Coworker Guy]

Yes, I suppose I can do the needfull.

> [Boss Guy],
>
> I know this server has been setup this way for quite a while, but I wouldn't be doing my job if I didn't mention that this is a huge security risk. There are a lot of unsecured inbound services with known exploits being asked for. We have no control over their patching or hardening methods, and response time to remediate a compromise is greatly extended because of that. They're sitting on our corporate VLAN, so any compromise gives an attacker full access to every network we have. If we choose to mitigate this risk, now is the time before it goes live again. I recommend putting it on a DMZ at the very least.
>
> [Boss Guy], if you choose to accept the risk, give me a written OK.
>
> All these ports should be open already. We haven't changed the config from the last server, which was on the same IP.
>
> Thank You, [Security Guy]

"Due to timing of the <Insert Important Event> let's get this up and running and we will circle back about patching and hardening methods.." - Boss Guy

"If security slows down production which in turn reduces profitability, [executive management is] never going to side with IT. It's a matter of risk balancing, and if they've never experienced a security breach, they're going to take the risky route until they do."

- Reddit Commenter

4. ROTATE & RANDOMIZE PRIVILEGED CREDENTIALS

- Ensure every local credential that has some type of admin right has a unique credential – no more shared passwords.
- Stop lateral movement by eliminating common credentials across endpoints.
- If credential is compromised, won't be useful for long, helping to contain losses.

5. PROTECT SERVICE ACCOUNTS

- Manage business uptime, but ensure those credentials can still be rotated.
- Critical business systems often have the same service account for years.
- Ensure critical systems stay productive and don’t have cascading failures while securing them.

6. FORTIFY APP TO APP SECURITY

- Malicious users can compromise hard coded credentials in a script or an application.
- Remove a prime target with app to app credential security.
- Obscure credential through an identity management solution and rotate to remove threat.

6 STEPS TO SECURE ACCESS

Secure the CONNECTION

Defend the CREDENTIAL

1. SECURE VENDOR ACCESS
2. SECURE INSIDER ACCESS
3. DISCOVER & SAFELY STORE PASSWORDS
4. ROTATE & RANDOMIZE PRIVILEGED CREDENTIALS
5. PROTECT SERVICE ACCOUNTS
6. FORTIFY APP TO APP SECURITY

SUMMARY

- You can’t eliminate breaches, but you can contain their impact to acceptable loss.
- By protecting both privileged identities and access pathways you can mitigate the damage done by attackers.
- Using automation will allow you to protect yourself against threats while increasing business productivity and performance.

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