How information sharing enhance protection to organizations

Tony LEE

Head of Consulting: Trend Micro HK & Macau

Industry

Consumers

Business

Government

Healthcare

Law Enforcement

Responsible disclosure

Alerts, blogs, news, reports, guidance

24X7 response, security updates, IPS rules…

Free tools

Public/Private Partnerships

Trend Micro Research

Cyber Threats

Vulnerabilities & Exploits

Targeted Attacks

AI & Machine Learning

IoT

OT / IIoT

Cybercriminal Undergrounds

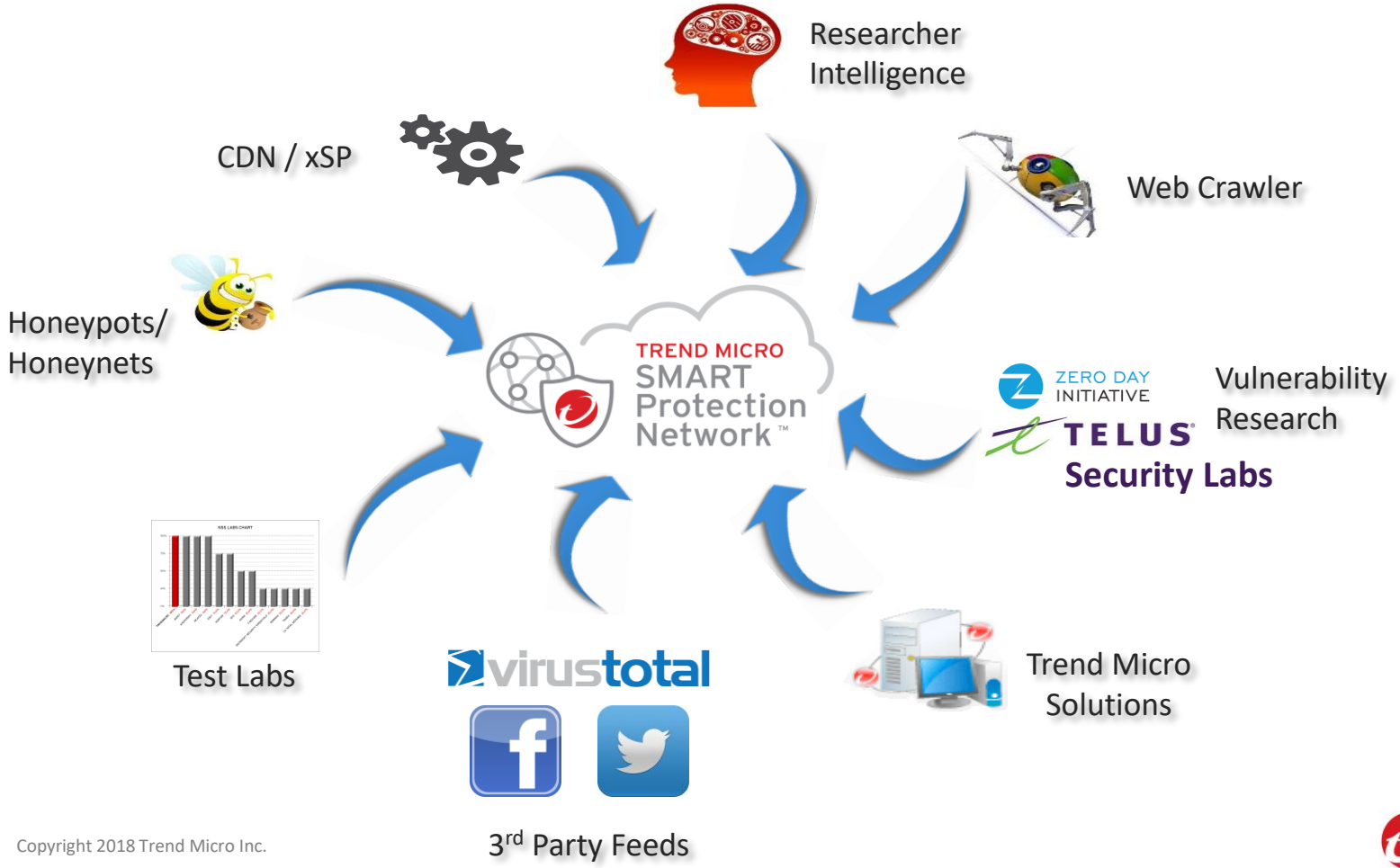
Future Threat Landscape

Insights to improve Trend Micro's core technology and products

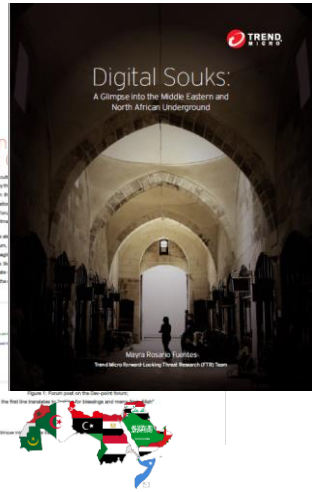
TREND MICRO

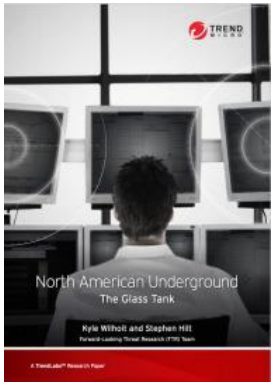
Global Reach: Threat Research Centers

Collected Data Comes From Many Sources

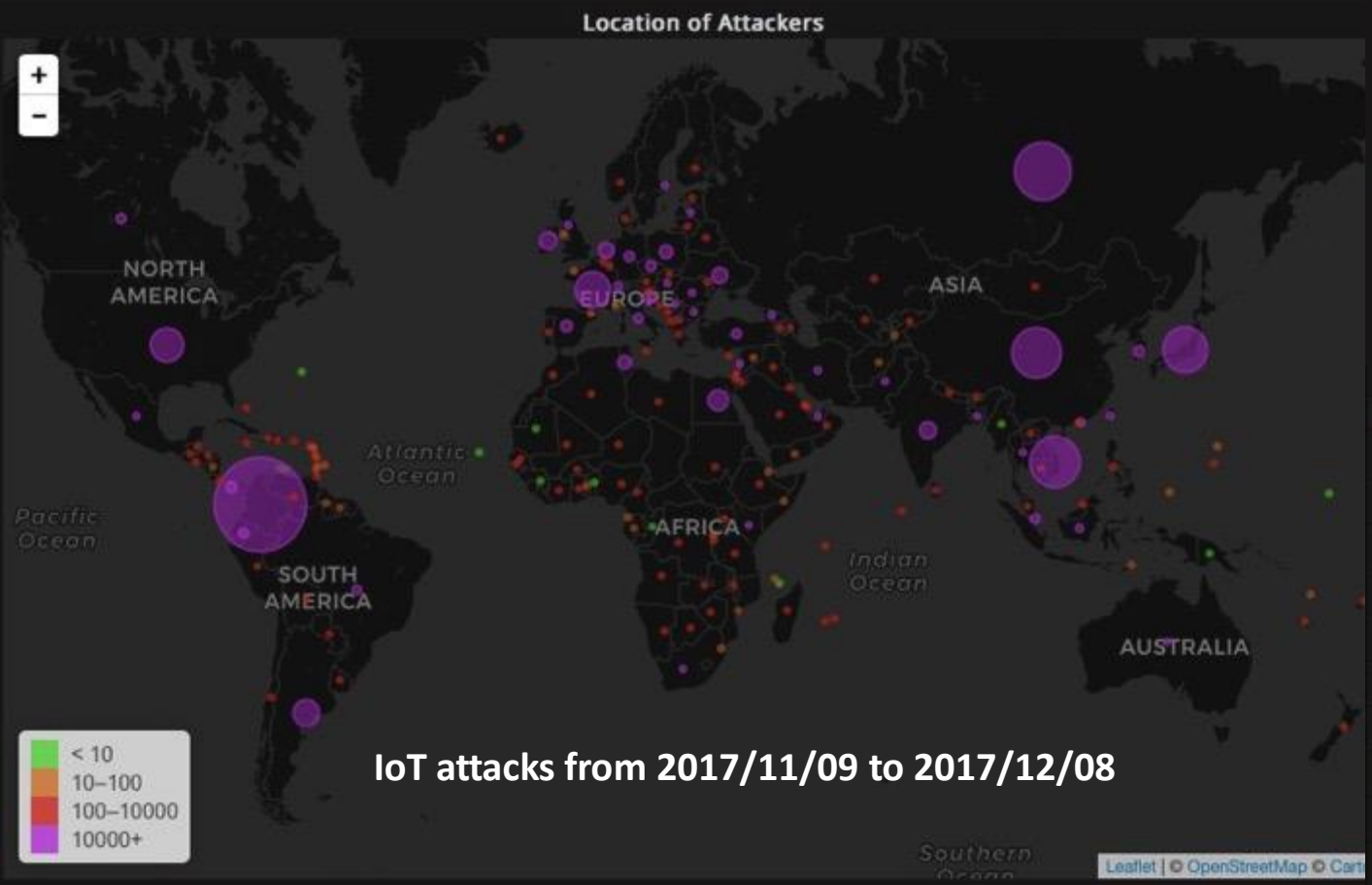


Global Underground Research

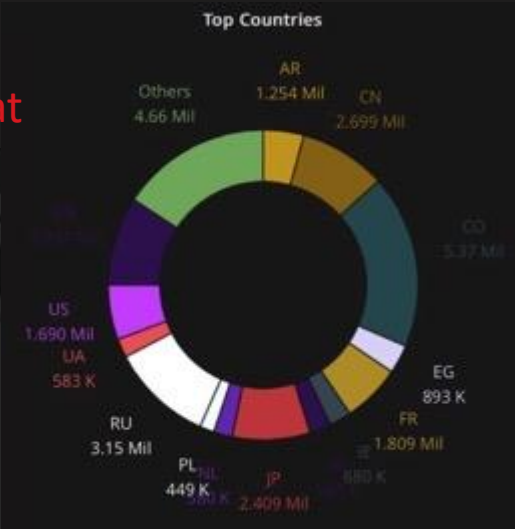




IoTRS Dashboard - Monitor the trend of global IoT threat



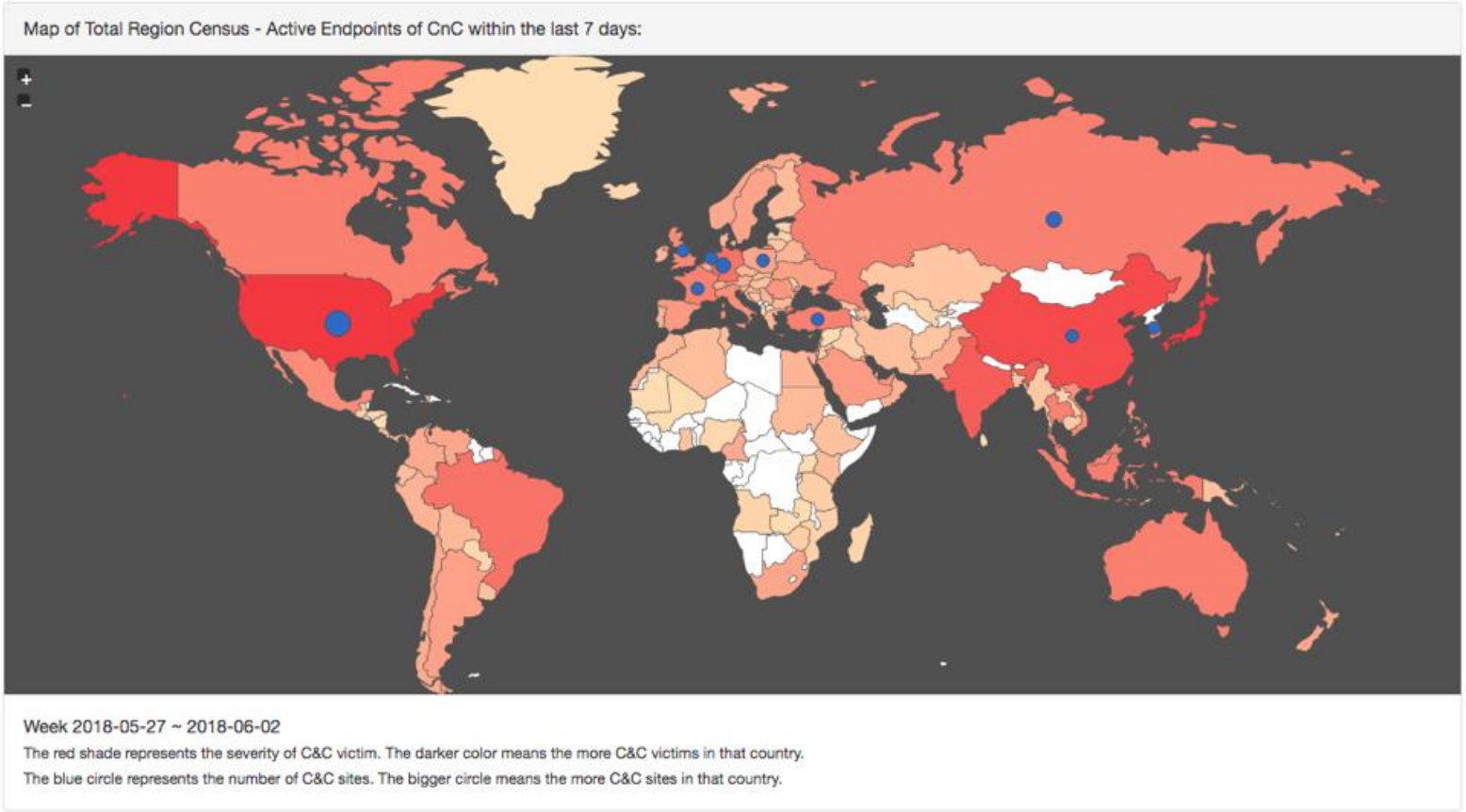
IoT attacks from 2017/11/09 to 2017/12/08



Top Attackers

IP	Country	Amount
185.188.207.12	RU	833.37 K
95.213.170.195	RU	321.78 K
185.13.37.96	FR	295.08 K
109.248.9.108	RU	271.98 K
193.201.224.206	UA	258.26 K
5.188.10.144	HR	258.25 K
195.22.127.83	PL	243.87 K
109.236.91.85	NL	239.95 K
195.154.151.12	FR	151.93 K
14.160.13.174	VN	151.80 K

Command & Control Research



- Dedicated researchers
- Internal/external C&C sourcing channels
- Pre-filtering automation before involving human analysis
- Query some internal/external services

Security Predictions

The Next Tier

The plateau of ransomware, more business process compromise, and the boom of cyberpropaganda–what big security concerns should we expect in 2017?

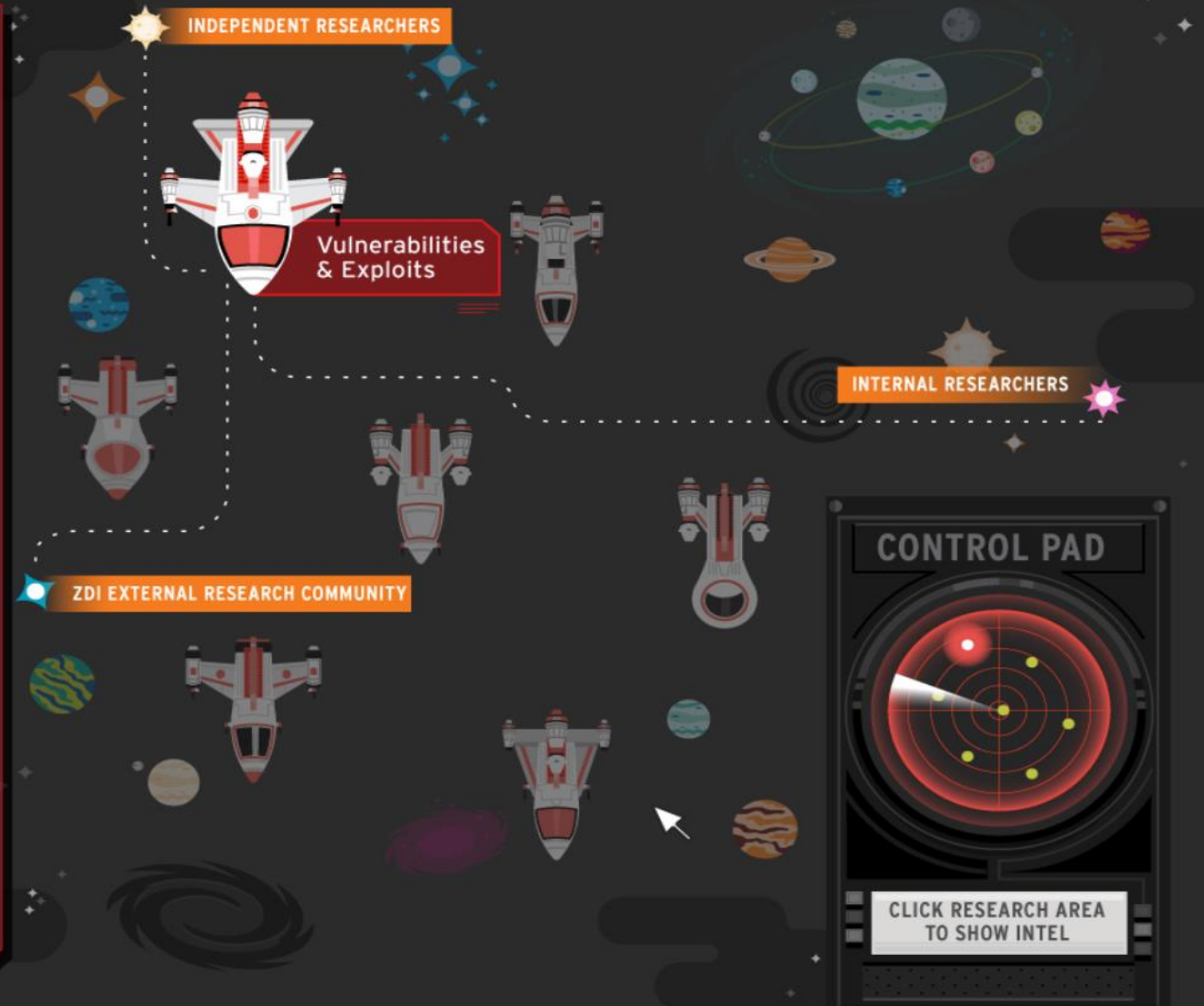
Vulnerabilities & Exploits

The Trend Micro Zero Day Initiative (ZDI) manages a bug bounty program where thousands of global security researchers inside and outside of Trend Micro discover and submit new vulnerabilities.

ZDI then manages the disclosure process with the affected vendor to ensure a patch can be created and deployed by the vendor in a responsible manner. ZDI covers many areas, including operating systems and applications across consumer and commercial software and mobile platforms. Part of the research is also understanding exploit code used by threat actors. As a security vendor, having this pre- and post- patch research allows us to quickly protect against these vulnerabilities.

For example, through information from the ZDI program, Trend Micro's TippingPoint product provides a virtual patch for a vulnerability on average 72 days before the vendor releases their formal patch. This minimizes the window of exposure the organization has against an exploit of the vulnerability. In 2017, ZDI disclosed 66.3% of the known vulnerabilities disclosed by the top reporting agencies in the world.*

*Read the complete analysis here.



Global Threat Intelligence

GLOBAL SENSOR NETWORK

Collects more threat information in more places

- 250M+ of sensors
- 3T+ Threat queries yearly
- Files, IPs, URLs, mobile apps, vulnerabilities, and more

GLOBAL THREAT INTELLIGENCE

Accurately analyzes and identifies threats faster

- TBs analyzed
- 6B+ new, unique threats identified yearly
- Advanced Analytics to detect real-time, 0-hour threats

PROACTIVE PROTECTION

Blocks new threats sooner

- 65B+ threats blocked yearly
- 500,000+ business
- Millions of individuals and families

2017 Trend Micro Zero-Day Coverage

512

TOTAL number of **zero-day filters** delivered in 2017 to Trend Micro customers

37.4% of all 2017 filters delivered were zero-day!

50

LARGEST number of zero-day filters delivered in a **single Digital Vaccine package**

42 DAYS

AVERAGE of zero-day predisclosed filter coverage for 2017 **Microsoft** Bulletins

~ 6 weeks of zero-day coverage on average!

63 DAYS

AVERAGE of zero-day predisclosed filter coverage for 2017 **Adobe** Bulletins

Over 2 months of zero-day coverage on average!

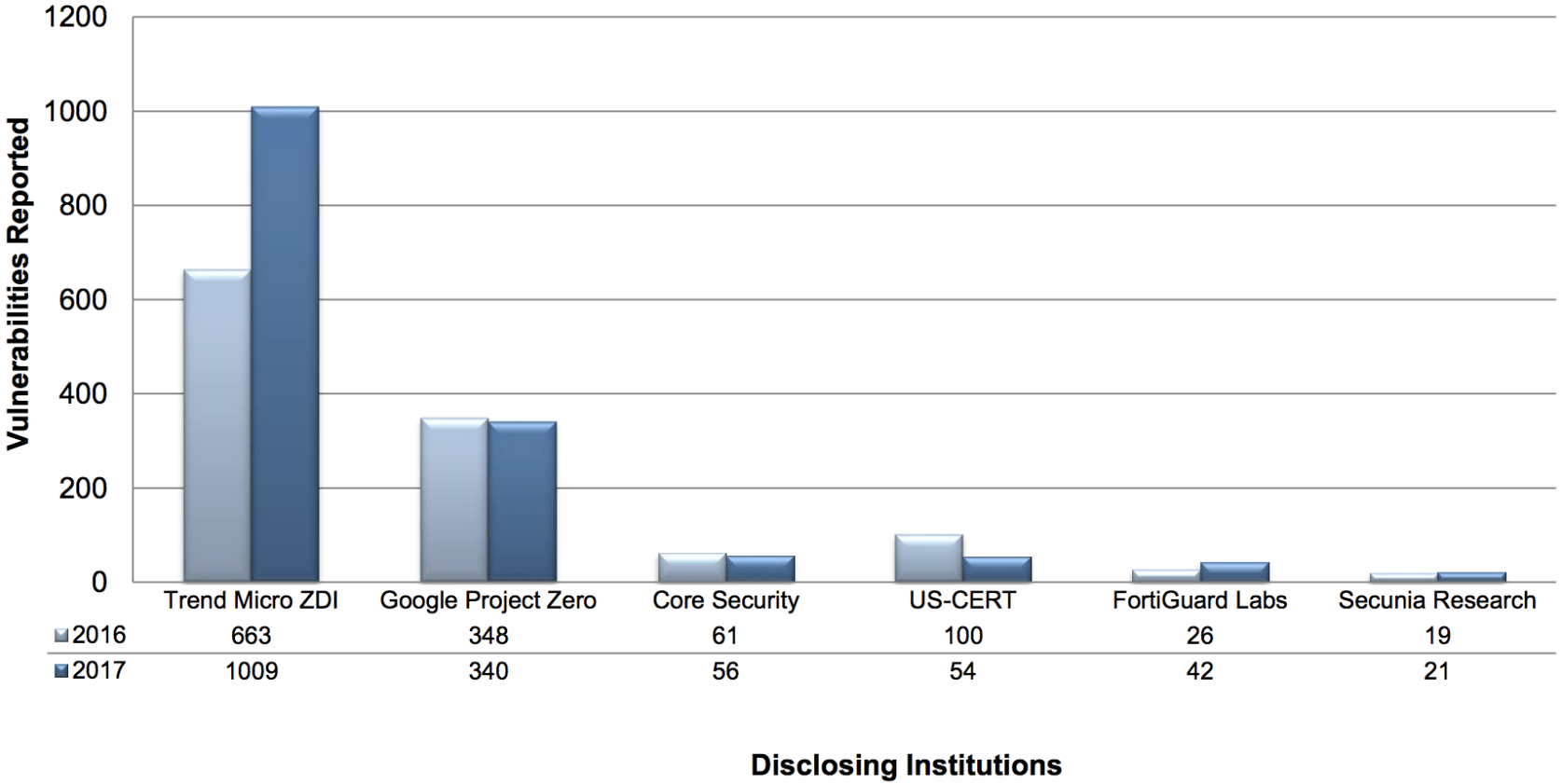
72 DAYS

AVERAGE of zero-day predisclosed filter coverage for 2017 **OVERALL**

~ 2½ months of zero-day coverage on average!

Disclosed 1009 vulnerabilities!

Public Vulnerability Research Market: Total Vulnerabilities by Disclosing Institutions, Global, 2016 and 2017



	Trend Micro ZDI	Google Project Zero	Core Security	US-CERT	FortiGuard Labs	Secunia Research
2016	663	348	61	100	26	19
2017	1009	340	56	54	42	21

Note: All figures are rounded. The base year is 2017. Source: Frost & Sullivan analysis.

Smart Protection Network in 2017

… received 3T+ reputation queries from customers

… blocked 65B+ total threats

… identified 6B+ new, unique threats

… Blocked 600M+ ransomware threats

TREND MICRO SMART Protection Network™

2017 Stats

Threat Queries to Trend Micro

28 Billion
Malicious App

106 Billion
Email

HTTPS **2.2 Trillion** Web

631 Billion File

TREND MICRO

TREND MICRO SMART Protection Network™

2017 Stats

Threats Blocked by Trend Micro

58 Million
Malicious Apps

1 Billion
Malicious URLs

58 Billion Email Threats

7 Billion Malicious Files

TREND MICRO

Threat Connect

Welcome to Threat Connect Internal Test Bed

This test bed is to be used only for testing activities by authorized Trend Micro personnel. Do not share access to this test bed with external parties.

Use the given examples or specify your own query parameters.		Examples
Detection Name:	Trend Micro detection name	PE_RAMNIT.DEN
File SHA-1:	SHA1 hash value	aa244ec0ab9c8073d194e954c429e1aadae48895
File MD5:	MD5 hash value	1f68490f559ba30210a8b2422557489f
IP Address:	IP address	59.120.54.79
FQDN:	Domain name	keyscratch.com
URL:	URL	http://synapsetest.ru/analizer/dtmf000/config.php
CVE:	CVE	CVE-2015-5122
Email Address:	Email address	0015gh@opqueqcnc.com
Mutex Name:	Mutex name	uxJLpe1m
Attacker Group:	Name of attacker group monitored by Trend Micro	F-Cross, LAH
DDI Rule ID:	Detection rule ID of Deep Discovery Inspector	255

Send Query Reset

Thanks

TMHK@TRENDMICRO.COM.HK