symantec™

A deep look into Symbian threats

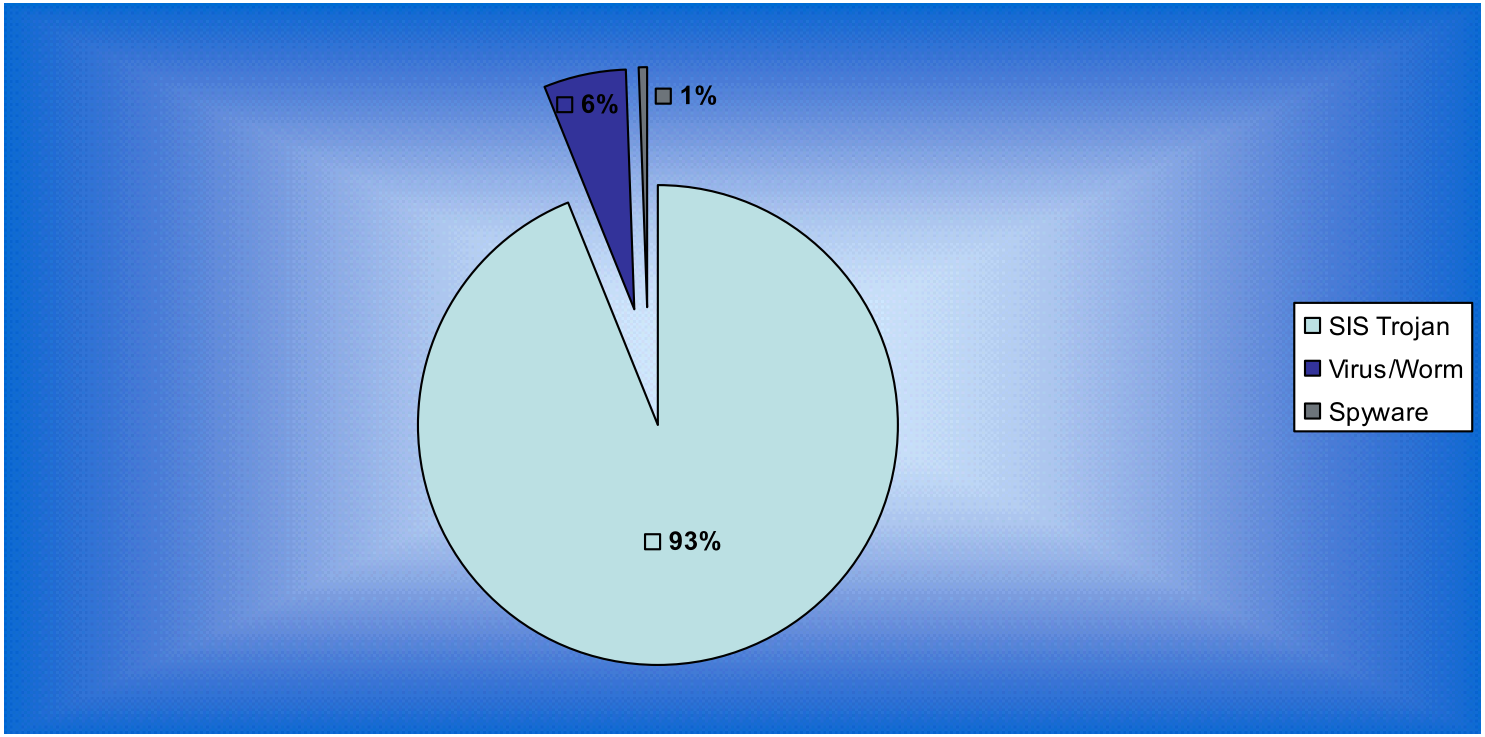
Robert Xiang Wang
Senior Security Analyst
Symantec Security Response

symantec.™

What behind the door?

- Agenda
  - Existing threats and security risks
  - How do they work?
  - Potential Risks
  - What are going to come live tomorrow?
  - Questions?

Existing threats and risks

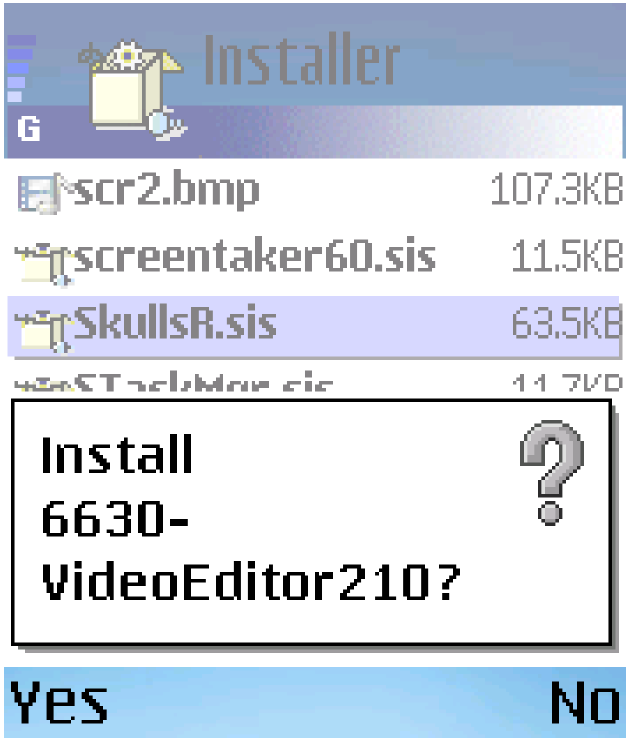


How do they work

- Delivery Vector
- Load Point
- Self-replication
- Stealth and Anti-Removal
- Watchdog
- Exploit
- Data Disclosure
- Payload

Delivery Vector

- SIS files
- Social engineering banner name
- MMC



Installer

scr2.bmp	107.3KB
screentaker60.sis	11.5KB
SkullsR.sis	63.5KB
STaskMgr.sis	11.7KB

Install 6630-VideoEditor210?

Before we go further…

- Two CPU state: ARM and THUMB
- Registers
- Standard API calls

```
; RApaLsSession::StartApp(CApaCommandLine const &)
StartApp__13RApaLsSessionRC15CApaCommandLine ; CODE XREF: start_commwarrior_c+E6□p
                LDR     R3, =__imp_StartApp__13RApaLsSessionRC15CApaCommandLine
                LDR     R3, [R3]
                BX      R3
; End of function RApaLsSession::StartApp(CApaCommandLine const &)

                ALIGN 4
off_1000046C    DCD __imp_StartApp__13RApaLsSessionRC15CApaCommandLine
                                        ; DATA XREF: RApaLsSession::StartApp(CApaCommandLine const &)
                                        ; RApaLsSession::StartApp(CApaCommandLine const &)
```

Load Points

- MDL files in “\system\recogs\” folder
- Exploit the insecure file searching mechanism
- Overwrite legitimate executable with a copy of the threat itself

```
void CCommwarriorARecognizer::LaunchCommwarrior()
{
    // absolute file path to Commwarrior
    TFileName fnCommwarriorPath = _L("\\system\\updates
\\commwarrior.exe");
    RFs fsSession;
    // file server session
    User::LeaveIfError(fsSession.Connect());
    CleanupClosePushL(fsSession);
    TFindFile findFile(fsSession);
    User::LeaveIfError(findFile.FindByDir(fnCommwarriorPath,
KNullDesC));
    CApaCommandLine* cmdLine = CApaCommandLine::NewLC();
    cmdLine->SetLibraryNameL(findFile.File());
    cmdLine->SetCommandL(EApaCommandOpen);
    RApaLsSession lsSession;
    // Application Architecture server session
    User::LeaveIfError(lsSession.Connect());
    CleanupClosePushL(lsSession);
    // launch Commwarrior
    User::LeaveIfError(lsSession.StartApp(*cmdLine));
    // Destroy fsSession, lsSession and cmdLine
    CleanupStack::PopAndDestroy(3);
}
```

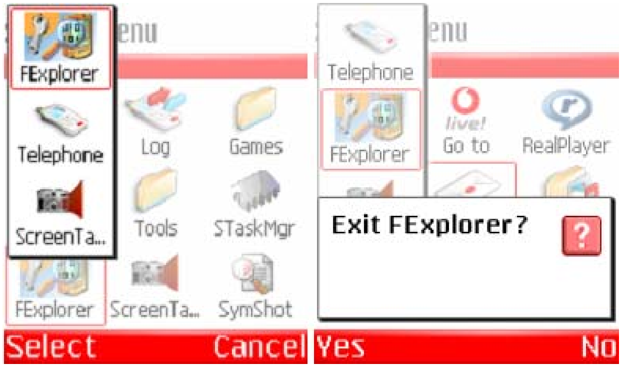
Self-replication

- Bluetooth
- Infrared
- MMS
- Removable multimedia card
- SIS file infector

TSockAddr
RSocketServ
RsSocketResolver
TBTSockAddr
TBTDevAddr
TObexBluetoothProtocolInfo
CObexClient
CObexFileObject
CPbkContactEngine
CPbkContactIter
CPbkContactItem
CMmsClientMtm
CMsvEntry

Stealth and Anti-Removal

- Hide from task list
- Use faked process/thread name
- Set process/thread into protected and system state
- Encrypted resource



Exit FExplorer?

```
void CICam::HideTask(void)
{
   Tint wgId = iEikonEnv->RootWin().Identifier();
   RWsSession wsSession = iEikonEnv->WsSession();
   CApaWindowGroupName* wgName =
CApaWindowGroupName::NewLC(wsSession, wgId);
   wgName->SetHidden(ETrue);
   wgName->SetWindowGroupName(iEikonEnv->RootWin());
   CleanupStack::PopAndDestroy();
   iEikonEnv->RootWin()->SetOrdinalPosition(-1);
}
```

Watchdog

- Interesting “feature” or “bug”: no file protection against running process
- Test CRC of its mdl module and main module, if different, then recreate from memory
- Request notification of specified process and restarts it if died

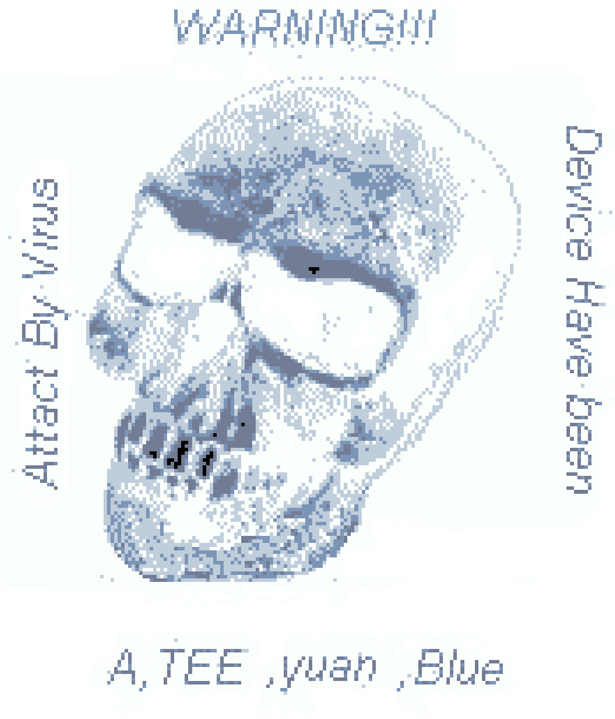
Data Disclosure

- Private information
- Device information
- SMS/MMS
- Video/Voice Calls
- Hidden cam

CContactDatabase
CContactItem
CContactItemField
CContactItemFieldSet
CContactTextField
CContactTextField
CLogClient
CLogView
CLogViewEvent
CLogViewRecent
CLogFilter
CMsvEntry
CClientMtmRegistry
CMsvSession
CMsvStore
CSmsClientMtm
CMdaAudioRecorderUtility
CVideoRecorderUtility
CCamera
HAL
PlpVariant

Various Payloads

- Disable specified applications
- Crash device
- Modify operator logo, background image
- Connect to specified server
- Dial to premium-rate number
- Insert Windows threats to MMC card



Potential risks on pre v9 OS

- Insecure file searching mechanism
- No file protection against running process
- Insecure recognizer auto-run mechanism
- No digital signature checking against executable
- Weak process/thread protection mechanism
- Weak checksum of E32 executable file
- Unprotected App. Manager settings
- Packing and unpacking

v9.x

- New E32 executable and SIS format
- Process capability set
- Data caging
- Signed SIS file
- Compressed target
- E32 executable header checksum
- Hash applications installed onto MMC
- Startup List Management API

What are going to come live tomorrow

- Adware
- Ad-Clicker
- Trackware
- Executable file infector
- And more…

Questions?

Are you ready for new challenge?

- Security is getting more and more important on Symbian OS. As security experts, we must be prepared for potential threats and security risks.

symantec™

Thank You!

Robert Xiang Wang

robert_xwang@symantec.com

(353) 1-8855744