ITDays – Security issues

“Malicious Intrusion, are we concerned in our Organization?”

7 steps to evaluate your situation!

Christophe Bianco - Christophe Rosenkranz – Paul Jung

November 2014

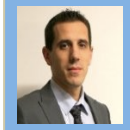
Agenda

- Are you concerned?
- Anatomy of an attack
- But how i can evaluate if i'm concerned?
- How to implemented that in my organization?
- Q&A

Who are we?

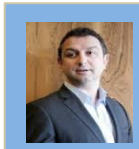
Paul **Jung**

Security Consultant



Christophe **Rosenkranz**

SOC Technical leader



christophe **Bianco**

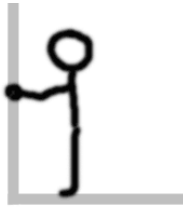
Managing Partner

- Excellium Services
  - Founded in Dec 2012
  - Focus on Application Security and Intrusion Management
  - 22 Security consultants and analysts
  - An operational Security Operation Center and a official Cert

Your speakers

- Christophe B. – In charge of the service offering
- Christophe R. – Monitoring and Incident management Specialist
- Paul J. – Intrusion & Forensic Specialist

Let’s start with a question!



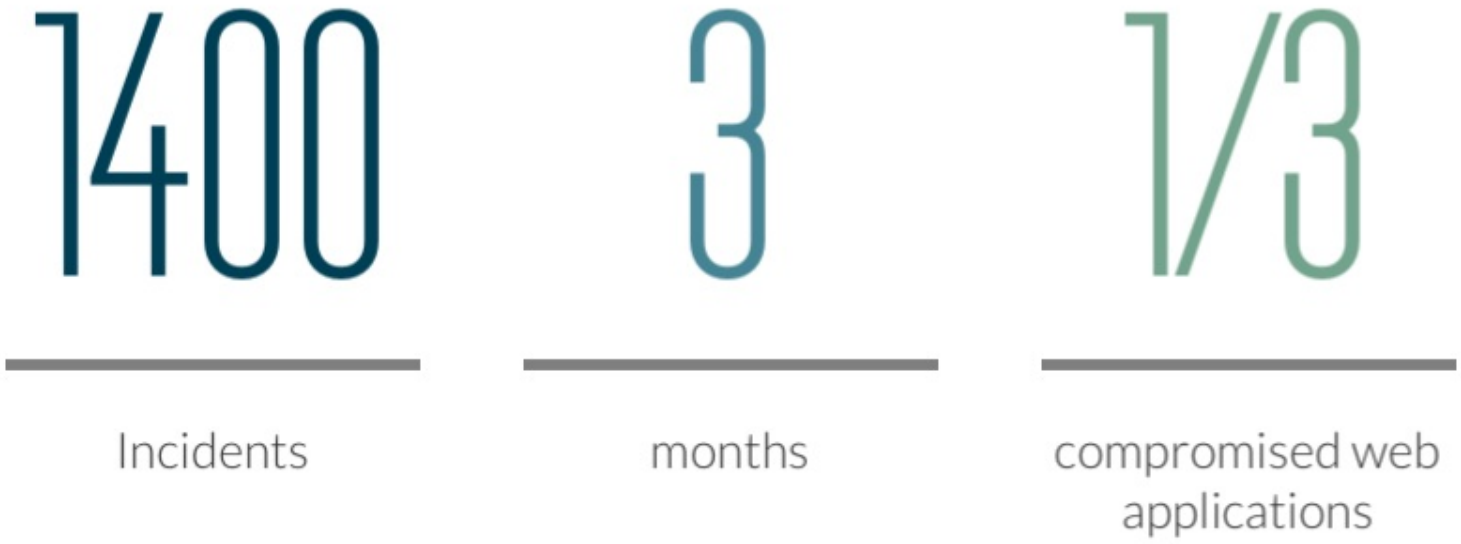
- Who has suffered an intrusion over the last 6 months?

- How do you discovered it?

Photo by keeva999 - Creative Commons Attribution-NonCommercial-ShareAlike License http://www.flickr.com/photos/54159370@N08

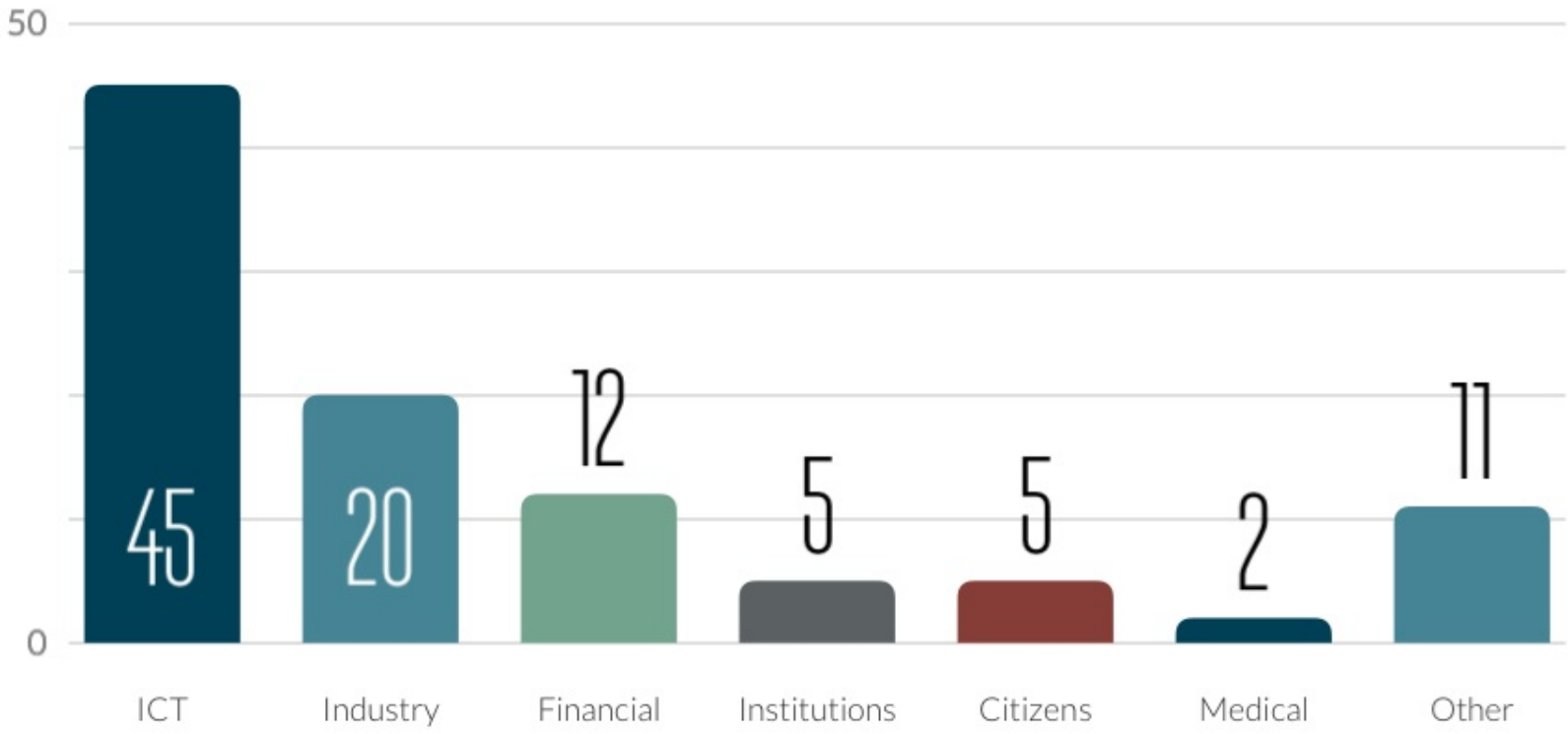
Created With Haiku Deck

Key figures



Created With Haiku Deck

By sector (%)



Created With Haiku Deck

Motivations

"cyber-crime"

(financial benefit, organised groups)

"cyber-activism"

(political / fun hacking)

"cyber-espionage"

(geo-political / state sponsored)

Created With Haiku Deck

Our recent engagements

Penetration Testing Mission

(100% in over the last 3)

- Passwords
- Web App vuln
- Network segmentation

Forensic Engagement

(3 in 2 weeks)

- Patchs
- Passwords
- AV not up to date

And we are not considering 0-day attacks!

Statements

According to multiple sources (Verizon DBIR report, M-Trends, Circl, ...)

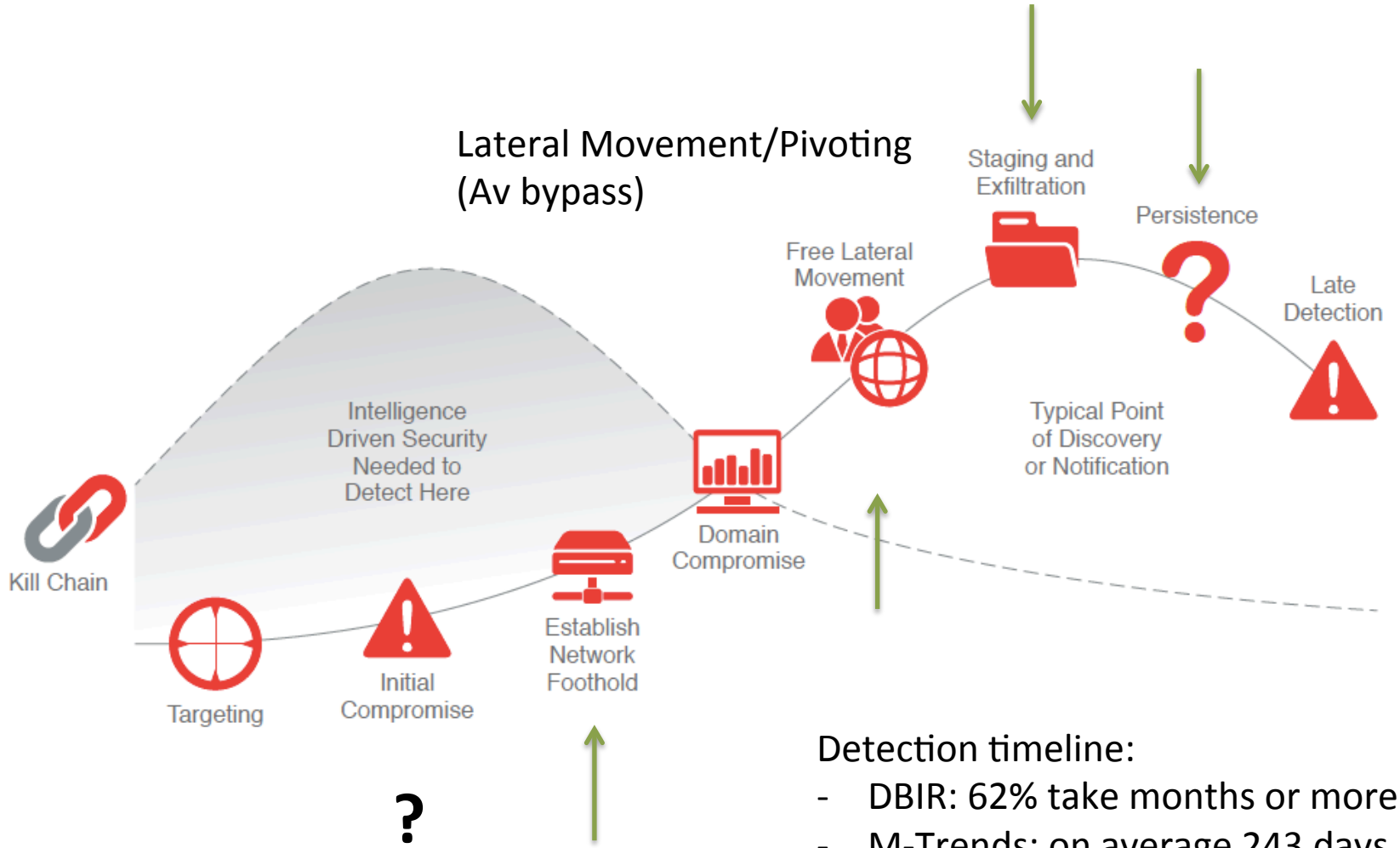
- Things do not look so good for organization
- Company are breached with impact repeatedly
- Intrusion is discovered because someone else told the organisation

.... Many many months after the compromise

AND issue is that most organizations are more than 80% preventive (with no reactive capability).

Anatomy of an attack

Advanced post-exploitation
(Encrypted C2 & outbound 443)



Detection timeline:

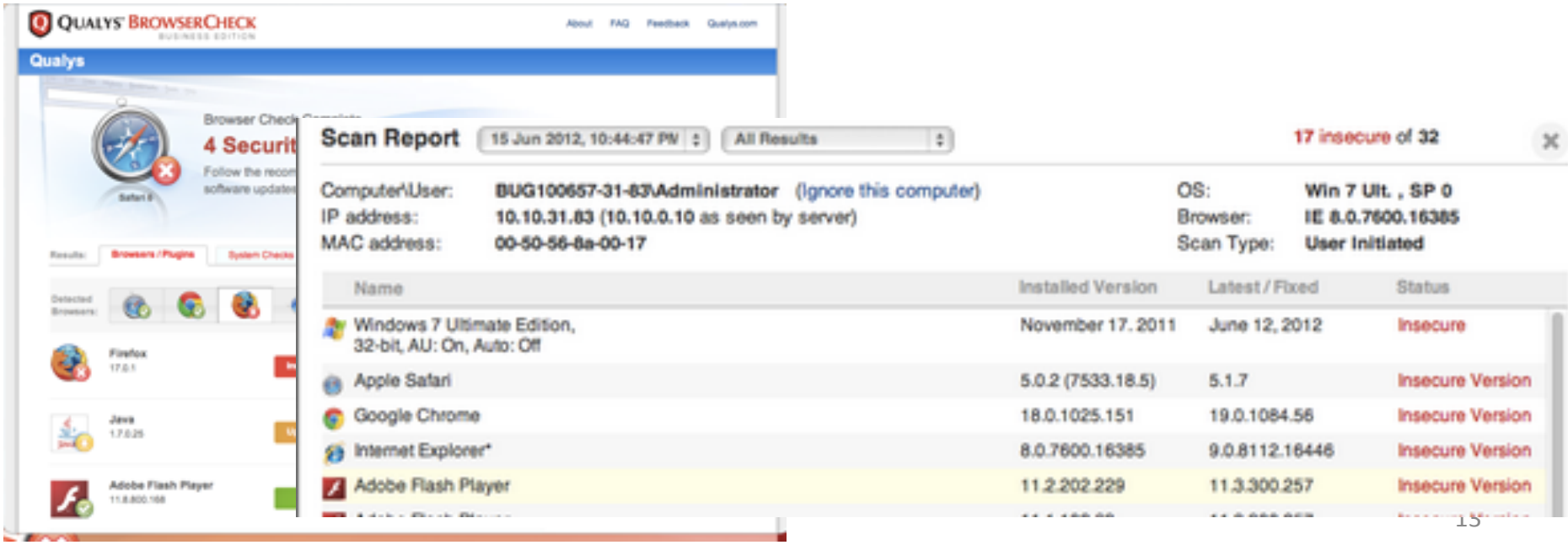
- DBIR: 62% take months or more
- M-Trends: on average 243 days

But can’t be just a keyword to look for!

Step 0 - Prevention

- Password Strength
  - Regular assessment

- Plugin Patches



Ok let’s look in detail!

First look in 7 steps!

A first stage of the ***Continuous Security Monitoring*** Concept!

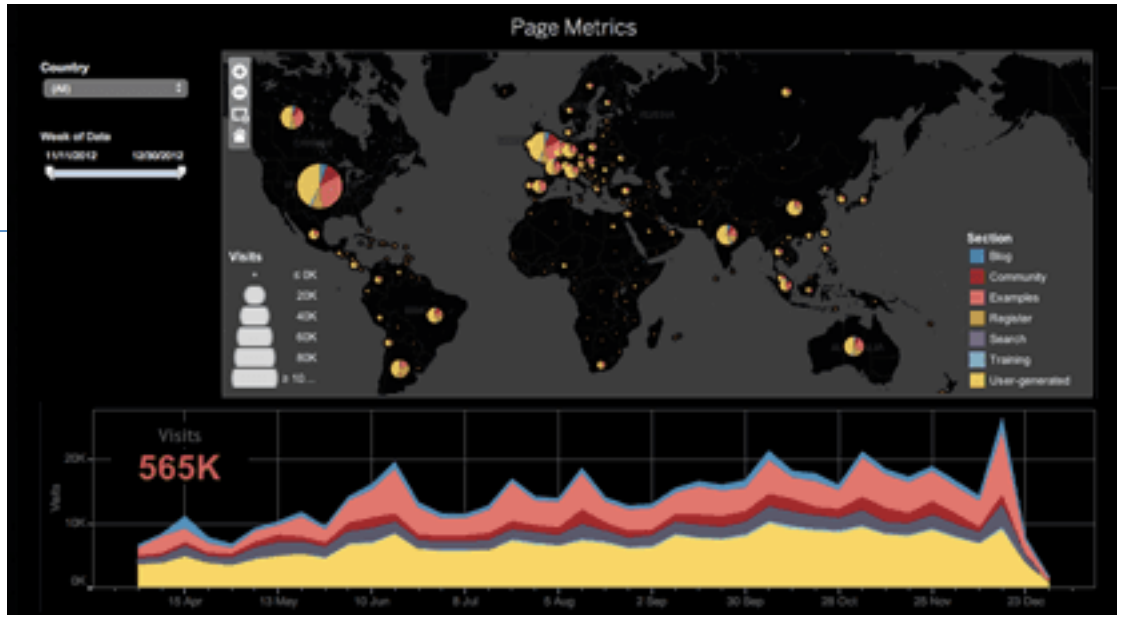
Step 1 – Profiling (assets, outbound traffic)

!!!! New form of attacks are less and less “stupid”

You need to understand normal behavior and look for oddities and anomalies

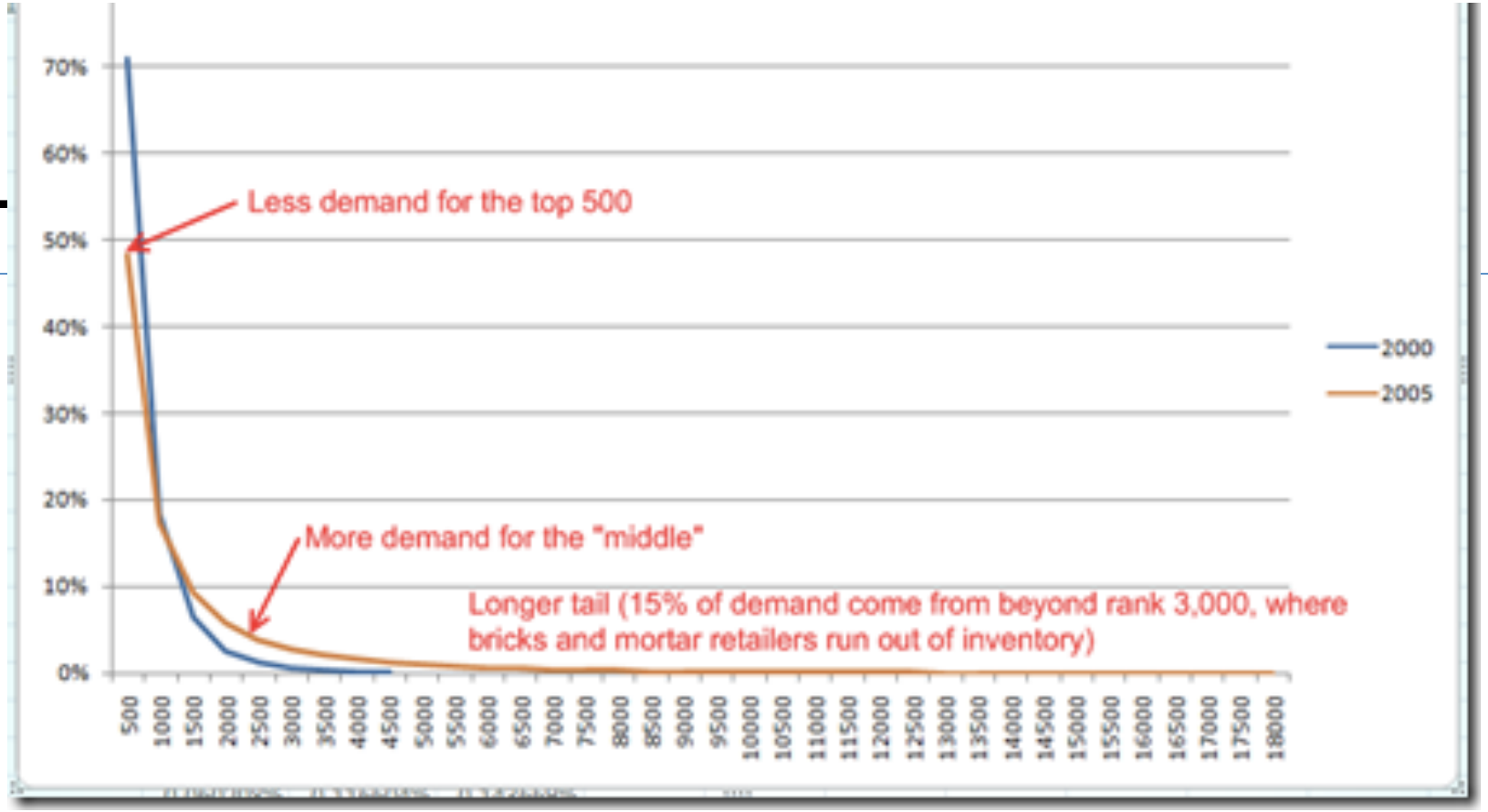
- What is your network? (network mapping – Host, port and service discovery or DHCP logs or CAM table)
- How much data is sent?
- Who sends the data (at proxy and firewall levels)
- Where are you sending the data (ip geolocated and port numbers)?
- When is the data sent?

Reco: **Perform this analysis over a 3 month volume of data and the scans at different time periods (nighly, week-end, ...)**


Page Metrics
Country
Week of Data
Visits
Section
Blog
Community
Examples
Register
Search
Training
User-generated
Visits
565K


Asia
Europe
Atlantic Ocean
Africa
South America
Indian Ocean
Australia
Google

L


70%
60%
50%
40%
30%
20%
10%
0%
Less demand for the top 500
More demand for the "middle"
Longer tail (15% of demand come from beyond rank 3,000, where bricks and mortar retailers run out of inventory)
2000
2005

Step 2 – Do we have illegal Registry Startup Keys? – Long Tail Analysis

1 – Query all startup registry keys on all systems

2 – Save to a file

3 – Sort in order of duplicates, least to most

4 – Then inspect the least frequently seen registry keys (works for windows event logs, installed software, startup registry keys & DNS logs)

The first pass may be somewhat time consuming

Once that process is complete

re-run the script nightly

report any new entries

Step 2 – Do we have illegal autorun? – Long Tail Analysis

Use Group Policy to audit registry keys or WMI by scripting to extract and monitor changes on:

Run, RunOnce, Start…

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shared Task
%userprofile%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup

And
HKCU\SOFTWARE\Wow6432node\Microsoft\Windows\CurrentVersion\Run
HKCU\SOFTWARE\Wow6432node\Microsoft\Windows\CurrentVersion\RunOnce

Or Powershell is your friend (or better a logon script!!!)

```
$user="starbuck”
$password="cyl0n”

$array = @("192.168.1.1", "192.168.1.2")

foreach ($ip in $array) {
  net use \\$ip $password /u:$user | out-null
  $ip
  reg query \\$ip\HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
  reg query \\$ip\HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce
  reg query \\$ip\HKU\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Run
  reg query \\$ip\HKLM\SOFTWARE\Wow6432node\Microsoft\Windows\CurrentVersion\Run
2> $null
  reg query \\$ip\HKLM\SOFTWARE\Wow6432node\Microsoft\Windows\CurrentVersion
\RunOnce 2> $null
}
```

Step 3 – Persistent / abnormal outbound connexions?

- Detect recurrent / regular illegal connexions (10 minutes or so is a good threshold)
- Start by a snapshot of night traffics
- Hackers make mistakes so look also filtered traffic on the proxy or inner firewall

Step 4 – Proxy logs?

- Setup correct logging
  - Source / Destination
  - URL
  - Category
  - User Agent
  - Bytes & header Size
  - Referrer

- Look for:
  - Abnormal volume logs
  - Check 403 denied and 407 Proxy Authrequest
  - Abnormal User Agents
  - Headers size (to catch the malicious ones)

Step 5 – Password & Rights

- Gain visibility of your privileged account environment
  - Discover all privileged and non-privileged accounts
  - Locate all privileged credentials including:
    - Passwords
    - SSH keys
    - Password hashes

- On a regular basis check the resistance of your key password

Download latest version

Name	Version	md5sum	Date
oclHashcat for AMD	v1.31	81f00b1f345a27e0edffae693707943c	2014.10.02
oclHashcat for NVidia	v1.31	b07045784ec7f4913293ea2cc6eac5ca	2014.10.02

- Control usage of the “Maleficent Seven”
  - Debug Programs
  - Impersonate a client
  - Act as Part of the OS
  - Create a token
  - Load drivers
  - Take Ownership
  - Restore files

Step 6 – Specific Monitoring

On Systems (Windows)

- Registry Key creation
- Service creation
- User creation
- Admin right changes
- Clearing the Event Log

- Parsing the psexec, consider specific alerts like AV catching mimikatz, wce, ..

- On the Network
  - DNS – log local DNS requests and resolution – look for long requests and responses (fail)

Step 7 – Windows Logs

Analyses of the following events

Type	Event IDs	Log
Create service	7030, 7045	System
Create user	4720, 4722, 4724, 4738	Security
Add user to group	4732	Security
Clear Event log	1102	Security
Create RDP certificate	1056	System
Insert USB	10000,100001,10100,20001,20002, 20003,24576,24577,24579	System
Disable firewall	2003	Firewall

www.nsa.gov/ia/_files/app/spotting_the_adversary_with_windows_event_log_monitoring.pdf

Step 7 – Windows Logs

- By script

  Get-WinEvent -FilterHashtable @{LogName="Security"; ID=4720,4722,4724,4738,4732,1102}

  Get-WinEvent -FilterHashtable @{LogName="System"; ID=7030,7045,1056,7045,10000,100001,10100,20001,20002,20003,24576, 24577,24579}

  Get-WinEvent -FilterHashTable @{LogName="Microsoft-Windows-Windows Firewall With Advanced Security/Firewall"; ID=2003}

- Control User Rights
  - Allow/deny Log On Locally
  - Allow Log On Through Remote Desktop Services
  - Deny Access via the Network
  - Logon as a service

How to implement that?

- Script and do it yourself

Or Call us!!!!

- Mission our EyeGuard Infection Assessment
- Implement log / siem consolidation tool
- Subscribe to our Eyeguard Services

Conclusion

- While exploits and 0-days are seriously cool and fun to talk about ... Who cares?

- The focus of modern cyber defense is to detect the post-exploitation activity (what is the end goal) !
  - 1er goal: detecting adversary activity toward their goal
  - 2nd goal: responding to the detection (responding to the detection before they own the domain)

- Tools for this new security paradigm
  - Defensible Security Architecture
  - Security operation
  - Network Security Monitoring
  - Continuous Security Monitoring

- And ***do not wait*** to be breach to start to think about your detection capability – you can not investigate with no info

"The only way a domain compromise can be remediated with a high level of certainty is a complete rebuild of it."

*http://blogs.technet.com/b/srd/archive/2014/11/18/additional-information-about-cve-2014-63**24.aspx***

Spend some times on the SANS Critical Security Controls

1: Inventory of Authorized and Unauthorized Devices
2: Inventory of Authorized and Unauthorized Software
3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
4: Continuous Vulnerability Assessment and Remediation
5: Malware Defenses
6: Application Software Security
7: Wireless Access Control
8: Data Recovery Capability
9: Security Skills Assessment and Appropriate Training to Fill Gaps
10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
11: Limitation and Control of Network Ports, Protocols, and Services
12: Controlled Use of Administrative Privileges
13: Boundary Defense
14: Maintenance, Monitoring, and Analysis of Audit Logs
15: Controlled Access Based on the Need to Know
16: Account Monitoring and Control
17: Data Protection
18: Incident Response and Management
19: Secure Network Engineering
20: Penetration Tests and Red Team Exercises

La Code hackademy
.... (codehackademy.lu)

- Initiative Excellium & Cases.lu – Première session en janvier 2015

- Formation à destination des professionnels du développement applicatif
  Entièrement gratuite, sur 10 semaines, un soir par semaine

- Thématiques abordées
  - Principes de sécurité des applications Web – introduction
  - De l'architecture logicielle à la mise en oeuvre
  - Test sécurité des applications – Techniques de hacking
  - Infrastructures sécurisées pour héberger les applications
  - Illustration de la sécurité d'un code – Java Security
  - Sécurité des bases de données – L'exemple d'Oracle
  - Approche d'un Software Developement Life Cycle
  - Malwares et leur analyse
  - Utilisation du Cloud
  - Paiement en ligne

Thanks!

Excellium Services – contact@excellium-services.com