netbull

1/4/2015

Security Intelligent: Advance Persistent Threat

Nikitas Kladakis
Information Security Manager

Agenda

- Company Profile
- Advance Persistent Threat (APT)
- How to combat against APT

Company Profile

- Netbull IT Services, founded in 2013 from executives of BULL Greece with experience in large projects of the public and private sectors, as a leading System Integrator

- Information Security Offer
  - Information Security Services
  - Security as a Service
  - 24 x 7 Security Monitoring
  - Information Security Products

- ISO/IEC 27001, ISO/IEC 9001

Advance Persistent Threat (APT)

What is an Advance Persistent Threat (APT)?

Advance

Sophisticated techniques using malware to exploit vulnerabilities in systems

Persistent

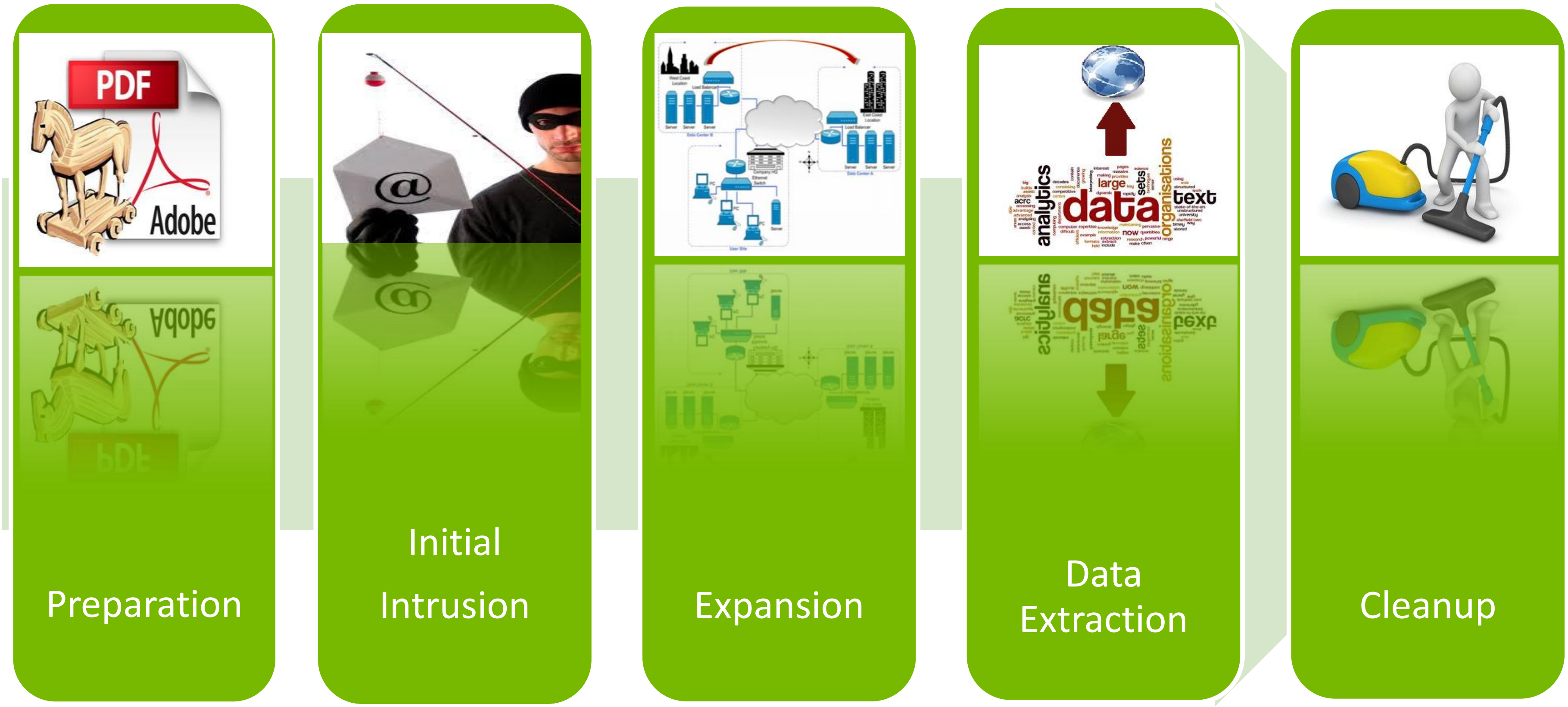
Continuously monitoring and extracting data from a specific target

Threat

Coordinated human involvement in the attack

Complex, sophisticated cyber-attack that can last months or even years

APT Methodology



Preparation

Initial Intrusion

Expansion

Data Extraction

Cleanup

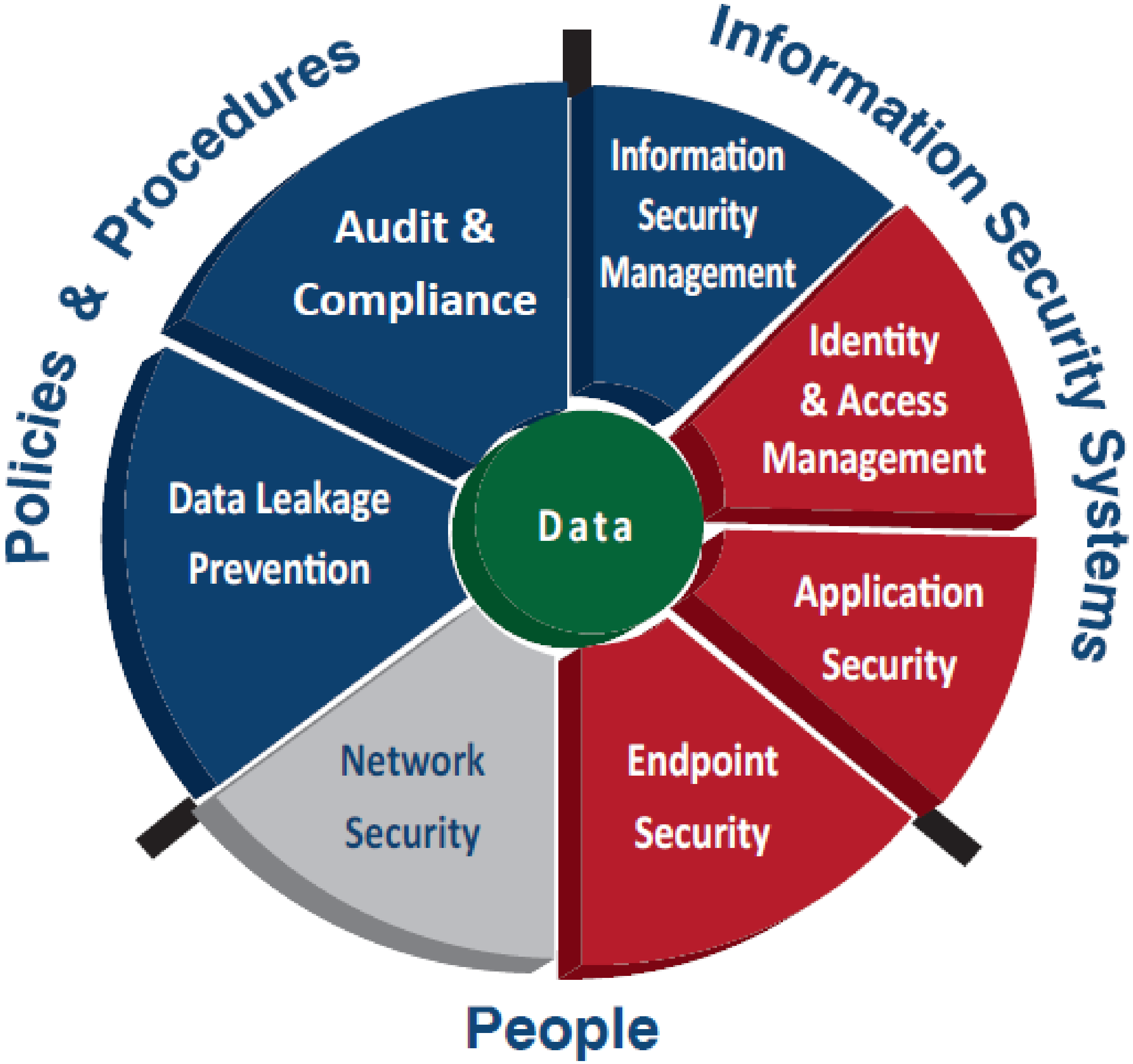
How to Combat Against APT

“Do Nothing” Strategy

- No Cost

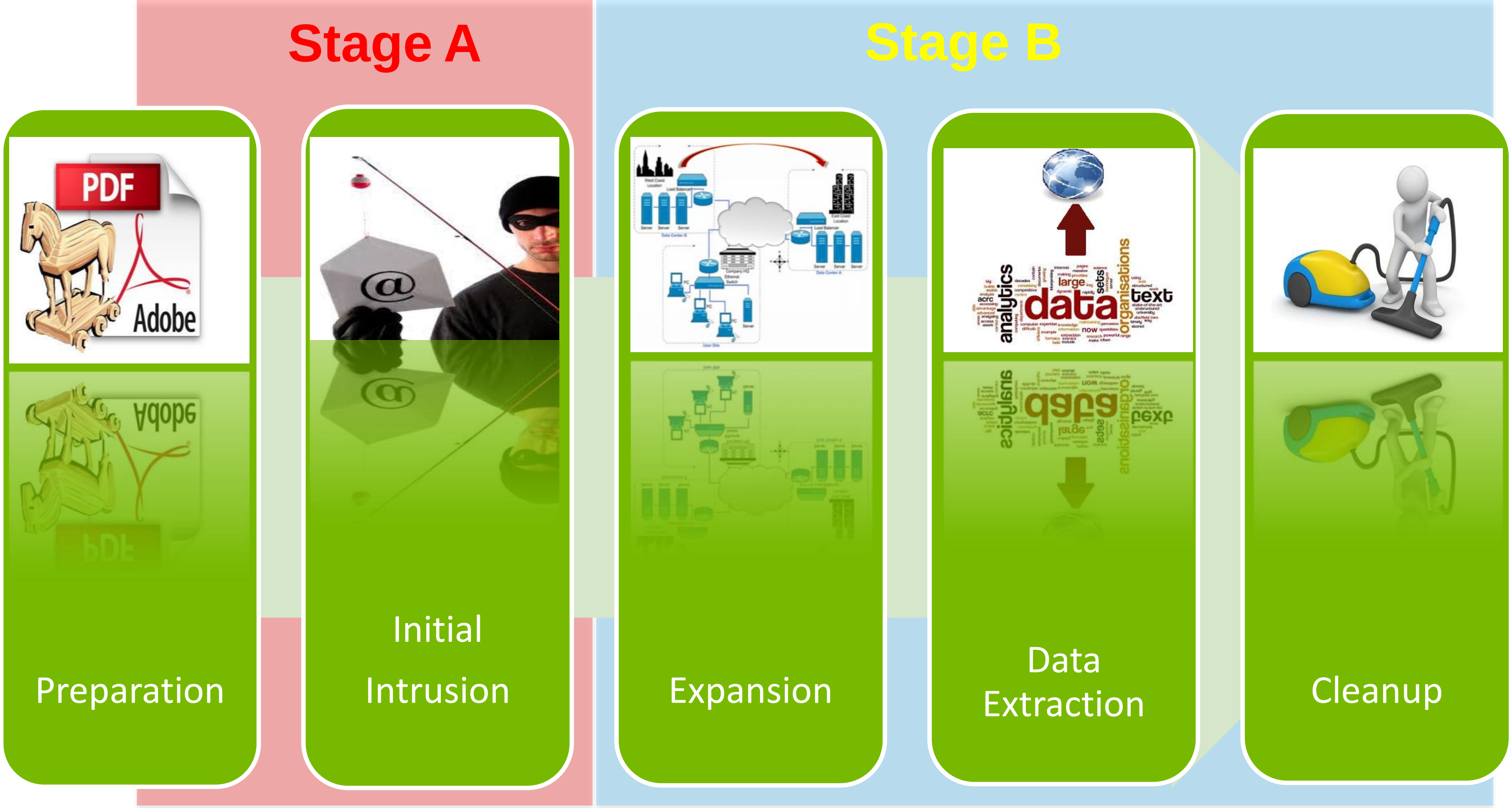
- High Impact
  - Loss of Critical Data
  - Loss of Availibility on Critical Business Services
  - Loss of Customer
  - Loss of Brand and Reputation

Holistic 3D Security Strategy



nSA: netbull 3D* Security Architecture

APT Detection and Prevention using nSA



Stage A

Stage B

Preparation

Initial Intrusion

Expansion

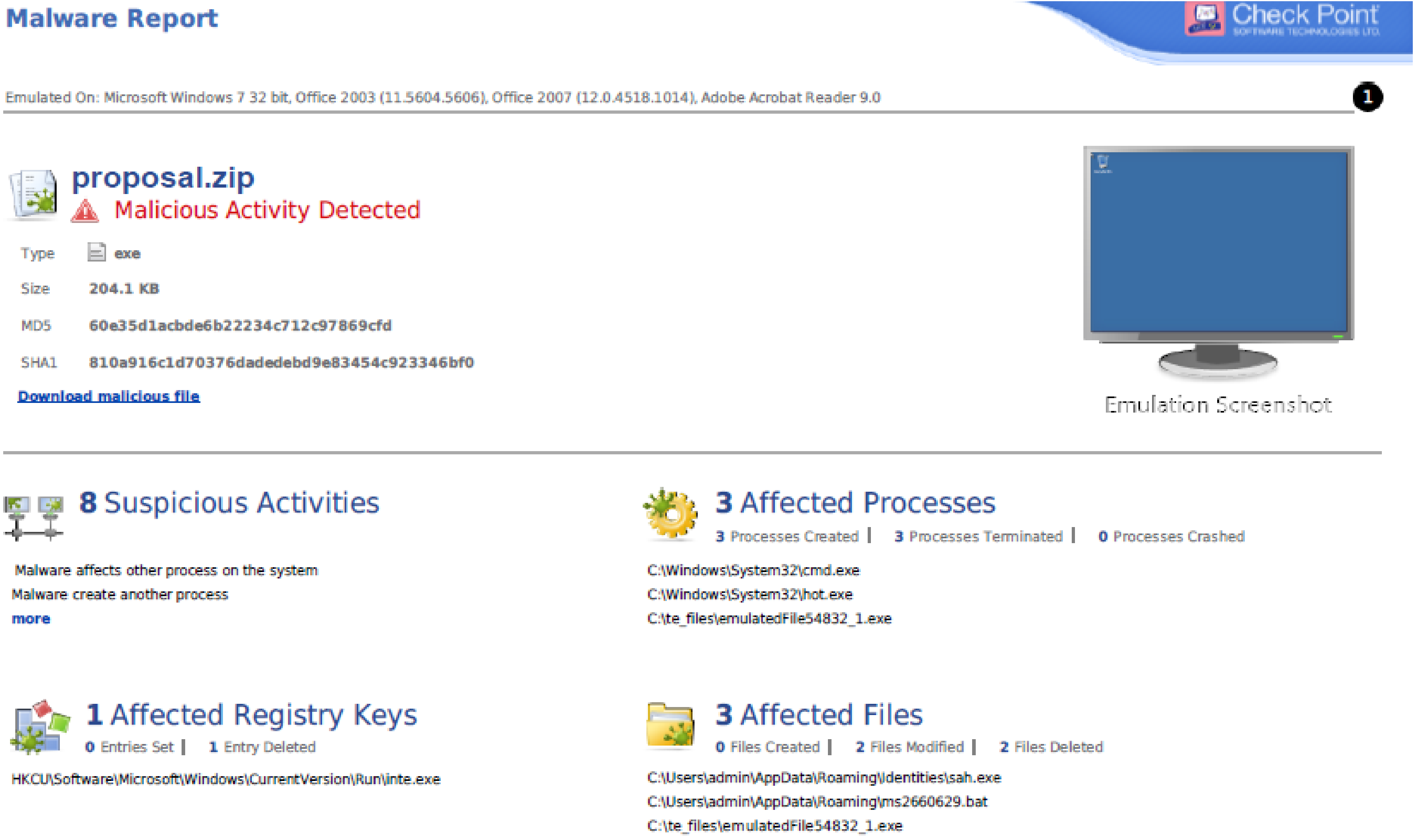
Data Extraction

Cleanup

Stage A: Detect and Prevent nSA Building Blocks

Signs of Intrusion	Description	Building Block
Suspicious e-mails	Email is the most widely used entry point for targeted attacks	E-mail Security Gateway
“Zero” Day Malware	**Malware are typically hidden in common file formats (pdf, html,exe etc)**	**Threat Emulation Technology (“Sandbox”)**
Suspicious Connections	Attacks can often use IP addresses, websites, files, and email servers with a history of malicious activity	• Threat Intelligent • Web Security Gateway • E-mail Security Gateway

Checkpoint Threat Emulation Technology



Malware Report

Emulated On: Microsoft Windows 7 32 bit, Office 2003 (11.5604.5606), Office 2007 (12.0.4518.1014), Adobe Acrobat Reader 9.0

proposal.zip

Malicious Activity Detected

Type	exe
Size	204.1 KB
MD5	60e35d1acbde6b22234c712c97869cfd
SHA1	810a916c1d70376dadedebd9e83454c923346bf0

Download malicious file

Emulation Screenshot

8 Suspicious Activities

Malware affects other process on the system
Malware create another process
more

3 Affected Processes

3 Processes Created | **3** Processes Terminated | **0** Processes Crashed

C:\Windows\System32\cmd.exe
C:\Windows\System32\hot.exe
C:\te_files\emulatedFile54832_1.exe

1 Affected Registry Keys

0 Entries Set | **1** Entry Deleted

HKCU\Software\Microsoft\Windows\CurrentVersion\Run\inte.exe

3 Affected Files

0 Files Created | **2** Files Modified | **2** Files Deleted

C:\Users\admin\AppData\Roaming\Identities\sah.exe
C:\Users\admin\AppData\Roaming\ms2660629.bat
C:\te_files\emulatedFile54832_1.exe

Stage B: Detect and Prevent nSA Building Blocks

Signs of Intrusion	Description	Building Block
Anomalous Traffic	Unexpected changes in protocol usage, traffic volume , and user behavior.	Network Anomaly Traffic Detection
Data Access Attempts	Unauthorized attempts to access critical database structures are a high sign your network may be compromised	• Database Activity Monitoring • File Share Monitoring
Data Transfer	Unauthorized attempts to access critical data are a high sign your network may be compromised	• Data Leakage Prevention • Network Anomaly Traffic
Bot Connections	Bots play a key role in targeted	• Antibot

24 x 7 Security Monitoring

- Protect against internal and external threats
- Obtain comprehensive visibility into the security activity on your network
- Extend your team with security experts at your service 24x7
- Threat Intelligent
- Security Operation Center

Implemented in days - not weeks or months

netbull