RSA Conference2016
San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: PDAC-W03F

End Island Hopping Hackers' Vacation in Your Information Supply Chain

Ed Cabrera
V.P. Cybersecurity Strategy
Trend Micro
@Ed_E_Cabrera

Tom Kellermann
C.E.O.
Strategic Cyber Ventures
@TAKellermann

Introductions

Ed Cabrera
V.P. Cybersecurity Strategy
Trend Micro

Tom Kellermann
C.E.O.
Strategic Cyber Ventures

TREND MICRO

Supply Chain and Third Party Risk

Information Supply Chain Risk

2015 Supply Chain Data Breaches

OPM

"22 Million Affected by OPM Hack"

- Attackers gained access to LAN May 7, 2014
  - Stolen Credentials
  - Dropping Malware
  - Creating Back Door
- First data exfiltration by attackers on July 3, 2014
- Attackers pivot to Interior Department systems in October 2014
- Attackers exfiltration data on December 15, 2014
  - SSL traffic
- Signs of a compromise were discovered on April 15, 2015

OPM

Attack Analysis

- Point of Entry - May 7, 2014 (2013?)
  - Stolen Credentials (KeyPoint) - **Undetected**
  - Dropping Malware – **Undetected**
  - Creating Back Door - **Undetected**
- C&C - **Undetected**
- Lateral Movement – **Undetected**
- First data exfiltration – **Partially Detected**
- Island Hop to DOI – **Undetected**
- Second data exfiltration via SSL - **Undetected**
- Breach discovered on April 15, 2015

News Wire Breaches

“Marketwired, Business Wire, PRN Hacked in $30 Million in illicit Trade Scheme”

- 2010 – 2012 Hackers Breached News Wire Cos
  - 390 SQL injections Attacks (Marketwired)
  - 219 stolen credentials (Business Wire)
  - Reverse Shell / Dropped Malware (All) (39)
- 2012 Malware detected and removed (PRN)
- 2012 – 2013 40,000 Press Releases Exfilled out of 150,000 (PRN)
- 2015 Phishing Attack thwarted (Marketwired)

News Wire Breaches

Attack Analysis

- Point of Entry – 2010 -2012
  - SQL Injection Attacks - **Undetected**
  - Stolen Credentials - **Undetected**
  - Dropping Malware – **Partially detected**
  - Reverse Shell - **Undetected**
- C&C - **Undetected**
- Lateral Movement – **Undetected**
- Data exfiltration 2012 – 2013 – **Undetected**
- Point of Entry – 2015
  - Spear Phishing - **Detected**

Ukrainian Energy Supply Chain

Pawn Storm Campaign

Stages of Attack

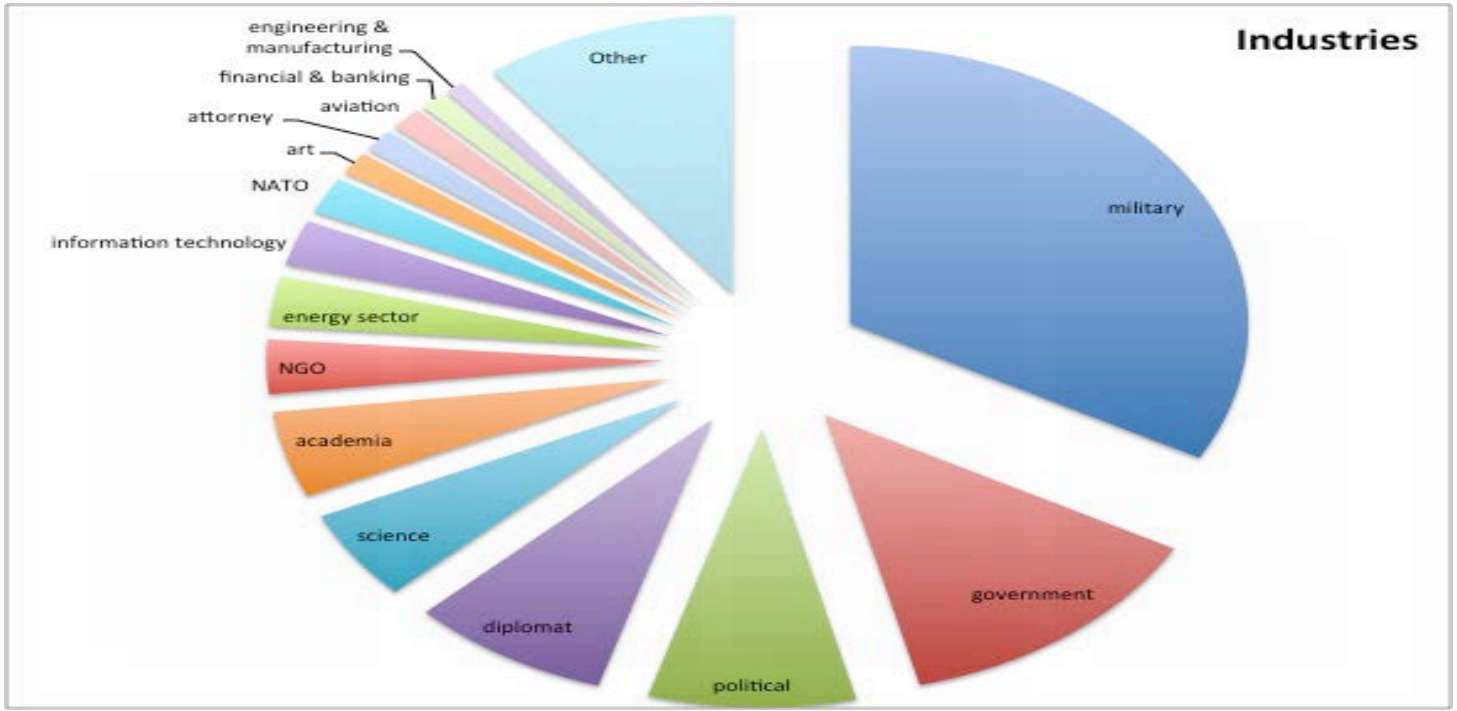
Point of Entry:

- Spearphish (Sednit infected)
- Watering Holes
- IOS Malware/proximity attacks
- File-less Malware
- Lateral Movement
- Island Hopping

Locations of Targets

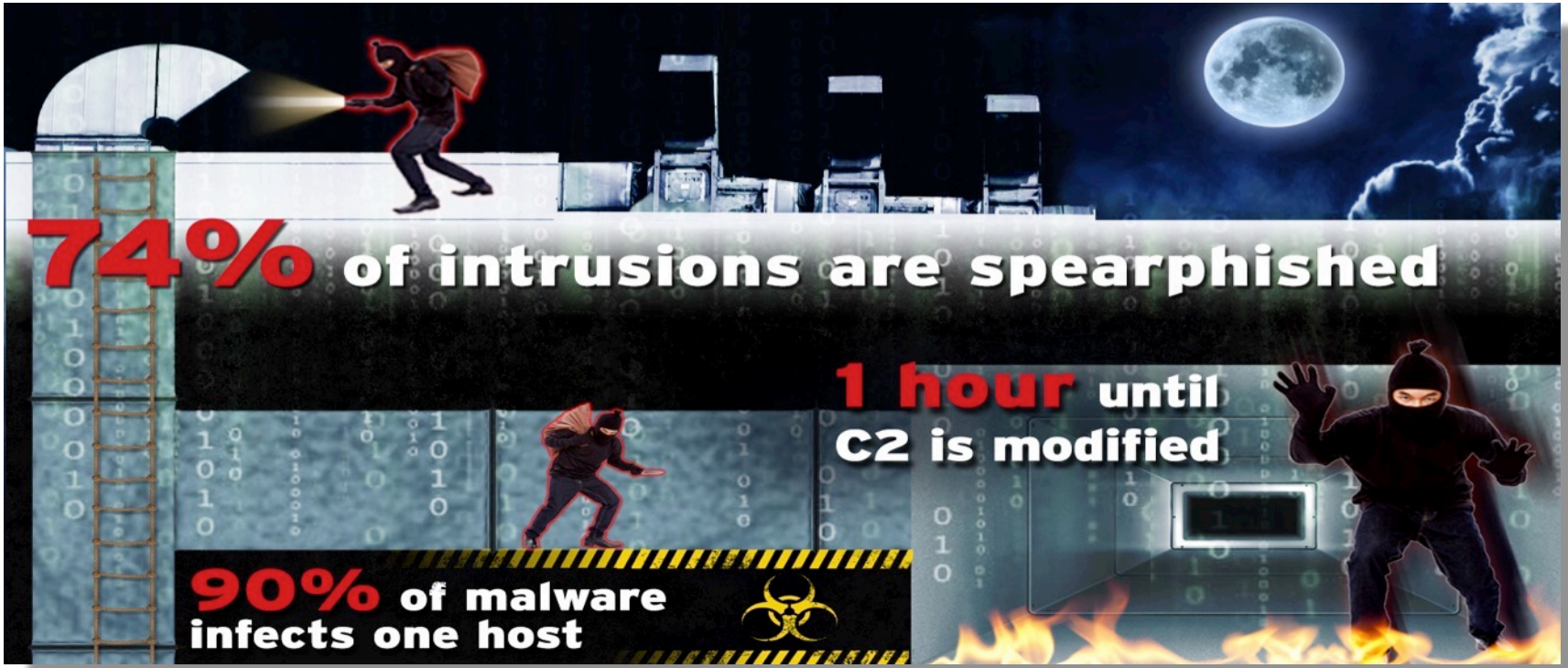
Ukraine	25%
United States	19%
United Kingdom	6%
Russia	6%
Georgia	4%
Hungary	3%
Romania	2%
Belgium	2%
Kazakhstan	2%
Sweden	2%
Others	29%

Attacks by Target Industry



2016 Stratagems of Elite Hackers

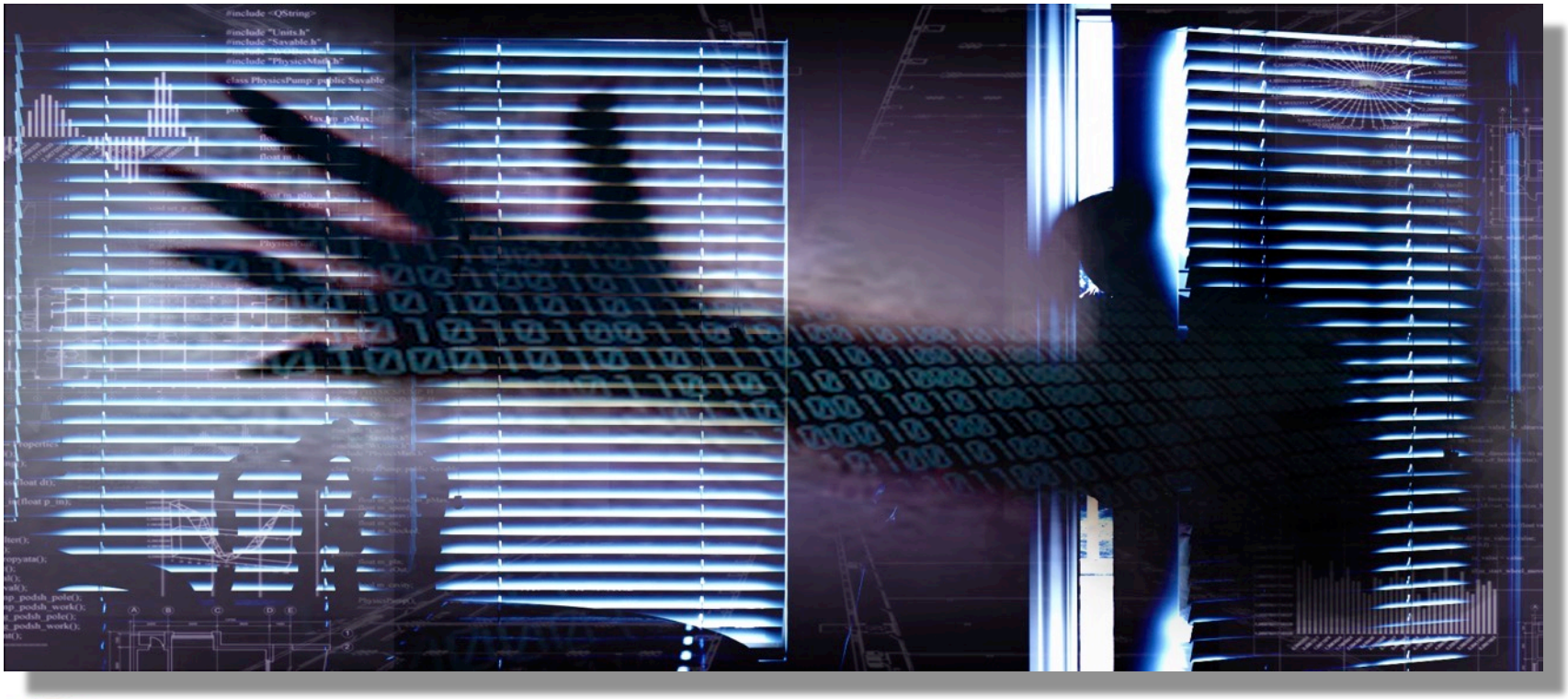
Shifts in M.O.


74% of intrusions are spearphished
1 hour until C2 is modified
90% of malware infects one host

Stages Of Attack

Lateral Movement

Backdoors and Remote Access Trojans



Steganography: Living Modern Art

Secondary Infections Occur within an Hour: Supply Chain Risk

Destroy the Forensics

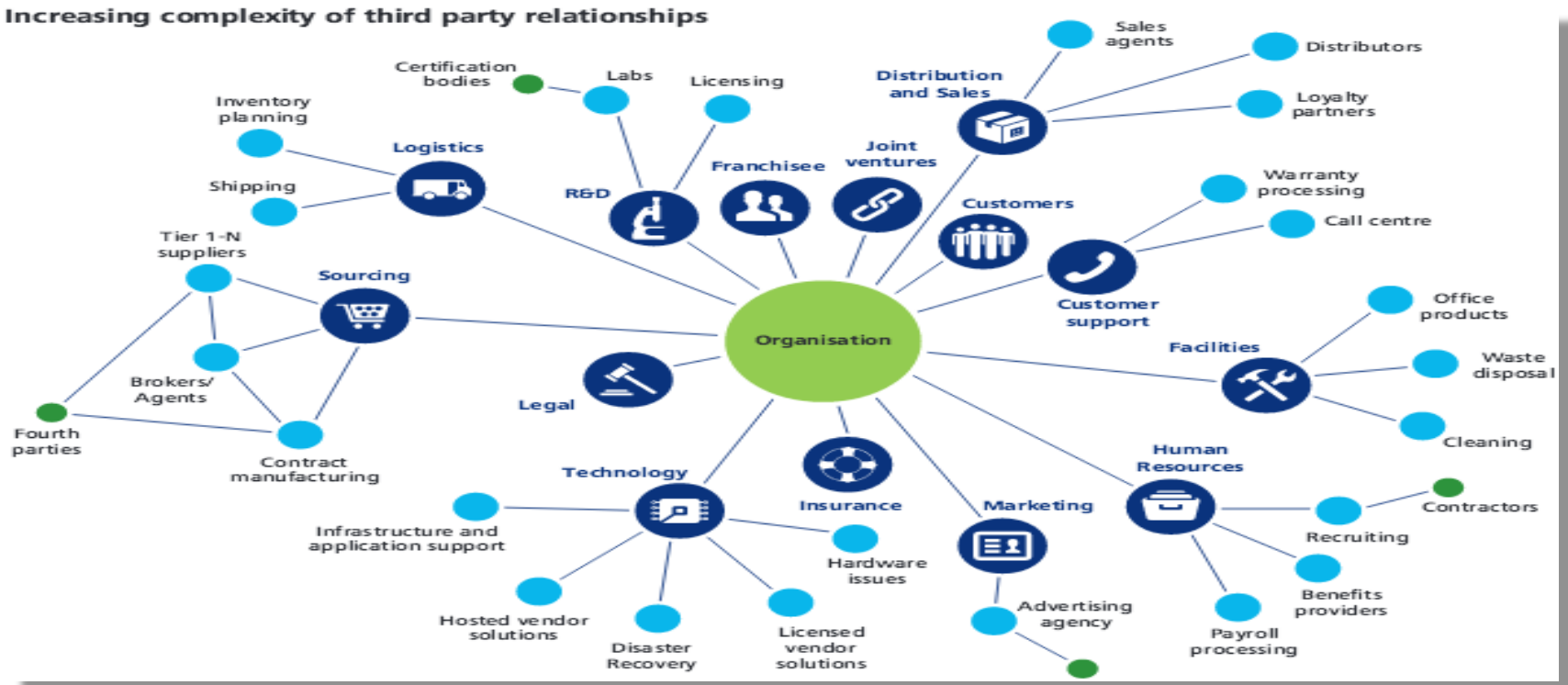
Crypto-Conspiracy

The Future of Cybersecurity

Intrusion Suppression

TREND MICRO™

Systemic and Technical Risk Mitigation



Systemic…

- Develop or improve your third party risk management program
  - **Organize** the relevant parties together internally (IT, legal, and procurement)
  - **Identify** your third parties and prioritize them based on risk
  - **Evaluate** your third parties' security posture
  - **Communicate** your security expectations to third parties through contract and contact
  - **Continuously monitor** critical third party performance

Technical Specifications for the SuperMax

- Enforce Third Party Policy with thorough risk & compromise assessments
- Enforce Network Segmentation
- Utilize Two-Factor Authentication for privileged and unprivileged users
- Sandbox your cloud apps
- Conduct file integrity monitoring
- Implement virtual shielding for zero day exploits.
- Deploy integrated Breach Detection and Intrusion Protection Systems

TREND MICRO

What Next…

- **Next week you should:**
  - Begin to assess or develop your supply chain and third party risk management program
  - Begin to assess or develop a threat focused enterprise risk management program
- **In the first three months following this presentation you should:**
  - Identify your third parties and prioritize them based on risk
  - Develop and/or deploy intrusion suppression strategies, policies, and technology
- **Within six months you should:**
  - Evaluate your third parties' security posture by conducting continuous risk & compromise assessments
  - Continuously monitor threats and vulnerabilities through integrated Breach Detection / Intrusion Protection Systems to you and your third parties