Operation Sentry Stopper: A Long-Standing Espionage

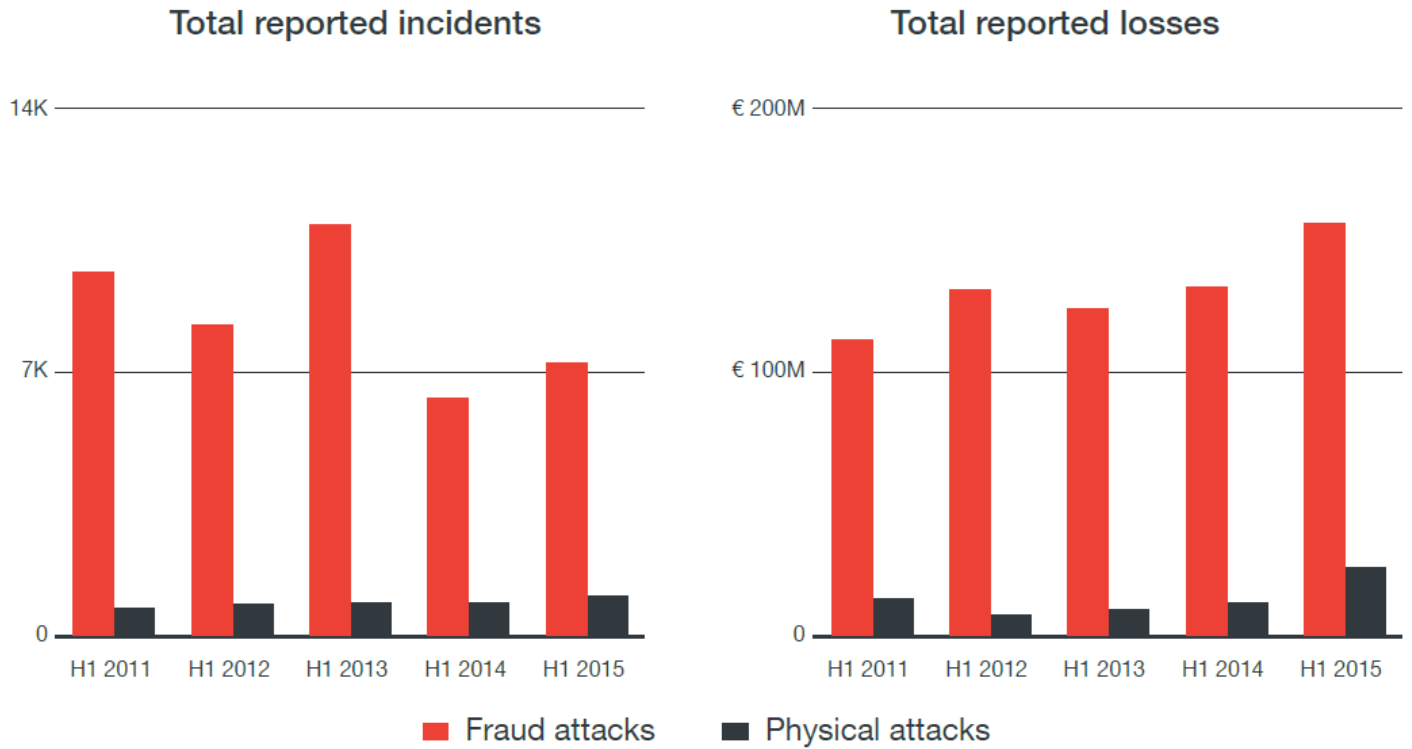
Lenart Bermejo, Razor Huang, Mingyen Hsieh

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



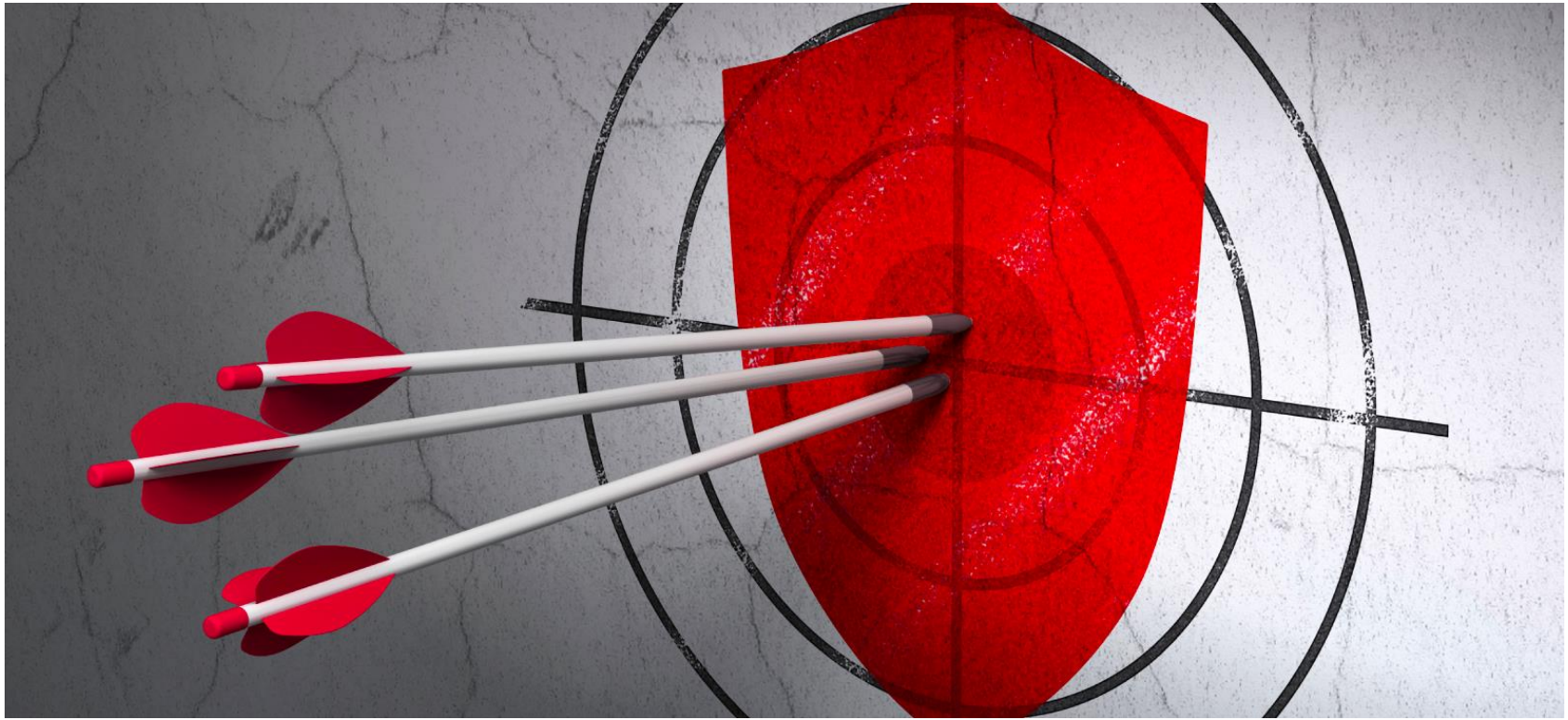
Source: http://blog.trendmicro.com/trendlabs-security-intelligence/atm-malware-on-the-rise/

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

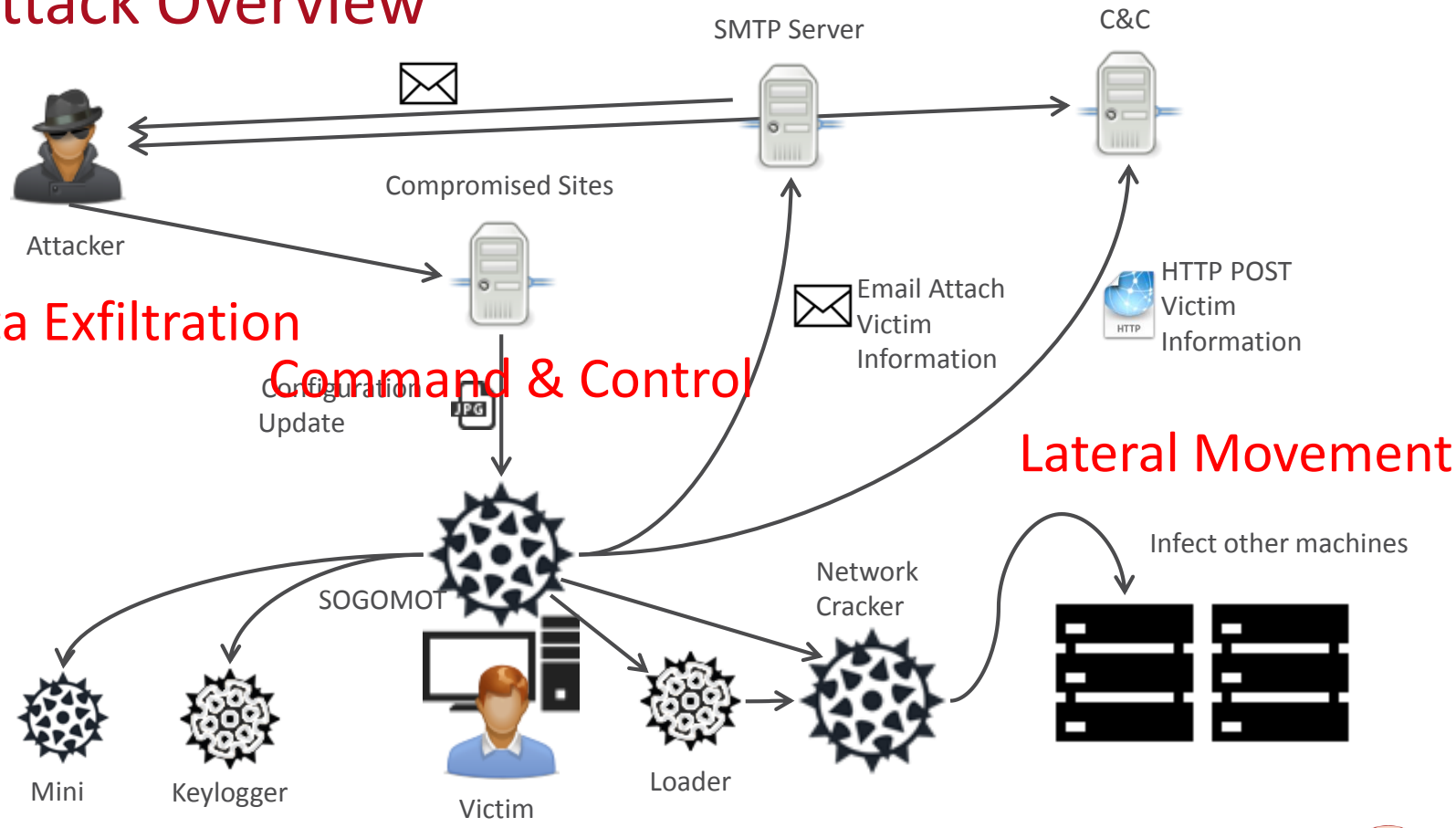
Before Financial Loss and Reputational Damage



Sentry Stopper

Target Region

Attack Overview

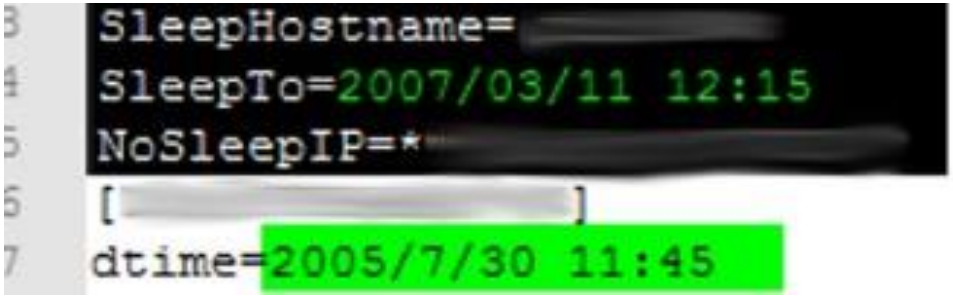


Since when?

- Earliest Sample - Feb 2009
  - Earliest Compile Time

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

- Earliest Timestamp from configuration file



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
业的APT（Advanced Persistent Threat，高级持
科技通过检测BKDR_CORUM家族、TSPY_GO
TROJ_GENERIC.APC等恶意病毒，目前将此威
估内部网络风险，谨防韩国金融行业APT攻击事

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"
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?

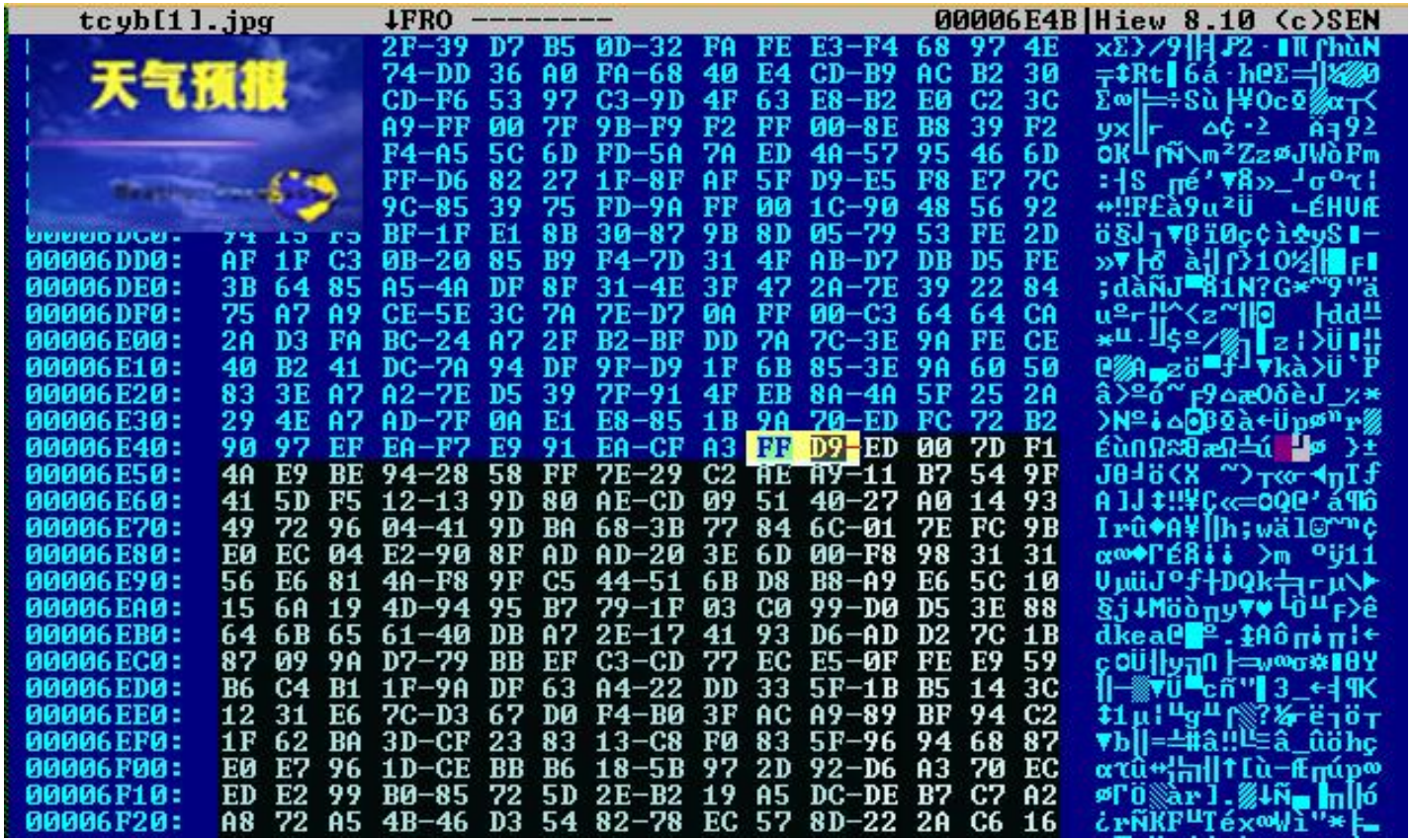
- Frequent Updates
- Pretend to have normal traffic
- Use legitimate Services
- Stop the Sentry

How did they maintain foothold?

- Frequent Updates

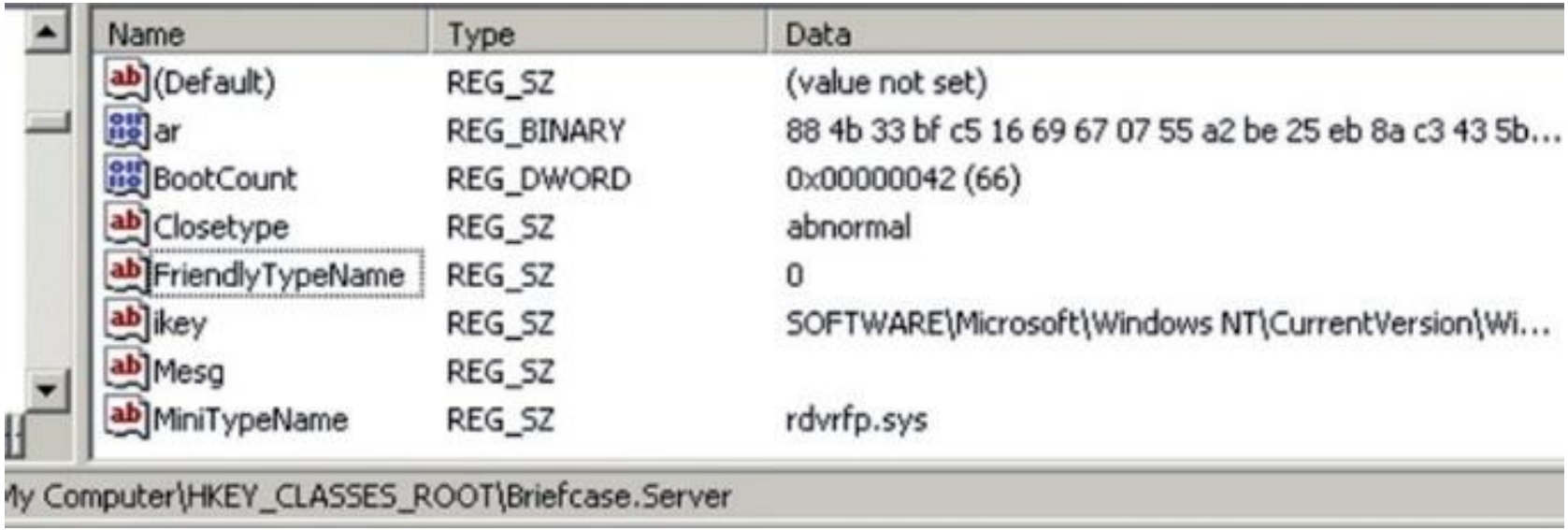
```
HttpPara=http://[redacted].com/admin/upimages/a_flow_r2_c3.jpg
HttpV1=http://[redacted].cn/images/L2.jpg
HttpMini=http://[redacted].com/images/wjyb.jpg
Http64=http://[redacted].com/images/wjktq.jpg
HttpEnumDll=http://[redacted].com/images/qiqiu.jpg
HttpGnaDll=http://[redacted].com/images/tcyb.jpg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

How did they maintain foothold?

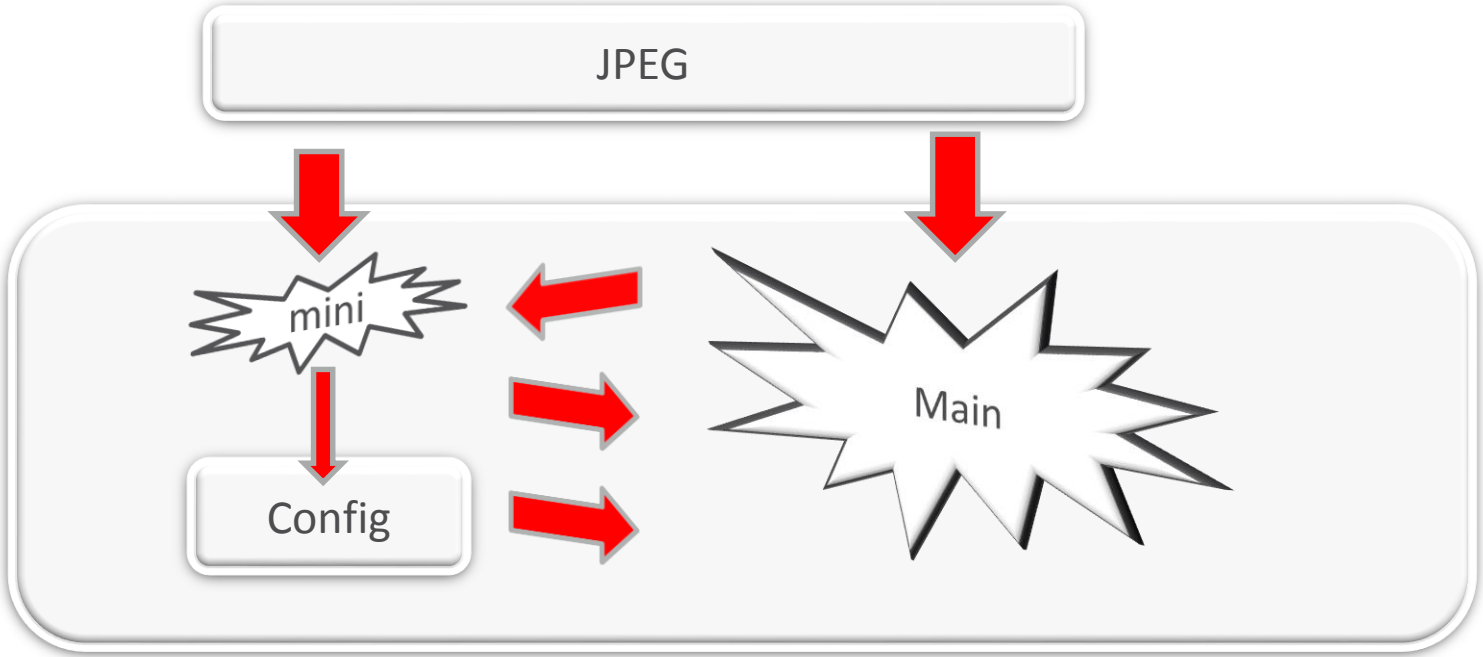


How did they maintain foothold?

- Frequent Updates



How did they maintain foothold?

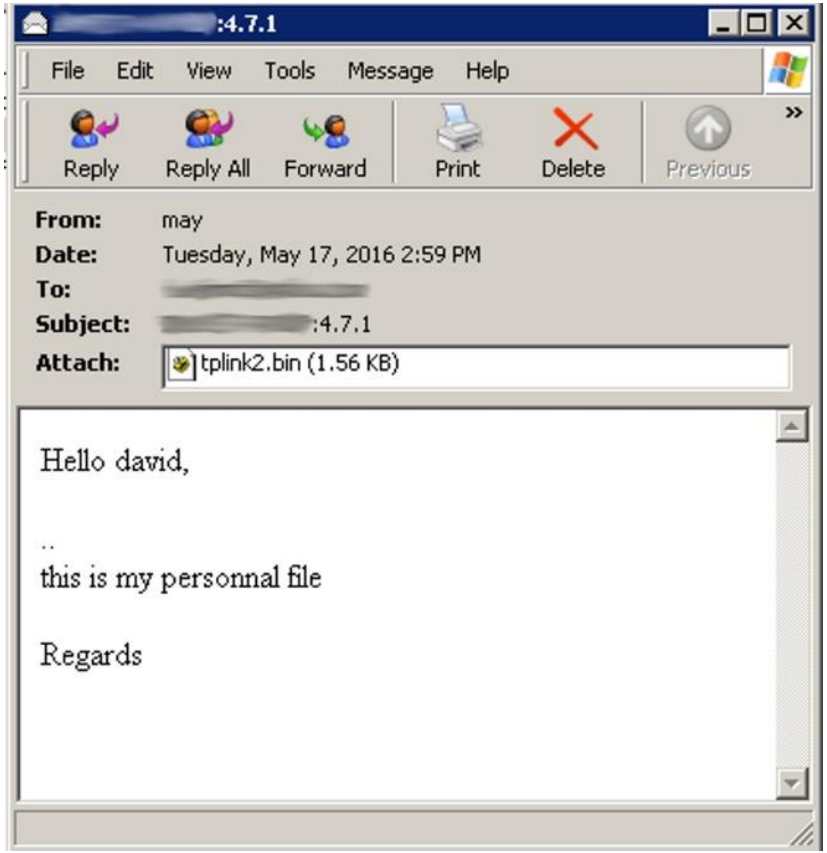


How did they maintain foothold?

- Pretend to have normal traffic

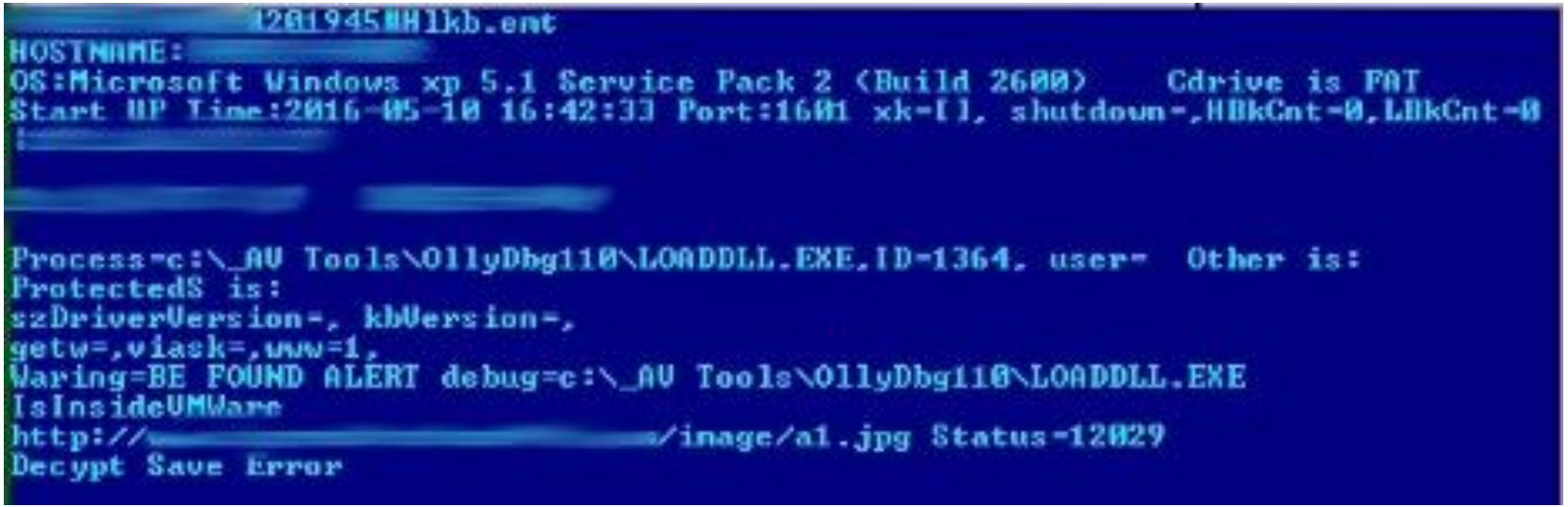
How did they maintain foothold?

- Use legitimate Services



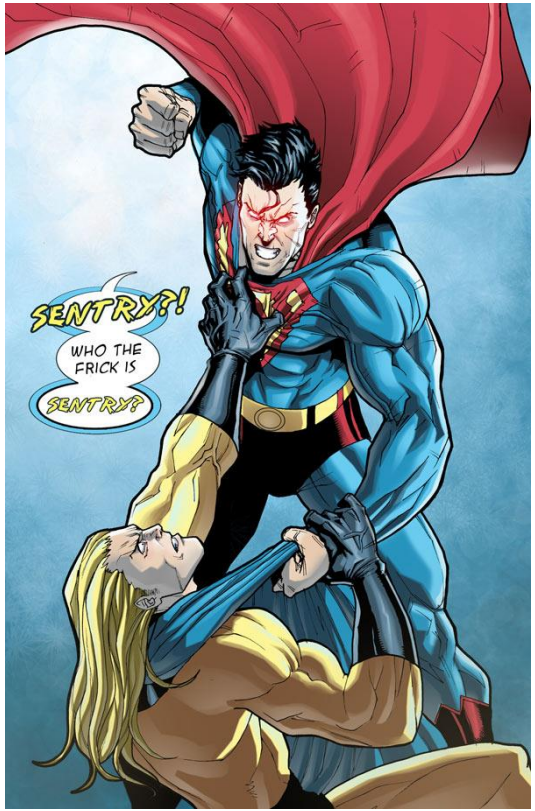
How did they maintain foothold?

- Use legitimate Services



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
```

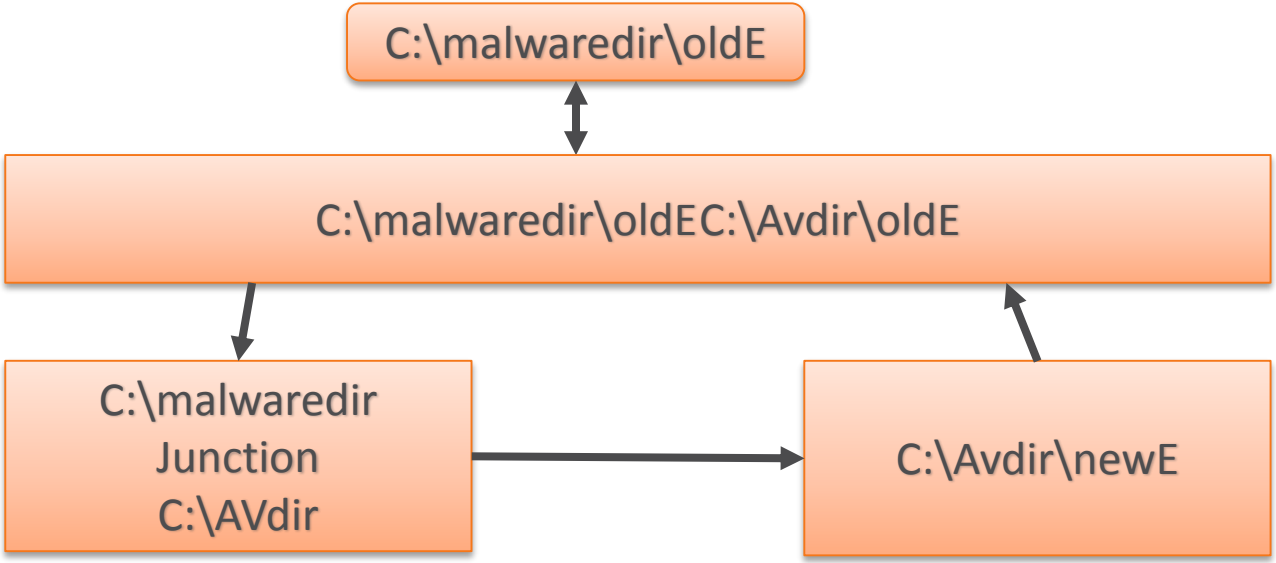
How did they maintain foothold?

- 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



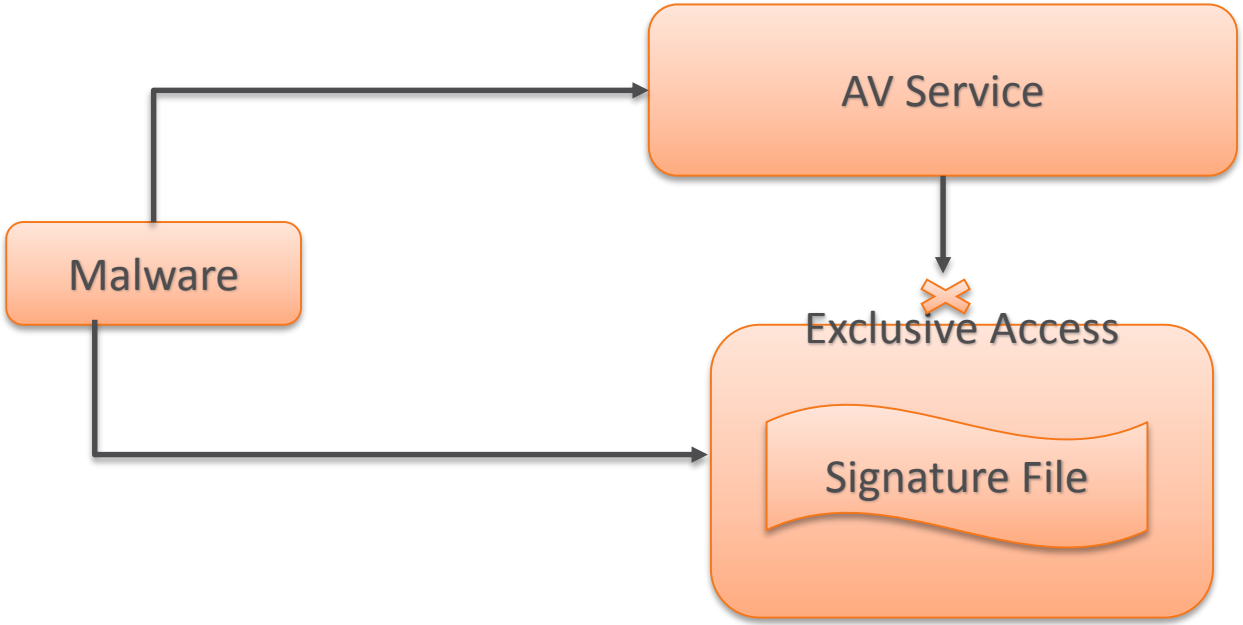
How did they maintain foothold?

- 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?

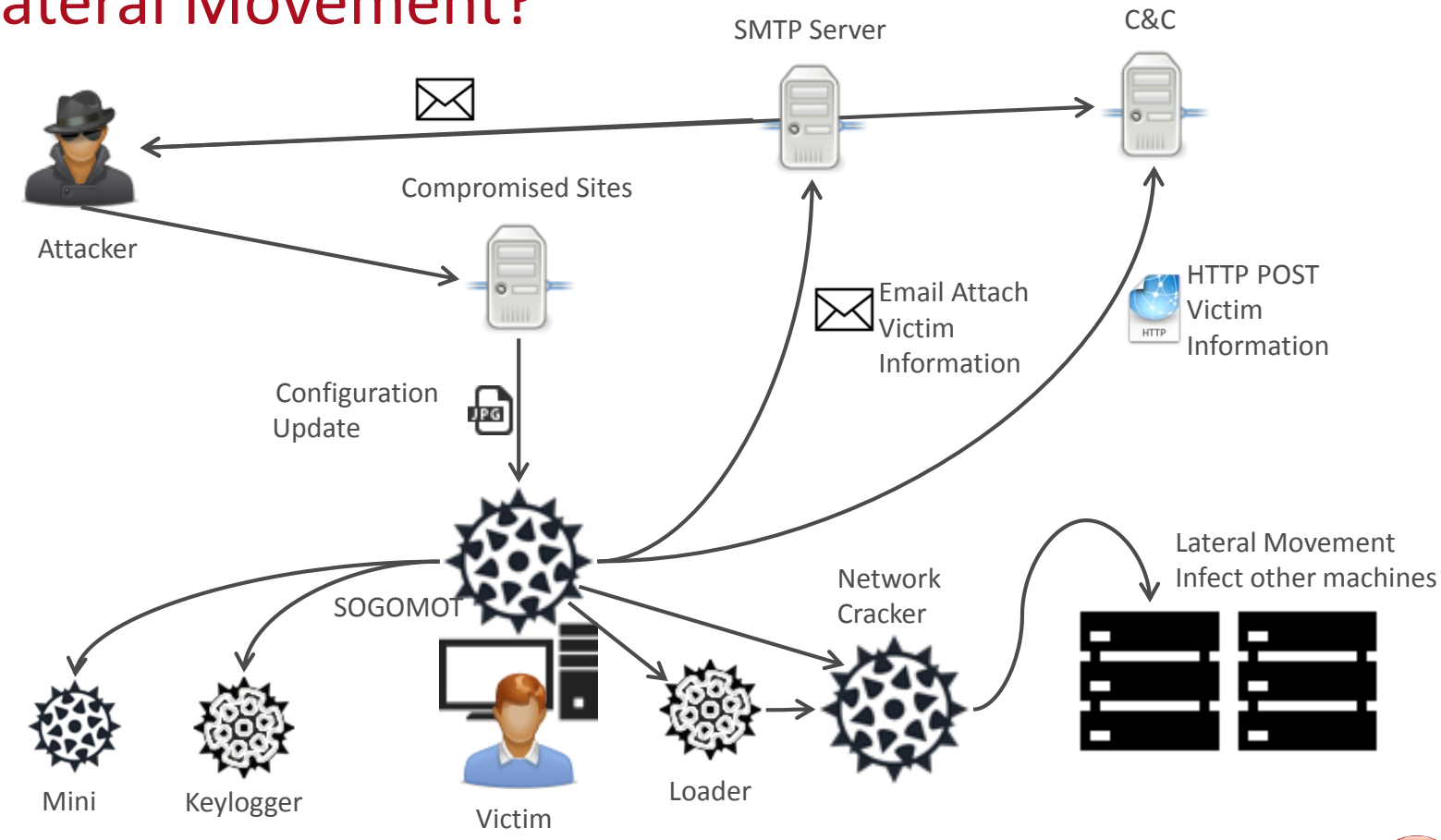
- Stop the sentry



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?



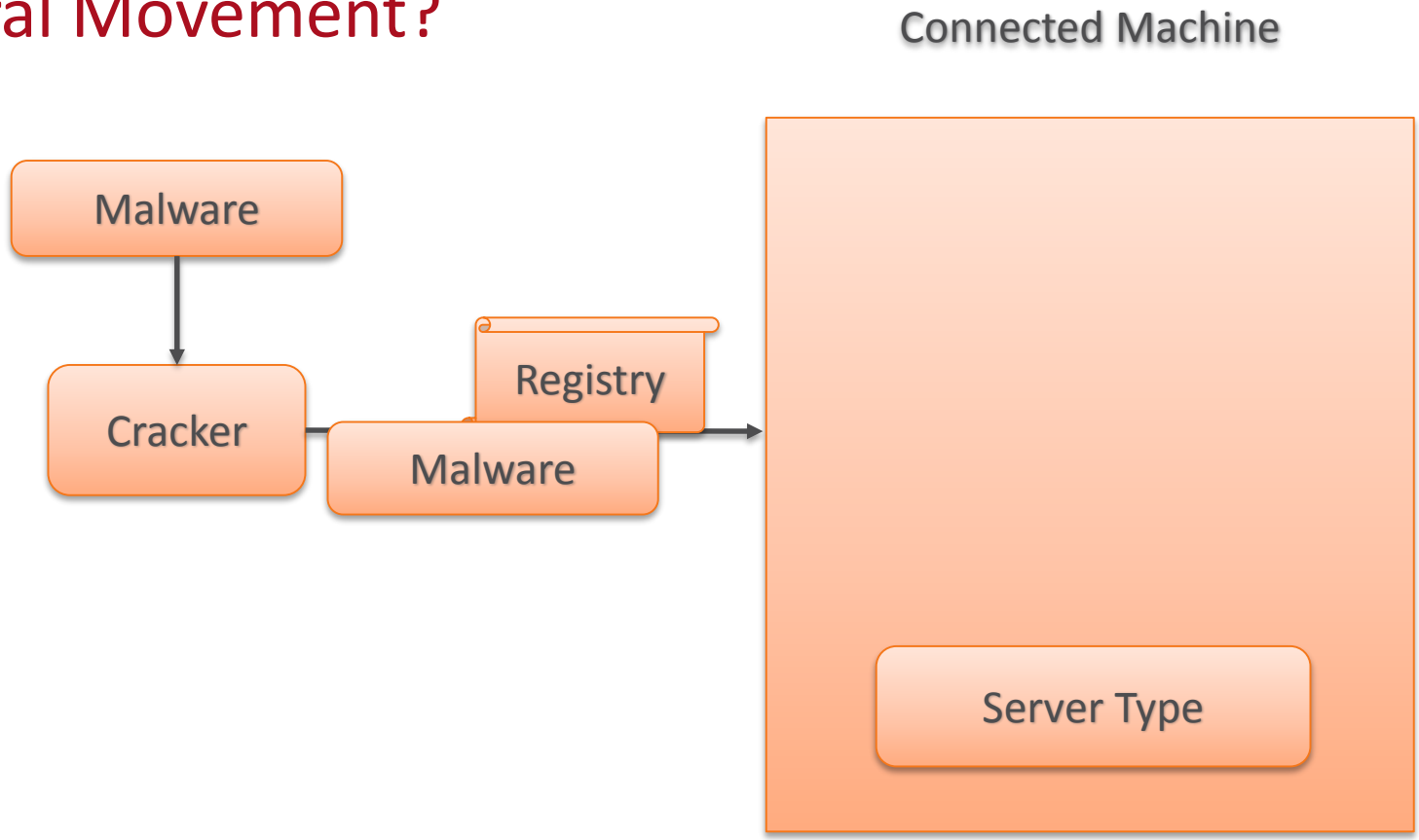
Lateral Movement?

```
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?

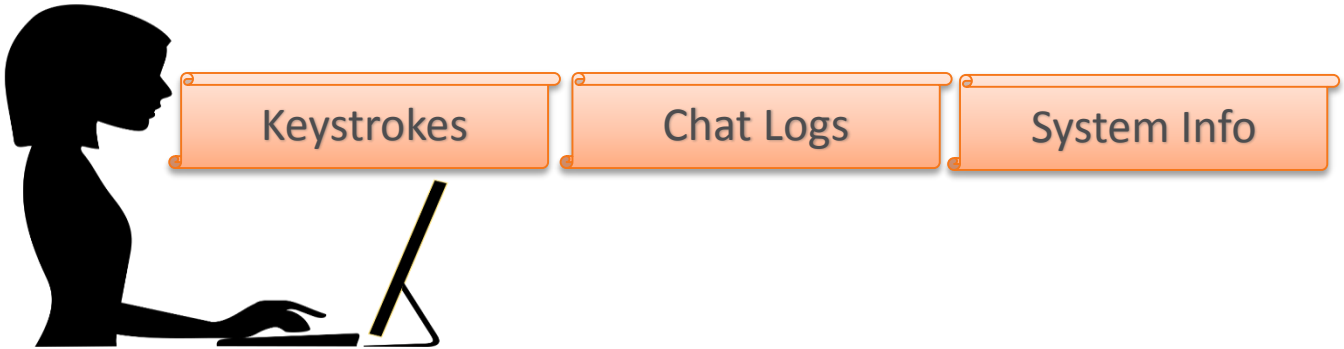
```
pop     esi
push    esi             ; int
push    4               ; dwType
push    offset a1       ; "1"
push    offset aStarthinstance ; "StarthInstance"
push    eax             ; lpSubKey
push    [ebp+phkResult] ; hKey
call    Create_install_reg_key
push    esi             ; int
push    esi             ; 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.