TREND MICRO™

Securing Your Journey to the Cloud

Building Castles in the Sky:
Advanced Persistent Response

JOIN THE JOURNEY

Raimund Genes
CTO

Reality Check

- **52% of companies failed to report or remediate a cyberbreach in 2011.**

  SAIC, 2011

- **Two new pieces of malware are created every second.**

  Trend Micro, 2012

- **A cyber intrusion occurs every 5 minutes.**

  US-CERT 2012

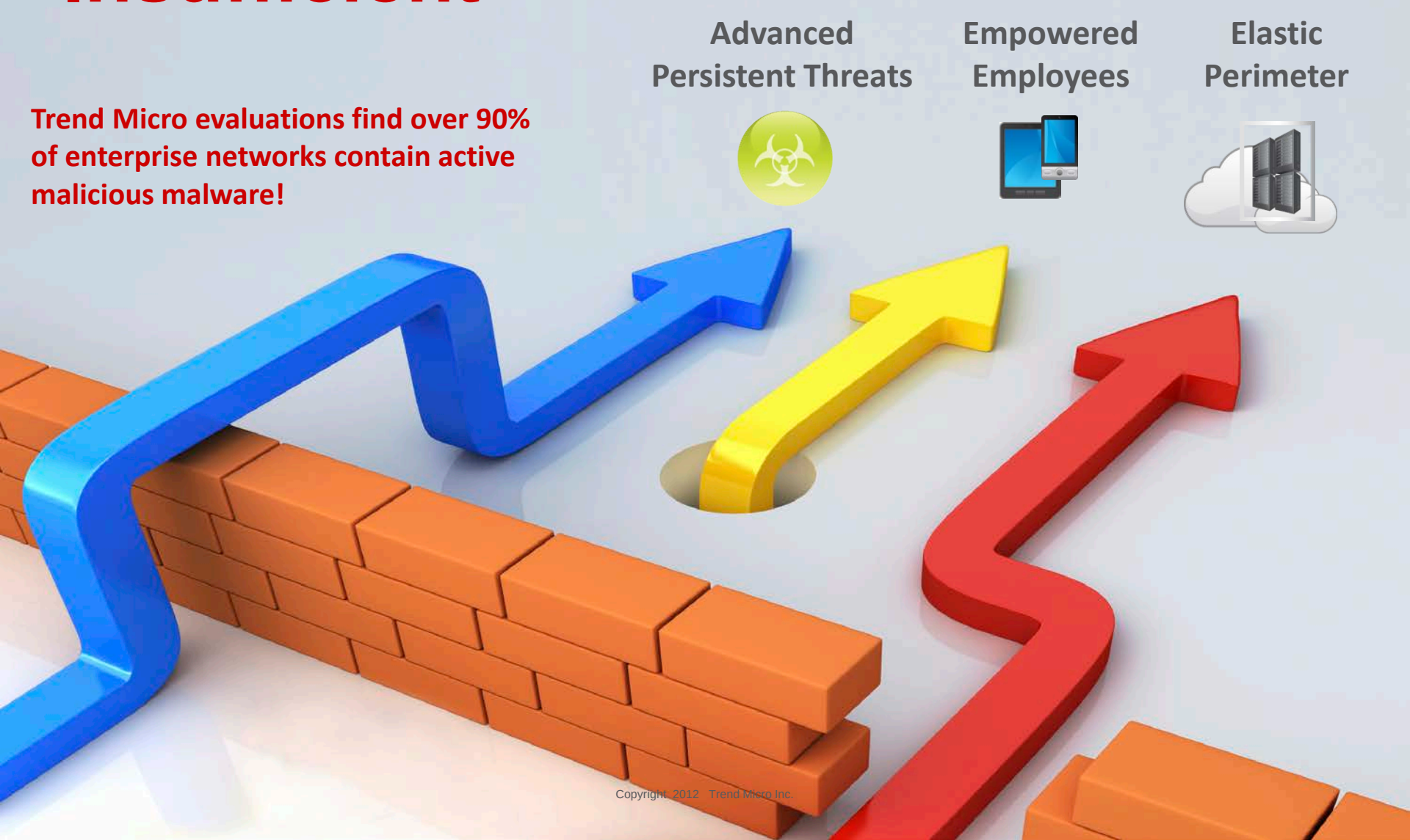
JOIN THE JOURNEY

Q1 Emerging Threats

- **Professionalization, and Commoditization of Exploit Kits. i.e.** BlackHole Exploit Kit.
- **Modularization:** We have also observed a high degree of modularization in more advanced malware like SpyEye.
- **Increased Sophistication with Traffic Direction Systems (TDS):** Traffic Direction Systems (TDS) are used as initial landing pages, also known as “doorway pages,” which direct traffic to content based on a variety of criteria such as operating system, browser version, user agent, and geographic location.
- **Continued Exploitation of Social Networks.**
- **New Exploitation Vectors Introduced via HTML5.**
- **Evolution of Mobile Threats.**

Traditional Security is Insufficient

Trend Micro evaluations find over 90% of enterprise networks contain active malicious malware!



APTs and Targeted Attacks

RSA, Sony, Mitsubishi, CitiGroup, Zappos … show power of targeted attacks

Stuxnet, DUQU, and 100's of attacks on company IP around the globe…

GhostNet: Vast Spy System Loots Computers in 103 Countries

Wikileaks & Anonymous– – Who's Next?

Trend Micro finds over 90% of enterprise networks contain active malicious malware

A Cyber Intrusion Every 5 Minutes… according to US-CERT

LUCKYCAT

- Victims and Targets

APT campaigns target specific industries or communities of interest in specific regions.

The Luckycat campaign has been linked to 90 attacks against the following industries and/or communities in Japan and India:


AEROSPACE


ENERGY


ENGINEERING


SHIPPING


MILITARY RESEARCH


TIBETAN ACTIVISTS

The threat actors behind the Luckycat campaign used a unique campaign code to track victims of specific attacks.

LuckyCat: Targeted Attacks

- A series of computer intrusions staged by threat actors that:
  - Aggressively pursue and compromise specific targets
    - Often leveraging social engineering
  - Maintain a persistent presence within the victim's network
  - Escalate privilege and move laterally within the victim's network
  - Extract sensitive information to locations under the attacker's control

Cyber Weapons Bazaar

JOIN THE JOURNEY

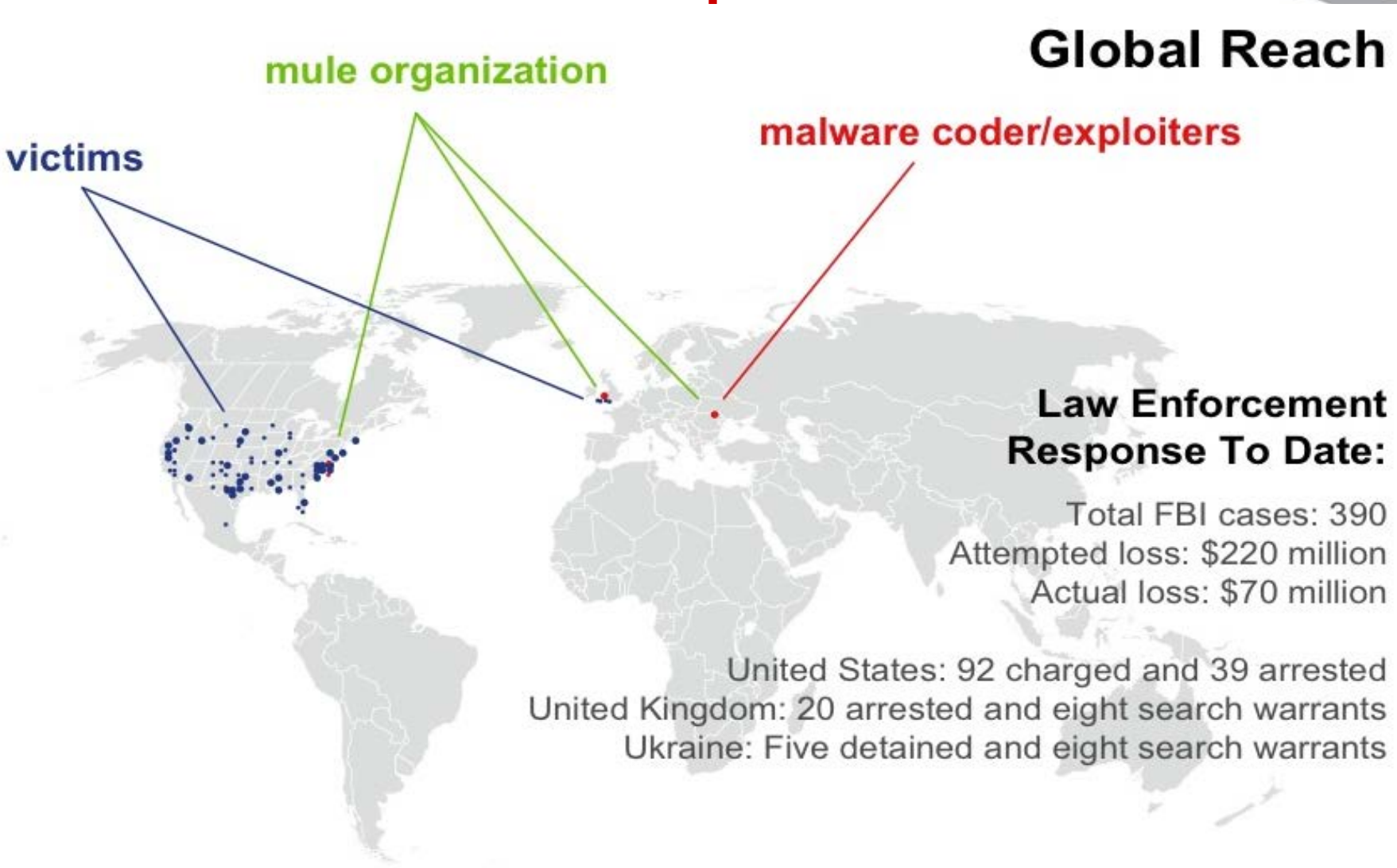
Offense Informs Defense: The Kill Chain

1. **Reconnaissance**
2. **Weaponization**
3. **Delivery**
4. **Exploitation**
5. **Command and Control**
6. **Propagation**
7. **Exfiltration**
8. **Maintenance**

Malware / Bot / APT Behavior Comparison Table

	APT	Bot	Malware
Distribution	With organized planning	Mass distribution over regions	Mass distribution over regions
Services interruption	No	No	Yes
Attack Pattern	Targeted (only a few groups/organizations)	Not targeted (large area spread-out)	Not targeted (large area spread-out)
Target Audience	Particular Organization/Company	Individual credentials including online banking account information	Random
Frequency of attacks	Many times	Once	Once
Weapon	-Zero-day exploit -Drop embedded RAT -Dropper or Backdoor	Multiple-Exploits, All in one	By Malware design
Detection Rate	Lower than 10%, if the sample comes out within one month	Around 86%, if the sample comes out within one month	Around 99%, if the sample comes out within one month

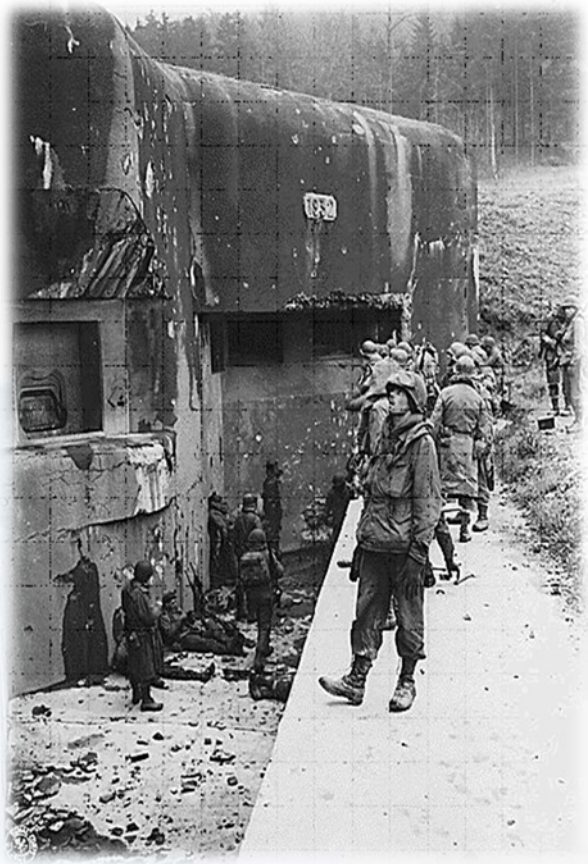
Shadow Economics: Mariposa



From Stuxnet to DUQU

JOIN THE JOURNEY

BYOD aka BYOM



The attack pathway/vector of choice is via remote access accounts.

External agents target applications and end-users most of the time.

Threat Action types post exploitation:

-Send data to external entity

-Backdoor

-Command and control

-Credential theft and exploitation

JOIN THE JOURNEY

How bad is it?

Home / News & Blogs / Hardware 2.0

Report: Mobile malware to affect more than 1 in 20 devices within 12 to 24 months

By Adrian Kingsley-Hughes | July 12, 2011, 5:40am PDT

Summary

Within 12 to 24 months over 1 in 20 (5.6%) of all

Within 12 to 24 months over 1 in 20 (5.6%) of all Android phones and iPads/iPhones could become infected with mobile malware if fraudsters start to integrate zero-day vulnerabilities into leading exploit kits, claims security firm Trusteer.

400 Percent Increase In Android Malware; Mobile Security Threats At Record High

MATT BURNS | Tuesday, May 10th, 2011 | 2 Comments

Juniper Networks today released a study concerned with potential threats to mobile technology, revealing a 400 percent increase in Android malware. The study also found that both enterprise and consumer mobile devices are being exposed to a record number of security threats, including highly targeted Wi-Fi attacks.

0

More Android Security Concerns

Posted by Sue Marquette Poremba Jul 4, 2011 10:35:39 AM

Once again, the security surrounding Google's products is being discussed.

On a personal level, I'm always a bit concerned whenever I see any article that combines the phrases "Android" and "Security Threat." I'm one of those people **PC World** said helped Android climb "to the top of the mobile OS mountain," and I'd really like to be sure that my Android smartphone is secure.

Five Top Mobile Device Risks and How to Protect Your Business

APRIL 2011		APRIL 2012
100M	**User Base** Substantial increase in the use of Android based mobile phones. *Global	300M
36.4%	**Android Market Share** Aggressive growth of Android Market Share. *U.S. Numbers only	50.1%
200k	**Available Applications** The increasing number of available apps in Google Play. *Not including 3rd party APP stores	500k
37.8%	**Application Use** The increasing number of people downloading and using APPs on their device. *US Only	49.5%
39.1%	**Browser Use** The increasing number of people using a browser on their device. *US Only	49.2%
28%	**Social Networking Use** The increasing number of people using social networking or blogging sites & APPS. *US Only	36.1%

JOIN THE JOURNEY

APRIL 2011		APRIL 2012
TENS	**Device Permutations** Vendors are aggressively releasing new device versions resulting in unique device & O/S permutations that will need to be managed in the future	HUNDREDS
14	**Android O/S Versions** Substantial growth in the number of unique Android Operating System versions that will need to be separately managed in the future	28
2	**Vulnerabilities** Reported vulnerabilities in Android OS	20
> 6 MONTHS	**Time To Patch Vulnerabilities** With the current ecosystem that exists between Manufacturer, Carrier, Google, patching vulnerabilities on phones is a dangerously slow procedure	> 6 MONTHS
20	**Malware** The number of malicious code attacks has significantly increased over the past year	11,000
	Criminal Knowledge of O/S Being open source, the Android O/S can easily be analyzed and exploited by any criminal with the right motivations. As time progresses, criminals will continue to repurpose their existing revenue models to exploit mobile platforms	

Feb
7

Trending Scams Seen in the Android Market

11:49 am (UTC-7) | by Kervin Alintanahin (Threats Analyst)

Shortly after we reported about a fake *Temple Run* app in the *Android Market*, we were alerted to yet another developer that uses popular apps as guises to trick users into downloading rogue apps.

Here, you can see the developer's name which appears to be quite similar to the one who developed the popular game, Angry Birds. You'll notice, though, that the said popular game is not on the list of this particular developer's offered apps.

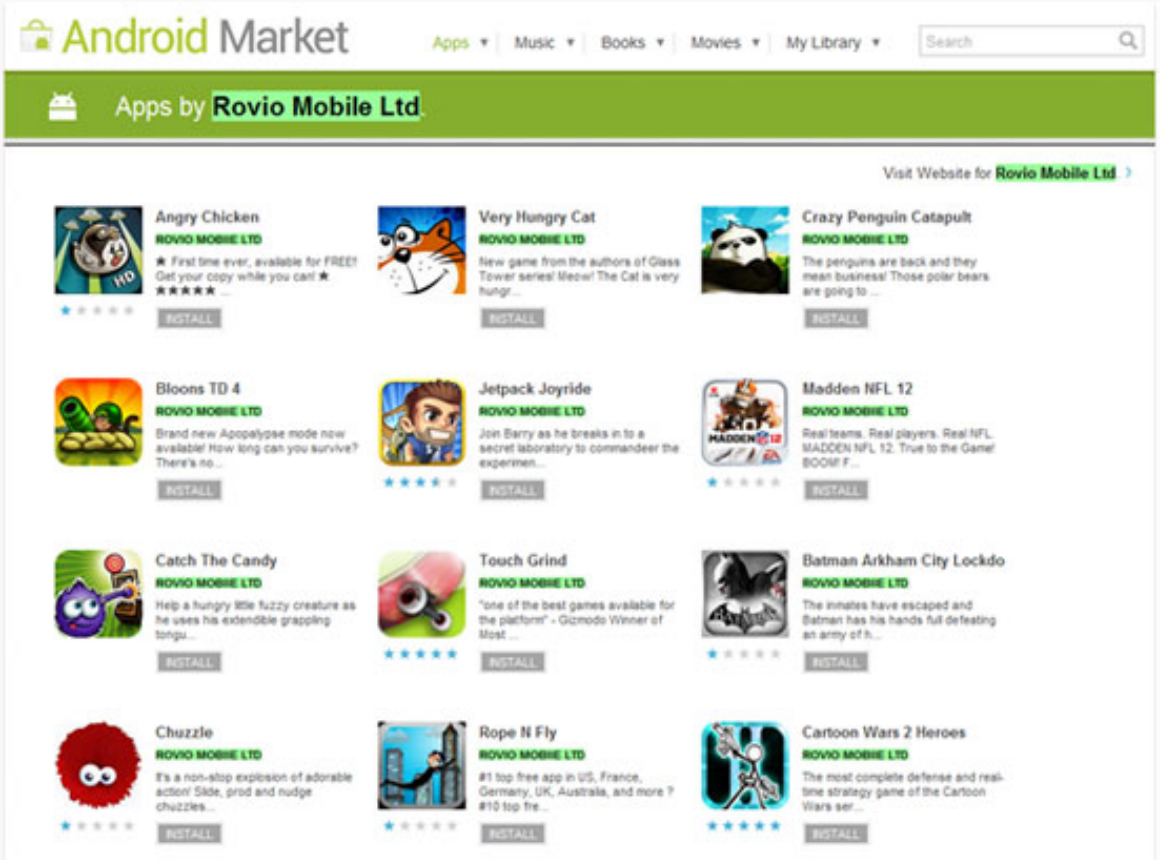


Figure 1. Apps supposedly offered by Rovio Mobile Ltd.

Mobile Spyware

ANDROIDOS_NICKISPY.C is capable of collecting data such as text messages, call logs, and GPS location from infected devices, which it then uploads to a certain URL through port 2018.

Like other ANDROIDOS_NICKISPY variants, ANDROIDOS_NICKISPY.C also has the capability to record phone calls made from infected devices. What makes this particular variant different is that it has the capability to automatically answer incoming calls.

Figure 2. The malicious app installed as "Google++"

http://blog.trendmicro.com/android-malware-eavesdrops-on-users-uses-google-as-disguise/

JOIN THE JOURNEY

Android Malware

http://blog.trendmicro.com/how-big-will-the-android-malware-threat-be-in-2012/

- 10K: Middle of 2012!
- 100K: End of 2012!

JOIN THE JOURNEY

A New Security Paradigm

- The way to address these is to apply providing **advanced situational awareness** in real time so as to manifest deep security.
- The solution resides in building better dungeons rather than castles in cyberspace.
- Ask yourself: How can we increase the level of discomfort to the adversary?

JOIN THE JOURNEY

2012 Predictions

1. **Mobile Malware** – continued strategic shift of attention from traditional platforms to mobile devices.

2. **Application Attacks** – switch from targeted attacks on the OS toward the application layer via browser (Adobe, Java) with social engineering.
3. **Botnet Migration** – migration from IRC botnets to HTTP botnets which double in size every 18 months.

4. **Cloud Attacks** – hacking into one central location where all data is kept.

JOIN THE JOURNEY

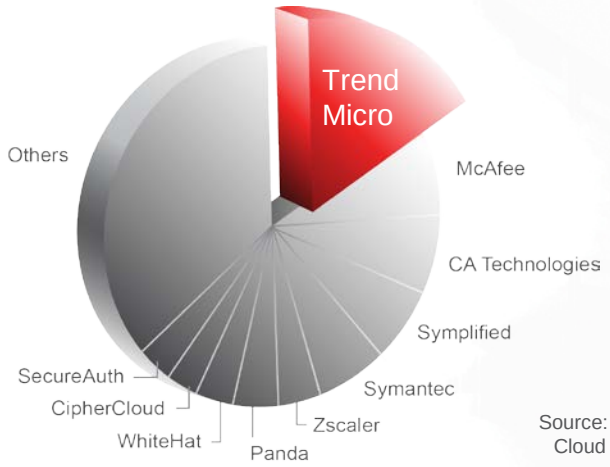
Risk Assessment 2012

1. How many third parties provide services to organization? Has their cyber security posture been audited?
2. Is access to all sensitive systems and computers governed by two factor authentication?
3. Does a log inspection program exist? How frequently are they reviewed?
4. Do you run web application scanners to simulate an attack of the website and determine its security?
5. Does file integrity monitoring exist?
6. Can vulnerabilities be virtually patched?
7. When is the last time the organization conducted a penetration?
8. Does a mobility risk management policy exist? Is Mobile Application Management software utilized?
9. Has a cloud security strategy been crafted? Can you migrate your layered security into the cloud environment?

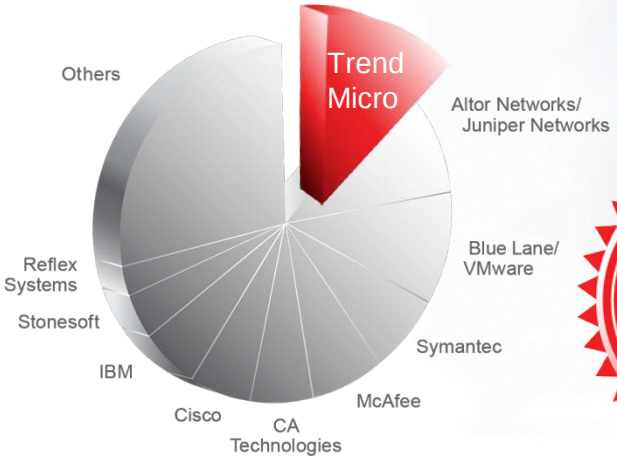
Trend Micro: Securing your journey to the cloud

JOIN THE JOURNEY

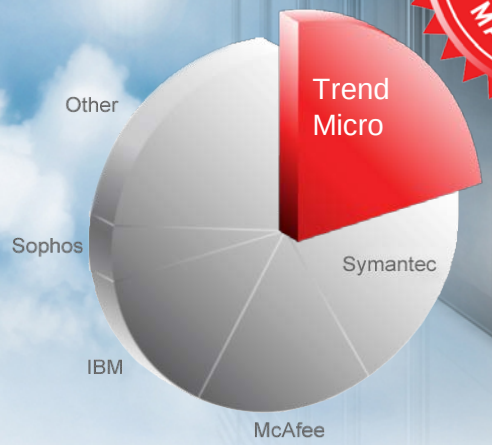
Trend Micro #1: Securing Your Journey to the Cloud



Source: 2012 Technavio – Global Cloud Security Software Market



Source: 2011 Technavio – Global Virtualization Security Management Solutions



Worldwide Endpoint Security Revenue Share by Vendor, 2010
Source: IDC, 2011

TREND MICRO

TREND MICRO™

Securing Your Journey to the Cloud

SECURING YOUR JOURNEY TO THE CLOUD

physical. virtual. cloud.