РЕПУБЛИКА СРБИЈА
РАТЕЛ
РЕГУЛАТОРНА АГЕНЦИЈА ЗА ЕЛЕКТРОНСКЕ КОМУНИКАЦИЈЕ И ПОШТАНСКЕ УСЛУГЕ

СРБ-ЦЕРТ

КАКО ПОСТУПИТИ УКОЛИКО СЕ РЕАЛИЗУЈЕ РАНСОМВЕР НАПАД

Припрема

- Потребно је добро познавање безбедносних политика оперативних система
- Потребно је добро познавање уобичајених политика корисничких профила
- Уверите се да су *endpoint* безбедносни уређаји ажурирани (имејл *gateway*-и, *proxy* кешеви)
- Будући да крајњи корисници најчешће открију ову претњу, подигните свест о ИТ подршци у вези са овом претњом
- Будите сигурни да имате одговарајуће и поуздане копије података локалних и мрежних корисника

Идентификација

Општи знакови присуства рансомвера

Неколико потенцијалних претпоставки може наговестити да би систем могао да буде угрожен рансомвером:

- Примају се необични професионални имејлови који садрже прилоге
- Порука о откупнини је приказана на монитору корисника и објашњава да су документи шифровани и тражи се новац за откуп
- Корисници се жале на то да су њихови фајлови на рачунару недоступни или оштећени или да су њихови фајлови који се деле путем мреже са необичним екстензијама (*.abc, .xyz, .aaa*, итд...).
- Много фајлова се мења у веома кратком року на мрежи

Идентификација код корисника

- Погледајте да ли се у профилима корисника налазе неуобичајене извршне бинарне датотеке (%ALLUSERSPROFILE% ili %APPDATA%) и %SystemDrive%
- Потражите горе наведене екстензије или поруке о откупнини
- Покушајте да видите заузету меморију компјутера, уколико је то могуће
- Проверите да ли има неуобичајених процеса
- Потражите у имејл порукама да ли има неуобичајених имејл прилога
- Проверите да ли има неуобичајених активности на мрежи или у интернет претраживачима; посебно обратите пажњу на конекције ка *Tor* ili *I2P IP*, *Tor gateways* (*tor2web*, itd) или ка *Bitcoin* веб страницама за плаћање.

Идентификација на мрежи

- Погледајте да ли има конекција ка *Exploit Kits*-овима
- Погледајте да ли има конекција ка рансомвер *C&C* серверима
- Проверите да ли има неуобичајених активности на мрежи или у интернет претраживачима; посебно обратите пажњу на конекције ка *Tor* или *I2P IP*, *Tor gateways* (*tor2web*, itd) или ка *Bitcoin* веб страницама за плаћање
- Потражите у имејл порукама да ли има неуобичајених имејл прилога

Спречавање даљег ширења

- Одмах изолујте све рачунаре који су угрожени и искључите их са мреже. Заражене системе треба уклонити са мреже што је пре могуће како би се спречило даље ширење рансомвера и нападне мрежа или дељени дискови
- Изолујте или искључите погођене уређаје који још нису у потпуности оштећени. Ово вам може пружити више времена за чишћење и обнављање података, задржавање штете и спречавање да се услови погоршају
- Ако не можете да изолујете рачунар, искључите/откажите (disconnect/cancel) конекције ка дељеним дисковима (NET USE k:\\unc\path\ /DELETE)
- Одмах обезбедите резервне копије података или система тако што ћете их искључити са мреже. Потребно је проверити да резервне копије не садрже злонамерни софтвер.
- Блокирајте саобраћај који је идентификован као рансомвер *C&C*
- Избришите вредности и фајлове из регистра, како бисте зауставили да се програм учитава
- Ако су доступни, покушајте да прикупите и обезбедите делове рансомвер фајлова који могу постојати. Узорке пошаљите крајњем провајдеру
- Пошаљите некатегорисани злонамерни URL, имена домена и IP адресе крајњем провајдеру
- Ако је могуће, промените све лозинке за online налоге и мрежне лозинке, након искључивања система са мреже. Поред тога, промените све системске лозинке након уклањања злонамерног софтвер из система.

Санација

- Уклоните бинарне датотеке и повезане уносе у регистре (ако их има) из компромитованих профила (% ALLUSERSPROFILE% ili % APPDATA%) и % SistemDrive%
- Ако претходни корак није могућ, урадите *reimage* рачунара првобитном инсталацијом која не садржи злонамерне фајлове.

Опоравак

Циљ : Враћање система у нормално функционисање

- Ажурирајте потписе антивирусне заштите за идентификоване злонамерне бинарне датотеке које треба блокирати
- Обезбедите да се мрежни саобраћај врати у нормалан режим рада
- Вратити документа корисника из резервних копија

Савет је да се претходне ставке ураде корак по корак и уз технички надзор.

Извештај

Извештај о инциденту треба да буде написан и доступан свим заинтересованим странама.

Требало би описати следеће:
- Када је инцидент откривен
- Акције које су предузете, као и временски рокови
- Шта је урађено како треба
- Како је дошло до инцидента
- Финансијски губитак који је инцидент поузроковао

Сумирање

На бази овог искуства требало би извући поуке, тако што ће се дефинисати акције за побољшање процеса детекције злонамерних софтвера и мрежа.

Извор:

https://github.com/certsocietegenerale/IRM/blob/master/EN/IRM-17-Ransomware.pdf