TREND MICRO™ | Securing Your Journey to the Cloud

Stealth by Legitimacy: Malware's Use of Legitimate Services

Jeffrey Bernardino

Nikko Tamaña

2012年5月2日

Malware take advantage of….

- Social media
- Email
- Vulnerabilities
- Advertisements
- Search engine results
- Fake antivirus/applications
- Legitimate services

TREND MICRO

Why cybercriminals use legitimate services?

- Malware utilizing legitimate services are definitely not unheard of.
- Running their malicious activities through legitimate channels can be an effective way to mask communication against network and file tracking techniques employed by most anti-malware products today.
- The sheer volume of users of popular legitimate services decrease the chance of malware activity discovery, as it will take time for IT departments to develop rules that will track malicious activity on legitimate channels.

Malware using legitimate services

- TSPY_SPCSEND
  - malware that grabs MS Word and Excel files from users' infected systems and then uploads them to the file hosting site sendspace.com. Sendspace is a file hosting website that offers file hosting to enable users to "send, receive, track and share your big files." Cybercriminals used *Sendspace* for rounding up and uploading stolen data.
  - It is a "grab and go" Trojan that searches the local drive of an affected system for *MS Word* and *Excel* files. The collected documents are then archived and password-protected using a random-generated password in the user's temporary folder

Malware using legitimate services

- BKDR_MAKADOC
  - Uses Microsoft Word documents that can either be downloaded directly from the Internet or dropped by other malware.
  - This backdoor remotely executes these commands: terminate itself, download and execute files, change IP, and open command line.
  - It continues by stealing information from the target, such as domain name, GUID, host name, user name, Windows version, and more.
  - It then uses legitimate site, http://docs.google.com as its proxy server to communicate with its C&Cs, thus avoiding detection.

BKDR_VERNOT.A Routine

Arrival

BKDR_VERNOT.A Arrival

- It may arrive on a system as a file dropped by other malware
- It may arrive as a file downloaded unknowingly by users when visiting malicious sites.

BKDR_VERNOT.A Routine

Arrival **Installation**

BKDR_VERNOT.A Installation

- First, it drops its DLL component

```
00406513  >  6A 00        PUSH 0                                   hTemplateFile = NULL
00406515  .  56           PUSH ESI                                 Attributes
00406516  .  FF75 F8      PUSH DWORD PTR SS:[EBP-8]                Mode
00406519  .  8D45 E4      LEA EAX,DWORD PTR SS:[EBP-1C]
0040651C  .  50           PUSH EAX                                 pSecurity
0040651D  .  FF75 F0      PUSH DWORD PTR SS:[EBP-10]               ShareMode
00406520  .  FF75 F4      PUSH DWORD PTR SS:[EBP-C]                Access
00406523  .  FF75 08      PUSH DWORD PTR SS:[EBP+8]                FileName
00406526  .  FF15 2481400( CALL DWORD PTR DS:[<&KERNEL32.CreateFil  CreateFileA
```

```
0012FCC4  0012FD7C  FileName "C:\DOCUME~1\WINXP~1.KAR\LOCALS~1\Temp\NETUT2.dll"
0012FCC8  40000000  Access =
0012FCCC  00000003  ShareMode = FILE_SHARE_READ|FILE_SHARE_WRITE
0012FCD0  0012FCEC  pSecurity = 0012FCEC
0012FCD4  00000002  Mode = CREATE_ALWAYS
0012FCD8  00000080  Attributes = NORMAL
0012FCDC  00000000  hTemplateFile = NULL
```

- “%User Temp%\NETUT2.dll”

BKDR_VERNOT.A Installation

- It opens the registry key to be modified

```
004019C8  .  MOV ECX,DWORD PTR SS:[ESP+C]
004019CC  .  PUSH ESI                          pHandle
004019CD  .  PUSH 20006                        Access = KEY_WRITE
004019D2  .  PUSH 0                            Reserved = 0
004019D4  .  PUSH EAX                          Subkey
004019D5  .  PUSH ECX                          hKey
004019D6  .  MOV BL,1
004019D8  .  CALL DWORD PTR DS:[<&ADVAPI32.RegOp  RegOpenKeyExA
004019DE  .  TEST EAX,EAX
```

```
0012F4FC  80000001  hKey = HKEY_CURRENT_USER
0012F500  00409048  Subkey = "Software\Microsoft\Windows NT\CurrentVersion\Windows"
0012F504  00000000
0012F508  00020006  Access = KEY_WRITE
0012F50C  0012F738  pHandle = 0012F738
```

- “HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows”

BKDR_VERNOT.A Installation

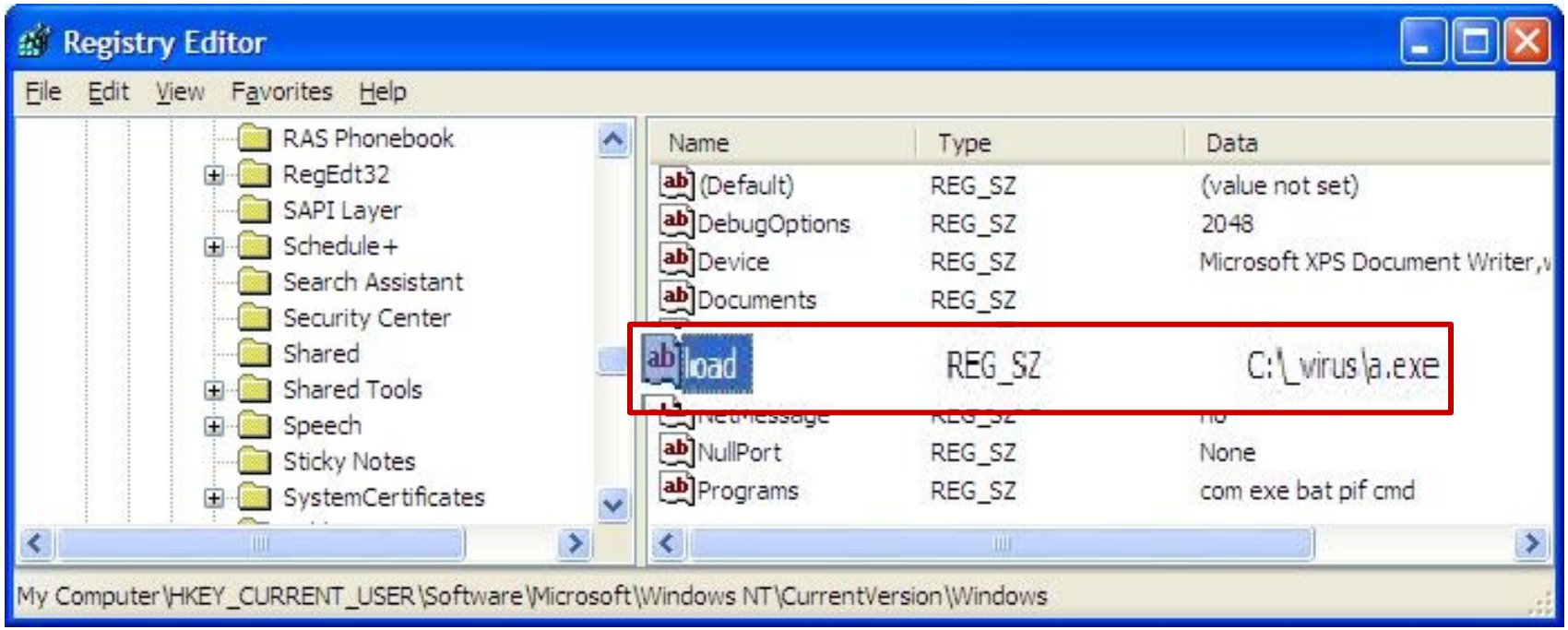
- Then it modifies the following registry entry to ensure it automatic execution at every system startup:

```
004019F1  .  PUSH ECX                                  BufSize
004019F2  .  PUSH EDX                                  Buffer
004019F3  .  MOV EDX,DWORD PTR SS:[ESP+20]
004019F7  .  PUSH 1                                    ValueType = REG_SZ
004019F9  .  PUSH EAX                                  Reserved
004019FA  .  MOV EAX,DWORD PTR DS:[ESI]
004019FC  .  PUSH EDX                                  ValueName
004019FD  .  PUSH EAX                                  hKey
004019FE  .  CALL DWORD PTR DS:[<&ADVAPI32.RegSe       RegSetValueExA
```

```
0012F4F4  00000038
0012F4F8  00409040   ValueName = "Load"
0012F4FC  00000000   Reserved = 0
0012F500  00000001   ValueType = REG_SZ
0012F504  0012F530   Buffer = 0012F530
0012F508  0000000F   BufSize = F (15.)
0012F50C  0012F634   ASCII "C:\_virus\a.exe"
```

BKDR_VERNOT.A Installation

- In Registry Editor



BKDR_VERNOT.A Routine

Arrival

Installation

DLL Injection

BKDR_VERNOT.A DLL Injection

- It first searches for EXPLORER.EXE in running processes

```
0040157C  .  896C2  MOV DWORD PTR SS:[ESP+10],EBP
00401580  .  55     PUSH EBP                                  ProcessID => 0
00401581  .  6A 02  PUSH 2                                    Flags = TH32CS_SNAPPROCESS
00401583  .  F3:AB  REP STOS DWORD PTR ES:[EDI]
00401585  .  E8 B2  CALL <JMP.&KERNEL32.CreateToolhelp32Snap   CreateToolhelp32Snapshot
0040158A  .  8BF0   MOV ESI,EAX
```

```
004015A2  .  C7442  MOV DWORD PTR SS:[ESP+10],128
004015AA  .  51     PUSH ECX                                  pProcessentry
004015AB  .  56     PUSH ESI                                  hSnapshot
004015AC  .  E8 85  CALL <JMP.&KERNEL32.Process32First>        Process32First
004015B1  .  85C0   TEST EAX,EAX
004015B3  .v 74 4E  JE SHORT a.00401600
004015B5  .  8D542  LEA EDX,DWORD PTR SS:[ESP+34]
004015BA  .  FFD3   CALL EBX                                  USER32.CharUpperA
004015BC  .  50     PUSH EAX
004015BD  .  8D842  LEA EAX,DWORD PTR SS:[ESP+13C]
004015C5  .  E8 06  CALL a.004071D0                           Compare if "EXPLORER.EXE"
004015CA  .  83C4   ADD ESP,8
004015CD  .  85C0   TEST EAX,EAX
```

BKDR_VERNOT.A DLL Injection

- If found, it opens EXPLORER.EXE

```
00401657  .  50     PUSH EAX                                  ProcessId
00401658  .  56     PUSH ESI                                  Inheritable => FALSE
00401659  .  68 2A  PUSH 42A                                  Access = CREATE_THREAD|VM_OPERATION
0040165E  .  FF15   CALL DWORD PTR DS:[<&KERNEL32.Oper        OpenProcess
00401664  .  8BF8   MOV EDI,EAX
```

- It then writes the DLL component to EXPLORER.EXE's memory space

```
004016A2  .  6A 00  PUSH 0                                    pBytesWritten = NULL
004016A4  .  53     PUSH EBX                                  BytesToWrite
004016A5  .  8B55   MOV EDX,DWORD PTR SS:[EBP+C]
004016A8  .  52     PUSH EDX                                  Buffer
004016A9  .  56     PUSH ESI                                  Address
004016AA  .  57     PUSH EDI                                  hProcess
004016AB  .  FF15   CALL DWORD PTR DS:[<&KERNEL32.Writ        WriteProcessMemory
004016B1  .  85C0   TEST EAX,EAX
```

BKDR_VERNOT.A DLL Injection

- Harvests the LoadLibraryW API

```
004016B9  .  68 28  PUSH a.00409128                    ProcNameOrOrdinal = "LoadLibraryW"
004016BE  .  68 10  PUSH a.0040911C                    pModule = "Kernel32"
004016C3  .  FF15   CALL DWORD PTR DS:[<&KERNEL32.GetM  GetModuleHandleA
004016C9  .  50     PUSH EAX                           hModule
004016CA  .  FF15   CALL DWORD PTR DS:[<&KERNEL32.GetP  GetProcAddress
004016D0  .  8BD8   MOV EBX,EAX
004016D2  .  895D   MOV DWORD PTR SS:[EBP-2C],EBX
```

BKDR_VERNOT.A DLL Injection

- Creates remote thread in EXPLORER.EXE by executing LoadLibraryW with the DLL component as its parameter

```
00401716  .   57            PUSH EDI                                  Arg1
00401717  .v  74 07         JE SHORT a.00401720
00401719  .   E8 72FAFFFF   CALL a.00401190                           a.00401190
0040171E  .v  EB 06         JMP SHORT a.00401726
00401720  >   FF15 3880400( CALL DWORD PTR DS:[<&KERNEL32.Crea        kernel32.CreateRemoteThread
00401726  >   8945 E4       MOV DWORD PTR SS:[EBP-1C], EAX
```

```
0012FC64  00000038
0012FC68  00000000
0012FC6C  00000000
0012FC70  7C80AEDB  kernel32.LoadLibraryW
0012FC74  00D70000
0012FC78  00000000
0012FC7C  00000000
```

Virtual Address where DLL component is injected

BKDR_VERNOT.A Routine

Arrival

Installation

DLL
Injection

Connect to
Evernote
(C&C)

BKDR_VERNOT.A Routines

- Backdoor Routine
  - After logging in, it can perform the following:
    - Create notes
      - Inform the cybercriminal of successful installation
    - Access notes
      - Get backdoor commands
    - Modify notes
      - Drop-off of stolen information

BKDR_VERNOT.A Routines

- VERNOT malwares are capable of performing the following backdoor commands:
  - Download files
  - Execute files
  - Rename files
  - Unzip archive files

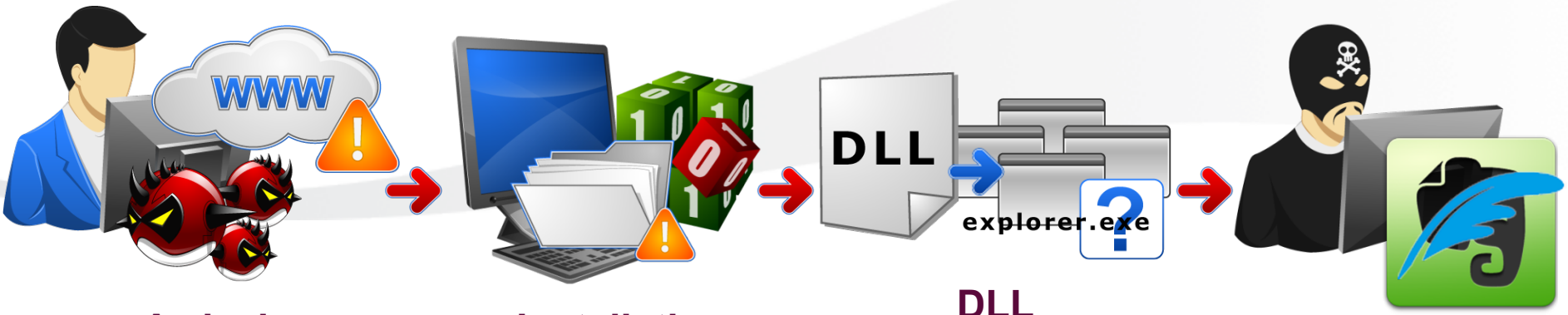
BKDR_VERNOT.A Routines

- VERNOT malwares are capable of stealing information such as:
  - Affected machine’s Registered Owner
  - Affected machine’s Registered Organization
  - Affected machine's OS information
  - Affected machine's Time Zone
  - Affected machine's User Name
  - Affected machine's Computer Name

BKDR_VERNOT.A Notes

- Evernote variant was not able to login successfully (Evernote Hacking Incident, March 2013)
- It did not exhibit interaction between the cybercriminal through the C&C servers during analysis

Comparing BKDR_VERNOT.A and BKDR_VERNOT.B



Arrival

Installation

DLL Injection

Connect to Evernote Blog (C&C)

What is Livedoor?

- Internet service provider
- Runs a web portal and other businesses
- Headquarters in Tokyo, Japan
- One of its services includes blogging site

livedoor® Blog

BKDR_VERNOT.B Overview

- Network Activity

#	Result	Protocol	Host	URL
1	302	HTTP		/r/user_login
2	302	HTTP		/login/?.sv=top
3	200	HTTP		
4	200	HTTP		
5	200	HTTP		
6	302	HTTP		/
7	302	HTTP		/member/
8	200	HTTP		/login?next_stored=3304d04b4a399df5
9	302	HTTP		
10	200	HTTP		
11	302	HTTP		/do_login?_key=3304d04b4a399df5&oic.time=1365598570-e8e071396b4e344d9838&openid.ns=http://s
12	200	HTTP		
13	200	HTTP		/do_login?_key=3304d04b4a399df5&oic.time=1365598570-e8e071396b4e344d9838&openid.mode=id_re
14	200	HTTP		
15	200	HTTP		/member/
16	200	HTTP		
17	200	HTTP		/blog/ /article/edit?id=26595269
18	200	HTTP		/blog/ /article/edit
19	200	HTTP		
20	302	HTTP		/member/
21	302	HTTP		/login?next_stored=69dbc9069392dfcc
22	200	HTTP		
23	302	HTTP		/do_login?_key=69dbc9069392dfcc&oic.time=1366537792-1c2c3509664d2eb43217&openid.ns=http://specs.openid.net/auth/2.0&c
24	200	HTTP		
25	302	HTTP		/do_login?_key=69dbc9069392dfcc&oic.time=1366537792-1c2c3509664d2eb43217&openid.mode=id_res&openid.claimed_id=http:/
26	200	HTTP		/member/
27	200	HTTP		
28	200	HTTP		/member/
29	200	HTTP		/blog/ /article/edit?id=26595269
30	200	HTTP		/blog/ /article/edit
31	200	HTTP		/member/
32	200	HTTP		

BKDR_VERNOT.B Overview

- Livedoor blog account

livedoor.blogcms.jp/blog/ /article/edit?id=26984750

livedoor Blog Personal Publishing Assistant

旧管理画面 livedoor ヘルプ

ログアウト

マイページ

FREE

(日記) [URL]

PV(アクセス) :昨日 0 / 今日 0 UU(訪問者) :昨日 0 / 今日 0

コメント :今日 0件 / 未読 0件 トラックバック :今日 0件 / 未読 0件 メッセージ :未読 0件

参加メンバー(一覧)

記事を書く

記事一覧

コメント/TB

画像/ファイル

アクセス解析

ブログ設定

えもじメーカー

再編集中... 公開時のURLを確認する

ブログTIPS カテゴリを整頓できる新機能『カテゴリ階層化』リリース！ 閉じる

WINXP

カテゴリ1

カテゴリ2

記事を書く 続きを書く プライベート

旧投稿画面で記事を書く

文字サイズ

画像

置換 HTMLタグ編集

$_$Today is a very important day for me.$Mon Apr 22 09:12:51 2013

BKDR_VERNOT.B Overview

- For every backdoor command BKDR_VERNOT.B does, it reports back to the blog draft by editing it and adding the following strings:
  - *file create failed*- If file download fails
  - *download file succeed* – If file download succeeds
  - *Run failed*- If file execution fails
  - *Run succeed* – If file execution succeeds
  - *Exe file not found* – If file to be executed is not found
  - *Unzip failed* – If extracting archive file fails
  - *Unzip succeed* – If extracting archive file succeeds
  - *Unzip file not found* – If archive file is not found
  - *rename file failed* – If renaming file fails
  - *rename file succeed* – If renaming file succeeds
  - *src file not found* – If file to be renamed is not found

BKDR_VERNOT.B Overview

- Livedoor blog account

livedoor.blogcms.jp/blog/r ' ' /article/

記事一覧
コメント/TB
画像/ファイル
アクセス解析
ブログ設定
えもじメーカー

一括操作 実行 すべてのカテゴリ すべての月 25件ずつ 下書きのみ

記事タイトル	カテゴリ	コメント	TB	公開設定	削除
WINXP 2013-04-22 09:12:08 記事をコピー	記事カテゴリなし / 記事カテゴリなし	0	0	下書き	
WINXP 2013-04-21 17:23:04 記事をコピー	記事カテゴリなし / 記事カテゴリなし	0	0	下書き	
BI 2013-04-17 11:10:49 記事をコピー	記事カテゴリなし / 記事カテゴリなし	0	0	下書き	
ANT 2013-04-13 02:28:35 記事をコピー	記事カテゴリなし / 記事カテゴリなし	0	0	下書き	
CI sa-35 2013-04-12 07:18:38 記事をコピー	記事カテゴリなし / 記事カテゴリなし	0	0	下書き	
CC 261245 2013-04-11 21:14:38 記事をコピー	記事カテゴリなし / 記事カテゴリなし	0	0	下書き	
TW 3 2013-04-11 13:21:02 記事をコピー	記事カテゴリなし / 記事カテゴリなし	0	0	下書き	
WINXP 2013-04-11 13:17:38 記事をコピー	記事カテゴリなし / 記事カテゴリなし	0	0	下書き	
WINXP 2013-04-11 03:32:38 記事をコピー	記事カテゴリなし / 記事カテゴリなし	0	0	下書き	
BR VF1 2013-04-10 11:21:02 記事をコピー	記事カテゴリなし / 記事カテゴリなし	0	0	下書き	
WINXP 2013-04-10 11:11:41 記事をコピー	記事カテゴリなし / 記事カテゴリなし	0	0	下書き	
CV 1 2013-04-10 10:41:54 記事をコピー	記事カテゴリなし / 記事カテゴリなし	0	0	下書き	
OE A 2013-04-10 08:01:51 記事をコピー	記事カテゴリなし / 記事カテゴリなし	0	0	下書き	

一括操作 実行 新しいカテゴリを作る

BKDR_VERNOT.B Notes

- It did not exhibit interaction between the cybercriminal through the C&C servers during analysis

Solutions

- Trend Micro Detection
  - BKDR_VERNOT.A (Evernote)
    - CPR 9.820.03
      - » 03/15/2013
    - OPR 9.821.00
      - » 03/16/2013
  - BKDR_VERNOT.B (Livedoor)
    - CPR 9.874.09
      - » 04/10/2013
    - OPR 9.875.00
      - » 04/11/2013

Solutions

- Proactive Sourcing
- Clean up
  - Supported by Genericlean
  - Version

1. Restart in Safe Mode
2. Delete the dropper and %User Temp%\NETUT.dll
3. Delete the added registry entry for automatic execution

Solutions

- Collaboration with concerned sites
  - Evernote
    - Collaborated with the CTO of Evernote

Best Community Share

Dave Engberg · 3 months ago

Nikko - I'm the CTO over at Evernote, and wanted to get more information about the requests this trojan is making against our service. Unfortunately, the JPEGs in your article don't show the parts of the bot or its requests that would allow us to uniquely identify the relevant account and/or fingerprint the requests to identify the compromised machines (IPs) that are talking to us to help the security community scope out this particular botnet.

We tried reaching out through LinkedIn to connect with your folks, but didn't get a reply. You can reach me via dengberg at my company's domain. Thanks!

14 Share ›

Solutions

- Collaboration with concerned sites
  - According to Dave Engbert
    - 4 more accounts are used similarly
    - Same connection requests
    - Some are registered as early as February 2013
    - Limited activities

Solutions

- Evernote implemented extra layers of security after the incident
  - Two-step Verification (Optional)
  - Authorized Applications
  - Access History Future

Solutions

- Access History Feature

https://www.evernote.com/AccessHistory.action

EVERNOTE

Go to no

Account Summary

Personal Settings

Security

Access History

Connected Services

Reminders

Upgrade

Access History

You are currently accessing Evernote from IP address 1C 3. 32 in Pampanga, Philippines.

The following apps have accessed your account since Thursday, August 8 2013

App	Accessed	IP Address (Estimated Location)
Evernote Web	8/8/2013	1C 3. 32 (Pampanga, Philippines)

TREND MICRO

Conclusion

- Relying on legitimate services to guard against threats may not provide ample security for users. With the consumerization of IT, enterprises in particular are vulnerable to data loss through compromised legitimate services brought by its employees for use in the office. The more employees bring their own apps or services in the corporate network without ample policy, the more risks there are to corporate data.
- This incident shows that cybercriminals treat legitimate services as assets with potential for malware use, which is something that many consumer and enterprise users may not be ready for. Should IT departments or individuals fail to look over these channels; chances of compromising sensitive information will remain high.

Questions?