STOP Ransomware လမ်းညွှန်

နိဒါန်း

၁။ STOP Ransomware သည် နိုင်ငံတကာတွင် ၂၀၁၇ ခုနှစ်၊ ဒီဇင်ဘာလ၌ စတင်တိုက်ခိုက်ခဲ့ပြီး မြန်မာနိုင်ငံတွင် စတင်တိုက်ခိုက်ခံရကြောင်း mmCERT ထံ ပထမဆုံး သတင်းပေးပို့သည့်ရက်စွဲမှာ ၂၀၁၉ ခုနှစ်၊ ဧန်နဝါရီလ (၂၉)ရက်နေ့တွင် ဖြစ်ပါသည်။ သို့သော် ၂၀၁၈ ခုနှစ်၊ နှစ်လယ်ပိုင်း ကတည်းက တိုက်ခိုက်ခံထားရမှုများ ရှိနေနိုင်ပါသည်။ STOP Ransomware နှင့်ပတ်သက်၍ mmCERT ထံသို့ တိုင်ကြားမှုများမှာ ၂၀၁၉ ခုနှစ်အတွင်း ဧန်နဝါရီလတွင် (၁)ကြိမ်၊ ဖေဖော်ဝါရီလတွင် (၁)ကြိမ်၊ မတ်လတွင် (၆)ကြိမ်၊ ဧပြီလတွင် (၂၇)ကြိမ်၊ မေလတွင် (၃၆)ကြိမ်၊ ဇွန်လတွင် (၉၁)ကြိမ် တိုက်ခိုက်ခံထားရပြီး ၂၀၁၉ ခုနှစ်အတွင်း စုစုပေါင်းတိုင်ကြားခဲ့မှုမှာ (၆၅၇)ကြိမ် ရှိခဲ့ပါသည်။ ၂၀၁၉ ခုနှစ်အတွင်း mmCERT သို့ တိုင်ကြားခဲ့သော Ransomware တိုက်ခိုက်ခံရမှုများတွင် STOP Ransomware (၆၅၇)ကြိမ်၊ Dharma Ransomware (၁၃)ကြိမ်၊ GandCrab 5.x Ransomware (၇)ကြိမ်၊ GlobalImposter Ransomware (၃)ကြိမ်၊ Scarab Ransomware (၃)ကြိမ်၊ Rapid Ransomware (၂)ကြိမ်၊ အမည်မသိ Ransomware (၂)ကြိမ်၊ Jamper Ransomware (၁)ကြိမ်၊ JSWorm 4.0.3 (၁)ကြိမ်၊ Paradise Ransomware (၁)ကြိမ်၊ Phobos Ransomware (၁)ကြိမ်၊ WannaCry Ransomware (၁)ကြိမ်နှင့် Hermes Ransomware (၁)ကြိမ် အသီးသီးရှိခဲ့ရာ STOP Ransomware တိုက်ခိုက်ခဲ့မှုသည် အများဆုံးဖြစ်ကြောင်း တွေ့ရှိရပါသည်။

STOP Ransomware မည်သို့ ကူးစက်ခံရပါသနည်း

၂။ STOP Ransomware သည် တရားမဝင်ဆော့ဖ်ဝဲလ်များကို အွန်လိုင်းတွင် download လုပ်မိရာမှ၊ crack ဖိုင်များကို download လုပ်မိရာမှ ထိုဆော့ဖ်ဝဲလ်များမှတဆင့် တိုက်ခိုက်ခံရခြင်း ဖြစ်ပါသည်။ ပြည်တွင်းတွင် လိုင်စင်ပါရှိသော ဆော့ဖ်ဝဲလ်များကို အသုံးပြုသူနည်းပါးခြင်းသည် Ransomware ၏ ပစ်မှတ်သားကောင် တိုးပွားလာစေခြင်း၏ အဓိကအကြောင်းရင်းဖြစ်ပါသည်။

STOP Ransomware ၏ ပစ်မှတ်များ

၃။ STOP Ransomware အနေဖြင့် ပစ်မှတ်ထားတိုက်ခိုက်သော ဖိုင်အမျိုးအစား (၁၂၇)မျိုး ရှိပါသည်။ ထိုအထဲတွင် Microsoft Excel ဖိုင်များ၊ Microsoft Word ဖိုင်များ၊ Adobe Acrobat ဖိုင်များ ပါဝင်သည့်အပြင် ယခုအခါ Program ဖိုင်များကိုပင် တိုက်ခိုက်လျက်ရှိပါသည်။

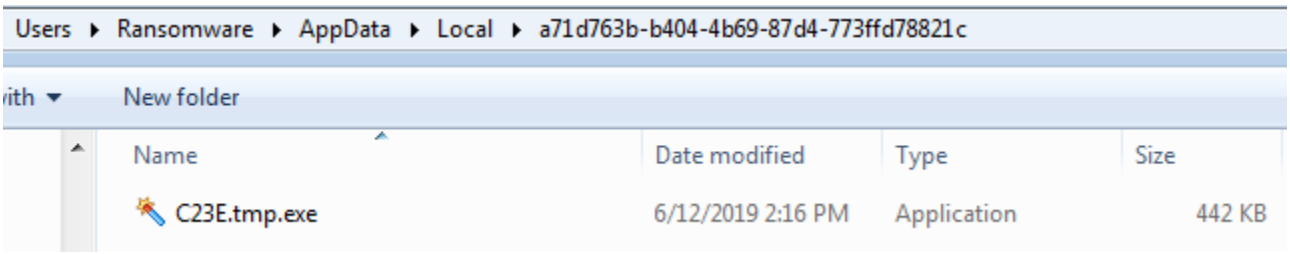
STOP Ransomware တိုက်ခိုက်ပုံ အကျဉ်းချုပ်

(**မှတ်ချက်**။ ဤတိုက်ခိုက်ပုံအကျဉ်းချုပ်သည် သာမန်ကွန်ပျူတာသုံးစွဲသူများအတွက် မဟုတ်ဘဲ နည်းပညာသမားများအနေဖြင့် ကိုးကားနိုင်ရန် ဖော်ပြခြင်းဖြစ်ပါသည်။)

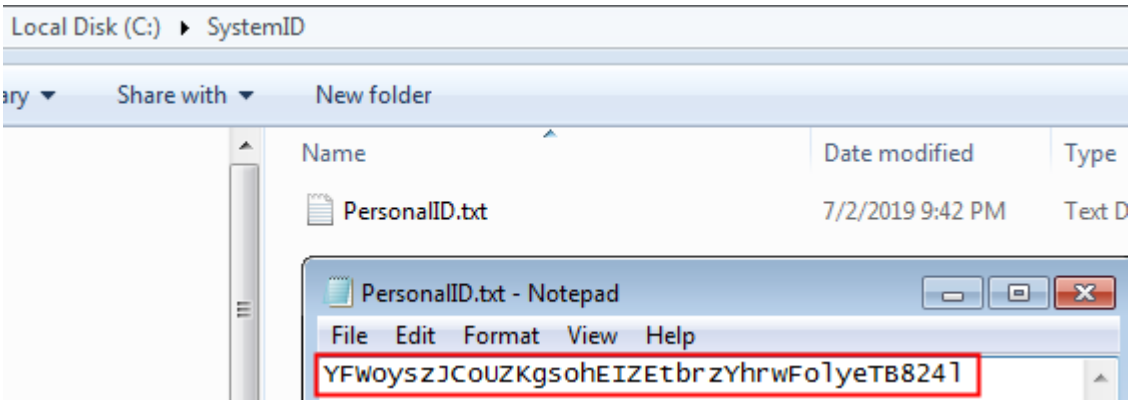
(က) Offline Key ဖြင့် တိုက်ခိုက်ခံရပုံ

၄။ STOP Ransomware ကို ဖွင့်မိသည့်အခါ အောက်ပါတို့ကို လုပ်ဆောင်ပါသည်-

(က) C:\Users\UserAccount\AppData\Local အောက်တွင် xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx အမည်ဖြင့် Random Folder တစ်ခုဖန်တီးပြီး Ransomware ဖိုင်ကို ထပ်မံပွားပါသည်။

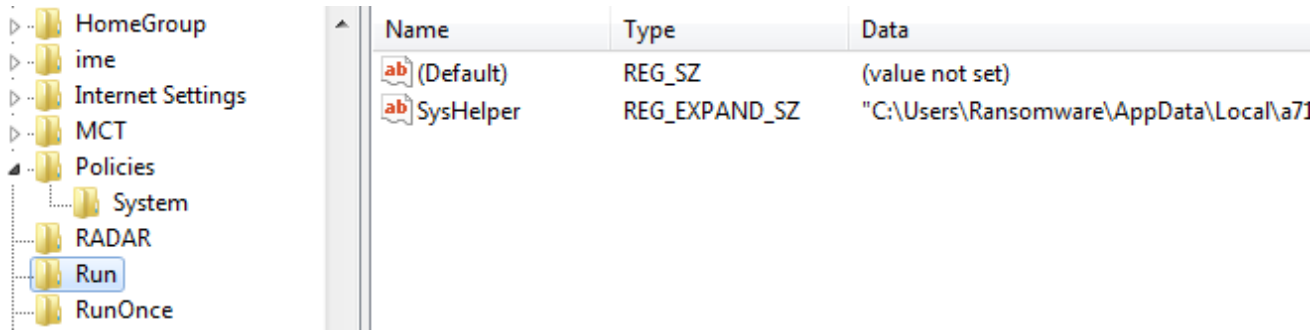


(ခ) ပထမဦးစွာ C&C Server ဖြစ်သော http://texet1.ug ကို လေးကြိမ်တိုင်တိုင် ချိတ်ဆက်ရန် ကြိုးစားပြီး C&C Server နှင့် ဆက်သွယ်မှုမရခဲ့ပါက C:\ အောက်တွင် SystemID Folder ကို တည်ဆောက်ပြီး PersonalID.txt ဖိုင်ကို ဖန်တီးပါသည်။ ၎င်းဖိုင်ထဲတွင် Offline Key ကို သိမ်းပါသည်။ (C&C Server အမည်သည် အမြဲတမ်း ပြောင်းလဲမှု ရှိပါသည်။)

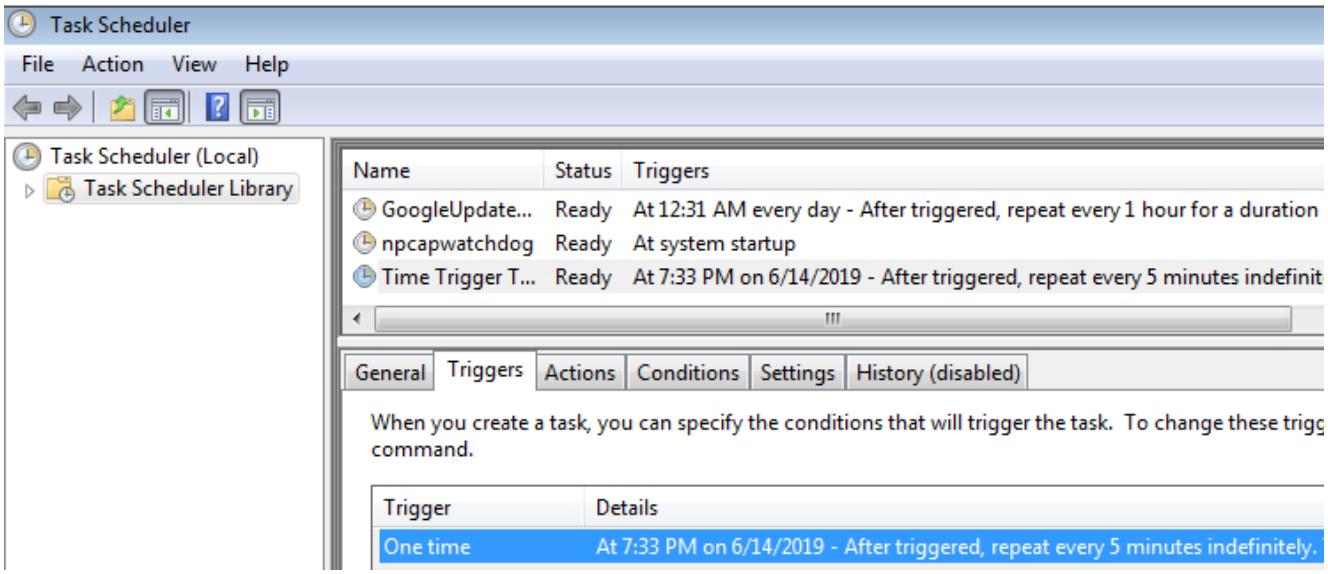


(ဂ) _readme.txt ဖိုင်ကို C:\ အောက်တွင် ဖန်တီးပြီး Offline Key တစ်ခုကို ဖန်တီးပါသည်။ ဤ _readme.txt ဖိုင်ကို Ransom Note ဟုခေါ်ဆိုပါသည်။ ဤဖိုင်ထဲတွင် Ransom ပေးချေရမည့်နည်းလမ်းများနှင့် Pesonal ID တို့ပါဝင်ပါသည်။

(ဃ) ကွန်ပျူတာထဲတွင် အမြဲတမ်းအလုပ်လုပ်စေနိုင်ရန် Run Key တွင် SysHelper အမည်ဖြင့် Registry တန်ဖိုးကို သတ်မှတ်ပါသည်။



(c) ၎င်းနောက် ၅မိနစ်တစ်ကြိမ် Ransomware အားအလုပ်လုပ်စေနိုင်ရန် scheduled task တစ်ခုအား ဖန်တီးပါသည်။



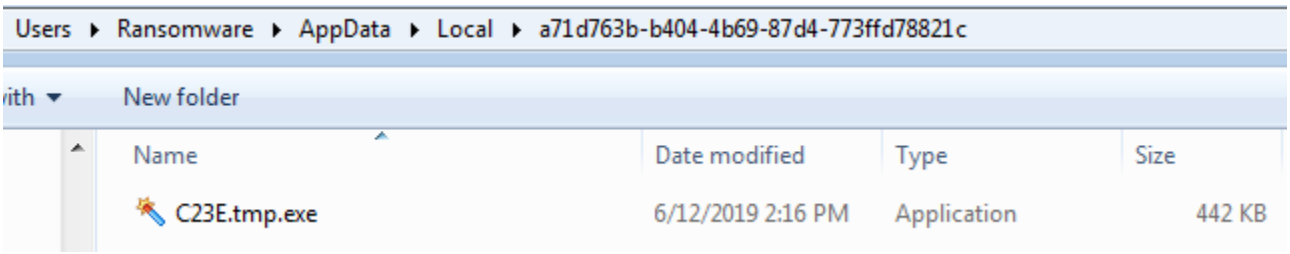
(စ) နောက်ဆုံးတွင် Antivirus များကို download လုပ်၍ မရစေနိုင်ရန် C:\Windows\system32\drivers\etc\ folder အောက်ရှိ host ဖိုင်တွင် website ပေါင်း (၂၄၀)ခုအား ဝင်မရစေရန် localhost IP ဖြင့် အစားထိုးပါသည်။

```
120   127.0.0.1 www.eset.com
121   127.0.0.1 eset.com
122   127.0.0.1 www.fortinet.com
123   127.0.0.1 fortinet.com
124   127.0.0.1 fortiguard.com
125   127.0.0.1 www.fortiguard.com
126   127.0.0.1 forticlient.com
127   127.0.0.1 www.forticlient.com
128   127.0.0.1 www.kpn.com
129   127.0.0.1 kpn.com
130   127.0.0.1 www.kaspersky.com
131   127.0.0.1 kaspersky.com
132   127.0.0.1 www.consumentenbond.com
133   127.0.0.1 consumentenbond.com
134   127.0.0.1 www.surfspot.com
```

(ခ) Online Key ဖြင့် တိုက်ခိုက်ခံရပုံ

၅။ STOP Ransomware ကို ဖွင့်မိသည့်အခါ အောက်ပါတို့ကို လုပ်ဆောင်ပါသည်-

(က) C:\Users\UserAccount\AppData\Local အောက်တွင် xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx အမည်ဖြင့် Random Folder တစ်ခုဖန်တီးပြီး Ransomware ဖိုင်ကို ထပ်မံပွားပါသည်။



(ခ) ပထမဦးစွာ C&C Server ဖြစ်သော http://texet1.ug ကို လေးကြိမ်တိုင်တိုင် ချိတ်ဆက်ရန် ကြိုးစားပြီး C&C Server နှင့် ဆက်သွယ်မှုရခဲ့ပါက http://texet2.ug (Domain အမည်သည် ပြောင်းလဲမှု ရှိနိုင်ပါသည်။) မှ 3.exe၊ 4.exe၊ 5.exe၊ updatewin.exe၊ updatewin1.exe၊ updatewin2.exe ဖိုင်များကို download လုပ်ရန်ကြိုးစားပါသည်။ (ယခုအချိန်တွင် 3.exe နှင့် 4.exe တို့သည် texet2.ug တွင် ထိန်းသိမ်းထားခြင်း မရှိတော့ပါ။)

(ဂ) C:\ အောက်တွင် SystemID Folder ကို တည်ဆောက်ပြီး PersonalID.txt ဖိုင်ကို ဖန်တီးပါသည်။ ၎င်းဖိုင်ထဲတွင် Online Key ကို သိမ်းပါသည်။

(ဃ) Windows PowerShell ကို ခေါ်၍ "*Set-MpPreference -DisableRealtime Monitoring*" command ဖြင့် Windows Defender ကို ပိတ်ပါသည်။

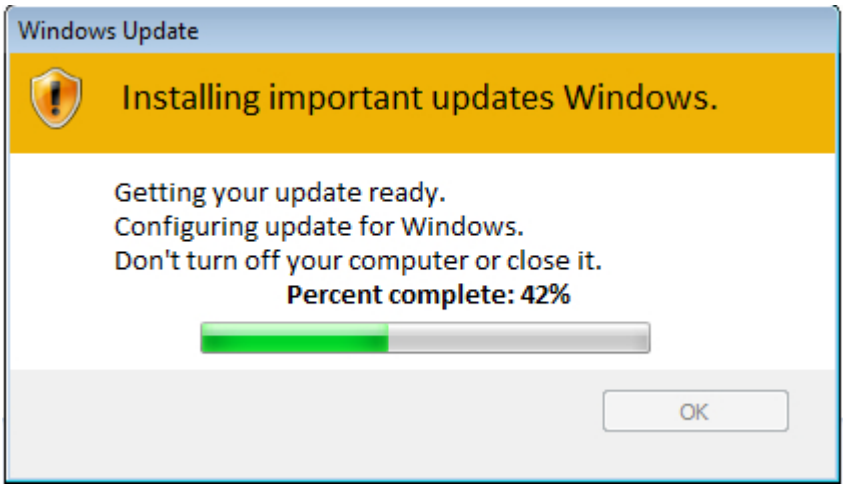
(c) MpCmdRun ကို အသုံးပြု၍ Virus Definition များကို ဖယ်ရှားပါသည်။

(စ) updatewin1.exe ဖိုင်ကို Admin permission ဖြင့် အလုပ်လုပ်စေပြီး ၎င်းဖိုင်မှ Windows Powershell ကိုခေါ်ယူ၍ "powershell -Command Set-ExecutionPolicy -Scope CurrentUser RemoteSigned"၊ "powershell -NoProfile -ExecutionPolicy Bypass -Command "& {Start-Process PowerShell -ArgumentList '-NoProfile -ExecutionPolicy Bypass -File ""C:\Users\admin\AppData\Local\script.ps1""' -Verb RunAs}"" နှင့် "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -NoProfile -ExecutionPolicy Bypass -File C:\Users\admin\AppData\Local\script.ps1" တို့ကို အလုပ်လုပ်စေပါသည်။ ၎င်းနောက် "C:\Program Files\Windows Defender\mpcmdrun.exe -removedefinitions -all"

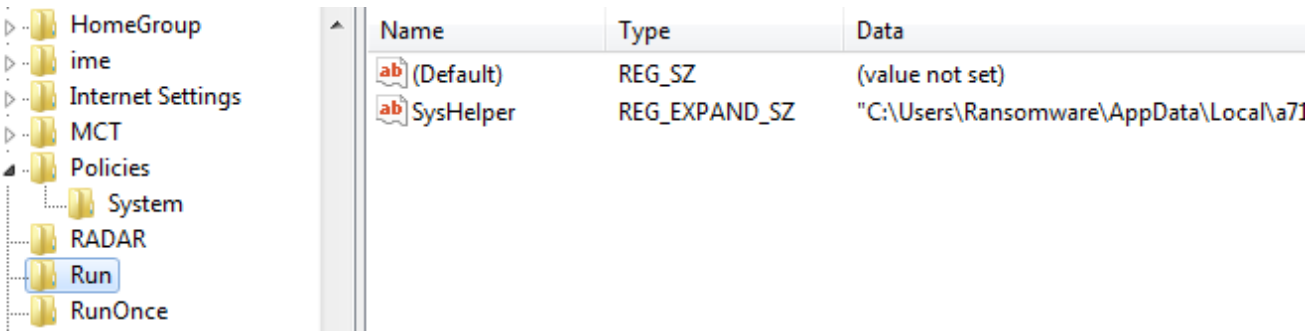
ဖြင့် Windows Defender ၏ virus definition များကို ဖျက်ဆီးပစ်ကာ “delself.bat” ဖိုင်ဖြင့် မိမိဖိုင်ကို ဖျက်ဆီးပစ်ပါသည်။

(ဆ) 5.exe ဖိုင်သည် သတင်းအချက်အလက်များကို ခိုးယူသော Azorult trojan ဖြစ်ပြီး ၎င်းသည် Google Update Installer အဖြစ် အယောင်ဆောင်ကာ ကွန်ပျူတာထဲတွင် ရေရှည်နေနိုင်စေရန်အတွက် GoogleUpdateInstaller အား အစားထိုးပစ်ပါသည်။ (၂၀၁၉ ခုနှစ်၊ စက်တင်ဘာလနောက်ပိုင်းတွင် Azorult trojan အစား Vidar information stealer အား ပြောင်းလဲသုံးစွဲလာပါသည်။)

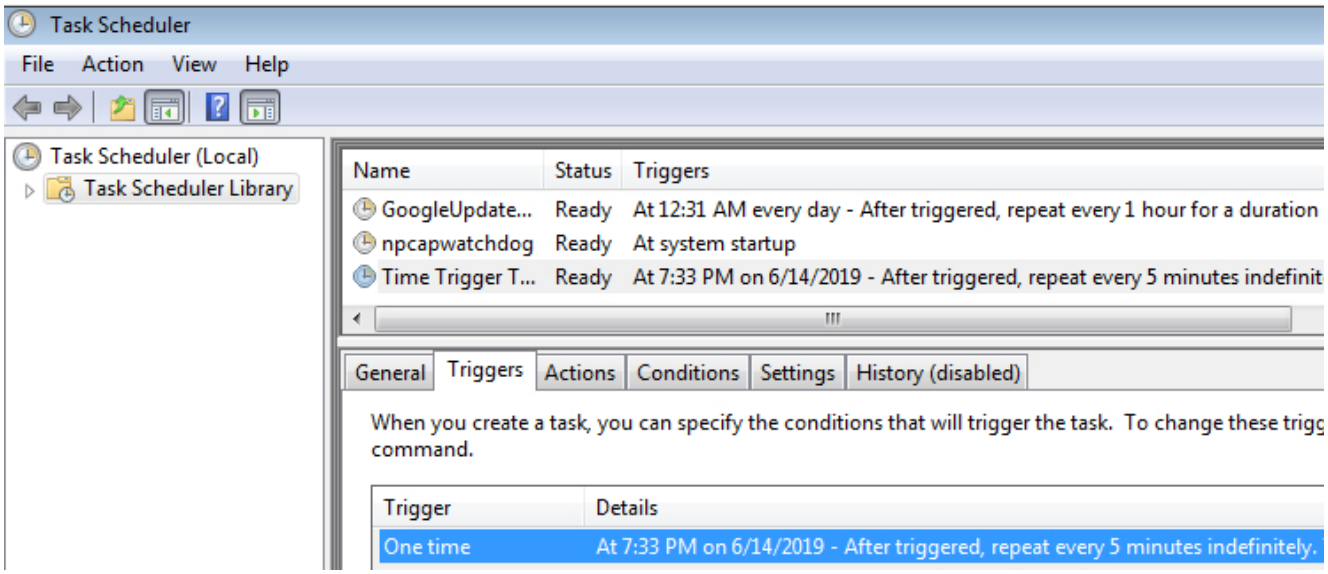
(ဇ) ပြီးနောက်တွင် updatewin.exe ဖိုင်ကို အလုပ်လုပ်စေကာ ပုံပါအတိုင်း Windows Update အသွင်ဟန်ဆောင်ကာ ကွန်ပျူတာ စနစ်ထဲတွင်ရှိသည့် Folder များအောက်ရှိ ဖိုင်များကို ရှာဖွေကာ ဖိုင်များကို ဝှက်ပါသည်။



(စျ) Windows Registry ထဲတွင် TaskManager အားခေါ်ကြည့်၍ မရစေရန် DisableTaskmgr key ကို ဝင်ရေး၍ ကွန်ပျူတာထဲတွင် အမြဲတမ်းအလုပ်လုပ်စေနိုင်ရန် Run Key တွင် SysHelper အမည်ဖြင့် Registry တန်ဖိုးကို သတ်မှတ်ပါသည်။



(ည) ၎င်းနောက် ၅မိနစ်တစ်ကြိမ် Ransomware အားအလုပ်လုပ်စေနိုင်ရန် scheduled task တစ်ခုအား ဖန်တီးပါသည်။



(၄) နောက်ဆုံးတွင် Antivirus များကို download လုပ်၍ မရစေနိုင်ရန် C:\Windows\system32\drivers\etc\ folder အောက်ရှိ host ဖိုင်တွင် website ပေါင်း (၂၄၀)ခုအား ဝင်မရစေရန် localhost IP ဖြင့် အစားထိုးပါသည်။

```
120   127.0.0.1 www.eset.com
121   127.0.0.1 eset.com
122   127.0.0.1 www.fortinet.com
123   127.0.0.1 fortinet.com
124   127.0.0.1 fortiguard.com
125   127.0.0.1 www.fortiguard.com
126   127.0.0.1 forticlient.com
127   127.0.0.1 www.forticlient.com
128   127.0.0.1 www.kpn.com
129   127.0.0.1 kpn.com
130   127.0.0.1 www.kaspersky.com
131   127.0.0.1 kaspersky.com
132   127.0.0.1 www.consumentenbond.com
133   127.0.0.1 consumentenbond.com
134   127.0.0.1 www.surfspot.com
```

STOP Ransomware တိုက်ခိုက်ခံထားရသည့် ဖိုင်များ

၆။ STOP Ransomware တိုက်ခိုက်ခံထားရပါက ဖိုင်များသည် အောက်ပါ extension တစ်ခုခုသို့ ပြောင်းလဲသွားမည်ဖြစ်ပြီး နောက်ဆုံးထွက်ရှိသော STOP Ransomware တိုက်ခိုက်ခံရပါက .budak ဖိုင်များ အဖြစ်ပြောင်းလဲသွားမည်ဖြစ်ပါသည်။ (ဤ extenstion များသည် (၂၁-၇-၂၀၂၀) ရက်နေ့ထိသာဖြစ်ပြီး ၃ရက်လျှင်တစ်ကြိမ်ခန့် STOP Ransomware အသစ်ထွက်ရှိတတ်သဖြင့် ဖိုင် extension အသစ်များ ထပ်မံတိုးပွားလာပါမည်။)

.STOP, .SUSPENDED, .WAITING, .PAUSA, .CONTACTUS, .DATASTOP, .STOPDATA, .KEYPASS, .WHY, .SAVEfiles, .DATAWAIT, .INFOWAIT, .puma, .pumax, .pumas, .shadow, .djvu, .djvuu,

.udjvu, .djvuq, .uudjvu, .djvus, .djvur, .djvut .pdff, .tro, .tfude, .tfudeq, .tfudet, .rumba, .adobe, .adobee, .blower, .promos, .promoz, .promock, .promoks, .promorad, .promok, .promorad2, .kroput, .kroput1, .charck, .pulsar1, .klope, .kropun, .charcl, .doples, .luces, .luceq, .chech, .proden, .drume, .tronas, .trosak, .grovas, .grovat, .roland, .refols, .raldug, .etols, .guvara, .browec, .norvas, .moresa, .verasto, .hrosas, .kiratos, .todarius, .hofos, .roldat, .dutan, .sarut, .fedasot, .forasom, .berost, .fordan, .codnat, .codnat1, .bufas, .dotmap, .radman, .ferosas, .rectot, .skymap, .mogera, .rezuc, .stone, .redmat, .lanset, .davda, .poret, .pidon, .heroset, .myskle, .boston, .muslat, .gerosan, .vesad, .horon, .neras, .truke, .dalle, .lotep, .nusar, .litar, .besub, .cezor, .lokas, .godes, .budak, .vusad, .herad, .berosuce, .gehad, .gusau, .madek, .tocue, .darus, .lapoi, .todar, .dodoc, .bopador, .novasof, .ntuseg, .ndarod, .access, .format, .nelasod, .mogranos, .cosakos, .nvetud, .lotej, .kovasoh, .prandel, .zatrov, .masok, .brusaf, .londec, .krusop, .mtogas, .nasoh, .nacro, .pedro, .nuksus, .vesrato, .masodas, .stare, .cetori, .carote, .coharos, .shariz, .gero, .hese, .xoza, .seto, .peta, .moka, .meds, .kvag, .domn, .karl, .nesa, .boot, .noos, .kuub, .reco, .bora, .leto, .nols, .werd, .coot, .derp, .nakw, .meka, .toec, .mosk, .lokf, .peet, .grod, .mbed, .kodg, .zobm, .rote, .msop, .hets, .righ, .gesd, .merl, .mkos, .nbes, .piny, .redl, .nosu, .kodc, .reha, .topi, .npsg, .btos, .repp, .alka, .bboo, .rooe, .mmnn, .ooss, .mool, .nppp, .rezm, .lokd, .foop, .remk, .npsk, .opqz, .mado, .jope, .mpaj, .lalo, .lezp, .qewe, .mpal, .sqpc, .mzlq, .koti, .covm, .pezi, .zipe, .nlah, .kkll, .zwer .nypd, .usam, .tabe, .vawe, .moba, .pykw, .zida, .maas, .repl, .kuus။

STOP Ransomware တိုက်ခိုက်ခံရမှုကြောင့် ဆုံးရှုံးခဲ့ရမှုများ

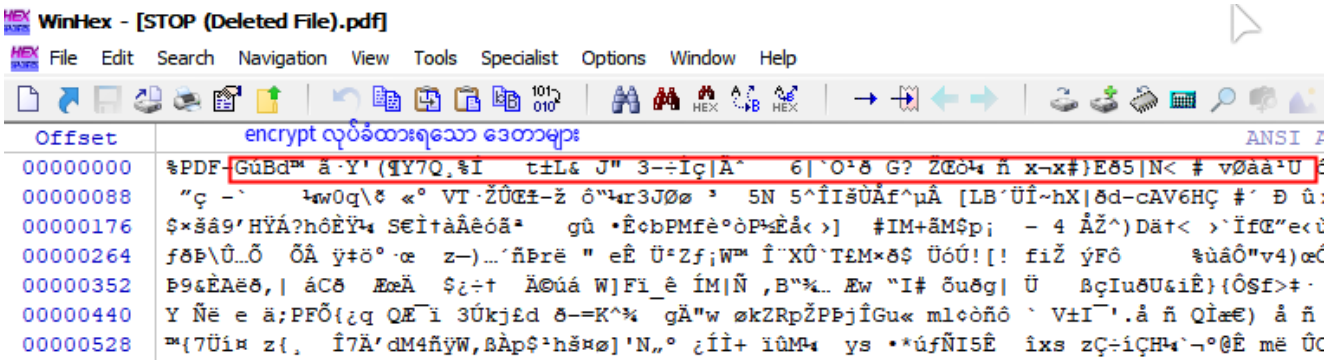
၇။ ၂၀၁၉ ခုနှစ်၊ ဇန်နဝါရီလမှ စက်တင်ဘာလအတွင်း mmCERT သို့ တိုင်ကြားခဲ့သော ဖြစ်စဉ် (၄၂၉)ခုဌ ဖြစ်စဉ်(၁၂၄)ခုတွင်သာ တိုက်ခိုက်ခံရသူများသည် မိမိတို့၏ ဖိုင်များကို ရာနှုန်းပြည့် ပြန်လည်ရရှိခဲ့ပါသည်။ ကျန်တိုက်ခိုက်ခံရမှုများ၌ တိုက်ခိုက်ခံရသူများသည် တိုက်ခိုက်ခံထားရသည့် ဖိုင်များအနက်မှ ဖိုင်အရွယ်အစားကြီးမားသောဖိုင်များကိုသာ ပြန်လည်ဆယ်တင်နိုင်ခဲ့ပါသည်။ တိုက်ခိုက်ခံရမှုများတွင် 8TB ဒေတာသိမ်းဆည်းထားသော NAS Server အားတိုက်ခိုက်ခံရခြင်း၌ ဖိုင်များကို မူလအတိုင်းပြန်လည်ရရှိခဲ့သော်လည်း အချို့သောအဖွဲ့အစည်းများ၊ ရုပ်သံမီဒီယာများ၊ ကုမ္ပဏီကြီးများရှိ ကွန်ပျူတာအများစု၏ ဒေတာပေါင်းများစွာ ဆုံးရှုံးနစ်နာခဲ့ရပြီး အရွယ်အစားကြီးမားသော ဖိုင်အချို့ကိုသာ ပြန်လည်ဆယ်တင် ရရှိနိုင်ခဲ့ပါသည်။

STOP Ransomware အား Antivirus များမှ ထောက်လှမ်းနိုင်မှု

၈။ Ransomware အများစုသည် Trojan Downloader အနေဖြင့် အသွင်ယူကြပြီး Encoded Link များကို အသုံးပြုကြသောကြောင့် Anti-virus များအနေဖြင့် ထောက်လှမ်းမသိရှိနိုင်ပါ။ အချို့သော Website များသည် Antivirus ကို ခေတ္တပိတ်ပေးထားရန် တောင်းဆိုတတ်ကြပြီး ထိုအချိန်တွင် Ransomware များက အလုပ်လုပ်ကြမည် ဖြစ်ပါသည်။ ဖြစ်စဉ်အများစုတွင် တိုက်ခိုက်ခံခဲ့ရသော ကွန်ပျူတာအများစုသည် Microsoft Windows Defender ကိုအသုံးပြုကြပြီး STOP Ransomware က ဦးစွာ Windows Defender ၏ Real-time Protection အား Windows Powershell Script အသုံးပြု၍ ပိတ်လိုက်ပြီး Windows Defender ၏ MpCmdRun.exe ကိုအသုံးပြု၍ Windows Defender ၏ Virus Definition ကို ဖယ်ရှားသဖြင့် Windows Defender မှ STOP Ransomware ကို ထောက်လှမ်း မသိရှိနိုင်တော့ပါ။

၉။ STOP Ransomware စတင်အလုပ်လုပ်ချိန်၌ C:\ Drive အောက်တွင် _readme.txt ဖိုင်တစ်ဖိုင်ကို ဖန်တီးကာ Personal ID ကို ဖန်တီးပါသည်။ ထိုဖိုင်ကို ဖန်တီးချိန်၌ Command & Control Server နှင့် အဆက်အသွယ်ရခဲ့လျှင် Online Key ကို ထုတ်ပေးပြီး အဆက်အသွယ်မရခဲ့လျှင် Offline Key ကို ထုတ်ပေးပါသည်။ Offline Key ဖြင့် တိုက်ခိုက်ခြင်းခံရလျှင် ဖိုင်များကို ရာနှုန်းပြည့် ပြန်လည်ရရှိနိုင်ပြီး Online Key ဖြင့် တိုက်ခိုက်ခံရသူများသည် ၂၀၁၉ ခုနှစ်၊ စက်တင်ဘာလမှစတင်၍ တိုက်ခိုက်သော .coharos, .shariz, .gero, .hese, .xoza, .seto, .peta, .moka, .meds, .kvag, .domn, .karl, .nesa, .boot, .noos, .kuub, .reco, .bora, .leto, .nols, .werd, .coot, .derp, .nakw, .meka, .toec, .mosk, .lokf, .peet, .grod, .mbed, .kodg, .zobm, .rote, .msop, .hets, .righ, .gesd, .merl, .mkos, .nbes, .piny, .redl, .nosu, .kodc, .reha, .topi, .npsg, .btos, .repp, .alka, .bboo, .rooe, .mmnn, .ooss, .mool, .nppp, .rezm, .lokd, .foop, .remk, .npsk, .opqz, .mado, .jope, .mpaj, .lalo, .lezp, .qewe, .mpal, .sqpc, .mzlq, .koti, .covm, .pezi, .zipe, .nlah, .kkll, .zwer .nypd, .usam, .tabe, .vawe, .moba, .pykw, .zida, .maas, .repl, .kuus အမျိုးအစား varaint များဖြင့် တိုက်ခိုက်ခံထားရသူများမှအပ ကျန်သူများသည် ဖိုင်များကို ပြန်လည်ရရှိနိုင်ပါသည်။

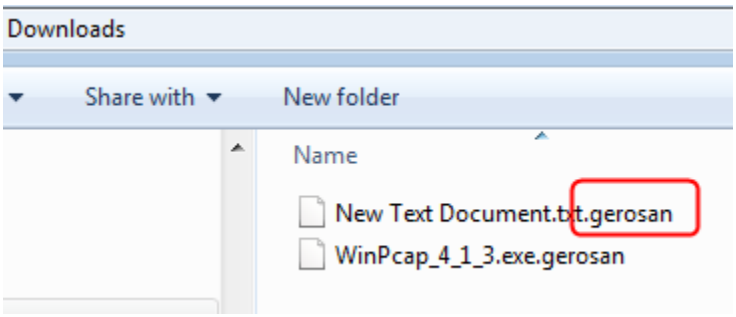
၁၀။ မိမိ၏ကွန်ပျူတာစနစ်တွင် System Restore Point ထားရှိထားပြီး STOP Ransomware က Restore Point အား ဖျက်ဆီးခြင်း မပြုခဲ့လျှင် ဖိုင်များကို ရာနှုန်းပြည့် ပြန်လည်ရရှိနိုင်ပါသည်။ File Repair Tool တစ်ခုခုအသုံးပြု၍ ဖိုင်များကို ပြန်လည်ဆယ်တင်နိုင်သော်လည်း STOP Ransomware က ဖိုင်များကို encrypted လုပ်ပြီးမှ ဖျက်သဖြင့် ဖိုင်များကို recovery/forensics tool များဖြင့် ပြန်လည်ဖော်ယူနိုင်သော်လည်း ဖိုင်များအား ဖွင့်၍ရမည် မဟုတ်ပါ။



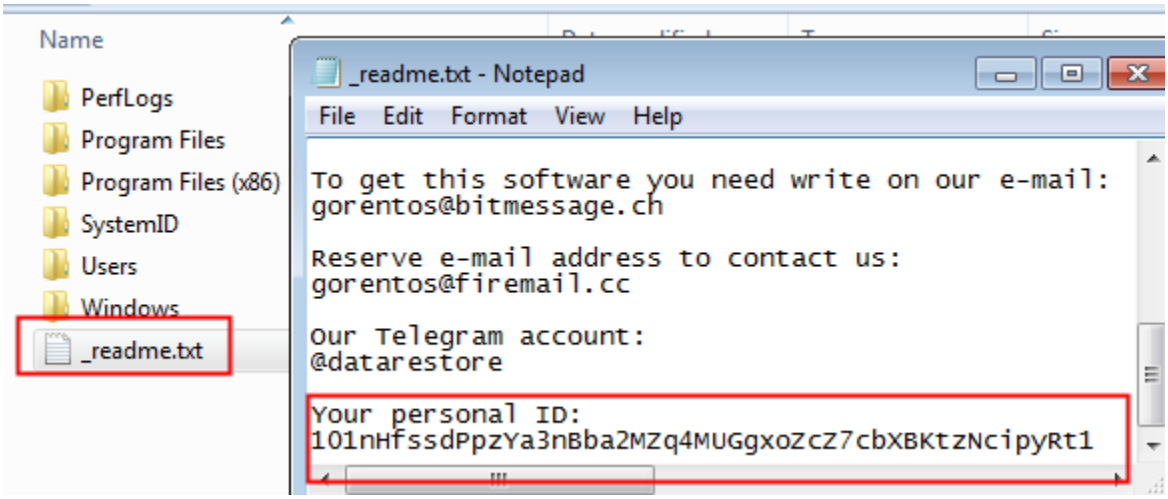
STOP Ransomware တိုက်ခိုက်ခံရလျှင် သတင်းပို့တိုင်ကြားခြင်း

၁၁။ STOP Ransomware တိုက်ခိုက်ခံရလျှင် ခံရချင်း infoteam@mmcert.org.mm နှင့် incident@ncsc.gov.mm တို့ထံသို့ အောက်ပါတို့ကို ပေးပို့ရန် လိုအပ်ပါသည်-

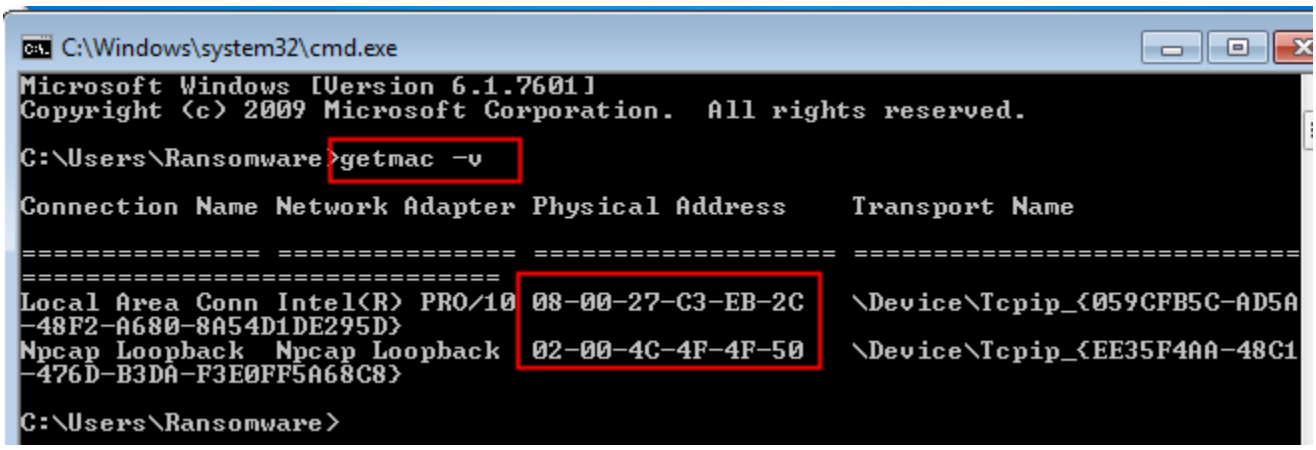
(က) **တိုက်ခိုက်ခံထားရသော ဖိုင်နမူနာတစ်ဖိုင်**။ (ဥပမာ - MS_Word_file.docx.**gerosan**။ gerosan သည် STOP Ransomware မှ သတ်မှတ်လိုက်သော နမူနာဖိုင် extension ဖြစ်ပါသည်။ (**မှတ်ချက်**။ ဓာတ်ပုံရိုက်၍ ပေးပို့ခြင်း မပြုရ။ ထိုဖိုင်ထဲတွင် Key ပါရှိသောကြောင့် ဖြစ်ပါသည်။)



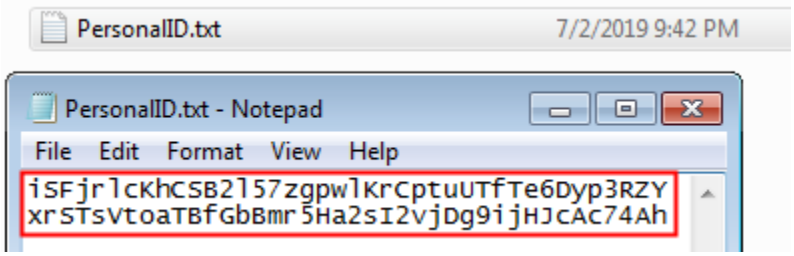
(ခ) **Ransom ငွေတောင်းခံသော ဖိုင်**။ ထိုဖိုင်သည် C:\ drive အောက်နှင့် အခြားသော folder များတွင် _readme.txt ဖိုင်အနေဖြင့် ရှိနေတတ်ပါသည်။ (**မှတ်ချက်**။ ဓာတ်ပုံရိုက်၍ ပေးပို့ခြင်း မပြုရ။ Personal ID အား ပေးပို့ခဲ့သော် ဓာတ်ပုံမှ ပြန်လည်စာရိုက်ရာတွင် အက္ခရာများလွဲနိုင်သောကြောင့် ဖြစ်ပါသည်။)



(ဂ) **တိုက်ခိုက်ခံထားသော ကွန်ပျူတာ၏ MAC Address များ။** (Command Prompt တွင် “getmac -v” command ကို အသုံးပြု၍ ရှာနိုင်ပါသည်။ အခြားနည်းဖြင့် ရရှိသော စုံလင်မှု မရှိသော MAC address များအား ပေးပို့ခြင်း၊ Windows ပြန်တင်ပြီးမှ MAC address ပေးပို့ခြင်း မပြုရ။)



(ဃ) **PersonalID ဖိုင်။** C:\SystemID အောက်တွင် PersonalID.txt ဖိုင် ရှိပါသည်။ Ransomware (၂)ကြိမ်တိုက်ခိုက်ခံရပါက ၎င်းဖိုင်ထဲတွင် Online/Offline key (၂)ခု ရှိတတ်ပါသည်။ ထိုဖိုင်မူရင်းကို ပေးပို့ရန်လိုအပ်ပါသည်။



(ငဂ) **မူရင်းဖိုင်။** မူရင်းဖိုင်ဆိုသည်မှာ တိုက်ခိုက်ခံရသောဖိုင်၏ တိုက်ခိုက်မခံရခင်ဖိုင်ကို ဆိုလိုပါသည်။ ဥပမာ - မူရင်းဖိုင်သည် DC01.jpg ဖိုင်ဖြစ်ပြီး တိုက်ခိုက်ခံရသော ဖိုင်သည် DC01.jpg.besub ဖိုင်ဖြစ်ပါသည်။ Online Key ဖြင့် တိုက်ခိုက်ခံရသူများ

သည် 150KB ထက်ကြီးသော ထိုဖိုင် (၂)ဖိုင်ကို တပြိုင်တည်းပေးပို့ရန် လိုပါသည်။ (မူရင်းဖိုင်ကို Gmail ၏ attachment အနေဖြင့်သော်လည်းကောင်း၊ System Restore လုပ်၍သော်လည်းကောင်း၊ external media ဖိုင်များ အနေဖြင့်သော် လည်းကောင်း ပြန်လည်ရှာဖွေတွေ့ရှိနိုင်ပါသည်။)

STOP Ransomware တိုက်ခိုက်ခံရလျှင် လုပ်ဆောင်ရန်

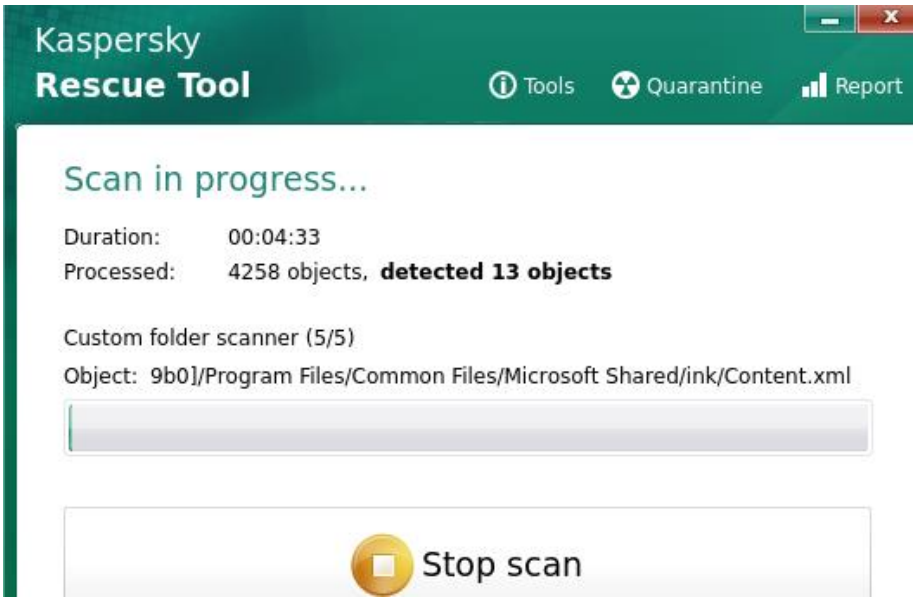
၁၂။ STOP Ransomware တိုက်ခိုက်ခံရလျှင် အောက်ပါတို့ကို လုပ်ဆောင်ရန် လိုအပ်ပါသည်-

(က) ကွန်ပျူတာအား ချက်ချင်း ပိတ်ပစ်လိုက်ပါ။ (Hibernate ပြုလုပ်သင့်ပါသည်။)

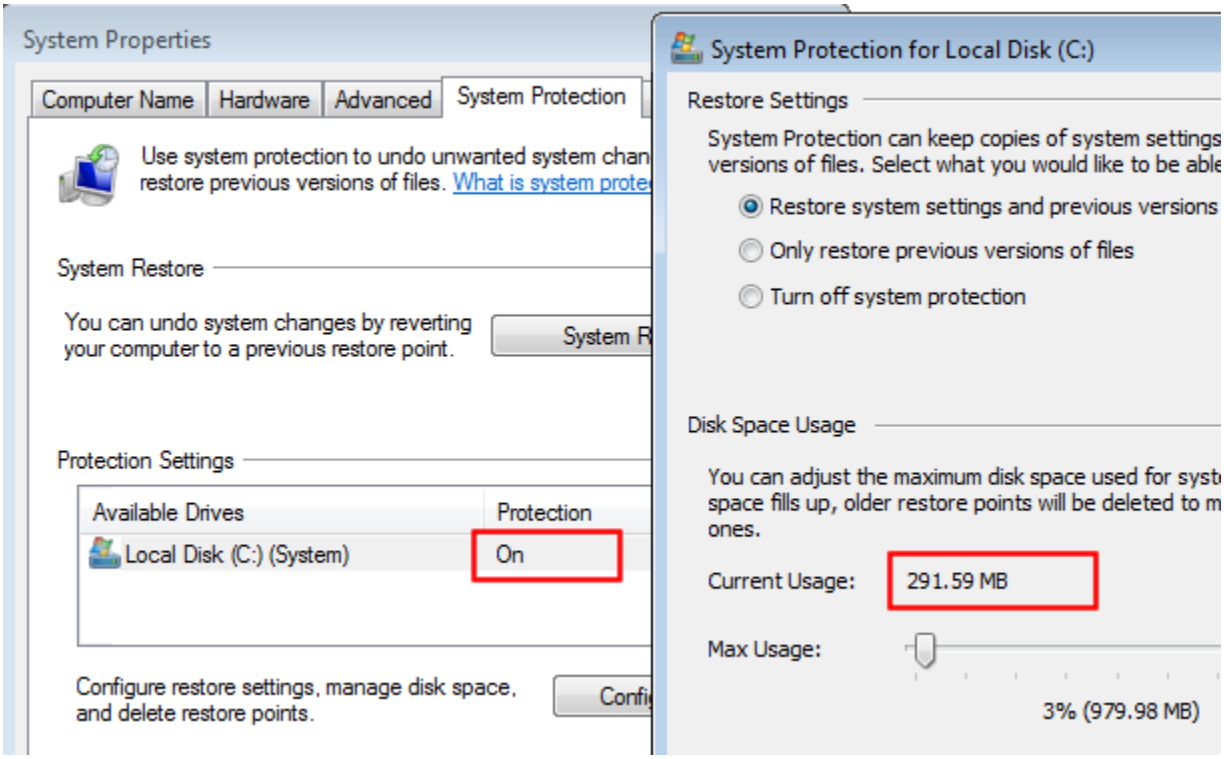
(ခ) အခြားကွန်ပျူတာတစ်ခုဖြင့် Kaspersky Rescue Disk ကို အောက်ပါ link မှ download လုပ်၍ ခွေဘန်းပါ။
https://www.kaspersky.com/downloads/thank-you/free-rescue-disk

(ဂ) Kaspersky Rescue Disk ခွေအား CD Drive တွင်ထည့်ပြီးလျှင် CD Drive အား Boot Option တွင် First Boot ရွေး၍ Boot တက်စေပြီး C:\Users\UserAccount\App Data\Local\xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx Folder အောက်တွင် Ransomware ကို ရှာဖွေ၍ Zip ဖိုင်အနေဖြင့် http://uppit.com တွင် upload လုပ်ပါ။ (ဤ Ransomware ဖိုင်၏ link ကို mmCERT/cc သို့ ပေးပို့နိုင်ပါက Key ကို ပြန်လည် ရရှိရန်အတွက် ပိုမိုအခွင့်အရေးရရှိမည် ဖြစ်ပါသည်။)

(ဃ) Ransomware ကို uppit.com တွင် upload လုပ်ပြီးပါက ကွန်ပျူတာတစ်ခုလုံးရှိ ဖိုင်များကို Kaspersky Rescue Tool အသုံးပြု၍ ဖယ်ရှားရန် လိုအပ်ပါသည်။



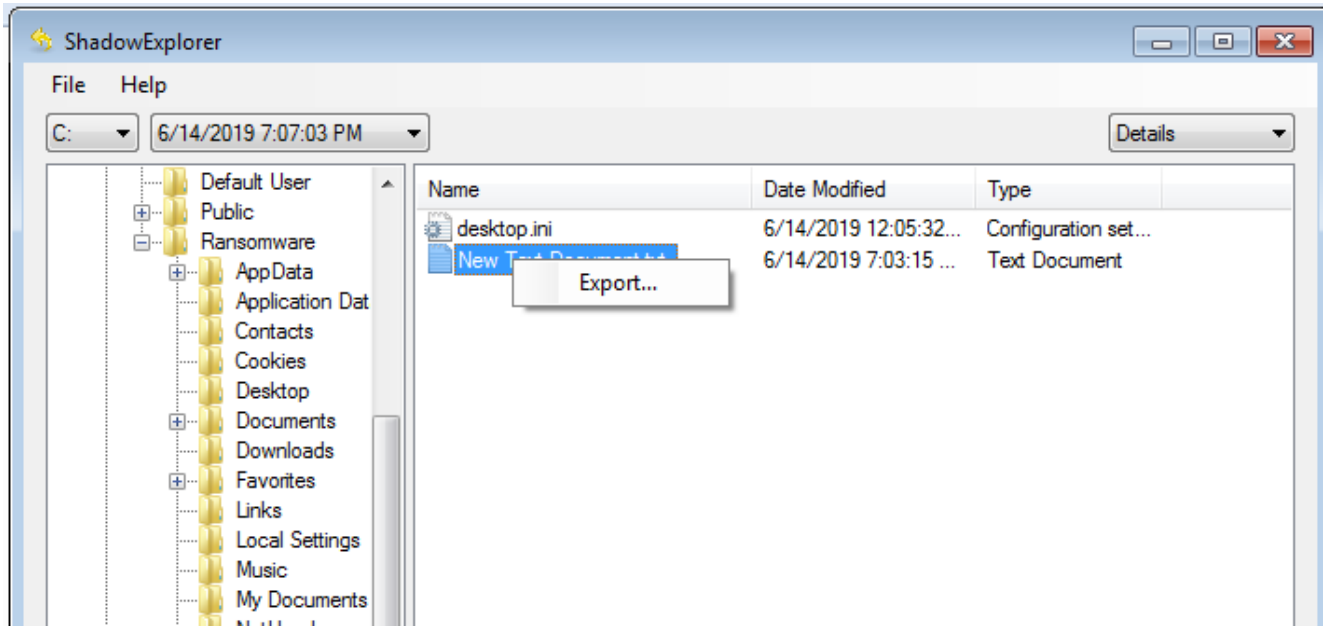
(င) မိမိ၏ System Restore Point များ ဖျက်ဆီးခံရခြင်း ရှိ၊ မရှိ စစ်ဆေးပါ။



(စ) System Restore Point များရှိခဲ့သော် Shadow Explorer Tool ကို အောက်ပါ Link မှ download လုပ်ပါ။ (Shadow Explorer ကို အသုံးပြုရန်အတွက် .NET Framework 3.5 ကို တင်ထားရန် လိုအပ်ပါသည်။)

https://www.shadowexplorer.com/downloads.html

(ဆ) Shadow Explorer မှ မိမိ ပြန်လိုချင်သောဖိုင်ကို ရွေးချယ်၍ ပြန်လည်ဆယ်တင်နိုင်ပါသည်။



(၉) System Restore Point မထားရှိခဲ့လျှင်သော်လည်းကောင်း၊ ဖျက်ဆီးခံရလျှင်သော်လည်းကောင်း File Repair Tool တစ်ခုခုဖြင့် ဖိုင်ပမာဏကြီးမားသော Video ဖိုင်များ၊ Audio ဖိုင်များ၊ PDF များ၊ ZIP ဖိုင်များ၊ RAR ဖိုင်များကို ပြန်လည်ပြုပြင်၍ ဆယ်တင်နိုင်ပါသည်။

အထူးသတိပြုရန်။ STOP Ransomware သည် ဖိုင်များကို encrypt လုပ်ပြီးမှ ဖျက်ပစ်သဖြင့် မည်သည့် recovery tool ဖြင့်မဆို ဖိုင်များကို ပြန်လည်ဆယ်တင်နိုင်မည် မဟုတ်ပါ။

Offline Key ဖြင့် တိုက်ခိုက်ခံရလျှင် လုပ်ဆောင်ရန်

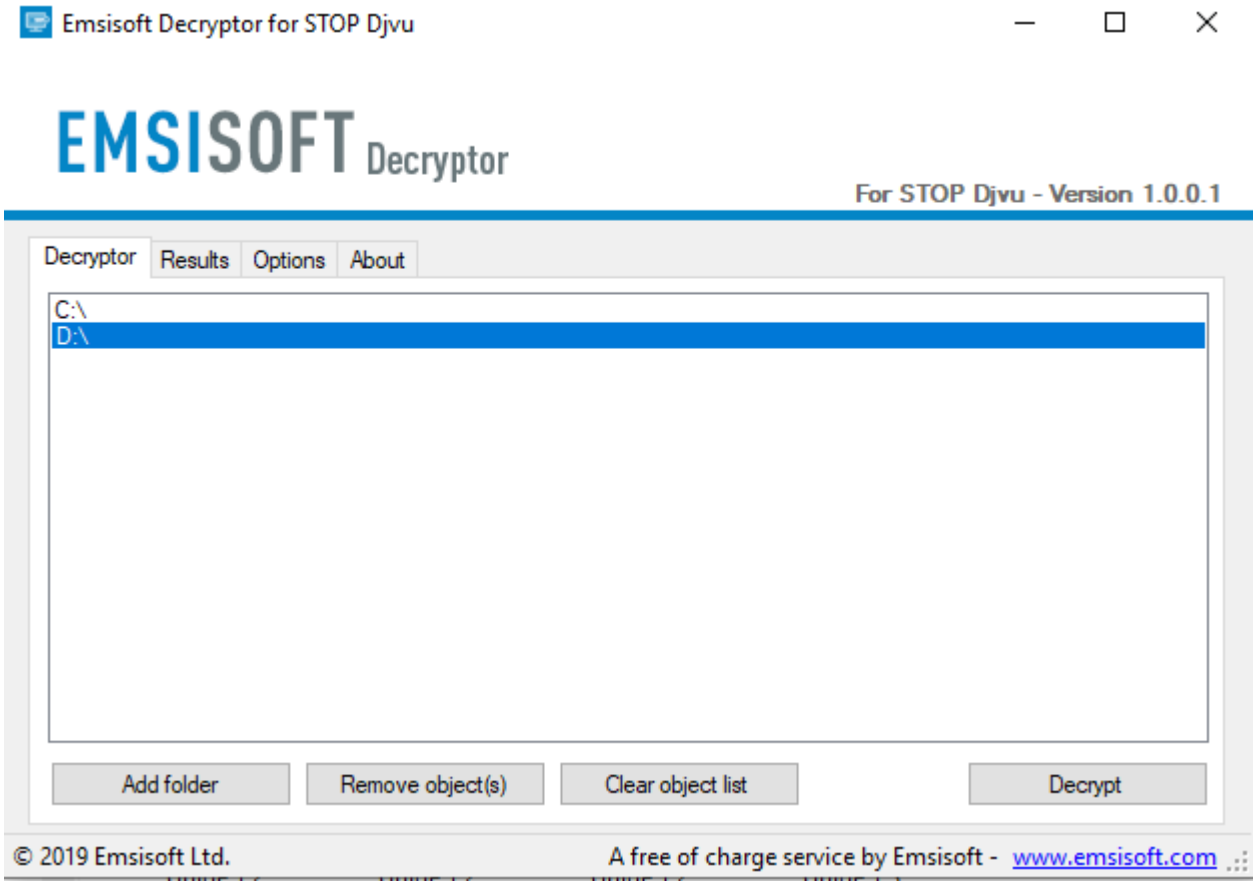
၁၃။ Offline Key ဖြင့် တိုက်ခိုက်ခံရလျှင် အောက်ပါတို့ကို လုပ်ဆောင်ရန် လိုအပ်ပါသည်-

(က) အပိုဒ်(၁၂-က၊ ခ၊ ဂ၊ ဃ) ပါအတိုင်း လုပ်ဆောင်ပါ။

(ခ) STOP Decryptor Tool ကို အောက်ပါ Link မှ download လုပ်ပါ။

https://www.emsisoft.com/ransomware-decryption-tools/download/stop-djvu

(ဂ) တိုက်ခိုက်ခံထားရသော ဖိုင်များရှိရာ Folder ကို ရွေးချယ်၍ decrypt ကိုနှိပ်ပါ။



မှတ်ချက်။ STOP Decryptor ကို Windows 7 တွင် အသုံးပြုမည်ဆိုပါက DotNet Framework 4.5.2 ကို install ပြုလုပ်ထားရန် လိုအပ်ပါသည်။

Onine Key ဖြင့် တိုက်ခိုက်ခံရလျှင် လုပ်ဆောင်ရန်

၁၄။ Online Key ဖြင့် တိုက်ခိုက်ခံရသူများသည် ၂၀၁၉ ခုနှစ်၊ စက်တင်ဘာလမှစတင်၍ တိုက်ခိုက်သော .coharos, .shariz, .gero, .hese, .xoza, .seto, .peta, .moka, .meds, .kvag, .domn, .karl, .nesa, .boot, .noos, .kuub, .reco, .bora, .leto, .nols, .werd, .coot, .derp, .nakw, .meka, .toec, .mosk, .lokf, .peet, .grod, .mbed, .kodg, .zobm, .rote, .msop, .hets, .righ, .gesd, .merl, .mkos, .nbes, .piny, .redl, .nosu, .kodc, .reha, .topi, .npsg, .btos, .repp, .alka, .bboo, .rooe, .mmnn, .ooss, .mool, .nppp, .rezm, .lokd, .foop, .remk, .npsk, .opqz, .mado, .jope, .mpaj, .lalo, .lezp, .qewe, .mpal, .sqpc, .mzlq, .koti, .covm, .pezi, .zipe, .nlah, .kkll, .zwer .nypd, .usam, .tabe, .vawe, .moba, .pykw, .zida, .maas, .repl, .kuus အမျိုးအစား varaint များဖြင့် တိုက်ခိုက်ခံထားရသူများမှအပ ကျန်သူများသည် ဖိုင်များကို Decryptor tool ဖြင့် decrypt လုပ်၍ ဖိုင်များကို ပြန်လည်ရရှိနိုင်ပါသည်။

၁၅။ Vidar Info Stealer သည် ကွန်ပျူတာတွင်းမှ password များအား ခိုးယူသွားပါသဖြင့် မိမိတို့၏ password များကို အမြန်ဆုံး ပြောင်းလဲပစ်ခြင်း၊ multi-factor authentication စနစ်ကို ကျင့်သုံးခြင်း များအား ပြုလုပ်ရပါမည်။ (Vidar Info Stealer နှင့်ပတ်သက်သော အချက်အလက်များကို “**Vidar Info Stealer လမ်းညွှန်**” တွင် ဖတ်ရှုနိုင်ပါသည်။)

STOP Ransomware တိုက်ခိုက်မှုမှ ကာကွယ်ခြင်း

၁၆။ STOP Ransomware တိုက်ခိုက်မှုမှ ကာကွယ်ရန်အတွက် အောက်ပါအချက်များကို လိုက်နာ ရန် လိုအပ်ပါသည်-

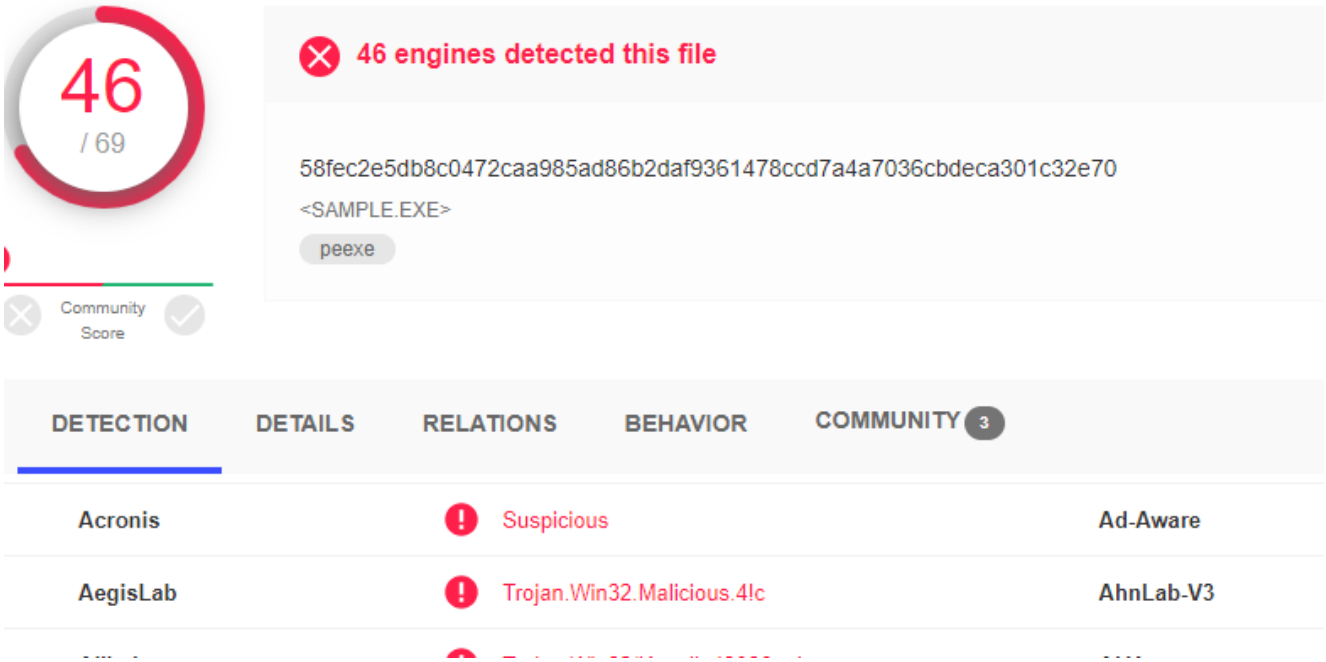
(က) Microsoft Windows တွင် ပါရှိသော Windows Defender တစ်ခုတည်းအား အသုံးပြု ခြင်းအစား အခြားသော Antivirus များ (ESET၊ Kaspersky၊ BitDefender စသည်)ကို အသုံးပြုရန် လိုအပ်ပြီး Virus definition များကို နောက်ဆုံးအခြေအနေအထိ update ပြုလုပ်ထားရန် လိုအပ်ပါသည်။

(ခ) မည်သည့်အကြောင်းရင်းဖြင့်မျှ Antivirus ကို မပိတ်ရ။ (Ransomware အများစုသည် Antivirus များကို ခေတ္တပိတ်ထားပေးရန် တောင်းဆိုတတ်ပါသည်။)

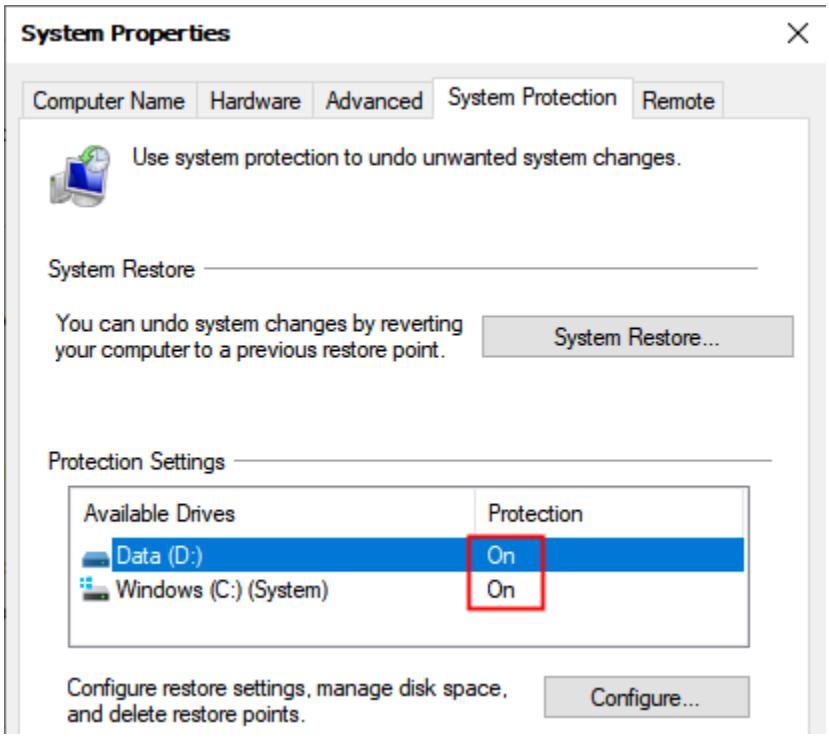
(ဂ) မယုံကြည်ရသော website များမှ မလိုအပ်ဘဲ ဖိုင်များကို download လုပ်ခြင်း မပြုရ။

(ဃ) Windows Acitvator၊ Crack ဖိုင်၊ Keygen ဖိုင်များ download လုပ်ထားခဲ့သည်ရှိသော် ထိုဖိုင်များကို www.virustotal.com သို့မဟုတ် www.hybrid-analysis.com တို့တွင် Malware ဟုတ်၊ မဟုတ် သေချာစွာ စစ်ဆေးရန် လိုအပ်ပါသည်။ ထိုထက်ပိုမိုစိတ်ချ

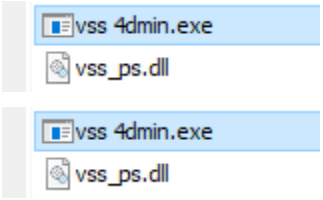
ရစေရန် VirtualBox နှင့် VMWare တို့တွင် Windows တစ်ခုခုအား Virtual Machine အနေဖြင့်စမ်းသပ်သုံးစွဲသင့်ပါသည်။



(c) System Restore Point ကို Volume Drive အားလုံးတွင် ထားရှိသင့်ပါသည်။



(ဈ) Ransomware မှ System Restore Point အား delete လုပ်၍ မရနိုင်စေရန်အတွက် C:\Windows\System32 အောက်ရှိ vssadmin.exe အား အခြားဖိုင်အမည် ပြောင်းလဲ ထားရပါမည်။



(ဆ) အရေးကြီးသော ဖိုင်များကို အခြားသော external storage များတွင် သိမ်းဆည်းခြင်း၊ Cloud တွင် သိမ်းဆည်းခြင်းမျိုး ပြုလုပ်ပါ။

(ဇ) အဖွဲ့အစည်းအတွင်း STOP Ransomware နှင့်ပတ်သက်၍ အသိပညာပေး ဆွေးနွေးမှုမျိုး လုပ်ဆောင်ပါ။

မှတ်ချက်။ ဤလမ်းညွှန်စာစောင်တွင်ပါရှိသော လမ်းညွှန်ချက်များသည် STOP Ransomware အတွက်သာ ဖြစ်ပြီး STOP Ransomware (.gerosan မျိုးကွဲ၊ .davda မျိုးကွဲ၊ .muslat မျိုးကွဲ၊ .besub မျိုးကွဲ၊ .lokas မျိုးကွဲ၊ .godes မျိုးကွဲ၊ .budak မျိုးကွဲ၊ .gero မျိုးကွဲ၊ .maas မျိုးကွဲနှင့် .repl မျိုးကွဲ) များအား စုံစမ်းစစ်ဆေး၍ တွေ့ရှိချက်များအပေါ် ပြုစုရေးသားထားခြင်းဖြစ်ပါသည်။ STOP Ransomware မဟုတ်သည့် အခြားသော Ransomware များအတွက်မူ လုပ်ဆောင်ချက်များသည် သဘောသဘာဝ ကွဲပြားခြားနားမှုများ ရှိနေနိုင်ပါသည်။ Ransomware (၂)မျိုး တပြိုင်နက်တည်း တိုက်ခိုက်ခံထားရခြင်း၊ Malware မြောက်မြားစွာ တပြိုင်နက်တည်း တိုက်ခိုက်ခံထားရခြင်းကဲ့သို့ အထူးဖြစ်စဉ်များသည် ဤလမ်းညွှန်ချက်တွင် အကျုံးမဝင်ပါ။

၁၇။ Ransomware တိုက်ခိုက်ခံရမှုနှင့် ပတ်သက်၍ အသေးစိတ်မေးမြန်းလိုပါက ၀၆၇-၃၄၂၂၂၇၂ သို့ ဖုန်းဆက်မေးမြန်းနိုင်ပြီး တိုက်ခိုက်ခံထားရသော ကွန်ပျူတာများကို စစ်ဆေးခံလိုပါက အမျိုးသားဆိုက်ဘာလုံခြုံရေးဗဟိုဌာန၊ S12 Exchange Building၊ ဇမ္ဗူကျက်သရေလမ်း၊ ဇမ္ဗူသီရိမြို့နယ်တွင် လာရောက်စစ်ဆေးနိုင်ပါကြောင်း အသိပေးအပ်ပါသည်။

မြန်မာနိုင်ငံကွန်ပျူတာအရေးပေါ်တုံ့ပြန်ရေးအဖွဲ့ (mmCERT/cc)

Reference

https://www.bleepingcomputer.com/forums/t/671473/stop-ransomware-stop-puma-djvu-promo-drume-help-support-topic/

https://www.bleepingcomputer.com/news/security/stop-ransomware-installing-password-stealing-trojans-on-victims/

https://twitter.com/demonslay335/status/1106322805791035393

https://app.any.run/tasks/5ba4be48-c19f-4fd6-bed2-23d58664dd8f/

https://app.any.run/tasks/4cee1b2c-d0f9-49c7-9941-47c10670a824/

https://www.bleepingcomputer.com/news/security/fake-vpn-site-pushes-cryptbot-and-vidar-info-stealing-trojans/

ထုတ်ဝေခြင်း

ပထမအကြိမ် ထုတ်ဝေခြင်း (၂၀၁၉ ခုနှစ်၊ ဇွန်လ ၁၅ ရက်)

ဒုတိယအကြိမ် ဖြည့်စွက်ထုတ်ဝေခြင်း (၂၀၁၉ ခုနှစ်၊ ဇွန်လ ၁၇ ရက်)

တတိယအကြိမ် ဖြည့်စွက်ထုတ်ဝေခြင်း (၂၀၁၉ ခုနှစ်၊ ဇူလိုင်လ ၁၇ ရက်)

စတုတ္ထအကြိမ် ဖြည့်စွက်ထုတ်ဝေခြင်း (၂၀၁၉ ခုနှစ်၊ နိုဝင်ဘာ ၆ ရက်)

ပဉ္စမအကြိမ် ဖြည့်စွက်ထုတ်ဝေခြင်း (၂၀၂၀ ပြည့်နှစ်၊ ဇူလိုင်လ ၂၁ ရက်)