WannaCry Ransomware အကြောင်းသိကောင်းစရာ

1.1 WannaCry အကြောင်း

WannaCry ဆိုသည်မှာ Ransomware အမျိုးအစား ဖြစ်ပြီး Worm ကဲ့သို့ပင် User ၏လုပ်ဆောင်ချက် မလိုပဲ ၄င်းကိုယ်တိုင် ပျံ့နှံ့နိုင်ပါသည်။ Ransomware ဆိုသည်မှာ Malcious Software ဖြစ်ပြီး Attacker သည် infected ဖြစ်သွားသော User (victim) ၏စက်အတွင်းရှိ File များ, Folder များကို Encrypt ပြုလုပ်လိုက်ပြီး victim မှ ၄င်းFile များကို အသုံးပြုလိုပါက Decrypt ပြုလုပ်ရန် Attacker ဆီသို့ငွေပေးချေရမည် ဖြစ်ပါသည်။

1.2 ဖြစ်စဉ်အကျဉ်းချုပ်

၄င်း Ransomware သည် ၂၀၁၇ခုနှစ် မေလ (၁၂)ရက်နေ့တွင် နိုင်ငံပေါင်း တစ်ရာကျော်ရှိ စက်ပေါင်း ၂၀၀,၀၀၀ ကျော် ကို ထိခိုက်စေခဲ့ပါသည်။

၄င်း Malware သည် လွန်ခဲ့သော လအနည်းငယ်က "ShadowBrokers" ဟုခေါ်သော အဖွဲ့က ထုတ်ပြန်ခဲ့သည့် Exploit များကို အသုံးပြုခဲ့ခြင်း ဖြစ်ပါသည်။ ရလဒ်အားဖြင့် ၄င်း Exploit ကို အသုံးပြုပြီး မကောင်းသောရည်ရွယ်ချက်ဖြင့် လုပ်ဆောင်မှုများကို မြင့်တက်စေပြီး ယခုကဲ့သို့ အခြေအနေများ ဖြစ်ပေါ်စေပါသည်။

Microsoft မှ နေ၍ ၄င်းအားနည်းချက်ကို ဖြေရှင်းထားသည့် Patch Update ကို ၂၀၁၇ ခုနှစ် မတ်လ (၁၄)ရက်နေ့တွင် ထုတ်ပြန်ပေးထားသော်လည်း Update လုပ်ထားသူ နည်းသည်ကို တွေ့ရပါသည်။ ထို့အတွက် ၄င်း Caseဖြစ်သည့် ၂၀၁၇ခုနှစ် မေလ (၁၂)ရက်နေ့မှာပင် Microsoft မှ အရေးပေါ် Patch Update ထုတ်ပြန်ပေးထားပါသည်။ ယခုအခါတွင် ၄င်း Malware ၏ New Version များနှင့် မျိုးကွဲ များထွက်ပေါ်လာပြီး ထိန်းချုပ်ဖို့ ခက်ခဲလာပါသည်။

1.3 Malware နာမည်များ

Wanna Decrypt0r, WCry, WannaCry, WannaCrypt, နှင့် WannCrypt0r

Copyright © 2017, Myanmar Computer Emergency Response Team, mmCERT/cc

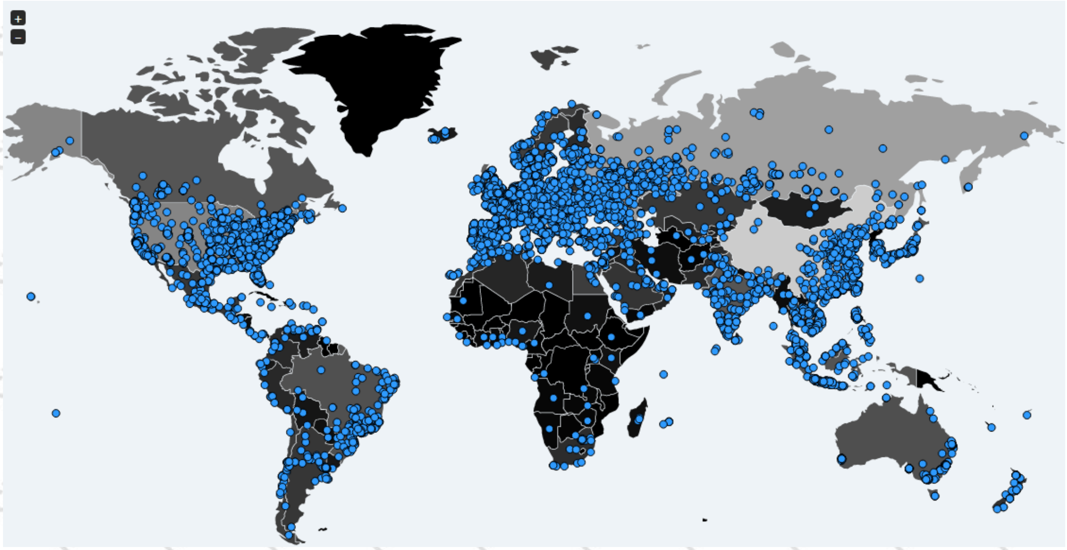
1.4 အားနည်းချက်ရှိသော စက်များ

Windows XP မှ Windows 8.1 (Windows 10 တွင် ၄င်းအားနည်းချက် မရှိပေ)

1.5 Update ပြုလုပ်နိုင်သော Link များ

- Microsoft released a patch MS17-010 (ETERNALBLUE)on 14 March: <https://technet.microsoft.com/en-us/library/security/ms17-010.aspx>
- Microsoft released a patch for the older unsupported Windows versions on 12 May:<https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/>

1.6 WannaCry Ransomware ပျံ့နှံ့ပုံ



1.7 ကြိုတင်ကာကွယ်ခြင်း

- Patch Update များပြုလုပ်ခြင်း
- Backup များပြုလုပ်ထားခြင်း
- Tcp Port 445 ကို Block ထားရပါမည်။ NetBIOS traffic များဖြစ်သော (TCP/137,
- TCP/139, TCP/445, UDP/137 and UDP/138)ကိုလည်း filter ပြုလုပ်သင့်ပါသည်။
- ၄င်းအားနည်းချက် အတွက် SMB1 service ကို Disable ပြုလုပ် ထားသင့်ပါသည်။

Copyright © 2017, Myanmar Computer Emergency Response Team, mmCERT/cc

(https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,-windows-server-2008-r2,-windows-8,-and-windows-server-2012)

1.8 ဖြေရှင်းခြင်း

- ယခုလက်ရှိတွင် အကောင်းဆုံးနည်းကတော့ Backup ပြုလုပ်ထားသည်များမှ Recover ပြန်လုပ်ခြင်း ဖြစ်ပါသည်။ Shadow Volume Copies ကိုအသုံးပြု၍ Fileများ , Folderများကို Recover ပြုလုပ်ခြင်းကို အောက်တွင် ဖော်ပြပေးထားပါသည်။ (https://www.bleepingcomputer.com/tutorials/how-to-recover-files-and-folders-using-shadow-volume-copies/)
- အကယ်၍ သင်၏စက်တွင် Infected ဖြစ်ခဲ့ပါက "DOUBLEPULSAR" Backdoor ကို ထည့်သွင်းထားမည် ဖြစ်သည့်အတွက် ၎င်းကို ဖယ်ရှားရမည် ဖြစ်ပါသည်။ ၎င်း Backdoor ကို ရှိမရှိစစ်ဆေးပြီး ဖယ်ရှားနိုင်သည့် Script ကို အောက်တွင်ဖော်ပြပေးထားပါသည်။ (https://github.com/countercept/doublepulsar-detection-script)

1.9 Reference

WannaCry Ransomware v0.2.pdf, compiled by ThaiCERT

Copyright © 2017, Myanmar Computer Emergency Response Team, mmCERT/cc