Троян Төрлийн Хөнөөлтэй Програмын Шинжилгээ

[1] Д.Бямбадорж, [2] Б.Өсөхбаяр, [2]Ж.Нямжав
[1]Улаанбаатар их сургууль
[2]МУИС, Хэрэглээний шинжлэх ухааны сургууль

Хураангуй- ***Програмыг хөнөөлтэй код агуулж буй эсэхийг шинжлэхэд статик ба динамик гэсэн үндсэн хоёр техникийг хэрэглэдэг. Статик нь програмыг системд ажиллуулахгүйгээр зөвхөн файлд нь шинжилгээ хийх техник бол, динамик нь тусгай хяналттай, тодорхой хамгаалалттай системд програмыг ажиллуулах замаар шинжилгээ хийх арга юм. Энэ ажлаар статик болон динамик анализ дээр тулгуурлан Win32 Malware gen гэж нэрлэгддэг хөнөөлтэй програмыг сонгон авч, тухайн програмын төрөл, ажиллагаа, хор хөнөөлийг тодорхойлох боломжийг авч үзсэн.***

Түлхүүр үг—Хөнөөлтэй програм-вирус мэдээллийн аюулгүй байдал

I. Оршил

Хөнөөлт програм нь компютер болон сүлжээгээр халдварлаж хор хөнөөл учруулч, улмаар компьютер дахь системийн файл болон регистрд өөрчлөлт оруулж үйл ажиллагаа идэвхжүүлэх зорилготой байдаг. Хөнөөлтэй програм нь компьютерт нэгэнт халдварлагдсан тохиодолд програмд агуулагдаж байгаа хор хөнөөл учруулах зорилготой кодын зааврын дагуу үйл ажиллагаа хийдэг. Хөнөөлтэй код агуулсан программуудыг viruses, worms, trojans, spywares, adwares гэх мэтээр үндсэн 14 төрөл болгон ангилсан байдаг [1]. Тухайн програмыг хөнөөлтэй эсэхийг судалж тогтооход статик анализ буюу код анализ нөгөө нь динамик анализ буюу шинж байдлын анализын аргыг ашигладаг [2,3]. Win32 Malware gen нь троян төрөлд хамаардаг хөнөөлтэй програм юм. Энэ програм нь сүлжээнд холбогдсон компьютерт зөвшөөрөлгүй хандалт хийх боломжийг олгох болон тодорхой зорилготой сайтыг ачааллах гэх мэт үүрэг функцтэй.

Програмыг хөнөөлтэй код агуулж буй эсэхийг шинжлэхэд статик ба динамик гэсэн үндсэн хоёр техникийг хэрэглэдэг.

Динамик анализ нь шинж байдал дээр тулгуурлан ажиглан судлахыг динамик анализ гэдэг. Халдварлаагүй орчныг snapshot хийх болон хөнөөлтэй програм халдварласны дараахь snapshot хоёрыг харьцуулан компьютерийн системд хэрхэн өөрчлөлт орсон дээр дүн шинжилгээ гаргахад оршино. Хөнөөлт програмыг динамик анализийн аргийг ашиглан процесс, регистр, сүлжээний ачаалал, нээлттэй порт зэргийг халдвар орсон болон ороогүй үеийн байдлаар харьцуулалт хийнэ. [4] Туршилт болон шинжилгээг ганц удаагийн туршилтаар хийх боломжгүй бөгөөд олон удаагийн туршилын үр дүн дээр хөнөөлтэй програмд дүн шинжилгээг хийдэг.

Статик анализ буюу код анализ - нь тухайн хөнөөлтэй програмын эсрэг анти-вирусны програм ашиглаж илрүүлэх болон script, HTML, GUI, password, команд, control string зэргийг бүгдийг нь record буюу бичлэг хийж авна. [4] Гарсан үр дээр үндэслэн хөнөөлтэй програмын эх кодонд анализ хийн дүн шинжилгээ гаргах юм. Мөн хөнөөлтэй програм нь системийн ямар ямар сангуудыг дуудаж ажиллуулдаг болон тэдгээрт хэрхэн нөлөөлж байгаа эсэхийг тодорхойлно.

II. СУДАЛГААНЫ ОРЧИН

Хөнөөлтэй програмын шинжилгээг хийхэд тусгаарлагдсан, тусгай хяналттай, тодорхой хамгаалалттай орчинг бүрдүүлэх шаардлагатай. Хяналттай, тусгаарлагдсан орчинг бүрдүүлсний дараа үйдлийн системийн эхний төлөвийн мэдээллийг цуглуулж дараах програмуудыг хэрэглэн хөнөөлтэй програмын шинжилгээг гүйцэтгэж болно.

- PEview програмаар 32вит (PE) файлын гүйцэтгэл болон зохион байгуултыг тодорхойлдог.
- PEiD програмаар пакетлагдсан эсэхийг шалгаж, ямар програмын хэл дээр бичсэнийг тодорхойлдог.
- DependsWalker програмаар 32 вит болон 64 вит ийн виндоусын файлын системээс импортлож байгаа API болон DLL файл дээр анализ хийдэг.
- Process Explorer хост дээр ажиллаж байгаа бүх төрлийн процессуудыг энэ програмаар хянадаг.
- Process Monitor Системийн файл системд өөрчлөлт болон ямар процесс ямар хүсэлт илгээж байгаа эсэхийг хянадаг.
- WireShark Сүлжээгээр дамжин өнгөрч буй пакет дээр анализ хийдэг програм юм.
- RegShot програмаар хостын ямар регистрт өөрчлөлт орж байгаа эсэхийг нарийн тодорхойлох боломжтой.

III. ТУРШИЛТ, ҮР ДҮН

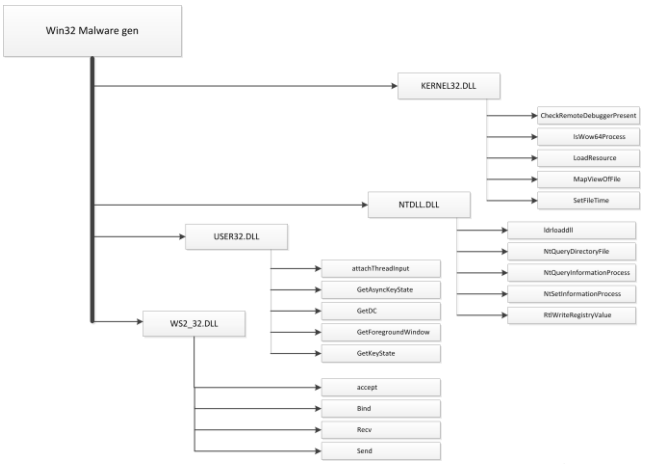
Энэ ажлаар статик болон динамик анализын аргаар програмын шинж чанарын судалгааг явуулсан. Туршилтыг явуулахдаа I7 цепутай 4 гига рамтай

компьютер дээр VMware програмыг ашиглан виртуал орчинд WINDOWS XP үйдлийн систем суулгаж үүсгэсэн. Виртуал орчинд үйдлийн системийн регистрийн мэдээллийг Regshot програмаар цуглуулсны дараа Win32 Malware gen хөнөөлтэй програмыг статик анализын аргаар тодорхойлохын тулд PEview, PEiD, DependsWalker програмын тусламжтай бүтэц, зохион байгуулалтын шинжилгээ хийсэн. Уг хөнөөлт програм нь:

- Үүссэн он сар: 2013.11.04
- www.virustotal.com сайтанд бүртгэгдсэн он сар 2015.04.11

Windows XP болон хамгийн сүүлийн NT системүүд дээр ажиллах чадвартай. Гол код нь visual C ++ програмын хэл дээр бичсэн.

Хөнөөлтэй ажиллагаа явуулахад ашиглаж байгаа DLL болон функцүүдийн схем зургийг Зураг 1-д үзүүлэв.



Зураг 1. Хөнөөлт програм нь системээс дуудаж байгаа DLL файл болон функцүүд

Зураг 1-т үзүүлсэн Win32 Malware gen програмд ашиглагдаж байгаа DLL файл болон фүнкцүүд нь дараах үндсэн үүргүүдтэй.

Kernel32.dll динамик сан нь хамгийн түгээмэл хэрэглэгддэг сан бөгөөд санах ой, файл, төхөөрөмжүүдтэй ажиллах үндсэн функцүүдийг агуулдаг сан.

- **IsWow64Process**
  Үйдлийн систем 32 вит үү эсвэл 64 витийн альнаар ачааллаж байгааг тогтооход ашигладаг.
- **MapViewOfFile**
  Хөнөөлт програм MapViewOfFile функцийн WriteFile дахь файлын бүтцийг өөрчлөхөд ашигладаг.
- **LoadResource**
  PE файлын санах ойн ачааллын бүтэц. Хөнөөлт програм ихэнхдээ мэдээллийн мөр төрлийг өөрчлөх замаар хөнөөлтэй код агуулсан файлыг хавсаргадаг.
- **SetFileTime**
  Хөнөөлт програм ихэвчлэн энэ функцийг хөнөөлтэй код нуухад ашигладаг.

User32.dll сан нь хэрэглэгчийн интерфейстэй холбоотой буюу хэрэглэгчийн үйлдэлд хариу өгөх функцүүдийг агуулдаг.

- **AttachThreadInput**
  Keyloggers болон spyware хэрэглэдэг функц, гол зорилго түлхүүр үг цуглуулах болон тагнах зорилготой.
- **GetAsyncKeyState**
  Хөнөөлт програм ихэнхдээ keylogger функцэд хэрэглэгддэг аргуудыг ашигладаг.
- **GetDC**
  Ихэвчлэн spyware програмд ашиглагддаг функцүүдийг ашиглан дэлгэцийн зураг авах үүрэгтэй.
- **GetForegroundWindow**
  Keyloggers нь голдуу виндоусын хэрэглэгчийн аль товч дарагдсныг тогтоох үүрэгтэй.
- **GetKeyState**
  Keyloggers хэрэглэж компьютерын гарны түлхүүр үгний төлөвийг нарийн тогтоох ашигладаг

Ntdll.dll сан нь Виндоус үйлдлийн системийн кернелтэй харьцах интерфейс функцүүдийг агуулдаг. Ерөнхийдөө програмуудын хувьд *Ntdll.dll* санг шууд өөрөө импорт хийх буюу дууддаггүй, харин *Kernel32.dll* сангаар дамжуулж шууд бусаар ханддаг. Хэрэв ямар нэг програм энэ санг шууд дуудсан байвал тухайн програм ихэвчлэн түүнийг ашиглаж, хэвийн бус үйлдлүүд гүйцэтгэх зорилготой байдаг. Тухайлбал, үйлдлээ нуух, эсвэл процесуудыг удирдаж болно.

- **RtlWriteRegistryValue**
  kernel-дэх бүртгэлийн утгыг өөрчлөхөд ашигладаг
- **NtQueryDirectoryFile**
  Файлын директорыг мэдээллийг тогтоох. Rootkits нь голдуу дараалсан файл нуух үүрэгтэй.

Ws2_32.dll сангуудад аливаа програм компьютерын сүлжээтэй ажиллахад хэрэглэгддэг функцүүд байдаг бол *Wininet.dll* сангийн хувьд FTP, HTTP, болон NTP гэх мэт протоколуудтай ажиллах буюу сүлжээний дээд түвшний функцүүдийг агуулсан байдаг.

- **Connect**
  Энэ функц нь алсын зайнаас холболт хийхэд хэрэглэдэг. Хөнөөлт програм нь доод түвшний функц болох комманд болон сервер удирдлагагыг ихэвчлэн ашигладаг.
- **Recv**

Алсын зайнаас холбогдсон компьютераас өгөгдөл хүлээн авдаг. Хөнөөлт програм нь өгөгдөл хүлээн авахдаа алсын зайнаас комманд болон сервер удирдлагагыг ихэвчлэн ашигладаг.

- **Send**
  Алсын зайнаас холбогдсон компьютерлуу өгөгдөл илгээдэг. Хөнөөлт програм нь өгөгдөл илгээхдээ алсын зайнаас комманд болон сервер удирдлагагыг ихэвчлэн ашигладаг.
- **Bind**
  Портны дотоод хаяг болон холбогдсон хаягийн жагсаалтуудыг ашигладаг.

Статик анализын аргаар Win32 Malware gen хөнөөлт програм нь файл системд өөрчлөлт оруулж, хөнөөлт код агуулсан програмаа нууж сүлжээний портуудыг ашиглах чадвартай болохыг тодорхойлсон.

Win32 Malware gen хөнөөлтэй програмыг динамик анализын аргаар тодорхойлохын тулд Process monitor, Process explorer, WireShack програмын тусламжтай бүтэц, зохион байгуулалтыг тусгаарлагдсан хяналттай орчинд ажиллуулж системийн аль хэсэгт нөлөөлж байгааг илрүүлсэн. Дэлгэрэнгүйг хүснэгт 2-д үзүүлэв.

Хүснэгт 1.Системийн файлд өөрчлөлт оруулсан хэсгүүд.

Системийн файл	Malware gen
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.6028_x-ww_61e65202	X
C:\Documents and Settings\Administrator\Local Settings\Temp\	X
C:\Documents and Settings\Administrator\Application Data	X
C:\Windows\Prefetch\	X
Windows registry	X

Дээрх хүснэгтээс харахад Win32 Malware gen хөнөөлтэй програм систем файлын C:\Documents and Settings\Administrator\ApplicationData хэсэгт ScreenSaver.scr файлыг хуулж хөнөөлтэй ажиллагаа явуулдаг. Үүнээс гадна системийн регистрд хэрхэн нөлөөлж байгааг хүснэгт 2-д дэлгэрэнгүй үзүүлэв. Виндоус үйдлийн системд регистр нь чухал үүрэг гүйцэтгэдэг бөгөөд үүнд системийн талаарх бүх мэдээлэл хадгалагддаг. Виндоус үйдлийн системд тус тусын үүрэгтэй 6-н төрлийн дээд түвшний регистр байдаг [7]. Malware gen хөнөөлт програм нь Виндоус үйдлийн системийн регистрд хэрхэн нөлөөлж байгааг хүснэгт 2-т дэлгэрэнгүй үзүүлэв.

Хүснэгт 2. Регистрд өөрчлөлт оруулсан хэсгүүд.

Windows registry	Malware gen
HKLM\Software\Microsoft	X
HKLM\System\ControlSet001\Control\	X
HKLM\Hardware\	
HKLM\System\CurrentControlset\Services\	X
HKLM\Software\Microsoft\Cryptography\	X
HKLM\Software\Microsoft\Windows NT\CurrentVersion\	X
HKU\S-1-5-21-602162358-492894223-299502267-500\Software\Microsoft\Windows\CurrentVersion\Run	X
HKLM\SOFTWARE\Microsoft\DirectDraw\MostRecentApplication	X
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Extensions\	X
HKLM\SYSTEM\ControlSet001\Enum\Root\	X

Бидний шинжилгээ хийж буй програмын өөрчлөлт хийсэн HKLM регистр нь HKEY_LOCAL_MACHINE гэсэн үгийн товчлол бөгөөд энэ регистр нь компьютерт суулгасан програмуудын бүртгэл болон драйверуудын талаарх мэдээлэл хадгалдаг[8]. HKEY_USERS бүртгэл нь (HKU)HKEY_CURRENT_USER товчлол бөгөөд тухайн хэсэгт Виндоус үйдлийн системд байгаа бүх хэрэглэгчдийн үндсэн тохиргоо мэдээлэл хадгалагдсан байдаг[8].

HKLM болон HKU өөрчлөлт оруулснаар хостын C:\Documents and Settings\Administrator\ApplicationData хэсэгт хадгалагдаж байгаа Screensaver.scr хөнөөлт програмыг дуудаж ажиллуулах болон кодлогдсон хөнөөлтэй програмын кодын мөр төрлийг хөрвүүлэх зорилготой өөрчлөлт оруулсан байна. Сүлжээний хандалтын талаарх мэдээллийг WireShark програмаар цуглуулсан үр дүнг Хүснэгт 3-т харуулав.

Хүснэгт 3. Хостын сул портыг ашигласан траффик

Порт	Протокол	Процесс
1140	TCP	Windows\syswow64\vmnate.exe
1140	TCP	Windows\syswow64\vmnate.exe

Win32 Malware gen хөнөөлт програм нь сүлжээнд холбогдсон хостуудад халдваралж өөрийгөө олшруулж тодорхой заагдсан сайтуудыг дуудаж ачааллаж сүлжээнд ачааллал үүсгэдэг.

IV. ДҮГНЭЛТ

Win32 Malware gen хөнөөлт програмыг сонгон авч түүний ажиллагаа болон шинж чанарыг тусгаарлагдсан хяналттай орчинд статик болон динамик анализын аруудаар судалгаа хийсэн. Статик анализын аргаар програмыг системд ачаалахгүйгээр зөвхөн файлд дүн шинжилгээ хийсэн. Дүн шинжилгээгээр Win32 Malware gen програм нь хөнөөлтэй програмын бэктор гэсэн ангилалд багтаж байгааг тогтоосон. Үйдлийн системд хэрхэн хор хөнөөл учруулж байгааг динамик анализын аргаар виртуал орчинд хөнөөлтэй програмыг ачааллаж судалгааг явуулсан. Уг хөнөөлт програм нь системийн файлд ScreenSaverPro.scr файлыг хуулж бүртгэлийн HKLM, HKEY_USERS

регистрд өөрчлөлт оруулж, системд нууцлагдсан байдлаар ажиллаж, клиент програмтайгаа холбогдож хостод хүссэн бүх үйдлээ гүйцэтгэж байгааг тодорхойлсон.

АШИГЛАСАН МАТЕРИАЛ

[1]. www.symantec.com/connect/articles/malware-analysis-administrators
[2]. “HackerDefender Rootkit for the Masses” –Chris Gates. 2007
[3]. “Malware Challenge” jerome.segura@gmail.com
[4]. “Malware Analysis Challenge III” – Dean De Beer. 2007
[5]. “An Enviroment for Contorelled Worm Replication and Analysis” – Bill Arnold, David Chess, John Morar. 2008
[6]. “Reverse-Engineering Malware” – Alla Segal. 2006
[7]. http://en.wikipedia.org/wiki/Windows_Registry
[8]. http://kb.chemtable.com/ru/windows-registry-main-keys.htm#hkcu