TeleTrusT
Pioneers in IT security.

TeleTrusT-Informationstag "IT-Forensik"

Berlin, 12.05.2016

Moderne Honigtöpfe im Zeitalter scheiternder Prävention

Bernhard Schildendorfer

SEC Consult Unternehmensberatung GmbH

whoami

Bernhard Schildendorfer | b.schildendorfer@sec-consult.com

Security Consultant | SEC Consult

… IT / Information Security in St. Pölten

… SEC-Consult since 02/2010

… Penetration Tester, Project Leader, …

… and some other interests

- A classical APT -

"The account of a user that was on vacation was locked due to failed logins"

- a SEC Consult Client


Foto: Fotolia 62727991, Westend61

… they succeeded … and they will come back

Conclusion

- Traditional Security fails against targeted attacks
- Too little is spent on monitoring & response
- Tailored security breaches are inevitable

What to do?

Security is all about
knowing & preparation!

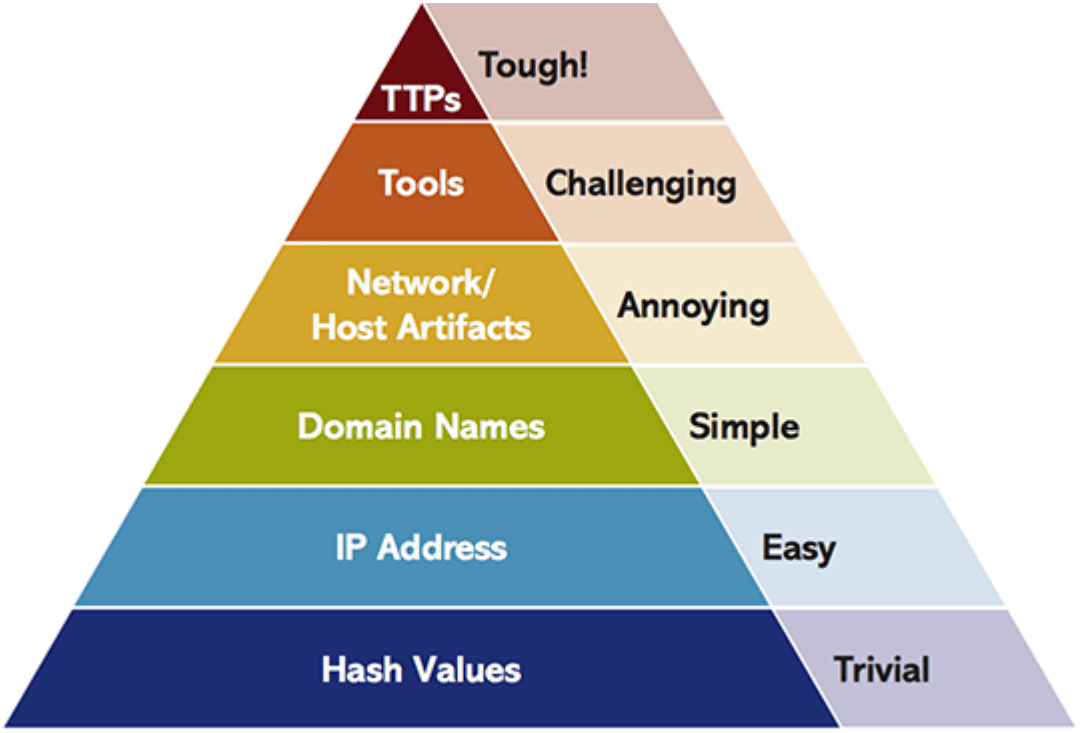
WHAT IF you are able to…

- get their **motivation**?
- get their **TTP**‘s
- **identify** the attacker(s)?

Knowing - Global Threat Intelligence?

Indicators of compromise (IOCs) / Signature feeds

- Malicious IPs
- Malicious domains
- Malware hashes
- Phishing e-mails
- Misc. fingerprints



Source: David J. Bianco, personal blog

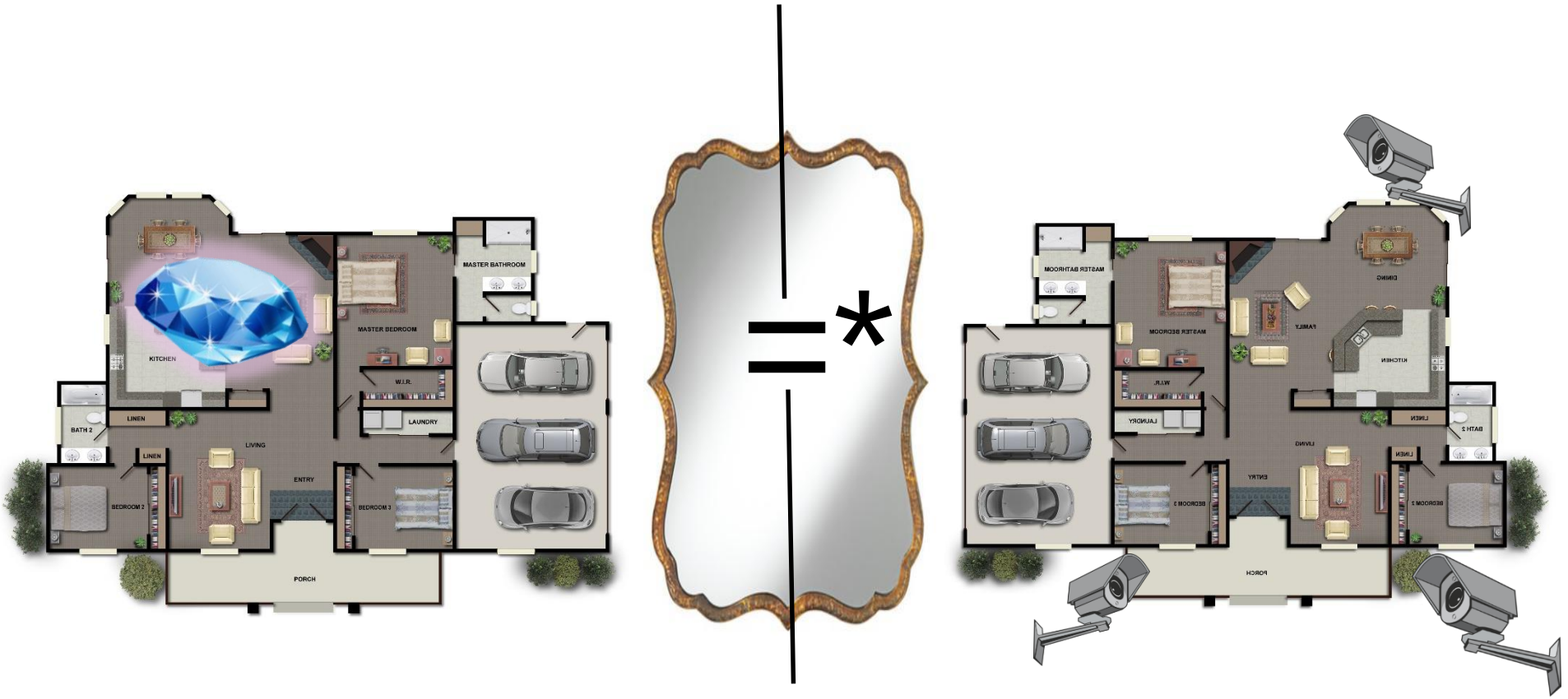
Patient 0

The Dilemma

- Patient 0
- Attacker only needs to **breach once**
- Defender needs to be **constantly aware**
- Defender can only **react** after breach

Why not change this?

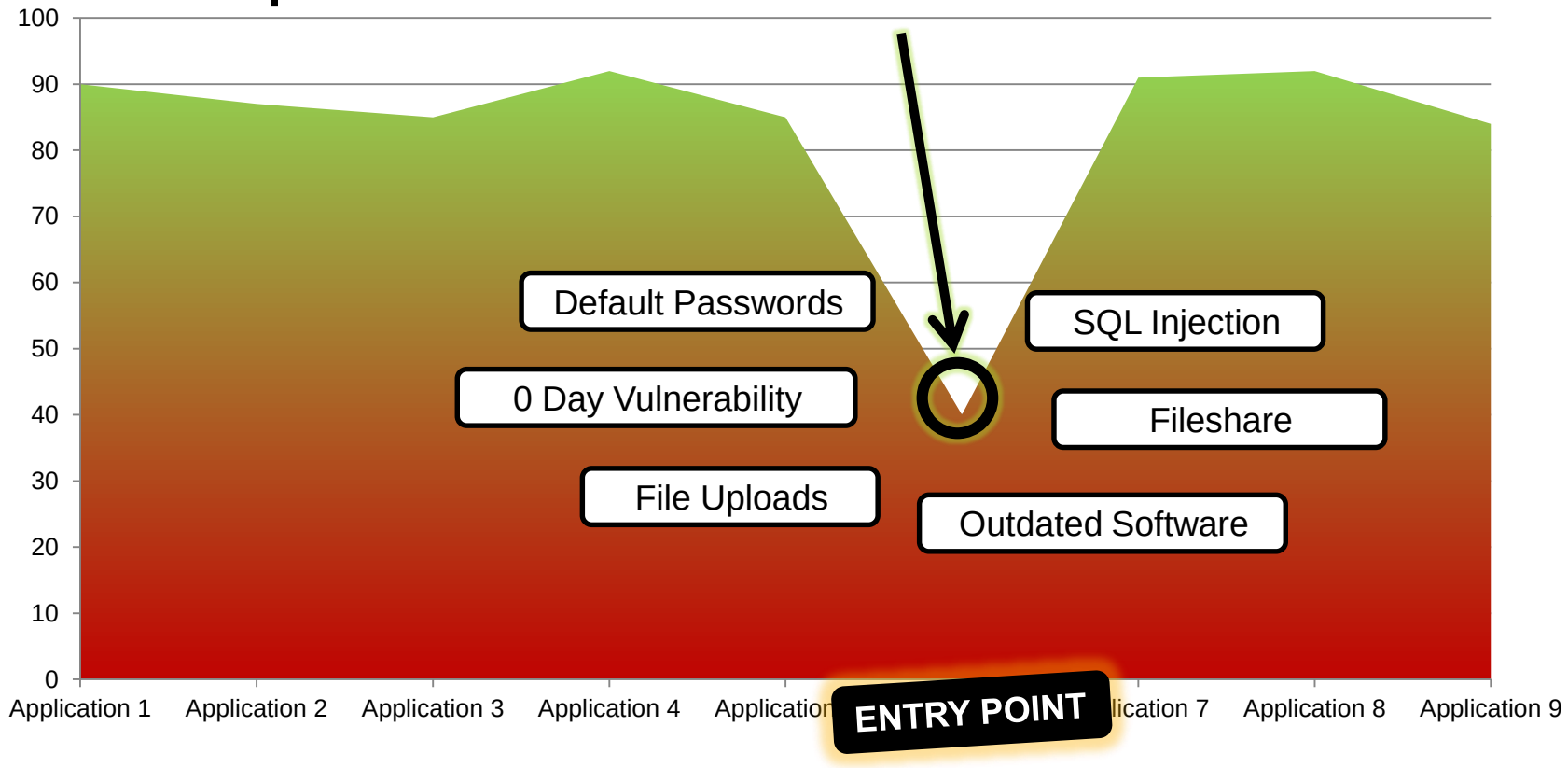
Look in the Mirror…



*Almost

How to Redirect the attacker?

Place a weak link in the exposed infrastructure



Looking at the Dilemma again

- ✓ Patient 0
- ✓ Attacker only needs to **breach once**
- ✓ Defender needs to be **constantly aware**
- ✓ Defender can only **react** after breach

Situation changed!

Know Your Enemy

Be close to your enemies!

- Find out **where** they come into your system
- Find out **what tools** they are using
- Find out **what they are after**
- Find out **what their motivation** is

Build your own
***LOCAL* THREAT INTELLIGENCE**

13.04.2015

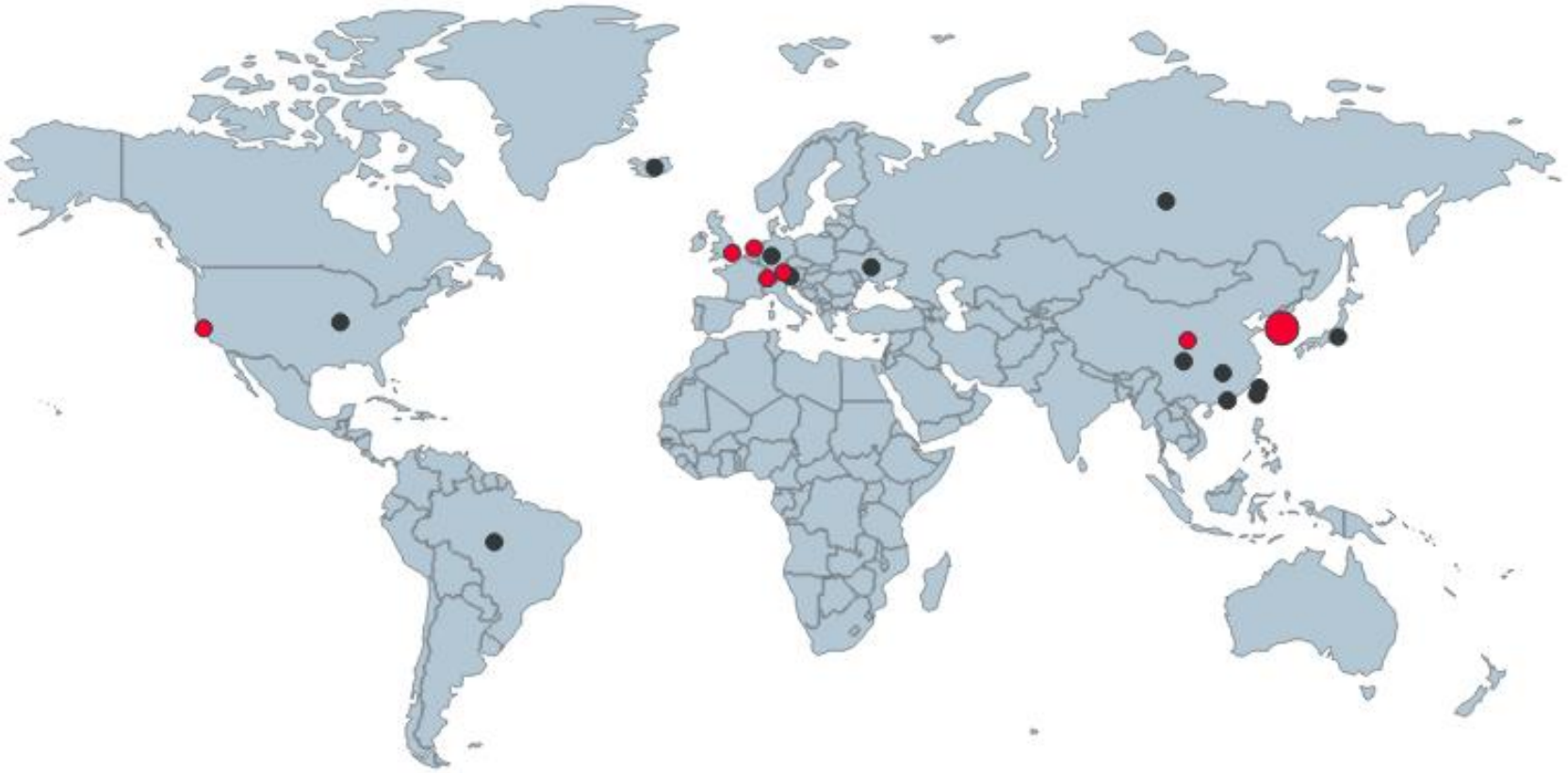
Hello!

4103 IOCs were detected on the following units:

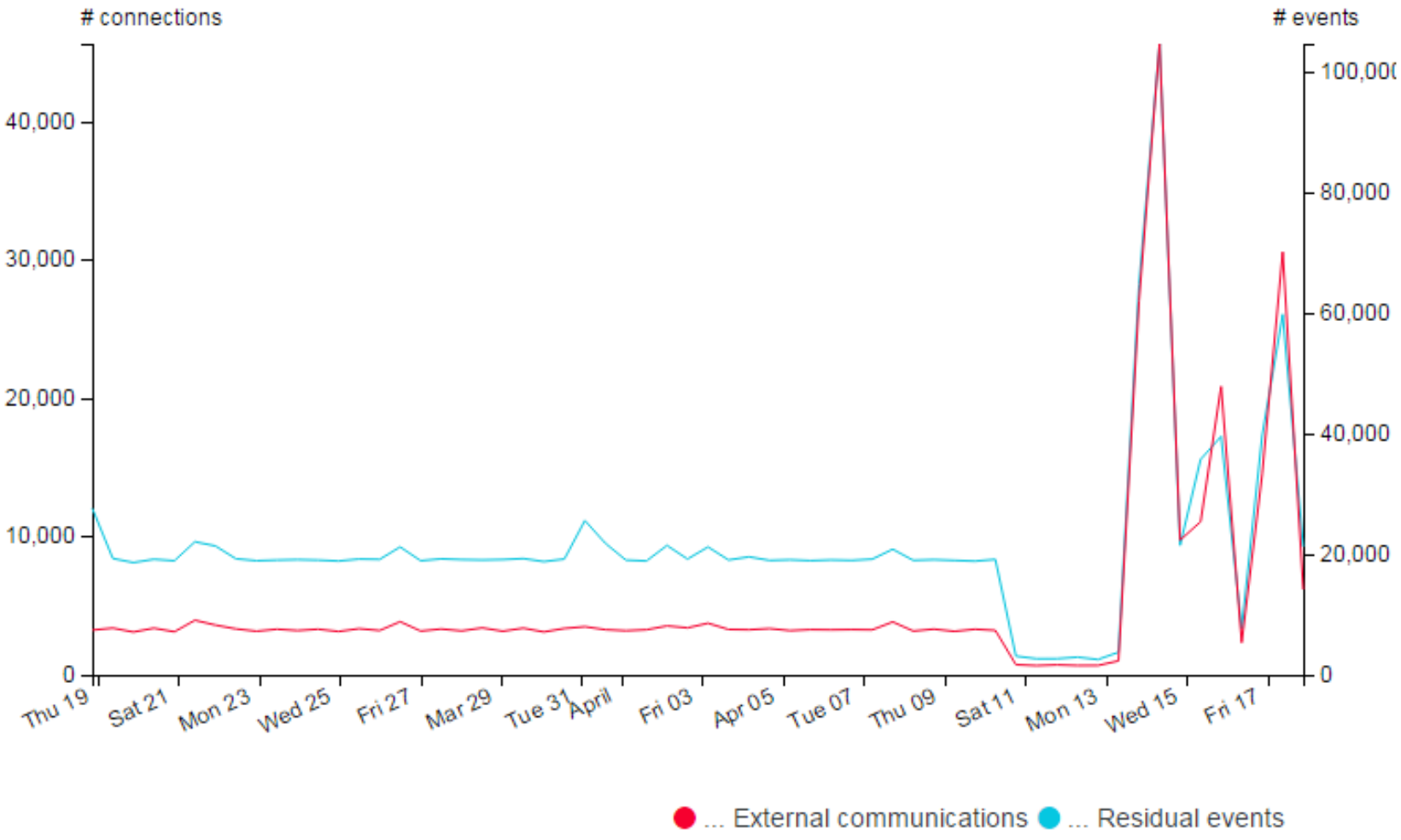
```
  websrv01.wbdmz.local: 3122
   dbsrv01.wbdmz.local:  981
```

Click here to access the Dashboard.

Connection Atlas



Activity Graph

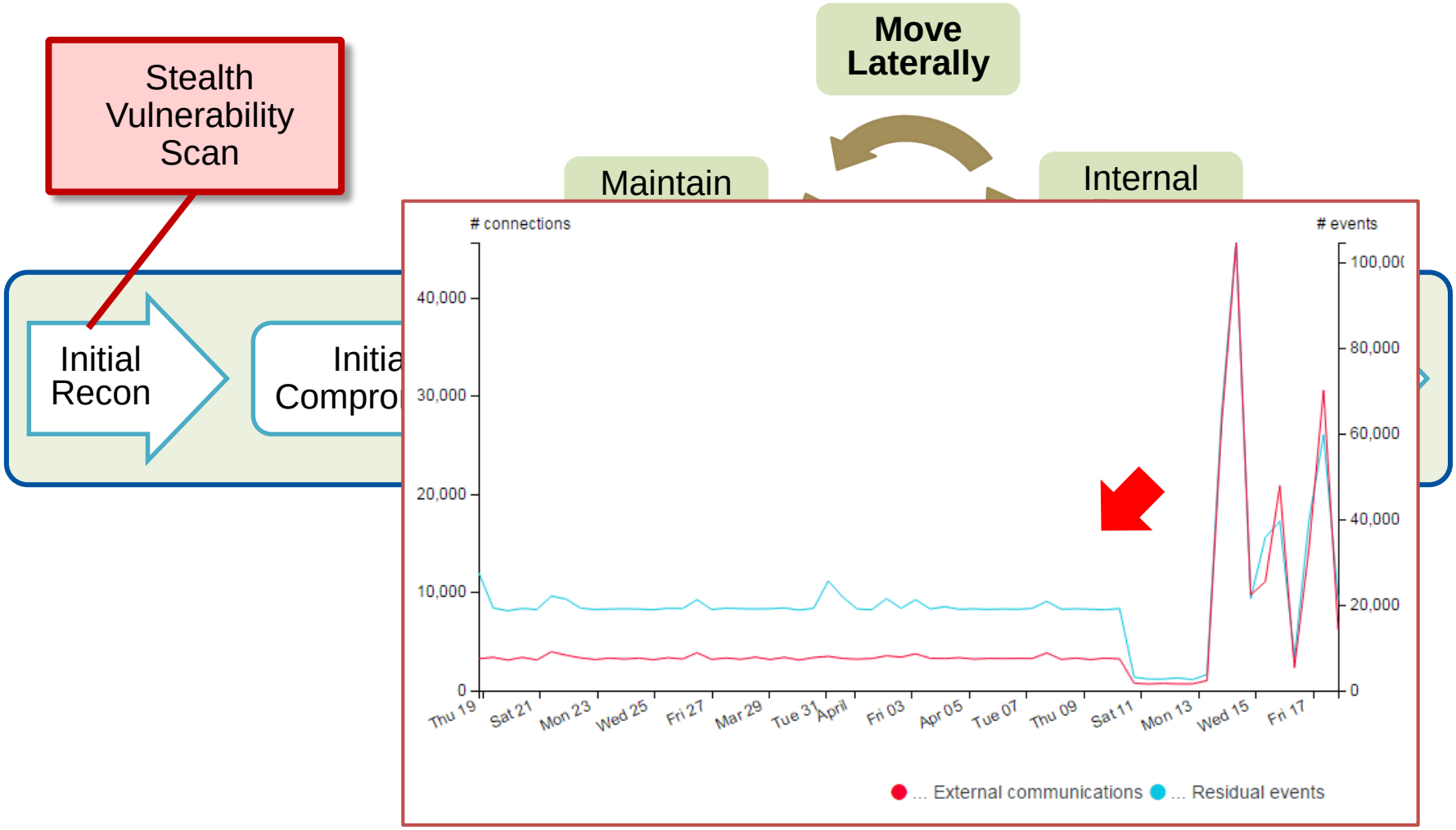


Live Alerts

Live Alerts ?

08:42:00	D	01	System	systeminfo
2015-04-13 08:42:00	D	01	System	cmd.exe /c systeminfo
2015-04-13 08:40:14	D	01	Network Commands	net view
2015-04-13 08:40:14	D	01	Network Commands	net view
2015-04-13 08:40:14	D	01	Network Commands	cmd.exe /c net view
2015-04-13 08:40:04	D	01	Network Commands	ipconfig
2015-04-13 08:40:04	D	01	Network Commands	cmd.exe /c ipconfig
2015-04-13 08:39:57	D	01	System	whoami
2015-04-13 08:39:57	D	01	System	cmd.exe /c whoami
2015-04-13 08:39:51	D	01	System	cmd.exe /c set
2015-04-13 08:36:10	D	01	Deployment Related	CREATE \Device\HarddiskVolume2\inetpub\wwwroot\upload\Admin\r00ts.aspx

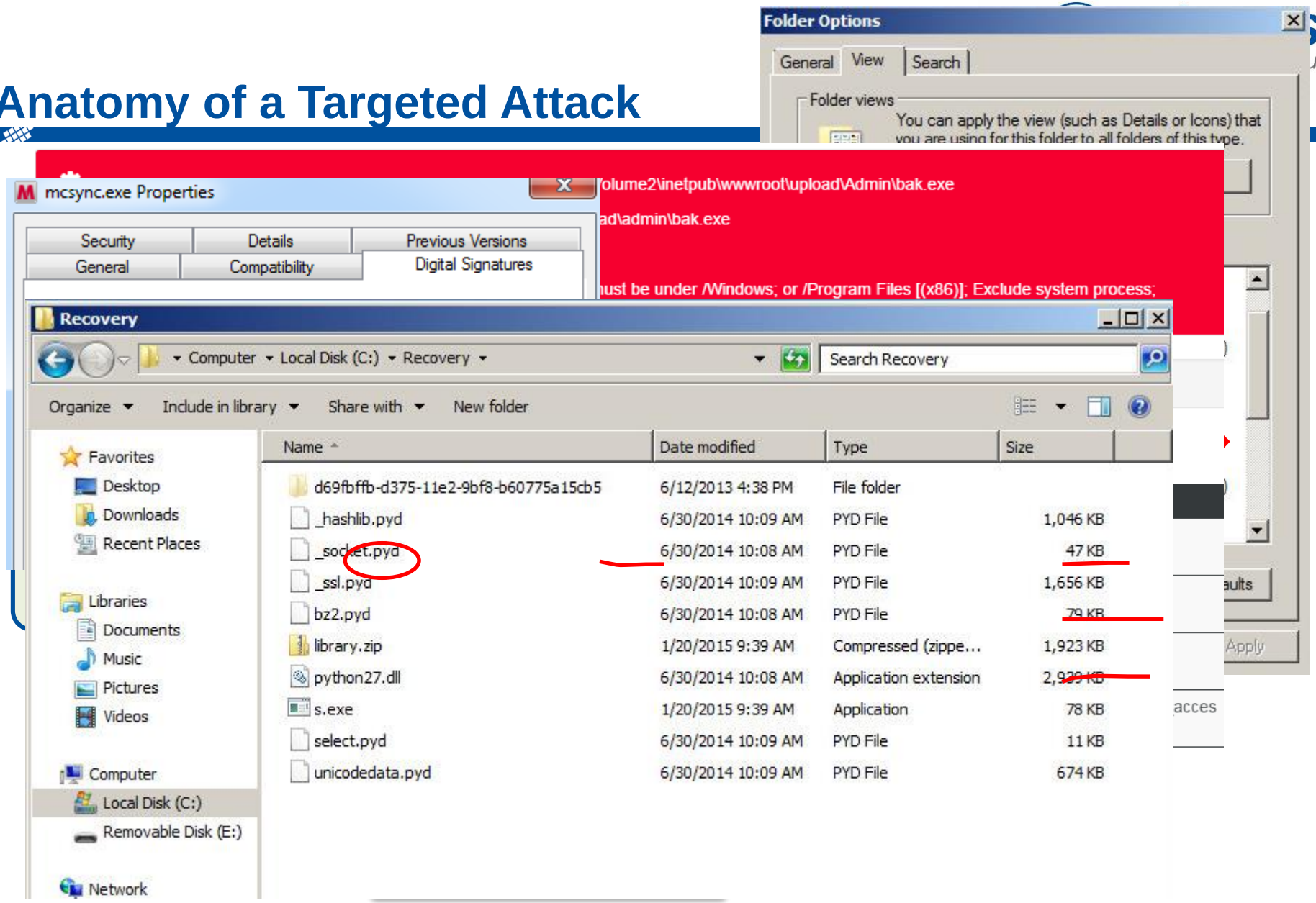
Anatomy of a Targeted Attack



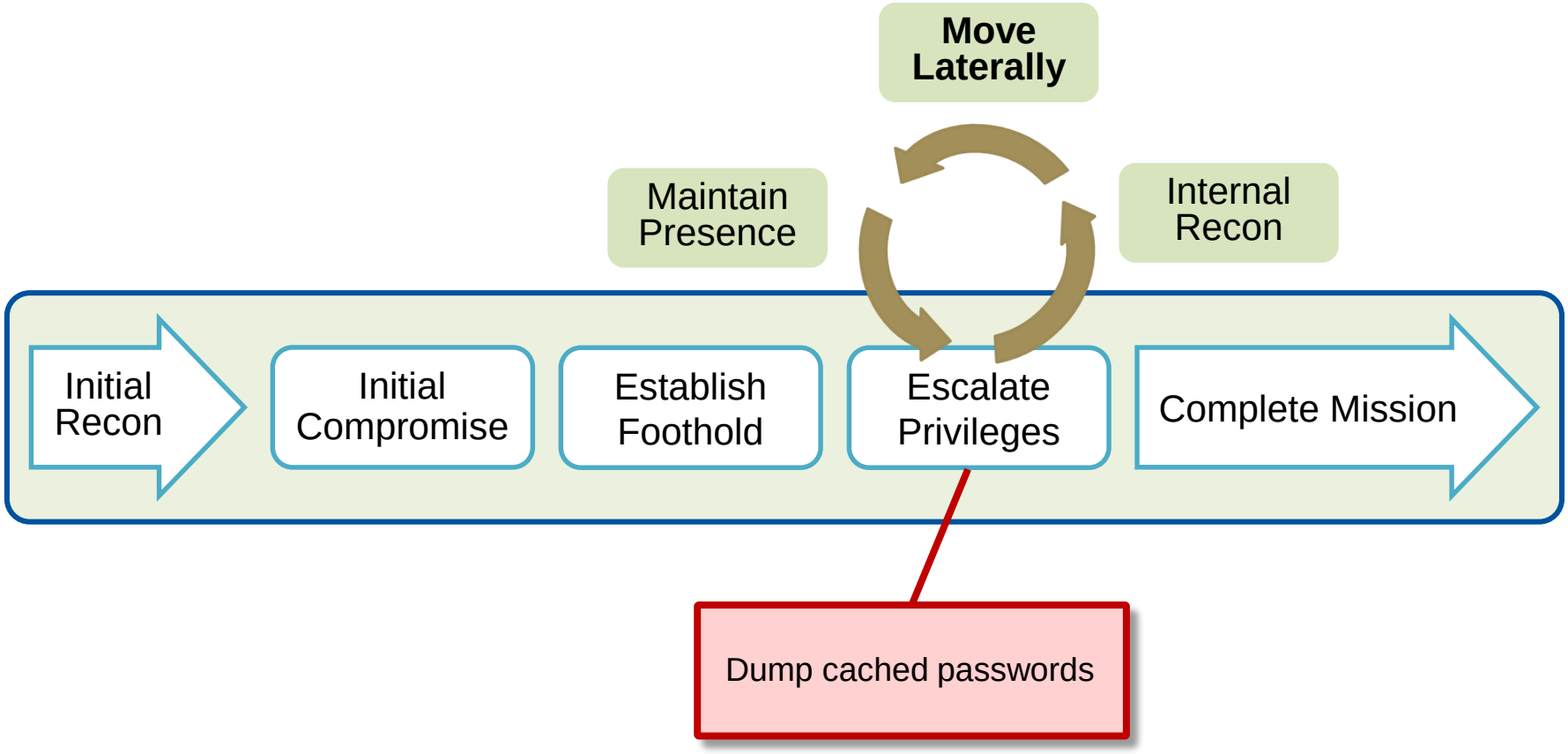
Anatomy of a Targeted Attack

- SQL Injection
- Broken File Upload

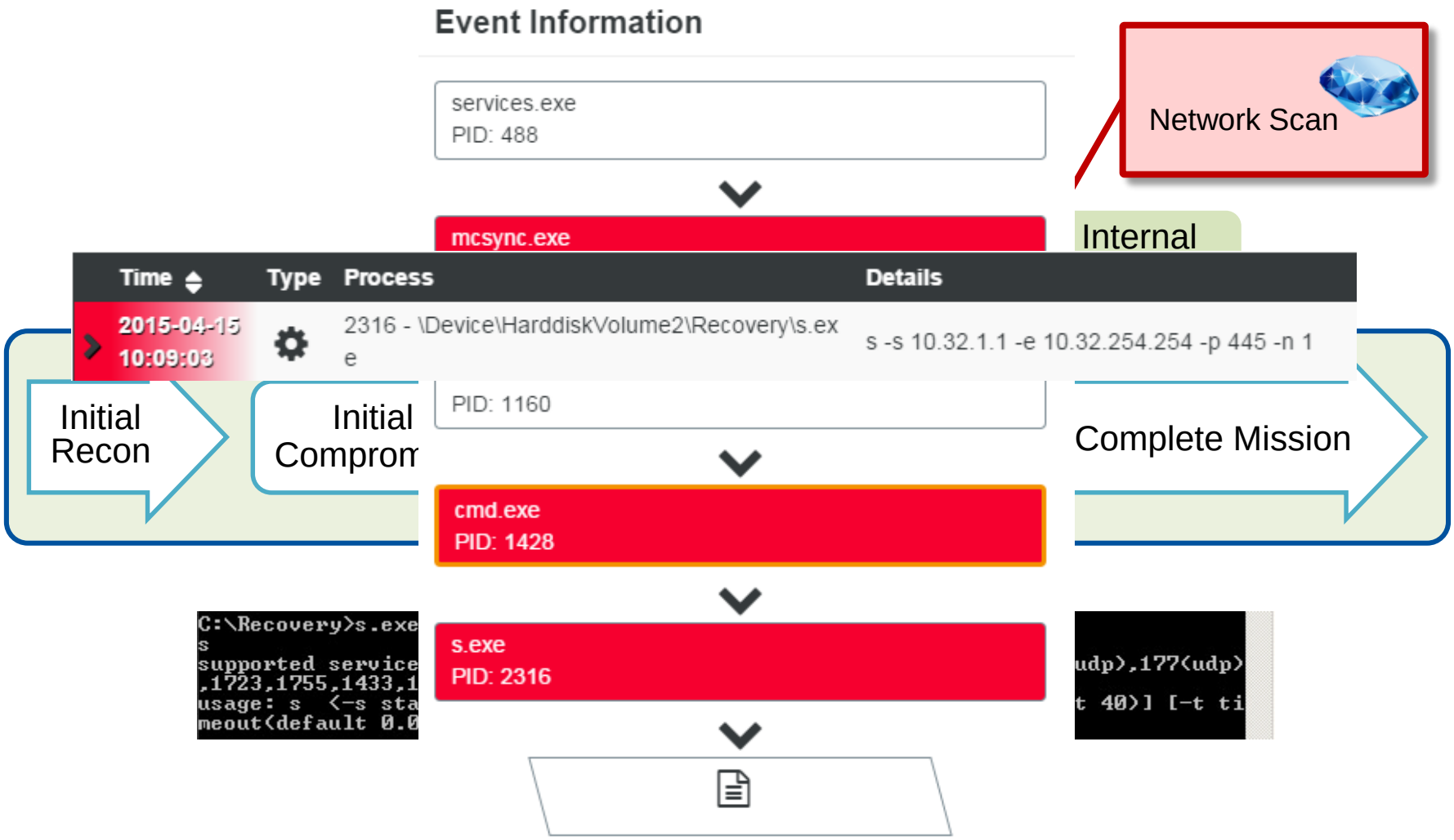
Anatomy of a Targeted Attack



Anatomy of a Targeted Attack



Anatomy of a Targeted Attack



Anatomy of a Targeted Attack

Move Laterally

- Windows commands
- Remote cronjob

Name	Status	Triggers	Next Run Time	Last Run Time
At1	Ready	At 8:02 AM on 4/14/2015		4/14/2015 8:02:00 AM
At2	Ready	At 3:49 AM on 4/14/2015		4/14/2015 3:48:59 AM

Unit	Time	Type	Process	Details
DI 01	2015-04-14 03:46:44		2512 - \Device\HarddiskVolume2\Windows\System32\cmd.exe	cmd.exe /c at \\DI 02 3:49 c:\windows\bak.exe
DI 01	2015-04-14 03:46:13		2288 - \Device\HarddiskVolume2\Windows\System32\cmd.exe	cmd.exe /c at \\D 02 8:02 c:\windows\bak.exe

General | Triggers | Actions | Conditions | Settings | History

When you create a task, you must specify the action that will occur when your task starts. To ch
task property pages using the Properties command.

Action	Details
Start a program	c:\windows\bak.exe

Conclusion

- Working time:
  ~ 3am - ~ 2pm (CET)
- Identified motivation
- Attributed infrastructure
- Generation of signatures

Takeaways

- Prevention fails
  - →**Preparation is key**
- Improve monitoring & detection capabilities
  - →**Know your enemies**
- **Increase time to defend**
  - →Homefield advantage
  - →Do the homework

Takeaways

„If you know your enemies and know yourself, you will not be imperiled in a hundred battles“

- Sun Tzu, The Art of War

Contact

AUSTRIA

SEC Consult Unternehmensberatung GmbH
Mooslackengasse 17
1190 Vienna

Tel +43 1 890 30 43 0 | **Fax** +43 1 890 30 43 15
Email office@sec-consult.com

www.sec-consult.com

GERMANY

SEC Consult Unternehmensberatung Deutschland GmbH
Ullsteinstraße 118
D-12109 Berlin

Email office-berlin@sec-consult.com

SWITZERLAND

SEC Consult (Schweiz) AG
Turbinenstrasse 28
8005 Zürich

Tel +41 44 271 777 0 | **Fax** +43 1 890 30 43 15
Email office-zurich@sec-consult.com

AUSTRIA

SEC Consult Unternehmensberatung GmbH
Komarigasse 14/1
2700 Wiener Neustadt

Tel +43 1 890 30 43 0
Email office@sec-consult.com

RUSSIA

CJCS Security Monitor
5th Donskoy proyezd, 15, Bldg. 6
119334, Moscow

Tel +7 495 662 1414
Email info@securitymonitor.ru

CANADA

i-SEC Consult Inc.
100 René-Lévesque West, Suite 2500
Montréal (Quebec) H3B 5C9

Email office-montreal@sec-consult.com

SINGAPORE

SEC Consult Singapore PTE. LTD
4 Battery Road
#25-01 Bank of China Building
Singapore (049908)

Email office-singapore@sec-consult.com

LITHUANIA

UAB Critical Security, a SEC Consult company
Sauletekio al. 15-311
10224 Vilnius

Tel +370 5 2195535
Email office-vilnius@sec-consult.com

THAILAND

SEC Consult (Thailand) Co.,Ltd.
29/1 Piyaplace Langsuan Building 16th Floor, 16B
Soi Langsuan, Ploen Chit Road
Lumpini, Patumwan | Bangkok 10330

Email office-vilnius@sec-consult.com