RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: PART2-W02

Defending against Multidimensional Attacks: The Evolution of Threat

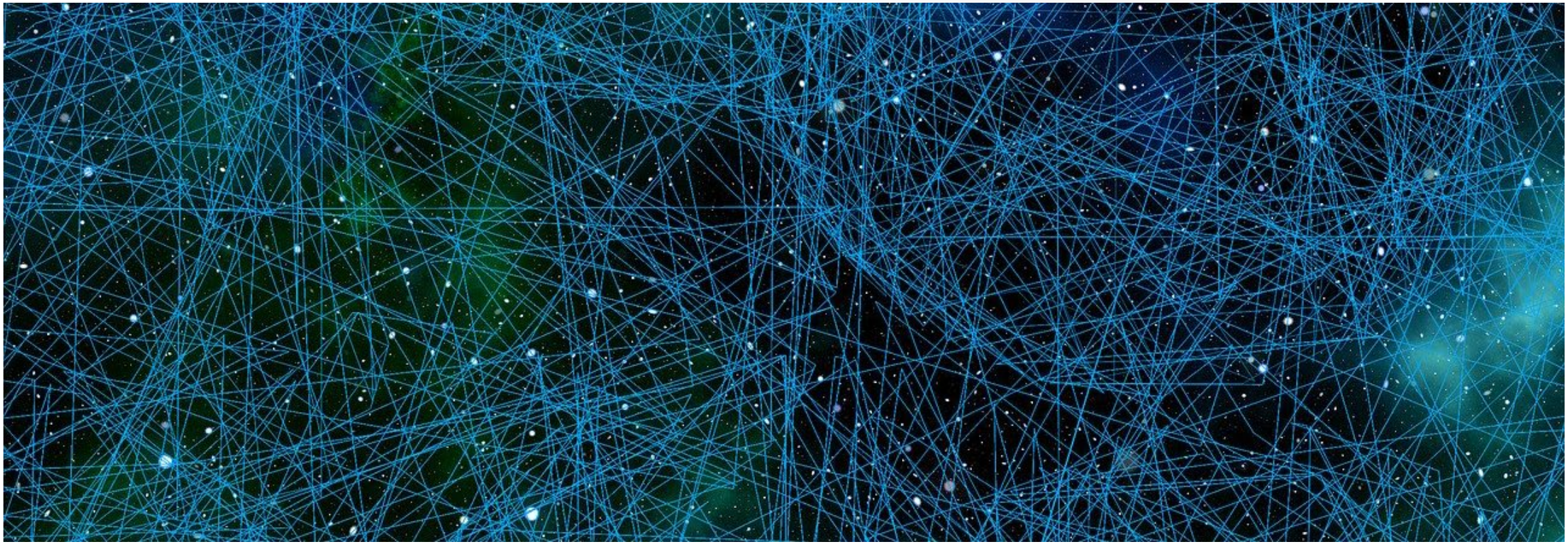
Josh Lemos

VP Research & Intelligence
Blackberry Cylance
@cylanceinc

Eric Milam

VP of Threat Intelligence
Blackberry Cylance
@cylanceinc

Multi-Dimensional Attacks



MULTI-DIMENSIONAL ATTACKS: EXPANSION OF ATTACK SURFACES INCLUDING EMPLOYEES, CONTACTORS, BUSINESS PARTNERS, THEIR PERSONAL AND COMPANY DEVICES, NETWORKS, AND APPLICATIONS.

Taxonomy

THREATS & THREAT ACTORS

Targets by Vertical

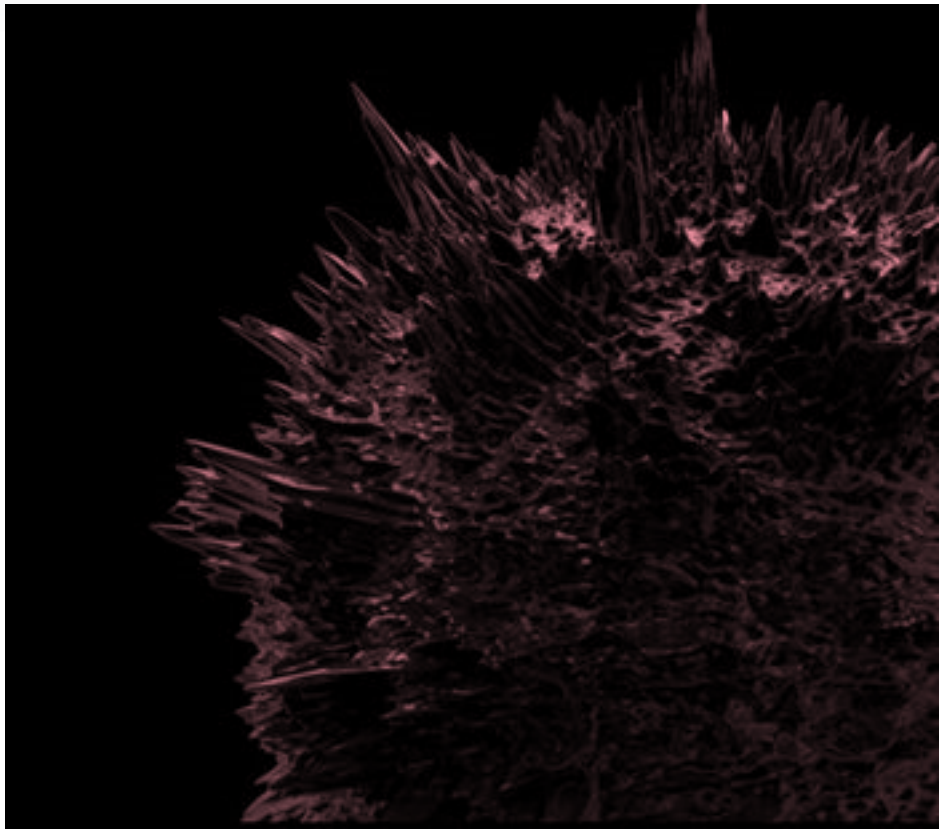
Target	Motivation/Assets	Description
Retail and Wholesale	Financial Information/ PII	Broad attack surface. Credit card data
Technology Software	Intellectual Property	• Intellectual property theft • Supply Chain Attacks
Service Providers	Managed Endpoints	Disable controls to allow for compromise.
Healthcare	Financial Gain	Life or death situations optimize for likelihood of payment
Finance/Banking	Financial Assets	That's where they keep the money.
Federal Government	Geopolitical	• Access to military intelligence • Access to financial information • Significant quantities of PII • Information about government contracts
State/Local Government	Financial Gain, Disruption of Service	Understaffed. Optimize for likelihood of payment

Tools – APT goes mainstream

- Off the shelf software
  - Remote management tools like Go2Assist or NinjaRMM
  - Passcape's password recovery tool
- Pentesting tools
  - Cobalt Strike
  - Powersploit
- Multi-stage loaders & payloads
  - Initial compromise steals data and using ransomware as leverage
  - Example: Tickbot serving Ryuk and Emotet

Host Dependent Encryption

- APT-related malware samples using host-dependent encryption to protect their payloads
- OceanLotus group has started to wrap their implants in a multi-stage loader
- Initial dropper copies itself and encrypts some of its malicious code using a one-time randomly generated key.



Ransomware as Disruption

- Ransomware families used in the highly targeted attacks of 2019 include Sodinokibi, Ryuk, and Zeppelin.
- At times payment infrastructure and/or the encryption routines are flawed making file decryption or ransom payment impossible
- Attacks resemble simple wipers, which pose as ransomware but ultimately only destroy data.

MSSPs Targeted to Deploy Ransomware

- The initial Sodonokibi compromise occurred via targeted phishing attacks aimed at managed service providers (MSPs)/MSSPs managing IT/security within the target organization
- Once inside, attackers deployed common tools like Passcape's password recovery tool to steal credentials.
- Allows attackers to easily pivot to the hundreds of other diverse and vulnerable targets in the environment

RSAConference2020

General Threat Trends 2019

Tools, Techniques, and Threat Actors

2019 Overall Trends

- Phishing
- Credentials
- Ransomware
- Coin Miners

Mobile Security Issues

- Learning From Other's Mistakes
- The Iceberg Effect
- Responding to Mobile Threats

RSAConference2020

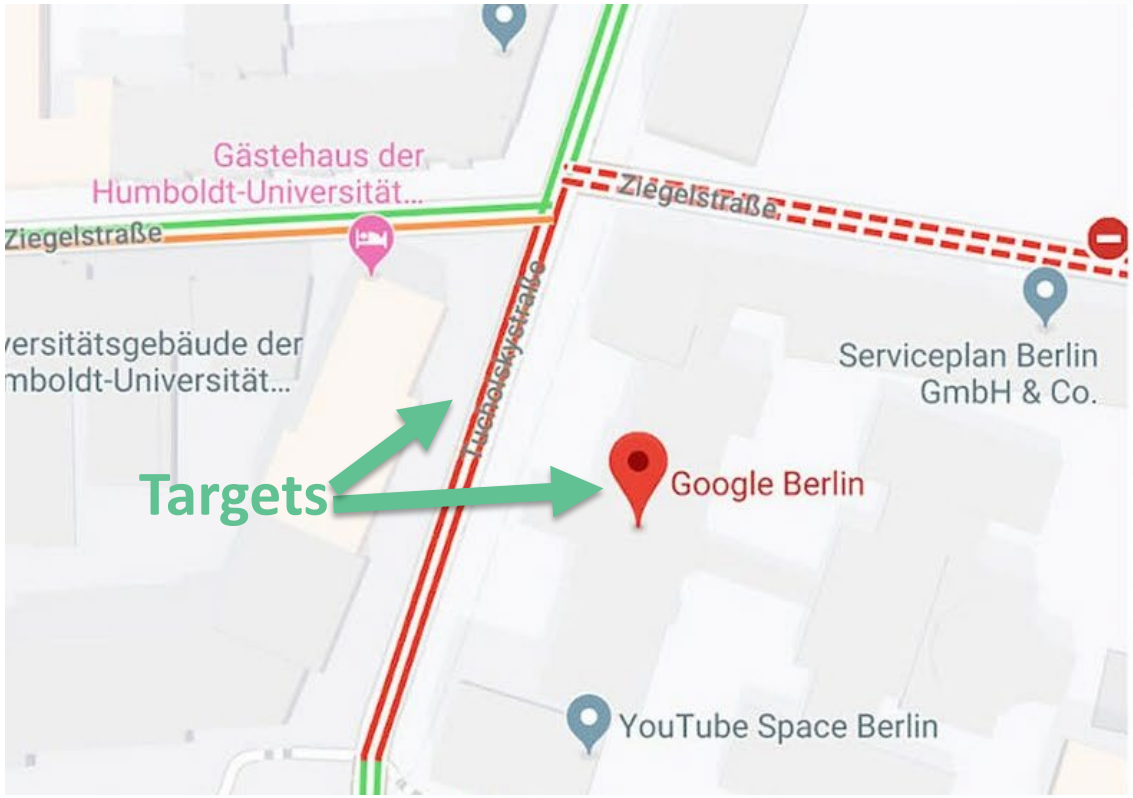
General Threat Trends 2020

Tools, Techniques, and Threat Actors

Adversarial ML or Nah

- Over the past year several attacks have surfaced which aim to influence ML classifiers and subvert a model's determination from malicious to benign
- One example is stuffing attacks that mutate existing threats by including excessive amounts of benign features
- Another is tampering attacks that alter file headers and modify code or data to mimic benign samples

Adversarial ML by Simon Weckert



Adversarial ML

Deep Fakes

Deep Fakes Supporting Threat Activity

Misconfigured Cloud

Increased Data Loss From Misconfigured Cloud Resources

Vulnerable Vehicles

- Technology Raises Vehicle Profiles
- Who Is Breaching Vehicles?
- What Can Be Done?
- The Road Ahead

Predictions - Looking Ahead

- Crimeware-as-a-Service Increases Ransomware Attacks
- Nuance Returns to The Facial Recognition Debate
- Mobile Cybersecurity Becomes A Major Concern for Organizations
- Operationalized Adversarial Machine Learning

What to do next? – IT Security

- Evaluate threat models to identify blind spots by taking stock of your current telemetry and security posture on all dimensions
- Develop a strategy to aggregate all intelligence and begin to automate low-level response actions
- Reduce attack surfaces on every dimension
  - Consider people centric and device centric security models
- Leverage ML Enabled Security Products to proactively reduce risk
- Consider zero-trust architectures and reduce access as an IT strategy
- Audit cloud and business apps with the same rigor as internal systems

What to do next? – Machine Learning

- Build environment specific ML models that can identify meaningful deviations from baselines to generate meaningful signal
- Extend training sets and refine feature spaces used for training models
- Consider model ensembles that include tamper detection capabilities
- Develop processes for ongoing model evaluation that can identify concept drift and identify the need for feature re-engineering

RSAConference2020

Questions