National Datacenter

DCERT

DATACENTER EMERGENCY RESPONSE TEAM

ХАЛДЛАГАД ХАРИУ ҮЙЛДЭЛ ҮЗҮҮЛЭХ БАГ

“Null Character Bug” нь “Windows 10” системийн “Anti-malware” самналтын интерфейсийг давах чадвартай.

Null тэмдэгтийг суулгасан хорт програм нь Windows 10 дахь Anti-Malware Scan Interface (AMSI) –ийн аюулгүй байдлын самналтуудыг тойрч гарах боломжтой юм.

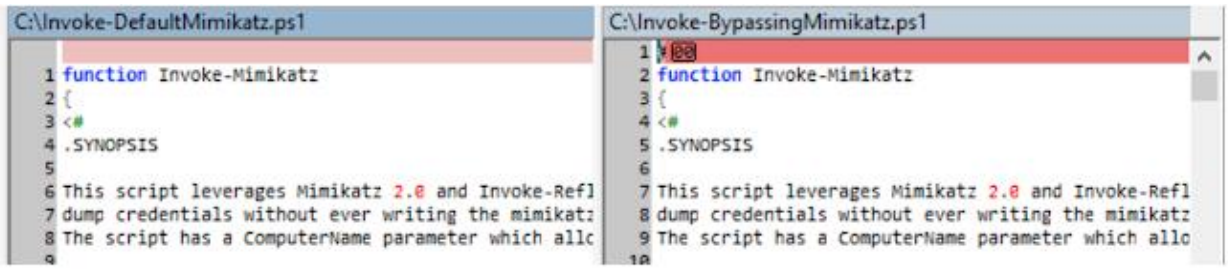
Microsoft энэ эмзэг байдлыг 2018 оны хоёрдугаар сарын аюулгүй байдлын шинэчлэлтээрээ засчээ.

Windows 10 AMSI аюулгүй байдлын онцлогт нөлөөлж буй сул тал нь:

- Anti-Malware Scan Interface (AMSI) –н эмзэг байдал нь ерөнхий аюулгүй байдлын функцэд апп-ууд болон үндсэн антивирусийн хэрэгсэл хооронд зуучлагч болон оршин тогтнож байна.
- AMSI нь апп –ыг дотоод аюулгүй байдлын программ хангамжаар самнуулахаар файлыг илгээж үр дүнг нь буцааж авдаг.
- AMSI нь windows 10 –тай хамт танилцуулагдсан бөгөөд үйлдвэрлэгч нь агностик буюу зөвхөн Windows Defender –т төдийгүй PC дээрх AMSI –д нийцтэй AV хэрэгсэлд файлыг автоматаар илгээдэг.
- AMSI нь бүх төрлийн файлуудыг самнадаг бол Microsoft AMSI –г PowerShell, VBScript, Ruby гэх мэт үйлдлийн скриптүүдийг шалгахад зориулан онцгойлон хөгжүүлсэн.

Өөрөөр хэлбэл AMSI нь гүйцэтгэсэн файлаар ачаалагдсан эсвэл түр хадгалагч нэмэлт эх үүсвэрийн гүйцэтгэлийн сканнерээр шалгадаг байна.

Техникийн дэлгэрэнгүй мэдээлэл, цөөн хэдэн жишээн дээр блог Tanda хортой PowerShell файлуудыг татан ажиллуулж, null тэмдэгтийн араас өөртөө хортой код агуулсан PowerShell командыг ажиллуулсан байна.



“Онолоор бол засварлахаас өөр арга хэмжээ авах шаардлагагүй” гэж Tanda өгүүлжээ. Гэсэн хэдий ч PowerShell агуулгыг хайхын тулд AMSI-ийг ашиглаж буй програм хангамж нь null тэмдэгтүүдийг зөв ажиллах чадвартай эсэхийг шалгах ёстой гэжээ.

Tanda, антивирусны програмууд өөрсдийн програм хангамжийг шалгаж өөрсдийн самнах хэрэгслүүд нь null тэмдэгт агуулсан файлуудыг богиносгодоггүй эсэхийг шалгах хэрэгтэйг мөн зөвлөж байна.

Bug Tanda зөвхөн AMSI-ийн PowerShell интерфейст нөлөөлж байгаа бөгөөд AMSI-ийн Windows Script Host-ийн орчуулагчид нөлөөлөхгүй байгааг илрүүлсэн.

Тэмдгийн алдаа нь жирийн мэт санагдаж болох ч тийм биш.

Сүүлийн жилүүдэд ажиглагдаж байгаа malware чиг хандлага дээр халдагчид хуурамч програмыг ашиглан Powershell скриптүүдээр дамжуулж хууль бус аппликейшн ашиглан шилжиж байна.

AMSI -г иймэрхүү байдлаар тойрч гарах нь классик malware -ээс хууль ёсны файл ашиглахад чиглэсэн шинэ хандлага руу шилжиж буй халдагчдад ашигтай болохыг баталж байна.

Эх сурвалж:
https://www.bleepingcomputer.com/news/security/null-character-bug-lets-malware-bypass-windows-10-anti-malware-scan-interface/