The CTI $hadOw Army: Tales from the Trenches

$mall Business Owner/$olopreneur Edition

By Xena Olsen @ch33r10

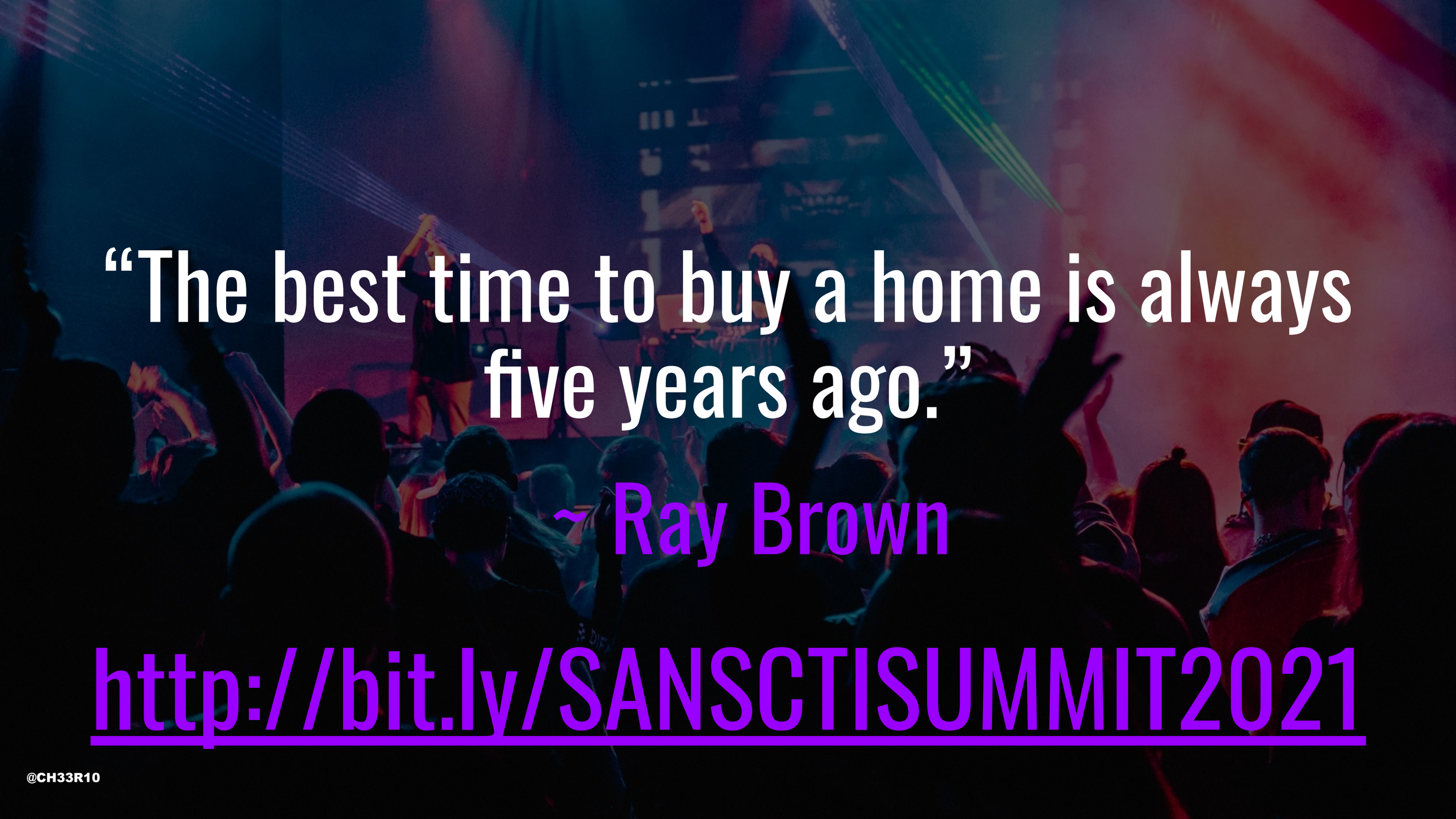
@ch33r10

MARYMOUNT
UNIVERSITY

http://bit.ly/SANSCTISUMMIT2021

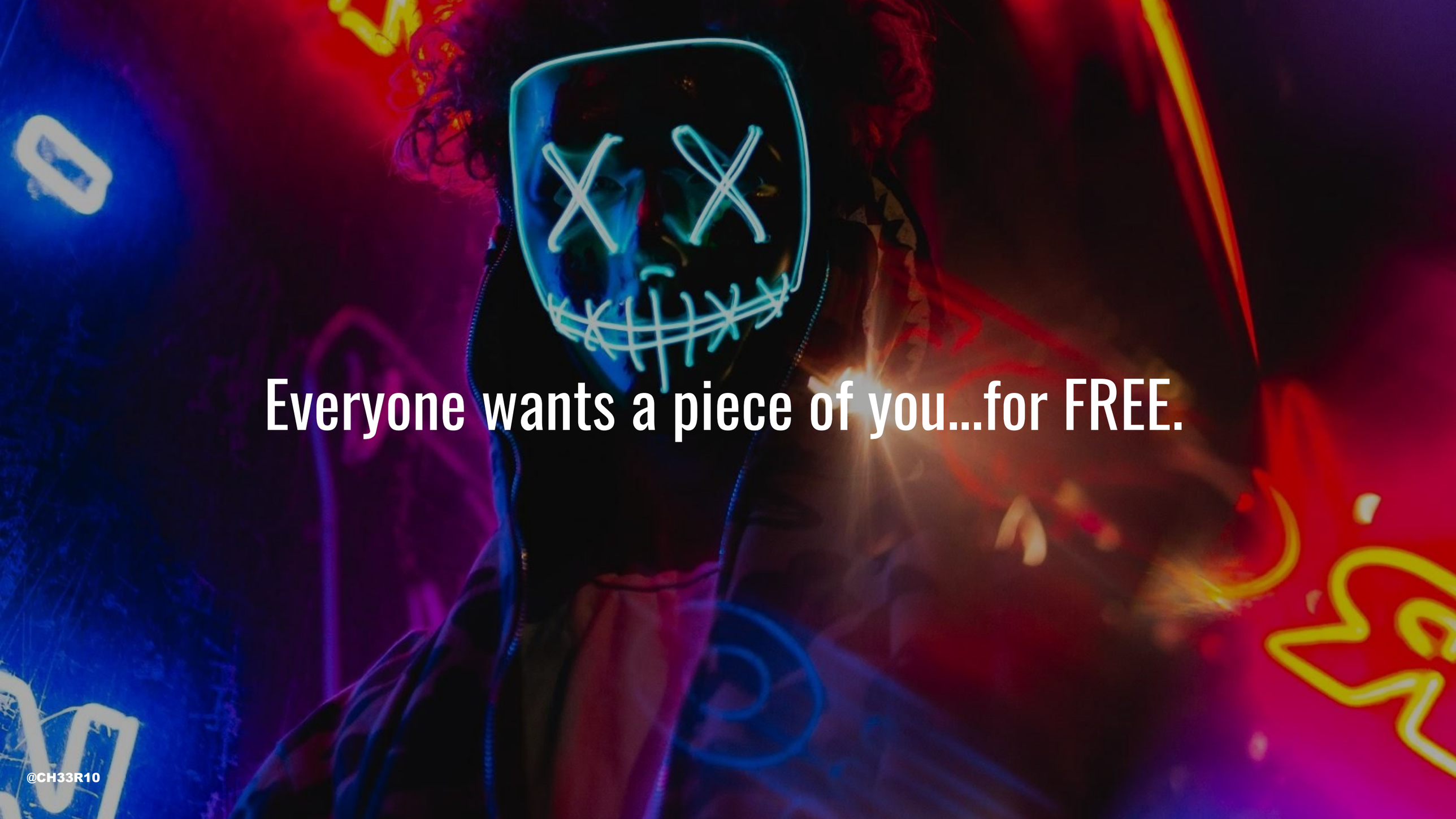
FOR THE LAWY3R$

"The opinions expressed in this presentation are those of the presenter, in their individual capacity, and not necessarily those of my employers."


“The best time to buy a home is always five years ago.”
~ Ray Brown
http://bit.ly/SANSCTISUMMIT2021
@CH33R10

#*%^&, Pay ME.

Who’s got your back?


Everyone wants a piece of you...for FREE.
@CH33R10

How & Where does CTI come in?

1. REAL ESTATE Overview
2. THREAT Landscape
3. HAWT TAKES
4. WIIFM

Sm Biz/$olopreneur

Understand Industry
Understand Threat Landscape
Understand Attackers
Build your own Threat Activity Groups
Operationalize CTI Efforts
Apply CTI skills to your Biz
Marketing yourself if Changing Careers

CTI PRO$

Understand a Different Industry
Understand a Different Threat Landscape
Apply CTI skills to a Different Industry & Get Ideas
Build a Team with Career Changers
Marketing yourself if Changing Careers

OV3RV1EW

$9.6 T G1oba11y

$164.8 B U$A

@CH33R10


REAL E$TATE
@CH33R10

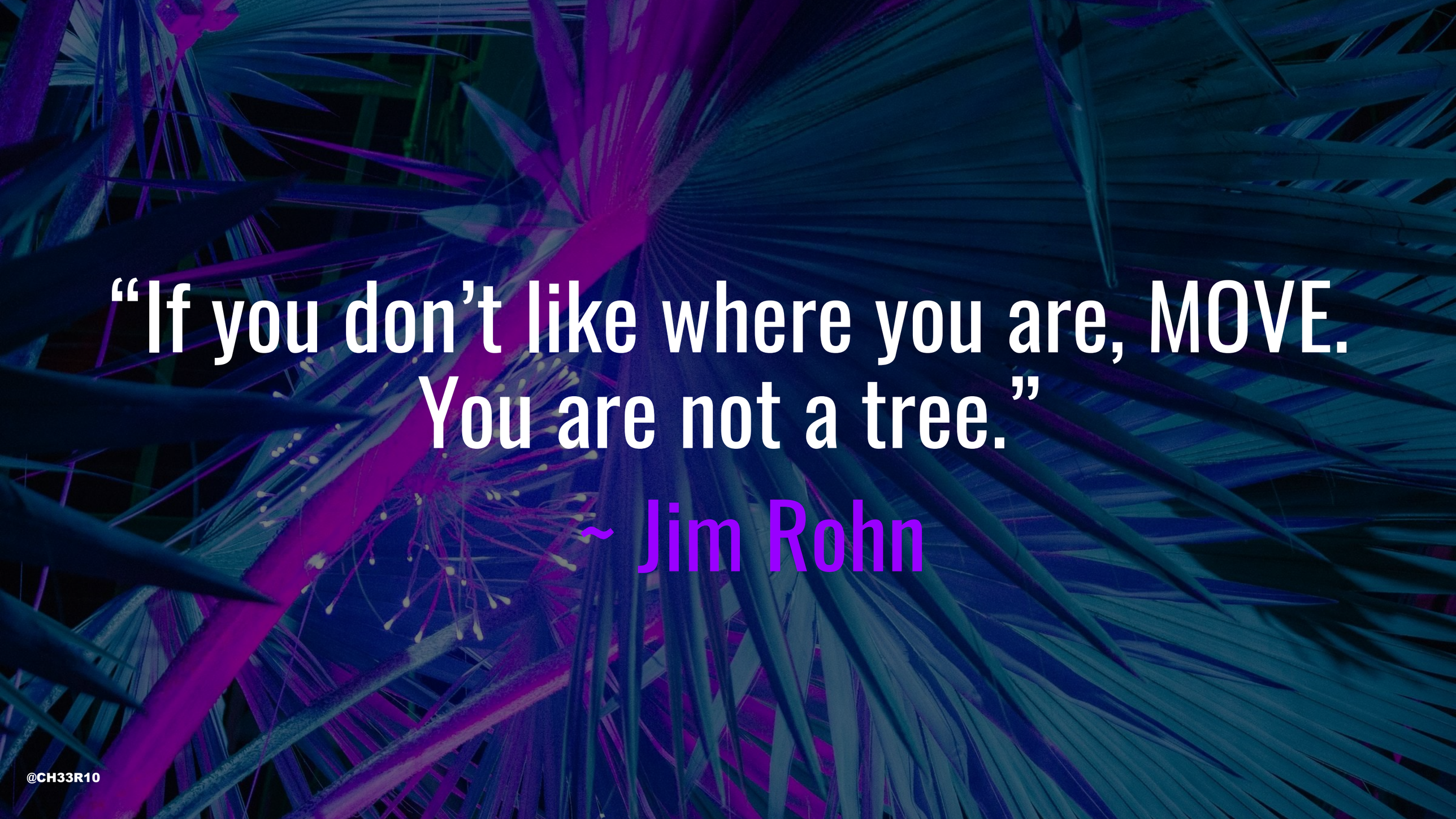

How different is Residential REAL ESTATE $ales to say...
employees or Corporate America???


What does $OLOPRENEUR mean really?

THr3At L4nD$C4pE

Criminals don’t care about your dream$.

@CH33R10


“If you don’t like where you are, MOVE.
You are not a tree.”
~ Jim Rohn

TYPE$ OF THREAT$

PHYSICAL $AFETY
WIRE FRAUD/BEC
ERROR$
PRIVILEGE MI$USE
UNAUTHORIZED ACCE$$
EXTORTION
CYBER!!!

TOP CYBER THREAT$

PHISHING
$OCIAL ENGINEERING
ERROR$

PHYSICAL $AFETY

@CH33R10

@CH33R10

ERROR$

@CH33R10


PRIVILEGE MI$USE
Pioneer


UNAUTHORIZED ACCE$S
@CH33R10


EXTORT1ON
@CH33R10

AKO (Ranzy), Avaddon, Clop, Conti, Darkside, Defray777, DoppelPaymer, Egregor, Everest, ID, Light, LockBit, Maze, MountLocker, Nefilim, Nemty, NetWalker, Pay2Key, Pysa, RagnarLocker, Ragnarok, Sekhmet, Sodinokibi, Suncrypt

RAN$OMWARE BLOG$

KEYWORD: REAL E$TATE

RELATED	
RANSOMWARE	AMT
CONTI	1
MAZE	1
NETWALKER	5
REVIL	3
TOAL	10

REAL ESTATE	
RANSOMWARE	AMT
CLOP	1
CONTI	6
DARKSIDE	1
DOPPELPAYMER	2
EGREGOR	5
NETWALKER	5
REVIL	4
SUNCRYPT	1
TOTAL	25

REAL E$TATE: 25 **RELATED: 10**

CLOP, CONTI, DARKSIDE, DOPPELPAYMER, EGREGOR, MAZE, NETWALKER, REVIL/SODINOKIBI, SUNCRYPT

REAL E$TATE TOP RAN$OMWARE

CONTI | EGREGOR | NETWALKER

RANSOMWARE	INITIAL ENTRY	CYBERSECURITY	SOURCE
CONTI	Phishing email > Link to Google Drive > Payload (PDF or other document) > Downloads Bazar Backdoor	PRE: Antivirus & Security Awareness Training POST: Backups & Procedure	CYBEREASON
EGREGOR	Phishing email/thread hijacking > Attachment > Qbot	PRE: Antivirus & Security Awareness Training POST: Backups & Procedure	SCYTHE SOPHOS
NETWALKER	Exploit Weblogic/Tomcat, RDP, or Phishing	PRE: Antivirus, Security Awareness Training, Patching, Security Best Practices POST: Backups & Procedure	SOPHOS THE DFIR REPORT

@CH33R10

REAL E$TATE CYBER$ECURITY $OLUTION$

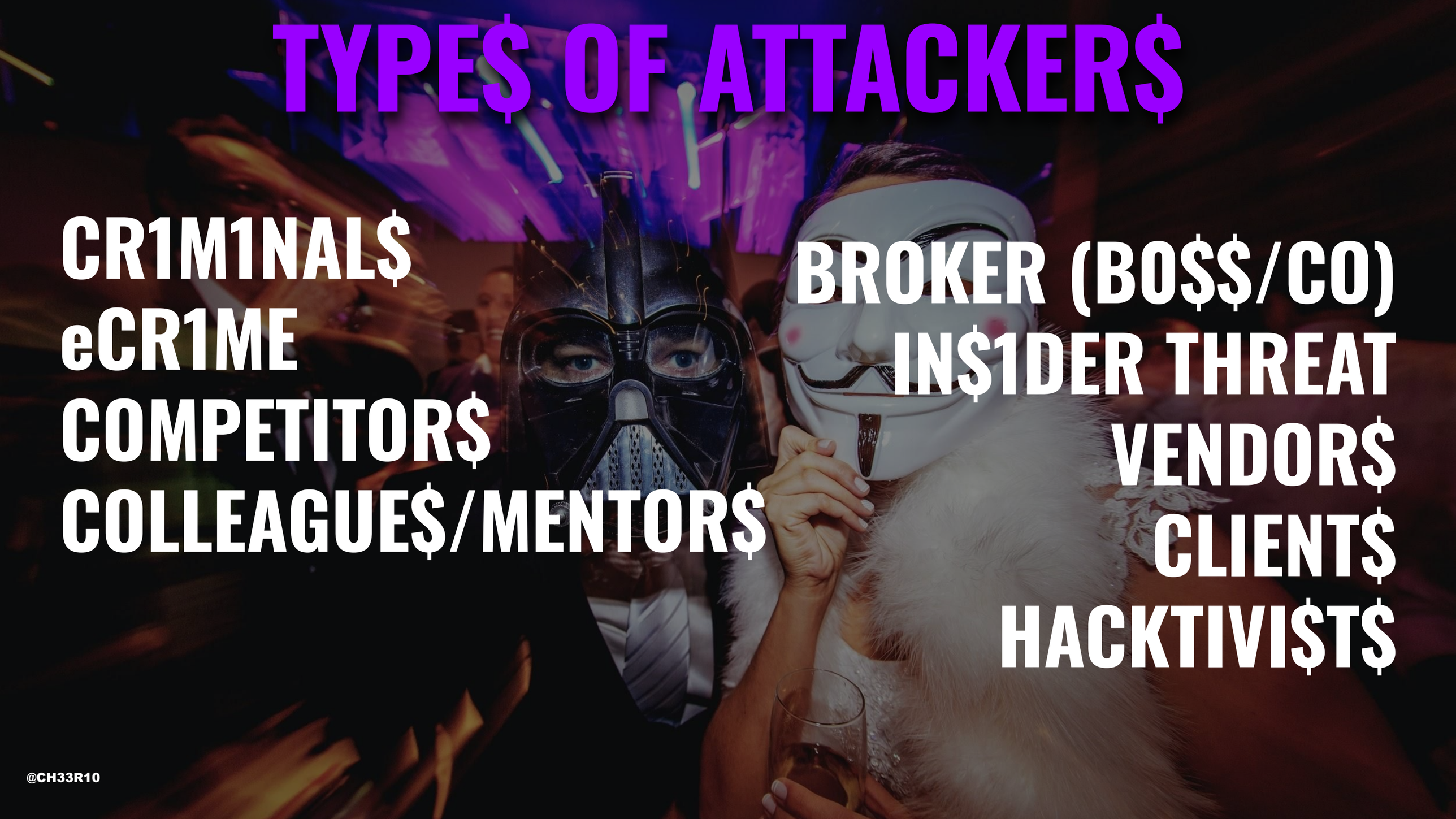
CYBER$ECURITY	THREAT$
2FA / ACCOUNT AUDIT / PASSWORD MANAGEMENT ANTIVIRUS PATCH MANAGEMENT PROCESS / POLICIES / PROCEDURES SECURITY AWARENESS TRAINING SECURITY BEST PRACTICES	BEC, Email Thread Hijacking, Errors, Extortion, Malicious Emails, Malware, Phishing, Privilege Misuse, Ransomware, Social Engineering, Software Compromise, Unauthorized Access, Wire Fraud

Practice DEFEN$E-IN-DEPTH. Implement MORE CYBER$ECURITY $olutions!

@CH33R10


“Find out where the people are going and buy the land before they get there.”
~ William Penn Adair
@CH33R10

TYPE$ OF ATTACKER$



CR1M1NAL$
eCR1ME
COMPETITOR$
COLLEAGUE$/MENTOR$

BROKER (BO$$/CO)
IN$1DER THREAT
VENDOR$
CLIENT$
HACKTIVIT

@CH33R10

THr3At AcT1v1TY GRoUp$

APT41

INITIAL ENTRY	CYBERSECURITY
Exploit public facing application	Patch Management
Phishing - link or attachment	Security Awareness Training & Antivirus
Vendor compromise	Security Awareness Training & Antivirus
Vendor software compromise	Antivirus

FIN6

INITIAL ENTRY	CYBERSECURITY
Compromised credentials	2FA/Account Audit/Password Management
Purchase entry via Trickbot infection	Security Awareness Training & Antivirus
Phishing - link, attachment, service like LinkedIn	Security Awareness Training & Antivirus

SOURCE: SCYTHE, MITRE ATT&CK, CTID (THE CENTER FOR THREAT-INFORMED DEFENSE)


SA1Nt JHN
@CH33R10

AQU4DROP

@CH33R10


M3DUZA
@CH33R10

H4Wt T4k3$


PEOPLE
PROCESS
TECHNOLOGY

peOPL3

PrOc3$s

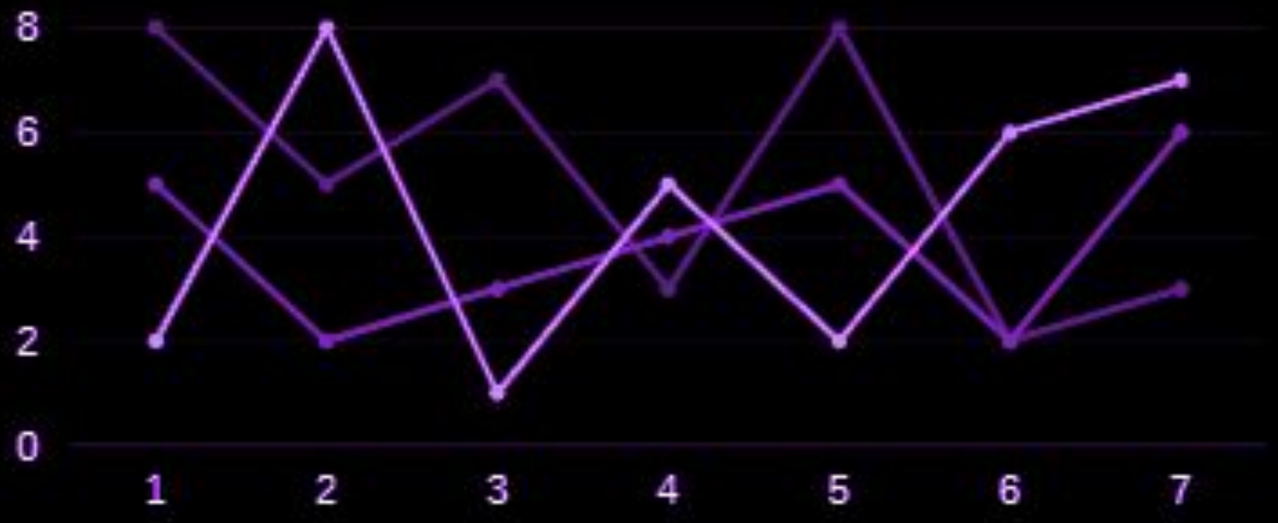
@CH33R10

KP💔P R3VOLUTION

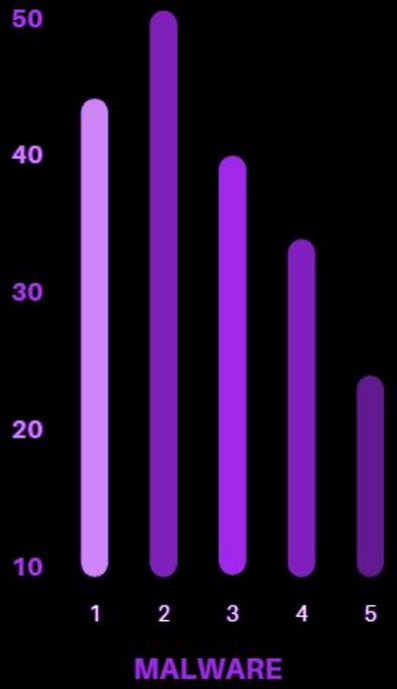
KP💔P THREAT LANDSCAPE REPORT Q3

OCTOBER 2020

TABLE OF CONTENTS

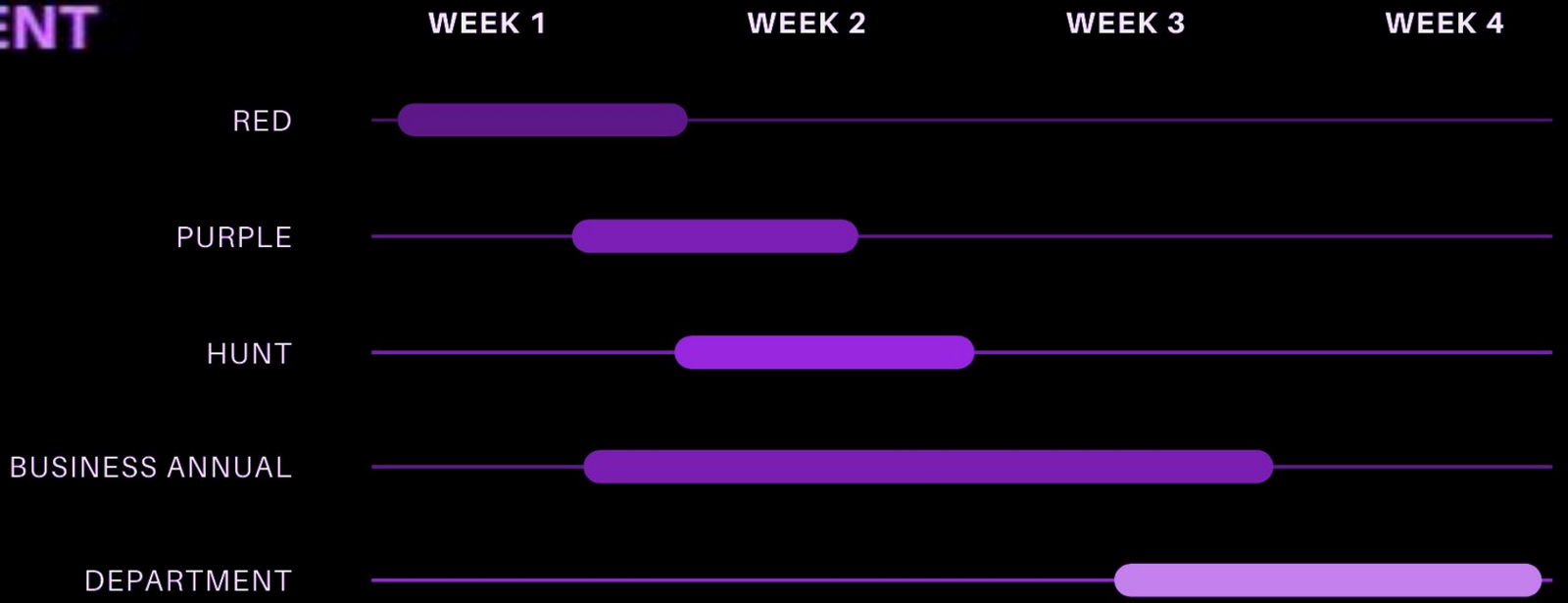


FINANCE DEPARTMENT



CTI INTELLIGENCE PRODUCTS

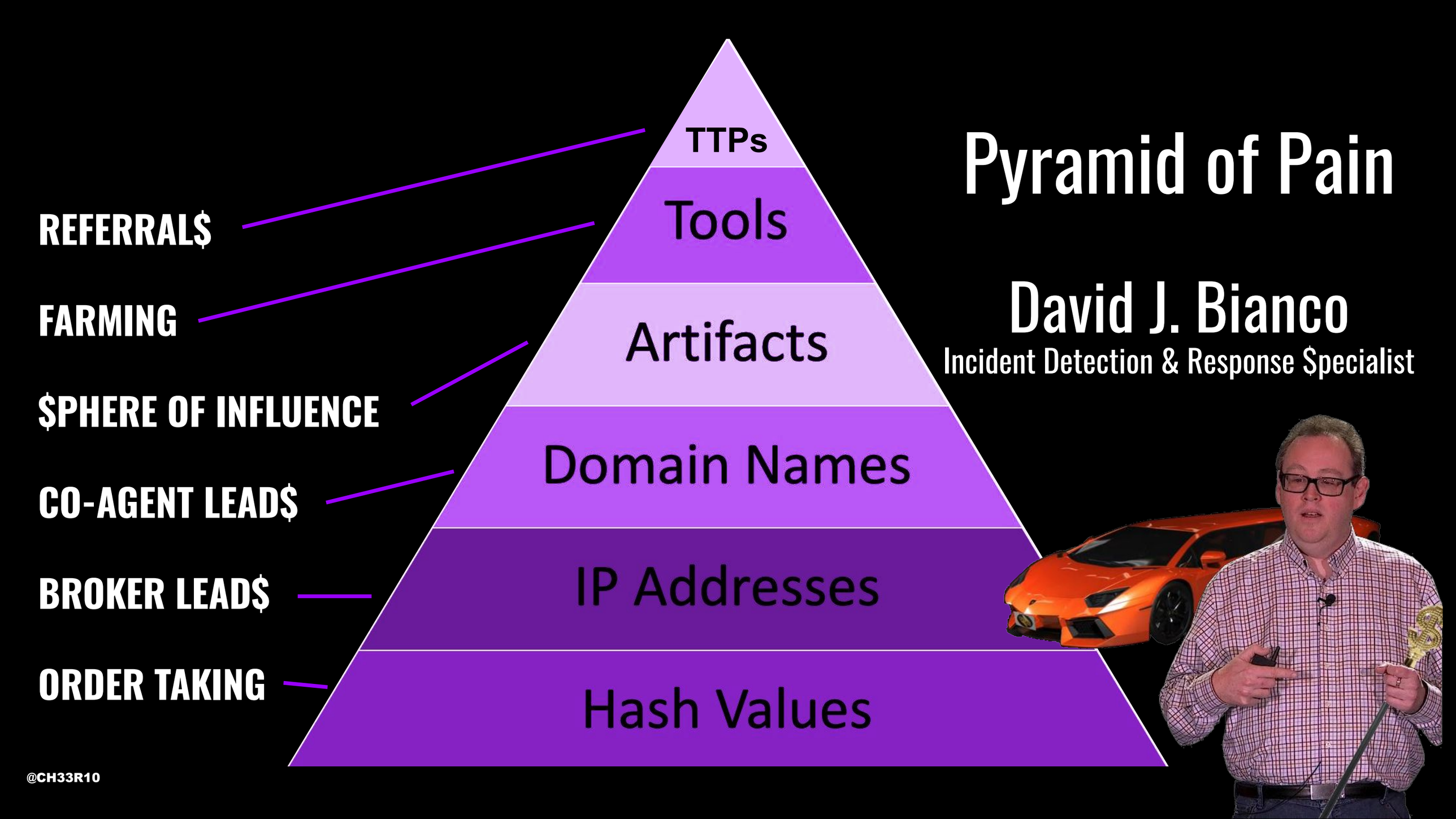
Target: December 31, 2020



@CH33R10

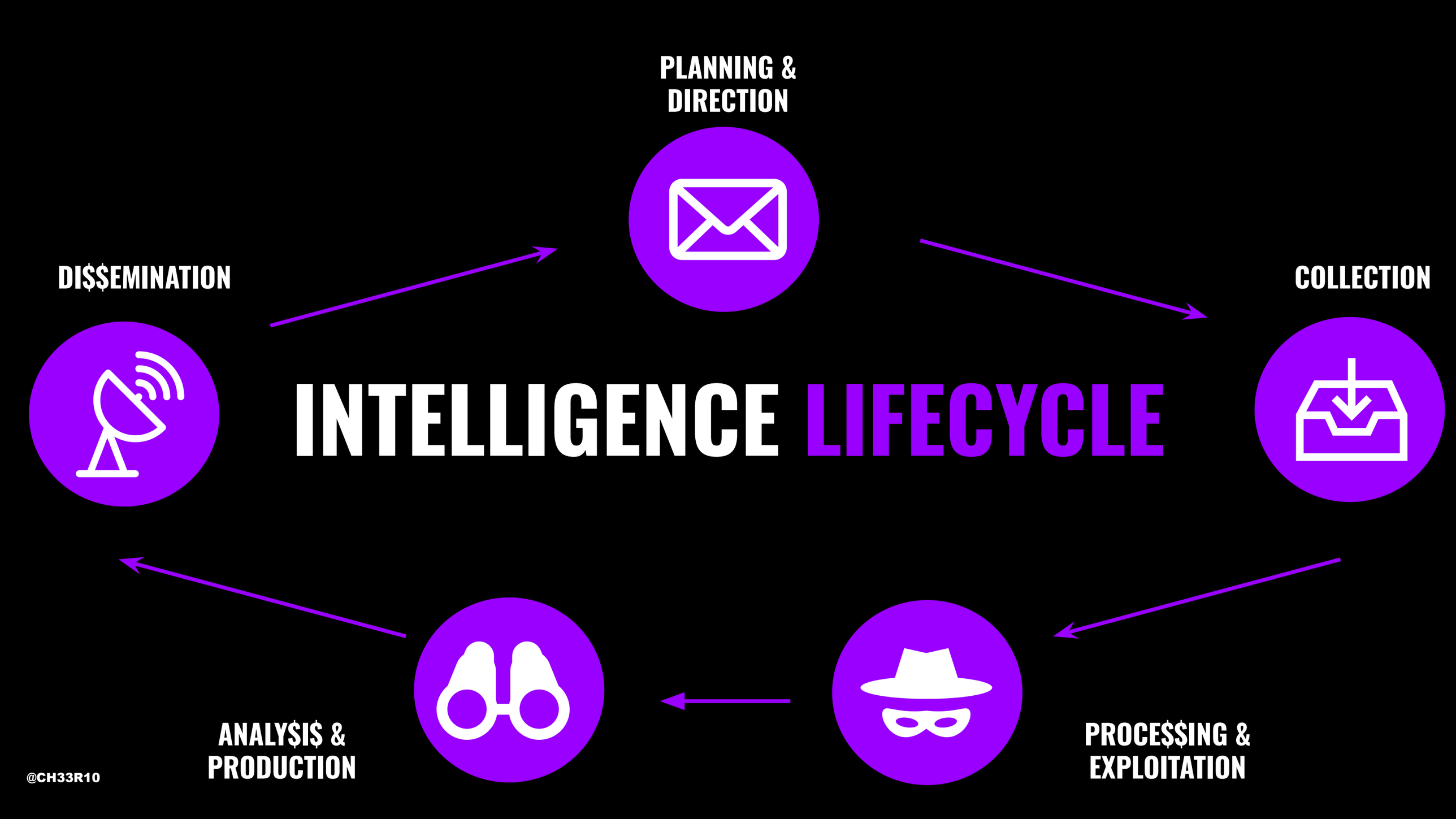
Pyramid of Pain

David J. Bianco
Incident Detection & Response $pecialist



@CH33R10

INTELLIGENCE LIFECYCLE

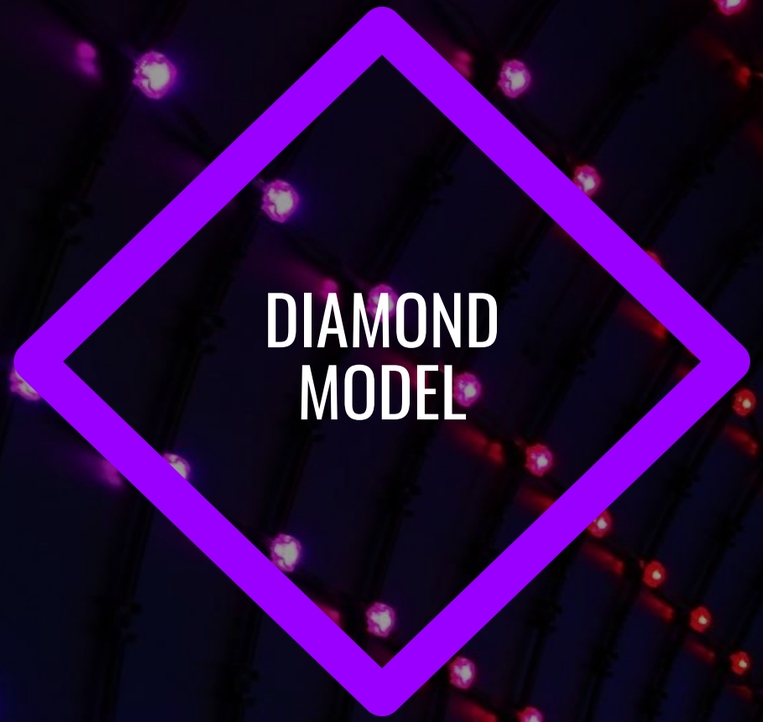


@CH33R10

MATRIX W HYPOTHEE

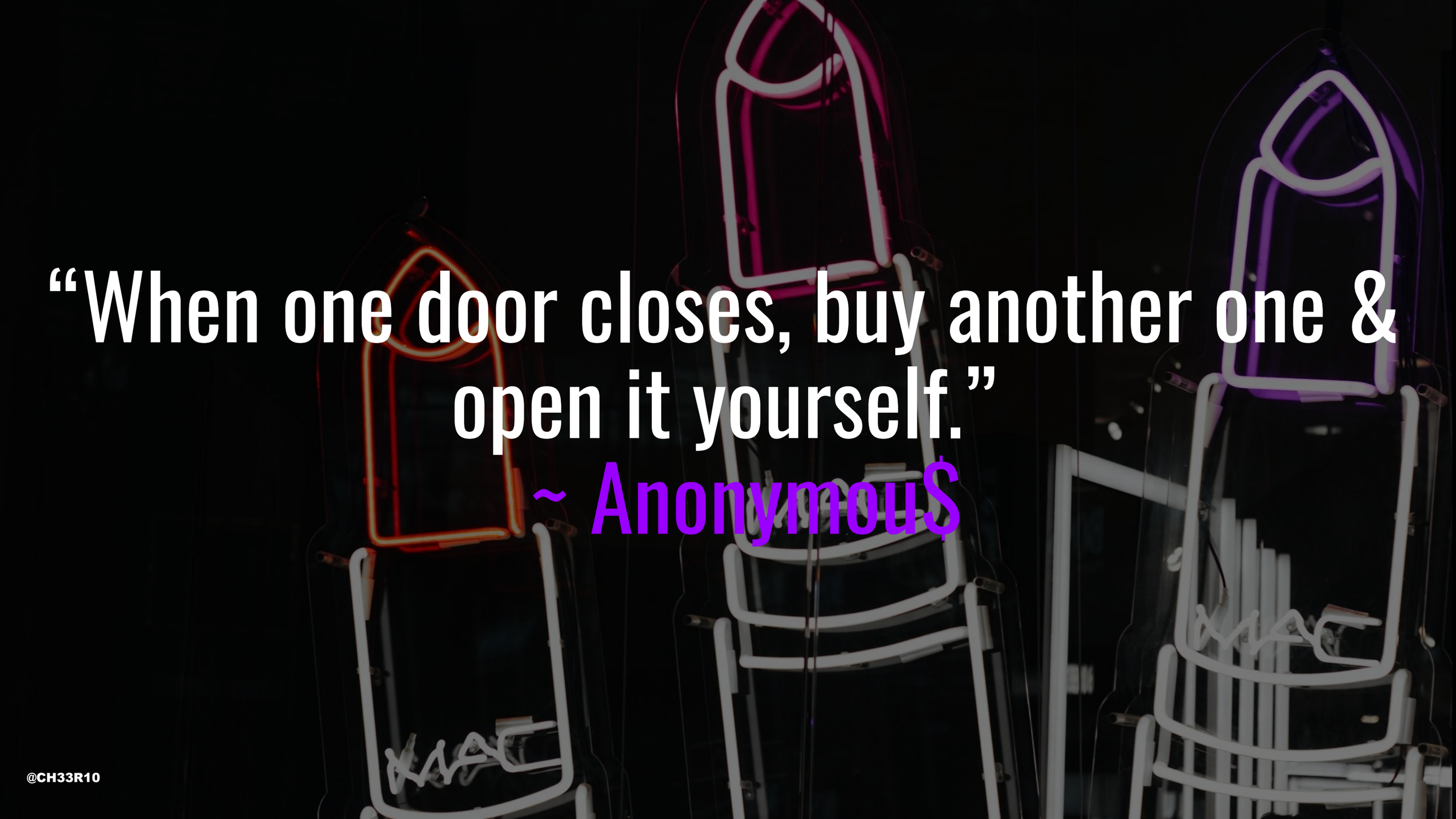
	H1	H2	H3	H4 +
EVIDENCE	CONSISTENT	INCONSISTENT	NEUTRAL	
EVIDENCE	CONSISTENT	INCONSISTENT	NEUTRAL	
EVIDENCE	CONSISTENT	INCONSISTENT	NEUTRAL	
EVIDENCE	CONSISTENT	INCONSISTENT	NEUTRAL	

The Diamond Model ... of REAL E$TATE



Sergio Caltagirone, Andrew Pendergast & Christopher Betz

T3cHN0LogY


“When one door closes, buy another one & open it yourself.”
~ Anonymou$

w1iFM

@CH33R10

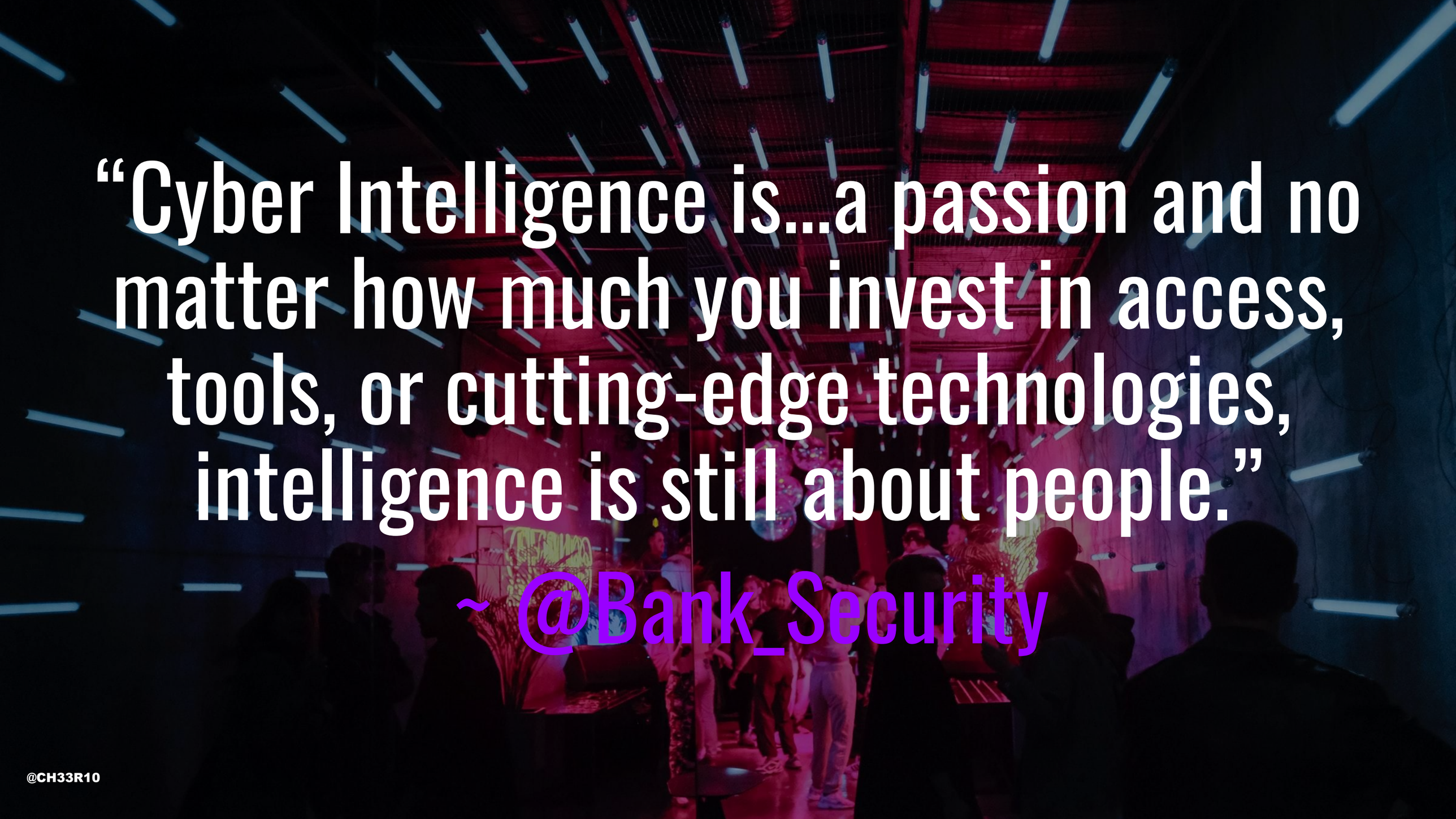
@CH33R10

Take what you can use & ignore the rest.

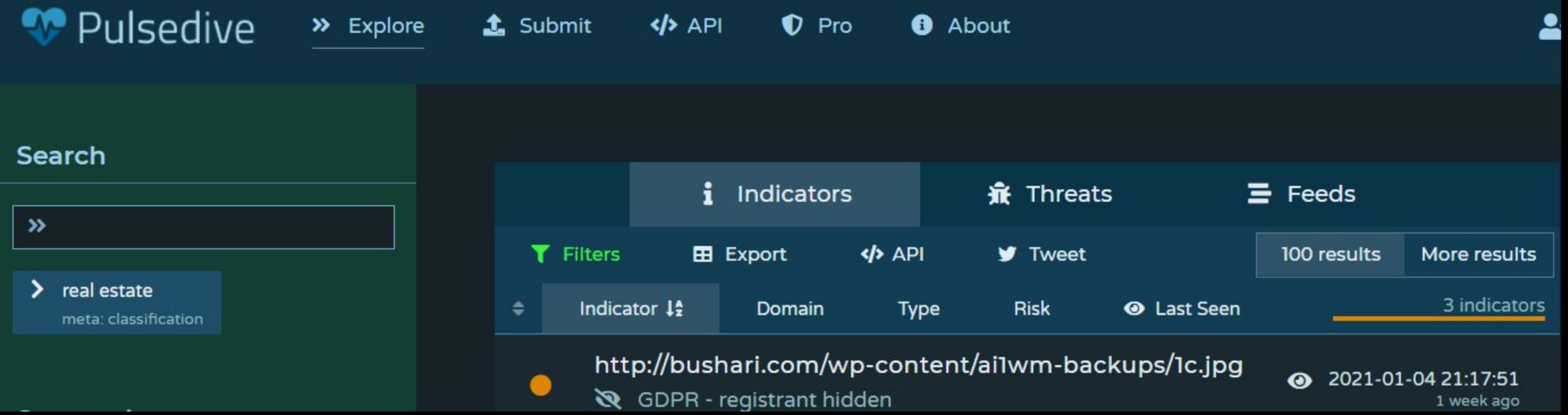
Give career-changers ?’s that make them $HINE.

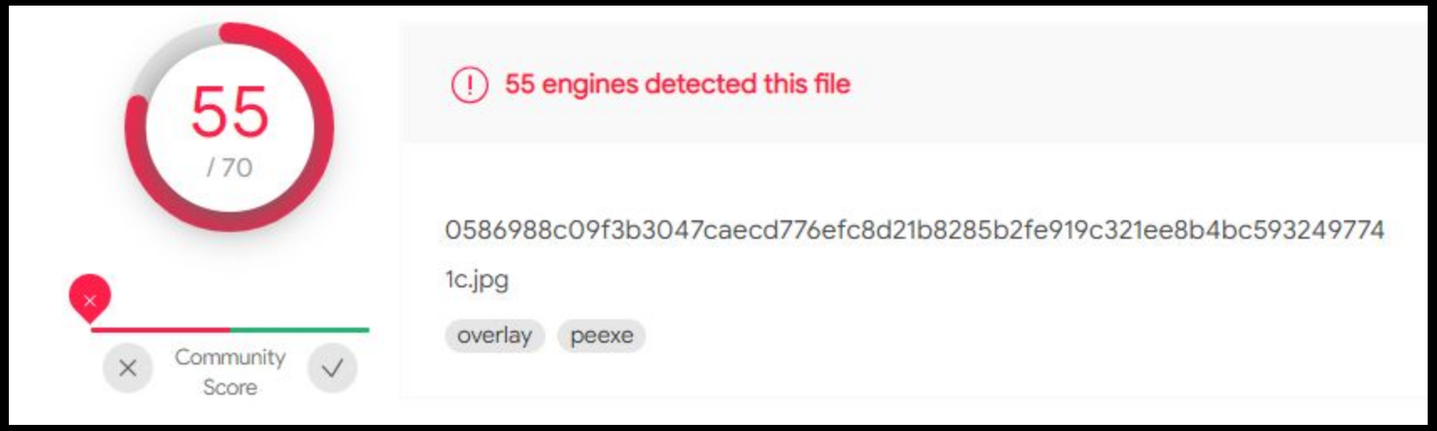
$m Biz/$olopreneurs $IMPLE & EA$Y solutions to [hopefully] NOT get $ued & still make $$$

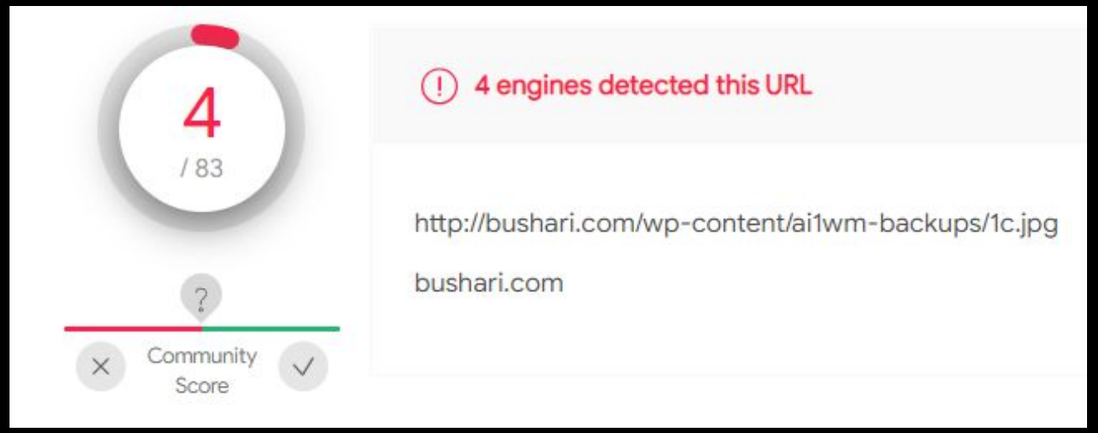
@CH33R10


“Cyber Intelligence is....a passion and no matter how much you invest in access, tools, or cutting-edge technologies, intelligence is still about people.”
~ @Bank_Security


AFTER PARTY







$HADE RAN$OMWARE

@CH33R10

From: "support@apple.com" <jmmotzgq@tlpknsjd.zgzxi>
Date: April 10, 2017 at 5:58:25 PM CDT

bit.ly/xyz+

Security Notice

We regret to inform you that your Apple ID has been locked for security reasons
The reason we have took this action is as follows :

On Thursday, 01 April 2017 19:35 GMT, we noticed an attempt to sign in to your account form an unrecognised device in United Kingdom

In order to safeguard your information we require you to unlock your Apple ID
By clicking the link below

Unlock Apple ID

Please Note: Failure to unlock your Apple ID can lead to permenant suspension

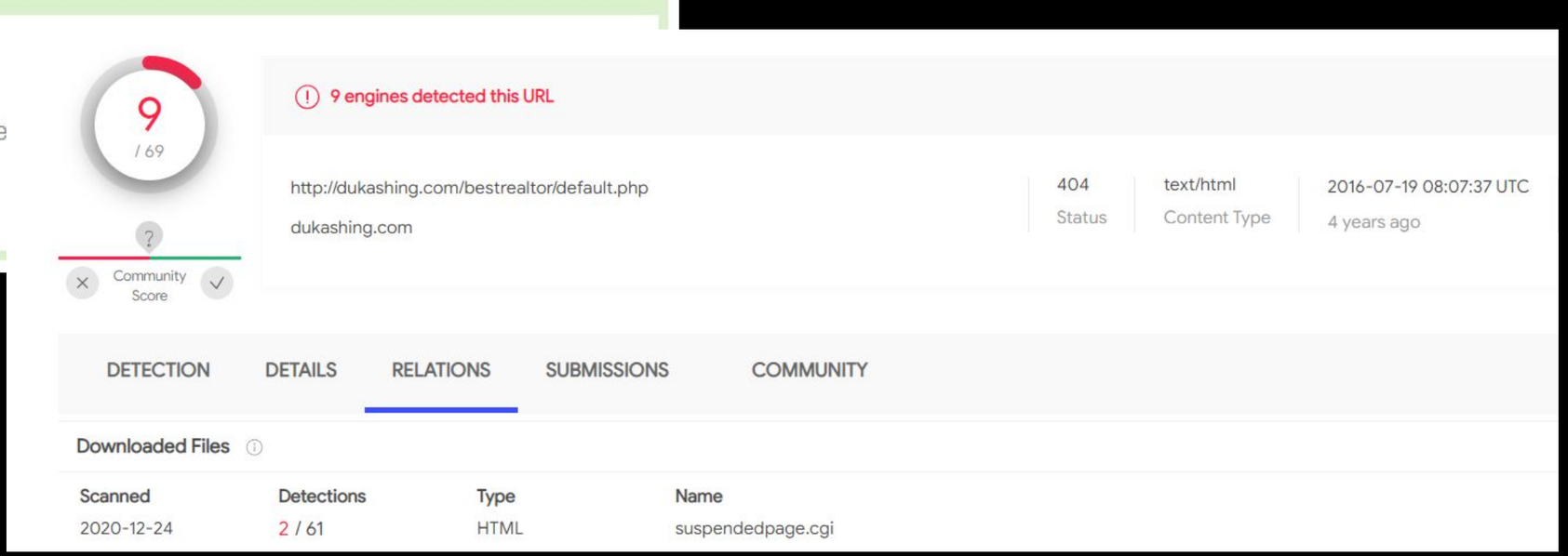
Apple Team

From: Caleb [redacted]
Date: April 21, 2016 at 5:03:19 PM CDT
To: Caleb [redacted]
Subject: Purchase Offer

You have a pending incoming docs shared with you via Google docs

Click to open: **eStatement**

Google Docs makes it easy to create, store and share



FIE$TA EXPLOIT KIT

Malwarebytes LABS

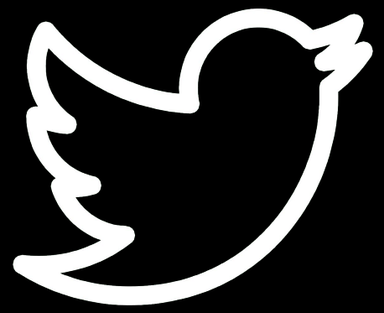
- Flash exploit (VT): CVE-2015-0311
- Silverlight exploit (VT): CVE-2013-0074
- PDF exploit (VT): CVE-2010-0188
- Java exploit (VT): CVE-2013-2465

@CH33R10


$15.9M
@CH33R10


THANK YOU
@CH33R10

Xena Olsen



@ch33r10

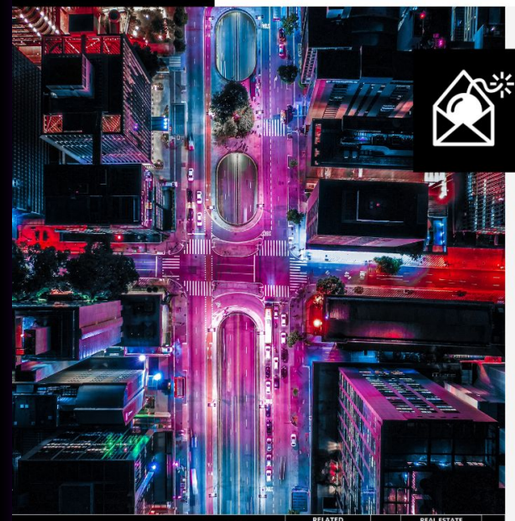
/in/xena-olsen

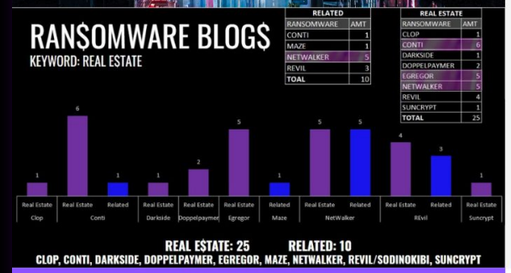
http://bit.ly/SANSCTISUMMIT2021

CYBER SECURITY

REAL ESTATE

THREAT LANDSCAPE





TOP THREAT VECTOR

EMAIL

Threat Summary

Types of Threats: Physical Safety, Wire Fraud, Business Email Compromise (BEC), Errors, Privilege Misuse, Unauthorized Access, Extortion, Cyber-related.

Cybersecurity Solutions: Antivirus, Security Awareness Training, Patch Management, Security Best Practices, 2FA, Account Audit, Password Management, Processes/ Policies/Procedures.

Reminder: It is cheaper to slow down when going through email than dealing with a cybersecurity incident.

TYPES OF ATTACKERS

- Criminals
- eCrime
- Competitors
- Colleagues/ Mentors
- Broker
- Insider Threat
- Vendors
- Clients
- Hacktivists

TOP CYBER THREATS

PHISHING
SOCIAL ENGINEERING
ERRORS

FOR MORE RESOURCES
@ch33r10
bit.ly/SANSCTISUMMIT2021

$pecial Thanks

SANS Institute
Jared Peck
Gert-Jan Bruggink
Ben Goerz
Jason Kichen
Joe Slowik
Cory Kennedy
Ryan Kovar
Katie Nickels
$ecret $quirrel$
FUZZYSNUGGLYDUCK


CALL FOR PRESENTATIONS IS NOW OPEN
PURPLE TEAM
SUMMIT & TRAINING
sansurl.com/purple-team-cfp
Live Online
FREE SUMMIT: May 24–25 | TRAINING: May 17–22
SANS
@CH33R10