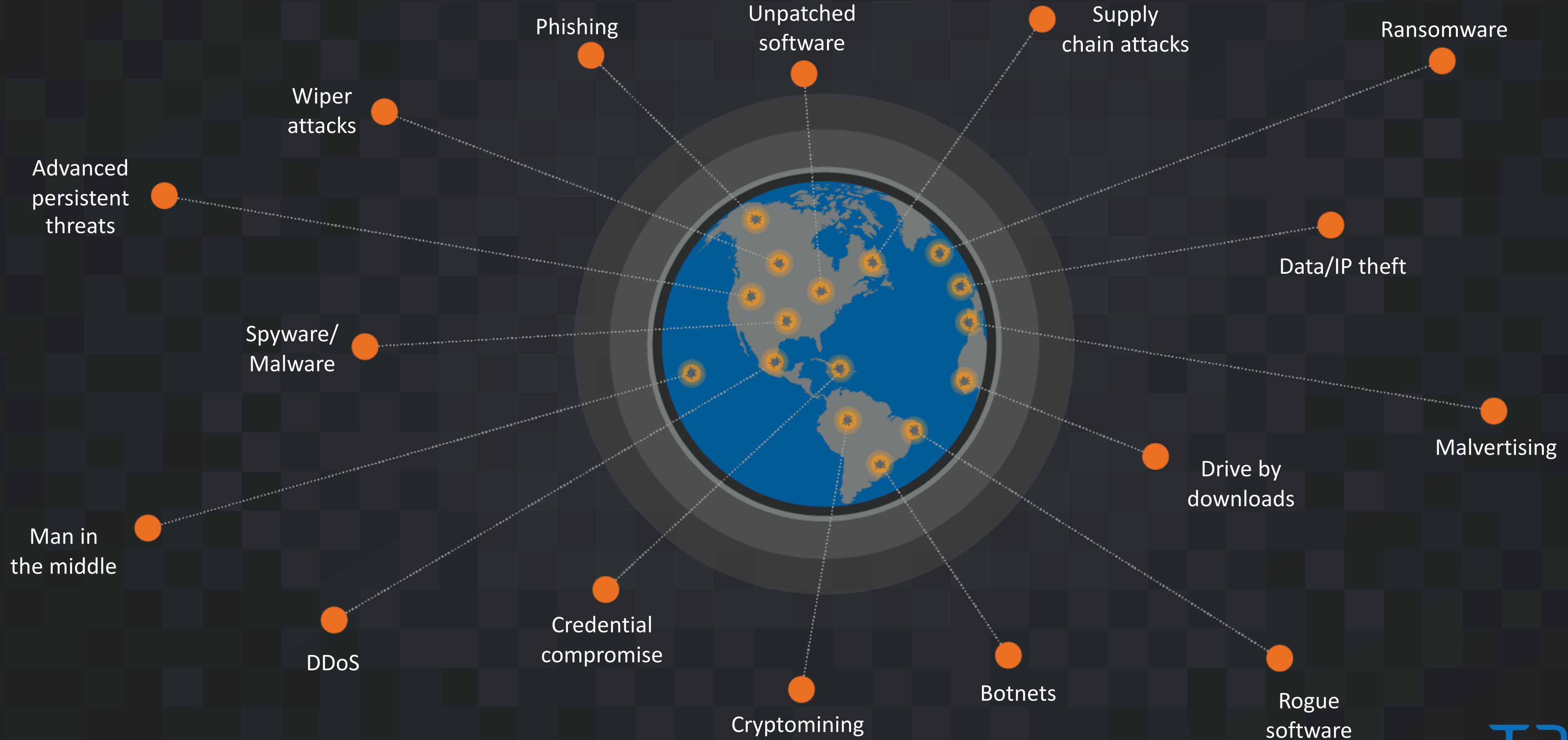
TALOS

Cisco Security Research

Fighting the Good Fight

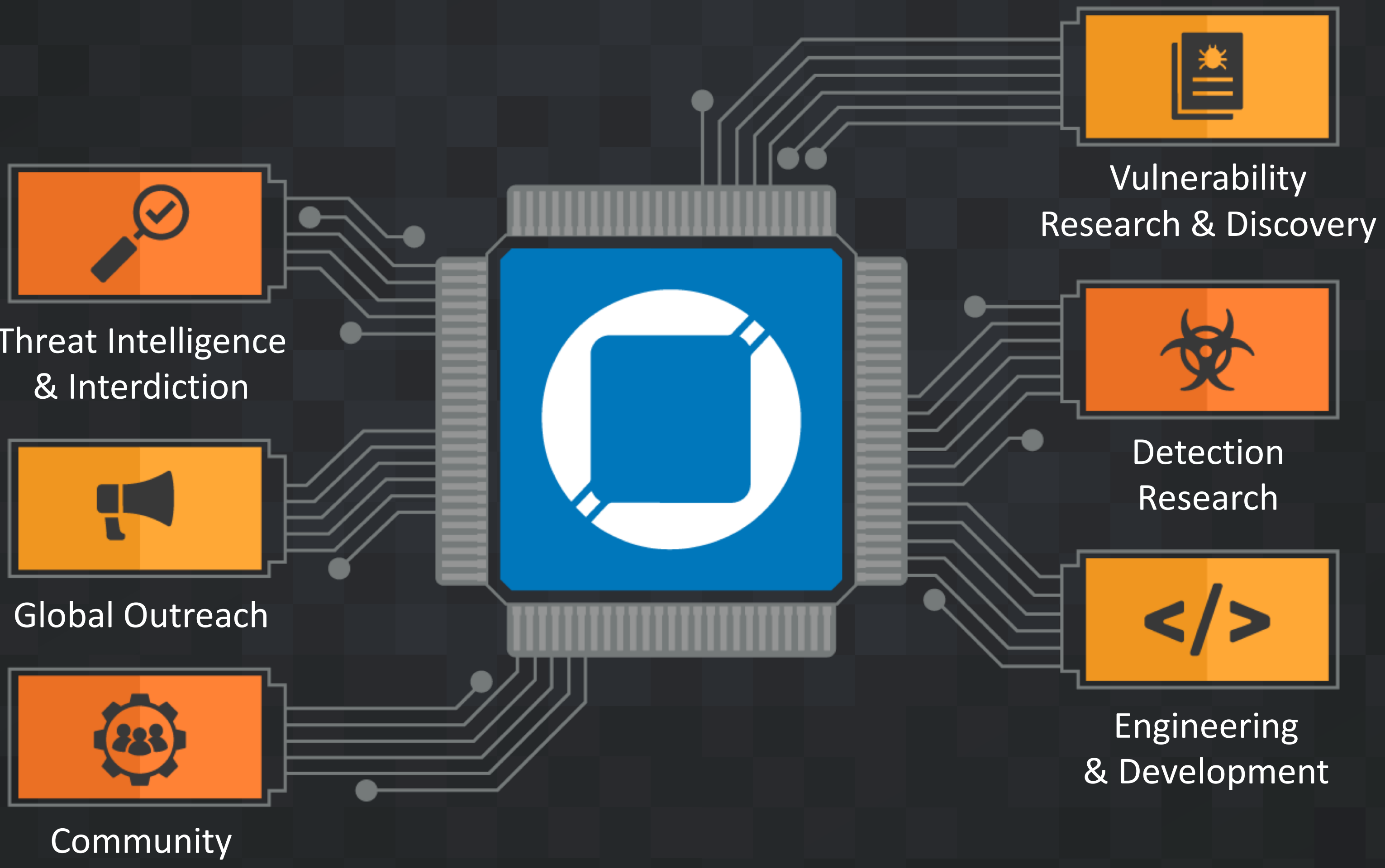
Protecting Customers



TALOS
Cisco Security Research

Our job is protecting your network

Talos is the threat intelligence group at Cisco. We are here to fight the good fight — we work to keep our customers, and users at large, safe from malicious actors.


Threat Intelligence & Interdiction
Global Outreach
Community
Vulnerability Research & Discovery
Detection Research
Engineering & Development

Talos
Cisco Security Research

Historic Threat Actor Behavior

Talos
Cisco Security Research

Broad Patternistic Behavior

“Never let a good disaster go to waste”

Year	Disaster
2014	Ebola Outbreak
2017	Hurricane Harvey
2019	Hurricane Dorian
2020	COVID-19 Pandemic

Targeting and Victimology

Targeting and Victimology

Current Cybercriminal TA Landscape

Our primary observations concerning recent and generally historic cybercriminal behavior continue to support the fact that many groups are highly opportunistic and frequently target organizations with sensitive or high value data.

These cybercrime threat actors look for the “low hanging fruit”. This tactic is not uncommon even when looking at more advanced adversaries such as those sponsored by a nation state.

Threat Evolution

Continually Evolving Threats

Ransomware is not a new form of extortion and as it has become more prevalent we have observed more safeguards being put in place – but so has the adversary.

Within the past six months we have observed a new group evolve from traditional ransomware attacks to include a new form of extortion – Maze.

We have started to see additional Maze copy-cats and expect to see this becoming a more common TA practice.

They are still human though, the Maze group made a public statement at the onset of COVID-19 that they “will not target” medical institutions.

What You Can Do

The Basics

There are no “silver bullets” despite what the sales guy tells you.

Maintain knowledge about what the adversary is doing, even at a high level, and use this knowledge to maintain vigilance.

Have your team focus on the basics and building comprehensive procedure around those basics.

Be less appealing than your neighbor.

Q&A

TALOSINTELLIGENCE.COM

blog.talosintelligence.com

@talossecurity

TALOS™

Cisco Security Research

TALOSINTELLIGENCE.COM