Дотоод сүлжээгээр дамжиж буй өгөгдлөөс хөнөөлт нэрвэгдэх хаягийг илрүүлэх нь

Д.Бямбадорж, С.Байгалтөгс
Улаанбаатарын Их Сургууль, Физик электроникийн тэнхим
ШУТИС, Бизнесийн удирдлага, Хүмүүнлэгийн сургууль
Улаанбаатар хот, Монгол улс
pheelectro2013@gmail.com, baigaltugs@must.edu.mn

Хураангуй— Мэдээлэл технологийн салбар хурдацтай хөгжихийн хирээр мэдээллийн аюулгүй байдлыг хангах нь нэн тэргүүний асуудал болоод байна. Иймд мэдээлэлийг дамжуулж байгаа компьютерийн сүлжээний хамгаалалт, хяналт зайлшгүй шаардлагатай бөгөөд антивирус, галт хана гэх мэт хамгаалалтын программ хангамжийнн тусламжтайгаар хамгаалах аргууд байдаг ч бүрэн дүүрэн хамгаалах боломжгүй. Тиймээс дотоодын цахим веб хуудас дээр дүн шинжилгээ хийж компьютерийн **сүлжээгээр дамжиж байгаа энгийн пакет болон хөнөөлтэй пакетуудыг wireshark болон Nmap хэрэгсэлийн тусламжтай дүн шинжилгээ хийснээр халдварлагдсан вэб хуудас нь хостын программ хангамжинд, регистрд нь хэрхэн халдварлаж host-ын үйл ажиллагааг доголдуулах болон IP хаяг нь өөрөө халдлагад өртөх магадлал хаягийг нарийн судлах юм.**

Түлхүүр үг— Халдалга, DoSattack, SYN-Flood, хөнөөлтөй программ, вирус, хакер, Wireshark

I. ОРШИЛ

Энэхүү өгүүлэл бичих заавар нь (paper template) IEE Судалгааны ажлын хүрээнд дотоод сүлжээний өгөгдлийн урсгалаас routher болон host- ын түвшний пакетууд дээр анализ хийж, сүлжээний аюулгүй байдалд хор, хөнөөл учруулах халдлага, дайралтыг Wireshark, Nmap, Regshot хэрэгслүүдийн тусламжтайгаар дүн шинжилгээ хийх болно. Цуглуулсан пакетуудаас IP хаяг нь өөрөө халдлагад өртөх магадлалтай хаягийг сонгон авсан бөгөөд IP хаягийг www.virustotalcam сайтаар шинжилгээ хийхэд www.copy.mn, www.xap.mn www.unen.mn сайтуудаас хохирогч host-ыг халдварлуулж алсын зайнаас халдлага, дайралтыг хэрхэн удирдаж байгааг тодорхойлох шаардлагатай болсон. Тухайн компьютерт Regshot хэрэгсэлийн тусламжтайгаар системийн файл, регистрийн файлд хэрхэн өөрчилөлт орж байгаа хэсгийг тодорхойлсон. Тодорхойлсоны үр дүнд Монголын үндэсний дата центрийн төвийн 80-р порт нь ямар нэгэн хамгаалалтгүй байсаныг тодорхойлж чадсан.

II. СУДАЛГААНЫ АРГАЧЛАЛ

Хэвийн ба хөнөөлтэй сүлжээний урсгалын шинжилгээг гүйцэтгэхдээ хяналттай тусгаарлагдсан орчинг бүрдүүлсний дараа host-ын үйлдлийн системийн халдварлагдаагүй эхний төлөвийн шаардлагатай мэдээллийг цуглуулсний [1-4] дараа Nmap хэрэгсэлээр дотоод сүлжээний топологи, нээлттэй болон хаалттай портуудын жагсаалтыг цуглуулсны дараа Wireshark хэрэгслийг ашиглаж сүлжээний урсгал дээр анализ хийсэн.

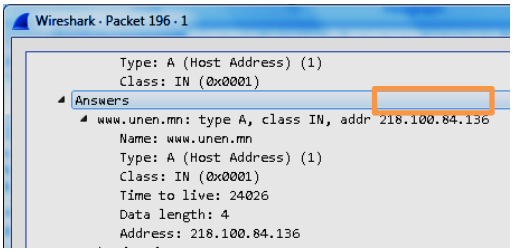
Wireshark хэргэсэл нь [1] нь пакет анализ хийгч бөгөөд сүлжээгээр дамжиж байгаа пакетуудыг хуулбарлан авч тухайн протоколууд ямар ямар өгөгдлүүд агуулж байгааг харж болдог.

Nmap хэрэгсэл нь [2] нь дотоод сүлжээний сул тал болон аюулгүй байдлыг шалгахад ашигладаг хэрэгсэл.

RegShot хэрэгсэл нь host-ын файл болон регистрт хэрхэн өөрчлөлт орж байгаа эсэхийг нарийн тодорхойлох боломжтой[3].

III. СУДАЛГААНЫ АРГАЧЛАЛ

Энэ ажлаар халдварлагдсан вэб хуудасыг ачааллаж сүлжээгээр дамжиж байгаа хэвийн болон халдлагатай пакет болон хостын регистр, системийн файл дээр дүн шинжилгээ хийсэн. Туршилтыг явуулахдаа I7процессортай 4 GB санах ойтой компьютер дээр WMware хэрэгсэлийг ашиглан виртуал орчинд Windows 7 үйлдлийн систем суулгаж үүсгэсэн. Виртуал орчинд үйлдлийн системийн регистрийн мэдээллийг Regshot хэрэгслээр цуглуулсны дараа дотоод сүлжээний төхөөрөмжүүдийн портын мэдээлэл сүлжээнд холбогдсон компьютерийн бүртгэлийг Nmap хэрэгслийн тусламжтай тодорхойлсон. Wireshark хэрэгслээр Улаанбаатарын их сургуулийн дотоод сүлжээний өгөгдлийн урсгалаас routher болон host-ын түвшний

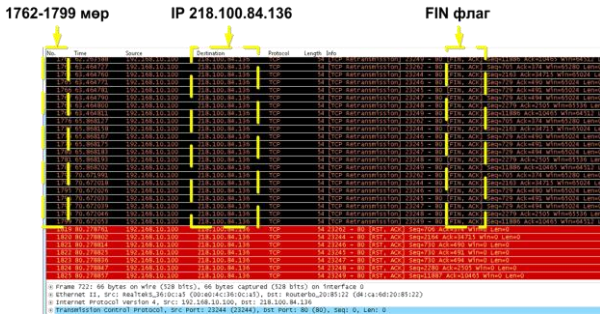


Зураг 1. IP нь хаяг өөрөө халдлагад өртөх магадлалтай

пакетуудын мэдээлэл дээр тулгуурлан халдлагатай

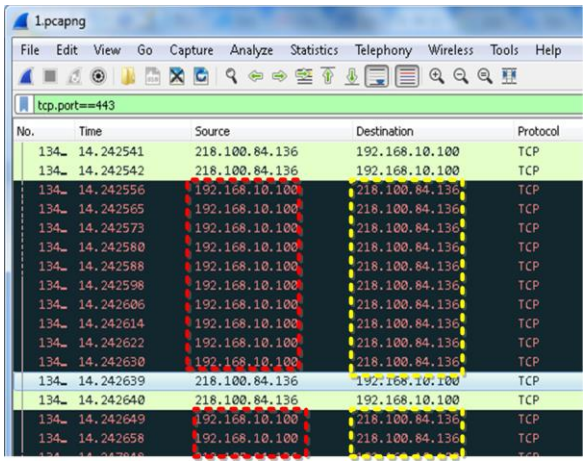
пакет дата дамжуулалт болон хүлээн авсан протокол дээр анализ хийсний үр дүнд IP хаягаар нь халдах магадлалтай хаягийг илрүүлсэн үнийг Зураг 1 үзүүлэв.

Уг IP хаягийг www.virustotal.com сайтад upload хийхэд Malware сайтууд болон Trojan/Win32.TSGeneric вирустэй www.unen.mn, www.wikimon.mn вэб сайт илэрсэн. www.unen.mn домайн хаягнаас IP 218.100.84.136-р хаяглуу холболт тогтоосныг Wireshark_хэрэгслээр шүүлт хийсэн үр дүнг Зураг 2 –т харуулав.



Зураг 2. Nmap болон SYN Flood халдлага

Зураг 2-аас харахад 1762-ээс 1799 мөрний хооронд FIN флаг төлөвтэй байгаа шинжээр нь энэхүү IP 218.100.84.136 хаяг нь халдлагт өртөж байгааг баталгажуулж байна. Харин 1819-ээс хойш пакет нь холболт тогтоох хүсэлтийг их хэмжээгээр илгээснээр сервисын үйл ажиллагааг доголдуулах зорилготой нь харагдаж байна.



Зураг 3. HTTPS портын халдлага

Зураг 3-т харуулсанаар тасархай шулуунаар тэмдэглэсэн хэсэгт хуулбарлсан ACK ыг олон давталттайгаар 192.168.10.100 IP хаягаас 218.100.84.136 IP хаяг руу илгээсэн. Үүний үр дүнд 218.100.84.136 IP хаягнаас 192.168.10.100 IP хаяг руу пакет илгээснээр хохирогч IP хаягийн хэрэглэгчийн өгөгдөл илгээгдэж хакерт эмзэг тал болон нээлттэй байгаа портуудын мэдээллийг мэдээлдэг. Хакерууд ихэвчлэн 443-р порт буюу HTTPS порт уруу халдлага дайралт хийдэг болохыг Зураг 3-аас харж болно.

IV. Судалгааны ажлын үр дүн

Дээрх 2 туршилтын үр дүнд IP 218.100.84.136-ийг шалгаж үзэхэд Монголын үндэсний дата центрийн вэб хуудас болохийг тодорхойлсон бөгөөд дээрх хаяг уруу Denial of Service төрлийн SYN-Flood болон Nmap төрлийн халдлагын түүл ашигласан болохыг тодорхойлсон. SYN-Flood халдлага нь TCP/IP аар их хэмжээний SYN пакетыг 80 портоор илгээж сервисийн үйл ажиллагааг удаашруулах зорилготой байдаг[5]. Харин Nmap төрлийн халдлагын түүл нь ихэвчлэн 443-р порт уруу хуулбарласан ACK илгээж host-ын эмзэг сул талыг илрүүлэх зорилготой байдаг[6].

Хүснэгт 1. Системийн файлд өөрчлөлт оруулсан хэсгүүд

Системийн файл хавтас	Нэмж хуулсан файлын нэр
C:\Windows\system32	msra.exe
C:\Windows\system32	MdSched.exe
C:\Windows\system32	unregmp2.exe
C:\ProgramFiles%\Windows Journal\	Journal.exe
C:\Windows\system32	unregmp2.exe

Физик машин дээр суурилсан виртуал үйлдлийн системийн файл болон регистрийн мэдээллийг урьдчилан Regshot хэрэгслээр цуглуулсны дараа халдварлагдаагүй үеийн регистр болон халдварлагдсан үеийн регистртэй харьцуулсан. Дээрх харьцуулалтаас харахад халдварлагдсан үеийн мэдээлэлийг хүснэгт 1-т үзүүлсэн. Хүснэгт 1-ээс хархад .exe файлууд нь вирус болон ямар хор хөнөөл учруулах нь тодорхойгүй. Мөн эдгээр файлууд нь Symantec компаны инженерүүд сэжиг бүхий файлууд гэж зөвлөсөн[7] байгаа хэдий ч цаашид дэлгэрэнгүй судлах шаардлагатай юм.

Хүснэгт 2. Регистрд өөрчлөлт оруулсан хэсгүүд

Windows registry	DoS attack
HKLM\Software\Microsoft	
HKLM\System\ControlSet001\Control\	
HKLM\Hardware\	
HKLM\System\CurrentControlset\Services\	
HKLM\Software\Microsoft\Cryptography\	
HKLM\Software\Microsoft\Windows NT\CurrentVersion\	
HKU\S-1-5-21-602162358-492894223-299502267-500\Software\Microsoft\Windows\CurrentVersion\Run	X
HKLM\SOFTWARE\Microsoft\DirectDraw\MostRecentApplication	

Харин хүснэгт 2-т үзүүлсэнээр HKU\S-1-5-21-602162358-492894223-299502267 регистрд

ихэвчлэн өөрчлөлт оруулдаг. HKEY_USERS бүртгэл нь (HKU) HKEY_CURRENT_USER товчлол бөгөөд тухайн хэсэгт Виндоус үйдлийн системд бүртгэгдсэн хэрэглэгчдийн үндсэн тохиргооны мэдээлэл хадгалагдсан байдаг[7].

ДҮГНЭЛТ

Бид энэхүү судалгааны ажлын хүрээнд Улаанбаатарын их сургуулын дотоодын сүлжээ дээр анализ хийсэн ба Wireshark хэрэгслийн тусламжтай IP хаяг нь өөрөө халдлагад өртөх магадлалтай хаяг болон халдварлагдсан домайн хаягийн пакет дээр судалгаа явуулсан. Судалгааны үр дүнд Malware сайт болон халдлагад өртөжбайгаа IP 218.100.84.136хаяг олдсон, дээрх хаягийг нарийн судалж үзэхэд Монголын үндэсний дата центрийн төвийн IP хаяг болохийг тодорхойлсон. IP 218.100.84.136 хаягаар холбогдож 80-р порт болон 443-р портлуу халдлага хийж байгааг тодорхойлсонбөгөөд Монголын нэр бүхий портал сайтууд болох www.copy.mn, www.xap.mn www.unen.mn халдварлагдсан сайтуудаас Монголын үндэсний дата центрийн үйл ажиллагааг тандах, сервисийн ажиллгагааг саатуулах зэрэг халдлагын шинж чанар агуулсан байх магадлалтай. Дээрх үр дүнгээс харахадМонголын үндэсний дата центрийн төвийн 80-р порт нь ямар нэгэн хамгаалалтгүй бөгөөд webmail.gov.mn сайтын HTTPS хамгаалалтын серфитикатын эрх нь дууссан тул хакерууд халдах боломжтой.

НОМ ЗҮЙ

[1] http://www.howtogeek.com/198679/how-to-use-regshot-to-monitor-your-registry/

[2] PRACTICAL MALWARE ANALYSIS.Copyright © 2012 by Michael Sikorski and Andrew Honig.

[3] G. Lyon, “Nmap 7.31 stability-focused point release,” Seclists.org, 2016.

[4] Nmap Installation for Windows. nmap.org.

[5] Nmap 5.50%94Now with Gopher protocol support%21. Seclists.org.

[6] U. Lamping, R. Sharpe, and E. Warnicke, “Wireshark User’s Guide For Wireshark 2.1.”

[7] Hacking tool reportedly draws FBI subpoenas. Securityfocus.com, 2004.

[8] Chapter 15. Nmap Reference Guide. Nmap.org, 2011.

[9] G. F. Lyon, Nmap network scanning : official Nmap project guide to network discovery and security scanning. Insecure.Com, LLC, 2008.

[10] A Data Mining Based Analysis of Nmap Operating System Fingerprint Database. .

[11] C. C. J. C. Burges, “A Tutorial on Support Vector Machines for Pattern Recognition,” Data Min. Knowl. Discov., vol. 2, no. 2, pp. 121–167, 1998.