DIGITAL GUARDIAN
Formerly VERDASYS

DEEPSEC
IN-DEPTH SECURITY

Temet Nosce: Know Thy Endpoint Through and Through

Thomas V. Fischer

I am …

- Threat Researcher
- 25+ years experience in InfoSec
- Spent number years in IR team positions

- Director @BSidesLondon

- Contact
  - tfischer@digitalguardian.com
  - tvfischer+sans@gmail.com
  - @Fvt
  - keybase.io/fvt

GIAC CERTIFIED INCIDENT HANDLER

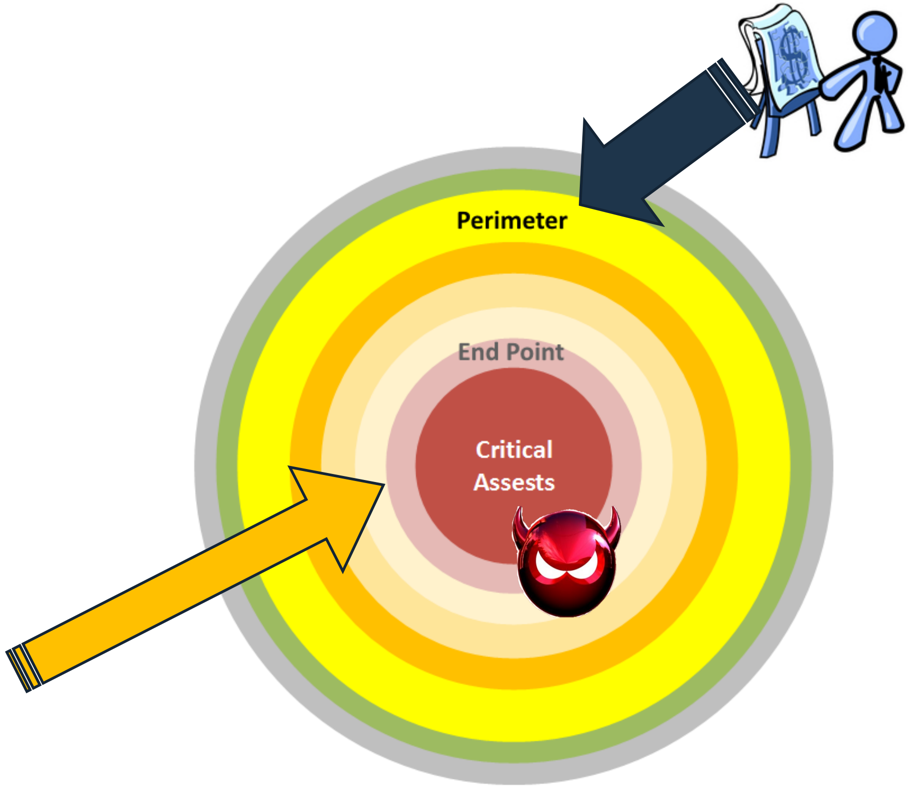
GCIH

A Journey into the end point

- Being in the right place at the right time
- Real time actionable intelligence
- (re)Enabling the end point as an active defence mechanism
- Detecting behaviour…

Defense in *un*-depth

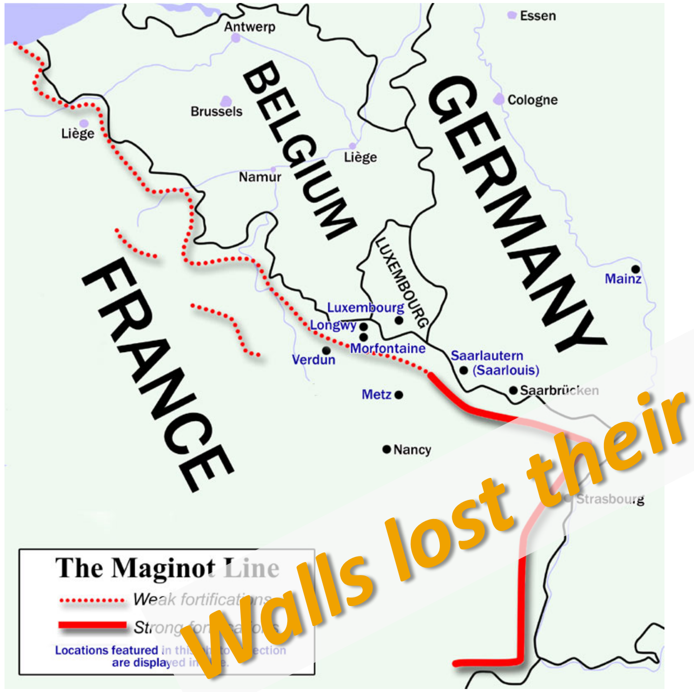
- Strong focus on network solutions
- Lost faith in the end point solutions
- Afraid to go back



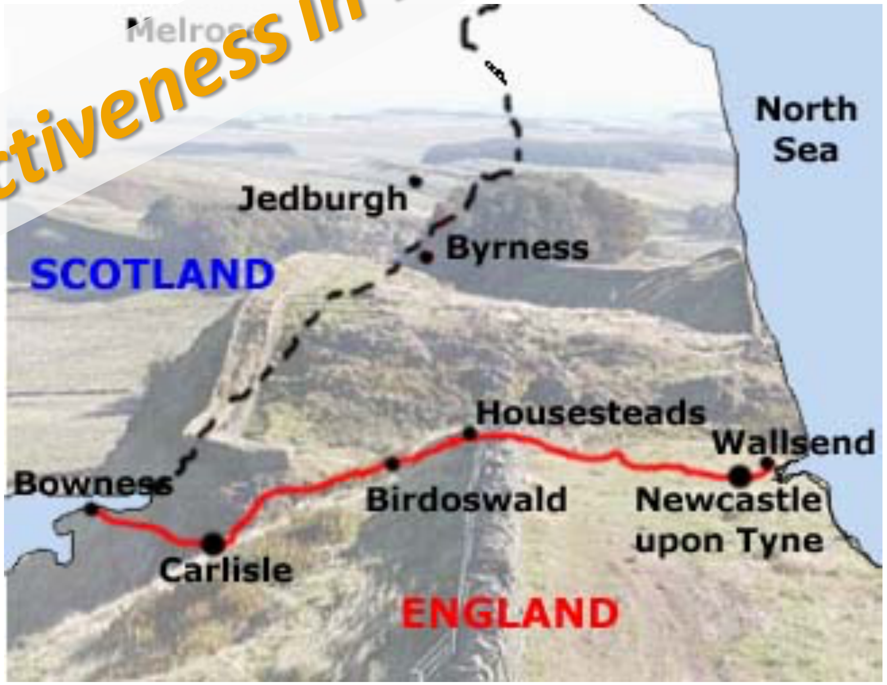
But that's not where the important stuff is…

DEEPSEC

Walls, Walls, Walls...



Walls lost their effectiveness in 1545

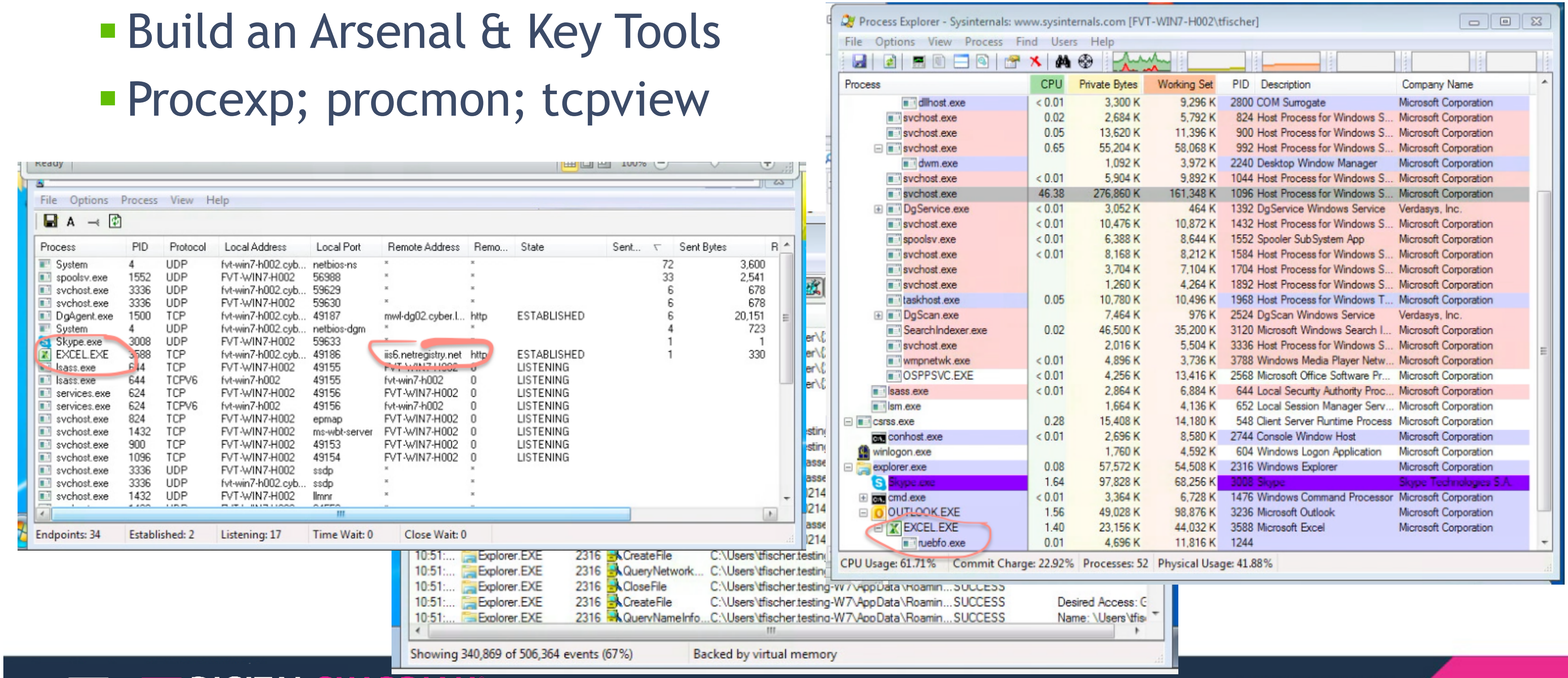


Are we in the wrong place

- Reliance on next-gen *network* detection
- Endpoint solution tend towards post incident
- Something suspicious in logs :- activate endpoint resolution
- Forensics ~ what changed != necessarily what happened

World of information...

- Build an Arsenal & Key Tools
- Procexp; procmon; tcpview



Process Explorer - Sysinternals: www.sysinternals.com [FVT-WIN7-H002\tfischer]

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
dllhost.exe	< 0.01	3,300 K	9,296 K	2800	COM Surrogate	Microsoft Corporation
svchost.exe	0.02	2,684 K	5,792 K	824	Host Process for Windows S...	Microsoft Corporation
svchost.exe	0.05	13,620 K	11,396 K	900	Host Process for Windows S...	Microsoft Corporation
svchost.exe	0.65	55,204 K	58,068 K	992	Host Process for Windows S...	Microsoft Corporation
dwm.exe		1,092 K	3,972 K	2240	Desktop Window Manager	Microsoft Corporation
svchost.exe	< 0.01	5,904 K	9,892 K	1044	Host Process for Windows S...	Microsoft Corporation
svchost.exe	46.38	276,860 K	161,348 K	1096	Host Process for Windows S...	Microsoft Corporation
DgService.exe	< 0.01	3,052 K	464 K	1392	DgService Windows Service	Verdasys, Inc.
svchost.exe	< 0.01	10,476 K	10,872 K	1432	Host Process for Windows S...	Microsoft Corporation
spoolsv.exe	< 0.01	6,388 K	8,644 K	1552	Spooler SubSystem App	Microsoft Corporation
svchost.exe	< 0.01	8,168 K	8,212 K	1584	Host Process for Windows S...	Microsoft Corporation
svchost.exe		3,704 K	7,104 K	1704	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,260 K	4,264 K	1892	Host Process for Windows S...	Microsoft Corporation
taskhost.exe	0.05	10,780 K	10,496 K	1968	Host Process for Windows T...	Microsoft Corporation
DgScan.exe		7,464 K	976 K	2524	DgScan Windows Service	Verdasys, Inc.
SearchIndexer.exe	0.02	46,500 K	35,200 K	3120	Microsoft Windows Search I...	Microsoft Corporation
svchost.exe		2,016 K	5,504 K	3336	Host Process for Windows S...	Microsoft Corporation
wmpnetwk.exe	< 0.01	4,896 K	3,736 K	3788	Windows Media Player Netw...	Microsoft Corporation
OSPPSVC.EXE	< 0.01	4,256 K	13,416 K	2568	Microsoft Office Software Pr...	Microsoft Corporation
lsass.exe	< 0.01	2,864 K	6,884 K	644	Local Security Authority Proc...	Microsoft Corporation
lsm.exe		1,664 K	4,136 K	652	Local Session Manager Serv...	Microsoft Corporation
csrss.exe	0.28	15,408 K	14,180 K	548	Client Server Runtime Process	Microsoft Corporation
conhost.exe	< 0.01	2,696 K	8,580 K	2744	Console Window Host	Microsoft Corporation
winlogon.exe		1,760 K	4,592 K	604	Windows Logon Application	Microsoft Corporation
explorer.exe	0.08	57,572 K	54,508 K	2316	Windows Explorer	Microsoft Corporation
Skype.exe	1.64	97,828 K	68,256 K	3008	Skype	Skype Technologies S.A.
cmd.exe	< 0.01	3,364 K	6,728 K	1476	Windows Command Processor	Microsoft Corporation
OUTLOOK.EXE	1.56	49,028 K	98,876 K	3236	Microsoft Outlook	Microsoft Corporation
EXCEL.EXE	1.40	23,156 K	44,032 K	3588	Microsoft Excel	Microsoft Corporation
ruebfo.exe	0.01	4,696 K	11,816 K	1244		

CPU Usage: 61.71% Commit Charge: 22.92% Processes: 52 Physical Usage: 41.88%

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remo...	State	Sent...	Sent Bytes
System	4	UDP	fvt-win7-h002.cyb...	netbios-ns	*	*		72	3,600
spoolsv.exe	1552	UDP	FVT-WIN7-H002	56988	*	*		33	2,541
svchost.exe	3336	UDP	fvt-win7-h002.cyb...	59629	*	*		6	678
svchost.exe	3336	UDP	FVT-WIN7-H002	59630	*	*		6	678
DgAgent.exe	1500	TCP	fvt-win7-h002.cyb...	49187	mwl-dg02.cyber.l...	http	ESTABLISHED	6	20,151
System	4	UDP	fvt-win7-h002.cyb...	netbios-dgm	*	*		4	723
Skype.exe	3008	UDP	FVT-WIN7-H002	59633	*	*		1	1
EXCEL.EXE	3588	TCP	fvt-win7-h002.cyb...	49186	iis6.netregistry.net	http	ESTABLISHED	1	330
lsass.exe	644	TCP	FVT-WIN7-H002	49155	FVT-WIN7-H002	0	LISTENING		
lsass.exe	644	TCPV6	fvt-win7-h002	49155	fvt-win7-h002	0	LISTENING		
services.exe	624	TCP	FVT-WIN7-H002	49156	FVT-WIN7-H002	0	LISTENING		
services.exe	624	TCPV6	fvt-win7-h002	49156	fvt-win7-h002	0	LISTENING		
svchost.exe	824	TCP	FVT-WIN7-H002	epmap	FVT-WIN7-H002	0	LISTENING		
svchost.exe	1432	TCP	FVT-WIN7-H002	ms-wbt-server	FVT-WIN7-H002	0	LISTENING		
svchost.exe	900	TCP	FVT-WIN7-H002	49153	FVT-WIN7-H002	0	LISTENING		
svchost.exe	1096	TCP	FVT-WIN7-H002	49154	FVT-WIN7-H002	0	LISTENING		
svchost.exe	3336	UDP	FVT-WIN7-H002	ssdp	*	*			
svchost.exe	3336	UDP	fvt-win7-h002.cyb...	ssdp	*	*			
svchost.exe	1432	UDP	FVT-WIN7-H002	llmnr	*	*			

Endpoints: 34 Established: 2 Listening: 17 Time Wait: 0 Close Wait: 0

10:51:...	Explorer.EXE	2316	CreateFile	C:\Users\tfischer.testing		
10:51:...	Explorer.EXE	2316	QueryNetwork...	C:\Users\tfischer.testing		
10:51:...	Explorer.EXE	2316	CloseFile	C:\Users\tfischer.testing-W7\AppData\Roamin...	SUCCESS	
10:51:...	Explorer.EXE	2316	CreateFile	C:\Users\tfischer.testing-W7\AppData\Roamin...	SUCCESS	Desired Access: G
10:51:...	Explorer.EXE	2316	QueryNameInfo...	C:\Users\tfischer.testing-W7\AppData\Roamin...	SUCCESS	Name: \Users\tfis

Showing 340,869 of 506,364 events (67%) Backed by virtual memory

Deep dive...

Application DNA

- Build information events

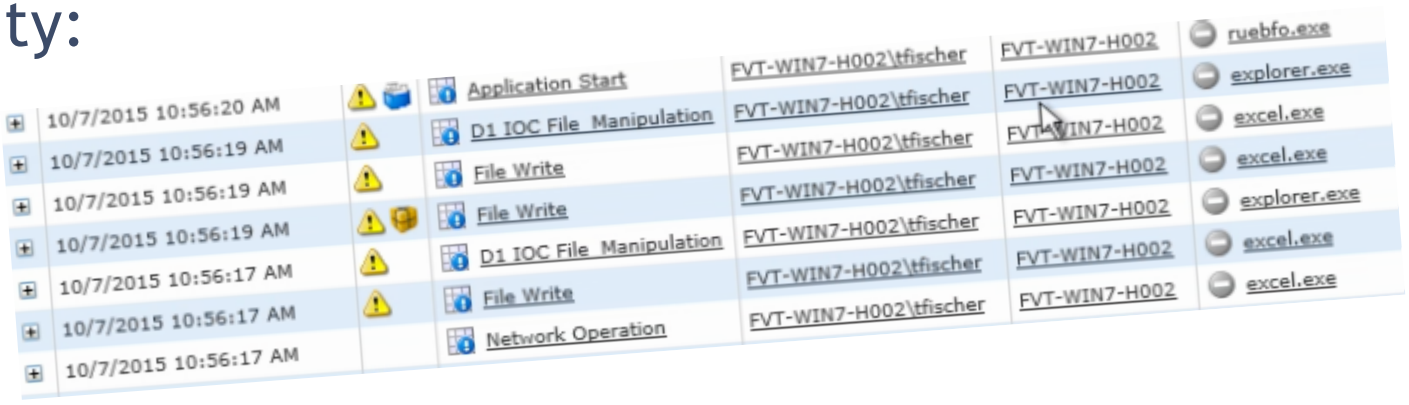
- Track similar events together

- Use the API right hooks where appropriate

- Associate a sequence of events into one action
  - Sequence of file read/file writes :- file edit
  - Track renames, or read/writes :- file move

Single Footprint Intelligence

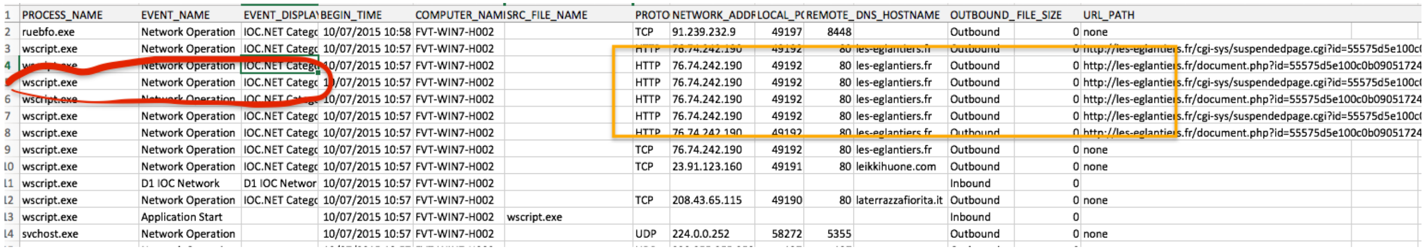
- Sysinternals tools on steroids
- High level of visibility:
  - File ops
  - Network ops
  - Registry ops
  - DLL activity
  - Process data



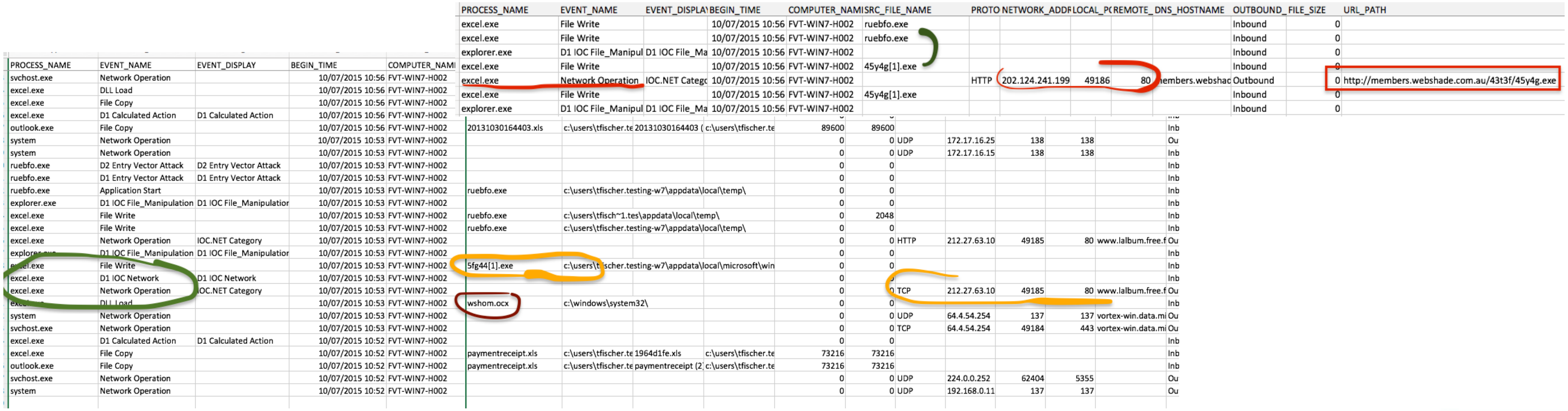
⊞	10/7/2015 10:56:20 AM	⚠	Application Start	FVT-WIN7-H002\tfischer	FVT-WIN7-H002	ruebfo.exe
⊞	10/7/2015 10:56:19 AM	⚠	D1 IOC File Manipulation	FVT-WIN7-H002\tfischer	FVT-WIN7-H002	explorer.exe
⊞	10/7/2015 10:56:19 AM	⚠	File Write	FVT-WIN7-H002\tfischer	FVT-WIN7-H002	excel.exe
⊞	10/7/2015 10:56:19 AM	⚠	File Write	FVT-WIN7-H002\tfischer	FVT-WIN7-H002	excel.exe
⊞	10/7/2015 10:56:17 AM	⚠	D1 IOC File Manipulation	FVT-WIN7-H002\tfischer	FVT-WIN7-H002	explorer.exe
⊞	10/7/2015 10:56:17 AM	⚠	File Write	FVT-WIN7-H002\tfischer	FVT-WIN7-H002	excel.exe
⊞	10/7/2015 10:56:17 AM		Network Operation	FVT-WIN7-H002\tfischer	FVT-WIN7-H002	excel.exe

Real Time Forensics Evidence

- Detect compromise events
- Log the foot prints



1	PROCESS_NAME	EVENT_NAME	EVENT_DISPLA\	BEGIN_TIME	COMPUTER_NAMI	SRC_FILE_NAME	PROTO	NETWORK_ADDF	LOCAL_PC	REMOTE_	DNS_HOSTNAME	OUTBOUND_	FILE_SIZE	URL_PATH
2	ruebfo.exe	Network Operation	IOC.NET Categc	10/07/2015 10:58	FVT-WIN7-H002		TCP	91.239.232.9	49197	8448		Outbound	0	none
3	wscript.exe	Network Operation	IOC.NET Categc	10/07/2015 10:57	FVT-WIN7-H002		HTTP	76.74.242.190	49192	80	les-eglantiers.fr	Outbound	0	http://les-eglantiers.fr/cgi-sys/suspendedpage.cgi?id=55575d5e100c(
4	wscript.exe	Network Operation	IOC.NET Categc	10/07/2015 10:57	FVT-WIN7-H002		HTTP	76.74.242.190	49192	80	les-eglantiers.fr	Outbound	0	http://les-eglantiers.fr/document.php?id=55575d5e100c0b09051724
5	wscript.exe	Network Operation	IOC.NET Categc	10/07/2015 10:57	FVT-WIN7-H002		HTTP	76.74.242.190	49192	80	les-eglantiers.fr	Outbound	0	http://les-eglantiers.fr/cgi-sys/suspendedpage.cgi?id=55575d5e100c(
6	wscript.exe	Network Operation	IOC.NET Categc	10/07/2015 10:57	FVT-WIN7-H002		HTTP	76.74.242.190	49192	80	les-eglantiers.fr	Outbound	0	http://les-eglantiers.fr/document.php?id=55575d5e100c0b09051724
7	wscript.exe	Network Operation	IOC.NET Categc	10/07/2015 10:57	FVT-WIN7-H002		HTTP	76.74.242.190	49192	80	les-eglantiers.fr	Outbound	0	http://les-eglantiers.fr/cgi-sys/suspendedpage.cgi?id=55575d5e100c(
8	wscript.exe	Network Operation	IOC.NET Categc	10/07/2015 10:57	FVT-WIN7-H002		HTTP	76.74.242.190	49192	80	les-eglantiers.fr	Outbound	0	http://les-eglantiers.fr/document.php?id=55575d5e100c0b09051724
9	wscript.exe	Network Operation	IOC.NET Categc	10/07/2015 10:57	FVT-WIN7-H002		TCP	76.74.242.190	49192	80	les-eglantiers.fr	Outbound	0	none
10	wscript.exe	Network Operation	IOC.NET Categc	10/07/2015 10:57	FVT-WIN7-H002		TCP	23.91.123.160	49191	80	leikkihuone.com	Outbound	0	none
11	wscript.exe	D1 IOC Network	D1 IOC Networ	10/07/2015 10:57	FVT-WIN7-H002							Inbound	0	
12	wscript.exe	Network Operation	IOC.NET Categc	10/07/2015 10:57	FVT-WIN7-H002		TCP	208.43.65.115	49190	80	laterrazzafiorita.it	Outbound	0	none
13	wscript.exe	Application Start		10/07/2015 10:57	FVT-WIN7-H002	wscript.exe						Inbound	0	
14	svchost.exe	Network Operation		10/07/2015 10:57	FVT-WIN7-H002		UDP	224.0.0.252	58272	5355		Outbound	0	none



PROCESS_NAME	EVENT_NAME	EVENT_DISPLA\	BEGIN_TIME	COMPUTER_NAMI	SRC_FILE_NAME	PROTO	NETWORK_ADDF	LOCAL_PC	REMOTE_	DNS_HOSTNAME	OUTBOUND_	FILE_SIZE	URL_PATH
excel.exe	File Write		10/07/2015 10:56	FVT-WIN7-H002	ruebfo.exe						Inbound	0	
excel.exe	File Write		10/07/2015 10:56	FVT-WIN7-H002	ruebfo.exe						Inbound	0	
explorer.exe	D1 IOC File_Manipul	D1 IOC File_Ma	10/07/2015 10:56	FVT-WIN7-H002							Inbound	0	
excel.exe	File Write		10/07/2015 10:56	FVT-WIN7-H002	45y4g[1].exe						Inbound	0	
excel.exe	Network Operation	IOC.NET Categc	10/07/2015 10:56	FVT-WIN7-H002		HTTP	202.124.241.199	49186	80	members.webshac	Outbound	0	http://members.webshade.com.au/43t3f/45y4g.exe
excel.exe	File Write		10/07/2015 10:56	FVT-WIN7-H002	45y4g[1].exe						Inbound	0	
explorer.exe	D1 IOC File_Manipul	D1 IOC File_Ma	10/07/2015 10:56	FVT-WIN7-H002							Inbound	0	

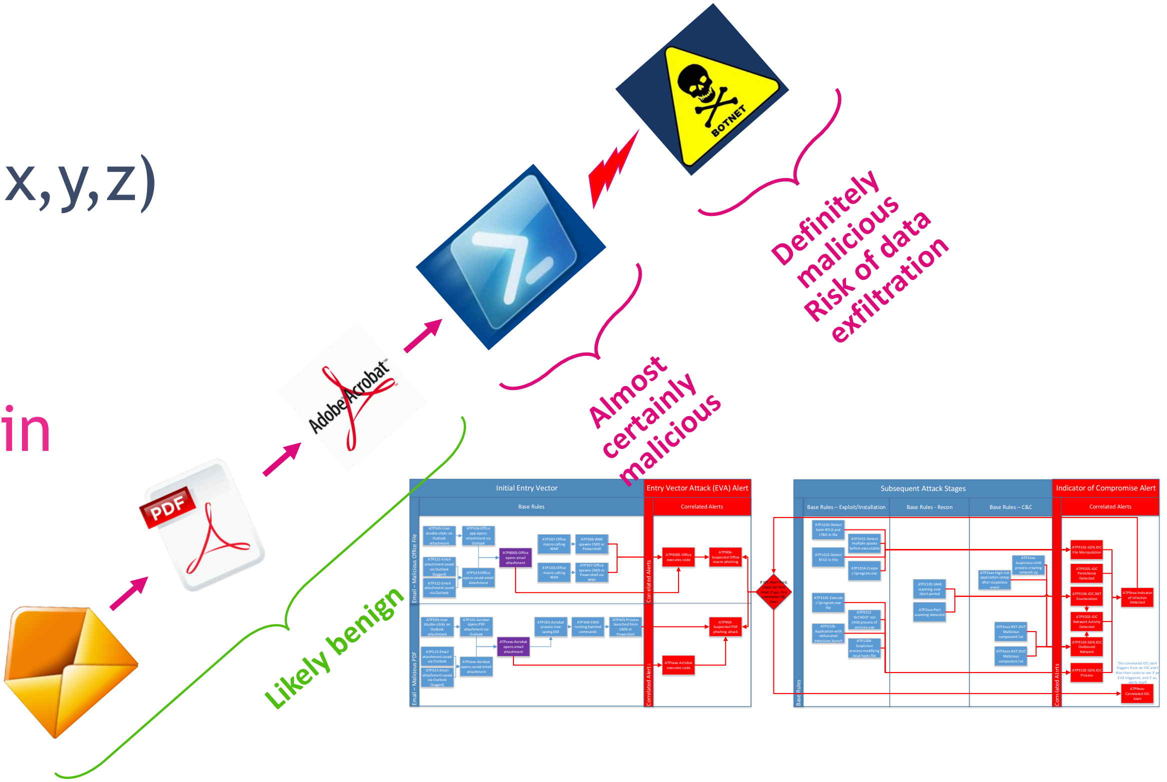
PROCESS_NAME	EVENT_NAME	EVENT_DISPLAY	BEGIN_TIME	COMPUTER_NAMI												
svchost.exe	Network Operation		10/07/2015 10:56	FVT-WIN7-H002												
excel.exe	DLL Load		10/07/2015 10:56	FVT-WIN7-H002												
excel.exe	File Copy		10/07/2015 10:56	FVT-WIN7-H002												
excel.exe	D1 Calculated Action	D1 Calculated Action	10/07/2015 10:56	FVT-WIN7-H002												
outlook.exe	File Copy		10/07/2015 10:56	FVT-WIN7-H002	20131030164403.xls	c:\users\tfischer.te	20131030164403 (	c:\users\tfischer.te	89600	89600						Inb
system	Network Operation		10/07/2015 10:53	FVT-WIN7-H002					0	0	UDP	172.17.16.25	138	138		Ou
system	Network Operation		10/07/2015 10:53	FVT-WIN7-H002					0	0	UDP	172.17.16.15	138	138		Inb
ruebfo.exe	D2 Entry Vector Attack	D2 Entry Vector Attack	10/07/2015 10:53	FVT-WIN7-H002					0	0						Inb
ruebfo.exe	D1 Entry Vector Attack	D1 Entry Vector Attack	10/07/2015 10:53	FVT-WIN7-H002					0	0						Inb
ruebfo.exe	Application Start		10/07/2015 10:53	FVT-WIN7-H002	ruebfo.exe	c:\users\tfischer.testing-w7\appdata\local\temp\			0	0						Inb
explorer.exe	D1 IOC File_Manipulation	D1 IOC File_Manipulatior	10/07/2015 10:53	FVT-WIN7-H002					0	0						Inb
excel.exe	File Write		10/07/2015 10:53	FVT-WIN7-H002	ruebfo.exe	c:\users\tfisch~1.tes\appdata\local\temp\			0	2048						Inb
excel.exe	File Write		10/07/2015 10:53	FVT-WIN7-H002	ruebfo.exe	c:\users\tfischer.testing-w7\appdata\local\temp\			0	0						Inb
excel.exe	Network Operation	IOC.NET Category	10/07/2015 10:53	FVT-WIN7-H002					0	0	HTTP	212.27.63.10	49185	80	www.lalbum.free.f	Ou
explorer.exe	D1 IOC File_Manipulation	D1 IOC File_Manipulatior	10/07/2015 10:53	FVT-WIN7-H002					0	0						Inb
excel.exe	File Write		10/07/2015 10:53	FVT-WIN7-H002	5fg44[1].exe	c:\users\tfischer.testing-w7\appdata\local\microsoft\win			0	0						Inb
excel.exe	D1 IOC Network	D1 IOC Network	10/07/2015 10:53	FVT-WIN7-H002					0	0						Inb
excel.exe	Network Operation	IOC.NET Category	10/07/2015 10:53	FVT-WIN7-H002					0	0	TCP	212.27.63.10	49185	80	www.lalbum.free.f	Ou
excel.exe	DLL Load		10/07/2015 10:53	FVT-WIN7-H002	wshom.ocx	c:\windows\system32\			0	0						Inb
system	Network Operation		10/07/2015 10:53	FVT-WIN7-H002					0	0	UDP	64.4.54.254	137	137	vortex-win.data.mi	Ou
svchost.exe	Network Operation		10/07/2015 10:53	FVT-WIN7-H002					0	0	TCP	64.4.54.254	49184	443	vortex-win.data.mi	Ou
excel.exe	D1 Calculated Action	D1 Calculated Action	10/07/2015 10:52	FVT-WIN7-H002					0	0						Inb
excel.exe	File Copy		10/07/2015 10:52	FVT-WIN7-H002	paymentreceipt.xls	c:\users\tfischer.te	1964d1fe.xls	c:\users\tfischer.te	73216	73216						Inb
outlook.exe	File Copy		10/07/2015 10:52	FVT-WIN7-H002	paymentreceipt.xls	c:\users\tfischer.te	paymentreceipt (2	c:\users\tfischer.te	73216	73216						Inb
svchost.exe	Network Operation		10/07/2015 10:52	FVT-WIN7-H002					0	0	UDP	224.0.0.252	62404	5355		Ou
system	Network Operation		10/07/2015 10:52	FVT-WIN7-H002					0	0	UDP	192.168.0.11	137	137		Ou

Data visualised...

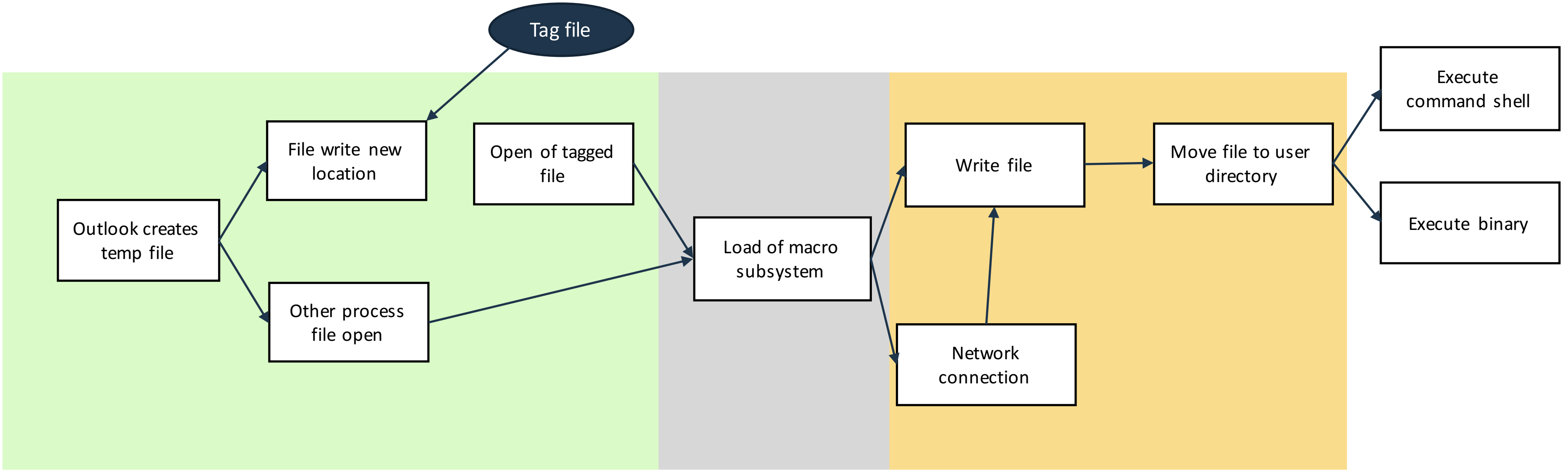
- Do you really know what that Chinese software is doing
- Dridex in realtime
- Those flash things

It’s Doing This so Probably Suspicious

- Enable behavioural analysis
- phishing :- (a+b),(c,(d|e)),!(x,y,z)
- Response ?
  Kill any point in the chain


BOTNET
Definitely malicious Risk of data exfiltration
Almost certainly malicious
Adobe Acrobat
PDF
Likely benign
Initial Entry Vector
Base Rules
Entry Vector Attack (EVA) Alert
Correlated Alerts
Subsequent Attack Stages
Base Rules – Exploit/Installation
Base Rules – Recon
Base Rules – C&C
Indicator of Compromise Alert
Correlated Alerts

Behaviour Tree



Attachment Opened

Active Attachment

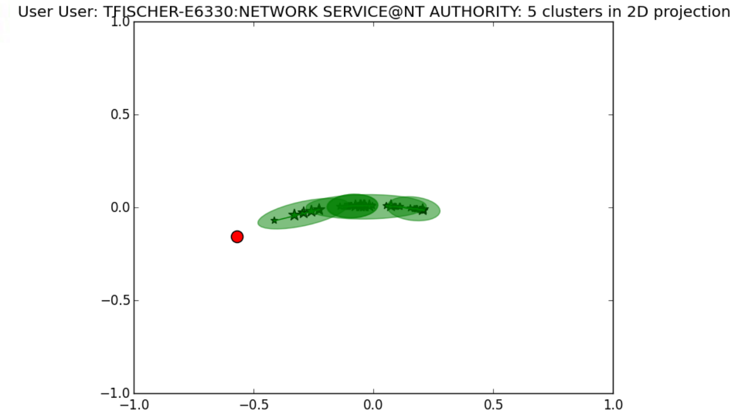
Risk - unknown

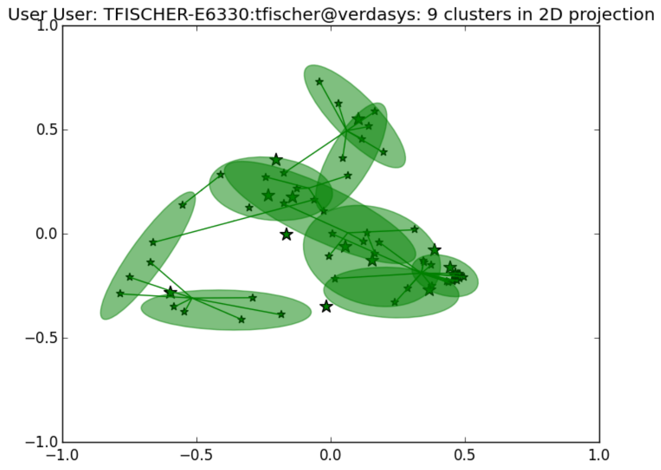
Risk - elevated

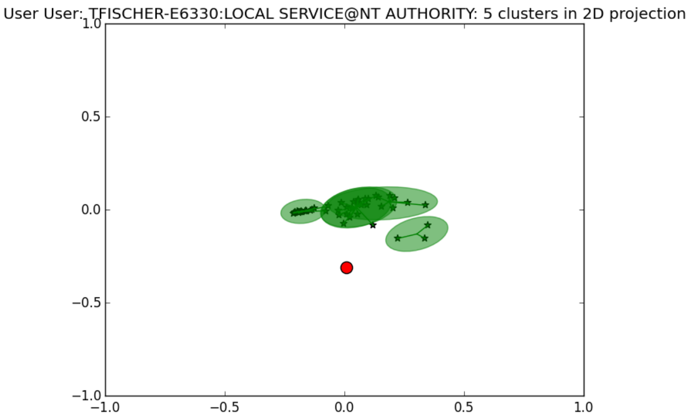
Suspicious activity

Keeping the Story Alive

- Increase Visibility:
  - More DLL events
  - Memory events
- Capture More…
- Automate anomaly detection







Let’s run a phishing attachment

Q&A

DEEPSEC

- tfischer@digitalguardian.com
- tvfischer+sec@gmail.com
- @Fvt
- keybase.io/fvt

Thank you...