Гарчиг

Зургийн жагсаалт

Хүснэгтийн жагсаалт

Товчилсон үгсийн жагсаалт

LAN Local Area Network

WAN Wide Area Network

VPN Virtual Private Network

SLA Service Level Agreement

MAN Metropolitan Area Network

GAN Global Area Network

HTTP Hypertext Transfer Protocol

IP Internet Protocol

ICMP Internet Control Message Protocol

PCAP (Packet Capture)

API Application Program Interface

NIC Network Interface Card

IDS Instrusion Detection System

NIDS Network-based Intersuion Detection System

BGP Border Gateway Protocol

UDP User Datagram Protocol

TCP Transmission Control Protocol

HDLC High-Level Data Link Control

DNS Domain Name System

WLAN Wireless Local Area Network

FTP File Transfer Protocol

SSH Secure Shell

SMTP Simple Mail Transfer Protocol

DHCP Dynamic Host Configuration Protocol

TFTP Trivial File Transfer Protocol

POP Post Office Protocol

NTP Network Time Protocol

SNMP Simple Network Management Protocol

LDAP Lightweight Directory Access Protocol

LDAPS Lightweight Directory Protocol over TLS/SSL

ARP Address Resolution Protocol

Бүлэг 1

Ерөнхий агуулга

1.1 Удиртгал

Компьютер техник технологи эрчимтэй хөгжихийн хэрээр мэдээллийн аюулгүй байдал болон системийн аюулгүй байдал гэдэг ойлоголт чухал асуудал болоод байна. Учир нь систем аюулгүй байсанаар гадны этгээд албан байгууллага, хувь хүн, засгийн газарын мэдээллийг хууль бусаар хулгайлах эрсдэлийг бууруулдаг. Системийн аюулгүй байдал гэдэг нь хэд хэдэн хүчин зүйлээс бүрдэх бөгөөд хорт програмыг систем дээр ачаалахгүй байх нь системийн аюулгүй байдлын нэгээхэн хэсэг мөн. Хорт програм гэдэг нь системийн мэдээллийг хэн нэгэн гадны этгээд үрүү зөвшөөрөлгүй нууцаар дамжуулж байдаг програм хангамжийг хэлнэ. Иймээс хорт програмыг илрүүлж системээс устгах нь нэн шаардлагатай асуудалуудын нэг юм.

1.2 Зорилго

Энэхүү төгсөлтийн ажлын гол зорилго бол систем дээр байгаа хорт програмыг илрүүлэх юм. Систем дээр хорт програм ажилласнаар тухайн системийн үнэт мэдээлэл болон системийн эмзэг байдал цаашлаад системд нэвтрэх хаалгыг нээж өгдөг. Хорт програмыг илрүүлнэ гэдэг нь тухайн програм хангамжийн ажиллагааг хянаж, зөвшөөрөгдөөгүй буюу аюултай үйл ажиллагааг явуулж байгаа эсэхийг тодорхойлох эсвэл тухайн програм хангамжийн бүрэн бүтэн байдал (integrity) -г шалгаж албан ёсны хувилбарт өөрчлөлт өрсөн эсэхийг илрүүлэх гэх мэт аргуудыг хэлнэ. Бүрэн бүтэн байдалд өөрчлөлт орсон гэдэг бол тухайн програм хангамжийн албан ёсны хувилбараас функц,

бүтэцийн хувьд өөрчлөгдсөн, өөр нэгэн халдагч этгээдийн зохиосон функцээр ажилладаг эсэхийг тодорхойлох юм. Компьютерийн бүх л төрлийн объектууд нь дахин давтагдашгүй тэмдэгт үүсгэх боломжтой бөгөөд үүнийг signature гэнэ. Иймд бүрэн бүтэн байдалыг шалгах хамгийн шалгарсан найдвартай арга бол MD5 алгоритмыг ашиглах явдал юм. Төгсөлтийн ажлын хүрээнд хийгдэж байгаа програм нь системийн файлуудын MD5 ыг тооцож өөрийн сантай харьцуулалт хийж тухайн програмын бүрэн бүтэн байдал алдагдсан эсэхийг илрүүлнэ.

Бүлэг 2

Malware гэж юу вэ?

Malware гэдэг нь Malicious Software үгийн товчлол юм. Malware гэж энгийн програм хангамж шиг ажиллагаатай боловч хууль бус, зөрчилтэй үйлдлийг хийдэг програм хангамжийг хэлнэ. Хууль бус зөрчилтэй үйлдэл гэдэг нь :

- Хэрэглэгчийн мэдээллийг цуглуулж өөр хост уруу дамжуулах
- Malware ажиллаж байгаа хост уруу нэвтрэх хаалгыг нээж өгөх (backdoor)
- Хэрэглэгчид хүсээгүй контентуудыг татуулах
- Хэрэглэгчийн компьютерийн хүчин чадлыг ашиглаж тооцоолол хийх

гэх мэт үйлдлүүд болно. Malware нь хийж байгаа үйлдэлээс хамаарч олон төрөлд хуваагддаг. Үүнд :

- Virus
- Trojan Horse
- Worm
- Spyware
- Backdoor

гэх мэт ангилагддаг. Malware ийг ангилах нь нэлээд төвөгтэй асуудал болдог. Учир нь шинээр гарч байгаа malware нь өмнөх хувилбарууд дээр тулгуурлан олон төрлийн malware ийн нэгтгэсэн хувилбар болж гарж ирдэг учир илрүүлж, ангилал хийхэд нэлээн төвөгтэй болдог. Malware нь хэрэглэгчийн компьютерт сууж хэрэглэгч тухайн

програмыг ачаалахад системд нэвтрэх эрх хэрэглэгчээс асуудаг. Ихэнх хэрэглэгчид malware мэдлэг хомс тул уг эрхийг олгодог. Ингэснээр тухайн Malware нь системийн файлд нэвтрэх, өөрчлөх, устгах бүрэн эрхтэй болдог байна. Ийм эрхтэй болсон malware нь төрлөөсөө хамаарч тухайн компьютерийн мэдээллийг устгаж эсвэл хуулж эхэлдэг. Malware -ээс сэргийлэх хамгийн үр дүнтэй аргуудын нэг бол вирусны эсрэг програм хангамжийг ашиглах юм. Аливаа нэгэн компаниас албан ёсоор гаргасан програм хангамж нь нууцаар хэрэглэгчийн хувийн мэдээлэлд халдаж байвал уг програм хангамж нь ч malware -т тооцогдох юм. Жишээлбэл Sony компанийн гаргасан Sony Rootkit юм. Үйлдвэрлэлээс гарахдаа өөр дээрээ trojan агуулж байдаг бөгөөд уг trojan нь хэрэглэгчийг хууль бус хуулбарлалт хийхээс сэргийлэхээс гадна зарим нэг эмзэг байдлыг нээж, хэрэглэгчийн мэдээллийг хуулж байдаг.

Malware нь анх гарахдаа туршилт болон шоглоом хийх зорилготой гарсан боловч өнөө үед хувь хүн, албан байгууллагын мэдээллүүдийг хулгайлах зорилготойгоор засгийн газар болон "Black Hat Hacker"гэх тодорхойлолттой бүлэг хүмүүс ашиглаж байна. Malware нь хөгжүүлэгчээс хамааран хамгаалалтын зориулалттай байдаг боловч ихэвчлэн хувь хүний мэдээллийг хулгайлах зорилготой байдаг.

Зураг 2.1

2.1 Virus

Вирус бол Malware ийн нэг төрөл юм. Вирусыг ажиллуулахад компьютерийн бусад програм хангамжийг өөрчилж өөрийн кодыг тухайн програм хангамжид хуулах замаар өөрийгөө хуулбарлаж байдаг. Ингээд вируст өртсөн буюу өвчилсөн програм хангамж нь компьютерийн мэдээлэл, хард дискны boot секторыг хуулбарлаж авах чадалтай байдаг. Вирус нь ажиллахын тулд хост програм буюу уг вирусыг тээж явах програм хэрэгтэй. Ингэснээр тухайн програм ажиллахад вирус идэвхэжнэ. Идэвхэжсэн вирус нь вирусны эсрэг програм хангамжийг зогсоох, өөрийгөө хуулбарлаж өөр нэгэн програм хангамжид суулгах, тухайн компьютерийн хамгаалалтыг унтраах чадалтай болдог. Вирус зохиогчид нь ихэвчлэн Windows үйлдлийн системийг онилдог учир нь компьютер хэрэглэгчдийн дийлэнх нь Windows үйлдлийн системийг хэрэглэж байдаг. Зохиогчид нь антивирусны програмд илрүүлэхгүйн тулд вирус гэж танихад нилээн төвөгтэй болгодог. Вирусны хор уршгаар жилд дунджаар тэрбум ам.долларыг системийн гэмтэл, мэдээллийн алдагдал, эвдэгдсэн мэдээлэл гэх мэт асуудлыг шийдэхэд зарцуулдаг байна

2.2 Worm

Worm бол вирустэй ижил ажиллагаатай боловч хост програм шаардлагагүй дангаараа ажиллах чадвартай мөн тархах аргаар ялгаатай байдаг. Вирус нь системийн файл, програмд халддаг бол worm нь сүлжээнд холбогдсон компьютер бүр лүү халддаг. Worm нь USB, DVD, External HDD гэх мэт зөөврийн хэрэгслүүдээр дамжин халдахаас гадна E-Mail -ээр дамжих чадвартай байдаг. Worm агуулж байгаа компьютер сүлжээнд нэвтрэхэд уг Worm өөрийгөө хуулбарлан сүлжээгээр цацаж эхэлдэг. Ингэснээр ямар нэгэн хамгаалалтгүй тухайн сүлжээнд холбогдсон компьютер нь шууд worm -д өртдөг.

2.3 Trojan horse

Trojan Horse нь Өөрийн гол зорилгыг нууж хэрэглэгч харахад хэвийн харагддаг програм хангамж юм. Өөрөөр хэлбэл тухайн нэг програм хангамж нь анх бүтээгдэхдээ хэрэглэгчийн мэдээллийг хуулж өөр нэг хост уруу дамжуулах зорилготой боловч үүнийгээ нууж энгийн үйлдэл хийдэг мэт харагддаг програм хангамжийг Trojan Horse гэнэ. Trojan Horse гэж нэрлэсэний учир нь эртний Грекийн түүхэнд Troy хотыг эзэлж

авахдаа модон моринд цэргүүдээ оруулж эзэлсэн байдагтай ижил учир Трояан Хорс буюу Trojan Horse гэж нэрлэсэн. Зарим Trojan Horse -ууд нь интернет хөтөчийн эмзэмг байдлыг ашиглан сүлжээний урсгалыг нууж чаддагаас гадна тухайн өвчилсөн компьютерийн IP хаягыг ашиглан хууль бус интернет орчны үйлдлүүдийг хийж чаддаг. Trojan Horse -ийг ашиглан халдагч этгээд нь доорх үйлдлүүдийг бүрэн хийж чаддаг байна.

- Мэдээллийг устгах
- Мэдээллийн урсгалыг зогсоох
- Мэдээллийг өөрчилөх
- Мэдээллийг хуулбарлах
- Сүлжээ болон компьютерийн үйл ажиллагааг доголдуулах

Trojan Horse нь дараах байдлаар хэрэглэгчийн компьютерд нөлөөлдөг.

- Backdoor
- Exploit
- Rootkit
- Trojan-Banker

  Хэрэглэгчийн нэвтэрч байгаа онлайн банкны мэдээлэлийг хулгайлах
- Trojan-DDoS

  Хэрэглэгчийн компьютерийг ашиглан аливаа нэг сервер уруу DDoS халдлага үйлдэх
- Trojan-Downloader

  Шинэ төрлийн Malware,Adware үүдийг хэргэлэгчийн компьютерд суулгах
- Trojan-Dropper

  Халдагч этгээдүүд энэ програмыг ашигладаг ба энэ нь malware-ийг антивирус илрүүлэхээс зайлсхийхэд тусалдаг.
- Trojan-FakeAV

  Хуурамч антивирусны програм болж ажилладаг бөгөөд таны компьютерт байгаа байхгүйгээс үл хамааран хэд хэдэн malware илрүүлж төлбөр нэхдэг.

- Trojan-GameThief

  Онлайн тоглоом тоглогчдын мэдээллийг хулгайлдаг

- Trojan-IM

  Yahoo, ICQ, MSN Messenger, AOL Instant Messenger, Skype гэх мэт онлайн мессежний програмаас хэрэглэгчийн нэр болон нууц үгийг хулгайлдаг

- Trojan-Ransom

  Энэ төрлийн trojan нь хэрэглэгчийн компьютерийн тодорхой хэсэг мэдээллийг өөрчилж тухайн үйлдлийн систем уг мэдээллийг хэрэглэх, унших боломжгүй болгодог. Энэ төрлийн Trojan нь сүүлийн үед нилээн дэлгэрэнгүй гарж байгаагын жишээ бол Ransomware, Petya-Ransomware, QuickRabbit гэх мэт trojan ууд юм. Эдгээр нь өөр өөр үйлдлийг гүйцэтгэдэг боловч ерөнхий суур нь хард дискны boot секторыг устгаж өөрийн бэлдсэн boot-ээр сольдог. Ингэснээр хэрэглэгч өөрийн системд нэвтрэх боломжгүй болдог байна.

- Trojan-SMS

  Энэ төрлийн Trojan нь таны гар утасыг ашиглан тусгай дугаар уруу мессеж илгээдэг зөвхөн хохирол учруулах зорилготой.

- Trojan-Spy

  Хэрэглэгчийн үйлдлийн системд хийж байгаа бүх л үйлдлийг хянах цуглуулах дамжуулж байдаг trojan.

- Trojan-Mailfinder

  Хэрэглэгчийн үйлдлийн системд бүртгэгдсэн кеешлэгдсэн бүх цахим шуудангын хаягыг цуглуулдаг.

2.4 Spyware

Хэрэглэгчид мэдэгдэхгүйгээр хэрэглэгчийн интернетийн түүх, хэрэглэгчийн хувийн мэдээлэл болох нэр нууц үг гэх мэт, хэрэглэгчийн байршил, хэрэглэгчийн үйлдлийн систем интернет хөтөчийн хувилбар гэх мэт мэдээллүүдийг цуглуулж халдагч этгээд уруу дамжуулж байдаг програм хангамжийг хэлнэ. Уг програм хангамж нь хэрэглэгчээс ихэвчлэн газар зүйн байршил, тусгай эрх буюу administrator permission шаарддаг.

2.5 Backdoor

Backdoor нь системд арын хаалга буюу хэрэглэгчид мэдэгдэхгүйгээр нэг портыг нээж өгдөг malware юм. Ингэснээр халдагч этгээд тухайн компьютер уруу алсаас хандах эрхтэй болохоос гадна тухайн компьютерийн админ эрхээр бүх үйлдлийг хийж чадахуйц болно. Backdoor нь хост компьютерийн user defined порт дундаас үүсгэгчийн(malware ийг бичсэн этгээд) зааж өгсөн портыг нээж, тухайн портыг сонсож байдаг. Ингэснээр халдагч этгээд хүссэн үедээ тухайн системийн нээлттэй портоор нэвтэрч орж чадах юм. Хамгийн энгийн жишээ бол linux үйлдлийн систем дээр файл дамжуулах үйлчилгээний 2.3.4 дээр илэрсэн backdoor юм. Vsftp 2.3.4 хувилбар ашиглаж байгаа сервер уруу 21 портоор тусгай бэлдсэн хортой кодыг дамжуулахад Backdoor нээгдэж халдагч этгээдэд системд алсын хандалт буюу ssh -ээр нэвтрэх бүрэн эрхийг олгодог.

```
40444/r--r--r--   4096    dir   1970-01-01 01:26:16 -0500  vendor

meterpreter > cd etc
meterpreter > ls

Listing: /system/etc
====================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
100444/r--r--r--  16117   fil   1970-03-20 18:32:24 -0500  CHANGELOG-CM.txt
100444/r--r--r--  164587  fil   1970-03-20 18:32:42 -0500  CHANGES.txt
100444/r--r--r--  238954  fil   1970-03-20 18:32:41 -0500  NOTICE.html.gz
40444/r--r--r--   4096    dir   1970-01-01 01:26:04 -0500  acdbdata
100444/r--r--r--  257630  fil   1970-03-20 18:32:31 -0500  apns-conf.xml
100444/r--r--r--  5491    fil   2008-08-01 08:00:00 -0400  audio_effects.conf
100444/r--r--r--  3314    fil   1970-03-20 18:32:29 -0500  audio_platform_info.x
ml
100444/r--r--r--  5805    fil   1970-03-20 18:32:27 -0500  audio_policy.conf
```

Зураг 2.2: Backdoor хийсэн байдал

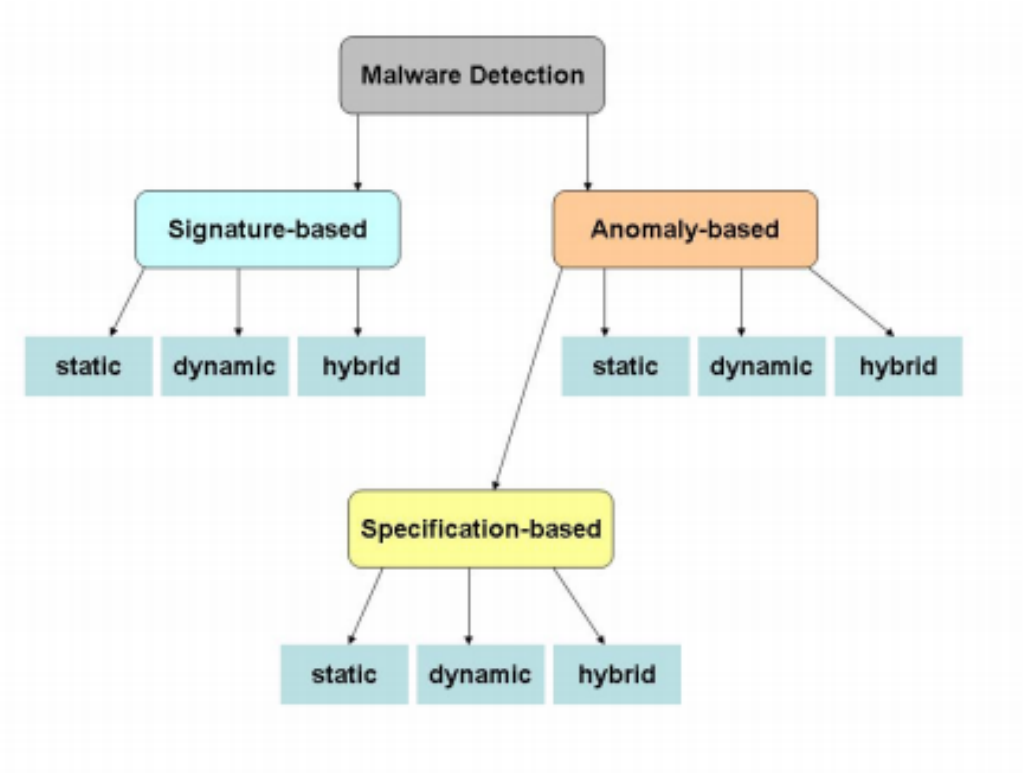
Бүлэг 3

Malware илрүүлэлт

3.1 Malware ийг хэрхэн илрүүлэх вэ?

Malware бол хэрэглэгчийн мэдээллийг цуглуулж алсад байгаа malicious host уруу цугларсан мэдээллийг дамжуулдаг програм хангамж юм. Халдагч этгээд нь уг мэдээллийг ашиглан хэрэглэгчийг сүрдүүлэх, доромжилох, мөнгө нэхэх, устгах, хэрэглэгчийн өмнөөс бусадтай харьцах гэх мэт хор уршигтай учир Malware ийг илрүүлэх нь нэн шаардлагатай. Malware илрүүлэлт нь маш том хүрээний асуудал юм. Malware -г илрүүлэхдээ ерөнхий Anomaly based detection буюу аномалид суурилсан арга болон Signature based detection буюу бүрэн бүтэн байдалд суурилсан гэж хоёр аргыг ашигладаг. Аномалид суурилсан арга нь тухайн програм хангамжийг хортой эсэхийг шийдэхдээ програм хангамжийн энгийн үйл ажиллагааны мэдээлэл дээр суурилан илрүүлдэг. Тусгай зориулалтын аномали илрүүлэлтийг Specification based detection гэж нэрлэж болдог. Энэ илрүүлэлт нь шалгагдаж байгаа програм хангамжид энгийн үйл ажиллагааны дүрэм тавьж өгснөөр хортой эсэхийг илрүүлэхэд түлхэц болж өгдөг. Уг дүрмийг зөрчиж байгаа програм хангамжийг anomalous гэх бөгөөд ихэнх тохиолдолд эдгээр програм хангамж нь хортой байдаг. Бүрэн бүтэн байдалд суурилсан илрүүлэлтийн арга нь хортой гэдэг нь тогтоогдсон програм хангамжийн характиристиктэй харьцуулж шалгаж байгаа програм хангамжийн хортой эсэхийг шийддэг. Зураг 3.1 -т үзүүлснээр Malware илрүүлэх арга нь гурван төрөлтэй төрөл бүр өөрсдийн статик, динамик болон хосолсон замаар илрүүлдэг. Статик илрүүлэлт нь шалгагдаж байгаа програм эсвэл процессийн синтакс эсвэл бүтцийн шинж чанарыг ашигладаг. Энгийнээр бол статик нь malware -ийг ажиллуулахаас өмнө илрүүлдэг бол динамик нь malware -ийг ажиллаж байх явцад

эсвэл ажиллаж дууссаны дараа системийн санах ойн аль хэсэгт хандаж байгаа болон хандсан мэдээллүүдийг цуглуулах замаар илрүүлдэг. Динамик илрүүлэлтийн давуу тал бол тухайн програм хангамжийг хортой эсэхийг илүү баталгаатай илрүүлдэг бөгөөд хортой үйлдэлд нэвтрэх эрхтэй болж чаддаг. Мөн энэ хоёрыг хослуулсан арга байдаг. Malware илрүүлэгчидийн арга сайжирах тусам Malware бүтээгчид уг илрүүлэгчийг давах, хуурах арга илүү нарийн болж ирдэг. Түгээмэл ашигладаг Malware илрүүлэгчээс нуудаг арга бол polymorphism, metamorphism, recording юм. Жишээлбэл хортой код нь өөрийгөө нууцалж энгийн болж хувирч програм ажиллаж эхлэхэд нууцалсан кодны хэсгийг буцаан decrypt(тайлах) хийж чаддаг. Recording хийнэ гэдэг нь Malware бүтээгчид тусгай програмын үсрэлтийн функцыг ашиглаж хортой кодыг хэсэгчилэн дуудах аргыг хэлнэ. Эдгээр аргууд нь статик аргад баригдахгүй боловч динамик аргыг давж чадахгүй. Polymorphism бол хортой кодыг хэсгийг нууцалж энгийн функц болгон харагдуулдаг.



Зураг 3.1: Malware илрүүлэх аргын задаргаа

3.2 Anomaly-д суурилсан илрүүлэлт

Anomaly -д суурилсан илрүүлэлт нь training-phase(суралцах үе) болон detection-phase(илрүүлэлтийн үе) гэж хоёр хуваагддаг. Training-phase -д шалгаж байгаа програмын хэвийн шинж чанарыг суралцана. Энэ үед илрүүлэгч нь хостын хэвийн шинж чанар болон шалгагдаж байгаа програмын шинж чанарыг сурах буюу таньж байдагаас гадна дээрх хоёрыг зэрэг сурч байдаг. Аномалид тулгуурласан илрүүлэлтийн гол давуу тал бол Zero Day халдлагыг илрүүлэх чадалтай байдаг. Zero day халдлага бол програм хөгжүүлэгч тухайн нэг прогорам гаргасан гэж үзвэл. Хөгжүүлэгч өөрийн програм дахь эмзэг байдлыг мэдэж засахаас өмнө хийгдэх халдлагыг хэлнэ. Тухайн хөгжүүлэгч эмзэг байдлаа мэдэн patch хийсэн үед Zero Day халдлага нь дуусдаг байна. Аномалид суурилсан илрүүлэлтийн арга нь тухайн агшинд шалгагдаж байгаа програмыг хэвийн үетэй нь харьцуулж хортой эсэхийг шийддэг арга юм. Аномали арга нь статик, динамик хосолсон гэж гурван төрөлд хуваагддаг.

3.2.1 Dynamic Anamoly-д суурилсан илрүүлэлт

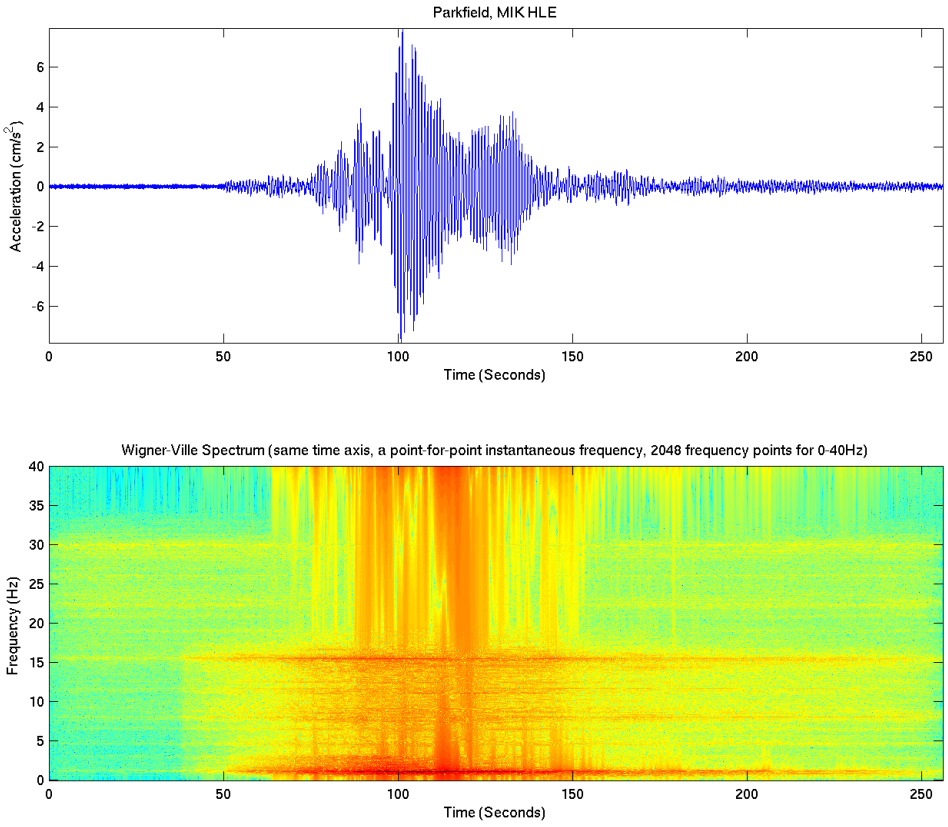
Динамик аномалид суурилсан илрүүлэлт нь програм ажиллаж байх үеийн мэдээлэл дээр суурилж хортой кодыг илрүүлэх арга юм. Илрүүлэлтийн үед training phase(суралцах үе)-ээс олж авсан мэдээллийн дагуу хоргүй эсэхийг шалгаж байгаа програм хангамжийг хянаж байдаг. Нэг ёсондоо тухайн програм хангамжийн шалгалтын явцад үзүүлсэн хариу үйлдэлийг бүртгэж байдаг байна. Жишээ болгон динамик аргуудыг ашигласан илрүүлэх хэрэгслүүдийг танилцуулъя

3.2.1.1 PAYL

Wang болон Stolfo нар нь системийн сервис бүрт зориулагдсан payload -ыг тооцоолдог PAYL хэрэгслийг бүтээсэн. Уг хэрэгсэл нь байтын давтамжын тархалтыг үүсгэдэг бөгөөд энэ нь хостын сервис бүрт тохируулсан centroid model(төв загвар) -г хөгжүүлэх боломжийг олгодог. Илрүүлэгч нь ирсэн payload -г төв загвартай харьцуулж Mahalanobis ийн уртыг хэмжидэг. Зураг 3.2-т Mahalanobis -н томъёог харуулсан. Уг томъёо нь зөвхөн векторын утгыг авахаар зогсохгүй вариац болон ковариацын хамгийн ойролцоо статистик утгуудыг авдаг. Хэрвээ ирсэн payload нь төв загвараас Mahalanobis -н урт хэтэрхий зөрүүтэй байвал уг payload -г хортой гэж үздэг. Энэ аргыг 1999 онд

$$D_M(\vec{x}) = \sqrt{(\vec{x} - \vec{\mu})^T S^{-1} (\vec{x} - \vec{\mu})}.$$

Зураг 3.2: Mahalanobis -н томъёо



Зураг 3.3: Байтын давтамж

MIT Lincoln Labs -н мэдээлэл дээр суурилан гаргаж ирсэн. Энэ мэдээлэл нь гурван долоо хоногын сургалтын мэдээлэл болон хоёр долоо хоногын туршилтын үр дүнг агуулсан байна. Нийт 201 удаагын халдлага хийснээс 97 халдлагыг Wang болон Stolfo нарын арга илрүүлж чадсан. Дунджаар уг арга нь 60% -тай илрүүлж байсан. Wang, Stolfo нар нь уг аргаа Columbia University Computer Science -ийн дата төвд хэрэгжүүлж үзсэн

бөгөөд Lincoln Lab -аас ялгаатай нь Columbia University Computer Science -н дата төвд бодит системд туршиж үзсэн юм. Columbia University -ийн нууцлалын дүрмийн дагуу уг мэдээлэлийг устгалд оруулсан байдаг учираас өөр судлаач, шинжээчид энэ мэдээллийг ашиглах боломжгүй болсон байна. Мөн PAYL нь CUCS -ийн дата төвд халдсан Code Red II халдлагын буфферийн халилтыг илрүүлж чадсан байна.

3.2.1.2 Data Mining аргаар халдлагыг илрүүлэх нь

Lee болон Stolfo нар нь халдлага илрүүлэх системд Data Mining болон дүрэм тавих аргыг нэмсэн. Дүрэм нь тухайн хостын аюулгүй ажиллагааг хангах зорилготой юм. Жишээлбэл ямарваа нэгэн програм хангамж нь ажиллаж байх хугацаандаа системийн тодорхойлогдсон хэсэг функцыг дуудахгүй, дуудсан функцээ тодорхой хугацаанд л ашиглах ёстой гэх мэт. Эдгээр дүрмүүд нь эргээд хостын хэвийн ажиллагааны зарчим болж өгдөг. Base илрүүлэлтийн агент нь тухайн системийн зарим хэсгийн нарийвчилсан загвар гаргадаг. Meta илрүүлэлтийн агент нь хэд хэдэн Base илрүүлэлтийн агентын мэдээллийг ашиглан халдлагын шинжийг гаргаж ирдэг. Үүнээс гарсан мэдээлэл нь аудит болдог бөгөөд илрүүлэгч нь тухайн аудит дээр тодорхойлсон дүрмийг хэрэгжүүлж хянадаг.

3.2.1.3 Компьютерийн Forensic аргыг ашиглан нууцлалгүй програм хангамжийг шинжих нь

Boldt болон Carlson нь програм хангамжийн нууцлалын тухай ойлголтыг нэвтрүүлсэн. Adware болон Spyware нь програм хангамж нь нууцлалгүй програм хангамжийн хамгийн том хоёр төрөл юм. Ихэнхи тохиолдолд нууцлалгүй програм хангамж нь файл дамжуулдаг програм болж ажилладаг. Boldt Carlson нар нь Forensic Tool Kit(үүнээс хойш FKT) ашиглаж нууцлалгүй програм хангамжийг илрүүлдэг. Хамгийн энгийн арга бол цэвэр систем буюу системийн бүтцэд нууцлалгүй програм хангамжийг нэвтрүүлэхгүй байх юм. Цэвэр системийн snapshot бол системийн үндсэн суурь юм. Snapshot нь хостын файл системийг илэрхийлдэг. Системийн үндсэн суурийг тогтоосний дараа хост дээр нууцлалгүй програм хангамжийг ажиллуулах зарим үйлдлүүд хийгддэг. Ad-Adware нь нууцлалгүй програмыг устгах хамгийн түгээмэл хэрэгсэл байсан учир хөгжүүлэгчид уг хэрэгслийг статик анализ болон forensic аргуудад ашиглаж эхэлсэн.

3.2.1.4 Системийн дуудалтын богино дараалал

Hofmeyr хорт програмыг илрүүлэхдээ системийн дуудалтын дарааллыг хянаж илрүүлэх аргыг танилцуулсан. Энэ арга нь системийн сервисийн энгийн(Энгийн гэдэг нь энэ тохиолдолд системийн дуудалтын богино дараалал юм.) шинж чанарыг үзүүлсэн профайл(дүр зураг) гаргана. Үүний дараа тухайн програм хангамж системийн дуудалтыг хэр ойрхон давтамжтай дуугдаж байгааг тооцохоос гадна дуудагдах бүрт дамжиж байгаа параметрүүдийн давтамжийг тооцдог. Энэ процесс нь аномали эсэхээс хамааран босго тавьж өгөх шаардлагатай байдаг. Энэ аргыг ашиглан Hofmeyr нь UNIX үйлдлийн системийн хэд хэдэн exploit болох sendmail, lpr, ftpd -ийн халдлагуудыг илрүүлсэн байна.

3.2.1.5 Процессыг задлах систем дуудалт

Sato нь системийн функц дуудалтын давтамж дээр суурилсан өөр нэгэн илрүүлэх аргыг гаргаж ирсэн. Процесс профайл нь системийн дуудалтын дугаарлалтаас бүрддэг. Процессийн суурь профайл нь систем дуудалтын давтамжаар эрэмбэлэгдсэн системийн функц дуудалттай байдаг. SUID нь системийн background -д ажиллаж байгаа програмын систем дуудалтын дугаарлалтыг бүртгэж байдаг. Процессийн профайл үүсгэгдсэний дараа шалгагдаж байгаа програмын ажиллах хугацааны мэдээлэл тухайн процессийн профайлтай харьцуулагдан зөрүүг тооцоолдог. Нэмэлт тулгах алгоритм болох DP тулгалт нь уг зөрүү утгыг өөртөө авдаг. DP -ийн утга нь системд зөвшөөрөгдсөн системийн дуудалтын тоотой харьцуулагдаж хортой эсэхийг тодорхойлоход ашиглагддаг. Хэрвээ процессийн систем дуудалт профайл хоёрын зөрүү системд бүртгэгдсэн нийт систем дуудалтын 1/4 ээс бага байвал хэвийн төлөвтэй гэж үзнэ. Хэрвээ зөрүү нь 1/4 ээс их 1/2 оос бага бол аюултай төлөвтэй гэж үздэг. Хэрвээ 1/2 оос их бол илэрсэн гэж үзнэ. Дээр дурьдсанаар систем дуудалтыг давтамжаар нь эрэмбэлдэг бол эрэмбэлэхдээ хоёр аргаар эрэмбэлдэг байна. Систем дуудалт бүрт өөрийнх нь бодит дуудалтын дугаараар давтамжийг үүсгэх эсвэл систем дуудалт бүрт санамаргүй тоон утгыг ашиглах гэсэн хоёр арга байдаг. Уг аргаар гаргасан хэвийн ажиллагааны шинж чанар нь хамгийн оновчтой байдаг бөгөөд энэ аргыг DP matching -тай хослуулан хэрэглэсэнээр RLOGIN буюу алсаас нэвтрэх, порт скан халдлагуудыг амжилттай илрүүлдэг байна.

3.2.1.6 Аудитын загварын уртад суурилах нь

Аудит хийгдсэн процессийн эвент нь pattern буюу хэсэгчилсэн хэлбэрүүдээс бүрдэг. Уг хэлбэр нь хамгийн багадаа хоёр удаа дуудагдаж хоёр эвенттэй байх ёстой. Хамгийн их pattern нь өөр нэгэн pattern -н үргэлжлэл биш байх бөгөөд бусад pattern -г бодвол харьцангуй их давтамжтайгаар ашиглагдсан байдаг. Алгоритм нь эхлэлээс төгсгөл хүртэл дараалалд оруулж хэрвээ шалгагдаж байгаа процесс нь илэрсэн процесстой цөөн тооны давхцалтай байвал тухайн процесс нь халдлага байх өндөр магадлалтай болно. Wepsi энэ аргыг FTPD процесс дээр туршисан. Мөн Hofmeyr -ийн аргатай харьцуулсан туршилт хийсэн бөгөөд үүнийг туршихдаа тодорхой заагдсан урттай pattern ашигласан. FTPD процессоос нийт 65 давтагдаагүй, хоргүй дарааллуудыг хүлээн авсан. Тодорхойлогдсон урттай pattern -н 17% нь FTPD ийн хоргүй дарааллудтай таарч байсан бол 72% нь хувьсах урттай pattern -тай таарч байсан юм. Үүнээс үзвэл хувьсах урттай pattern нь тодорхойлсон урттай pattern ашигласанаас илүү үр дүнтэй нь харагдаж байна.

3.2.2 Статик аномалид суурилсан илрүүлэлт

Статик аномалид суурилсан илрүүлэлт нь шалгагдаж байгаа програмын файл бүтцийг ашиглан хортой кодыг илрүүлдэг. Статик аргын гол давуу тал бол тухайн програм хангамжийг системд ажиллуулахгүйгээр хортой эсэхийг илрүүлж болдогт оршидог.

Fileprint Анализ

Уг арга нь файлын өргөтгөлөөс хамаарч файлын шалгалтыг хийдэг юм. Хөгжүүлэгчидийн үзэж байгаагаар хоргүй файл нь өргөтгөлөөсөө хамаарч тааварлаж болохуйц байтуудын бүтэцтэй байдаг. Өөрөөр хэлбэл хоргүй pdf файл нь exe, doc өргөтгөлтэй өөр байтын бүтэцтэй гэсэн үг юм. Training-phase -д модел эсвэл моделуудын цуглуулгаас хэд хэдэн төрлийн файлын байт бүтцийн характиристикыг олж авдаг ба шалгалтын явцад өгөгдсөн моделоос хэтэрхий зөрүүтэй файлыг сэжигтэй гэж үзэн дараагийн шатны malware илрүүлэх механизм уруу шилждэг. Уг аргыг ашиглан malware оруулсан PDF файлыг шалгаж туршихад 72.1-94.5% -тай илрүүлж байсан бол COTS AV нь 0 үзүүлэлттэй байсан байна. Гэхдээ туршилтын явцад PDF файл дотор malware -ийг хийхдээ зөвхөн header эсвэл tail хэсэгт хийж өгсөн.

3.3 Specification-based Detection

Нарийвчилсан илрүүлэлт нь аномалид суурилсан илрүүлэлтийн нэг хэлбэр бөгөөд ихэнхи аномалид суурилсан илрүүлэлттэй холбоотой гардаг түгээмэл хуурамч илрүүлэлтийг нарийвчилдаг арга юм. Програм эсвэл системийн ажиллагааг тооцоолохын оронд нарийвчилсан илрүүлэлт нь тухайн програм эсвэл системийн шаардлагууд буюу эрхүүдийг тооцоолдог. Нарийвчилсан илрүүлэлтийн хувьд training-phase нь хамгаалах гэж байгаа систем эсвэл шалгах гэж байгаа програмын аюулгүй ажиллагааны загварыг гаргаж ирдэг. Нарийвчилсан илрүүлэлтийн хязгаарлагдмал байдал нь системийн аюулгүй ажиллагааны дүрэмийг бүхэлд нарийн тодорхой, оновчтой гаргахад хүндтрэлтэйд оршидог.

3.4 Dynamic Specification-based Detection

Дээр хэлсэнчилэн динамик нарийвчилсан арга нь ч мөн адил програм ажиллаж байх хугацаанд хортой эсэхийг илрүүлдэг.

Програмын аюулгүй байдлын аюултай түвшинг хянах

Хэрэгжүүлэгч нь системд зориулсан нууцлалын бодлогыг тодорхойлж өгдөг. Энэ нь аудитын механизмаар дамжидаг эвентийг ажиллуулах дараалал юм. Хөгжүүлэгчид нь програмын сонхрончлолын алдааг илрүүлдэг параллель орчин үүсгэж Distribution Program Execution Monitor буюу DPEM аргыг нэвтрүүлсэн. Уг аргыг ашиглан UNIX үйлдлийн системийн програмд зориулсан 15 төрлийн аюулгүй байдлын бодлогыг гаргасан. Эдгээр бодлогуудын нэг нь RDIST програмд зориулагдсан бөгөөд DPEM нь RDIST програм уруу халдаж байгаа зөрчилтэй үйлдэл болох халдлагыг илрүүлж байсан байна. Халдлага нь халдага хийж эхэлснээс 0.6 секундын дараа илэрсэн бол passwd болон vi програмууд дээр ч мөн адил хугацааны хоцролтойгоор халдлагыг илрүүлсэн байна. sendmail болон binmail дээр хийгдсэн халдлага нь DPEM ээр 0.1 секундэд илэрсэн байна.

Динамик өгөгдлийн урсгал ашиглан аппликейшныг хамгаалах нь

DIFA буюу Dynamic Information Flow Analysis нь Java програмуудад зориулагдан гарсан хэрэгсэл юм. Уг хэрэгсэл нь аппликейшны байткодын ангилалыг ашиглаж аппликейшни ажиллаж байх явцад функцуудыг хянах боломжтой хэрэгсэл юм. Ингэснээр аппликейшны функц дуудагдах бүрт дамжигдах өгөгдлийн урсгалыг барьж авч танигдсан

буюу системд мэдэгдэж байгаа өгөгдлийн урсгалтай харьцуулалт хийх боломжтой болох юм. Жишээлбэл аюулгүй байдлын бодлогоор тодорхойлсон хандах ёсгүй директор байгаа гэж үзвэл. Хортой аппликейшн нь уг директорын файлыг хуулбарлах үйлдэл хийхэд (SEND() function) DIFA нь илрүүлж чадах юм.

ACT Attachment Chain Tracing

Уг аргын гол зорилго бол электрон шуудангаар цацагдсан malware ээс сэргийлэх юм. ACT -ын арга нь шалгарсан тархалт судлалын онолын загварыг ашигласан. Тархалтын онолоор холболт нь A болон B хостын хооронд байдаг. Хэрвээ A хост B уруу электрон шуудан явуулсан гэж үзвэл, хост нь A node -г явуулна. I болох хавсаргалттай майл нь эхний давхаргад байх ёстой боловч хэрвээ A node нь Z node -н майл хаягыг агуулж байвал Z node нь эхний давхаргад ордог. Тархалтын онолоор хэрвээ

3.5 Signature -д суурилсан илрүүлэлт

Компьютерийн объект бүрт өөрийн гэсэн дахин давтагдашгүй тэмдэг буюу гарын үсгийг гаргах боломжтой байдаг үүнээс цааш Signature гэж нэрлэнэ. Signature -ийг гаргахдаа MD5 буюу Message Digest 5 алгоритмыг ашигладаг. Уг алгоритм нь өгөгдсөн тэмдэгт мөр, файл, програм гээд бүхий л төрлийн объектоос 128 битий урттай хээш буюу hash гаргаж ирдэг. Hash нь тухайн объектийн таних түлхүүр болж өгдөгөөс гадна уг hash -г тайлах хугацаа нь асар удаан байдагаараа давуу талтай юм. Жишээлбэл 42 ASCII тэмдэгтийн hash бол 0cca9b3eeae7b8747eaf61f8d282156d юм. Хэрвээ уг hash ийг тайлвал ойролцоогоор секундэнд тербум hash унших чадалтай тербум компьютер нийлж 170 тербум жилийг зарцуулах юм. Учир нь MD5

Номзүй

[1] Computer Networking : Principles, Protocols and Practice, Release 0.25

[2] Pcap Function https://en.wikipedia.org/wiki/Pcap

[3] tcpdump https://en.wikipedia.org/wiki/Tcpdump

[4] Programming with pcap http://www.tcpdump.org/pcap.html

[5] Wireshark Network Analysis: the Official Wireshark Certified Network Analyst Study Guide (2nd Edition)

[6] Snort IDS and IPS Toolkit (Jay Beale's Open Source Security)

[7] NetFlow https://en.wikipedia.org/wiki/NetFlow

[8] Optimizing Bandwidth

[9] Principles of Broadband Switching and Networking

[10] Capsa (software) https://en.wikipedia.org/wiki/Capsa_(software)

[11] Analysis of Computer Networks: Edition 2

[12] Kismet Wireless https://www.kismetwireless.net/

[13] Nmap: the Network Mapper - Free Security Scanner https://nmap.org/

[14] Scapy https://en.wikipedia.org/wiki/Scapy