MCPA ADVISORY

Petya/NotPetya နှင့် ပတ်သက်၍ မြန်မာနိုင်ငံကွန်ပျူတာပညာရှင်အသင်းမှ ထုတ်ပြန်သော သတိပေးအကြံပြုချက် ၂/၂၀၁၇

Petya/NotPetya

MS17–010 vulnerabilities များမှ ကာကွယ် ပေးသည့် patch များကို ထည့်သွင်းထားရမည် ဖြစ်ပါသည်။

မယုံကြည်ရသော စက်များမှ TCP/445 traffic များကို network / host–based firewalls များဖြင့် ပိတ်ဆို့ပါ။ ဖြစ်နိုင်ပါက Internet–facing Windows စက်များ အား လုံးထံ 445 inbound တားမြစ်ပါ။

SMBv1, WMI, PsExec များကို သင်၏ Network အတွင်း တားမြစ်ထားရန် စဉ်းစားပါ။

Protect Yourself

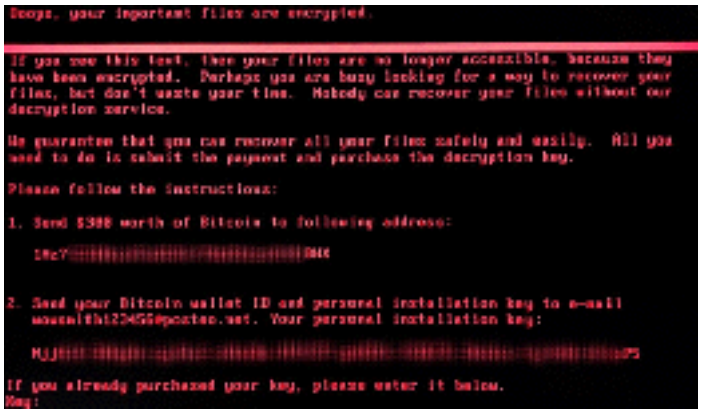
ကွန်ပျူတာ သုံးစွဲသူများသည် အောက်ပါများကို အမြဲလိုက်နာသင့်ပါသည်။

Security Patches and Regular Updates – လုံခြုံရေးဆိုင်ရာ Security Patch များနှင့် ကွန်ပျူတာ OS များကို အစဉ်အမြဲ update ပြုလုပ်ခြင်း

Regular Backups – မိမိတို့ ကွန်ပျူတာ ဖိုင်များကို အခြား လုံခြုံစိတ်ချရသော တစ်နေရာတွင် အရန်အဖြစ် သိမ်းဆည်းခြင်း

Security software – မိမိတို့ anti–virus ဆော့ဖ်ဝဲများကို အမြဲ update လုပ်နေခြင်း၊ anti–malware, anti–ransomware စွမ်းဆောင်ချက်များ ပါဝင်သည့် security software များ တပ်ဆင်ခြင်း

Beware Phishing – မည်သူမှန်း မသိပါက သို့မဟုတ် သိကျွမ်းသူ ဖြစ်သော်လည်း ပုံမှန်မဟုတ်သည့် ဖိုင်များ ပေးပို့လာပါက နှိပ်ဖွင့်ခြင်းမှ ရှောင်ကြဉ်ခြင်း



MCPA's Advisory on Petya/NotPetya Ransomware

Petya/NotPetya အမည်ရ ဆိုက်ဘာတိုက်ခိုက်မှု တစ်ခုသည် Microsoft Windows စနစ်များကို ဦးတည် တိုက်ခိုက်လျက် ရှိပါသည်။ တိုက်ခိုက်ခံရပါက မိမိ၏ ဖိုင်များကို သာမန် ကြည့်ရှု သုံးစွဲခွင့် မပြုနိုင်တော့ရန် encrypt လုပ်ကာ သိမ်းဆည်းခြင်း၊ သို့မဟုတ် ဖျက်ဆီးခံရပြီး (wipe) စနစ်တစ်ခုလုံး သုံးစွဲခြင်း မရနိုင်ရန် အထိ ဖြစ်သွားနိုင်ပါသည်။ ယခုအချိန်တွင် encrypt / wipe လုပ်ခံရသော ဖိုင်များကို ပြန်ရရန် နည်းလမ်း မရှိသေးပါ။

How it spreads

ထို malware သည် စက်၏ credentials များ (User IDs, Passwords) ကို ထုတ်ယူကာ Microsoft system management tools များဖြစ်သည့် WMI နှင့် PSEXEC တို့ကို သုံးစွဲကာ ချိတ်ဆက်ထားသည့် Microsoft Windows Networks များသို့ ဆက်လက် ပျံ့နှံ့စေပါသည်။

Other References

1. Myanmar CERT ၏ သတိပေးကြေညာချက် (မြန်မာဘာသာ)
2. SecureList
3. Malware Bytes
4. New Zealand CERT

www.mcpamyanmar.org