# Endpoint Protection

## SWIFT attackers' malware linked to more financial attacks

1 Recommend

May 26, 2016 01:10 PM

A L Johnson

Statistics
0 Favorited
2 Views
0 Files
0 Shares
0 Downloads

Symantec has found evidence that a bank in the Philippines has also been attacked by the group that stole US$81 million from the Bangladesh central bank and attempted to steal over $1 million from the Tien Phong Bank in Vietnam.

Malware used by the group was also deployed in targeted attacks against a bank in the Philippines. In addition to this, some of the tools used share code similarities with malware used in historic attacks linked to a threat group known as Lazarus. The attacks can be traced back as far as October 2015, two months prior to the discovery of the failed attack in Vietnam, which was hitherto the earliest known incident.

The attack against the Bangladesh central bank triggered an alert by payments network SWIFT, after it was found the attackers had used malware to cover up evidence of fraudulent transfers. SWIFT issued a further warning, saying that it had found evidence of malware being used against another bank in a similar fashion. Vietnam's Tien Phong Bank subsequently stated that it intercepted a fraudulent transfer of over $1 million in the fourth quarter of last year. SWIFT concluded that the second attack indicates that a "wider and highly adaptive campaign" is underway targeting banks.

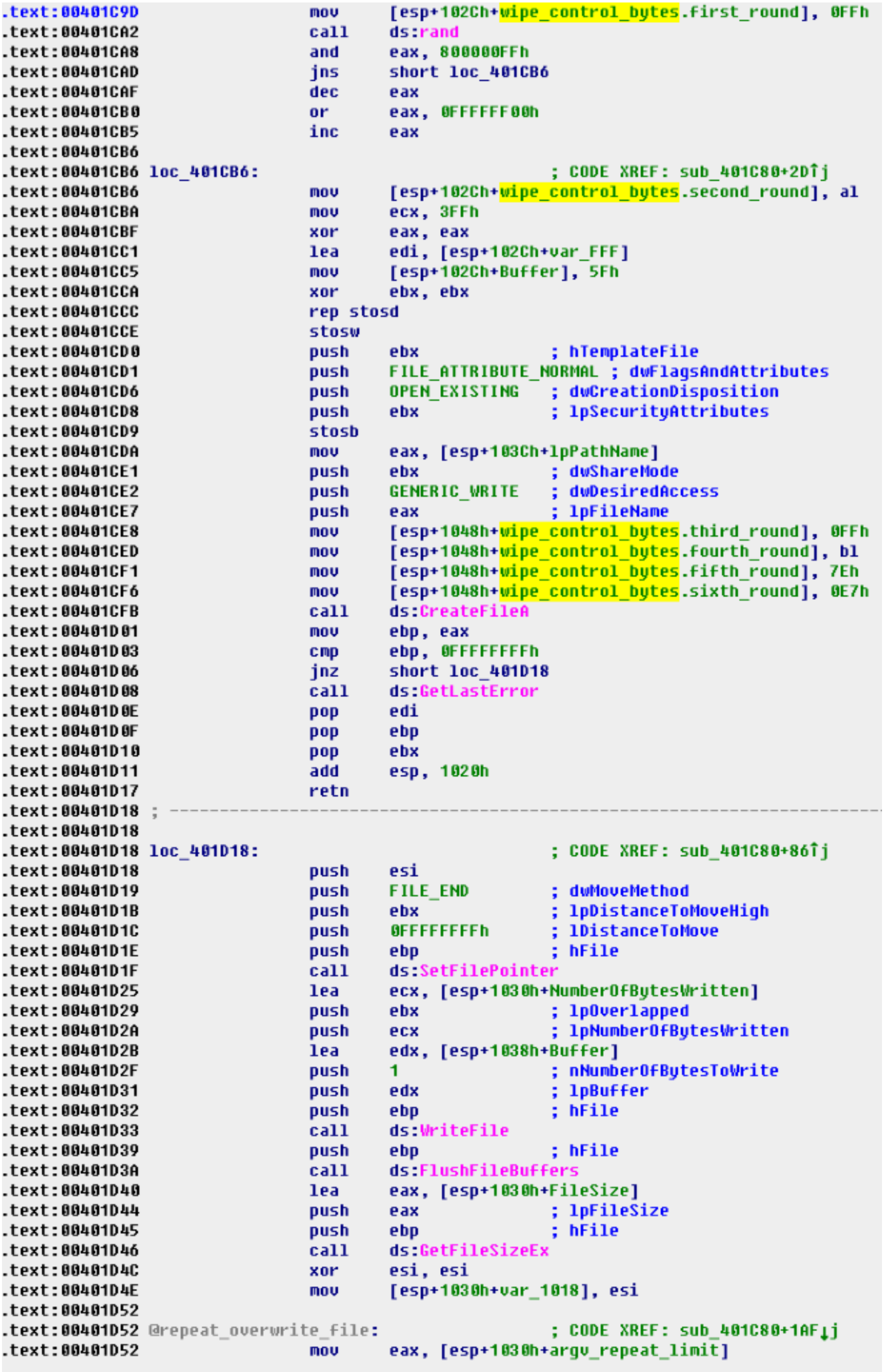
A third bank, Banco del Austro in Ecuador, was also reported to have lost $12 million to attackers using fraudulent SWIFT transactions. However, no details are currently known about the tools used in this incident or if there are any links to the attacks in Asia.

**Discovery of additional tools used by attackers**
Symantec has identified three pieces of malware which were being used in limited targeted attacks against the financial industry in South-East Asia: Backdoor.Fimlis, Backdoor.Fimlis.B, and Backdoor.Contopee. At first, it was unclear what the motivation behind these attacks were, however code sharing between Trojan.Banswift (used in the Bangladesh attack used to manipulate SWIFT transactions) and early variants of Backdoor.Contopee provided a connection.

While analyzing samples of Trojan.Banswift, a distinct file wiping code was found. Some of the distinctive properties of the wiping code include:

- Function takes two parameters: path of file to overwrite and number of iterations (max six)

- It will initially overwrite the last byte of the target file with 0x5F
- Six “control” bytes are supplied which dictate what bytes are used during the overwrite process



```
.text:00401C9D                 mov     [esp+102Ch+wipe_control_bytes.first_round], 0FFh
.text:00401CA2                 call    ds:rand
.text:00401CA8                 and     eax, 800000FFh
.text:00401CAD                 jns     short loc_401CB6
.text:00401CAF                 dec     eax
.text:00401CB0                 or      eax, 0FFFFFF00h
.text:00401CB5                 inc     eax
.text:00401CB6
.text:00401CB6 loc_401CB6:                             ; CODE XREF: sub_401C80+2D↑j
.text:00401CB6                 mov     [esp+102Ch+wipe_control_bytes.second_round], al
.text:00401CBA                 mov     ecx, 3FFh
.text:00401CBF                 xor     eax, eax
.text:00401CC1                 lea     edi, [esp+102Ch+var_FFF]
.text:00401CC5                 mov     [esp+102Ch+Buffer], 5Fh
.text:00401CCA                 xor     ebx, ebx
.text:00401CCC                 rep stosd
.text:00401CCE                 stosw
.text:00401CD0                 push    ebx             ; hTemplateFile
.text:00401CD1                 push    FILE_ATTRIBUTE_NORMAL ; dwFlagsAndAttributes
.text:00401CD6                 push    OPEN_EXISTING   ; dwCreationDisposition
.text:00401CD8                 push    ebx             ; lpSecurityAttributes
.text:00401CD9                 stosb
.text:00401CDA                 mov     eax, [esp+103Ch+lpPathName]
.text:00401CE1                 push    ebx             ; dwShareMode
.text:00401CE2                 push    GENERIC_WRITE   ; dwDesiredAccess
.text:00401CE7                 push    eax             ; lpFileName
.text:00401CE8                 mov     [esp+1048h+wipe_control_bytes.third_round], 0FFh
.text:00401CED                 mov     [esp+1048h+wipe_control_bytes.fourth_round], bl
.text:00401CF1                 mov     [esp+1048h+wipe_control_bytes.fifth_round], 7Eh
.text:00401CF6                 mov     [esp+1048h+wipe_control_bytes.sixth_round], 0E7h
.text:00401CFB                 call    ds:CreateFileA
.text:00401D01                 mov     ebp, eax
.text:00401D03                 cmp     ebp, 0FFFFFFFFh
.text:00401D06                 jnz     short loc_401D18
.text:00401D08                 call    ds:GetLastError
.text:00401D0E                 pop     edi
.text:00401D0F                 pop     ebp
.text:00401D10                 pop     ebx
.text:00401D11                 add     esp, 1020h
.text:00401D17                 retn
.text:00401D18 ; ---------------------------------------------------------------------------
.text:00401D18
.text:00401D18 loc_401D18:                             ; CODE XREF: sub_401C80+86↑j
.text:00401D18                 push    esi
.text:00401D19                 push    FILE_END        ; dwMoveMethod
.text:00401D1B                 push    ebx             ; lpDistanceToMoveHigh
.text:00401D1C                 push    0FFFFFFFFh      ; lDistanceToMove
.text:00401D1E                 push    ebp             ; hFile
.text:00401D1F                 call    ds:SetFilePointer
.text:00401D25                 lea     ecx, [esp+1030h+NumberOfBytesWritten]
.text:00401D29                 push    ebx             ; lpOverlapped
.text:00401D2A                 push    ecx             ; lpNumberOfBytesWritten
.text:00401D2B                 lea     edx, [esp+1038h+Buffer]
.text:00401D2F                 push    1               ; nNumberOfBytesToWrite
.text:00401D31                 push    edx             ; lpBuffer
.text:00401D32                 push    ebp             ; hFile
.text:00401D33                 call    ds:WriteFile
.text:00401D39                 push    ebp             ; hFile
.text:00401D3A                 call    ds:FlushFileBuffers
.text:00401D40                 lea     eax, [esp+1030h+FileSize]
.text:00401D44                 push    eax             ; lpFileSize
.text:00401D45                 push    ebp             ; hFile
.text:00401D46                 call    ds:GetFileSizeEx
.text:00401D4C                 xor     esi, esi
.text:00401D4E                 mov     [esp+1030h+var_1018], esi
.text:00401D52
.text:00401D52 @repeat_overwrite_file:                 ; CODE XREF: sub_401C80+1AF↓j
.text:00401D52                 mov     eax, [esp+1030h+argv_repeat_limit]
```

*Figure 1. Unique wiping code found in Trojan.Banswift and additional Lazarus tools*

Already this code looked fairly unique. What was even more interesting was that when we searched for additional malware containing the exact combination of “control” bytes, an early variant of Backdoor.Contopee and the *“msoutc.exe”* sample already discussed in the recent BAE blog analyzing the Bangladesh attack were also found.

Symantec believes distinctive code shared between families and the fact that Backdoor.Contopee was being used in limited targeted attacks against financial institutions in the region, means these tools can be attributed to the same group.

**Historical attacks**

Backdoor.Contopee has been previously used by attackers associated with a broad threat group known as Lazarus. Lazarus has been linked to a string of aggressive attacks since 2009, largely focused on targets in the US and South Korea. The group was linked to Backdoor.Destover, a highly destructive Trojan that was the subject of an FBI warning after it was used in an attack against Sony Pictures Entertainment. The FBI concluded that the North Korean government was responsible for this attack.

The group was the target of a cross-industry initiative known as Operation Blockbuster earlier this year, which involved major security vendors sharing intelligence and resources in order to assist commercial and government organizations in protecting themselves against Lazarus. As part of the initiative, vendors are circulating malware signatures and other useful intelligence related to these attackers.

**Ongoing danger**
The discovery of more attacks provides further evidence that the group involved is conducting a wide campaign against financial targets in the region. While awareness of the threat posed by the group has now been raised, its initial success may prompt other attack groups to launch similar attacks. Banks and other financial institutions should remain vigilant.

**Protection**
Symantec and Norton products protect against these threats with the following detections:

**Antivirus**

- Trojan.Banswift
- Trojan.Banswift!gen1
- Backdoor.Contopee
- Backdoor.Fimlis
- Backdoor.Fimlis.B

## Tags and Keywords

## Related Entries and Links

No Related Resource entered.

PRODUCTS APPLICATIONS SUPPORT COMPANY HOW TO BUY