RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: HUM-W10

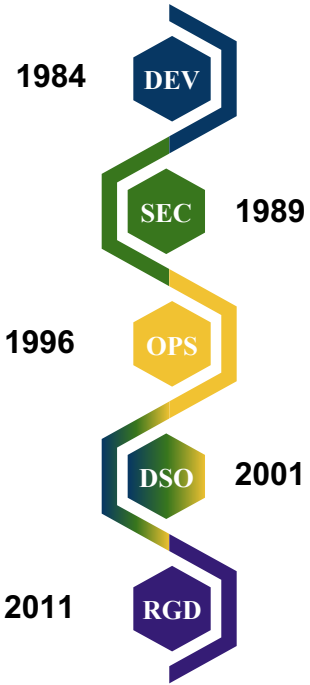
Your Ideal Victim Is My Hero

Shannon Lietz
Director, DevSecOps Leader
Intuit

Myoki Spencer
Manager, Security Automation
Intuit

<me />

MY pseudo JOURNEY LINE...



WHAT MAKES ME HUMAN...

Sugar plum fairies

COMICS

HOW I SPEND MY DAYS...

DEV SEC OPS | SOFTWARE SAFER SOONER

intuit

IANS

HACKERGIRL

myoki

- 10 PRINT “Coding since 1981!”
- ~~Joined the DARK SIDE~~ Became passionate about security ~ 10 years ago

DEV SEC OPS
SOFTWARE SAFER SOONER

intuit

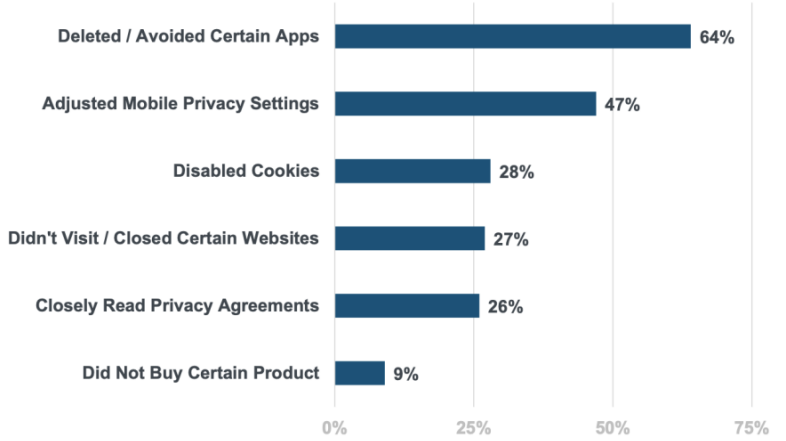
HACKERGIRL

60 million.

People are becoming more paranoid...

…Most Online Consumers Protect Data When Benefits Not Clear

Consumers Taking Action To Address Data Privacy Concerns



% of Respondents that Took Action in the Last 12 Months Due to Data Privacy Concerns, USA

KLEINER PERKINS 2018 INTERNET TRENDS

Source: Deloitte *To share or not to share* (9/17)
Note: n = 1,538 USA consumers in cooperation with SSI.

Money is being made in Cyber Crime...

Cybersecurity = Threats Increasingly Sophisticated...Targeting Data

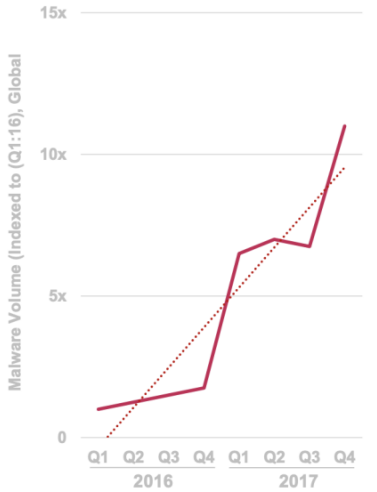
Adversaries are taking malware to unprecedented levels of sophistication & impact...

Weaponizing cloud services & other technology used for legitimate purposes...

And for some adversaries, the prize isn't ransom, but obliteration of systems & data.

- Cisco 2018 Annual Cybersecurity Report, 2/18

Observed Malware Volume



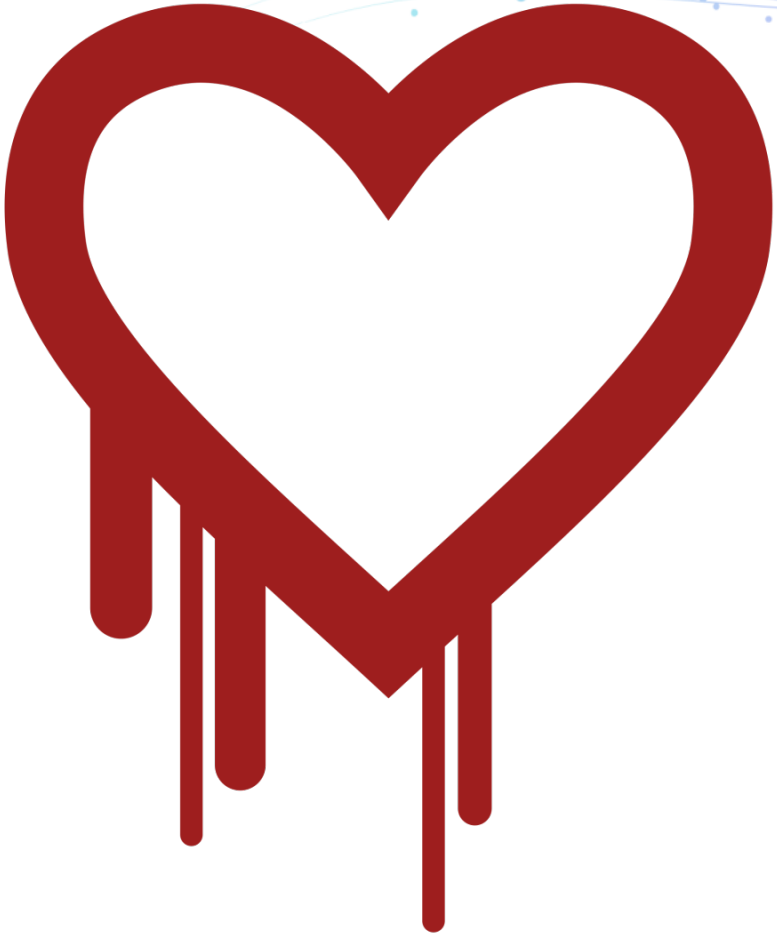
KLEINER PERKINS 2018 INTERNET TRENDS

Source: Cisco 2018 Annual Cybersecurity Report. Note: Data collected by Cisco endpoint security equipment / software. While Malware volume increased ~11x from Q1:16 to Q4:17, traffic events process by the same equipment only increased ~3x.

211

Think like an adversary.

Know every attack.



DIRTY COW

20k+ per year

- Too much focus on ***threat actors*** can be overwhelming.
- Figuring out every ***attack vector*** will make you crazy.
- Picking the ***"best defense"*** is nothing short of a miracle.

What if it doesn't have to be so difficult?

The Ideal Victim.

What do we know about Adversaries?

- An adversary is a person or group that sets out to take advantage of a ***weakened person*** or ***thing*** for personal gain.
- Adversaries spend most of their time on crafting, trading and sharpening ***weapons***.
- Adversaries have the ***odds*** on their side.
- An adversary is ***nothing*** without a victim.

Why study ideal victims?

Unlike attacks and adversaries:

- the number of victims is bounded
- victims are easier to study
- victims share intuitive commonalities
- victims are easy to synthetically replicate

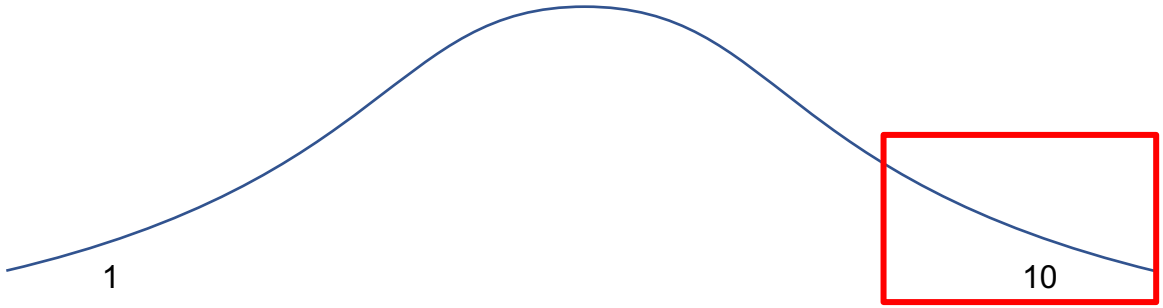
What is an ideal victim?

- An ideal victim is an ***attractive target*** for an adversary.
- Victims have personal and system ***characteristics*** which identify them as worth pursuing.
- The larger the pool of an ***ideal victim type*** the more pervasive and persistent the adversary.


GCI PROTOCOL

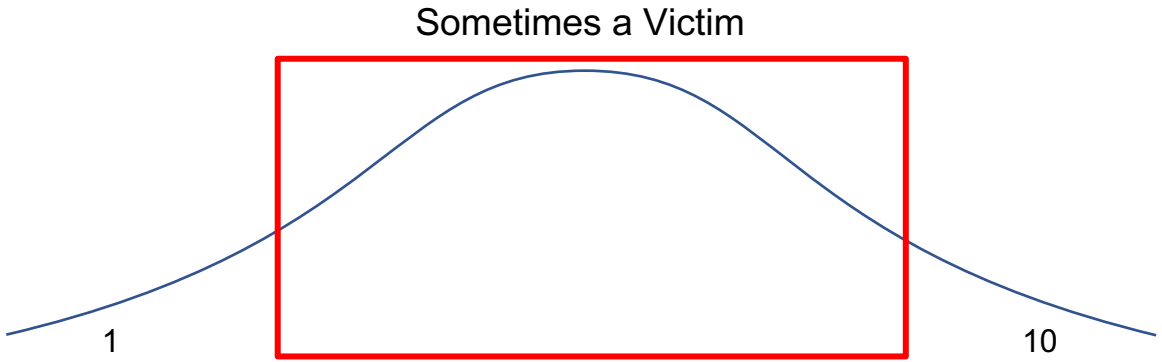
You might be a victim if...

Characteristics of a cyber victim - Skeptics



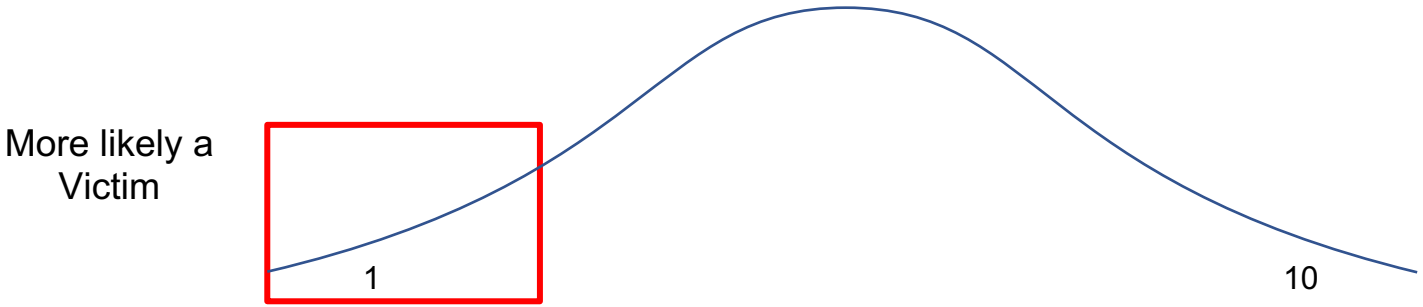
Busy		Thorough
Risk Taker		Risk Averse
Emerging		Commodity
Willing		Unwilling
Modern		Traditional
Uneducated		Educated

Characteristics of a cyber victim - Popular Vote



Busy		Thorough
Risk Taker		Risk Averse
Emerging		Commodity
Willing		Unwilling
Modern		Traditional
Uneducated		Educated

Characteristics of a cyber victim - Leads the Pack



Busy		Thorough
Risk Taker		Risk Averse
Emerging		Commodity
Willing		Unwilling
Modern		Traditional
Uneducated		Educated

Cyber Victim Model

Cyber Victim Model (CVM)

Send a phishing email to a list of people to gain authentication credentials

{HOW} **{WHO}**

{WHY}

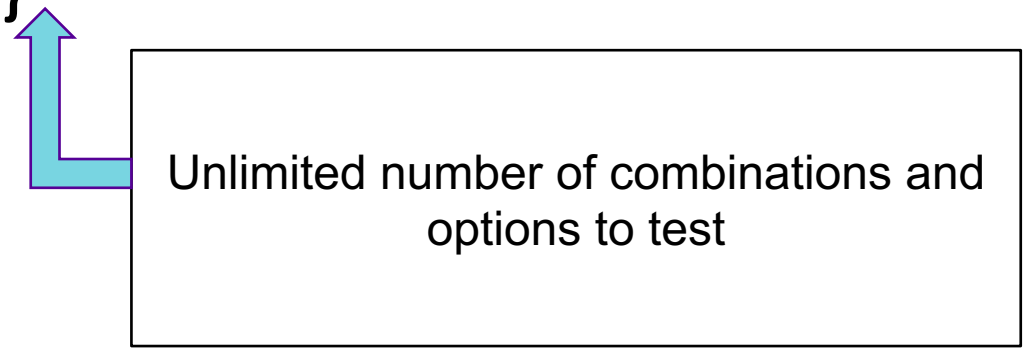
Cyber Victim Model (CVM)

Send a phishing email to a list of people to gain authentication credentials

{HOW}

{WHO}

{WHY}



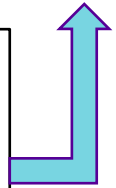
Cyber Victim Model (CVM)

Send a phishing email to a list of people to gain authentication credentials

{HOW} **{WHO}**

{WHY}

Very few “why’s” but focus here can create significant unnecessary friction



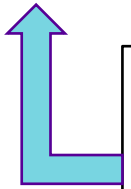
Cyber Victim Model (CVM)

Send a phishing email to a list of people to gain authentication credentials

{HOW}

{WHO}

{WHY}



- Is this a valuable list or cruft?
- Why are these people on this list?
- Who's on this list?
- How could we predict these victims?
- How many phishing emails need to be sent?

Test “Victims”

Why use Deception & Honeypots?

- Creating a sitting duck can be very rewarding
- It's a powerful capability for understanding adversary interest
- Honeypots are commonly deployed and intel can be shared
- There is a high level of fidelity in the results

This technique exists in the Real World

Port 31337

to a list of people

{WHO}

to a list of people

{WHO}

“busy”

to a list of people

{WHO}

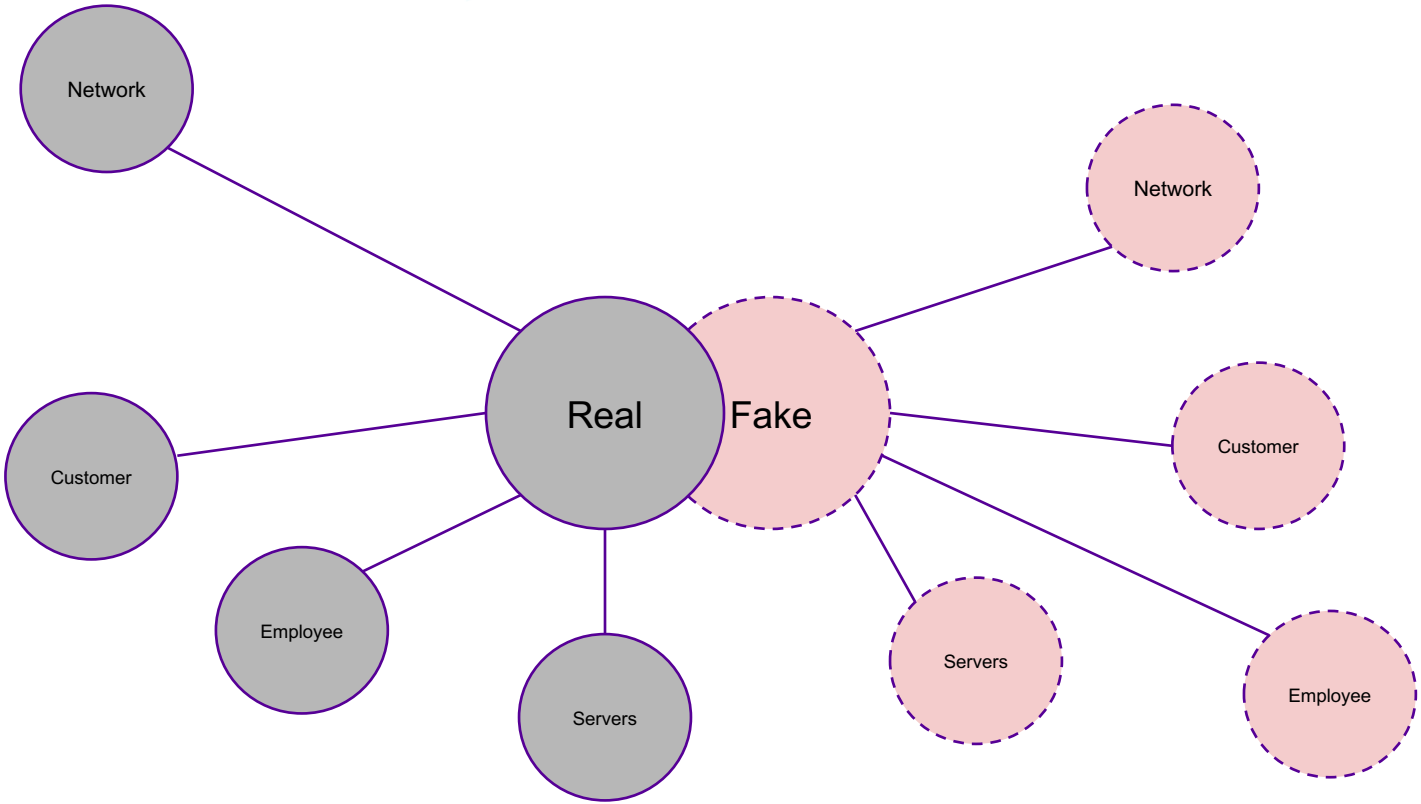
“busy”

Social Media:

search “busy”

782,403

potential victims


Network
Customer
Employee
Servers
Real
Fake
Network
Customer
Servers
Employee

The Results

1 in 531

malware infected emails

1 in 121

malware infected emails

“Apply Slide”

- **This week**
  - Model victims for your environment
  - Find vendors who provide deception technology
- **Next 3 Months**
  - Research the most ideal victims in your environment
  - Build tests to defend your environment
  - Improve software to reduce the number of ideal victims
- **This Year**
  - Use results to further your defenses
  - Participate in community victim modeling

Community **A**buse **R**egister **@ 50.red**
June 2019

What do we need help with?

I’m writing a book along with James Wickett, Ernest Mueller and John Willis on DevSecOps.

We are looking for stories of DevSecOps transformations, journeys, successes and failures.

book@devsecops.org

RSAConference2019

Q&A

Let’s chat!