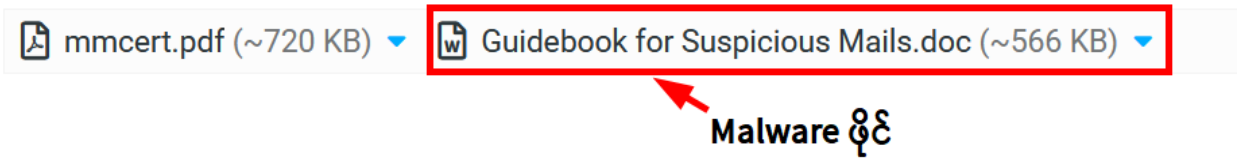
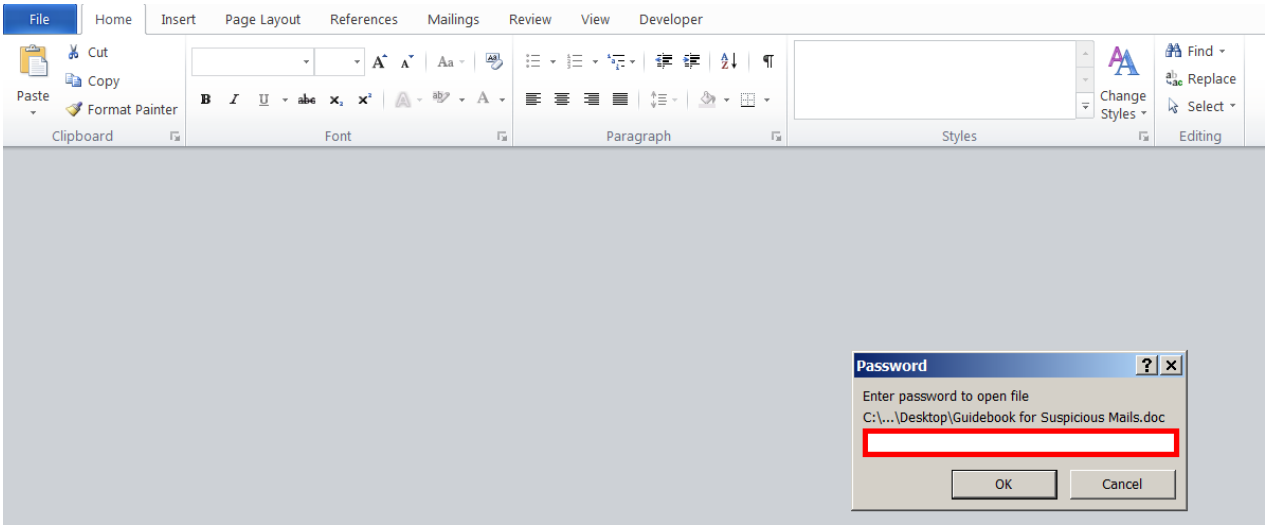
မသမာသူများမှ Phishing မေးလ်များ ပေးပို့ခြင်းနှင့် ပတ်သက်၍ သတိပေးချက်

၁။ မသမာသူများသည် သတင်းအချက်အလက်ခိုးယူရန်အတွက် messenger.inf0rmationn@gmail.com မေးလ်အကောင့်အား အသုံးပြု၍ အီးမေးလ်၏ Subject တွင် "**mmcert ၏ လမ်းညွှန်ချက်အားပေးပို့ခြင်း**" အမည်ဖြင့် အဖျက်အမှောက်ဖိုင်ပါရှိသော မေးလ်များ ပေးပို့လျက်ရှိပါသည်။ အဆိုပါ အီးမေးလ်တွင် mmcert.pdf ဖိုင်နှင့် Guidebook for Suspicious Mails.doc ဖိုင်တို့ပါဝင်ပြီး ပါဝင်သော ဖိုင်နှစ်ဖိုင်အနက် mmcert.pdf ဖိုင်သည် မြန်မာနိုင်ငံကွန်ပျူတာအရေးပေါ်တုံ့ပြန်ရေးအဖွဲ့မှ ရေးသားထုတ်ဝေထားသည့် "**အန္တရာယ်ဖြစ်စေနိုင်သည့် အီးမေးလ်များ လက်ခံရရှိပါက လိုက်နာဆောင်ရွက်ရမည့်အချက်များ Version 1.0**" ဖိုင်ဖြစ်ပြီး **Guidebook for Suspicious Mails.doc** ဖိုင်သည် အယောင်ဆောင်ထားသည့် အဖျက်အမှောက်ကုဒ်များပါရှိသောဖိုင် ဖြစ်ပါသည်။



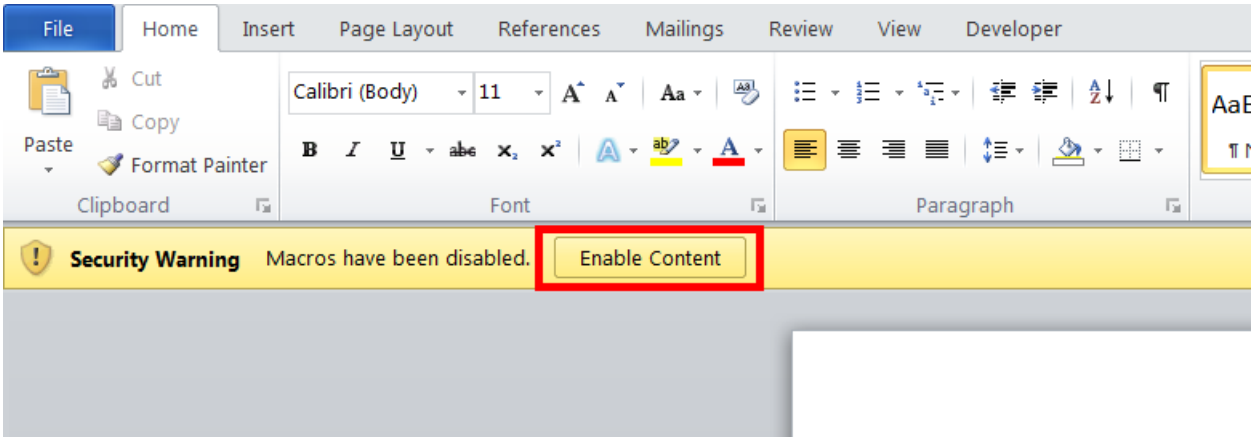
ပုံ(၁) အဖျက်အမှောက်ကုဒ်များပါသော Malware (Microsoft Word ဖိုင်)

၂။ အဖျက်အမှောက်ကုဒ်ပါသော Microsoft Word ဖိုင်အား ဖွင့်ပါက ပုံ(၂)ပါအတိုင်း Password ကိုတောင်းခံမည်ဖြစ်ပါသည်။ Malware များသည် Antivirus၊ Firewall နှင့် အီးမေးလ်လုံခြုံရေးစနစ်များကဲ့သို့သော ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာစောင့်ကြည့်စနစ်များ၏ စုံစမ်းမှုကို ကျော်လွှားနိုင်ရန်အတွက် Passsword ကို အသုံးပြုကြပြီး Password များကိုလည်း Mail Body များတွင် တစ်ပါတည်း ထည့်သွင်းဖော်ပြတတ်ပါသည်။



ပုံ(၂) အဖျက်အမှောက်ဖိုင်အား ဖွင့်ရန်အတွက် Password တောင်းခံပုံ

၃။ Password အား ရိုက်ထည့်ပါက ပုံ(၃)ပါအတိုင်း Security Warning တစ်ခုကို မြင်တွေ့ရမည်ဖြစ်ပြီး "**Enable Content**" Button ကိုနှိပ်ပါက အဖျက်အမှောက်ဖိုင်ပါသော Macros ကုဒ်များက အလုပ်လုပ်မည်ဖြစ်ပါသည်။



ပုံ(၃) အဖျက်အမှောက် Macro ကုဒ်များပါရှိကြောင်း Microsoft Word ၏ သတိပေးချက်

၄။ အကယ်၍ "**Enable Content**" Button ကို နှိပ်ခဲ့ပါက Malware သည် အောက်ပါနေရာများသို့ အဖျက်အမှောက်ကုဒ်များပါသော ဖိုင်များကို နေရာချထားမည် ဖြစ်ပါသည် -

(က) C:\Users\Admin\AppData\Local**DQkUKLto2XbEHq3.vbs**

(ခ) C:\Users\Admin\AppData\Local**eventviewr.exe**

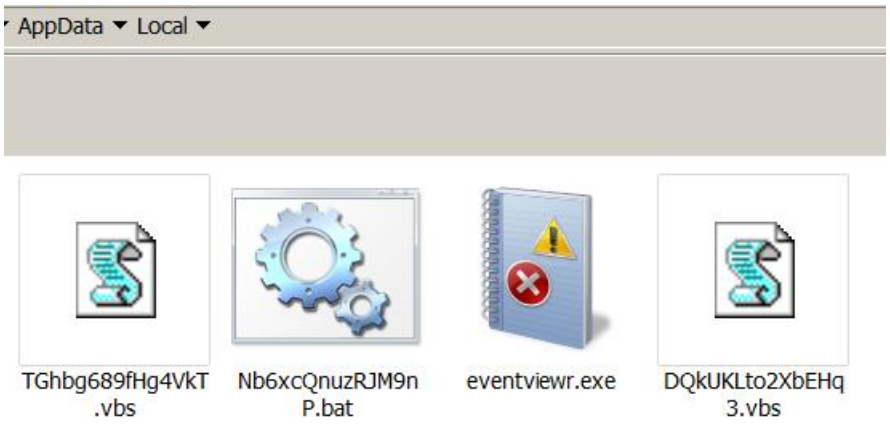
(ဂ) C:\Users\Admin\AppData\Local**Nb6xcQnuzRJM9nP.bat**

(ဃ) C:\Users\Admin\AppData\Local**TGhbg689fHg4VkT.vbs**

(င) C:\Users\Admin\AppData\Local\Microsoft**eventviewr.zip**

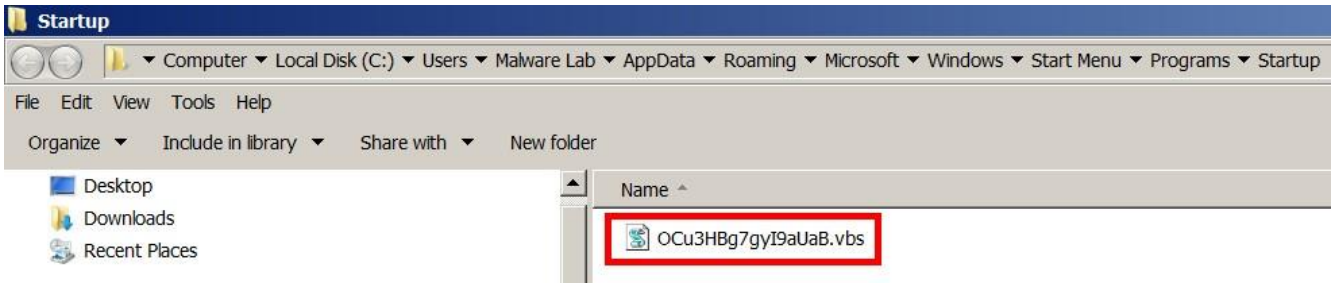
(စ) C:\Users\Admin\AppData\Roaming\Microsoft\Windows\StartMenu\Programs\Startup**OCu3HBg7gyl9aUaB.vbs**

(ဆ) C:\Windows\System32\Tasks**EventViewerLog**

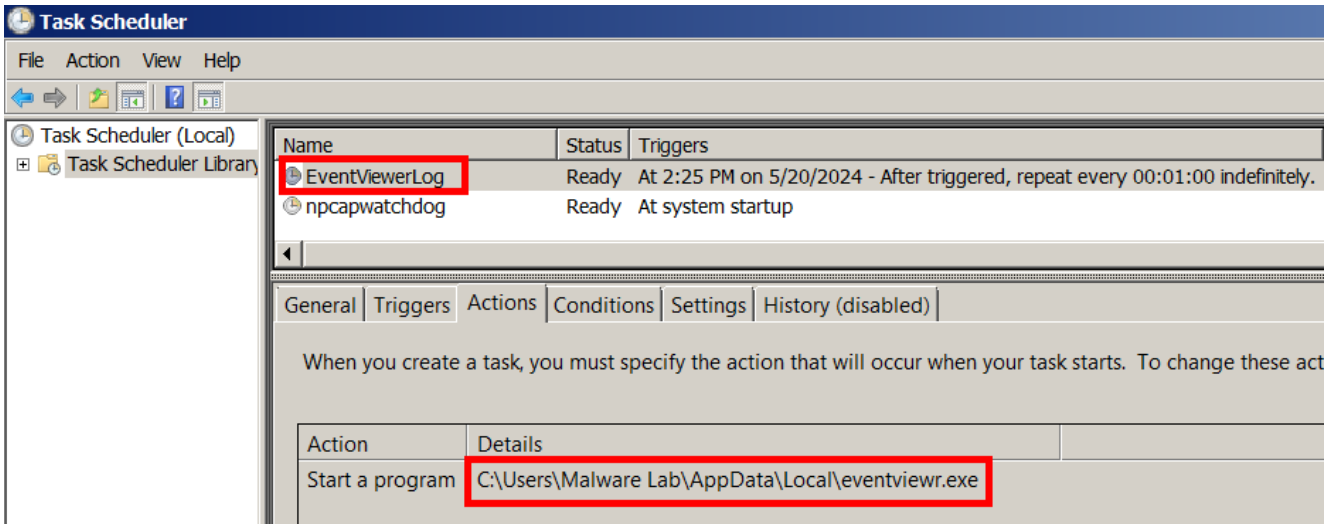


ပုံ(၄) C:\Users\Admin\AppData\Local\ Folder အောက်ရှိ အဖျက်အမှောက်ဖိုင်များ

၅။ Malware သည် တိုက်ခိုက်ထားသော ကွန်ပျူတာတွင် အချိန်ပြည့်အလုပ်လုပ်နိုင်ရန်အတွက် Startup အနေဖြင့်သော်လည်းကောင်း၊ Scheduled Task အနေဖြင့်သော်လည်းကောင်း အလုပ်လုပ်ပါသည်။



ပုံ(၅) Malware မှ ကွန်ပျူတာဖွင့်တိုင်း အလုပ်လုပ်နိုင်ရန် Startup Folder တွင် ထားရှိထားပုံ



ပုံ(၆) Malware သည် တစ်မိနစ်ကြာတိုင်း အလုပ်လုပ်စေရန် Scheduled Task တွင်ရေးသားထားပုံ

၆။ Malware သည် သတင်းအချက်အလက်များကို ခိုးယူရန်နှင့် နောက်ထပ်သော အဖျက်အမှောက်ဖိုင်များကို အင်တာနက်မှ Download ရယူနိုင်ရန်အတွက် အောက်ပါ Domain များကို ချိတ်ဆက်နိုင်ပါသည် -

(က) **http://myanmar-apn.serveftp.com**

(ခ) **http://mytel-mm.servehttp.com**

(ဂ) **http://telenor-mm.redirectme.net**

(ဃ) **http://windows-update.hopto.org**

၇။ Microsoft Windows များတွင်ပါရှိသည့် Event Viewer အယောင်ဆောင်ထားသော အဖျက်အမှောက်ဖိုင် (**eventviewr.exe**) အား လက်ရှိတွင် AntiVirus ၄ ခုကသာ စုံစမ်းသိရှိသည့် အတွက် အခြားသော Antivirus များမှ အဆိုပါဖိုင်အား စုံစမ်းသိရှိနိုင်ခြင်း မရှိသေးပါ။

Bkav Pro	W32.AIDetectMalware.CS	Kaspersky	UDS:Trojan.MSIL.Khalesi.gen
Webroot	W32.Malware.Gen	ZoneAlarm by Check Point	UDS:Trojan.MSIL.Khalesi.gen
Acronis (Static ML)	Undetected	AhnLab-V3	Undetected
Alibaba	Undetected	AliCloud	Undetected
ALYac	Undetected	Antiy-AVL	Undetected
Arcabit	Undetected	Avast	Undetected
AVG	Undetected	Avira (no cloud)	Undetected
Baidu	Undetected	BitDefender	Undetected
BitDefenderTheta	Undetected	ClamAV	Undetected

ပုံ(၇) Malware အား www.virustotal.com Website တွင် စစ်ဆေးထားပုံ

၈။ Malware တိုက်ခိုက်ခံထားရသောကွန်ပျူတာများ (**Word Document ဖိုင်အား ဖွင့်မိထားသော သူများ**)သည် အပိုဒ်(၄)တွင်ဖော်ပြထားသော နေရာများမှ **ဖိုင် ၇ ဖိုင်**ကို ကိုယ်တိုင်ဖျက်ပစ်ရန် လိုအပ်ပါသည်။

၉။ မိမိတို့အဖွဲ့အစည်းများတွင် Network-based Firewall များတပ်ဆင်ထားပါက (သို့) Host-based Firewall (Windows Defender Firewall) အသုံးပြုပါက အပိုဒ်(၆)ပါ Domain လိပ်စာများအား Firewall တွင် ပိတ်ပင်ထားရန် လိုအပ်ပါသည်။

၁၀။ သံသယဖြစ်ဖွယ်မေးလ်များ လက်ခံရရှိပါက မြန်မာနိုင်ငံကွန်ပျူတာအရေးပေါ်တုံ့ပြန်ရေးအဖွဲ့မှ ထုတ်ဝေထားသည့် **“အန္တရာယ်ဖြစ်စေနိုင်သည့် အီးမေးလ်များ လက်ခံရရှိပါက လိုက်နာဆောင်ရွက်ရမည့်အချက်များ Version 1.0”** လမ်းညွှန်ချက်ပါအတိုင်း လိုက်နာဆောင်ရွက်ရန် လိုအပ်ပါသည်။

Download လုပ်ရန်။ https://www.mmcert.org.mm/en/file-download/download/public/378

၁၁။ ဆိုက်ဘာတိုက်ခိုက်မှုနှင့်ပတ်သက်၍ တိုင်ကြားလိုပါက အမျိုးသားဆိုက်ဘာလုံခြုံရေးဗဟိုဌာန၊ ဇမ္ဗူကျက်သရေလမ်း၊ ဇမ္ဗူသီရိမြို့သို့ လူကိုယ်တိုင်ဖြစ်စေ၊ ဆက်သွယ်ရန်ဖုန်းနံပါတ်ဖြစ်သော ၀၆၇-၃၄၂၂၇၂ သို့ ဖုန်းဖြင့်ဖြစ်စေ၊ infoteam@mmcert.org.mm နှင့် incident@ncsc.gov.mm တို့သို့ အီးမေးလ်ပေးပို့၍ဖြစ်စေ တိုင်ကြားနိုင်ပါကြောင်း အသိပေးအပ်ပါသည်။

မြန်မာနိုင်ငံကွန်ပျူတာအရေးပေါ်တုံ့ပြန်ရေးအဖွဲ့