

Summary Of Mobile Threats For Year 2005

The first Mobile Threat that appeared in year 2004, that is Cabir.A has shown that mobile phone threat is a proof-of-concept application.. However, most Symbian malwares are still quite primitive and most of them are not in the form of executable code. It is able to replicates itself via bluetooth devices that supporting Symbian Series 60 user interface platform.

To date, Cabir.A has been spreaded widely until affected many countries such as Malaysia, United States, United Kingdom, Italy, Russia, Indonesia, Japan, New Zealand, Australia, Singapore etc.

Cell phone threat are currently targeting on Symbian Series 60 user interface platform only because its population has been increased.

Year 2005 has been proved to us that more than 120 types of variants that exists worldwide today and virus creators has been use Cabir as a basis to create more damageable malware.

The matter that worried by anti-virus firm is that virus creators release and release their source code. A very good example is, a Brazilian fella has spreaded the cabir source code since last year December and now causing more than 26 variants that detected as Cabir Variant!

⊕ **Understanding Basic Symbian File System.**

Symbian file system can be divided into four groups and their functions are summarize as shown below:

<i>Type of drive:-</i>	<i>Functions:-</i>
C drive	Act as a flash RAM and it contains user installed applications, user data such as phonebook data, multimedia files, messaging data etc.
D drive	Act as a temporary RAM that store temporary files for applications and also some data about WAP contents.
E drive	Act as a media card drive which enable user to expand the memory storage by using an appropriate card to store applications, pictures, videos and songs.
Z drive	Act as an OS ROM which is the “heart” of the OS that contains mostly of the system and applications file.

✚ What is a Mobile Phone Virus and how does it spread?

Cell phone virus is a proof-of-concept application that might describe same as computer viruses that install itself into the targeted device and executes its malicious code to “infect” the phone with preset command.

Currently, Cell phone viruses are spreading using:

❖ *Bluetooth Wireless Technology:*

It is capable replicates itself in 10metre Bluetooth wireless range and search for bluetooth devices that are active in discovery mode. Upon detected it will pop up as Screen as shown below:



If user click yes and he may facing risk that he will be infected by this suspicious file since he didn't practice well in mobile security knowledge and he may proceed to the installation process.



During installation, it will pop up a security message as shown below:

User should be aware that installing application that without valid certificate will cause them facing a very high risk of cell-phone-viruses infection and they should only install those applications which are trustworthy.

❖ *Multimedia Messaging Services (MMS)*

This year January 2005, a new type of mobile viruses that capable spreading itself via bluetooth but also MMS has been causing public attention and AV firm pretend this is the most effective way for mobile viruses to replicates itself.

Besides, it is able to generates different codes to send itself via MMS by scanning user phonebooks contacts that might causing other innocent users with less expose to mobile security knowledge get confused and proceed to the installation process which giving opportunities to cell-phone-malware to executes itself.

Anyway, user should aware of third party application that doesn't contain any valid certificates that might be a virus!

❖ Faked games, applications and security patches at Warez/Shareware site.

This is also a way that cell phone viruses developers used to spread their stuff at which usually most people like to browse those site to get “free” stuff and didn't aware that actually it has been packed with mobile **trojan/malwares** inside them.

This year, those cell phone malwares has been disguised as mobile security software, Security patches, desirable games and application by user and also those most wanted themes that containing pornographic.

⊕ **Evolution of Cell Phone Viruses**

- ❖ June 2004—Cabir detected and it's a proof-of-concept application that able to spread itself via Bluetooth devices and it will only executes itself on Symbian Series 60 User Interface Platform.
- ❖ August 2004—Qdial found and it is capable sending premium rate messages to multimedia provider and causing unwanted charge and it is spreading in a Famous Camera-Shooting Mosquito game. User in United Kingdom, Germany, the Netherlands, and Switzerland are affected with this Trojan
- ❖ November 2004—Skulls.A Trojan found and it will replace those application icon into a skulls icon and it will disable those infected application from running by replacing a non-functional file into the targeted system.
- ❖ December 2004—Mgdropper detected and it will disable user from uninstalling it and disguised by a famous PC game—Metal Gear
- ❖ December 2005—Lasco.A reported and it is able to infects other *.SIS file by injecting itself to the targeted *.SIS installation file besides spreading via Bluetooth.

- ❖ February 2005—Locknut.A found and it is capable disable certain application in the phone and causing the phone system crashes. Only installing disinfection tool can fix it only.
- ❖ March 2005—Dampig.A Trojan found and it is cable to prevent targeted application from running and it's also packing with several Cabir variant together.
- ❖ April 2005—Fontal.A reported and it's the first cell-phone-virus that capable disable the phone from rebooting and causing user data lost unworthy.
- ❖ April 2005—Hobbes.A found and it will only crashes phone menu system that running on older Symbian OS.
- ❖ April 2005—71 cell-phone-trojan found and most of them was packed in those most-wanted application and games.
- ❖ July 2005—OneHoop.A and Booton.A Trojan found that capable spreading simultaneously via Bluetooth and replace the phone icon with a Heart-Shaped icon.
- ❖ July 2005—Cadomesk.A/B found and it will disable a large amount of application and spreading cabir variant after it has been installed.
- ❖ July 2005—Skudoo.B found and it claims itself a famous games called Splinter Cell.
- ❖ July 2005—Mabtal.A detected and it's able to trick user to reboot the phone automatically once the user access the installed application.
- ❖ August 2005—Blankfont.A Trojan found and it is capable causing the phone caption to be invisible and causing user fail to distinguish those options and menu properties.
- ❖ September 2005—DoomBoot.A found and causing the phone fail to boot itself on the next restart.
- ❖ September 2005—Multidropper.A and its variant found and it contains a large amount of repack Trojan that crashes the phone system.
- ❖ October 2005—Commwarrior.C reported and it is able to self-protecting from user to delete or remove them manually, besides, it is able to changed user wallpaper and operator logo and it's causing while user access WAP site, it will link into the creator homepage about the worm. Only installing the right disinfection tool or anti-virus application will fix it only.
- ❖ November 2005—CardTrap.A found and it's the first cell-phone-trojan bundle with PC malwares and it's capable disable a large amount of application in the phone.
- ❖ November 2005—CardBlock.A found and it's capable disable the phone from startup and it's also capable locking the media card with random password to avoid user to access their data.
- ❖ December 2005—PbSender.A, PbSender.B and PbSender.C found and it's capable packing user PhoneBook, Calendar, To-Do and Notes into a text file and sent through Bluetooth which access user data without their permissions or confirmations.

Source: McAfee Inc. and TrendMicro Inc.

✚ Analysis on Mobile Malwares:

❖ *SymbOS\Mabtal.A*

Profimail v2.75_FULL.SIS/ Mabtal.A is a SIS file malware that pretends to be a cracked version of Profimail which is a very popular E-Mailing third party application in Symbian Platform, in fact, it is a malware which drops Mabir.A, Caribe and Fontal variants into the phone system, besides, it also drops some corrupted binaries file which causing the phone auto-restart and showing fatal error message. Next the phone will fail to boot-up permanently.

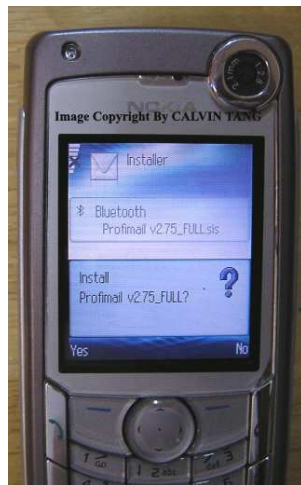
Suspicious file tested using the following handsets:

NOKIA 3660 (Symbian OS 6.1)

NOKIA 6680 (Symbian OS 8.0)

Positive analysis results:

While tested using the above handsets, both platform is affected. When user tries to install the suspicious file into his phone, it will look like the above image:

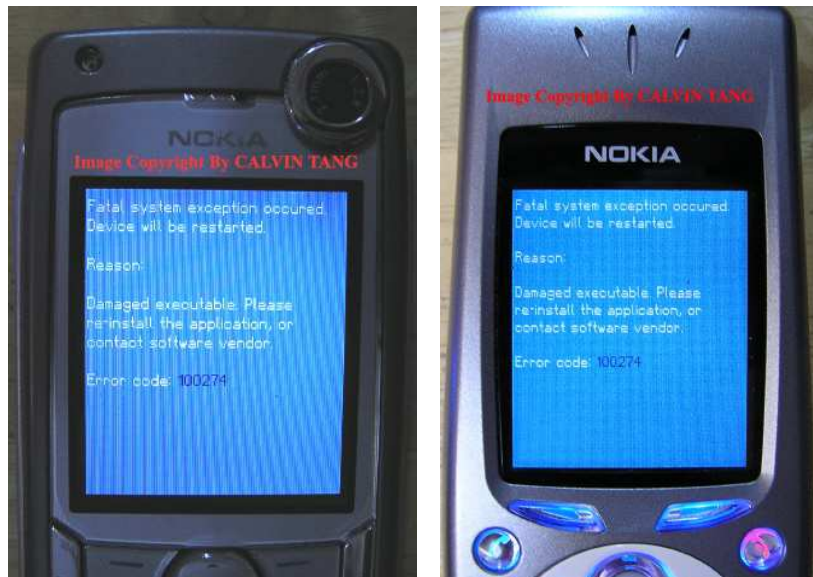


While installing the suspicious file, it will show a message as shown below:



This suspicious file automatically installed all files into the phone memory. Cabir virus will start spreading via Bluetooth and keeps listening if any incoming message arrives in the phone, when any SMS/MMS message arrives in the phone, mabir.A virus will immediately sent itself out via MMS for spreading purpose.

When user tries to access the **Profimail** and **ProfiExplorer** third party application, it may display an error message as shown below:



After it has successfully restarted, due to the corrupted fonts, the device can't boot up permanently.

By using SISscan(A Symbian malwares analyzing tool), the following files were detected as a malware file:

11x12 euro_fonts.gdr detected as SymbOS.Fontal.A
CARIBE0.APP detected as SymbOS.Mabir.A
CARIBE0.RSC detected as SymbOS.Cabir
flo0.mdl detected as SymbOS.Mabir.A
flo.mdl detected as SymbOS.Mabir.A
caribe.app detected as SymbOS.Mabir.A
caribe.rsc detected as SymbOS.Cabir
Appinst.app detected as SymbOS.Cabir.U2
Appinst.aif detected as SymbOS.Cabir.U2

This malware doesn't come with any valid digital certificate but it can replicate itself via Bluetooth or MMS(Mabir.A) and it will cause severe damage to Symbian OS 6.1 handsets!

❖ *SymbOS/CardBlock.A*

Description:

SymbOS/CardBlock.A capable deleting the phone system data file and it will block the memory card from being accessed.

Affected Platforms:

Tested on:

- Nokia 6680
- Nokia 3660

Affected:

- Nokia 6680 ONLY

Analysis/Observation:

This Trojan was distributed in an application file and it is spreading in instantsis.v2.1.cracked.by.binzpda.SIS.

Symptoms:

When user tries to install this suspicious file, the image below shown is the screenshot taken during installation process:



SymbOS/CardBlock.A claims to be a Series 60 third party application. Upon installation an agreement will be shown and ask user if he or she agree with those terms listed and proceed to the next step to finalize the installation process.

After installation completed, the application icon will be shown in the phone as shown below:



Method of Infection

This Trojan will execute itself only while user tries to access them.

While user try to access the suspicious application, it will looks like the image below:



While user try to access the options panel and proceed to "Send>Via Bluetooth", the trojan will start to executes itself and the phone will started to hang and lagging and the memory card will locked by it with random password code.



It will generate different password to lock up the media card. Further info will be confirmed by Anti-Virus firm. I personally have scarified my 64MB DV-RS-MMC for testing this Trojan and it proves to me that it is capable locking the memory card.

While one of the component file being disassembled, the following strings was observed that will delete the phone system data:

```
C:\system\install
C:\system\data
C:\system\libs
C:\system\mail
```

C:\system\bootdata

After those file was damaged and it will prevents the phone from starting up after the phone is rebooted and shows the following error messages:

'Phone startup failed, contact the retailer. '



Prevention:

SymbOS/CardLock.A requires that the user intentionally install them into the device. As always, users should not install any third party application from unknown site. According to the security expert that I met him, this trojan is really spreading widely in WAREZ site, please take alert about it!

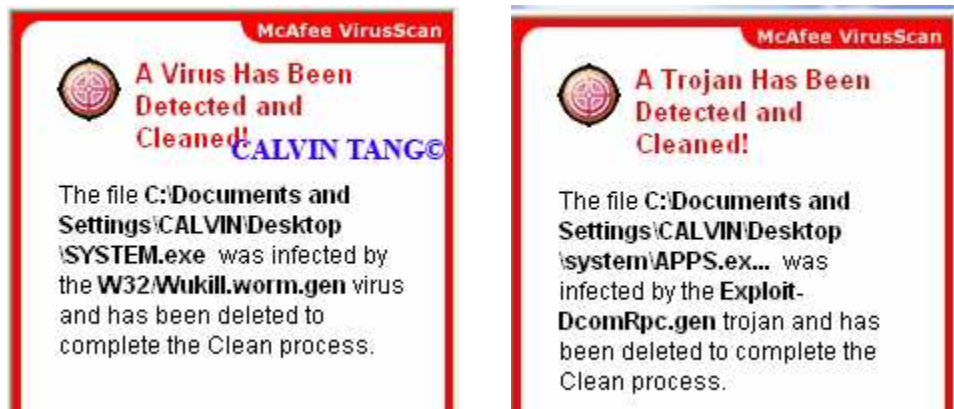
How to uninstall:

If the phone has been rebooted, hard reset method must be apply to the phone and password protected memory card can be formatted in NOKIA 9210/6630/6680/6681 only, else, user may advise to take back to the retailer to be sent back to the factory.

❖ *SymbOS/CardTrap.B or SymbOS/MultiDropper.H*

Description:

SymbOS/CardTrap.B(F-SECURE) \ SymbOS/MultiDropper.H contains SymbOS/Skulls.H, SymbOS/Cabir.B, SymbOS/Doomboot.A, SymbOS/Cabir.A which will disable most of the functional application to non-working application. It was packed together with an application and named itself as CamcorderPro v3.00 final.SIS. It replaces a large number of application file into non-functional file. Besides, it also contains Windows Platform Worms, namely **W32/Wukill.Worm,BackDoor-AXJ, Win32/Exploit-DcomRpc.gen**



Affected Platforms:

Tested on:

- Nokia 6680

Affected:

- Nokia 6680

Payload:

This trojan was packed together with an application and spreaded in one of the warez site. This trojan will drops a large amount of non-functional and corrupted files together with Windows platform worms which will executed during autorun. Theoretically, the dropping of Doomboot. A trojan will cause the phone ail to reboot next time, but due to some 'technical problem', no harm was observed in NOKIA 6680. Anyway, The other phones like NOKIA 6600 and NOKIA 3650 might attacked by it.

The Windows malwares that packed inside the *.SIS file contains an autorun.inf file. The purpose of this file is to run the script it contains upon the mounting of a drive. However, it will not working for the Windows malwares that installed in the media card but only for CD-ROM media is affected only.



Analysis/Observation:

This trojan was distributed in an application file and it is spreading in **CamcorderPro v3.00 final.SIS**.

Symptoms:

When user tries to install this suspicious application, the screenshot below will be present during installation process:



The only observable change, beside from the additional Win32 payload, it changes to the text displayed during install "CamcorderPro v3.00 final release cracked by B_S".



Prevention:

SymbOS/CardTrap.B(F-SECURE) \ SymbOS/MultiDropper.H (McAfee) requires that the user intentionally install them into the device. As always, users should never install any third party application from unknown site or sources.

Method Of Infection:

This Trojan requires the user intentionally install it. Win32 payload will only be triggered if it manually run from a Windows PC

How to uninstall:

First, Use Anti-Virus software to scan through the media card, make sure the AV scanning engine is up-to-date. Second, by installing Anti-Virus application into the phone to disinfect it.

Source: McAfee Inc.

❖ *SymbOS\PbSender.A***Description:**

This type of mobile virus is very interesting that it'll steal user phonebook data and then it will compile it into a text file and sent it through Bluetooth without user confirmation.

So far, this is the first Symbian Virus that I've seen that it will steal user data without user confirmation and sent through other Bluetooth supported devices.

Affected Platforms:

Tested on:

- Nokia 6680
- Nokia 3660

Affected:

- Nokia 6680

Analysis/Observation:

This trojan was distributed in an application file and it is spreading in **pbexplorer.SIS**.

Symptoms:

When user tries to install this suspicious *.SIS file, the image shown below is screenshot taken during installation process:

After installation complete, the application has set to run automatically and will display the following text:



```
| Phone Book |  
| Compacting |  
| by: lajel 202u |  
| |  
| please wait... |  
|_____|
```

```
| Compacting |  
| your contact(s),step 2 |  
| |  
| Please wait again |  
| until done... |  
|_____|
```

After the malicious process done, it will pop out a message:

"Done!!!"

If user presses [OK] the malicious program will ended itself and after some times, it will start searching for Bluetooth devices and sent all phonebook information in

text file via Bluetooth.

Prevention:

This malware requires that the user intentionally install them upon the device. As always, users should never install third party application from unknown site.

How to uninstall:

By uninstalling it at Application Manager manually.

❖ *SymbOS\PbSender.B*

Description:

There is a slightly changed in PbStealer.B, besides stealing user Phone Book data, it will also steal user “NOTES” data and compile it into a text file and sent through targeted Bluetooth devices that are in online mode or in active discovery mode.

In the analysis process, it shown that it is capable running on older Symbian phone that running on version 6.1 such as NOKIA 3650\3660\3620\7650\N-GAGE\QD etc.

For some user, they might be store their important data such as Credit Card number, ATM card PIN number, Bank Account PIN code and private and confidential company or personal data.

Therefore, user should always avoid from installing unknown source software into the phone.

Affected Platforms:

Tested on:

- Nokia 6680
- Nokia 3660

Affected:

- Nokia 6680
- Nokia 3660

Analysis/Observation:

This trojan was distributed in an application file and it is spreading in

PBEX_VIN.SIS.

Symptoms:

When user tries to install this suspicious *.SIS file, the image shown below is screenshot taken during installation process:



After installation complete, the application has set to run automatically and will display the following text:

```
| Phone Book |  
| Compacting |  
| by: lajel 202u |  
| |  
| please wait... |
```



After the malicious process done, it will pop out a message:

"Done!!!"

If user presses [OK] the malicious program will ended itself and after some times, it will start searching for Bluetooth devices and sent all phonebook information and the “NOTES” data in a text file via Bluetooth.

Propagation:

This malware will based on the file that generated at c:/System/mail/phonebook.txt and send those compiled data via Bluetooth. Here are some images that user data being compiled into a text file:



Prevention:

This malware requires that the user intentionally install them into the device. As always, users should never install third party application from unknown site or sources.

How to uninstall:

By using latest version of CalvinStinger© Symbian Viruses Disinfection Tool or just manually disinfect the phone by uninstalling it at application manager.

❖ *SymbOS\PbSender.C***Description:**

There is a slightly changed in PbStealer.c, besides stealing user Phone Book data, it will also steal user "NOTES", "To-Do" and "Calendar" data and compile it into a text file and sent through targeted Bluetooth devices that are in online mode or in active discovery mode.

In the analysis process, it shown that it is capable running on older Symbian phone that running on version 6.1 such as NOKIA 3650\3660\3620\7650\N-GAGE\QD etc but it seems fail to run on Latest Symbian OS v8.0 phones such as NOKIA 6630/6680/6681/N70/N90.

For some user, they might be store their important data such as Credit Card number, ATM card PIN number, Bank Account PIN code and private and confidential company or personal data in the phone.

Therefore, user should always avoid from installing unknown source software into the phone. This is a very good example of Symbian "Spyware" which can steal user data.

Affected Platforms:

Tested on:

- Nokia 6680
- Nokia 3660

Affected:

- Nokia 3660

Analysis/Observation:

This trojan was distributed in an application file and it is spreading in **PBCompressor.SIS**.

Symptoms:

When user tries to install this suspicious *.SIS file, the image shown below is screenshot taken during installation process:



After installation complete, the application has set to run in hidden mode that user would be surprise no application icon in the menu system but it's actually running in the phone background and sent user data without their confirmation.

Propagation:

This malware will based on the file that generated at c:/System/mail/phonebook.txt and send those compiled data via Bluetooth. Here are some images that user data being compiled into a text file:



```
(To-do list .h. . T ..Chimes *$j. NQ ... .. *$j.. .Hello calvin. ).

NOTES:
P .d. . .#c$0
÷ . . . . .
memo... . i@ . e.N àñññà .X...eégév,yly0â; .N-yñ,_èNPà!! . . . . .

CALENDAR & TO DO:
P ...:Y.jññ. <. gT.Q (Q..± . . . . . : .$.i. . .@. .@.@
4: .. #€ € | .. i .. DE... . ... : *$i.. .Calvin. . )=$â.=$â.ñ
```

This malware requires that the user intentionally install them upon the device. As always, users should never install third party application from unknown site or sources.

By using latest version of CalvinStinger© Symbian Viruses Disinfection Tool or using Symbian anti-virus application, updated virus database is a must in order to fully disinfect your phone.

⊕ Anti-Virus Application and Disinfection Tool

❖ *Symantec Anti-Virus*

Symantec anti-virus is one of the anti-virus application that built in with powerful firewall functionality. This AV product will automatically startup each time the phone switch on, besides, so far, no any other known mobile malwares which can disable and replace a corrupted file to disable this AV products, anyway, users are advice to keep updated their virus definition to ensure protected from latest mobile threats.

When tested using a couple of mobile malwares into my NOKIA 6680, before any infected file that target to install certain directory in the phone or memory card, it will pop-up a message stating that what virus is trying to gain access into the phone system and prompt user whether they allow to permit the action or not. Refer to the above image for more details:



By disinfecting the phone, I have run the Symantec AV products to scan virus, although the scan time take a bit long to perform the scan(Usually depends on user, if users phone memory or memory card occupied a large amount of space, sure, it takes a long time to perform its action). When the scanning is in progress, it will look like the image below, by stating how many viruses has been found and what directory is currently scanning.



When scanning is complete, it will pops up a message stating that how many virus is detected and show what virus is infecting the phone, sadly, Symantec AV company didn't implement a command to delete all infected files one-time-go, but it prompt users to delete them one by one which is wasting of time.

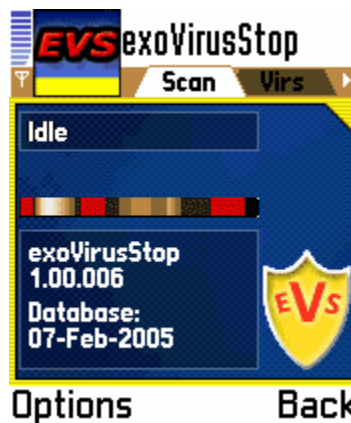
Besides, although it scanning engine is much more accurate if compare with other AV vendors product but it fail to perform its 'Anti-Virus' functionality, after I have deleted all the infected file and the phone has been restarted, the same thing happen, the malwares is still exists in targeted directory





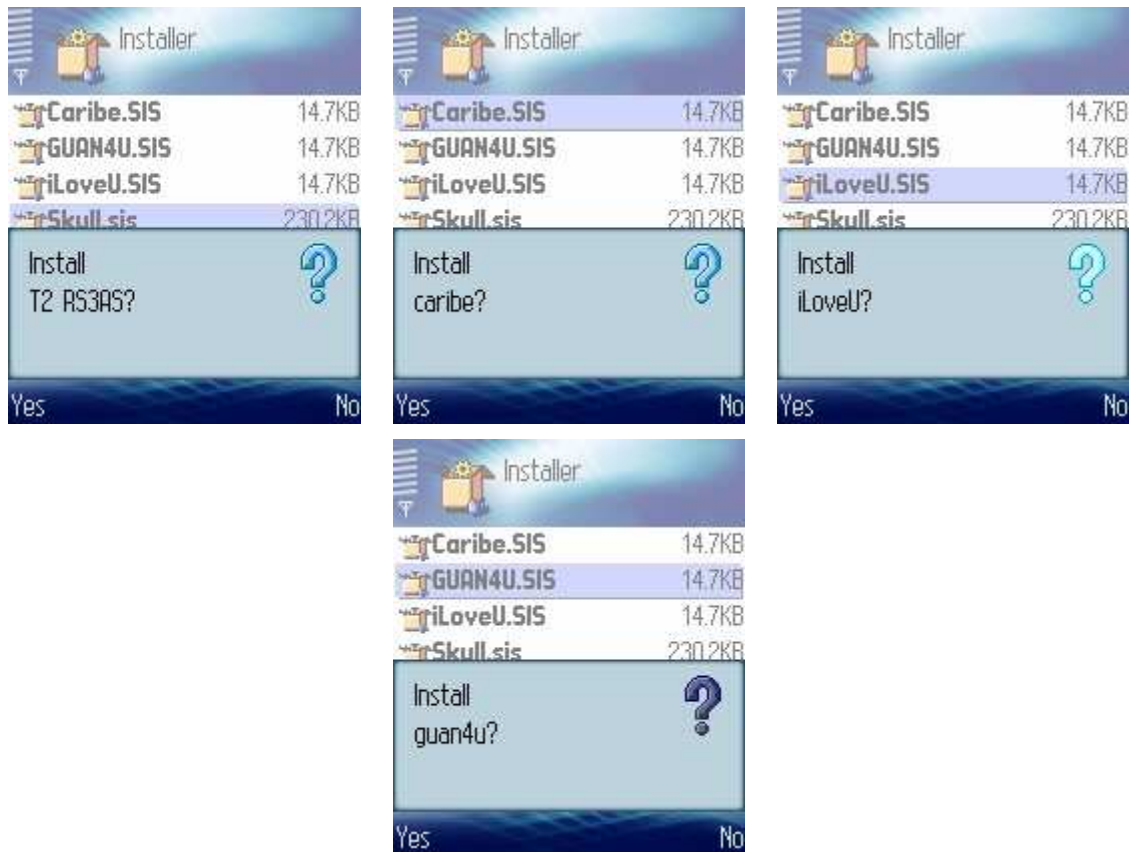
Symantec anti-virus built with strong firewall functionality is the most powerful anti-virus application that I have tested, that is, it will prompt users whether they allow or deny the infected file to be installed in targeted directory.

❖ ExosVirusStop



ExoVirusStop is an anti-virus application which protect user free from mobile viruses. It consume only a little memory when it's running because of it's small file size. Besides, it provides a Virus Dictionary which can let user to know more about mobile viruses. The scanning engine just takes a few seconds to perform its scanning action.

To test this anti-virus application, I've installed **Cabir.B**, **Cabir.S**, **Cabir.T**, **Skulls.C**, **Skulls.H** and **Trojan Mosquito**.



While I was testing them with cabir variants, only Cabir.B was detected and the rest of them were not detected by it. Yes, it can remove Caribe virus successfully but unfortunately, from this testing results, this prove that ExoVirusStop scanning engine is not that strong and accurate and thus its scanning engine may out-to-date if compare to others anti-virus products.

When testing them with skulls trojan, it only capable detecting Skulls.C only and skulls.H was not detected in the testing progress. When Skulls trojan is detected, it will automatically remove it but it require user to reboot the phone to finish disinfection process. While I was following their instruction, my phone was stuck on the next reboot and menu system can be access and thus all my phone system being disabled.

When trojan mosquito was installed into the phone, it will detect it as a Trojan Mosquito but not removing them, it will pop out a message stating if it's a warez version mosquito game, please uninstall it.

Generally, this anti-virus application is not up-to-date and this may cause user vulnerable to new viruses.

❖ McAfee Stinger

Cingular & McAfee have partnered to provide disinfection tool for Series 60 user. This Stinger application is able to detect and removes the following mobile malwares:-



- * CommWarrior.A
- * CommWarrior.B
- * Drever.A
- * Locknut.B
- * Fontal.A

This application had been tested by me and it works fine. For me, this is a very great disinfection tools if compare to F-SECURE and other AV vendors because this application can one time detect and remove 5 malwares in just one time scan!

While I was testing them with some malwares installed in the phone, it will come out

with a text stating what malware has been detected and auto remove it just less than 10 second!

```
McAfee Stinger Mobile  
(C) 2005 McAfee, Inc.  
Virus found ...  
Removing 'Fontal'
```

Summary:-

Pros:-

- 1. Scanning engine detects malware accurately.**
- 2. Memory consumption is very least, just about 9.5Kb**
- 3. Detecting 5 malware in just one time scan**
- 4. Scan malware just less than 10 seconds.**

Cons:-

- 1. Due to lack of graphical user interface(GUI), user may panic if it is a virus.**

❖ Trend Micro Mobile Security

TrendMicro is one of the anti-virus vendors which also provide security solution to devices that are running on Symbian Series 60 User Interface Platform.

It provides latest security features such as Anti-Spam to block unwanted contents and it is also providing BlueStab protection in order to detect those malwares arrive in Bluetooth Connection accurately.



For reviewing how good this Anti-Virus is, I've installed a couple of latest mobile malware that had just been reported such as Commwarrior.C, CardTrap C and also the latest one, PbSender.A.

While it's scanning the phone if it contains any viruses, it contains also a notification of how many suspicious files have been found:



After Scanning completed, it will pop-up a message on the screen with message:



After user click [OK] and it will pop out a screen indicating what and how many viruses that had been executes its malicious activity in the phone:



This anti-virus also provides a log to provide user a convenient way to check recent activities in the phone:



Generally, this is a very user-friendly anti-virus besides providing anti-spam features. Unfortunately, this Av application only protect phone that running on latest Symbian OS v7.0 or higher only.

Summary:-

Pros:

- 1. Updated Virus Definitions**
- 2. Powerful scanning engines that scan through the phone accurately.**
- 3. Anti-Spam features.**
- 4. Providing Real-Time Scan**

Cons:

- 1. It can just installs into the internal memory only and thus causing user have to provide enough memory for the internal memory to ensure no lagging or crashing phenomenon occur.**
- 2. Unfortunately, it is only supporting phones that running on Symbian OS v7.0 or higher and older phone like NOKIA3650/3660/7650/N-Gage etc may not able to install this product due to limited application compatibility**

❖ F-Secure Anti-Virus



F-Secure Anti-Virus for Symbian Series 60 platform provides real-time protection against cell phone viruses and it's also providing the latest virus definition to ensure user less vulnerable to latest mobile threat.

Before getting the anti-virus working, you must first activate your product via GPRS/EDGE/3G packet data network prior to get it works.



While any incoming suspicious file that contains malwares signature, F-Secure AV immediately generate a warning message to avoid user from installing the suspicious file into the phone:



It will shows what malwares had been detected and list out the infected directory and the file name:



It will automatically quarantine the infected file:



While scanning is in the progress:



After scanning completed, it will shows a total number of how many mobile malware found and how many file are being scanned or haven't scanned:



It will show what files had been quarantine:



To test the accuracy of the scanning engine and their security solution to handle cell phone malwares, I've installed one of the Skulls Trojan in the 52 repack Trojans that reported last time.

Although its scanning engine is quite accurate to detect those malwares but unfortunately, it has proven that its security solution is still not good enough because it doesn't quarantine/delete the infected malicious file and causing certain unwanted file or non-functional icon still exists in the phone.

Generally, the most attracting part of F-Secure Anti-Virus is they react fast when a mobile virus exists and they provide latest virus definition for user. Unfortunately, due to its large size of its application, some low processing phone like NOKIA 7650/3650/3660 will cause some annoying phenomenon like lagging or crashing phenomenon occur. Besides, its security solution handling method is very poor and doesn't fix the infected phone successfully.

Summary:-

Pros:-

- 1. Accurate scanning engine**
- 2. Providing latest virus definition**
- 3. Providing real-time scan**

Cons:-

- 1. It will takes up a lot of memory and may cause lagging or system crashing phenomenon occur in lower processing phone such as NOKIA 7650/3650/3660etc.**
- 2. It can only installs itself into the phone internal memory**
- 3. Its security solution method is still not very strong and causing certain unwanted files or non-functional files still exists in the phone.**

❖ McAfee Virus Scan



McAfee is one of the “Giant Company” in AV firm and it’s famous with its Security product and today more than 100 million computers worldwide were protected by McAfee. Nevertheless, it’s also providing an Anti-Virus for Symbian Series 60 User Interface Platform.

McAfee Virus Scan provides latest definitions from its server to keep user protected from newly discover virus and it’s also providing real-time-scan to ensure it will not disabled by mobile viruses and also protected user from infected by viruses.

Besides, it’s also providing Message scan for all incoming files that will reach at user Inbox’s to prevent user infected by viruses.

I’ve install a couple of Trojans and worms into the phone and seems that right after the file reaches the phone, McAfee Virus Scan will automatically generates a warning message to ensure user do not install it.



User can select either to grant access for the suspicious file to be installed into the phone or ignore the warning message:



There have 5 options for user to select on how will the anti-virus perform its work and this is the only anti-virus application that I've found that providing many options to let user to choose their desire option:



While it's in scanning progress:



Summary after scanning has completed:



It will also show what file had been detected:



It also provide a log feature to provide user to check the activities that done by the anti-virus:



This anti-virus application also provide Quarantine feature and the image shown below is screenshot indicating what file has been quarantined:



Unfortunately, McAfee Virus Scan still has not been officially announced yet and they are still working hard to release the final testing version to ensure the AV working in a very fine condition!

Generally, this Anti-Virus application provides latest virus definitions and it is also providing real-time scanning for the phone and also real-time protection for all incoming message. Just that it's a BETA version and may contains some software bugs!

Summary:

Pros:-

- 1. Providing latest virus definitions from time to time**
- 2. Real Time scanning on the phone**
- 3. Incoming data are being monitored to ensure user protected from viruses.**
- 4. Accurate scanning engine.**

Cons:-

- 1. It's a BETA version and may contains software bugs.**

The Future of Mobile Viruses. Will they die? Or Will They Just Evolve into Something MORE?

For the year 2005, the number of mobile viruses has reached about 120 types of them including those variants.

The Symbian operating system now has an 80.5% market share. Just as virus writers now focus on Microsoft's OS and creating viruses on it. Same as Symbian OS, due to the increasement of population and thus Symbian Series 60 be the favorite target for virus writers to create more mobile malwares.

Commwarrior incident has been best described that Telco's has take attention on them and certain operator like T-Mobile, TeliaSonara and Elisa has been cooperates with F-Secure Anti-Virus Company to fight against those mobile malwares and protect their customer from infected by mobile malwares.

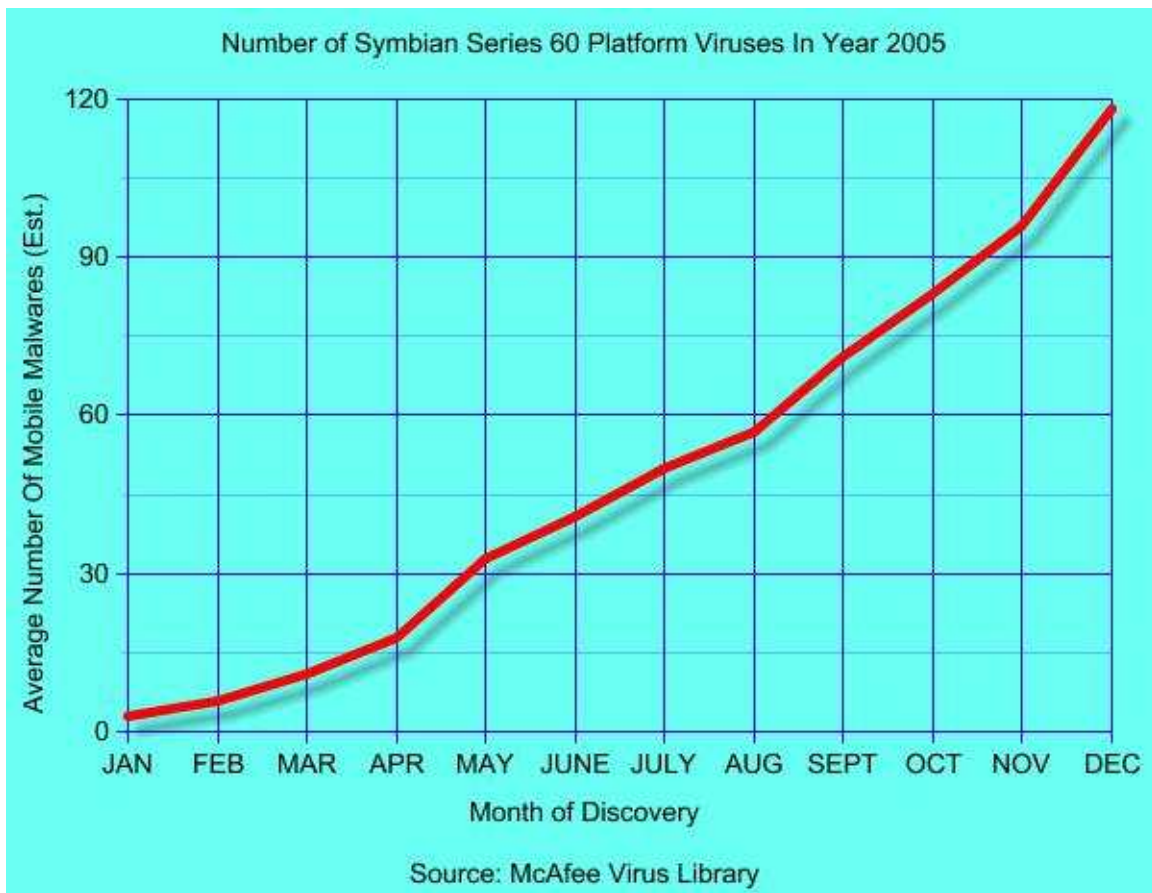
Right now, most cell-phone-viruses only a repack stuff done by those annoying kids who like to get credit only but if we pay a study carefully, what we notice is there are only 4 real Symbian OS virus creators namely Lab 29A, Velasco, el01dr and Lajel only. Will there be any new virus creator in the future? For me, there will be still have a small amount of new creator in the future and might be increase from time to time. The matter that worried most by AV firm is that virus creators try to post their source code in the internet and make it as an opening source project that might causing a large number of variants created!

Mobile threats will never stop and virus creators are trying to exploit as much security vulnerabilities as they can. For now, Symbian OS contains many "holes" and it may give chance for them to exploit the vulnerabilities of the Operating System and thus more Symbian user will be affected by mobile malwares if they didn't practice well in handling a suspicious file that might be a malwares or threat.

However, we can see some "light" from Symbian about their improvement in security feature. Well, Symbian is "eclipsing" its new executable format which means where the loader loads DLLs located on a higher order drive (e.g. C drive) to dynamically replace files on the firmware (Z drive). Therefore, "skulls trojan" attacks no longer function in Symbian OS v9.0 onwards.

There are still some undiscoverable method of infection that have not been reported yet but I pretend there will be in the future as virus creators always come up with idea with different infection method to causing effective damage to the phone and also computer. For an example, they can lock the user data, self-replicating itself, self protecting itself and also format the phone data without user authorization.

⊕ Graph Indicating Mobile Malwares Exists In Year 2005





Introduction of Author:

Calvin Tang was born in Malaysia in 1988 and currently work as an Independent Mobile Malware Researcher for Anti-Virus firm. He's specialized in researching mobile malware and capable analyzing minor part of a mobile malware.

He has started his researching job since April 2005 and to date he had discovered and found about 70+ mobile malwares that exists in the internet. He had posted his analysis report of those mobile malwares in several forum to keep public get attention about new malware.

He has also released his first disinfection tool to the public on December of 2005 namely "*CalvinStinger*" and now he's working on his latest version of the disinfection tool and publish his first while paper of title "*Summary Of Mobile Threats For Year 2005*".

Currently, he's still studying in a high school and will complete his high school study on this November.



Contact

Author: **Calvin Tang**

For more info about mobile viruses, please visit:

www.pipx.net/calvinstinger

If you have any suspicious file, feel free and submit it to

calvin@topplus.com.my

Calvin Tang 2006 © All rights reserved.