

# The CTI Shadow Army: Tales from the Trenches

A wide-angle photograph of a coastal pier at sunset. The sky is a gradient of orange, yellow, and purple. In the foreground, the ocean waves are visible. On the left, a wooden pier extends into the water, featuring a restaurant with a flag flying from its top. To the right, a large amusement park structure is illuminated, with a prominent ferris wheel and a roller coaster track. The overall atmosphere is festive and scenic.

Small Business Owner/Solopreneur Edition

By Xena Olsen [@ch33r10](https://twitter.com/ch33r10)

# @ch33r10



MARYMOUNT  
UNIVERSITY

<http://bit.ly/SANSCTISUMMIT2021>

# FOR THE LAWY3RS

“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>

A photograph of a bar counter at night. The scene is dimly lit with blue and purple neon lights reflecting off the surfaces. On the counter, there are several bottles of alcohol, glasses, and some coins scattered around. In the background, there are shelves filled with more bottles and a large window with a grid pattern. The overall mood is mysterious and moody.

DANCE  
AGAIN

#\*%& Pay ME.

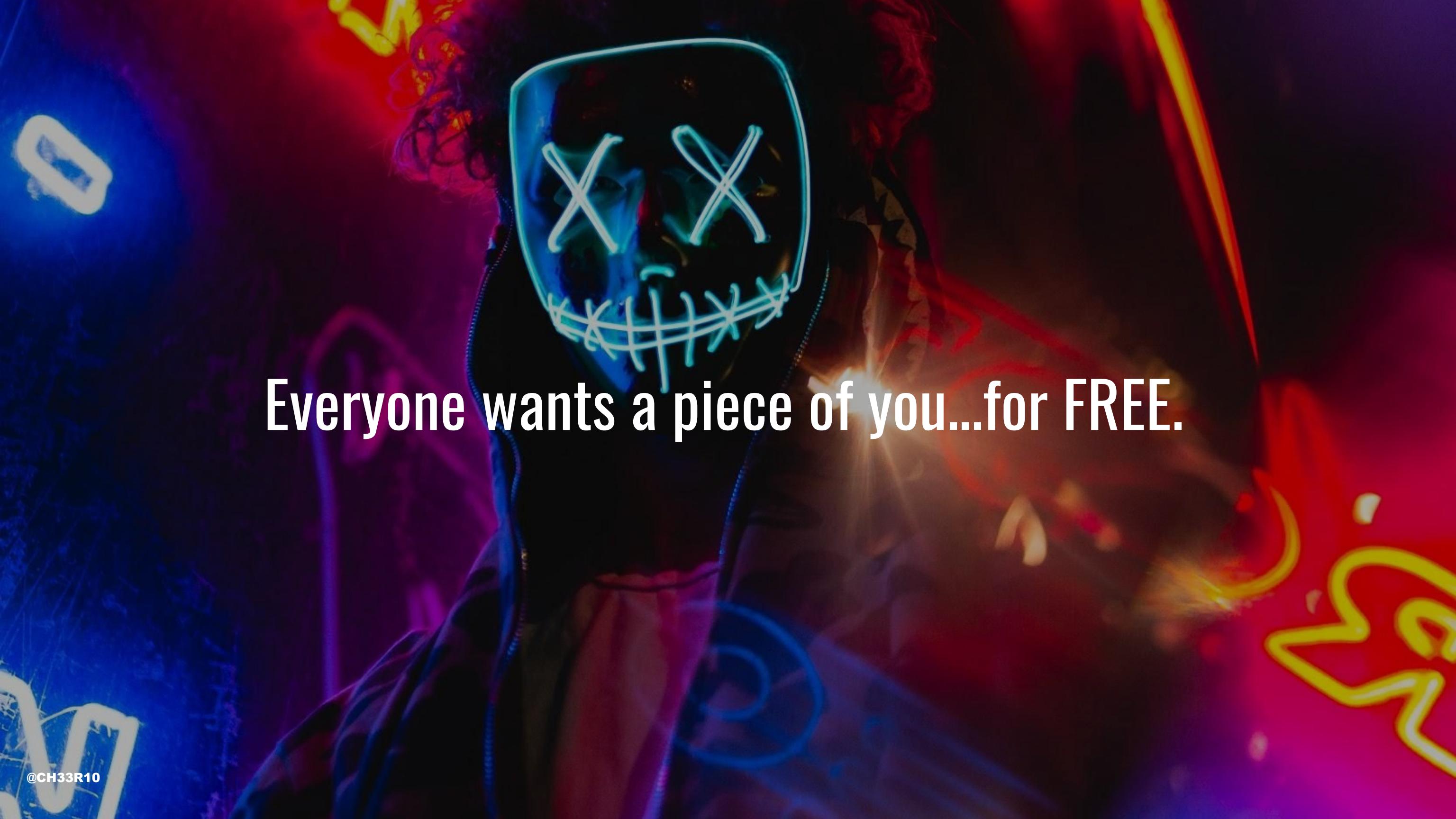
<<REW

--:--



Who's got your back?

プログレス



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



How & Where does CTI come in?

1. REAL ESTATE Overview

2. THREAT Landscape

3. HAWT TAKES

4. WIIFM

# Sm Biz/Solopreneur

**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 Globally

\$164.8 B USA



# REAL ESTATE



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



What does \$OLOPRENEUR mean really?

THr3At L4nD\$C4pE

1NF:rM@7iON 1S P0vvErr

Criminals don't care about your dream\$.



Iniciando Protocolo sombra v1.9...

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

~ Jim Rohn

# **TYPES\$ OF THREAT\$**

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

**TOP CYBER THREAT\$  
PHISHING  
\$OCIAL ENGINEERING  
ERROR\$**

# PHYSICAL SAFETY



# WIRE FRAUD / BEC

A photograph of a DJ booth at a concert. The background features a large screen displaying a Shell logo and two stylized green lions. The DJ is visible behind the turntables. The scene is lit with red and blue stage lights, creating a vibrant atmosphere.

# ERROR\$

The background of the image is a blurred photograph of a DJ's workspace. It features a prominent Pioneer DJ turntable on the right side, with its brand name visible in white. To the left of the turntable, there's a large, multi-colored DJ mixer with numerous knobs and buttons. A microphone stand with a microphone is positioned on the far left. The scene is bathed in low-key, colorful lighting, primarily in shades of blue, purple, and red, creating a moody and professional atmosphere.

PRIVILEGE MISUSE

# UNAUTHORIZED ACCESS

# EXTORTION



**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**

# RANSOMWARE BLOGS

KEYWORD: REAL ESTATE



RELATED	
RANSOMWARE	AMT
CONTI	1
MAZE	1
NETWALKER	5
REVIL	3
<b>TOAL</b>	<b>10</b>

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

REAL ESTATE: 25

RELATED: 10

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

# REAL ESTATE TOP RANSOMWARE

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/Tomecat, RDP, or Phishing	PRE: Antivirus, Security Awareness Training, Patching, Security Best Practices POST: Backups & Procedure	SOPHOS THE DFIR REPORT

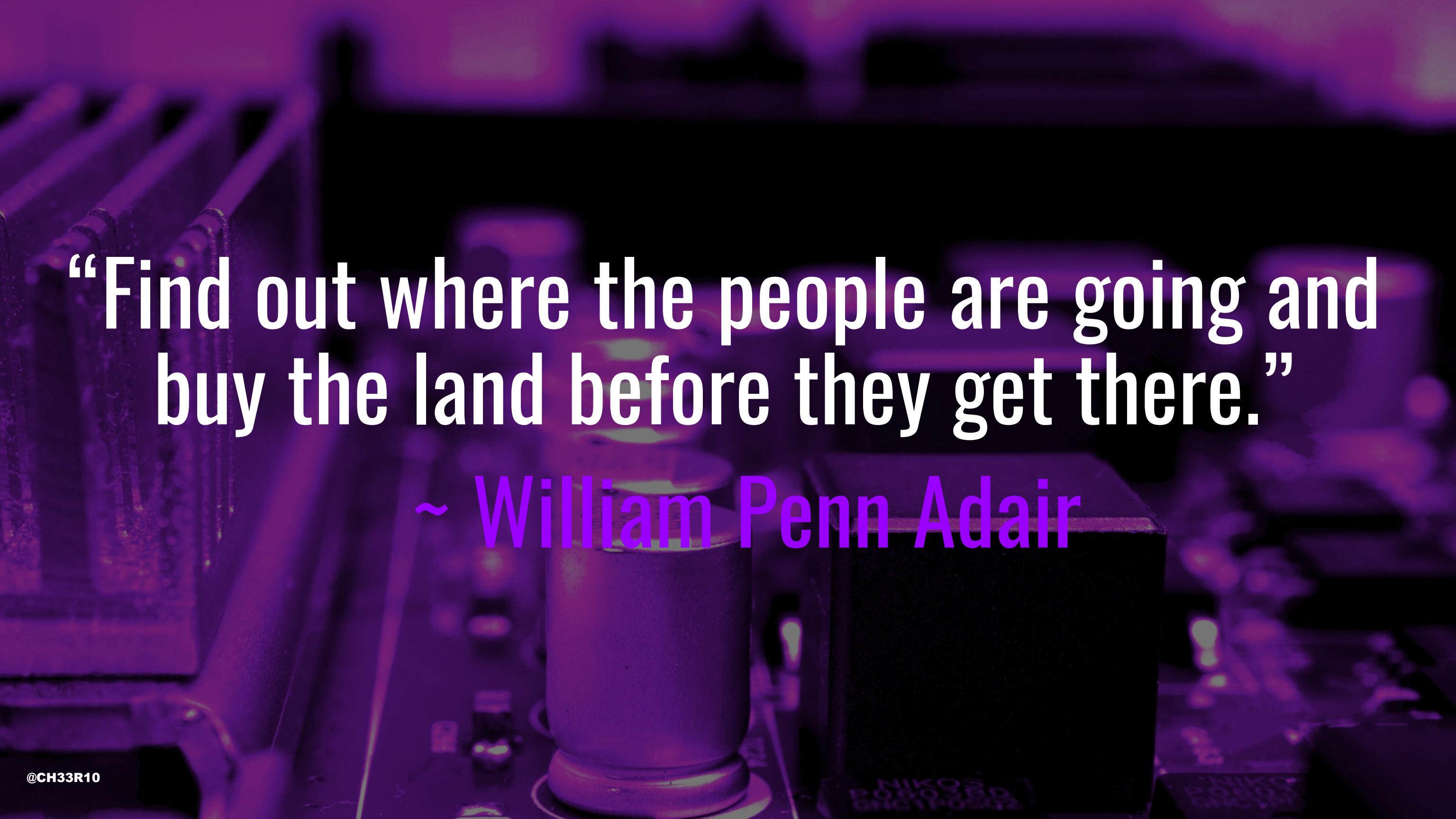


CYBER CYBER CYBER

# REAL ESTATE CYBER\$ECURITY SOLUTION\$

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

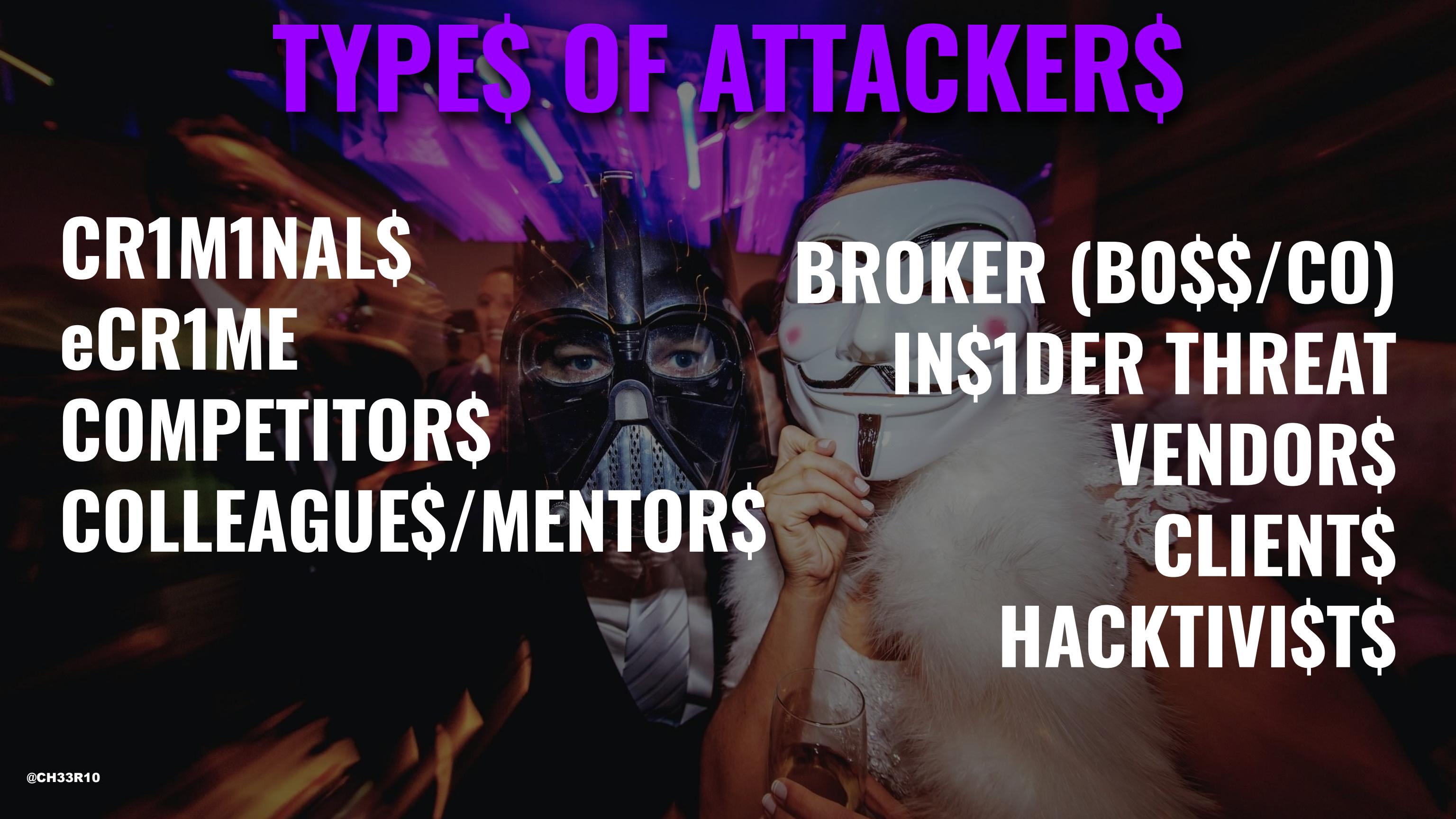
Practice DEFENSE-IN-DEPTH. Implement MORE CYBER\$ECURITY \$olutions!



“Find out where the people are going and buy the land before they get there.”

~ William Penn Adair

# TYPE\$ OF ATTACKER\$

A woman with long dark hair, wearing a white fur-trimmed coat, holds a clear cocktail glass filled with a light-colored liquid. She is wearing a black mask with glowing blue eyes. The background is dark and out of focus.

CR1M1NAL\$

eCR1ME

COMPETITOR\$

COLLEAGUE\$/MENTOR\$

BROKER (BO\$\$/CO)

IN\$1DER THREAT

VENDOR\$

CLIENT\$

HACKTIVI\$T\$

# THr3At AcT1v1TY GRouP\$

# APT41

## INITIAL ENTRY

Exploit public facing application

Phishing - link or attachment

Vendor compromise

Vendor software compromise

## CYBERSECURITY

Patch Management

Security Awareness Training & Antivirus

Security Awareness Training & Antivirus

Antivirus

# FIN6

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

@CH33R10

## INITIAL ENTRY

Compromised credentials

Purchase entry via Trickbot infection

Phishing - link, attachment, service like LinkedIn

## CYBERSECURITY

2FA/Account Audit/Password Management

Security Awareness Training & Antivirus

Security Awareness Training & Antivirus

A photograph of a DJ, identified as SAINT JHN, performing at a club. He is wearing a dark purple long-sleeved shirt and black headphones. He is leaning over a turntable, his hands positioned on the vinyl records and the turntable's surface. The background is dark, typical of a nightclub environment.

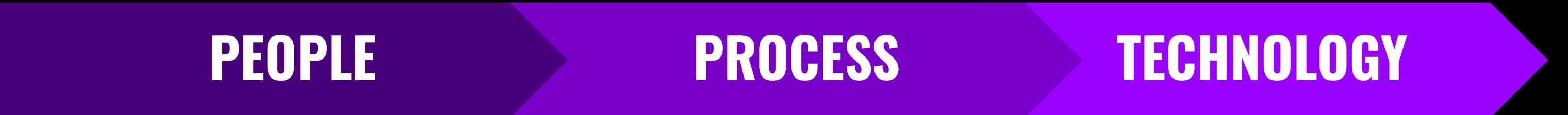
SA1NT JHN



# AQU4DROP

# M3DUZA

H4Wt T4k3\$



PEOPLE

PROCESS

TECHNOLOGY

pe0PL3

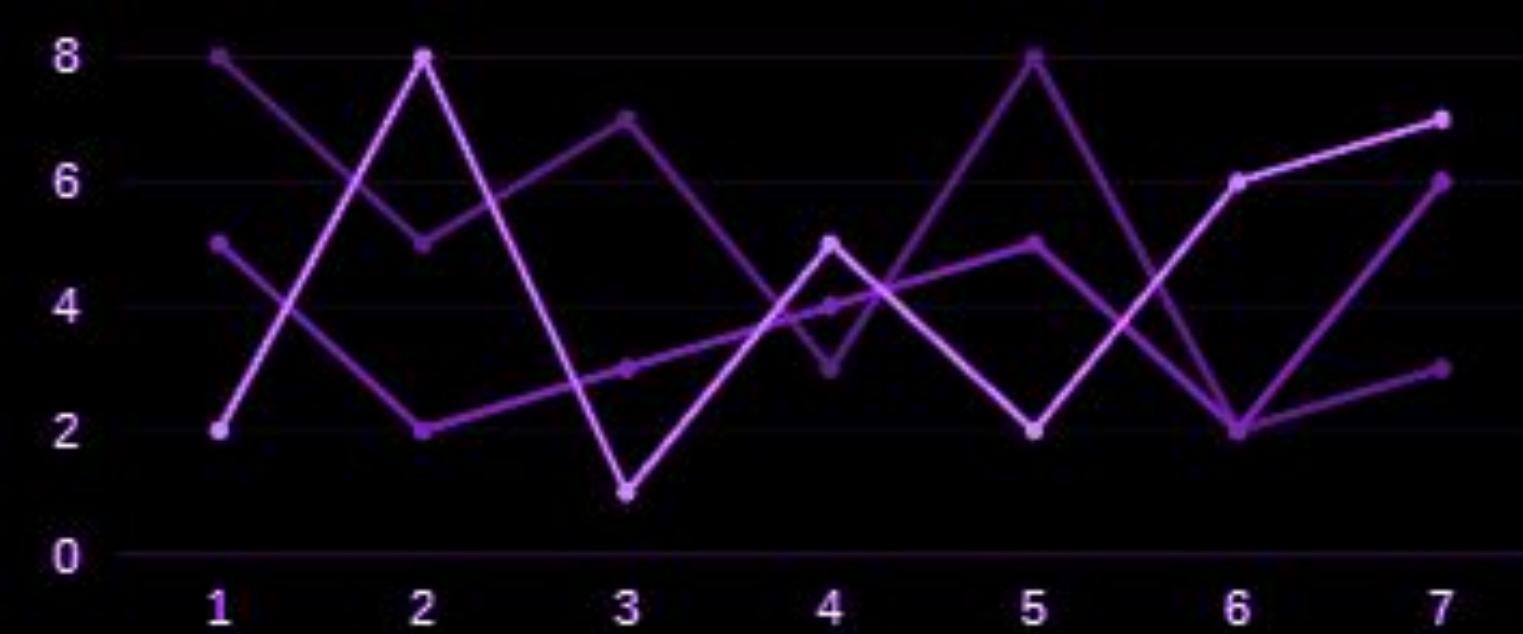
Pr0c3\$

OCTOBER 2020



## TABLE OF CONTENTS

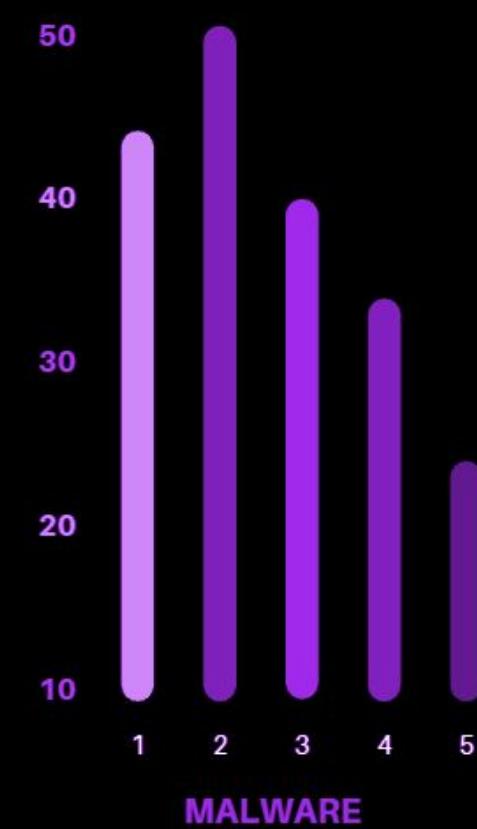
KP ❤ P STANS SUMMARY	P. 2
KP ❤ P VULNERABILITIES ACTIVELY ATTACKED & PATCHING STATUS	P. 2
KP ❤ P MALWARE & PHISHING CAMPAIGNS	P. 3
KP ❤ P HIGHLY TARGETED DEPARTMENTS & USERS	P. 9
KP ❤ P THREAT ACTOR ACTIVITY	P. 11
KP ❤ P STRATEGIC CTI & THIRD PARTIES	P. 20
KP ❤ P CTI ANALYSIS	P. 25



## CTI INTELLIGENCE PRODUCTS

Target: December 31, 2020

## FINANCE DEPARTMENT



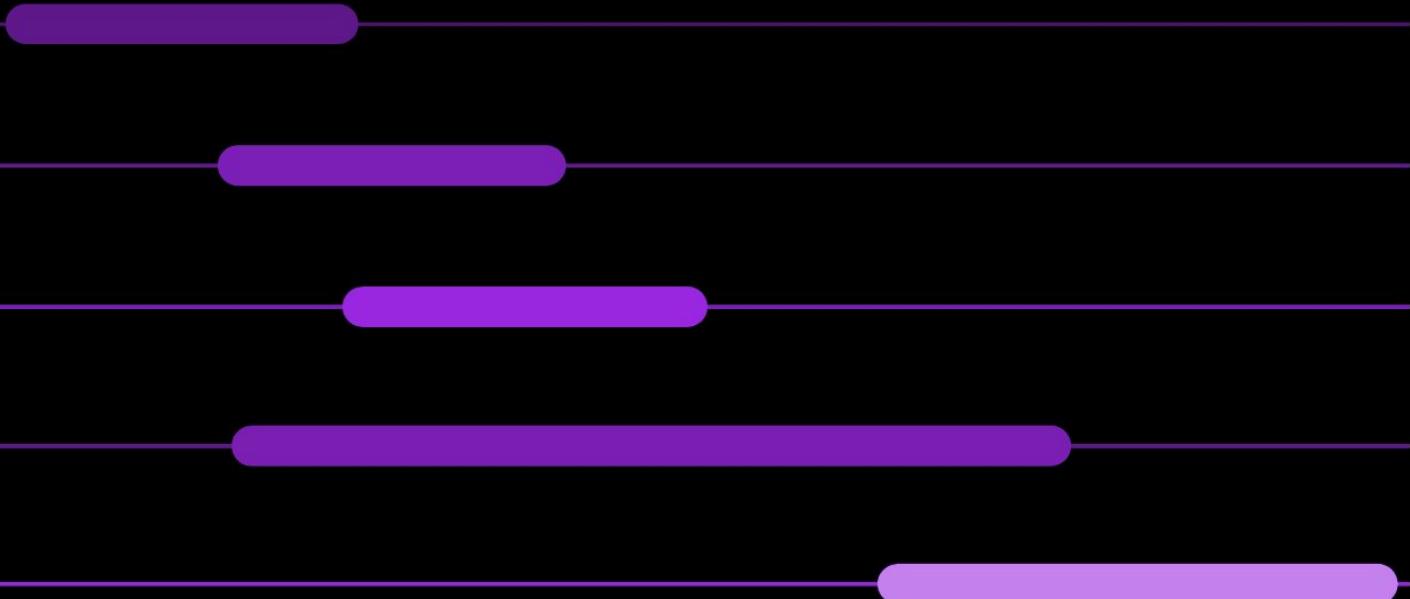
RED  
PURPLE  
HUNT  
BUSINESS ANNUAL  
DEPARTMENT

WEEK 1

WEEK 2

WEEK 3

WEEK 4



# Pyramid of Pain

REFERRALS\$

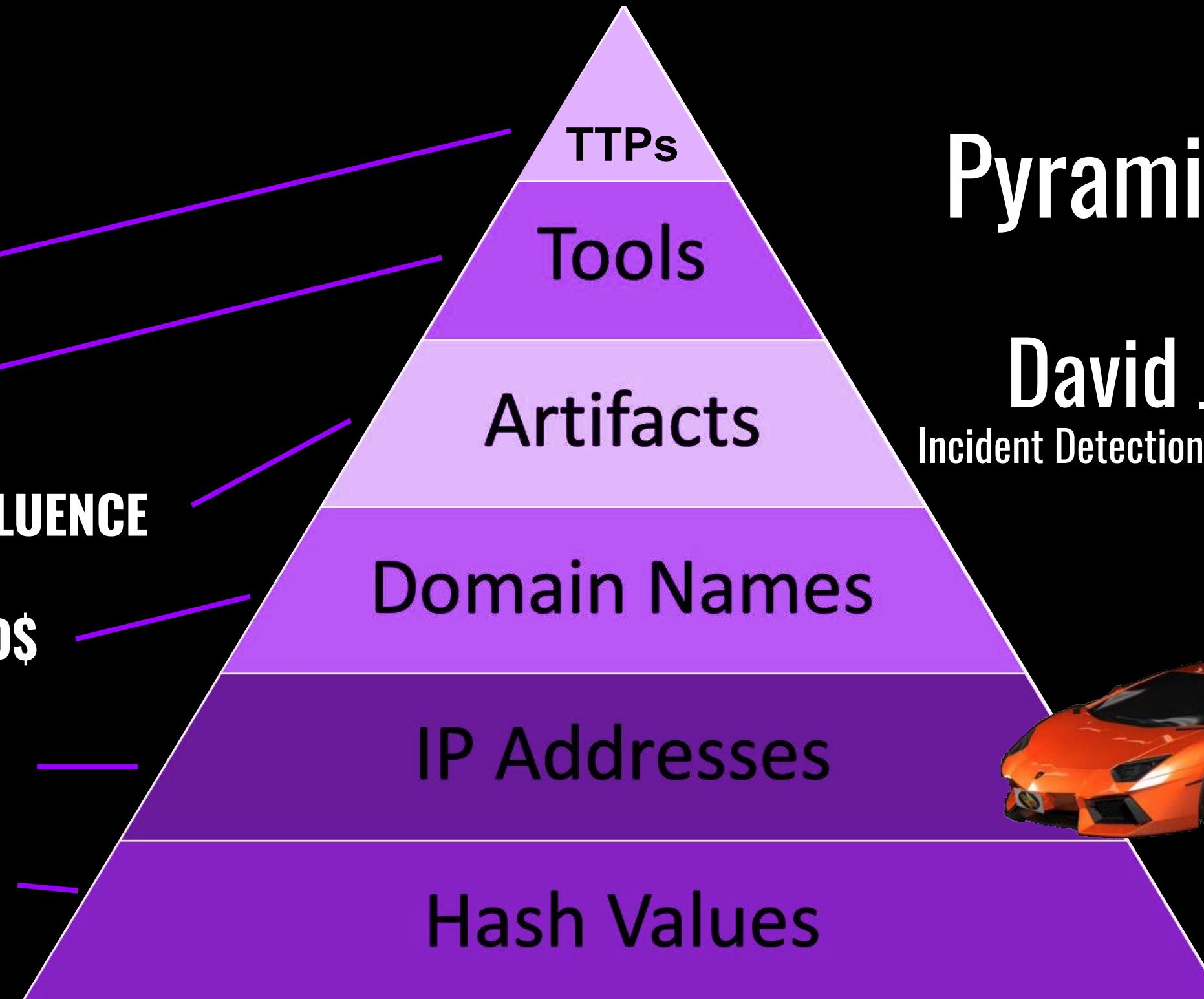
FARMING

\$PHERE OF INFLUENCE

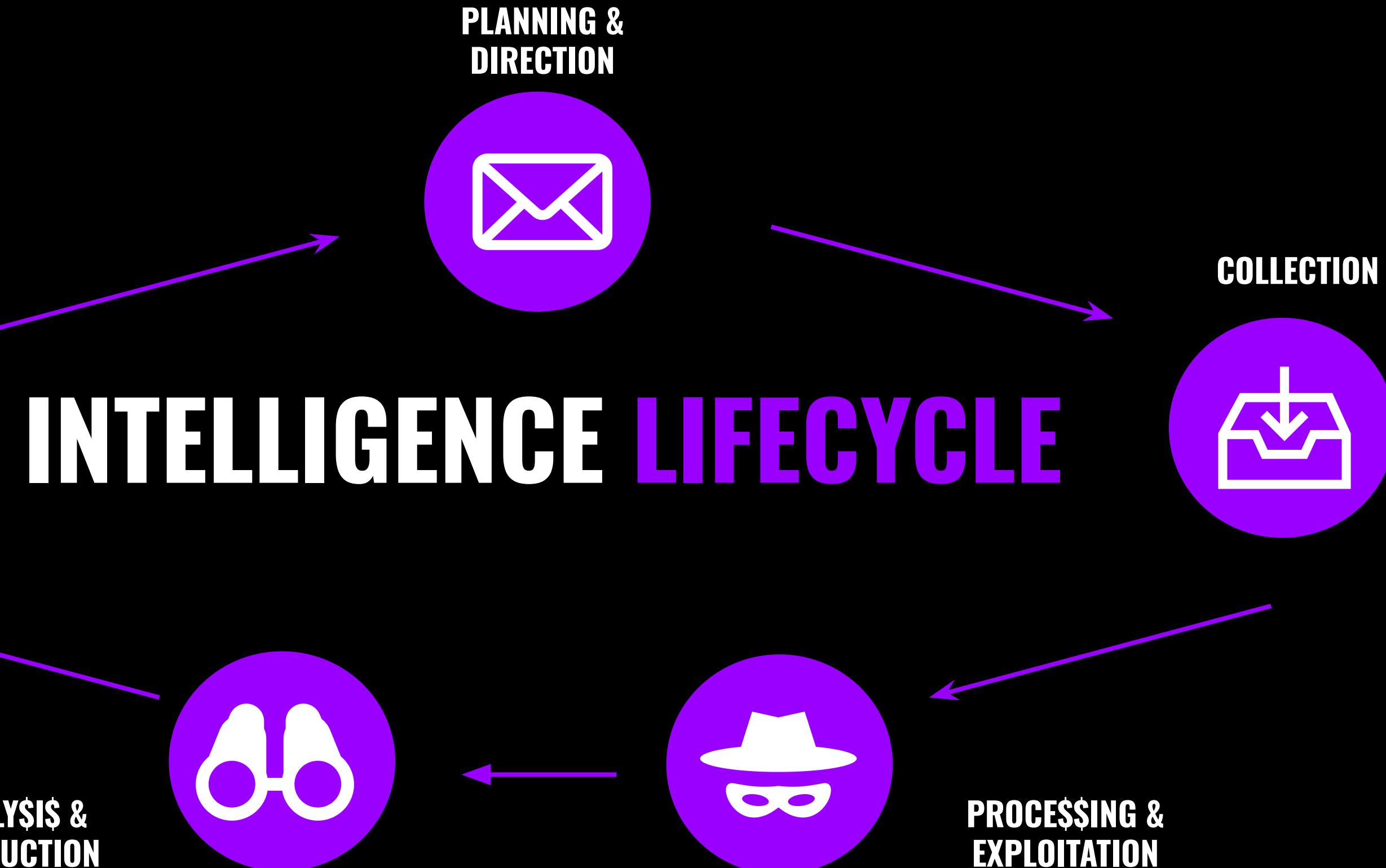
CO-AGENT LEADS\$

BROKER LEADS\$

ORDER TAKING



**David J. Bianco**  
Incident Detection & Response Specialist



# MATRIX W HYPOTHESES

H1 | H2 | H3 | H4 +

EVIDENCE  
EVIDENCE  
EVIDENCE  
EVIDENCE

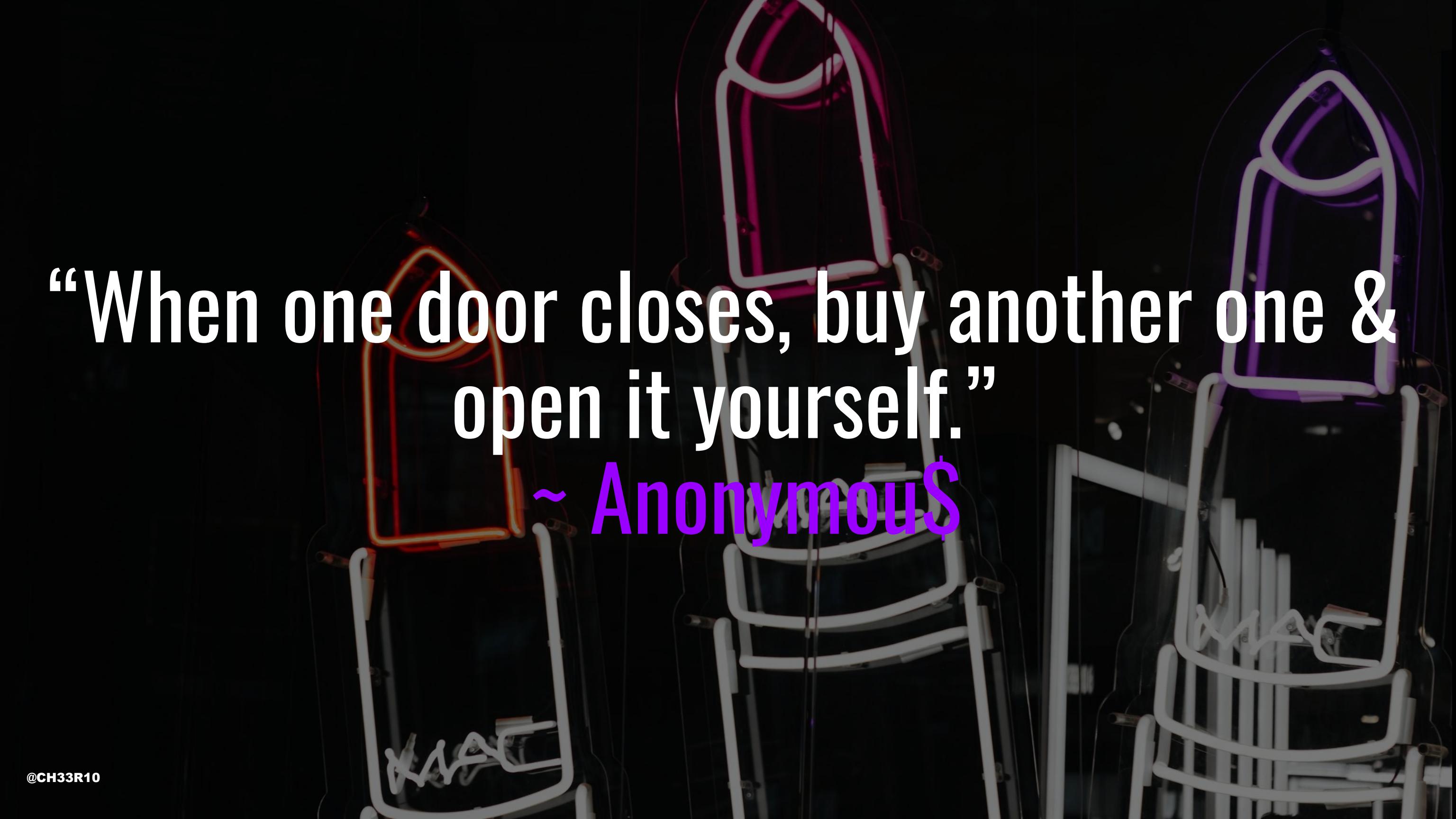
CONSISTENT | INCONSISTENT | NEUTRAL

# The Diamond Model ... of REAL ESTATE



Sergio Caltagirone, Andrew Pendergast & Christopher Betz

# T3CHNOLOGY



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

~ Anonymous

w1iFM

FOR  
THE  
MATERIAL  
WORLD

Take what you can use  
& ignore the rest.

Give career-changers  
?’s that make them  
SHINE.





YOU  
WANNA  
PIZZA  
ME?

\$m Biz/\$olopreneurs  
SIMPLE & EASY solutions to  
[hopefully] NOT get Sued &  
still make \$\$\$

A photograph of a roller coaster at night, viewed from below. The structure is a complex web of steel beams and supports, all illuminated by numerous small, glowing lights in various colors like red, blue, green, and yellow. The lights create a vibrant, almost futuristic atmosphere against the dark night sky.

# FUTURE PLANS

“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

## Search

»

real estate

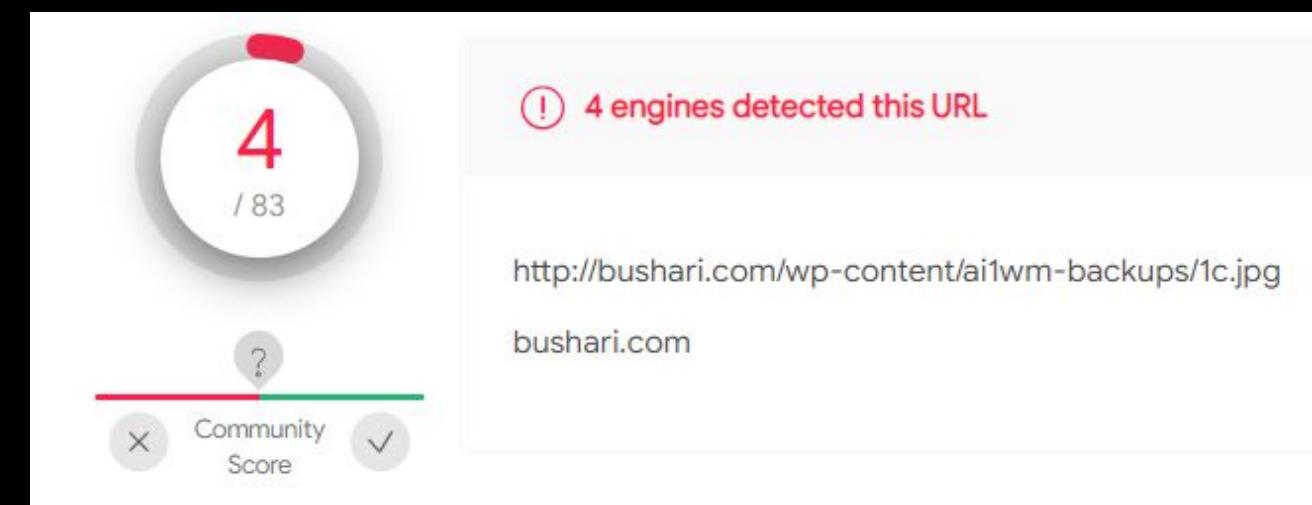
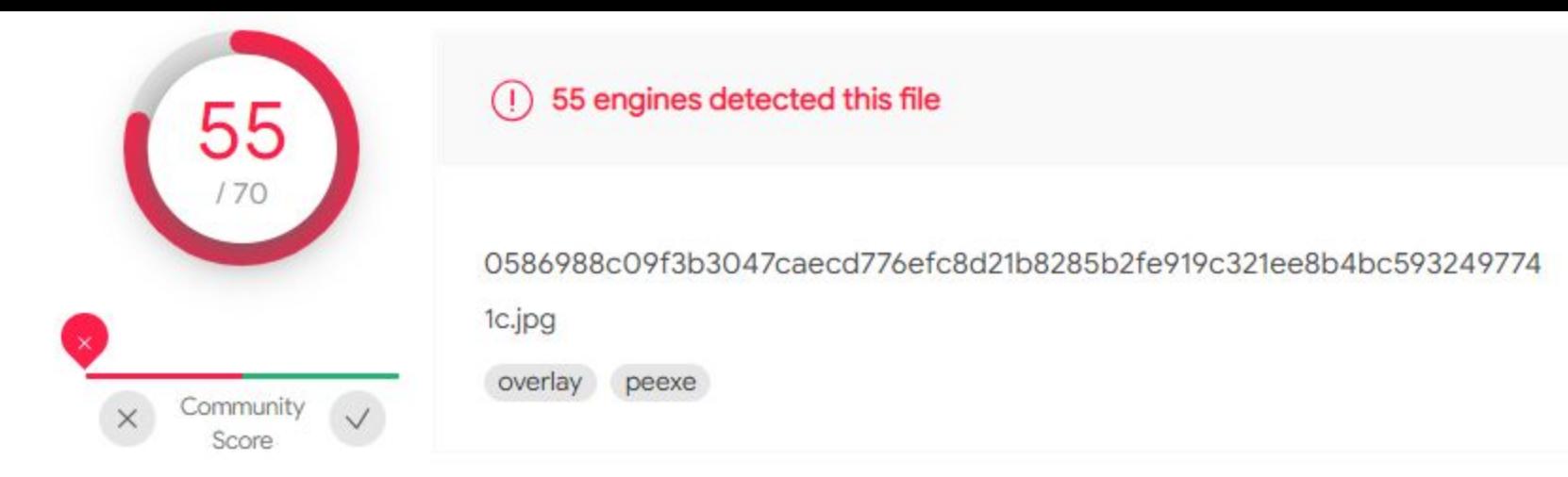
meta: classification

Indicators Threats Feeds

Filters Export API Tweet 100 results More results

Indicator ↓ Domain Type Risk Last Seen 3 indicators

http://bushari.com/wp-content/ai1wm-backups/1c.jpg 2021-01-04 21:17:51  
GDPR - registrant hidden 1 week ago



# SHADE RANSOMWARE

**From:** "[support@apple.com](mailto:support@apple.com)" <jmmotzgq@tlpknsjd.zgxxi>

**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 permanent suspension**

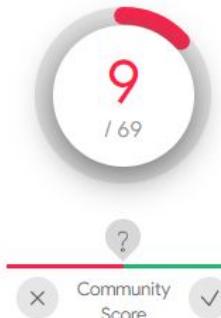
Apple Team

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

#[green square] 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



! 9 engines detected this URL

http://dukashing.com/bestrealtor/default.php  
dukashing.com

404 Status | text/html Content Type | 2016-07-19 08:07:37 UTC | 4 years ago

DETECTION DETAILS RELATIONS SUBMISSIONS COMMUNITY

Downloaded Files ⓘ

Scanned	Detections	Type	Name
2020-12-24	2 / 61	HTML	suspendedpage.cgi

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

# FIE\$TA EXPLOIT KIT

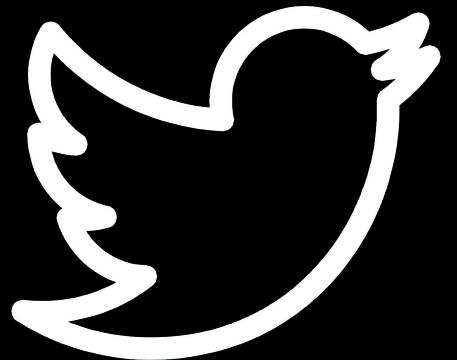


\$15.9M



# THANK YOU

# Xena Olsen



@ch33r10



/in/xena-olsen

<http://bit.ly/SANSCTISUMMIT2021>



**CYBER SECURITY**

# REAL ESTATE THREAT LANDSCAPE

**TOP THREAT VECTOR**  
**EMAIL**

## Ransomware Blogs

KEYWORD: REAL ESTATE

RELATED	REAL ESTATE
RANSOMWARE	AMT
CONTI	1
MAZE	1
NETWALKER	5
REVIL	3
<b>TOTAL</b>	<b>10</b>

REAL ESTATE	
RANSOMWARE	
CLOP	1
CONTI	6
DARKSIDE	1
DOPPELPAYER	2
EGREGOR	5
MAZE	1
NETWALKER	5
REVIL	4
SUNCRYPT	1
<b>TOTAL</b>	<b>25</b>

REAL ESTATE: 25 RELATED: 10  
CLOP, CONTI, DARKSIDE, DOPPELPAYER, EGREGOR, MAZE, NETWALKER, REVIL/SODINOKIBI, SUNCRYPT

## 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](https://bit.ly/SANSCTISUMMIT2021)

# Special Thanks

SANS Institute

Jared Peck

Gert-Jan Bruggink

Ben Goerz

Jason Kichen

Joe Slowik

Cory Kennedy

Ryan Kovar

Katie Nickels

Secret Squirrels

FUZZYSNUGGLYDUCK

**CALL FOR PRESENTATIONS IS NOW OPEN**

**PURPLE TEAM  
SUMMIT & TRAINING**

[sansurl.com/purple-team-cfp](https://sansurl.com/purple-team-cfp)

Live Online 

**FREE SUMMIT:** May 24–25 | **TRAINING:** May 17–22

**SANS**  
