

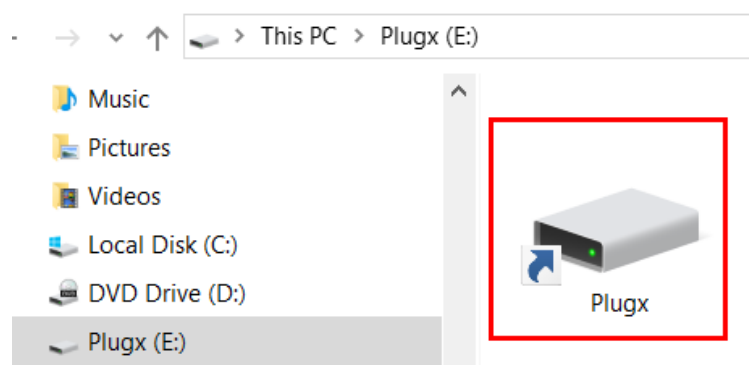
PlugX Remote Access Trojan (RAT) ဖယ်ရှား ရှင်းလင်းနည်းလမ်းညွှန်

PlugX RAT ၏ သမိုင်းကြောင်း

၁။ တရုတ်နိုင်ငံအခြေပြု ဟက်ကာအဖွဲ့ဖြစ်သော Mustang Panda သည် ၂၀၁၂ ခုနှစ်မှစ၍ အာရှ-ပစိဖိတ်ဒေသတွင်း နိုင်ငံများအား ပစ်မှတ်ထား၍ ဆိုက်ဘာတိုက်ခိုက်လျက်ရှိပြီး သတင်း အချက်အလက်များကို ခိုးယူရန် ကြိုးစားလျက်ရှိကာ ၂၀၁၉ ခုနှစ်တွင် မြန်မာနိုင်ငံကို ပစ်မှတ်ထား၍ PlugX RAT ဖြင့် တိုက်ခိုက်ရန်ကြိုးစားလျက်ရှိပြီး မြန်မာနိုင်ငံအတွင်းရှိ ကွန်ပျူတာ အများစုသည် PlugX RAT ၏ တိုက်ခိုက်ခြင်းခံရလျက်ရှိပါသည်။

PlugX ၏ စတင်ပျံ့နှံ့ပုံနှင့် အလုပ်လုပ်ပုံ

၂။ PlugX မျိုးကွဲများသည် မူလအစတွင် Phishing Mail များမှတစ်ဆင့် Attachment ဖိုင်များ အနေဖြင့် ရောက်ရှိလာခြင်းဖြစ်ပြီး Email လက်ခံရရှိသူသည် အဆိုပါ Attachment ဖိုင်ကို ဖွင့်မိရာမှ Attachment တွင်ပါလာသော အဖျက်အမှောင့်ကုဒ်များမှ စတင်အလုပ်လုပ်ပြီး ကွန်ပျူတာတွင် ခြေကုပ်ယူပါသည်။ ထို့နောက်ကွန်ပျူတာသို့ လာရောက်ချိတ်ဆက်သော Memory Stick နှင့် External Hard Disk ကဲ့သို့ External Storage Devices များထံသို့ ကူးစက်ကာ အခြား ကွန်ပျူတာများထံသို့ ပျံ့နှံ့ရန် ကြိုးစားပါသည်။ PlugX သည် Memory Stick ကဲ့သို့သော External Storage Devices များတွင် ကူးစက်ခံထားရလျှင် Shortcut ဖိုင် (.lnk ဖိုင်) အနေဖြင့် ပုံ(၁)ပါအတိုင်း အယောင်ဆောင်ထားမည် ဖြစ်သည်။ အချို့သော PlugX မျိုးကွဲများတွင် Disk Icon အယောင်ဆောင်ထားသော .exe ဖိုင်အဖြစ် တွေ့နိုင်ပါသည်။



ပုံ(၁)- PlugX RAT မှတိုက်ခိုက်ပြီးသော Storage Device တွင် Shortcut အယောင်ဆောင်ထားသောဖိုင်အဖြစ် တွေ့မြင်ရပုံ

၃။ အဆိုပါ PlugX ကူးစက်ခံထားရသော Memory Stick ကို ကွန်ပျူတာနှင့်ချိတ်ဆက် အသုံးပြု သည့်အခါ ၎င်း Shortcut ဖိုင်ကိုဖွင့်မိပါက ကွန်ပျူတာ၏ C:\ProgramData\AAM Updates\lms

Folder အောက်တွင် AAM Updates.exe၊ hex.dll နှင့် adobeupdate.dat ဖိုင်ကိုဖန်တီးမည် ဖြစ်ပါသည်။ AAM Updates.exe သည် Symantec ဆိုက်ဘာလုံခြုံရေး ကုမ္ပဏီမှ Sign လုပ်ထားသော Adobe CEF Helper ဖြစ်ပြီး ၎င်းဖိုင်မှ DLL Hijacker ဖြစ်သော hex.dll ဖိုင်ကိုဖွင့်ကာ ၎င်းမှတစ်ဆင့် Encrypted လုပ်ထားသော Payload ဖြစ်သည့် adobeupdate.dat ကို ဖွင့်မည်ဖြစ်ပါသည်။ PlugX သည် တိုက်ခိုက်ခံရသော ကွန်ပျူတာမှ Microsoft Word ဖိုင်များ (.doc နှင့် .docx)၊ Microsoft Powerpoint ဖိုင်များ (.ppt, .pptx)၊ Microsoft Excel ဖိုင်များ (.xls, .xlsx) နှင့် Adobe Acrobat ဖိုင်များ (.pdf) တို့ကို ခိုးယူကာ အမိန့်ပေးထိန်းချုပ်ရေးဆာဗာ (Command and Control (C2C) Server) များသို့ ဒေတာများပေးပို့ပါသည်။ ထိုသို့ အမိန့်ပေးထိန်းချုပ်ရေးဆာဗာများ ထံသို့ ဒေတာများပေးပို့ရန် နှင့် ၎င်း၏ အမိန့်ပေးထိန်းချုပ်ရေးဆာဗာများနှင့် လွတ်လပ်စွာ ဆက်သွယ်နိုင်စေရန်အတွက် Windows ၏ Firewall Setting များကို ပြင်ဆင်မည် ဖြစ်ပါသည်။

၄။ PlugX RAT သည် မျိုးကွဲများမတူသည့်အလျောက် ၎င်းတို့၏ အမိန့်ပေးထိန်းချုပ်ရေးဆာဗာများ သည်လည်း မတူညီကြောင်းကိုတွေ့ရပါသည်။ ၎င်းတို့၏ အမိန့်ပေးထိန်းချုပ်ရေးဆာဗာများမှာ အောက်ပါအတိုင်း ဖြစ်ပါသည်-

- (က) 45.251.240.55 (AAMupdates.exe)
- (ခ) 42.99.117.95 (AAMupdates.exe)
- (ဂ) 45.134.83.41 (AcroRd32.exe)
- (ဃ) 217.26.61.158 (fsguidll.exe) (unisers.com)
- (င) 27.133.148.196 (unsecapp.exe) (www.apple-net.com)
- (စ) 167.88.180.11 (unsecapp.exe) (www.mmfhlele.com)

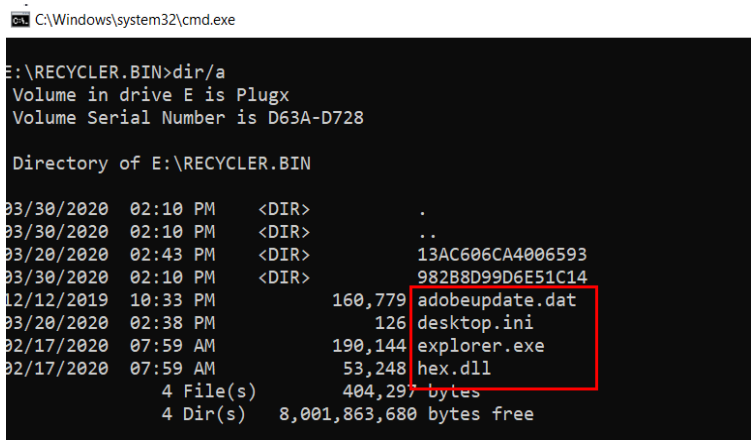
၅။ အထက်ဖော်ပြပါ C2C Server မှ တိုက်ခိုက်ခံရသော ကွန်ပျူတာအား ဝင်ရောက်ကာ မိမိ၏ Credential များအား ခိုးယူနိုင်ခြင်း၊ Memory Stick များကို ကွန်ပျူတာတွင် လာရောက်တပ်ဆင်ပါက Encryption စနစ်ဖြင့် ဝှက်ထားသော ဖိုင်များကို Memory Stick ၏ RECYCLER.BIN Folder အောက်ရှိ CLSID နံပါတ်ပေးထားသော Folder အောက်တွင် သိမ်းဆည်းခြင်း၊ တိုက်ခိုက် ခံရသူ၏ ကွန်ပျူတာနှင့် ပတ်သက်သော အချက်အလက်များ၊ အသုံးပြုလျက်ရှိနေသော Port များ၊ အလုပ်လုပ်နေသော Services နှင့် ပရိုဂရမ်များကို မှတ်တမ်းတင်ခြင်းတို့ကို ပြုလုပ်ပါသည်။

၆။ PlugX RAT သည် တိုက်ခိုက်ပြီးသော ကွန်ပျူတာနှင့် Storage Device များတွင် Hidden ဖိုင်များ၊ Hidden Folder များကို ဖန်တီးရယူပြီး ကွန်ပျူတာတွင် Background Process များအနေဖြင့် အလုပ်လုပ်ကာ

ဒေတာများကို ခိုးယူပါသည်။ ၎င်းမှ ဖန်တီးထားသော Hidden ဖိုင်များ၊ Hidden Folder များကို အောက်ပါနေရာများတွင် တွေ့ရှိနိုင်ပါသည်-

- (က) C:\ProgramData\AAM Updates\
- (ခ) C:\Users\[User Name]\ AAM Updates\
- (ဂ) [Storage Device's Logical Drive]\RECYCLER.BIN\ (သို့မဟုတ်)
 [Storage Device's Logical Drive]\RECYCLERS.BIN\
- (ဃ) HK Current User\Software\Microsoft\Windows\Current Version\Run
 (Registry တွင် Persistent အဖြစ် သတ်မှတ်ခြင်း)

၇။ အကယ်၍ အင်တာနက်မှတစ်ဆင့် C2 ဆာဗာသို့ ချိတ်ဆက်၍မရခဲ့လျှင် ၎င်းတို့ခိုးယူမည့် ဖိုင်များကို Memory Stick ကဲ့သို့သော External Storage Devices များ၏ RECYCLER.BIN (သို့မဟုတ်) RECYCLERS.BIN folder အောက်တွင် သိမ်းဆည်းမည်ဖြစ်ပါသည်။ ခိုးယူထားသော ဖိုင်များကို CLSID တန်ဖိုးများဖြင့် တည်ဆောက်ထားသော Folder အောက်တွင် ဖွက်၍ သိမ်းဆည်းမည် ဖြစ်ပါသည်။ ၎င်းဖိုင်များကို Command Prompt မှ ခေါ်ယူ၍သာ ကြည့်နိုင်မည် ဖြစ်ပါသည်။ ပုံ(၂)



ပုံ(၂)- တိုက်ခိုက်မည့် PlugX ဖိုင်သည် External Storage Device ၏ RECYCLER.BIN\ အောက်တွင် explorer.exe (သို့မဟုတ်) AAMupdates.exe အနေဖြင့် ပုန်းအောင်းနေမည်ဖြစ်ပါသည်။

PlugX RAT မျိုးကွဲများ၏ ယေဘုယျ လက္ခဏာများ

၈။ PlugX RAT သည် မျိုးကွဲတစ်ခုနှင့်တစ်ခုအပေါ်မူတည်၍ File Name များ မတူညီသော်လည်း အောက်ပါ ဖိုင်အမျိုးအစား(၃)ခုကို အပိုဒ်(၆)တွင် ဖော်ပြခဲ့သည့်နေရာများ၏ Folder တစ်ခုချင်းစီ အောက်တွင် ဖန်တီးပါသည်-

- (က) တရားဝင် Signed လုပ်ထားသောဖိုင် (ဥပမာ- AAM Update.exe)၊

- (ခ) Signed လုပ်ထားသောဖိုင်မှ ခေါ်ယူအသုံးပြုသည့် DLL ဖိုင် (ဥပမာ- hex.dll)၊
- (ဂ) Dll ဖိုင်မှ ခေါ်ယူအသုံးပြုမည့် အန္တရာယ်ရှိသော ကုဒ်များပါဝင်သည့် binary (payload) ဖိုင် (ဥပမာ- Adobeupdate.dat)။

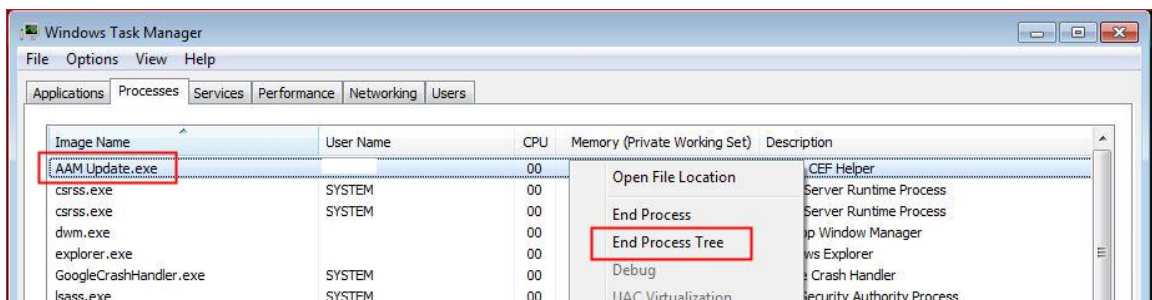
၉။ အမျိုးသားဆိုက်ဘာလုံခြုံရေးဗဟိုဌာန၏ Malware Analysis ပြုလုပ်ချက်များအရ ဖော်ပြပါ PlugX RAT မျိုးကွဲများအား စစ်ဆေးတွေ့ရှိရပါသည်-

PlugX မျိုးကွဲများ	Sign လုပ်ထားသောဖိုင်	Dll ဖိုင်	Payload ဖိုင်	Registry တွင် Persistent ထားရှိသော အမည်နှင့် တည်နေရာ
Adobe CEF Helper	AAM Update.exe	hex.dll	Adobeupdate.dat	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run (AAM UpdatevIm)
ESET HTTP Server Service	unsecapp.exe	http_dll.dll	http_dll.dat	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run (Microsoft Malware ProtectionOr)
F-Secure GUI component	fsguidll.exe	fslapi.dll	fslapi.dll.gui	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run (QgBtBbK)

PlugX RAT အား တိုက်ခိုက်ခံထားရသော ကွန်ပျူတာမှ ရှင်းလင်းဖယ်ရှားခြင်း

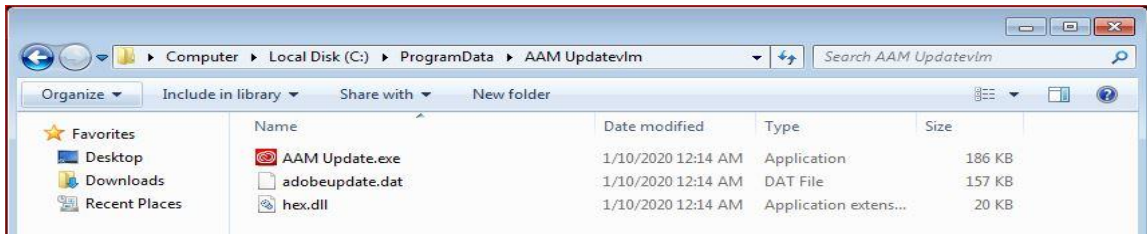
၁၀။ PlugX RAT တိုက်ခိုက်ခံထားရသော ကွန်ပျူတာမှ PlugX RAT အား ရှင်းလင်းပုံအဆင့်အဆင့်မှာ အောက်ပါအတိုင်းဖြစ်ပါသည်-

- (က) ပထမဦးစွာ ပုံ(၃)ပါအတိုင်း မိမိကွန်ပျူတာတွင် အလုပ်လုပ်လျက်ရှိနေသော PlugX RAT ၏ Process (AAM Updates.exe) ကို Task Manager မှ End Process Tree လုပ်ပါ။



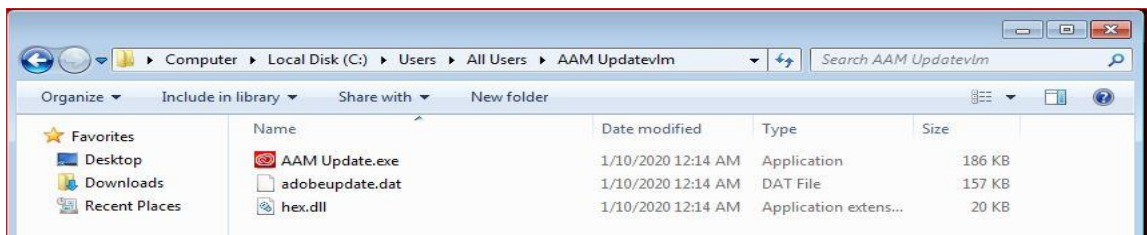
ပုံ(၃)- Task Manager တွင် အလုပ်လုပ်လျက်ရှိသော PlugX RAT ၏ Process အား ရပ်ဆိုင်းခြင်း

- (ခ) PlugX RAT သည် တိုက်ခိုက်ခံရသောကွန်ပျူတာတွင် ခြေကုပ်ရယူရန်အတွက် ပုံ(၄)တွင် ဖော်ပြထားသောနေရာတွင် ဖိုင်(၃)ဖိုင်ကို ဖန်တီးသည့်အတွက် C:\ProgramData\ folder အောက်ရှိ AAM UpdatevIm Folder အောက်ရှိ AAM Update.exe၊ hex.dll နှင့် adobeupdate.dat ဖိုင်များကို ဖျက်ရမည်။



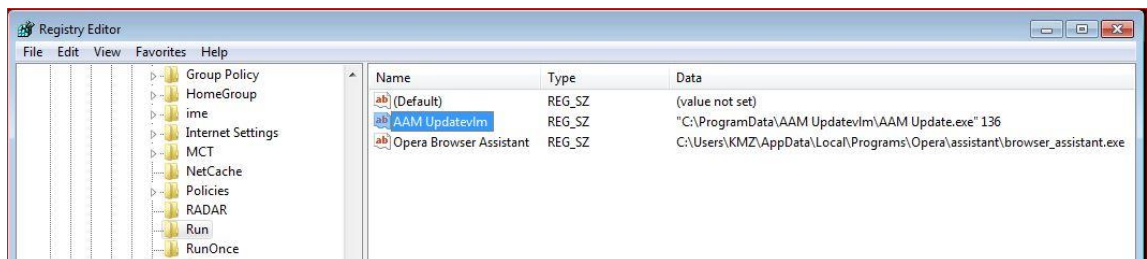
ပုံ(၄)- C:\ProgramData\ folder အောက်တွင် PlugX RAT မှ ဖန်တီးထားသော ဖိုင်များ

- (ဂ) အချို့ PlugX RAT မျိုးကွဲများသည် ပုံ(၅)တွင်ဖော်ပြထားသည့်အတိုင်း C:\Users\All Users Folder အောက်ရှိ AAM UpdatevIm Folder တွင်လည်း ၎င်း၏ဖိုင်(၃)ခုအား သွားရောက်ဖန်တီးသည်ကို တွေ့ရသည့်အတွက် ၎င်း Location အောက်တွင်ရှိသော AAM Update.exe၊ hex.dll နှင့် adobeupdate.dat ဖိုင်များကိုလည်း ဖျက်ပေးရမည်။



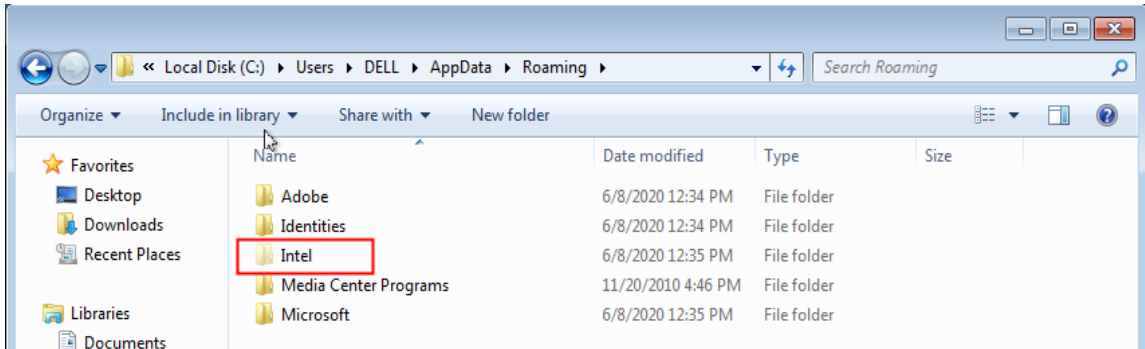
ပုံ(၅)- C:\Users\All Users Folder အောက်တွင် PlugX RAT မှ ဖန်တီးထားသော ဖိုင်များ

- (ဃ) PlugX RAT သည် ကွန်ပျူတာထဲတွင် အမြဲတမ်းအလုပ်လုပ်နေစေရန် အတွက် Registry ထဲရှိ HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\Run\ အောက်တွင် AAM UpdatevIm အမည်နှင့် ဖန်တီးထားသည်ကို တွေ့ရမည်ဖြစ်ပြီး ၎င်းကိုလည်း ဖျက်ပေးရန် လိုအပ်ပါသည်။



ပုံ(၆)- Registry အောက်တွင် အမြဲအလုပ်လုပ်ရန်အတွက် PlugX RAT မှ Run Key ဖန်တီးထားပုံ

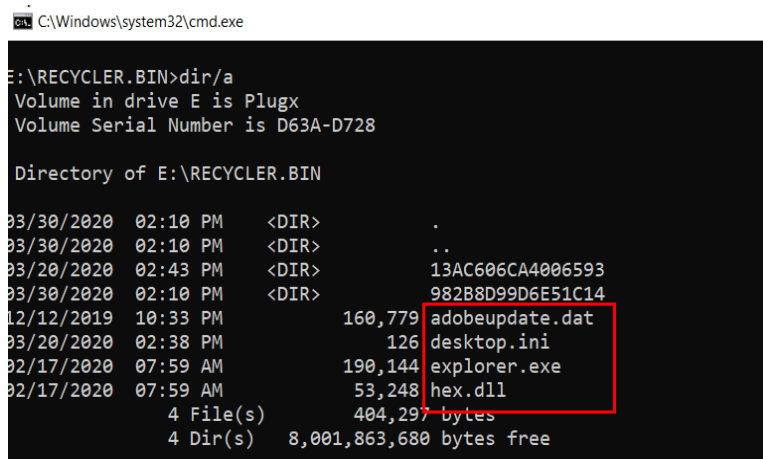
- (c) ခိုးယူမည့်ဖိုင်များကို C:\Users\[UserName]\AppData\Roaming\Intel\[CLSID] အောက်တွင် သိမ်းထားခြင်းဖြစ်သဖြင့် ၎င်းFolderကိုလည်း ဖျက်ပေးရန်လိုအပ်ပါသည်။



ပုံ(၇)- တိုက်ခိုက်ခံထားရသောကွန်ပျူတာမှ ဒေတာများကို C2C Server သို့ပေးပို့ရန် ယာယီထားရှိထားသောနေရာ

PlugX RAT အား တိုက်ခိုက်ခံထားရသော Storage Devices များမှ ရှင်းလင်းဖယ်ရှားခြင်း

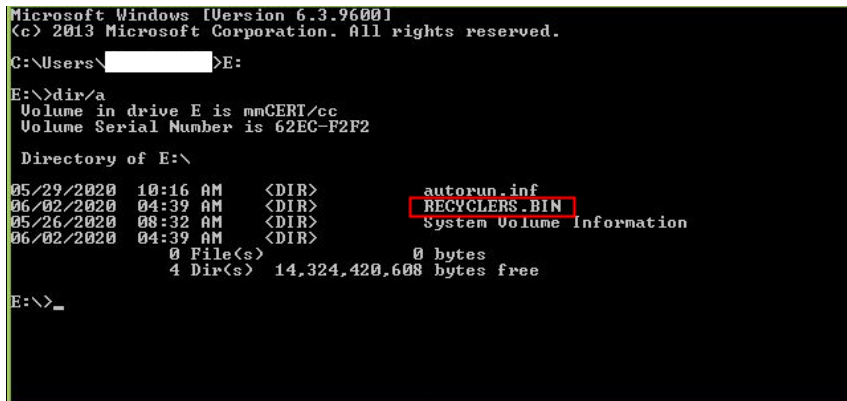
၁၂။ PlugX RAT သည် တိုက်ခိုက်ခံရသောကွန်ပျူတာမှ C2C Server ထံသို့ အင်တာနက်မှတစ်ဆင့် ချိတ်ဆက်၍မရခဲ့လျှင် ၎င်းတို့ခိုးယူမည့်ဖိုင်များကို Memory Stick ကဲ့သို့သော External Media များ၏ RECYCLER.BIN (သို့မဟုတ်) RECYCLERS.BIN Folder အောက်တွင် သိမ်းဆည်းမည်ဖြစ်ပြီး C2C Server နှင့် ချိတ်ဆက်မိသည့်အခါတွင်မှ ဒေတာများကို ပေးပို့မည်ဖြစ်သည်။ PlugX RAT အား တိုက်ခိုက်ခံရသော Storage Device များမှ ဖယ်ရှားရန်အတွက် ပုံ(၈)တွင်ပြထားသည့် Location တွင် သွားရောက်ဖျက်ပေးရမည်ဖြစ်သည်။



ပုံ(၈)- Storage Device များအတွင်းတွင် PlugX RAT မှ ဖန်တီးထားသော ဖိုင်များ

၁၃။ တိုက်ခိုက်ခံထားရသော Storage Device များမှ PlugX RAT အား ဖယ်ရှားပုံအဆင့်ဆင့်မှာ အောက်ပါအတိုင်းဖြစ်ပါသည်-

- (က) Windows ၏ Run Box မှတစ်ဆင့် Command Prompt (cmd.exe) ကို ခေါ်ယူကာ မိမိကွန်ပျူတာက တပ်ဆင်အသုံးပြုထားသော Storage Device အတွက် ဖော်ပြပေးသော Drive အတွင်းသို့ ဝင်ရောက်ပါ။
- (ခ) ထို့နောက် “dir/a” Command ကိုအသုံးပြုကာ Storage Device အတွင်းတွင် မည်သည့် Folder များ ရှိသည်ကို စစ်ဆေးပါ။ ထိုသို့ စစ်ဆေးရာတွင် RECYCLER.BIN (သို့မဟုတ်) RECYCLERS.BIN ကို တွေ့ရှိပါက ၎င်း Storage Device သည် PlugX RAT တိုက်ခိုက်ခံထားရပြီး ဖြစ်ပါသည်။



ပုံ(၉)- PlugX RAT တိုက်ခိုက်ခံထားရသော Storage Device တွင် RECYCLERS.BIN အား မြင်တွေ့ရပုံ

- (ဂ) “cd RECYCLERS.BIN” command ကိုအသုံးပြု၍ RECYCLERS.BIN (သို့မဟုတ်) RECYCLER.BIN အတွင်းသို့ဝင်ရောက်၍ “dir/a” Command ကို အသုံးပြုပြီး အတွင်းရှိ ဖိုင်များကို စစ်ဆေးပါ။ ထိုသို့စစ်ဆေးရာတွင် ပုံ(၁၀)တွင် ဖော်ပြထားသည့်အတိုင်း AdobeUpdate .exe (သို့မဟုတ်) အချို့မျိုးကွဲများတွင် explorer.exe၊ hex.dll နှင့် adobeupdate.dat ဖိုင်တို့ကို တွေ့ရမည်ဖြစ်သည်။ ထိုသို့တွေ့ရှိရပါက command prompt မှ “del *.*” Command ကို အသုံးပြု၍ ဖိုင်များအားလုံးကို ဖျက်ပေးရမည်။ “del *.*” Command နှင့် ဖိုင်များကို ဖျက်သည့်အခါ ဖိုင်များကို ဖျက်၊ မဖျက် Are you sure (Y/N)? ဟုမေးလျှင် “y” ကိုရွေးချယ်ပြီး ဖျက်ပေးရမည်။ ပြီးလျှင် ဖိုင်များကျန်ရှိနေခြင်း မရှိစေရန် “dir/a” command ကို အသုံးပြု၍ ပြန်လည်စစ်ဆေးပေးရန် လိုအပ်ပါသည်။

```
E:\RECYCLERS.BIN>dir/a
Volume in drive E is mmCERT/cc
Volume Serial Number is 7047-EC0B

Directory of E:\RECYCLERS.BIN
06/03/2020 02:56 AM <DIR> .
06/03/2020 02:56 AM <DIR> ..
01/10/2020 01:14 AM 160,267 adobeupdate.dat
01/10/2020 01:14 AM 190,144 AdobeUpdate.exe
06/03/2020 02:56 AM 126 desktop.ini
01/10/2020 01:14 AM 20,480 hex.dll
4 File(s) 371,017 bytes
2 Dir(s) 15,521,632,256 bytes free

E:\RECYCLERS.BIN>del *.*
E:\RECYCLERS.BIN>*.*, Are you sure (Y/N)? y

E:\RECYCLERS.BIN>dir/a
Volume in drive E is mmCERT/cc
Volume Serial Number is 7047-EC0B

Directory of E:\RECYCLERS.BIN
06/03/2020 02:59 AM <DIR> .
06/03/2020 02:59 AM <DIR> ..
06/03/2020 02:56 AM 126 desktop.ini
1 File(s) 126 bytes
2 Dir(s) 15,522,009,088 bytes free
```

ပုံ(၁၀)- RECYCLERS.BIN အတွင်းရှိ PlugX RAT မှ ဖန်တီးထားသော ဖိုင်များဖျက်ပုံအဆင့်ဆင့်

(ဃ) အကယ်၍ C2C Server သို့ချိတ်ဆက်နိုင်ခြင်းမရှိသေးလျှင် တိုက်ခိုက်ခံထားရသော Storage Device များတွင် ခိုးယူထားသောဖိုင်များကို ပုံ(၁၁)ပါအတိုင်း တွေ့ရမည်ဖြစ်ပြီး အဆိုပါဖိုင်များကို ဖျက်ပစ်ရန်လည်း Folder name နှင့် “del *.*” Command တို့ကို အသုံးပြုရမည်။

```
E:\>cd RECYCLER.BIN
E:\RECYCLER.BIN>dir/a
Volume in drive E is
Volume Serial Number is 7047-EC0B

Directory of E:\RECYCLER.BIN
06/09/2020 03:03 AM <DIR> .
06/09/2020 03:03 AM <DIR> ..
06/09/2020 03:03 AM <DIR> 7E6A6672ED364119
12/13/2019 02:03 AM 160,779 adobeupdate.dat
06/09/2020 03:01 AM 126 desktop.ini
12/13/2019 02:03 AM 190,144 explorer.exe
02/17/2020 12:29 PM 53,248 hex.dll
4 File(s) 404,297 bytes
3 Dir(s) 15,521,476,608 bytes free

E:\RECYCLER.BIN>_
```

ပုံ(၁၁)- ခိုးယူမည့်ဒေတာများကို 7E6A6672ED364119 Folder တွင် ယာယီသိမ်းဆည်းထားပုံ

PlugX RAT တိုက်ခိုက်မခံရအောင် ကာကွယ်ခြင်း

- ၁၄။ PlugX RAT တိုက်ခိုက်မှု မခံရရေးအတွက် အောက်ပါအတိုင်း လိုက်နာဆောင်ရွက်သင့်ပါသည်-
 - (က) မိမိသိရှိသောသူများမှပေးပို့သော မည်သည့်ဖိုင်ကိုမဆို၊ Link များကိုမဆို မစစ်ဆေးဘဲ အလွယ်တကူဖွင့်မကြည့်ရန်။
 - (ခ) မိမိသိရှိသောသူမှ ပေးပို့သောမေးလ်ဖြစ်ခဲ့လျှင် မည်သည့်အကြောင်းကြောင့် ထိုမေးလ်ကို လက်ခံရရှိသည်ကို ဝေခွဲမရသည့်အခါတွင် ပေးပို့သူအား သေချာအောင် မေးမြန်းပြီးမှသာ မေးလ်အားဖွင့်ကြည့်ရန်။

- (ဂ) မသင်္ကာဖွယ်မေးလ်များ လက်ခံရရှိပါက ထိုမေးလ်များအား အခြားသူများထံ Forward လုပ်ခြင်းများ မလုပ်ဘဲ mmCERT သို့ပေးပို့၍ တိုင်ကြားရန်။
- (ဃ) မယုံကြည်ရသော Website များမှ ပရိုဂရမ်များ၊ ဖိုင်များ Download လုပ်ရာတွင် Virustotal (www.virustotal.com) ကဲ့သို့ Website များတွင် သေချာအောင် စစ်ဆေးပြီးမှ ဖွင့်ကြည့်ရန်။
- (င) Microsoft Word ဖိုင်အဖြစ် ပေးပို့လာသောဖိုင်များအား Microsoft Word ဖိုင် ဟုတ်၊ မဟုတ် Notepad ဖြင့် စစ်ဆေးရန်။
- (စ) Memory Stick ထဲရှိ ဖိုင်များကို ဖွင့်ရာတွင် ပရိုဂရမ်ဖိုင်များ၊ Shortcut ဖိုင်များ ပါရှိပါက စစ်ဆေးပြီးမှသာ ဖွင့်ကြည့်ရန်။
- (ဆ) မိမိတို့၏ Microsoft Windows၊ Microsoft Office ပရိုဂရမ်များနှင့် Anti-virus ပရိုဂရမ်များကို နောက်ဆုံးအခြေအနေအထိ Update ပြုလုပ်ပြီး Anti-virus အား မည်သည့်အကြောင်းကြောင်းဖြင့်မျှ မပိတ်ရန်။

၁၅။ PlugX RAT တိုက်ခိုက်ခံရမှုနှင့်ပတ်သက်၍ အသေးစိတ်မေးမြန်းလိုပါက ၀၆၇-၃၄၂၂၇၂ သို့ ဖုန်းဆက်မေးမြန်းနိုင်ပြီး တိုက်ခိုက်ခံထားရသော ကွန်ပျူတာများကို စစ်ဆေးခံလိုပါက အမျိုးသားဆိုက်ဘာလုံခြုံရေးဗဟိုဌာန၊ S12 Exchange Building၊ ဇေယျာကျက်သရေလမ်း၊ ဇေယျာသီရိမြို့နယ်တွင် လာရောက်စစ်ဆေးနိုင်ပါကြောင်း အသိပေးအပ်ပါသည်။

မြန်မာနိုင်ငံကွန်ပျူတာအရေးပေါ်တုံ့ပြန်ရေးအဖွဲ့ (mmCERT/cc)

Reference

<https://cyware.com/news/plugx-rat-the-tale-of-the-rat-that-has-been-used-in-various-cyber-espionage-campaigns-7aabe7b2>

<https://insights.oem.avira.com/new-wave-of-plugx-targets-hong-kong/>

<https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/112/pulling-the-plug-on-plugx>