Дэлхийг донсолгож буй Ransomware цахим халдлага

Мэдээллийн технологийн хэлтэс
2019 он

FR

Ransomware халдлага

Ransomware төрлийн програм анх 1989 онд бүртгэгдэж байсан. Харин 2009 оноос Bitcoin буюу crypto currency-н анхны хэлбэр хэрэглээнд орсноор ransomware төрлийн хортой програм хурдацтай хөгжих болсон. Учир нь Bitcoin-оор хийгдэж байгаа гүйлгээг шууд хянах боломжгүй, хэнээс гараад хэн гэдэг хүний дансанд орсныг тодорхойлох боломж бараг байдаггүйтэй холбоотой. Ransomware-г өгөгдөл барьцаалж байгаа арга хэлбэрээр нь хэд ялгаж үздэг. Үүнд: шифрлэлт хийх ransomware, түгжих ransomware, задлах ransomware, утасны ransomware.

Ransomware халдлага

- Шифрлэлт хийх ransomware нь мэдээлэл нууцлах арга буюу шифрлэлт ашиглан хэрэгтэй мэдээллийг нууцалж, буцааж тайлах боломжийг санал болгож, мөнгө шаарддаг.
- Түгжих ransomware нь файл дээр ямар нэг нууцлалт хийхгүй, харин тухайн төхөөрөмжийг ашиглах боломжийг хааж түгждэг. Мэдээж түгжээг тайлах аргыг мөнгөөр санал болгоно.
- Задлах ransomware нь ерөнхийдөө тухайн төхөөрөмжийн агуулж байгаа эмзэг мэдээлэл бүхий файлуудыг хулгайлж, шаардсан мөнгө өгөхгүй бол интернетийн орчинд тухайн файлуудыг дэлгэдэг.
- Утасны ransomware нь ухаалаг төхөөрөмжүүд дээр ажиллах боломжтой хувилбар юм.

FR

За тэгэхээр саяхныг хүртэл дэлхий дахинд шуугиан тариад байгаа WannaCry бол шифрлэлт хийдэг ransomware, бусад ransomware-үүдээс ялгаатай нь энэ ransomware нь NSA-аас алдагдсан тагнуулын зорилгоор ашиглаж байсан Windows үйлдлийн системийн SMB протокол дээр гарсан цоорхойг, Miscosoft засаж түгээхтэй зэрэгцэж ашигласан явдал юм.

FR

WannaCry хэрхэн ажилладаг талаар

WannaCry: The Anatomy of the Attack

1 ROOT CAUSE

?

2 FIRST STAGE EXECUTED

invokes SMB protocol for port scanning

3 PROPOGATION STEP 1

Attempts 'DoublePulsar' backdoor to send WCry to target endpoint , propogates

4 PROPOGATION STEP 2

'EternalBlue' scans servers for DoublePulsar'; If not found, delivers Wcry and propagates

5 DROPS TOR CLIENT

Launches Tor client on infected endpoint, anonymizing communications

6 INITIATES ENCRYPTION

Encrypts 160 file extensions and deletes shadow copies

7 RANSOWARE NOTICE

Displays ransomware message with instructions to decrypt

LATEST INTEL

- Crippled at least 100K organizations across multiple industries in over 150 countries
- 200K+ infected endpoints
- $60,000 paid so far but will rise and paying ransom is not recommended
- Ransomware slowed down by the accidental discovery of a killswitch
- However new variants have emerged with no killswitch or different domains

FR

WannaCry-н ажиллах зарчим маш энгийн, сүлжээнд Windows SMB ашиглаж байгаа машиныг хайж олоод NSA-с алдагдсан EternalBlue гэх exploit буюу хортой кодыг тухайн машин дээр ажиллуулж, улмаар өөрийгөө суулгаж, цааш дахин боломжтой бусад сүлжээнд тандалт хийж, тархах боломжийг хайна. Ингээд тандалт дуусах үед тухайн машин дээр байгаа чухал файлуудыг шифрлээд анхааруулах мэдээлэл гаргадаг.

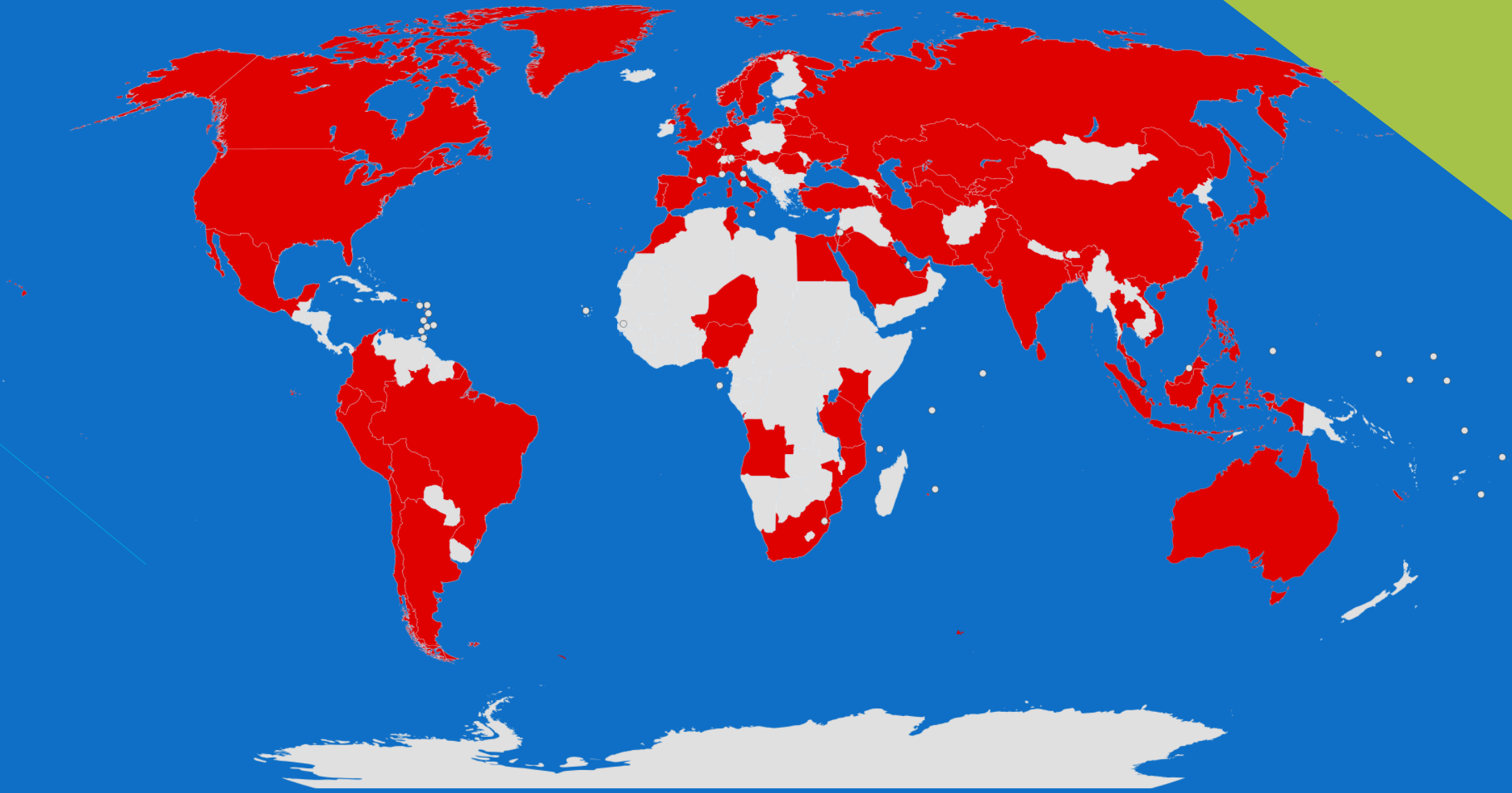
FR

Монгол улс WannaCry халдлагад хэр их өртсөн бэ?

- CERT-н шугамаар авсан мэдээлэлд Монгол улсын хэмжээнд 50 гаруй албан байгууллага, хувь хүний сервер WannaCry гэх ransomware-д өртсөн байх магадлалтай гэсэн мэдээлэл ирсэн. Гэхдээ энэ нь зөвхөн манай гадаад сүлжээнд илэрсэн тоон үзүүлэлт юм. Харин дотоод сүлжээнд үүнээс хавьгүй их тохиолдол байгаа болов уу, учир нь Монголчууд бидний хэрэглээ болоод өөрийн цахим мэдээлэлтэй хайхрамжгүй ханддагаас болж шинэ, хуучин гэлтгүй янз бүрийн хортой програмын тархах таатай нөхцөлийг бүрдүүлж байна.
- Хэд хэдэн онц чухал төрийн байгууллага дээр ганц нэг тохиолдол гарсан гэсэн дам яриа байгаа боловч яг бодитой мэдээлэл бүртгэгдээгүй байна.

Монгол улс WannaCry халдлагад хэр их өртсөн бэ?

FR



FR

Энэ халдлагын тархалт зогссон уу?

Тийм, нөгөө талаар бас үгүй. Учир нь WannaCry зүгээр л нэг төрлийн ransomware юм. Өнөөдөр сүлжээний орчинд хэдэн зуун төрлийн ransomware, янз бүрийн арга замаар хэрэглэгчийн мэдээллийг барьцаалах оролдлого хийж байна. Тэгвэл WannaCry зүгээр л тэдгээрийн хамгийн амжилттай тарсан тохиолдлын нэг гэж ойлгож болно. Учир нь уг ransomware нь NSA-ээс алдагдсан, тагнуулыг зорилгоор нуун ашиглаж байсан, Windows үйлдлийн системийн SMB протоколын цоорхойг ашигласан явдал юм. Уг цоорхой олон нийтэд ил болох тэр үед дөнгөж Microsoft тухайн алдааг илрүүлж, засах оролдлого хийж байсан нь цаг хугацааны хувьд уг ransomware сүлжээний орчинд хурдацтай тарах таатай нөхцөлийг бүрдүүлсэн юм. Хэдий өнөөдөр wannacry гэх уг ransomware-н тохиолдол буурч байгаа боловч шинээр илүү боловсронгуй болгосон Petya гэх шинэ ransomware тархаж эхлээд байна!

FR

Ransomware халдлагаас урьдчилан сэргийлэх

WannaCry гэх энэ ransomware интернет орчинд хэдэн зуун мянган серверийг өөрийн болгоод, цаашлаад илүү олон компьютерийг дотоод сүлжээнд нь өөрийн болгож чадсан нь, өнөөдөр бидний ашиглаж байгаа ямар ч antivirus-ний програм бидний компьютерийг бүрэн хамгаалах боломжгүй гэдгийг харуулсан том жишээ болсон.

- Хамгийн түрүүнд чухал мэдээллээ заавал нөөцөлж байх хэрэгтэй. Мэдээж нөөцлөлт маань ашиглаж байгаа төхөөрөмжөөс тусдаа байх шаардлагатай.
- Antivirus ашиглах, ингэхдээ ransomware төрлийн халдлагаас сэргийлэх тохиргоог идэвхжүүлж ашиглах.

FR

Хадлагад өртөхгүй байх арга зам

- Юу хэрэглэж байгаа, юу ашиглаж байгаагаа байнга анхаарч хянамгай байх.

  Үүнд:

  - Нээлттэй сүлжээ бүрд холбогдох (free-wifi)
  - Таарсан програм бүрийг ажиллуулах (Тоглоом, зураг)
  - Ирсэн и-мэйл бүрийг нээх (харилцагч биш хүнээс ирсэн мэйл)
  - Хаа хамаагүй вэб хуудсаар тэнэх (кино үзэх файсбүүхээс линкээр нэвтрэх)

  гэх мэт.

Систем Ransomware-т өртсөн тохиолдолд ямар арга хэмжээ авах вэ?

FR

- Хэрэв нөөцлөлт бүрэн байгаа бол тухайн системийг бүрэн шинэчлэх нь хамгийн хялбар найдвартай шийдэл байж болох юм.
- Нөөцлөлт байхгүй тохиолдолд машиныг шууд унтрааж болохгүй, учир нь зарим тохиолдолд түр санах ой дээр тухайн ransomware-г тайлах түлхүүр байх магадлалтай!
- Тухайн ransomware-г тодорхойлох шаардлагатай. Хэрэв та өөрөө шууд танихгүй байгаа бол https://id-ransomware.malwarehunterteam.com вэбсайтыг ашиглан тухайн ransomware-г тодорхойлж болох юм.
- Хэрэв ransomware-г амжилттай тодорхойлсон бол одоо тухайн ransomware-г тайлах програм буюу decryptor гарсан эсэхийг https://www.nomoreransom.org/ болон https://noransom.kaspersky.com/ сайтуудыг ашиглан шалгана.

FR

Мэдээллээ аврахын тулд ямар арга хэмжээ авбал зохих вэ? Систем, мэдээллээ аврахын тулд гэмт хэрэгтэнд хүссэн мөнгийг нь төлбөл яах вэ?

- Нэг зүйлийг ойлгох хэрэгтэй ransomware-д мөнгө төллөө гээд тухайн нууцлагдсан файлыг ямар ч асуудалгүй бүрэн сэргэнэ гэсэн баталгаа байхгүй.
- Үнэхээр гарцаагүй тохиолдолд арга байхгүй. Харин энэ сонголт дээр буухгүйн тулд **нөөцлөлт** гэдэг зүйлийг сайн хийж байх хэрэгтэй.

FR

Дүгнэлт

- Хаа явсан газраа үнэгүй WiFi гээд ороод байх шаардлагагүй.
- Энэ сайхан үнэтэй програм крактайгаа байна гээд суулгах хэрэггүй.
- Өө найзаас сонирхолтой хаяг, холбоос явуулж гээд нээж үзээд байх хэрэггүй.
- И-мэйл хаяг дээр ирсэн болгоныг ажиллуулахгүй байх.

АНХААРАЛ ТАВЬСАНД БАЯРЛАЛАА