Facebook дээр Байршуулсан Сошиал Медиа Мэдээллийн Урсгалыг Анализ Хийсэн Үр Дүн

Э.Мөнхцэцэг, Б.Дэнсмаа, Д.Бямбадорж
Соёл-Эрдэм дээд сургууль
Улаанбаатарын Их Сургууль, Физик электроникийн тэнхим
emuugiimm@gmail.com , densmaa2012@gmail.com, pheelectro2013@gmail.com

Хураангуй— Монголын facebook хэрэглэгчдийн дунд олон хандалттай сошиал медиа өгөгдлийг Wireshark, Nmap, RegShot хэрэгслүүдийн тусламжтай бид дүн шинжилгээ хийсэн. Үүний үр дүнд amjilt.com домайн хаягийг халдлагад өртсөнийг тодорхойлсон бөгөөд IP 202.21.123.83 хаягаар хандалт хийсэн host-уудыг халдварлуулан мөн тухайн дотоод сүлжээнд холбогдсон бусад host-ууд руу зохион байгуулалттайгаар алсын зайнаас удирдаж, халдлага дайралтанд ашиглаж байгааг олж тогтоосон.

Түлхүүр үг — NMAP, DoS attack, malware, RegShot

I. ОРШИЛ

Бид энэхүү судалгааны ажлын хүрээнд нийгмийн сүлжээ болох Facebook сайтад байршуулсан сошиал медиа маркетинг мэдээллийн аппликейшнүүдийн өгөгдөл болон дотоод сүлжээний TCP/IP-аар дамжиж буй хөнөөлт пакет болон IP хаяг нь халдлагад өртөх боломжтой пакетуудыг Wireshark, Nmap, RegShot хэрэгслүүдийн тусламжтай дүн шинжилгээ хийсэн. Судалгаагаар домайн хаяг нь халдлагад өртөх магадлалтай IP 202.21.123.83 хаяг байсан бөгөөд уг IP хаягийг хяналттай тусгаарлагдсан виртуал физик машин дээр нарийн судалгаа хийж үзэхэд хөнөөлтэй программ агуулсан www.amjilt.com/news домайн хаяг болохыг тодорхойлсон. Уг домайн хаягийг RegShot хэрэгслийн тусламжтай host-ийн системийн файл болон регистрийн файлд хэрхэн өөрчлөлт оруулж байгааг тодорхойлох болно.

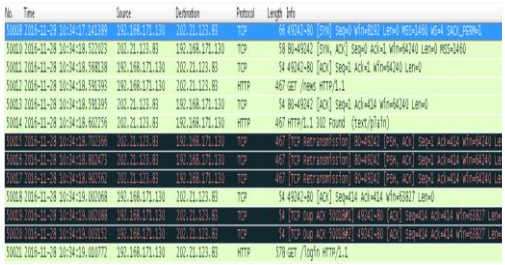
II. СУДАЛГААНЫ АРГАЧЛАЛ

Халдлагад өртөх магадлалтай домайн хаягаар дамжиж байгаа хөнөөлт өгөгдөл дээр шинжилгээ хийхдээ хяналттай тусгаарлагдсан физик машин дээр суулгасан виртуал үйдлийн системийн халдварлагдаагүй эхний төлөвийн системийн мэдээллийг цуглуулсний дараа[1–3] Nmap хэрэгслээр физик машин болон виртуал host- ын сүлжээний топологи болон портуудын мэдээллийг мөн цуглуулан WireShark [4]хэрэгслийг ашиглаж сүлжээнээр дамжиж байгаа өгөгдөл дээр анализ хийсэн [5].

- Wireshark хэргэсэл нь [4] пакет анализ хийгч бөгөөд сүлжээгээр дамжиж байгаа пакетуудыг хуулбарлан авч тухайн протоколууд ямар ямар өгөгдлүүд агуулж байгааг харж болдог.
- Nmap хэрэгсэл нь [6] нь дотоод сүлжээний сул тал болон аюулгүй байдлыг шалгахад ашигладаг хэрэгсэл.
- RegShot хэрэгсэл нь [7] host-ын файл болон регистрт хэрхэн өөрчлөлт орж байгаа эсэхийг нарийн тодорхойлох боломжтой.

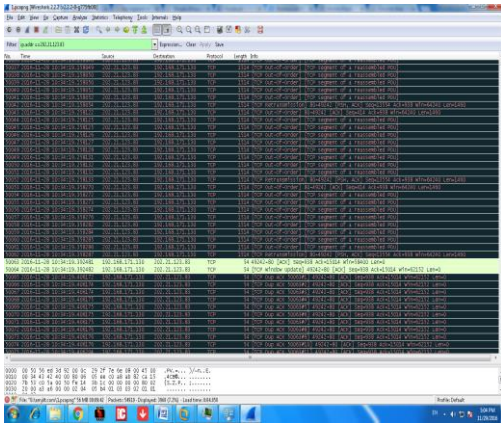
III. СУДАЛГААНЫ ЯВЦ

Бид энэхүү судалгаандаа нийгмийн сүлжээ болох Facebook сайтад байршуулсан маркетинг, медиа, аппликейшнүүдийн өгөгдөл болон дотоод сүлжээний TCP/IP-аар дамжиж буй хөнөөлт пакет болон IP хаяг нь халдлагын шинж чанартай пакетууд мөн эсэх, host-ын регистр, системийн файл дээр дүн шинжилгээ хийсэн. Туршилтыг явуулахдаа I5 процессортай 4GB санах ойтой зөөврийн компьютер дээр VM ORACLE хэрэгсэлийг ашиглан виртуал орчинд WIN7 үйдлийн систем суулгаж судалгаа явуулахад шаардлагатай үндсэн тохиргоонуудыг урьдчилан тохируулж бэлэн болгосон. Виртуал орчинд суулгасан WIN7 үйдлийн системийн халдварлаагүй үеийн мэдээллийг RegShot цуглуулсны дараа виртуал host-ын сүлжээний порт болон физик машины сүлжээний портын мэдээллийг мөн цуглуулж Wireshark хэрэгслээр физик болон виртуал сүлжээгээр дамжиж байгаа TCP/IP протокол дээр анализ хийсний үр дүнд халдлагад өртсөн IP хаягийг тодорхойлсон бөгөөд IP 202.21.123.83 хаягийг www.virustotal.com сайтад upload хийж анализ хийж үзэхэд http://www.amjilt.com/news домайн хаяг илэрсэн. Уг домайн хаяг нь хөнөөлт программ агуулсан сайт байсан. Зураг 1-д халдлага хийж байгаа хэсгийг үзүүлэв.



Зураг 1. IP 202.21.123.83 хаягнаас IP192.168.171.130 хаяглуу тандалт хийж байгаа хэсэг

Зураг 1 дээр харуулснаар Nmap халдлагын хэрэгслээр TCP протоколын үйл ажиллагааг тандах болон хуулбарласан ACK илгээсэн байна.



Зураг 2. TCP Flag- халдлагад өртөж байгаа хэсэг

Зураг 2–д TCP Flag-ын үйл ажиллагааг доголдуулсны дараа Nmap халдлагын хэрэгслээр TCP протоколын үйл ажиллагааг тандалт хийсний дараа хуулбарласан ACK их хэмжээгээр илгээсэн байна. TCP Flag-ийг дүүргэн дахин windows update хийж байна.

IV. Судалгааны үр дүн

Туршилтаар домайн хаяг нь хөнөөлтэй программ хангамж агуулсан IP 202.21.123.83 хаягийг илрүүлсэн. Уг IP 202.21.123.83 хаягаас виртуал үйдлийн системийн IP 192.168.171.130 хаяг уруу тандалт хийж TCP протоколын үйл ажиллагааг удаашруулах болон хуулбарласан ACK-ыг их хэмжээгээр илгээж байгаа нь харагдаж байна. IP 202.21.123.83 хаягаар дамжиж байгаа пакетууд дээр дотоод сүлжээний сул тал болон нээлттэй болон хаалттай портуудыг тандалт хийснээр алсын зайнаас удирдах болон халдлага дайралтанд ашиглах зорилготой болох нь харагдаж байна.

Физик машин дээр суулгасан виртуал үйлдлийн системийн файл болон регистрийн мэдээллийг урьдчилан Regshot хэрэгслээр[8], [9] цуглуулсны дараа халдварлагдаагүй үеийн регистр болон халдварлагдсан үеийн регистртэй харьцуулсан. Дээрх харьцуулалтаас харахад халдварлагдсан үеийн мэдээлэлийг хүснэгт 1-т үзүүлсэн.

Хүснэгт 1.Халдварлагдсан регистрийн мэдээлэл

Windows registry	DoS attack
HKLM\Software\Microsoft	
HKLM\System\ControlSet001\Control\	
HKLM\Hardware\	
HKLM\System\CurrentControlset\Services\	
HKLM\Software\Microsoft\Cryptography\	X
HKLM\Software\Microsoft\Windows NT\CurrentVersion\	X

Хүснэгт 1-ээс харахад HKU болон HKLM регистрүүдэд өөрчлөлт оруулсан байна. Дээрх HKU регистр нь HKEY_USERS бүртгэл нь (HKU)HKEY_CURRENT_USER товчлол бөгөөд тухайн хэсэгт windows үйдлийн системд бүртгэгдсэн хэрэглэгчдийн үндсэн тохиргооны мэдээлэл хадгалагдсан байдаг [10], [11].

Дүгнэлт

Нийгмийн сүлжээ болох Facebook сайтад байршуулсан сошиал медиа маркетинг мэдээллийн аппликейшнүүд нь сүлжээнд холбогдсон компьютерийн системийн файл болон үйлдлийн системийн регистрт хэрхэн өөрчлөлт оруулсан болон дотоод сүлжээгээр дамжиж байгаа TCP/IP протокол дээрх IP хаягууд халдлагад өртөх боломжтой пакетуудыг Wireshark, Nmap, RegShot хэрэгслүүдийн тусламжтай дүн шинжилгээ хийсэн. Үүний үр дүнд домайн хаяг нь халдлагад өртөх магадлалтай IP 202.21.123.83 хаяг байсан бөгөөд уг IP хаягийг хяналттай тусгаарлагдсан физик машин дээр суулгасан виртувал үйлдийн систем нарийн судалгаа хийсэний үндсэн дээр хөнөөлтэй программ агуулсан www.amjilt.com/news домайн хаягийг тодорхойлсон. Уг домайн хаягийг RegShot хэрэгслийн тусламжтай сүлжээнд холбогдсон үйлдлийн системийн регистр болох HKU\S-1-5-21-602162358-492894223-299502267-500\Software\Microsoft\Windows\CurrentVersion\Run регистрийн файлд өөрчлөлт оруулсанаар хор хөнөөл учруулах зорилготой клиент программыг дуудаж ачаалсанаар алсын зайнаас сүлжээнд холбогдсон компьютерд халдах боломжыг хакерт олгосоноор тухайн хэрэглэчийг тандах боломжтой.

References

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

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

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

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

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

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

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

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

[9] 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.

[10] B. Dondogmegd, U. B., and N. J., “A Malware Analysis Using Static and Dynamic Techniques,” http://www.sciencepublishinggroup.com, vol. 5, no. 1, p. 20, 2015.

[11] D. Ashley and P. Bueno, “Analysis of a Simple HTTP Bot GIAC (GREM) Gold Certification Analysis of a Simple HTTP Bot 2.”