



# Cyber Threat 2014: Defense in Depth Strategy for Data Privacy

Jim Sortino, CISSP  
Vice President, Trend Micro



220K new malware programs daily!



# Number of Active C&C Servers

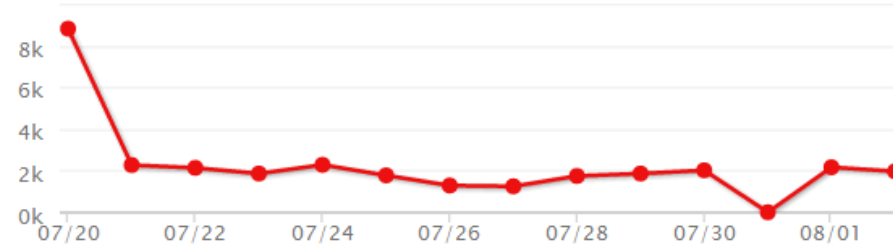


According to the director of FBI's cyber division, Joseph Demarest, Botnet has become one of the biggest enemies of the Internet today, and therefore its impact has been significant.

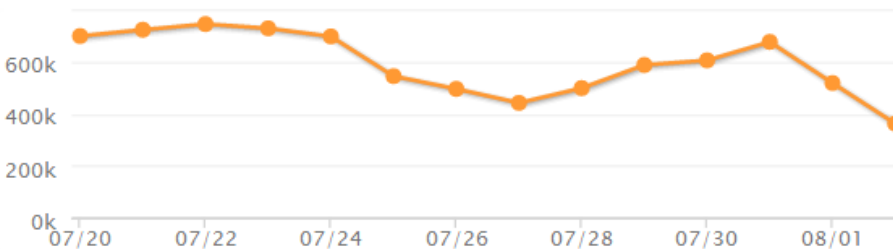
Every second, 18 computers worldwide are part of botnet armies, which amounts to over 500 million compromised computers per year.

Source: [http://www.fbi.gov/news/news\\_blog/fbi-cyber-executive-briefs-congress-on-joint-efforts-to-bust-botnets](http://www.fbi.gov/news/news_blog/fbi-cyber-executive-briefs-congress-on-joint-efforts-to-bust-botnets)

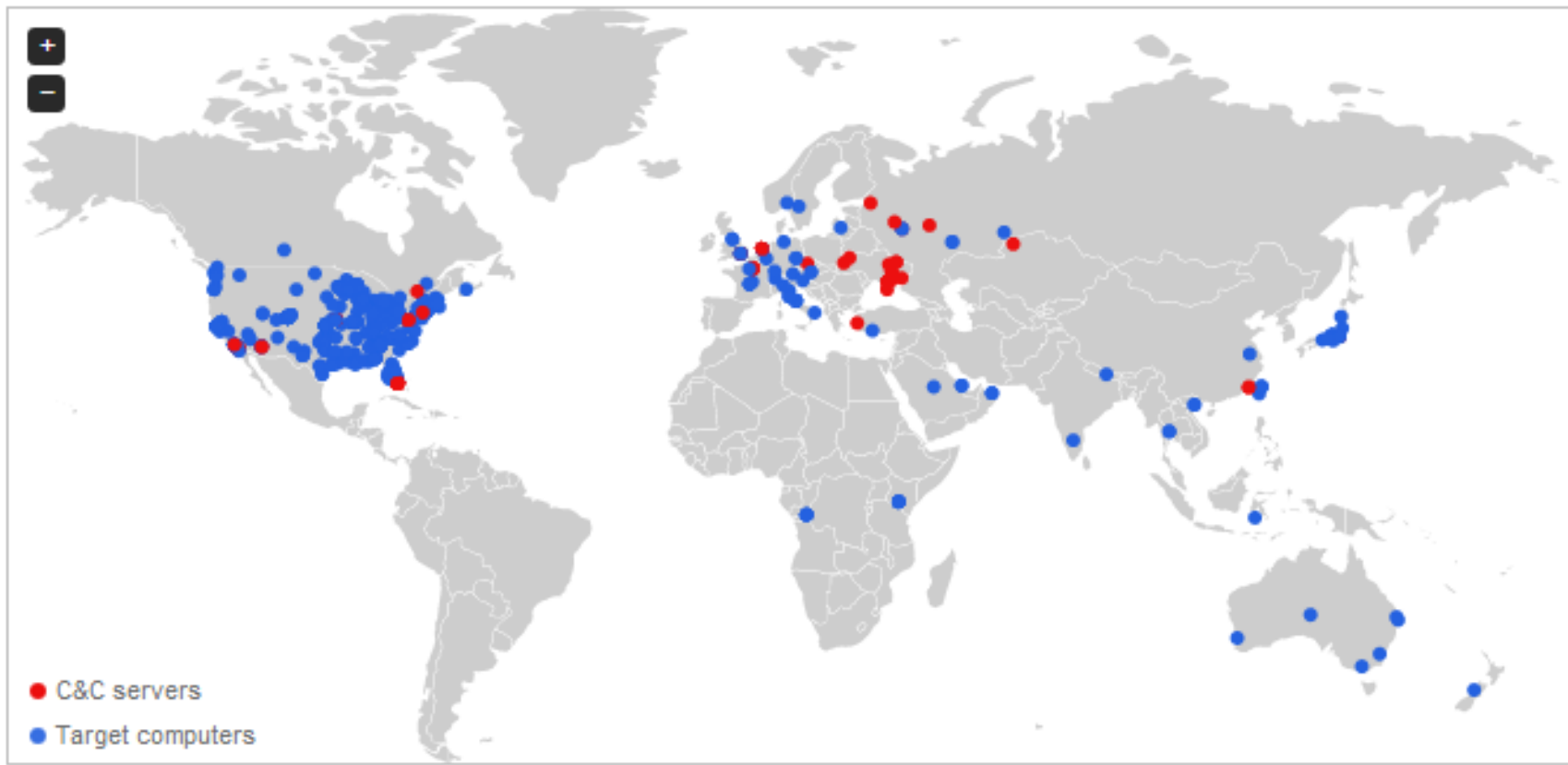
C&C servers  
**13484**  
active in the last 14 days



Botnet connections  
**8,296,326**  
active in the last 14 days



# Geographic distribution of targets



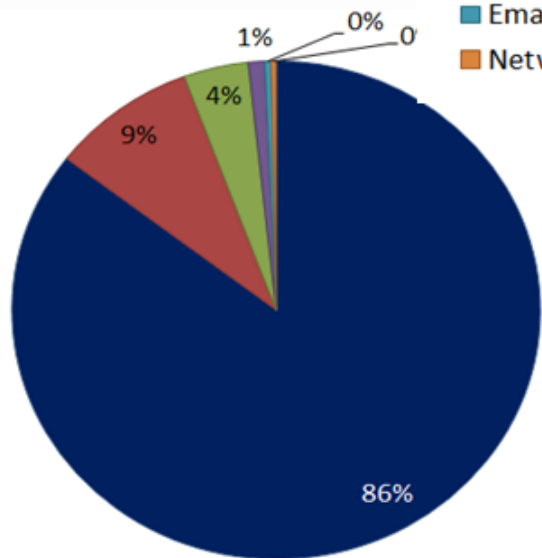
How are they doing it?

# Arrival Vectors in APT - Email

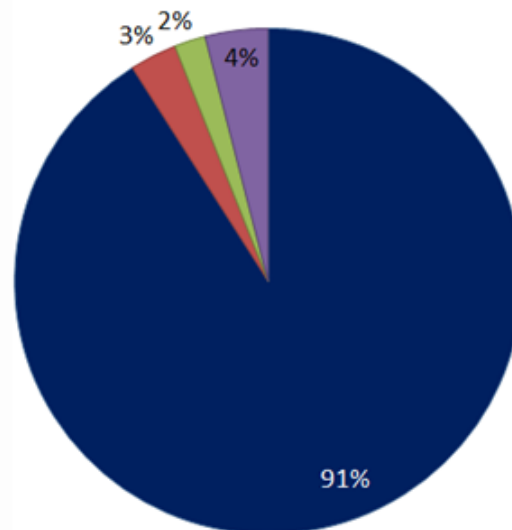


2013

- Email (Attachment)
- Malware Samples
- Unknown
- Java/IE Exploits
- Email (URL)
- Network Share



2014



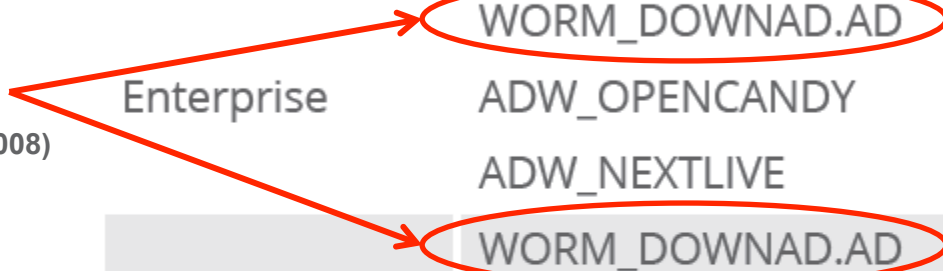
- Email (Attachment)
- Email (URL)
- Java/IE Exploits
- Unknown

# Worried about 0day threats? Old Still Works

## Top 3 Malware by Segment

SEGMENT	DETECTION NAME	VOLUME
Enterprise	WORM_DOWNAD.AD	69K
	ADW_OPENCANDY	25K
	ADW_NEXTLIVE	25K
SMB	WORM_DOWNAD.AD	28K
	ADW_SENSAVE	12K
	ADW_MONTIERA	12K
Consumer	ADW_NEXTLIVE	266K
	ADW_OPENCANDY	240K
	ADW_SENSAVE	234K

DOWNAD = Conficker (Patched in 2008)



# Attackers Try Everything

## Multiple Ports

### Poison Ivy

40%	Port 443	HTTPS
30%	Port 80	HTTP
11%	Port 220	IMAP
9%	Port 143	IMAP
4%	Port 8080	HTTP_ALT
2%	Port 1234	HYPER TEXT
1%	Port 53	DNS
1%	Port 110	POP3
1%	Port 25	SMTP
1%	Port 995	POP3S

Monitoring a few ports is not sufficient

## Apps & protocols

### Evilgrab



Monitoring a few apps & protocols is not sufficient

## Morphing

### IXESHE

Changes in C&C,  
IP addresses,  
signatures & behavior



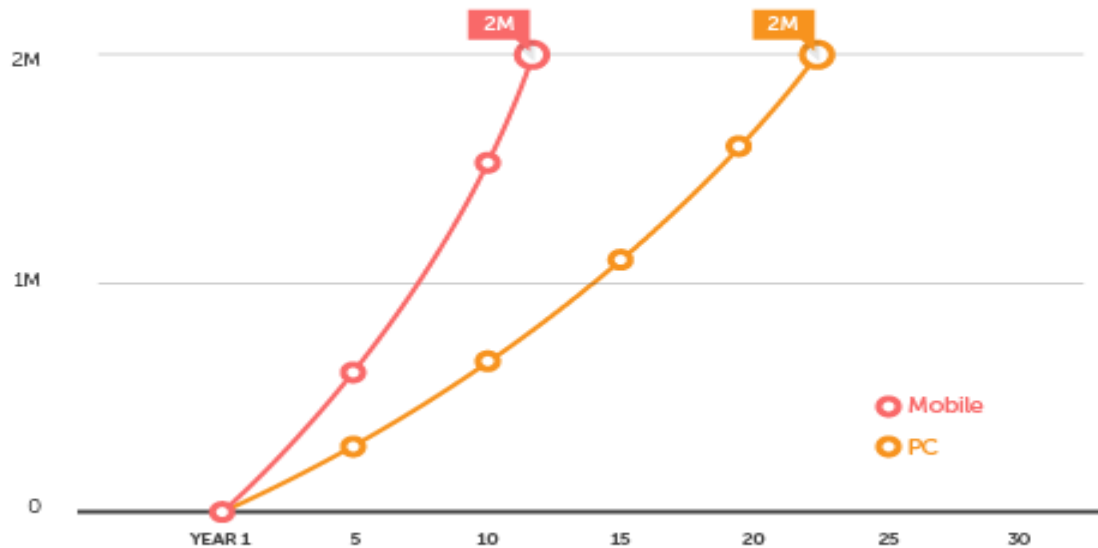
It's extremely difficult to track the attack



# Mobile matches PC Rate 1H'14



## PC and Mobile Malware Growth Rate



# EMMENTAL

The image displays a terminal window with the following content:

```
securitytube@ubuntu:~$ cat Payload.py
#!/usr/bin/python
import os
os.mkdir("/tmp/hacked")
securitytube@ubuntu:~$ ./UploadAndExecute.py 192.168.1.15 securitytube st123 Payload.py
securitytube@ubuntu:~$ ssh securitytube@192.168.1.15
Warning: authenticity of host '192.168.1.15 (192.168.1.15)' can't be established.
RSA key fingerprint is 8d:c2:5f:12:e4:7b:29:3a:fa:39:73:14:cd:52:9e:c7.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.15' (ECDSA) to the list of known hosts.
securitytube@192.168.1.15's password:
Welcome 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

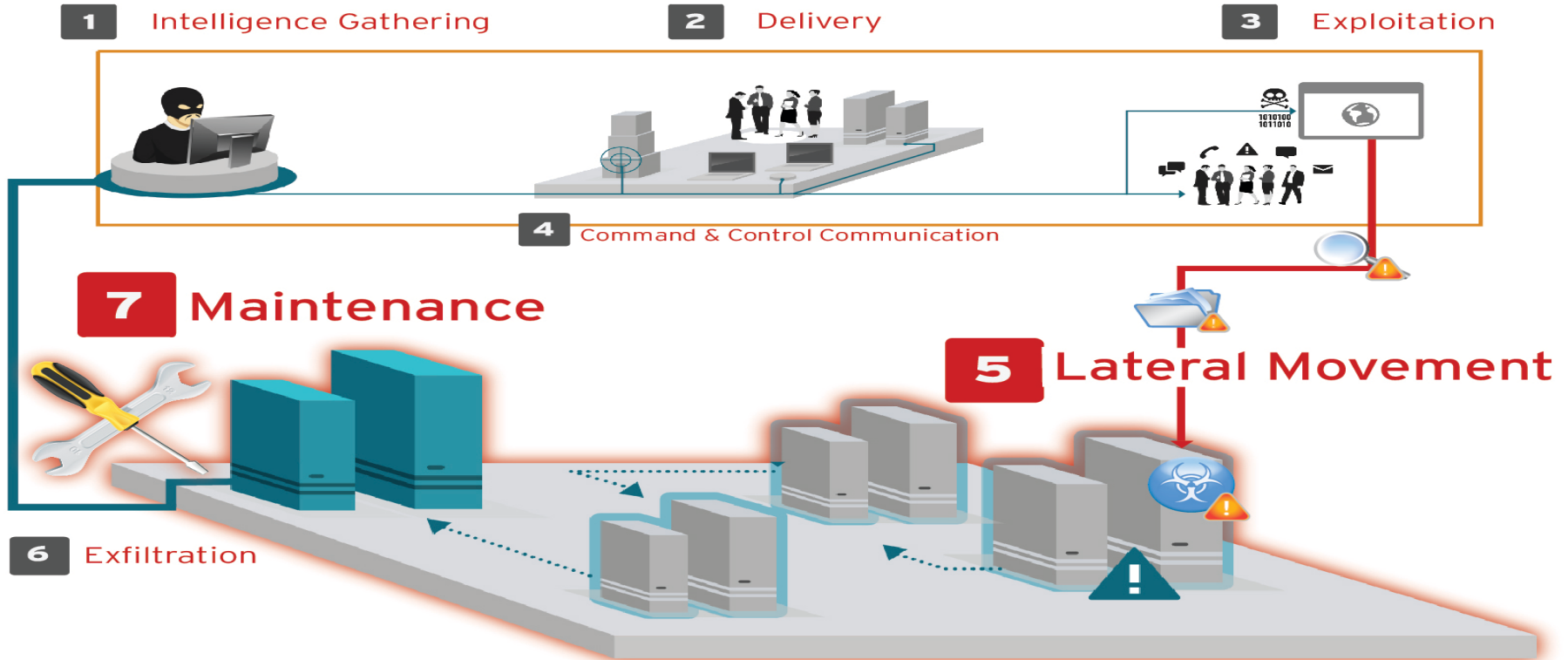
System load:  0.0          Processes:      68
Usage of /:   14.3% of 7.12GB    Users logged in:  1
Memory usage: 21%          IP address for eth1: 192.168.1.15
Swap usage:   0%

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

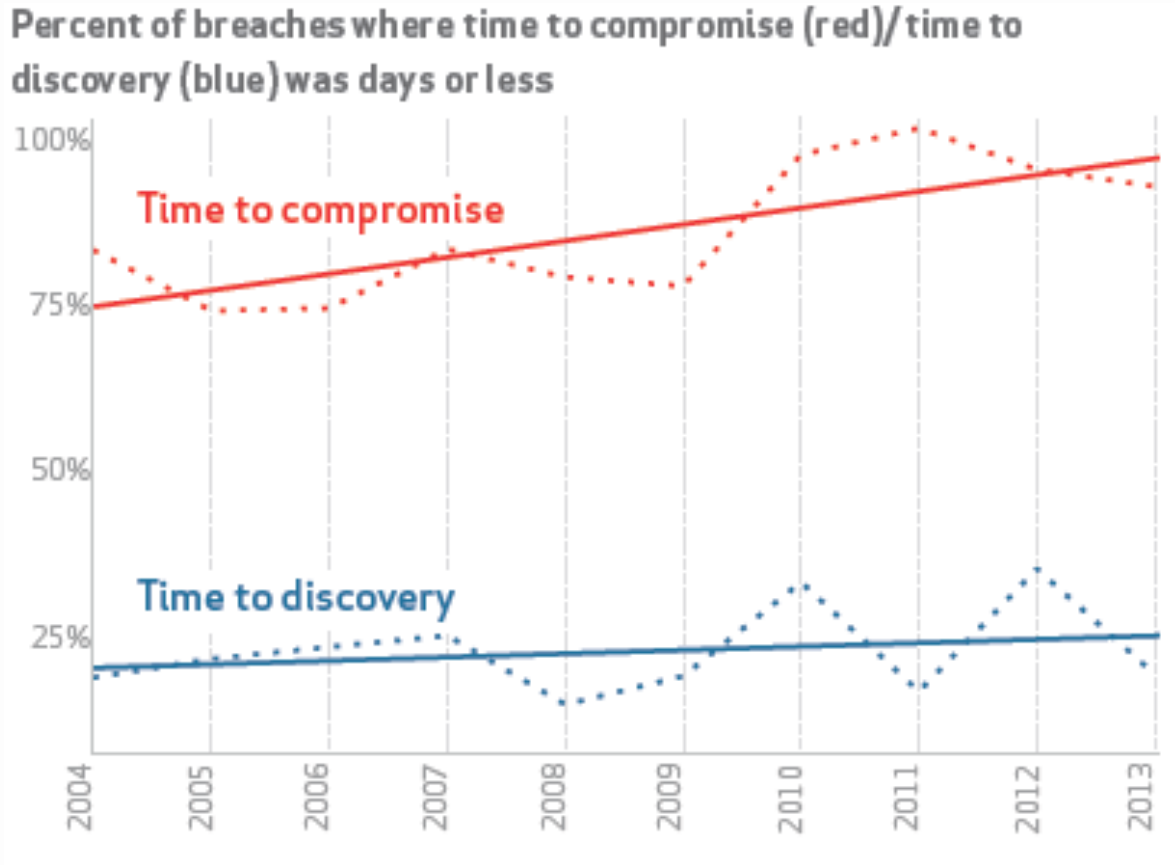
Your system can be updated.
Thu Apr  4 12:29:56 2013
```

The terminal output is overlaid on a background image of a classical building with columns and a sign that says "BANK". The image is also decorated with a pattern of green Euro symbols (€) and a small Android phone icon in the bottom left corner.

# Offense Must Inform Defense

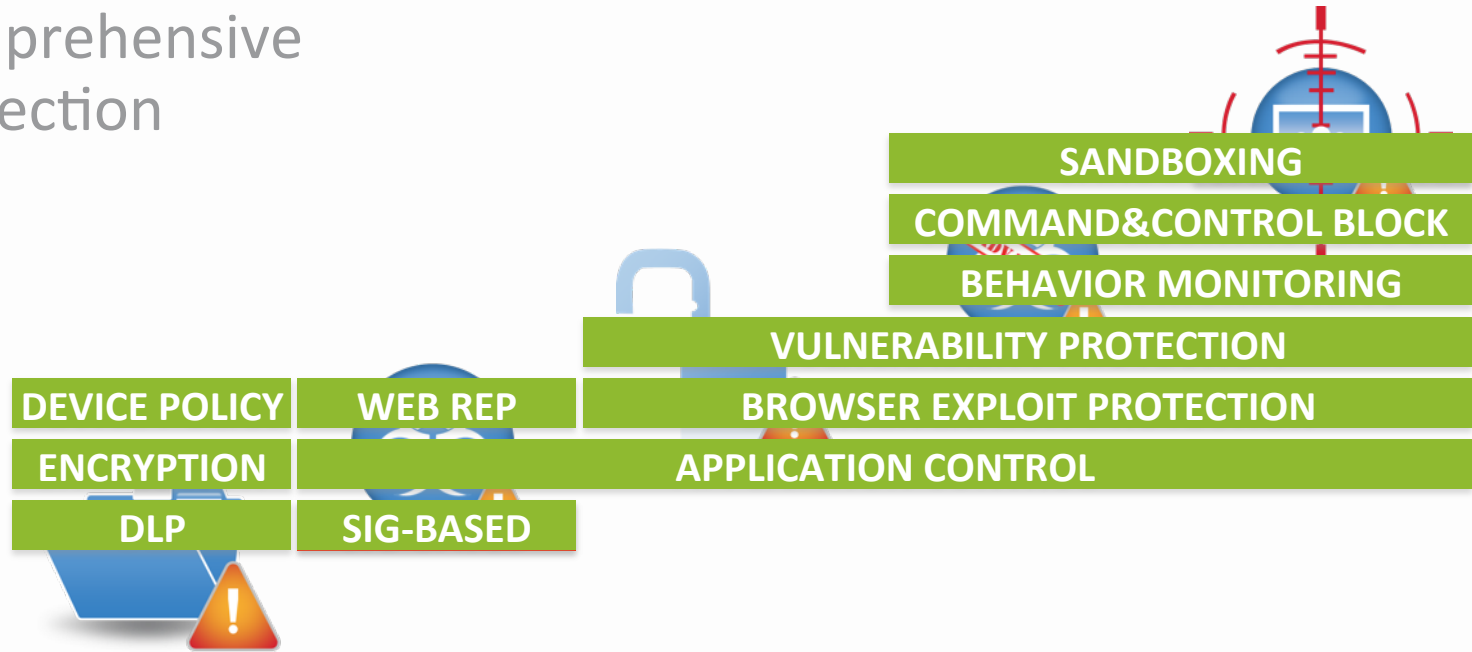


# Time to compromise vs discovery - Verizon



Source: <http://www.verizonenterprise.com/DBIR/>

# Comprehensive Protection



Employee Data  
Leaks

Traditional  
malware

Vulnerability  
exploits

Advanced  
Malware

Targeted  
Attacks

# Risk Management in 2014



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.

# Securing your journey to the cloud

