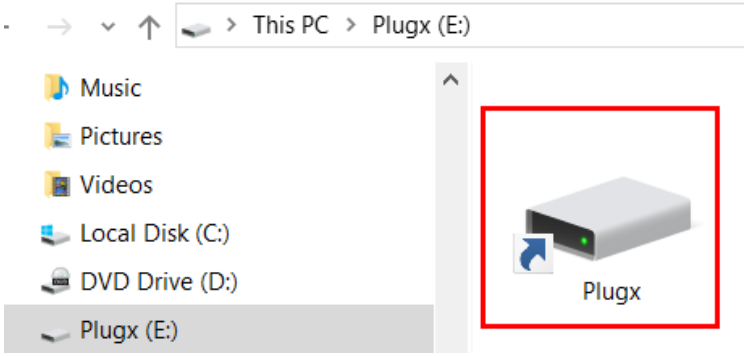
PlugX Remote Access Trojan (RAT) ဖယ်ရှား ရှင်းလင်းနည်းလမ်းညွှန်

PlugX RAT ၏ သမိုင်းကြောင်း

၁။ တရုတ်နိုင်ငံအခြေပြု ဟက်ကာအဖွဲ့ဖြစ်သော Mustang Panda သည် ၂၀၁၄ ခုနှစ်မှစ၍ အာရှ-ပစိဖိတ်ဒေသတွင်း နိုင်ငံများအား ပစ်မှတ်ထား၍ ဆိုက်ဘာတိုက်ခိုက်ပြီး သတင်းအချက်အလက်များကို ခိုးယူရန် ကြိုးစားလျက်ရှိကာ ၂၀၁၉ ခုနှစ်တွင် မြန်မာနိုင်ငံကို ပစ်မှတ်ထား၍ PlugX RAT ဖြင့် တိုက်ခိုက်ခဲ့ပြီး မြန်မာနိုင်ငံအတွင်းရှိ ကွန်ပျူတာအများစုသည် PlugX RAT ၏ တိုက်ခိုက်ခြင်း ခံရလျက်ရှိပါသည်။

PlugX ၏ စတင်ပျံ့နှံ့ပုံနှင့် အလုပ်လုပ်ပုံ

၂။ PlugX မျိုးကွဲများသည် မူလအစတွင် Phishing Mail များမှတဆင့် စိတ်ဝင်စားဖွယ်ရာ Attachment ဖိုင်များအနေဖြင့် ရောက်ရှိလာခြင်းဖြစ်ပြီး Email လက်ခံရရှိသူသည် အဆိုပါ Attachment ဖိုင်ကို ဖွင့်မိရာမှ Attachment တွင်ပါလာသော အဖျက်အမှောင့်ကုဒ်များမှ စတင်အလုပ်လုပ်ပြီး ကွန်ပျူတာတွင် ခြေကုပ်ယူပါသည်။ ထို့နောက်ကွန်ပျူတာသို့ လာရောက်ချိတ်ဆက်သော Memory Stick နှင့် External Hard Disk ကဲ့သို့သော External Storage Devices များထံသို့ ကူးစက်ကာ အခြားကွန်ပျူတာများထံသို့ ပျံ့နှံ့ရန် ကြိုးစားပါသည်။ PlugX သည် အင်တာနက်ချိတ်ဆက်မထားသော ကွန်ပျူတာများထံမှ သတင်းအချက်အလက်များကို ခိုးယူရန် အထူးဖန်တီးထားသော Remote Access Trojan ဖြစ်ပါသည်။ Memory Stick ကဲ့သို့သော External Storage Devices များတွင် PlugX ကူးစက်ခံထားရလျှင် မိမိတို့သိမ်းဆည်းထားသော ဖိုင်များအားလုံး ပျောက်ဆုံးနေမည်ဖြစ်ပြီး ပုံ(၁)ပါ အတိုင်း Shortcut ဖိုင် (.lnk ဖိုင်) တစ်ခုတည်းကိုသာ တွေ့မြင်ရမည် ဖြစ်သည်။ (**မှတ်ချက်**။ အချို့သော PlugX မျိုးကွဲများတွင် Disk Icon အယောင်ဆောင်ထားသော .exe ဖိုင်တစ်ခုကိုသာ တွေ့နိုင်ပါသည်။)



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

၃။ PlugX ကူးစက်ခံထားရသော Memory Stick ကို ကွန်ပျူတာနှင့်ချိတ်ဆက်အသုံးပြုသည့်အခါ ၎င်း Shortcut ဖိုင်ကိုဖွင့်မိပါက ကွန်ပျူတာ၏ C:\ProgramData\AAM Updatesvlm Folder အောက်တွင် AAM Updates.exe၊ hex.dll နှင့် adobeupdate.dat ဖိုင်(၃)ဖိုင်ကို ဖန်တီးမည်ဖြစ်ပါသည်။ (**ရှင်းလင်းချက်**။ PlugX Remote Access Trojan တွင် ဖိုင်(၃)ဖိုင် အမြဲတွဲပါလေ့ရှိပါသည်။ .exe ဖိုင်သည် Adobe၊ Microsoft၊ SmadAV၊ Avast၊ ESET တို့မှ ထုတ်လုပ်ရောင်းချဖြန့်ချိသော တရားဝင်ပရိဂရမ်ဖြစ်ပါသည်။ .dll ဖိုင်မှာ ၎င်း .exe ဖိုင်နှင့်တွဲဖက်အသုံးပြုသော တရားဝင် Dynamic Link Library ဖိုင်ဖြစ်ပြီး ထိုဖိုင်မှတဆင့် နောက်ထပ် .dat ဖိုင်တစ်ခုအားဖတ်ရှုနိုင်ရန် ဟက်ကာများက ပြုပြင်ရေးသားထားပါသည်။ .dat ဖိုင်သည် Encrypt လုပ်ထားသော အဖျက်အမှောင့်ကုဒ်များပါသည့် ဖိုင်တစ်ဖိုင်ဖြစ်ပြီး ၎င်းဖိုင်ထဲတွင် ဟက်ကာများ၏ အမိန့်ပေးထိန်းချုပ်ရေးဆာဗာနှင့်ပတ်သက်သော အချက်အလက်များ၊ သတင်းအချက်အလက်များခိုးယူမည့် ကုဒ်များပါဝင်ပါသည်။ (ဤလမ်းညွှန်တွင် ရှင်းလင်းဖော်ပြချက်များသည် Adobe CEF Explorer အယောင်ဆောင်ထားသော PlugX မျိုးကွဲများအတွက်သာဖြစ်ပါသည်။)

၄။ AAM Updates.exe ဖိုင်သည် Symantec ဆိုက်ဘာလုံခြုံရေးကုမ္ပဏီမှ Sign လုပ်ထားသော Adobe CEF Helper ဖြစ်ပြီး ၎င်းဖိုင်က DLL Hijacker ဖြစ်သော hex.dll ဖိုင်ကိုဖွင့်ကာ ၎င်းမှတဆင့် Encrypted လုပ်ထားသော Payload ဖိုင်ဖြစ်သည့် 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 ၎င်း၏အမိန့်ပေးထိန်းချုပ်ရေးဆာဗာ (Command and Control Server) ထံသို့ သတင်းအချက်အလက်များအား ပေးပို့ပါသည်။ ထိုသို့ အမိန့်ပေးထိန်းချုပ်ရေးဆာဗာများထံသို့ သတင်းအချက်အလက်များကို ခိုးယူပေးပို့ရန်နှင့် ၎င်း၏ အမိန့်ပေးထိန်းချုပ်ရေးဆာဗာများနှင့် လွတ်လပ်စွာဆက်သွယ်နိုင်စေရန်အတွက် Windows ၏ Firewall Setting များကို ပြင်ဆင်ပါသည်။

၅။ PlugX RAT သည် မျိုးကွဲများမတူသည့်အလျောက် ၎င်းတို့၏ အမိန့်ပေးထိန်းချုပ်ရေးဆာဗာများသည်လည်း မတူညီကြောင်းကိုတွေ့ရပါသည်။ မြန်မာနိုင်ငံအားပစ်မှတ်ထားတိုက်ခိုက်သော PlugX မျိုးကွဲများအတွက် အမိန့်ပေးထိန်းချုပ်ရေးဆာဗာများမှာ အောက်ပါအတိုင်း ဖြစ်ပါသည်-

စဉ်	PlugX မျိုးကွဲဖိုင်	စတင်တွေ့ရှိရက်	အမိန့်ပေးထိန်းချုပ်ရေးဆာဗာ
၁	AAM Updates.exe	(၁၀-၁၀-၂၀၁၉)၊ (၃-၁၂-၂၀၁၉)၊	154.223.150.105
	AcroRd32.exe	(၁၃-၁၂-၂၀၁၉)၊	42.99.117.95
	AdobeUpdate.exe	(၂၇-၁၂-၂၀၁၉)၊ (၁၀-၁-၂၀၂၀)၊	45.134.83.41
	AdobeHelp.exe	(၁၅-၁-၂၀၂၀)၊ (၁၇-၁-၂၀၂၀)၊	45.251.240.55
	Explorer.exe	(၁၀-၂-၂၀၂၀)၊ (၁၇-၂-၂၀၂၀)	news.169mt.com

၂	Unsecapp.exe	(၃-၃-၂၀၂၀)	Antivirus များက http_dll.dll ဖိုင် အားဖျက်သွားသဖြင့် C2 ဆာဗာကို သိရှိနိုင်ခြင်းမရှိပါ။
၃	AdobeHelp.exe Adobelm.exe	(၂၃-၆-၂၀၂၀)	45.248.87.162
၄	SmadAv.exe Rzcef.exe AdobePlay.exe RzCefRenderProcess.exe RzProcess.exe	(၅-၈-၂၀၂၀)၊ (၃-၉-၂၀၂၀) (၂၅-၉-၂၀၂၀)	43.254.217.165
၅	dbg.exe Acrobat Read.exe AdobeUpdat.exe	(၁၅-၁၂-၂၀၂၀)	160.20.147.254

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

၇။ PlugX RAT သည် တိုက်ခိုက်ပြီးသော ကွန်ပျူတာနှင့် Storage Device များတွင် Hidden ဖိုင်များ၊ Hidden Folder များကို ဖန်တီးပြီး ကွန်ပျူတာတွင် Background Process များအနေဖြင့် အလုပ်လုပ်ကာ သတင်းအချက်အလက်များကို ခိုးယူပါသည်။ ၎င်းမှ ဖန်တီးထားသော Hidden ဖိုင်များ၊ Hidden Folder များကို အောက်ပါနမူနာနေရာများတွင် တွေ့ရှိနိုင်ပါသည်-

(က) C:\ProgramData\AAM Updatesvlm\

(ခ) C:\Users\[User Name]\AAM Updatesvlm\

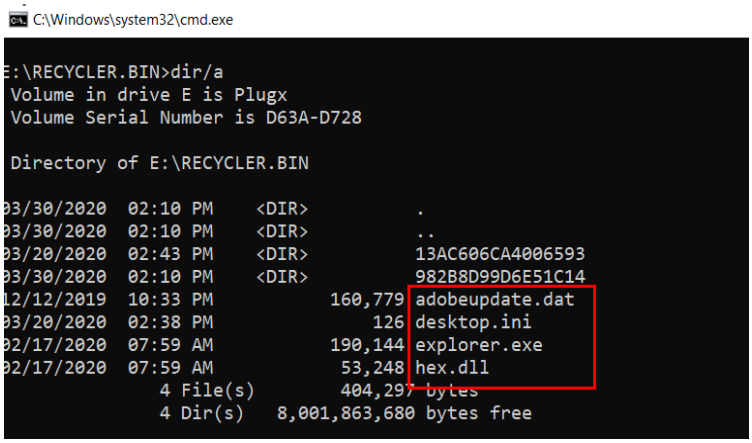
(ဂ) [Storage Device's Logical Drive]\RECYCLER.BIN\ (သို့မဟုတ်)

[Storage Device's Logical Drive]\RECYCLERS.BIN\

(ဃ) HK Current User\Software\Microsoft\Windows\Current Version\Run

(Registry တွင် Persistent အဖြစ် သတ်မှတ်ခြင်း)

၈။ အကယ်၍ အင်တာနက်မှတဆင့် 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 ၏ RECYCER.BIN\ အောက်တွင် explorer.exe (သို့မဟုတ်) AAMupdates.exe အနေဖြင့် ပုန်းအောင်းနေမည်ဖြစ်ပါသည်။

PlugX RAT မျိုးကွဲများ၏ ယေဘုယျ လက္ခဏာများ

၉။ PlugX RAT သည် မျိုးကွဲတစ်ခုနှင့်တစ်ခုအပေါ်မူတည်၍ ဖိုင်အမည်များ 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)၊

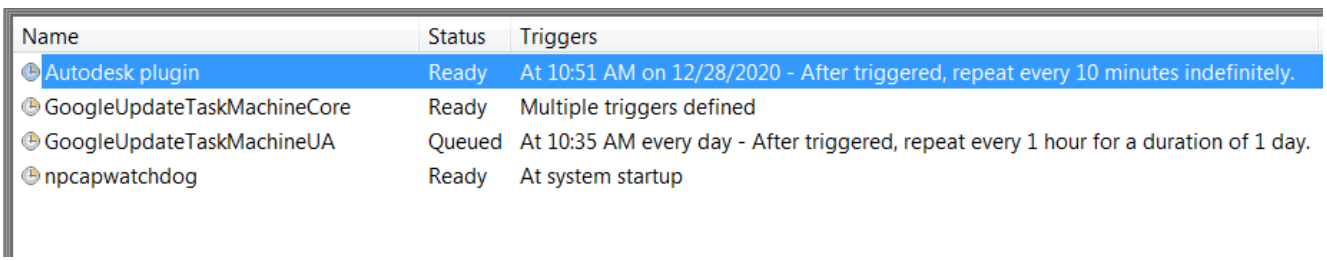
(ဂ) Dll ဖိုင်မှ ခေါ်ယူအသုံးပြုမည့် အန္တရာယ်ရှိသော ကုဒ်များပါဝင်သည့် binary (payload) ဖိုင် (ဥပမာ- Adobeupdate.dat)။

၁၀။ အမျိုးသားဆိုက်ဘာလုံခြုံရေးဗဟိုဌာန၏ Malware Analysis စစ်ဆေးချက်များအရ ဖော်ပြပါ PlugX RAT မျိုးကွဲများအား အောက်ပါ Registry နေရာများတွင်ရှိကြောင်းစစ်ဆေးတွေ့ရှိရပါသည်-

PlugX မျိုးကွဲများ	Sign လုပ်ထားသောဖိုင်	Dll ဖိုင်	Payload ဖိုင်	Registry တွင် Persistent ထားရှိသော အမည်နှင့် တည်နေရာ

Adobe CEF Helper	AAMUpdate.exe	hex.dll	Adobeupdate.dat	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run (**AAM Updatevlm**)
ESET HTTP Server Service	unsecapp.exe	http_dll.dll	http_dll.dat	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run (**Microsoft Malware ProtectionbOr**)
Smadav Whitelisting Protection	Smadav.exe	SmadHook32c.dll	smadavupdate.dat	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run (**SmadavlUe**)
Razar Chromium Render Process	RzCef.exe	RzLog4CPP_Logger.dll	volenum.dat	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run (**RzCefcqf**)
Razar Chromium Render Process	RzCefRenderProcess.exe	RzLog4CPP_Logger.dll	adobeupdates.dat	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run (xxxx)
Razar Chromium Render Process	RzProcess.exe	RzLog4CPP_Logger.dll	RzLogger.dat	xxx
x64dbg	dbg.exe	x32bridge.dll	USB.dat	xx

၁၁။ PlugX RAT သည် ကွန်ပျူတာဖွင့်တိုင်းတွင် အမြဲတမ်းအလုပ်လုပ်နိုင်ရန်အတွက် Windows Registry တွင်ဝင်ရေးသလို ပရိုဂရမ်အား ပိတ်ခဲ့လျှင်ပင် ဆယ်မိနစ်တစ်ကြိမ် အလုပ်လုပ်နိုင်ရန် အတွက် Scheduled Task တစ်ခုကိုလည်း ဖန်တီးပါသည်။ ပုံ(၃)။

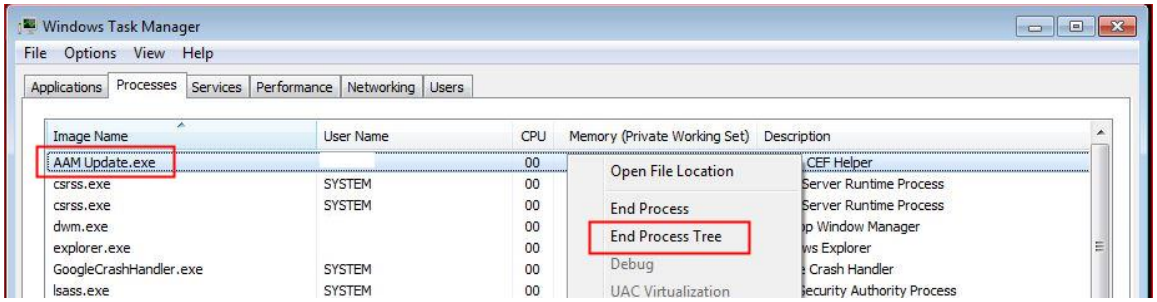


ပုံ(၃) - PlugX သည် ကွန်ပျူတာတွင် ဆယ်မိနစ်တစ်ကြိမ်အလုပ်လုပ်နိုင်ရန်အတွင် Scheduled Task ဖန်တီးထားပုံ

PlugX RAT အား တိုက်ခိုက်ခံထားရသော ကွန်ပျူတာမှ ရှင်းလင်းဖယ်ရှားခြင်း

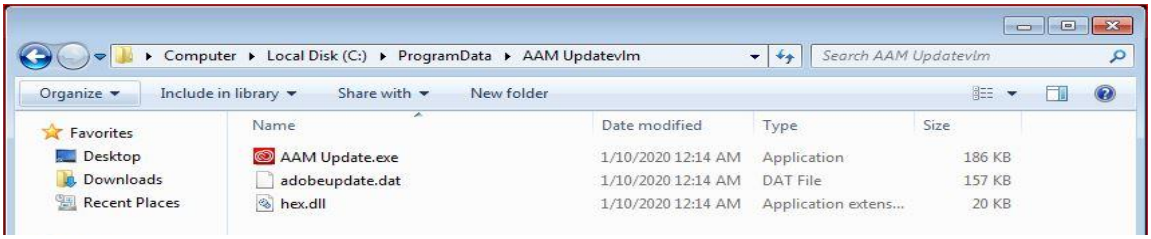
၁၂။ PlugX RAT တိုက်ခိုက်ခံထားရသော ကွန်ပျူတာမှ PlugX RAT အား ရှင်းလင်းပုံအဆင့်အဆင့်မှာ အောက်ပါအတိုင်းဖြစ်ပါသည်-

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



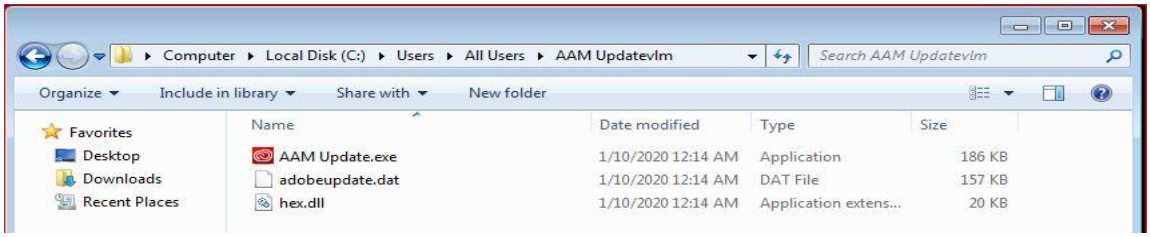
ပုံ(၄) - Task Manager တွင် အလုပ်လုပ်လျက်ရှိသော PlugX RAT ၏ Process အား ရပ်ဆိုင်းခြင်း

(ခ) PlugX RAT သည် တိုက်ခိုက်ခံရသောကွန်ပျူတာတွင် ခြေကုပ်ရယူရန် ပုံ(၅)တွင် ဖော်ပြထားသောနေရာ၌ ဖိုင်(၃)ဖိုင်ကို ဖန်တီးသည့်အတွက် C:\ProgramData\AAM Updatevlm Folder အောက်ရှိ AAM Update.exe၊ hex.dll နှင့် adobeupdate.dat ဖိုင်များကို ဖျက်ရမည်။



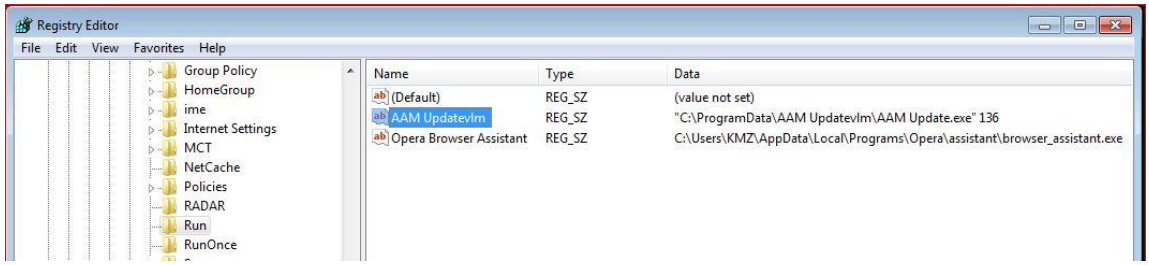
ပုံ(၅) - C:\ProgramData\ folder အောက်တွင် PlugX RAT မှ ဖန်တီးထားသော ဖိုင်များ

(ဂ) အချို့ PlugX RAT မျိုးကွဲများသည် ပုံ(၆)တွင်ဖော်ပြထားသည့်အတိုင်း C:\Users\All Users\AAM Updatevlm Folder တွင်လည်း ၎င်း၏ဖိုင်(၃)ခုအား ဖန်တီးထားရှိသည်ကို တွေ့ရသည့်အတွက် ၎င်း Location အောက်တွင်ရှိသော AAM Update.exe၊ hex.dll နှင့် adobeupdate.dat ဖိုင်များကိုလည်း ဖျက်ပေးရမည်။



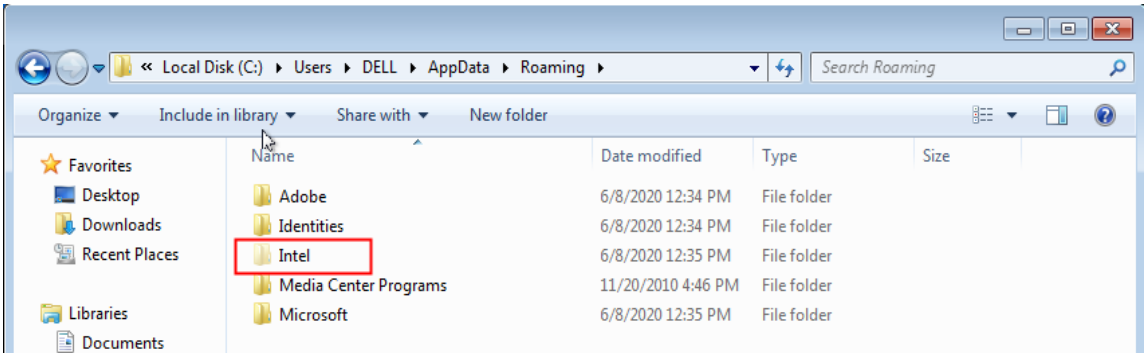
ပုံ(၆) - C:\Users\All Users\AAM Updatevlm Folder အောက်တွင် PlugX RAT မှ ဖန်တီးထားသော ဖိုင်များ

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



ပုံ(၇) - Registry အောက်တွင် အမြဲအလုပ်လုပ်ရန်အတွက် PlugX RAT မှ Run Key ဖန်တီးထားပုံ

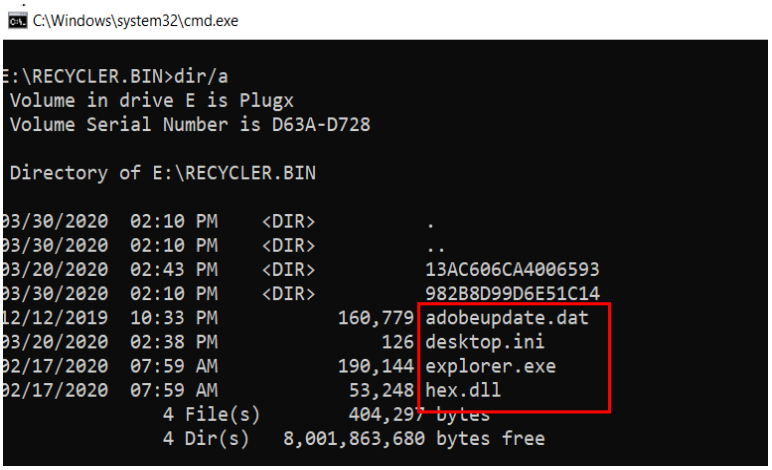
(c) ခိုးယူမည့်ဖိုင်များကို C:\Users\[UserName]\AppData\Roaming\Intel\[CLSID] အောက်တွင် သိမ်းထားခြင်းဖြစ်သဖြင့် ၎င်း Folder ကိုလည်း ဖျက်ပေးရန်လိုအပ်ပါသည်။ (**မှတ်ချက်**။ အချို့သောမျိုးကွဲများတွင်မူ အခြားအမည် ဖြစ်နေနိုင်ပါသည်။ ဥပမာ - rzcef.exe ဖိုင်၌ Render ဆိုသော Folder အမည်ကို အသုံးပြုပါသည်။)



ပုံ(၈) - တိုက်ခိုက်ခံထားရသောကွန်ပျူတာမှ ဒေတာများကို C2C Server သို့ပေးပို့ရန် ယာယီထားရှိထားသောနေရာ

PlugX RAT အား တိုက်ခိုက်ခံထားရသော Storage Devices များမှ ရှင်းလင်းဖယ်ရှားခြင်း

၁၃။ PlugX RAT သည် တိုက်ခိုက်ခံရသောကွန်ပျူတာမှ C2C Server ထံသို့ အင်တာနက်မှတဆင့် 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(၉)တွင်ပြထားသည့် Location တွင် သွားရောက်ဖျက်ပေးရမည်ဖြစ်သည်။

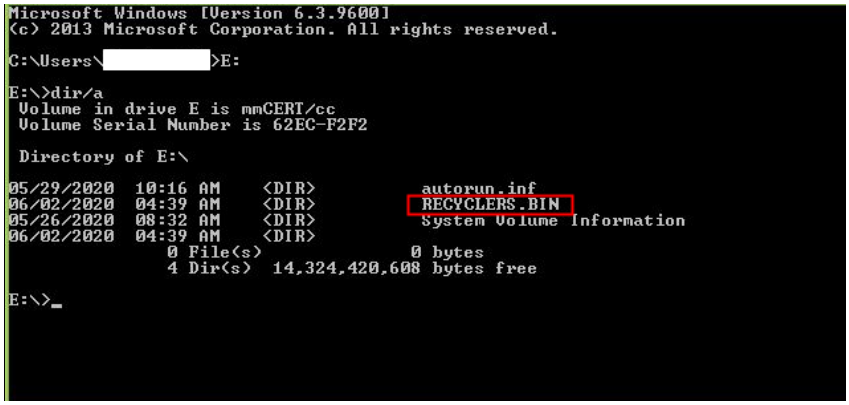


ပုံ(၉) - Storage Device များအတွင်းတွင် PlugX RAT မှ ဖန်တီးထားရှိသော ဖိုင်များ

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

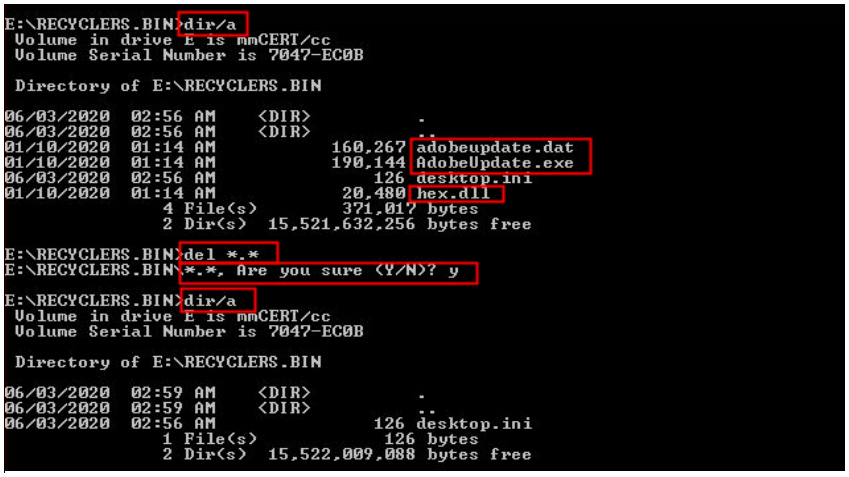
(က) Windows ၏ Run Box မှတဆင့် Command Prompt (cmd.exe) ကို ခေါ်ယူကာ မိမိကွန်ပျူတာက တပ်ဆင်အသုံးပြုထားသော Storage Device အတွက် ဖော်ပြပေးသော Drive အတွင်းသို့ ဝင်ရောက်ပါ။ (ပုံ(၁၀)တွင် ကြည့်ရှုနိုင်ပါသည်။)

(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။



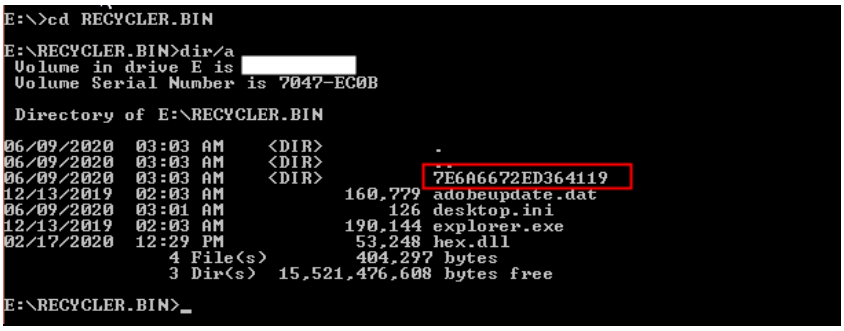
ပုံ(၁၀) - PlugX RAT တိုက်ခိုက်ခံထားရသော Storage Device တွင် RECYCLERS.BIN Folder အား မြင်တွေ့ရပုံ

(၈) “cd RECYCLERS.BIN” Command ကိုအသုံးပြု၍ RECYCLERS.BIN (သို့မဟုတ်) RECYCLER.BIN အတွင်းသို့ဝင်ရောက်ကာ “dir/a” Command ကို အသုံးပြုပြီး Folder အတွင်းရှိ ဖိုင်များကို စစ်ဆေးပါ။ ထိုသို့စစ်ဆေးရာတွင် ပုံ(၁၁)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 ဖိုင်များကျန်ရှိနေခြင်းမရှိစေရန် “dir/a” command ကို အသုံးပြု၍ ပြန်လည်စစ်ဆေးပေးရန် လိုအပ်ပါသည်။



ပုံ(၁၁) - RECYCLERS.BIN အတွင်းရှိ PlugX RAT မှ ဖန်တီးထားသော ဖိုင်များဖျက်ပုံအဆင့်ဆင့်

(ဃ) အကယ်၍ C2C Server သို့ချိတ်ဆက်နိုင်ခြင်းမရှိသေးလျှင် တိုက်ခိုက်ခံထားရသော Storage Device များတွင် ခိုးယူထားသောဖိုင်များကို ပုံ(၁၂)ပါအတိုင်း Folder တစ်ခု တည်ဆောက်၍ သိမ်းဆည်းထားခြင်းကို တွေ့ရမည်ဖြစ်ပြီး အဆိုပါဖိုင်များကို ဖျက်ပစ်ရန် “del foldername” Command ကို အသုံးပြုရမည်။



ပုံ(၁၂) - ခိုးယူမည့်ဒေတာများကို 7E6A6672ED364119 Folder တွင် ယာယီသိမ်းဆည်းထားပုံ

PlugX RAT တိုက်ခိုက်မခံရအောင် ကာကွယ်ခြင်း

၁၅။ PlugX RAT တိုက်ခိုက်မှု မခံရရေးအတွက် အောက်ပါအတိုင်း လိုက်နာဆောင်ရွက်သင့်ပါသည်-

(က) မိမိမသိရှိသောသူများမှပေးပို့သော မည်သည့်ဖိုင်ကိုမဆို၊ Link များကိုမဆို မစစ်ဆေးဘဲ အလွယ်တကူဖွင့်မကြည့်ရန်။

(ခ) မိမိသိရှိသောသူမှ ပေးပို့သောမေးလ်ဖြစ်ခဲ့လျှင် မည်သည့်အကြောင်းကြောင့် ထိုမေးလ်ကို လက်ခံရရှိသည်ကို ဝေခွဲမရသည့်အခါတွင် ပေးပို့သူအား သေချာအောင် မေးမြန်းပြီးမှသာ မေးလ်အားဖွင့်ကြည့်ရန်။

(ဂ) မသက်ဆိုင်သောမေးလ်များ 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။

(c) Microsoft Word ဖိုင်အဖြစ် ပေးပို့လာသောဖိုင်များအား Mircosoft Word ဖိုင် ဟုတ်၊ မဟုတ် Notepad ဖြင့် စစ်ဆေးရန်။

(စ) Memory Stick ထဲရှိ ဖိုင်များကို ဖွင့်ရာတွင် ပရိုဂရမ်ဖိုင်များပါရှိပါက စစ်ဆေးပြီးမှသာ ဖွင့်ကြည့်ရန်။ Shortcut ဖိုင်များကို ဖွင့်မကြည့်ရန်။

(ဆ) မိမိတို့၏ Microsoft Windows၊ Microsoft Office ပရိဂရမ်များနှင့် Anti-virus ပရိဂရမ်များကို နောက်ဆုံးအခြေအနေအထိ Update ပြုလုပ်ပြီး Anti-virus အား မည်သည့်အကြောင်းကြောင်းဖြင့်မျှ မပိတ်ရန်။

၁၆။ PlugX RAT တိုက်ခိုက်ခံရမှုနှင့်ပတ်သက်၍ အသေးစိတ်မေးမြန်းလိုပါက ၀၆၇-၃၄၂၂၂၇၂ သို့ ဖုန်းဆက်မေးမြန်းနိုင်ပြီး တိုက်ခိုက်ခံထားရသော ကွန်ပျူတာများကို စစ်ဆေးခံလိုပါက အမျိုးသားဆိုက်ဘာလုံခြုံရေးဗဟိုဌာန၊ S12 Exchange Building၊ ဓမ္မာ့ကျက်သရေလမ်း၊ ဓမ္မာသီရိ မြို့နယ်တွင် 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

Indicators of Compromise (IOCs)

File Name	MD5 Value
adobeupdate.dat	38baabddffb1d732a05ffa2c70331e21, cf3eca063449eb5b3aa5b5e33b13ebd4, 8cedb5d84b80d76d281a768487ab913c, e21e8f398c6d61ae8335664b1ad0444f, 11a9f4e43fcf839c2d5c4bba0b1d98c5, 70e8898810ac014a3820e6579519bee5, 0e2c8d92d63e33eb26ccbcef12694855, 1557d751b7a760a39ec743e27ad2af58, bb705766d736447b1dc8f720d5a9388b, 6c08a93af10d065551c6078911e064c1 461fefae3ea10d82cd2c76e257622c67
adobehelp.exe	c43de22826a424b2d24cf1b4b694ce07, f26179d65b42720b2a4984d717c309de
hex.dll	21ae18f2fc557e2751840bc517eaf8b5, 041415cdc204f8efa12e01581205dec1, 43529e54971a2302ae736c40f39d65df, c33d3d6970dbb19062ae09505a6eb376,

	60a4cd6356aa47d507bc41ea59074f7a, 8166372d3aace7f9965f0a57fa03fc4e 4c36ab90a5f74df2c37e7ad029d52ece
volenum.dat	798810d4ab0637916e699eeeffb393db
wmiav.exe	e0d96cb8e6e6e40f5ef3c70cc4aab69a
RzLog4CPP_Logger.dll	5afa942f967ec2952b1ae295f3de8230
smadavupdate.dat	504a73639a7868ed8576ea3cbafc0239
smadav.exe	ab5d85079e299ac49fcc9f12516243de
SmadHook32c.dll	fc55344597d540453326d94eb673e750
adobeupdates.dat	aa59340b2be14c4d9d4eb69329729b7b
AdobePlay.exe	440277d0c826aba62ba95d65a67c4aa7
RzLog4CPP_Logger.dll	29ed39c6e66a8882fb8571db34473c4e
Rzlogger.dat	747bce4a7891a9e186ccd80ce6e196a5
RzProcess.exe	ea7f5b7fdb1e637e4e73f6bf43dcf090
RzLog4CPP_Logger.dll	ed9372ec28556ff71efd4810a0a3ac6e
USB.dat	089f71fb66a4bd2a158e34a130635f68
dbg.exe	18315184dc464bbad1f202306c055d1e
x32bridge.dll	8fa9dec74b1a6ef999bd31bd3bce1027

ထုတ်ဝေခြင်း

၁။ ပထမအကြိမ်ထုတ်ဝေခြင်း (၂၀၁၉ ခုနှစ်၊ ဇွန်လ ၉ ရက်)

၂။ ဒုတိယအကြိမ်ဖြည့်စွက်ထုတ်ဝေခြင်း (၂၀၂၀ ပြည့်နှစ်၊ ဒီဇင်ဘာလ ၃၀ ရက်)