RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

Intelligence Driven Security

SESSION ID: STU-W01A

Adam Meyers

CrowdStrike, Vice President, Intelligence

ORGANIZATIONS BELIEVE THEY HAVE

A MALWARE PROBLEM

ORGANIZATIONS BELIEVE THEY HAVE

AN ADVERSARY PROBLEM

WHO ARE THE ADVERSARIES?

Adversaries are humans

Targeted Attackers

Motivation can range from disruption, theft, to even destruction

They need to get in

They will likely need to move laterally

Spray and Pray (Prey):

They don’t care who they target (sometimes what)

The more they compromise the more they win

Motivation can range from disruption, theft, to even destruction

Adversary Categorization

CATEGORIZATION | Adversary Groups

1. Tactics, Techniques, and Practices
2. Never assume relationships exist Between indicators
3. Recognize adversaries are constantly changing
4. But RECOGNIZE they are HUMAN

ADVERSARY CATEGORIES

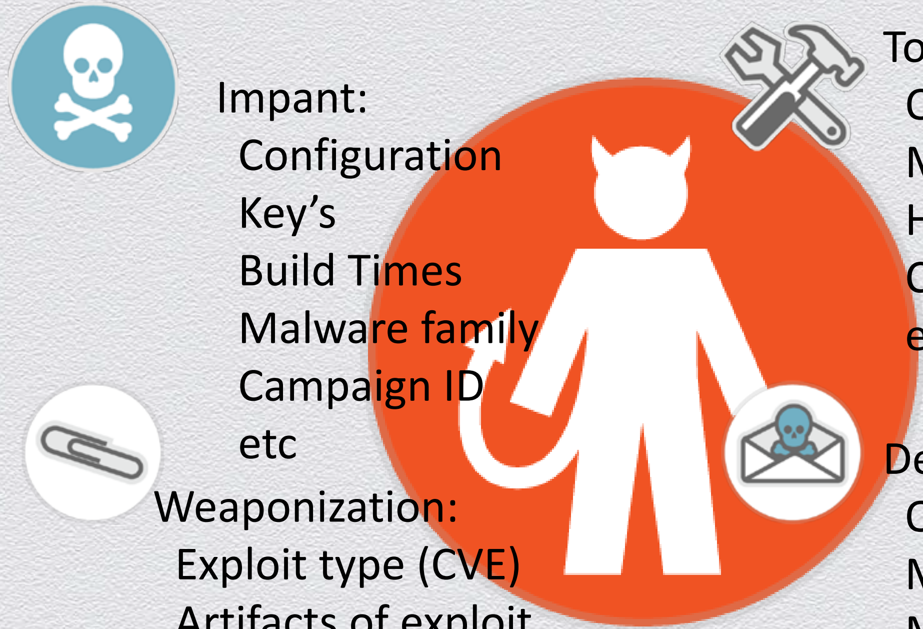
Different Motivations

- State Sponsored
- Criminal Motivated
- Hacktivist
- Activist
- Terrorist
- Others?

Sub-categorization

- TTP specific categories
  - Implant Configuration Overlap
  - Infrastructure Overlap
  - Delivery/Exploit Overlap
- Complications
  - PlugX?
  - 9001?
  - Zeus?

Adversary Categorization



Impant:
- Configuration
- Key’s
- Build Times
- Malware family
- Campaign ID
- etc

Weaponization:
- Exploit type (CVE)
- Artifacts of exploit
- Techniques
- Shellcode
- etc

Tools:
- Origin
- Modifications
- Hashes
- Combination
- etc

Delivery:
- Origin
- Method of Delivery
- Metadata around delivery
- Campaign ID
- etc

Intelligence: Financial Sector Targeting

CHINA

- Comment Panda
- Vixen Panda
- Numbered Panda
- Samurai Panda
- Deep Panda
- Impersonating Panda

CRIMINAL

- Singing Spider
- Shark Spider
- …

NORTH KOREA

- Silent Chollima

INDIA

- Viceroy Tiger

ACTIVIST

- DeadEye Jackal
- Corsair Jackal

Intelligence Driven Security Application

- Your enterprise is being targeted by humans
- Out of the box security solutions aren’t catching anything
- Avoid the noise
- Understand who is targeting you and defend against that

RSA®CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

CROWDSTRIKE