မသမာသူများမှ Phishing မေးလ်များ ပေးပို့ခြင်းနှင့် ပတ်သက်၍ သတိပေးချက်

၁။ မသမာသူများသည် သတင်းအချက်အလက်ခိုးယူရန်အတွက် အဖွဲ့အစည်းများ/ကုမ္ပဏီများမှ ခိုးယူထားသော မေးလ်အကောင့်များအား အသုံးပြု၍ ထိုအကောင့်များနှင့် မေးလ်ပို့ဖူးထားသူများထံ "**Meeting Invitation**" အမည်ဖြင့် အဖျက်အမှောက်ဖိုင်ပါရှိသော မေးလ်များ ပေးပို့လျက်ရှိပါသည်။

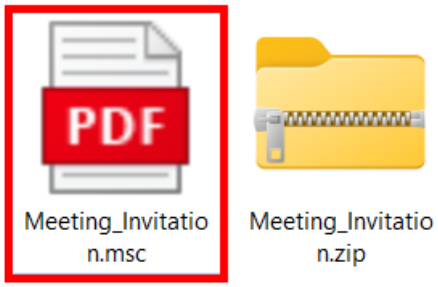
Please kindly check the attached file.

Meeting_Invitation.zip

Warmest Regards,

ပုံ(၁) အဖျက်အမှောက်ဖိုင်ပါသော အီးမေးလ်

၂။ အဆိုပါ အီးမေးလ်တွင် Hyperlink ချိတ်ဆက်ထားသော **Meeting_Invitation.zip** ဖိုင်ပါဝင်ပြီး အဆိုပါ Link ကို နှိပ်ပါက **https://versaillesinfo.com/kbezndno Website** မှ **Meeting_Invitation.zip** ဖိုင်ကို Download လုပ်ယူမည်ဖြစ်ပါသည်။ Zip ဖိုင်အားဖြည်ပါက PDF ဖိုင်အယောင်ဆောင်ထားသော **Meeting_Invitation.msc** ကို တွေ့ရှိရမည်ဖြစ်ပါသည်။



ပုံ(၂) အဖျက်အမှောက်ကုဒ်ပါသော Meeting_Invitation.msc ဖိုင်

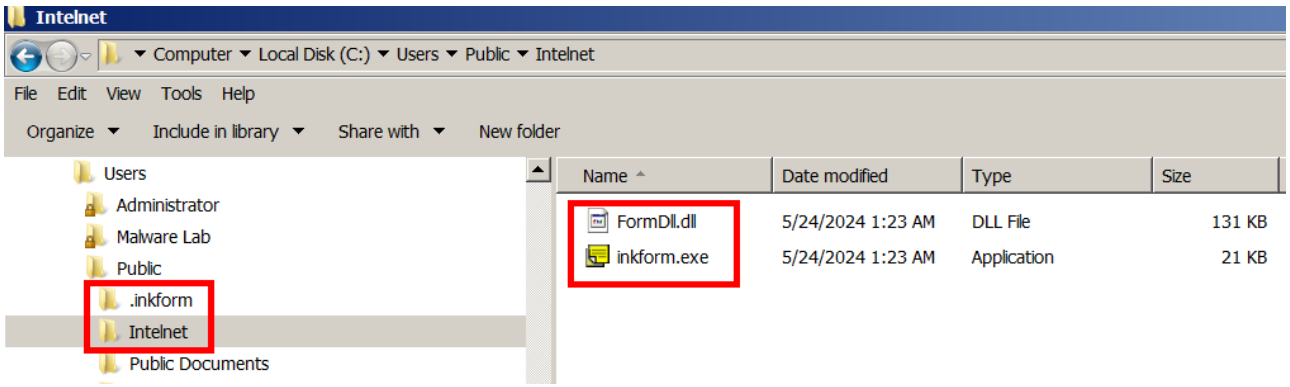
၃။ Meeting_Invitation.msc ဖိုင်ကို ဖွင့်ကြည့်ပါက ၎င်းတွင်ပါဝင်သော အဖျက်အမှောက်ကုဒ်များက အလုပ်လုပ်မည်ဖြစ်ပြီး **https://versaillesinfo.com/** Website မှ Microsoft Software Installer (.msi) ဖိုင်ဖြစ်သော **brjwcabz** ဖိုင်ကို Download လုပ်ယူပြီး အဆိုပါဖိုင်က Malware များကို အောက်ပါနေရာများသို့ နေရာချထားမည်ဖြစ်ပါသည်-

(က) C:\Users\Public\Intelnet**inkform.exe**

(ခ) C:\Users\Public\Intelnet**FormDll.dll**

(ဂ) C:\Users\Public\.inkform**inkformDB.dat**

(ဃ) C:\Users\CurrentUser\AppData\Local\Temp**Meeting_Invitation.pdf**

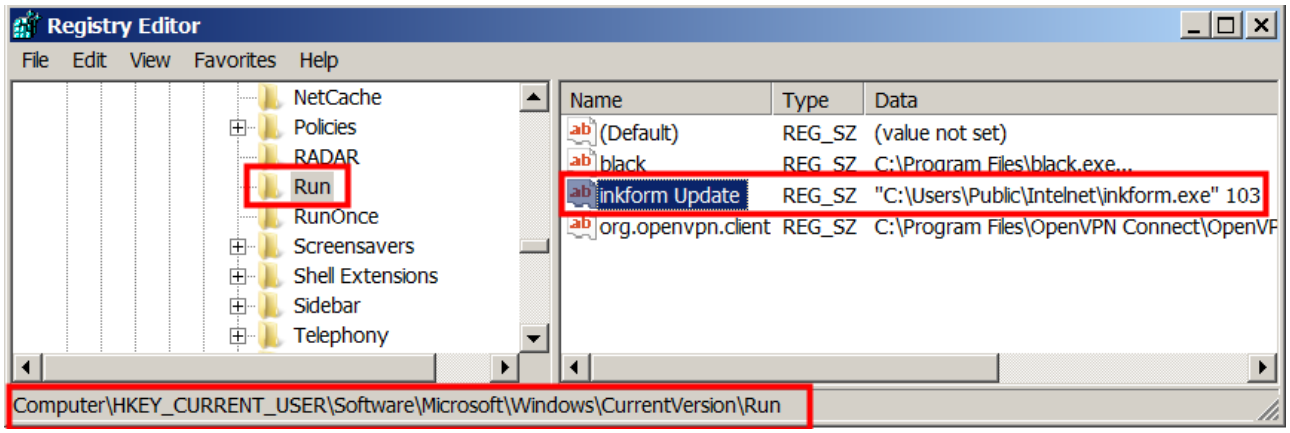


ပုံ(၃) Malware များထားရှိရာနေရာ

၄။ inkform.exe သည် Microsoft Corporation မှ တရားဝင်ရေးသားဖြန့်ဖြူးထားသော Ink Form MAPI Notes Server ပရိဂရမ်ဖြစ်သောကြောင့် Anti-virus များက Malware အဖြစ် စုံစမ်းသိ ရှိနိုင်မည် မဟုတ်ပါ။ inkform.exe အလုပ်လုပ်သောအခါ FormDll.dll ကို ခေါ်ယူသုံးစွဲပြီး အဆိုပါ .DLL ဖိုင်မှ Encrypted လုပ်ထားသော inkformDB.dat ကို Decrypt လုပ်ကာ အဆိုပါ .DAT ဖိုင်တွင် ပါသော အဖျက်အမှောက်ကုဒ်များကို အလုပ်လုပ်စေမည်ဖြစ်ပါသည်။ Malware သည် သတင်းအချက်အလက် ခိုးယူရန် အထူးတီထွင် ဖန်တီးထားသော PlugX Remote Access Trojan (RAT) ဖြစ်ပြီး ခိုးယူထားသော အချက်အလက်များကို ဟက်ကာများ၏ အမိန့်ပေးထိန်းချုပ်ရေးဆာဗာဖြစ်သော shreyaninfotech.com သို့ပေးပို့မည်ဖြစ်သည်။ PlugX RAT နှင့်ပတ်သက်သော အသေးစိတ် အချက်အလက်ကို အောက်ပါ Link တွင် ဖတ်ရှုနိုင်ပါသည်။

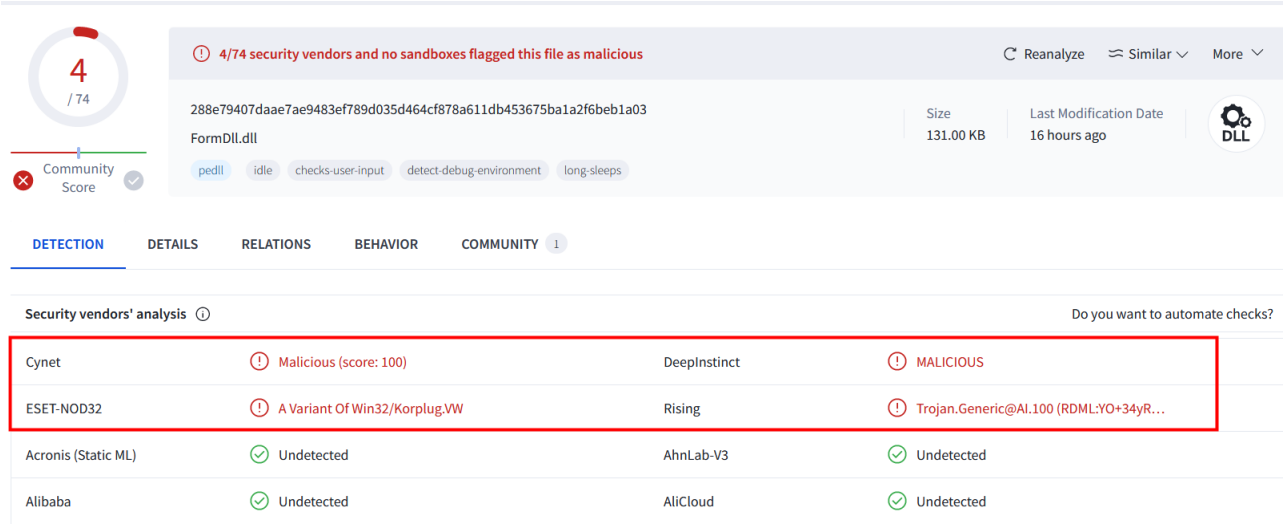
https://www.mmcert.org.mm/index.php/mm/file-download/download/public/374

၅။ Malware သည် တိုက်ခိုက်ထားသော ကွန်ပျူတာတွင် အချိန်ပြည့်အလုပ်လုပ်နိုင်ရန်အတွက် Windows Registry တွင် inkform Update အမည်ဖြင့် String တစ်ခုကို ဖန်တီးရေးသားပါသည်။



ပုံ(၄) Malware က Windows Registry တွင် Key တစ်ခုအား ရေးသားသတ်မှတ်ထားပုံ

၆။ Malware သည် DLL Sideloading နည်းပညာကို အသုံးပြုထားသည့်အတွက် လက်ရှိတွင် AntiVirus ၄ ခုကသာ စုံစမ်းသိရှိပြီး အခြားသော Antivirus များမှ အဆိုပါဖိုင်အား စုံစမ်းသိရှိနိုင်ခြင်း မရှိသေးပါ။



ပုံ(၅) Malware အား www.virustotal.com Website တွင် စစ်ဆေးထားပုံ

၇။ Malware တိုက်ခိုက်ခံထားရသောကွန်ပျူတာများ (**Malware ဖိုင်အား ဖွင့်မိထားသောသူများ**)သည် အပိုဒ်(၃)တွင်ဖော်ပြထားသော နေရာများမှ **ဖိုင် ၄ ဖိုင်** နှင့် ပုံ(၄)တွင် ဖော်ပြထားသော **Registry Key** ကို ကိုယ်တိုင်ဖျက်ပစ်ရန် လိုအပ်ပါသည်။

၈။ မိမိတို့အဖွဲ့အစည်းများတွင် Network-based Firewall များတပ်ဆင်ထားပါက (သို့) Host-based Firewall (Windows Defender Firewall) အသုံးပြုပါက Malware အား Download လုပ်ယူခြင်း မရှိနိုင်စေရန်နှင့် သတင်းအချက်အလက်များ ခိုးယူခံရခြင်း မရှိစေရန် **https://versaillesinfo.com/** နှင့် **shreyaninfotech.com** Domain တို့အား Firewall တွင် ပိတ်ပင်ထားရန် လိုအပ်ပါသည်။

၉။ သံသယဖြစ်ဖွယ်မေးလ်များ လက်ခံရရှိပါက မြန်မာနိုင်ငံကွန်ပျူတာအရေးပေါ်တုံ့ပြန်ရေးအဖွဲ့မှ ထုတ်ဝေထားသည့် **“အန္တရာယ်ဖြစ်စေနိုင်သည့် အီးမေးလ်များ လက်ခံရရှိပါက လိုက်နာဆောင်ရွက်ရမည့်အချက်များ Version 1.0”** လမ်းညွှန်ချက်ပါအတိုင်း လိုက်နာဆောင်ရွက်ရန် လိုအပ်ပါသည်။
https://www.mmcert.org.mm/en/file-download/download/public/378

၁၀။ ဆိုက်ဘာတိုက်ခိုက်မှုနှင့်ပတ်သက်၍ တိုင်ကြားလိုပါက အမျိုးသားဆိုက်ဘာလုံခြုံရေးဗဟိုဌာန၊ ဇမ္ဗူကျက်သရေလမ်း၊ ဇမ္ဗူသီရိမြို့သို့ လူကိုယ်တိုင်ဖြစ်စေ၊ ဆက်သွယ်ရန်ဖုန်းနံပါတ်ဖြစ်သော ၀၆၇-၃၄၂၂၂၇၂ သို့ ဖုန်းဖြင့်ဖြစ်စေ၊ infoteam@mmcert.org.mm နှင့် incident@ncsc.gov.mm တို့သို့ အီးမေးလ်ပေးပို့၍ဖြစ်စေ တိုင်ကြားနိုင်ပါကြောင်း အသိပေးအပ်ပါသည်။

မြန်မာနိုင်ငံကွန်ပျူတာအရေးပေါ်တုံ့ပြန်ရေးအဖွဲ့

Malware နှင့်ပတ်သက်သော IOC များ

၁။ https://versaillesinfo.com/kbezndno

၂။ https://versaillesinfo.com/brjwcabz

၃။ shreyaninfotech.com:443

၄။ Meeting_Invitation.zip (MD5: dc8d487370cb76f6fcc74e50695f0660)

၅။ Meeting_Invitation.msc (MD5: 6aeeedbc67d02e4b2a5a5440570d4319)

၆။ brjwcabz.msi (MD5: aec98e476bf077bddcb5431ed579ca47)

၇။ Meeting_Invitation.pdf (MD5: aa7b8be89ab82a102a2019ff74cf85b6)

၈။ inkform.exe (MD5: 4ec8ac4b2b5ff0e396fa23f32d602f59)

၉။ FormDll.dll (MD5: 5ff177af80ed012fe64422b7ebd52fbd)

၁၀။ inkformDB.dat (MD5: 52aa1f5aa176ac5a4e72bf4d1214b63c)