Spinning the Chess Board

Tom Kellermann, CISM
Chief Cybersecurity Officer, Trend Micro

Copyright 2014 Trend Micro Inc.

2014 to 213 BC

Connected Devices Outnumber People

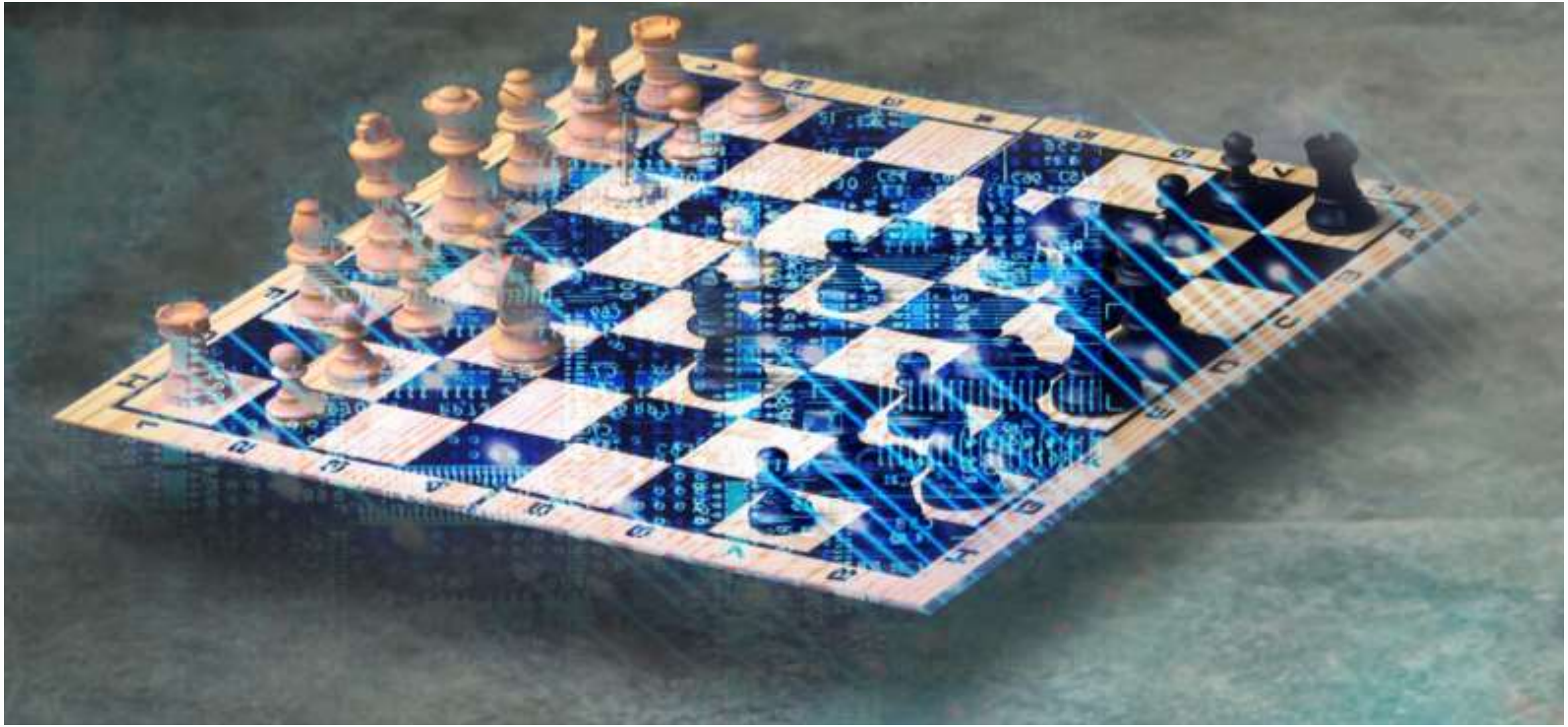
220,000

NEW malware programs EVERY day!

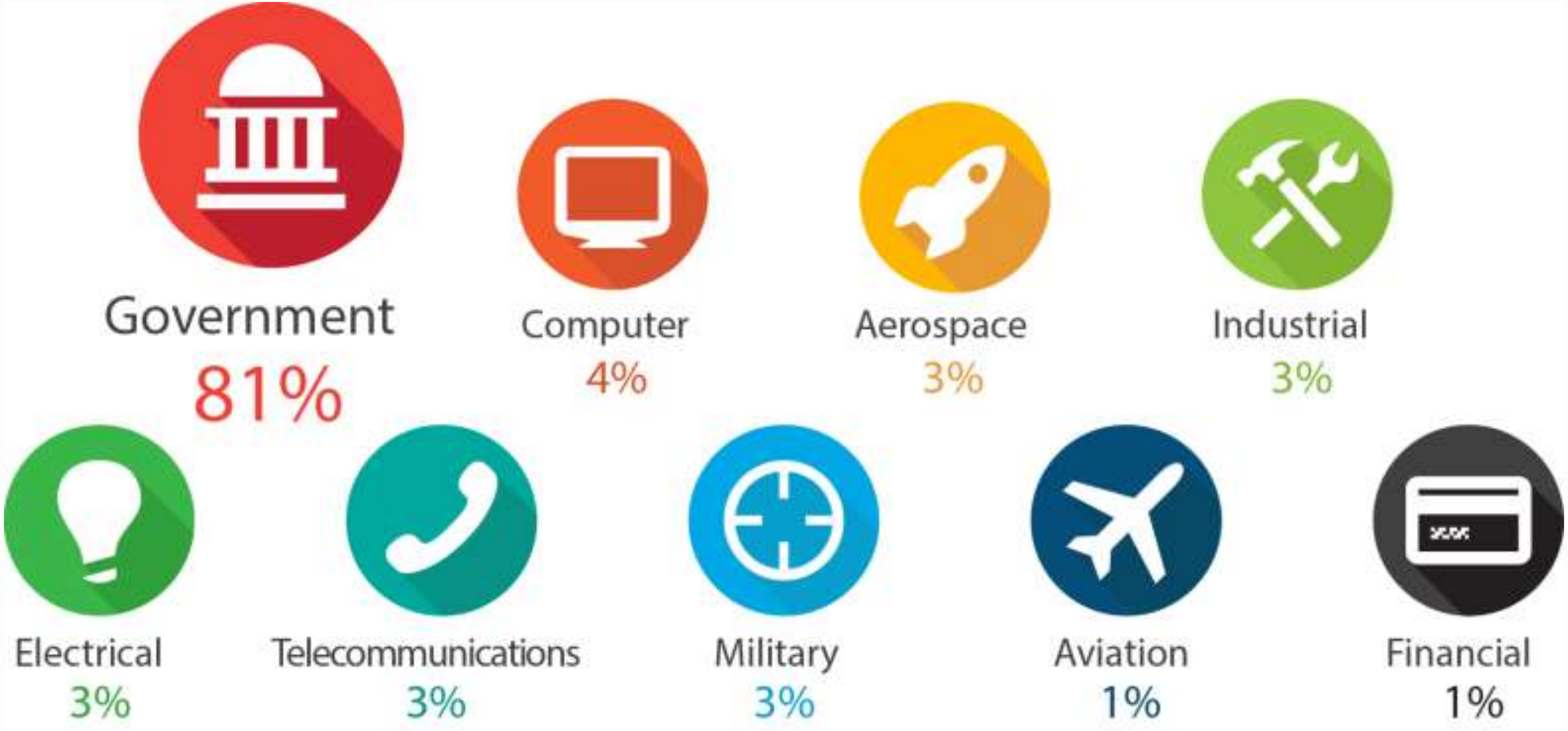
Employee Data Leaks → Traditional Malware → Vulnerability Exploits → Advanced Malware → Targeted Attacks

Source: AVTest.Org

Offense Must Inform Defense



Q2 Industry Attack Campaigns



Government	81%
Computer	4%
Aerospace	3%
Industrial	3%
Electrical	3%
Telecommunications	3%
Military	3%
Aviation	1%
Financial	1%

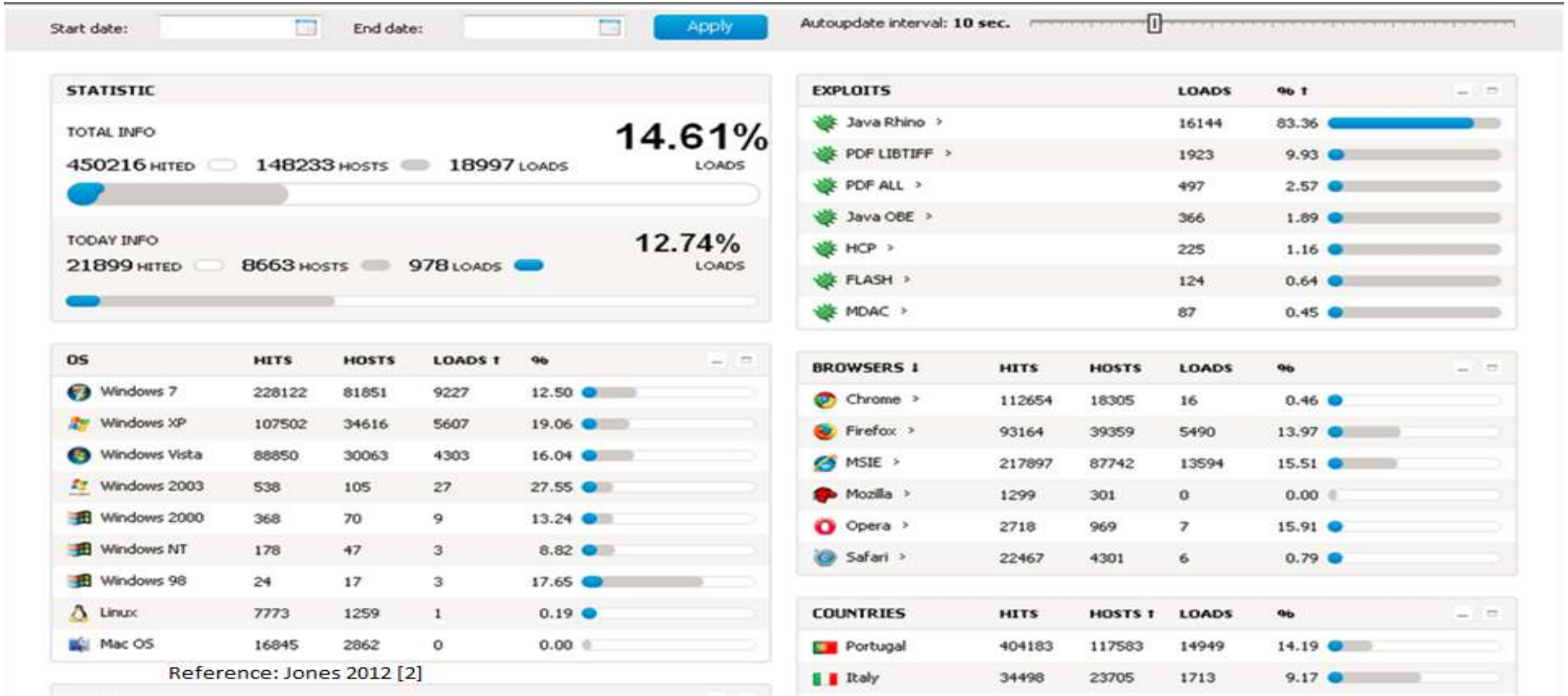
Who Are We Up Against?

Arms Bazaar of Attack Code

Menu for Full Service Hacking

	monthly	onetime
VPN Service	$25	$0
Botnet Framework	$40	$125
Bulletproof hosting	$52	$0
Exploit Kit	$38	$120
	$0	$20
Domain names	$70	$25
Dropper file and crypt	$8	$80
Modules	Total: $225	$370

Exploit Kits: Do-it-Yourself



Autoupdate interval: **10 sec.**

STATISTIC

TOTAL INFO

450216 HITED 148233 HOSTS 18997 LOADS

14.61% LOADS

TODAY INFO

21899 HITED 8663 HOSTS 978 LOADS

12.74% LOADS

OS	HITS	HOSTS	LOADS ↑	%
Windows 7	228122	81851	9227	12.50
Windows XP	107502	34616	5607	19.06
Windows Vista	88850	30063	4303	16.04
Windows 2003	538	105	27	27.55
Windows 2000	368	70	9	13.24
Windows NT	178	47	3	8.82
Windows 98	24	17	3	17.65
Linux	7773	1259	1	0.19
Mac OS	16845	2862	0	0.00

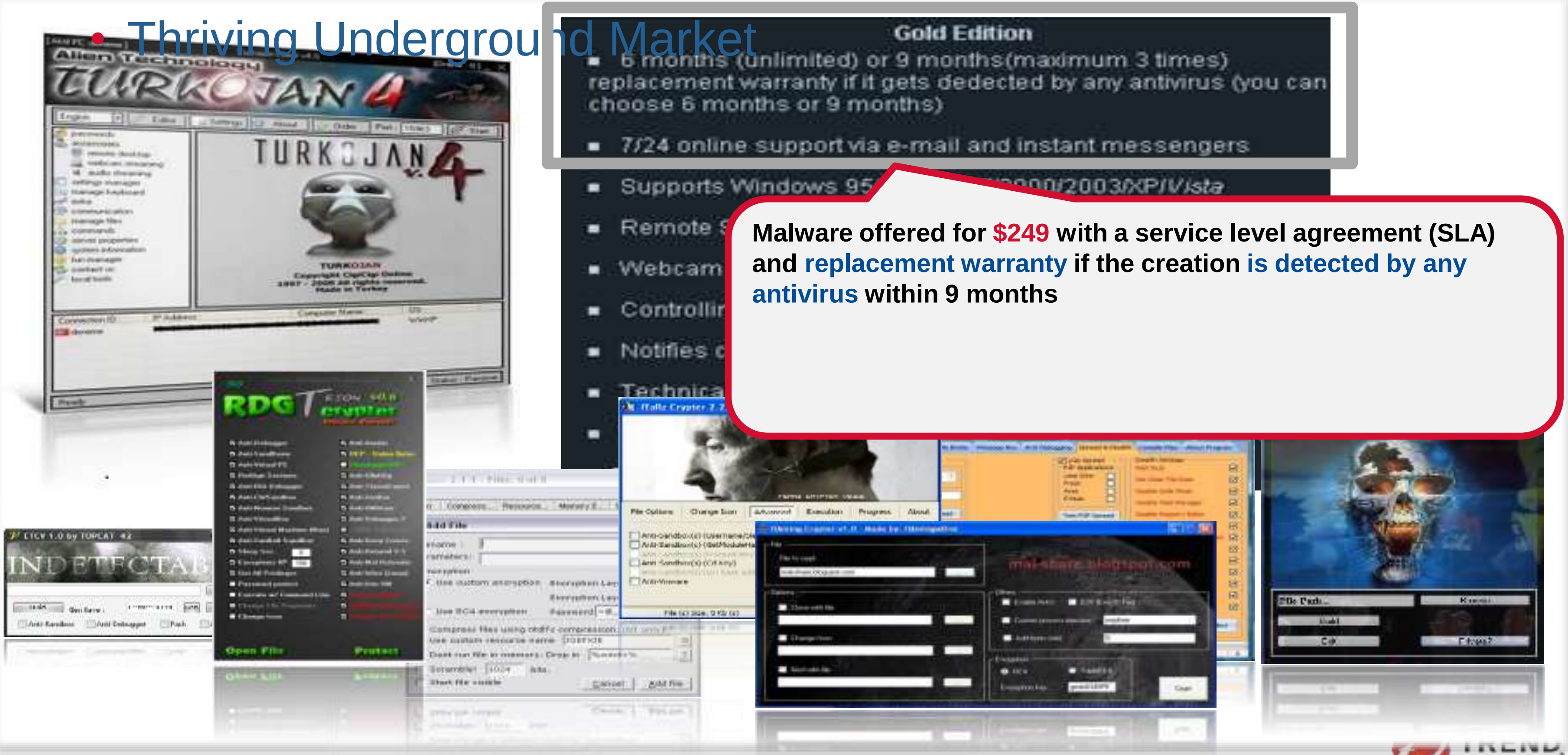
EXPLOITS	LOADS	% ↑
Java Rhino ›	16144	83.36
PDF LIBTIFF ›	1923	9.93
PDF ALL ›	497	2.57
Java OBE ›	366	1.89
HCP ›	225	1.16
FLASH ›	124	0.64
MDAC ›	87	0.45

BROWSERS ↓	HITS	HOSTS	LOADS	%
Chrome ›	112654	18305	16	0.46
Firefox ›	93164	39359	5490	13.97
MSIE ›	217897	87742	13594	15.51
Mozilla ›	1299	301	0	0.00
Opera ›	2718	969	7	15.91
Safari ›	22467	4301	6	0.79

COUNTRIES	HITS	HOSTS ↑	LOADS	%
Portugal	404183	117583	14949	14.19
Italy	34498	23705	1713	9.17

Reference: Jones 2012 [2]

- Thriving Underground Market

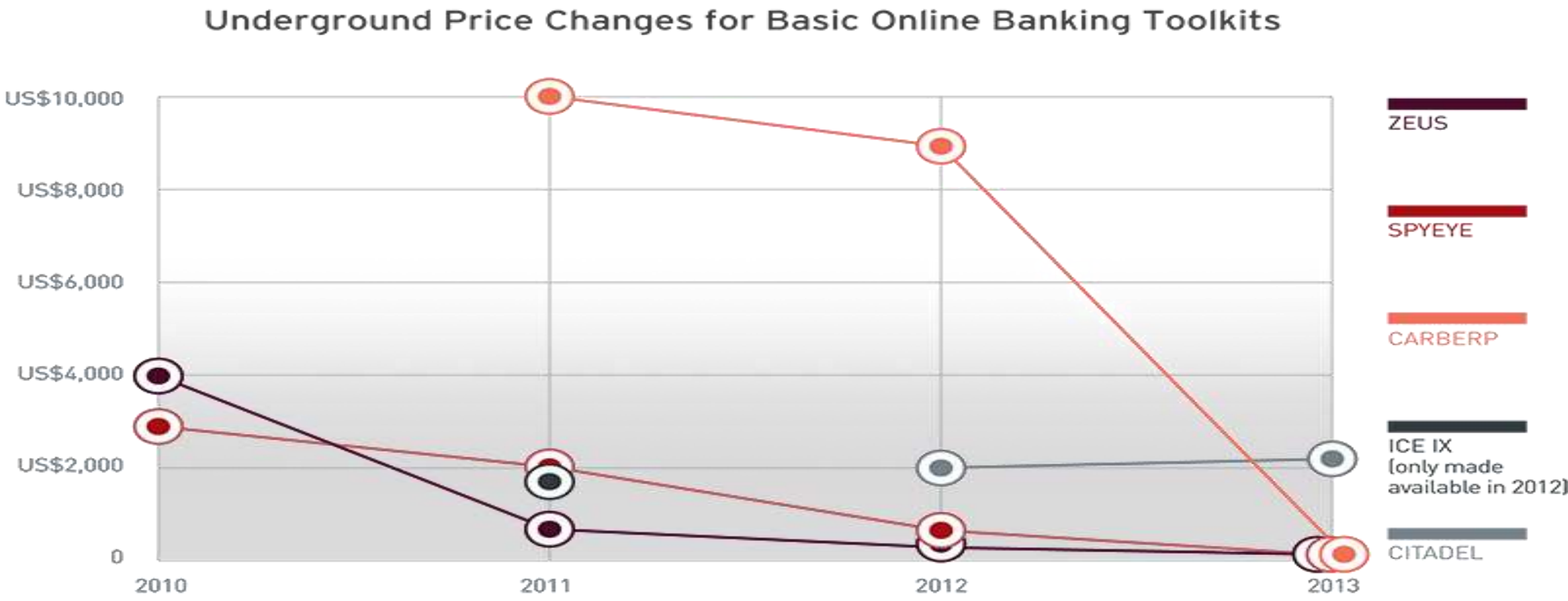


Gold Edition

- 6 months (unlimited) or 9 months(maximum 3 times) replacement warranty if it gets dedected by any antivirus (you can choose 6 months or 9 months)
- 7/24 online support via e-mail and instant messengers
- Supports Windows 95/2000/2003/XP/Vista
- Remote S
- Webcam
- Controllin
- Notifies c
- Technica

Malware offered for $249 with a service level agreement (SLA) and replacement warranty if the creation is detected by any antivirus within 9 months

Banking Crimekits Decrease in Price



Underground Price Changes for Basic Online Banking Toolkits

These are estimated going rates.
Note that ZeuS and SpyEye have been around since before 2010.

GameOverZeus: GOZ

Zberb

A Comparison of Russian and Chinese Hackers

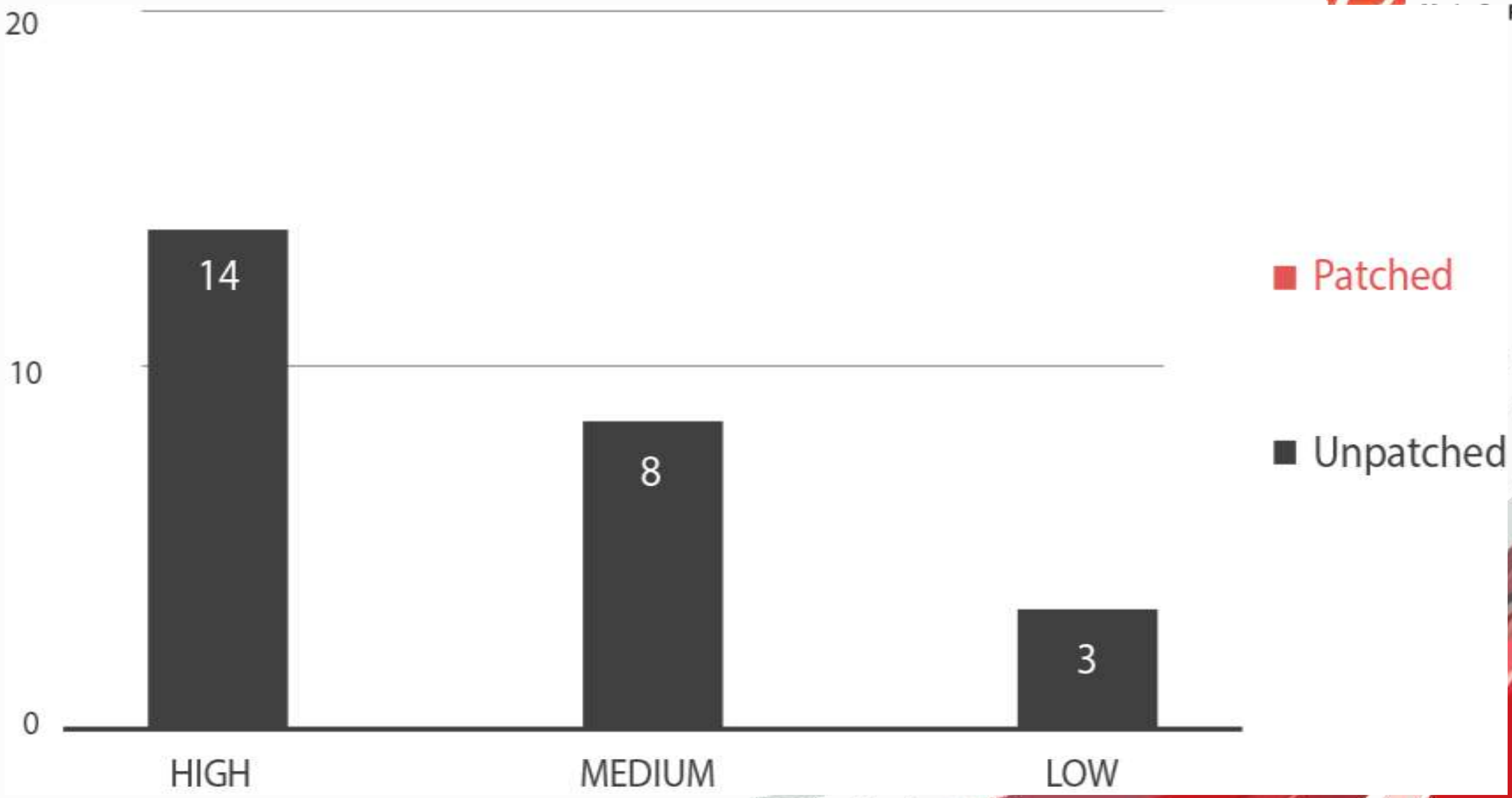
Weapons Grade Arsenal

- Greater reconnaissance
- Utilization of 0-days
- Undetectable by anti-virus
- Able to withstand normal disinfection methods like reinstalling OS
- Calling home is undetected by DLPs and IPS/IDS
- Data extraction, command and control even across an air gap

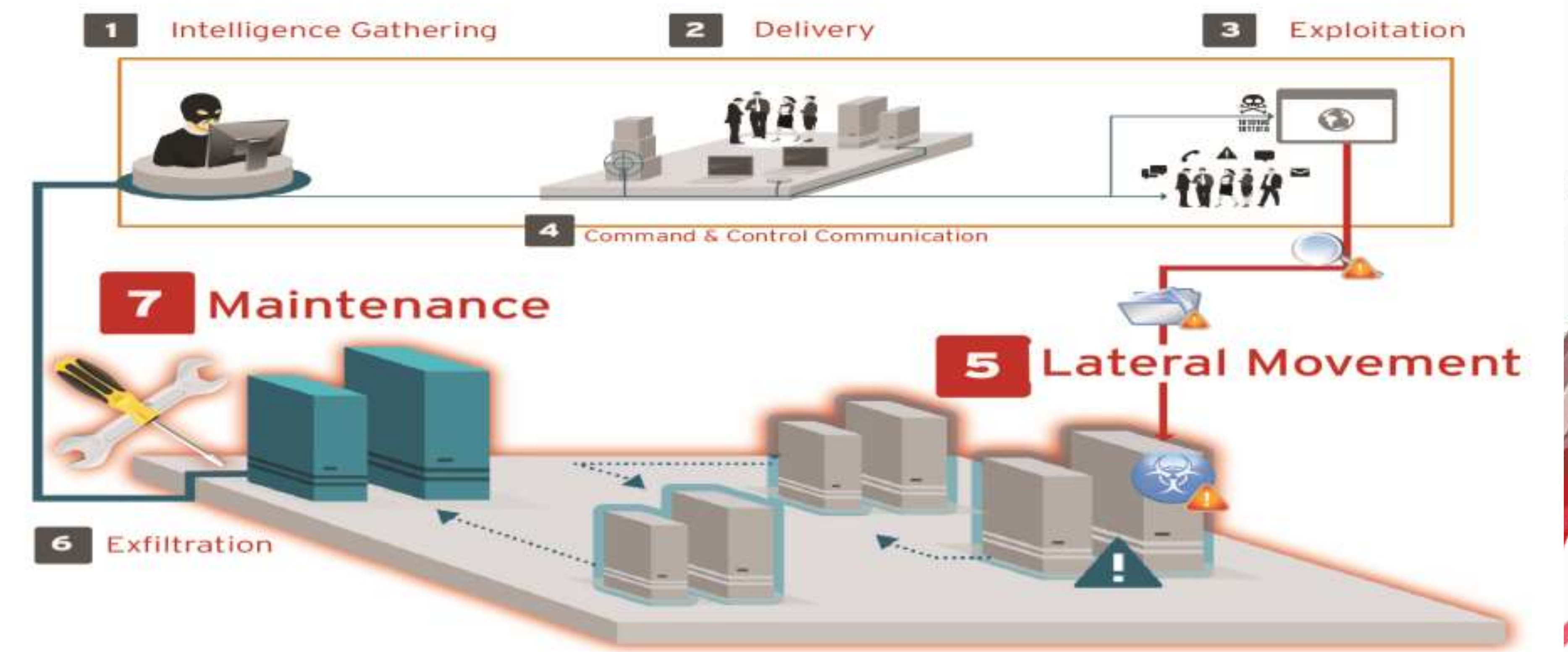
What are the Trends of Attack?

Java
Java
Java
Java
Java
Java

Q2 Serious Java Vuls



Offense Must Inform Defense



Exfiltration: Most Used APPs and Protocols

Evasions

- Packers
- Compressors
- Metamorphism
- Port Binding
- Polymorphism
- Virtual Machine
- Sandbox

Dropping In

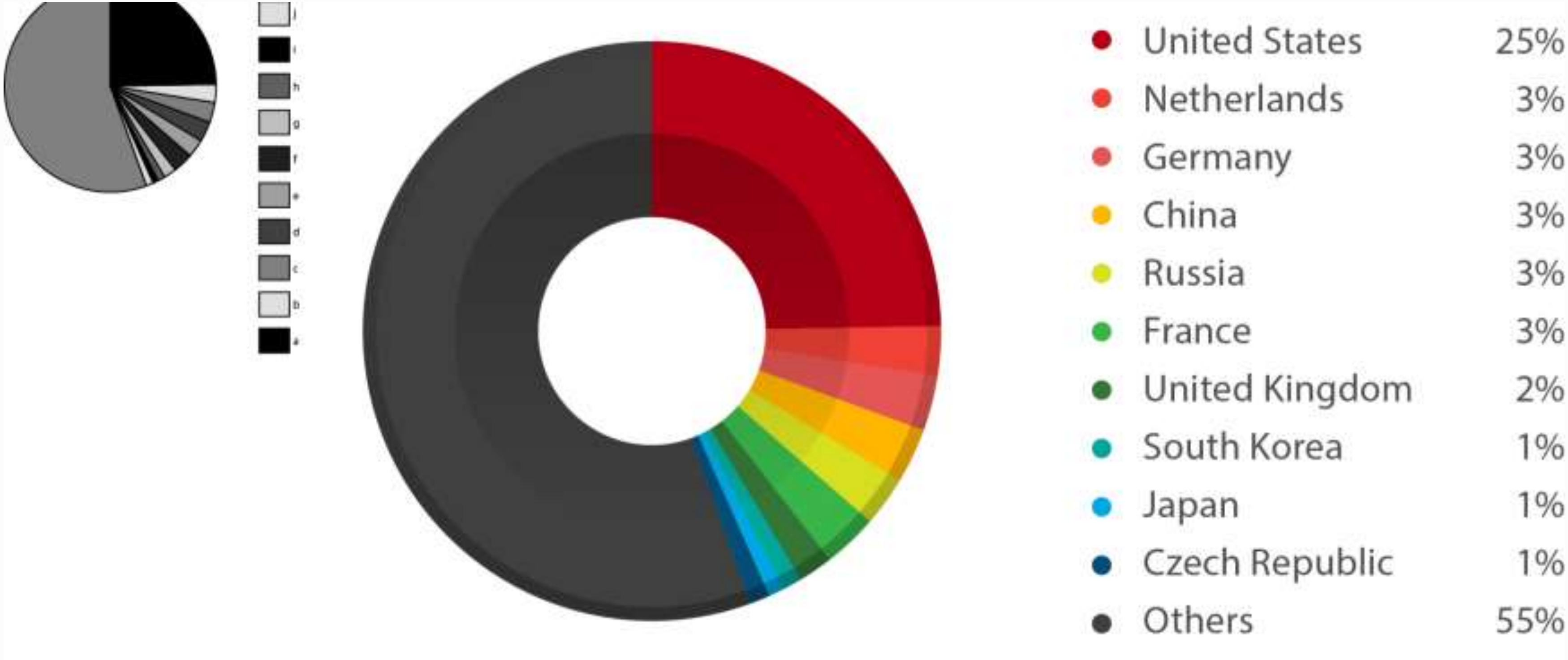
What are the *new* attack vectors?

Watering Hole Attacks

Source: Trend Micro Q2'14 Treat Roundup Report

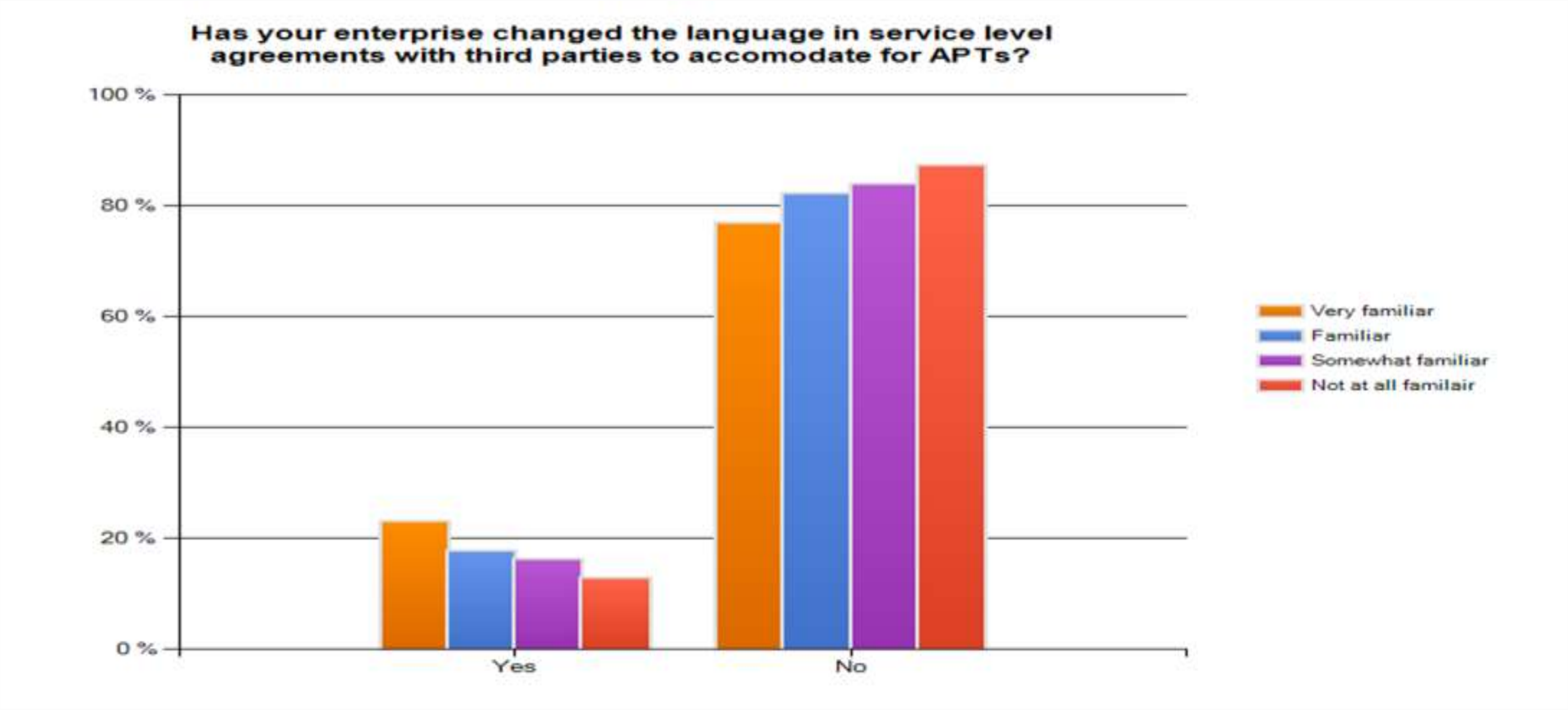
Copyright 2014 Trend Micro Inc.

Malicious URLs by Country



Island Hopping

81% Have Not Updated SLAs



Man-in-the-Browser Attacks

EMMENTAL

```
curitytube@ubuntu:~$ cat Payload.py
 /usr/bin/python

port os

.mkdir('/tmp/hacked')

curitytube@ubuntu:~$
curitytube@ubuntu:~$ ./UploadAndExecute.py 192.168.1.15 securitytube st123 Payload.py
curitytube@ubuntu:~$
curitytube@ubuntu:~$ ssh securitytube@192.168.1.15
e authenticity of host '192.168.1.15 (192.168.1.15)' can't be established.
DSA key fingerprint is 8d:c2:5f:12:e4:76:29:1d:fa:39:73:14:cd:52:9e:c7.
e you sure you want to continue connecting (yes/no)? yes
rning: Permanently added '192.168.1.15' (ECDSA) to the list of known hosts.
curitytube@192.168.1.15's password:
lcome to Ubuntu 12.10 (GNU/Linux 3.5.0-17-generic x86_64)

 Documentation:  https://help.ubuntu.com/

 System information as of Thu Apr  4 12:35:46 IST 2013

 System load:  0.0               Processes:           68
 Usage of /:   14.3% of 7.12GB   Users logged in:     1
 Memory usage: 21%               IP address for eth1: 192.168.1.15
 Swap usage:   0%

 Graph this data and manage this system at https://landscape.canonical.com/

         can be updated.

         Thu Apr  4 12:29:56 2013
```

Confidential | Copyright 2012 Trend Micro Inc.

The Evolution of Mobile Attacks

Mobile Ransomware: Svpeng & Locker

Proximity Attacks Realized

(NEST, 2014)

Geopolitics as Harbingers for Attack

Confidential © 2013 Trend Micro Inc.

Energetic Bear

Confidential | Copyright 2013 Trend Micro Inc.

2014 Cyber Attack Trends

1. Island Hopping
2. Mobile Malware/Proximity attacks
3. Cross-Platform Attacks
4. Man-in- the- Browser Attacks
5. Watering Hole Attacks
6. Ransomware
7. *Cloud Attacks*

Foiling the Digital Insider

Copyright 2013 Trend Micro Inc.

Opportunities to Detect the Breach

Check for Injected DNS Records
Failed/Irregular Logins
FAILED LOGIN
LOGIN SUCCESSFUL
Security Warnings
SECURITY THREAT
Abnormal Protocols
Increased Email Activity
HTM
PL
CSS
Strange Large Files
Abnormal Connections

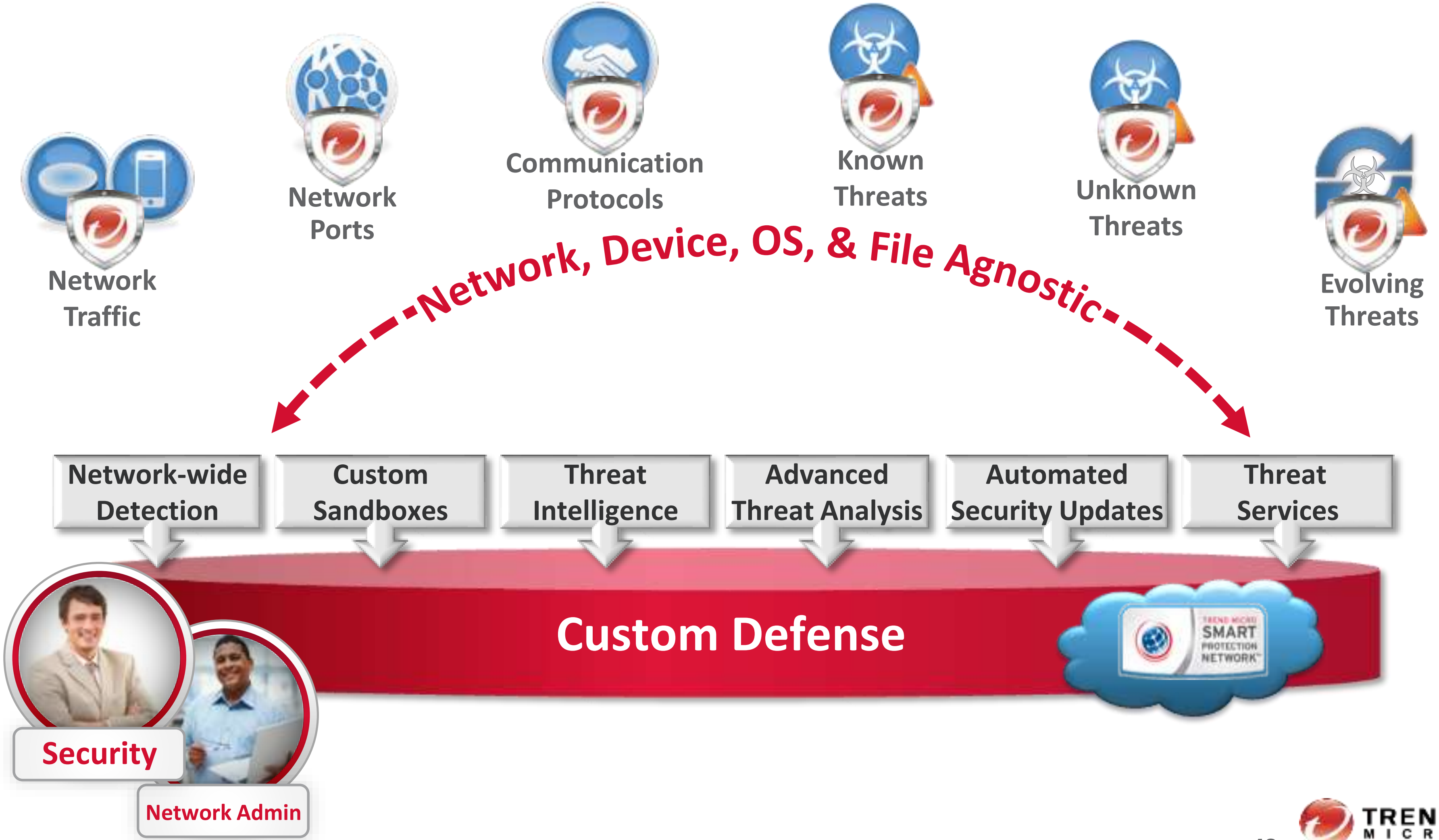
Advanced Persistent Response

Advanced Malware Detection

Contextual Threat Analysis

Attacker Activity Detection

Threat Impact Assessment



Network Traffic

Network Ports

Communication Protocols

Known Threats

Unknown Threats

Evolving Threats

Network, Device, OS, & File Agnostic

Network-wide Detection

Custom Sandboxes

Threat Intelligence

Advanced Threat Analysis

Automated Security Updates

Threat Services

Custom Defense

Security

Network Admin

Copyright 2013 Trend Micro Inc.

Risk Management in 2014

TREND MICRO

1. Conduct Pen test of all third parties.
2. Use Two-factor authentication.
3. Conduct egress filtering.
4. Deploy file integrity monitoring.
5. Implement virtual shielding for zero day exploits.
6. Deploy both an MDM and Mobile Application Reputation software.
7. Deploy a DLP.
8. Implement whitelisting.
9. Manage the crypto keys for your cloud data.
10. Implement DMARC.
11. Deploy context aware Threat Intelligence.
12. Utilize a Breach Detection System.

Breach Detection with Deep Discovery

360 Degree Detection

- Custom sandboxing
  - Matching precise customer specs
  - Mobile, Mac, and more
- Beyond malware
  - C&C comms, attacker activity
- Beyond web & email traffic
  - 80+ protocols/apps over all ports

Custom Intelligence

- Smart Protection Network & Threat Researchers
- Threat Connect for custom intel

Custom Detection and Intelligence

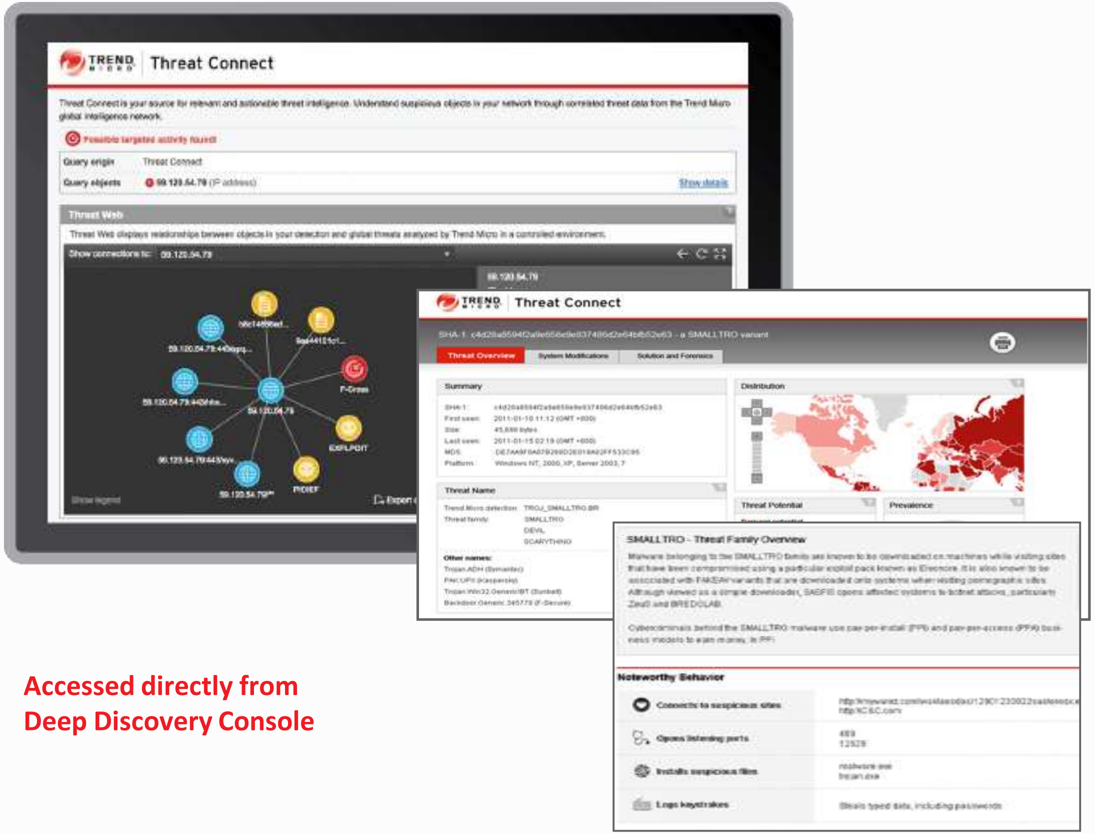
Advanced Protection Integration

Custom Security Updates

Forensics, Containment, Remediation

Copyright 2014 Trend Micro Inc.

Threat Connect Portal – Impact Analysis



TREND MICRO | Threat Connect

Threat Connect is your source for relevant and actionable threat intelligence. Understand suspicious objects in your network through correlated threat data from the Trend Micro global intelligence network.

Possible targeted activity found!

Query origin	Threat Connect
Query objects	59.120.54.79 (IP address) Show details

Threat Web

Threat Web displays relationships between objects in your detection and global threats analyzed by Trend Micro in a controlled environment.

Show connections to: 59.120.54.79

TREND MICRO | Threat Connect

SHA-1: c4d28a8594f2a9e656e9e837406d2e64bfb52e63 - a SMALLTRO variant

Summary

SHA-1:	c4d20a8594f2a9e656e9e837406d2e64bfb52e63
First seen:	2011-01-10 11:12 (GMT +800)
Size:	45,888 bytes
Last seen:	2011-01-15 02:19 (GMT +800)
MD5:	DE7AA9F9A07B288D2E01BA02FF533C95
Platform:	Windows NT, 2000, XP, Server 2003, 7

Distribution

Threat Potential

Prevalence

Threat Name

Trend Micro detection:	TROJ_SMALLTRO.BR
Threat family:	SMALLTRO DEVIL SCARYTHING

Other names:

Trojan.ADH (Symantec)
PAK:UPX (Kaspersky)
Trojan.Win32.Generic!BT (Sunbelt)
Backdoor.Generic.345778 (F-Secure)

SMALLTRO - Threat Family Overview

Malware belonging to the SMALLTRO family are known to be downloaded on machines while visiting sites that have been compromised using a particular exploit pack known as Eleonore. It is also known to be associated with FAKEAV variants that are downloaded onto systems when visiting pornographic sites. Although viewed as a simple downloader, SASFIS opens affected systems to botnet attacks, particularly ZeuS and BREDOLAB.

Cybercriminals behind the SMALLTRO malware use pay-per-install (PPI) and pay-per-access (PPA) business models to earn money. In PPI

Noteworthy Behavior

Connects to suspicious sites	http://[illegible] http://C&C.com
Opens listening ports	459 12529
Installs suspicious files	malware.exe trojan.exe
Logs keystrokes	Steals typed data, including passwords

Accessed directly from Deep Discovery Console

Threat profile: What are the characteristics, origins and variants of this malware.

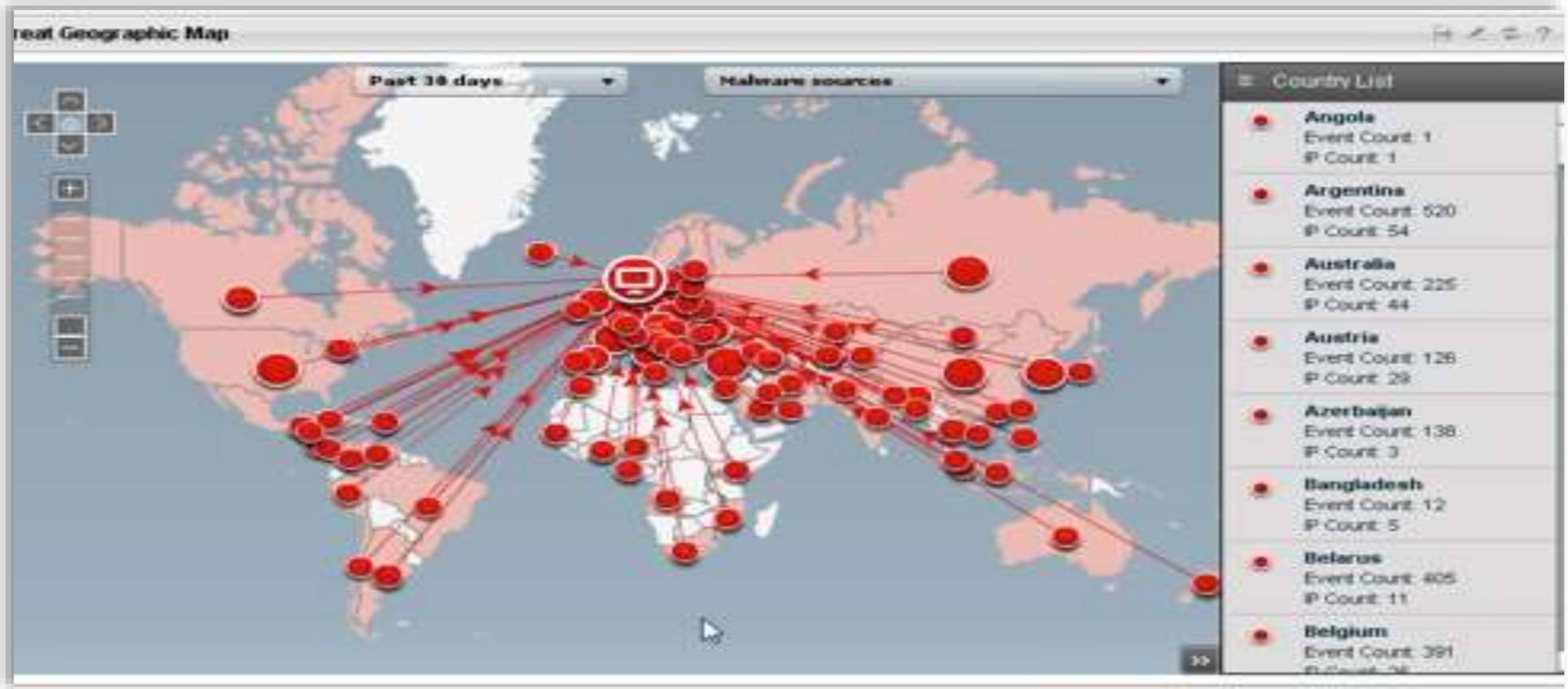
Related IPs/Domains: What are the known C&C comms for this attack.

Attack Group/Campaign: Who and what is behind this threat.

Containment and remediation: What to look for, how to eradicate.

TREND MICRO SMART PROTECTION NETWORK™

Situational Awareness



reat Geographic Map

Past 30 days

Malware sources

Country List

- Angola
  Event Count: 1
  IP Count: 1
- Argentina
  Event Count: 520
  IP Count: 54
- Australia
  Event Count: 225
  IP Count: 44
- Austria
  Event Count: 126
  IP Count: 29
- Azerbaijan
  Event Count: 138
  IP Count: 3
- Bangladesh
  Event Count: 12
  IP Count: 5
- Belarus
  Event Count: 405
  IP Count: 11
- Belgium
  Event Count: 391
  IP Count: 26

Securing your journey to the cloud