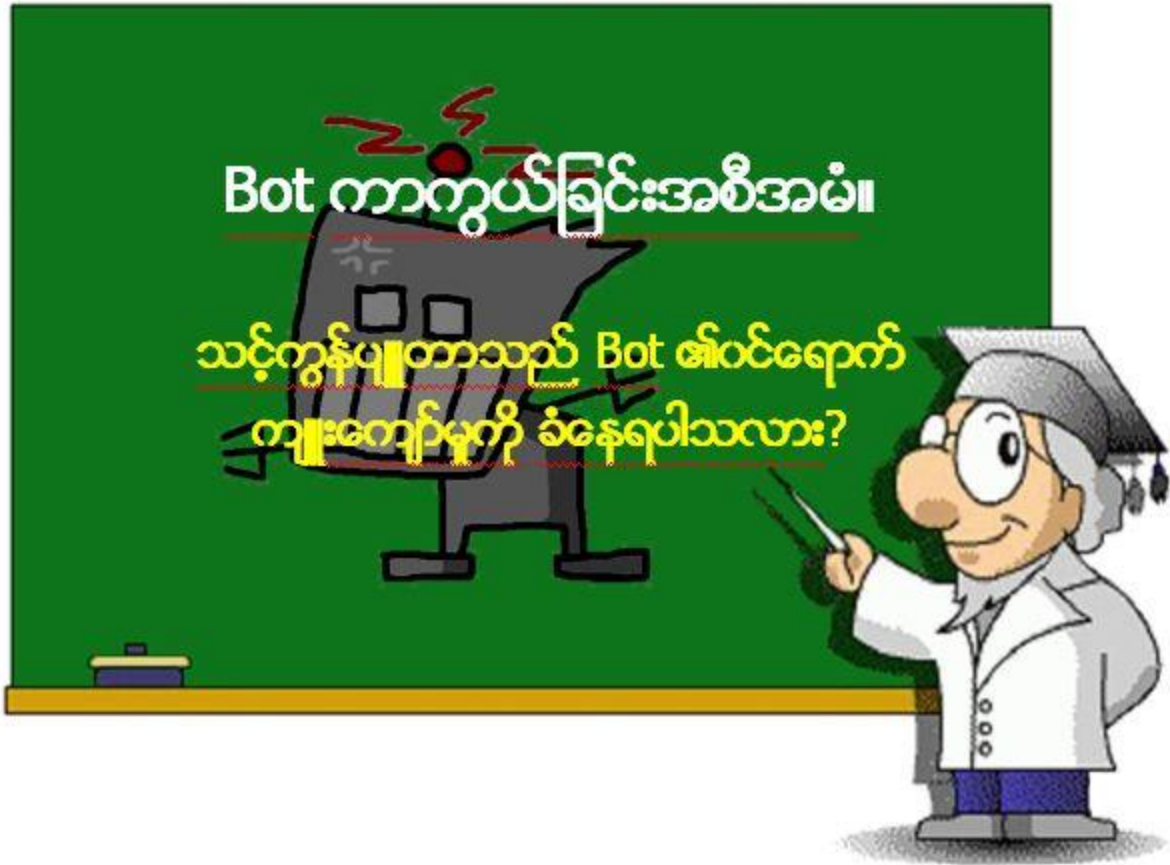


ကီးကီး



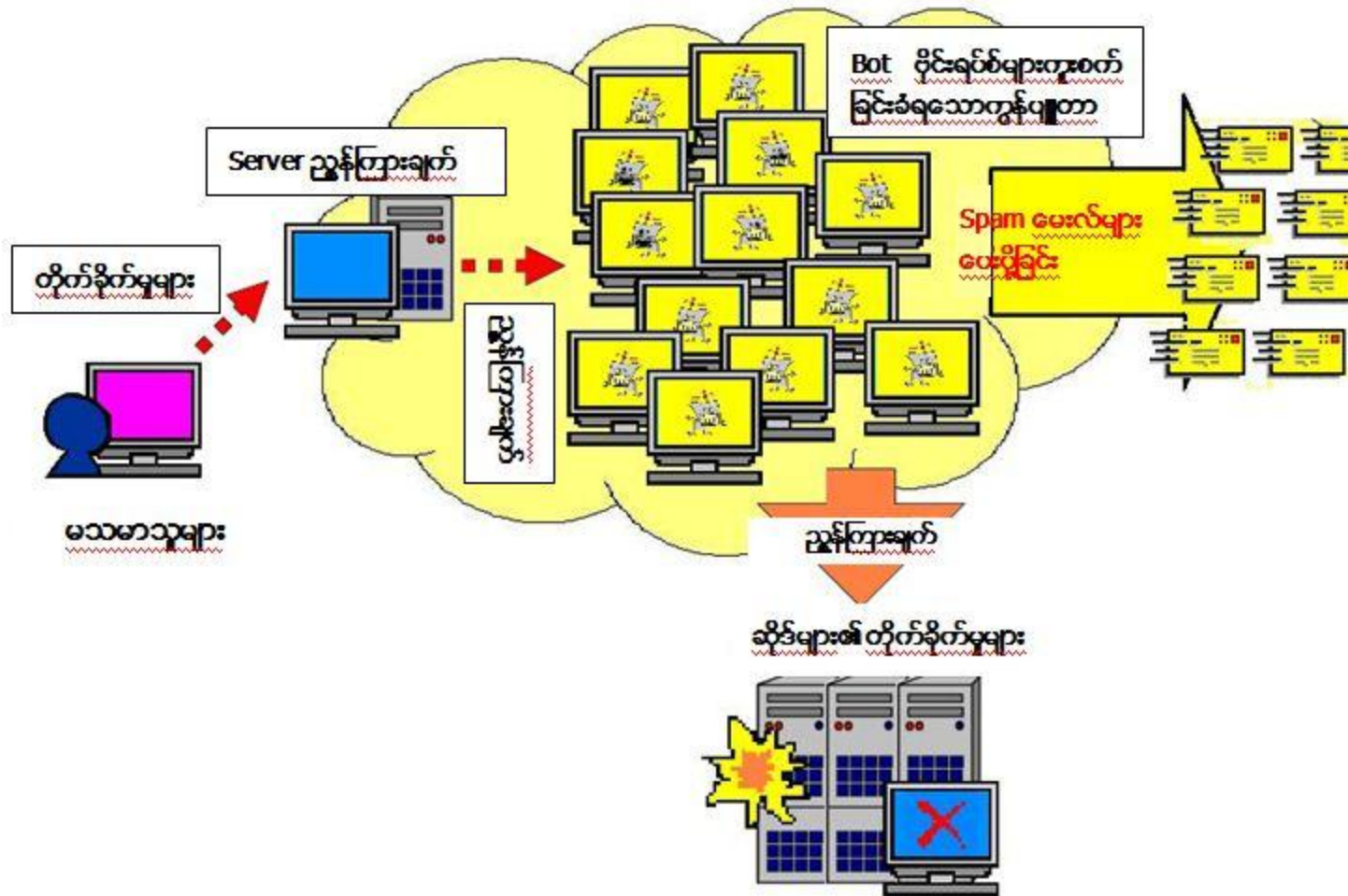
၁။ Bot ဆိုသည်မှာ



Bot ဆိုသည်မှာ ကွန်ပျူတာဗိုင်းရပ်စ် တစ်မျိုးဖြစ်ပြီး အင်တာနက်မှ တဆင့် ကွန်ပျူတာအတွင်း ကူးစက်ပျံ့ပွားသော ကွန်ပျူတာညွှန်ကြား ချက်စနစ် ဖြစ်ပါသည်။
၎င်းဗိုင်းရပ်စ်များ၏ ကူးစက်ခြင်းခံရပါက ၎င်းဗိုင်းရပ်စ်များသည် အပြင် အင်တာနက်မှ ညွှန်ကြားစေခိုင်းချက်များအတိုင်း မိမိကွန်ပျူတာအတွင်း တွင် ထိန်းချုပ်လုပ်ဆောင်ခြင်းများကို ပြုလုပ်ပါသည်။ Robot ကဲ့သို့ အလို အလျောက် လှုပ်ရှားမှုများကြောင့် ၎င်းကို Bot ဟုခေါ်ဆိုခြင်းဖြစ်ပါသည်။

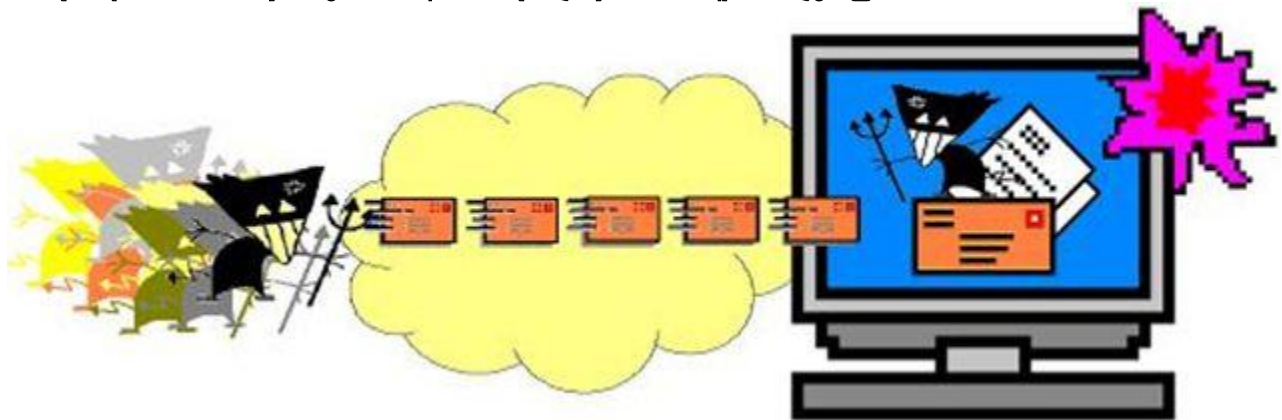
၂။ Bot Network ၏ခြင်းခြောက်မှု

မြောက်များစွာသော (ရာထောင်သောင်းထက်မကသော) Bot ဗိုင်းရပ်စ်များသည် Server တစ်ခုကိုဗဟိုပြု၍ Network ၏ ညွှန်ကြားစေခိုင်းချက်များအောက်တွင်ရှိနေသောကြောင့် Bot Network ဟုခေါ်ဆိုခြင်းဖြစ်ပါသည်။ Bot Network သည် Phishing (*1) မြောက်များစွာသော Spam မေးလ်များပေးပို့ခြင်း (*2) ၊ သတ်မှတ်ထားသော ဆိုင်များ၏ DDoS တိုက်ခိုက်မှုများ (*3) စသည်တို့တွင် အသုံးပြုခြင်းခံရပါက အလွန်အန္တရာယ် ဖြစ်ပေါ်စေနိုင်ပါသည်။



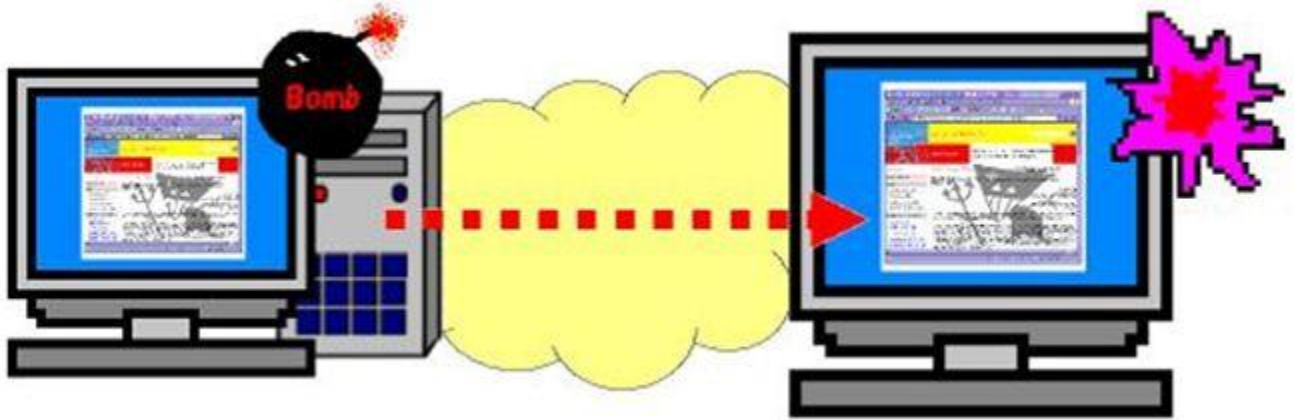
၃။ ဘယ်လို ကူးစက်ပျံ့ပွားသလဲဆိုရင်
ကူးစက်ပျံ့ပွားနည်းများကို အောက်တွင်ဖော်ပြထားပါသည်။

1) ဗိုင်းရပ်စ်အီးမေးလ်နှင့် တွဲဆက်နေသော ဗိုင်းရပ်စ်များမှတစ်ဆင့် ကူးစက်ပျံ့ပွားခြင်း။

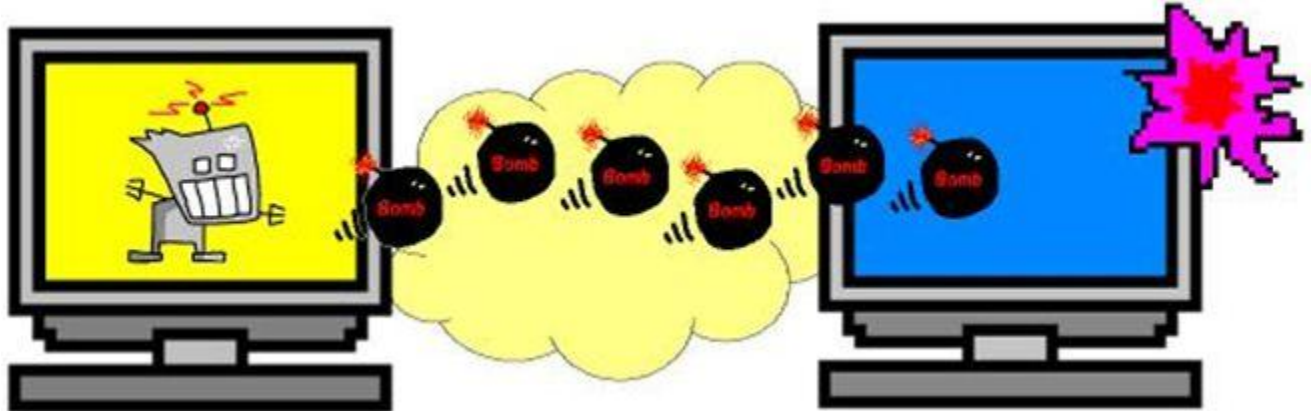


2) သံသယဖြစ်ဖွယ် ဆိုင်များသို့ ဝင်ရောက်ရာမှတစ်ဆင့် ကူးစက်ပျံ့ပွားခြင်း။

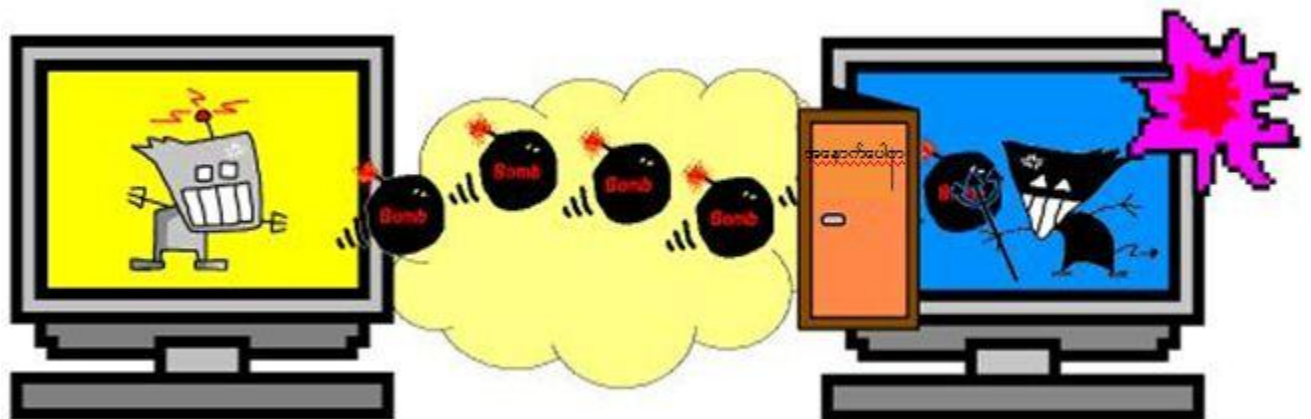
3) Spam မေးလ်များတွင် ဖော်ပြသောလင့်ခ် (URL) များသို့ ဝင်ရောက်ရာမှတစ်ဆင့် တရားမဝင်သောဆိုင်များသို့ ရောက်ရှိ သွားပြီး ထိုမှတစ်ဆင့်ကူးစက်ပျံ့ပွားခြင်း။



4) ကွန်ပျူတာ၏ လုံခြုံရေးစနစ်အားနည်းချက် (*4) များရှိပါက အင်တာနက်မှတစ်ဆင့် သံသယဖြစ်ဖွယ်ဆိုင်များမှ ဗိုင်းရပ်စ်များ ကူးစက်ပျံ့ပွားခြင်း။



5) တခြားသော ဗိုင်းရပ်စ်များ၏ ကူးစက်ခြင်းခံရသောအခါ ကွန်ပျူတာ၏စနစ်အတွင်းရှိ backdoor (*5) မှတစ်ဆင့် အင်တာနက်မှ ဗိုင်းရပ်စ်များ ကူးစက်ပျံ့ပွားခြင်း။



ထို့အပြင် အောက်ပါနည်းများအတိုင်း ကူးစက်ပျံ့ပွားခြင်းများရှိသောကြောင့် အထူးဂရုပြုရန် လိုအပ်ပါသည်။

6) ဗိုင်များအချင်းချင်း လဲလှယ်ခြင်း (PtoP) မှတစ်ဆင့် ကူးစက်ပျံ့ပွားခြင်း။

7) Instant messenger (*6) ကို အသုံးပြုရာမှတစ်ဆင့် ကူးစက်ပျံ့ပွားခြင်း။

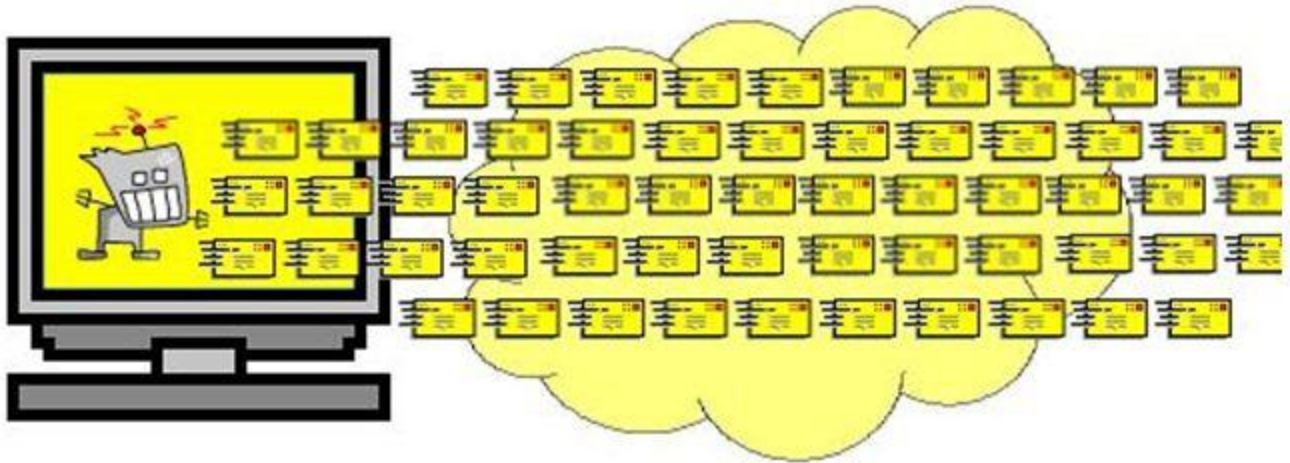
၎င်းတို့များထဲတွင် 4) ၏ ကွန်ပျူတာလုံခြုံရေးစနစ်အားနည်းချက်မှတစ်ဆင့် ကူးစက်ပျံ့ပွားခြင်းသည် အင်တာနက်နှင့် ချိတ်ဆက်ရုံဖြင့် ကူးစက်ပျံ့ပွားစေတတ်ပါသည်။ ၎င်းသည် ကွန်ပျူတာအသုံးပြုသူမသိချိန်အတွင်းတွင် အလိုအလျောက် ကူးစက်ပျံ့ပွားစေတတ်သဖြင့် အထူးဂရုပြုရန် လိုအပ်ပါသည်။ ဤကိစ္စသည် Microsoft Update စသည်တို့ဖြင့် မိမိကွန်ပျူတာ၏ လုံခြုံရေးစနစ်အားနည်းခြင်းကို ဖယ်ရှားပေးရုံသာမက Network မှသံသယဖြစ်ဖွယ်ဆိုင်များကို ကာကွယ်ခြင်း များပြုလုပ်ခြင်းဖြင့် ခုခံနိုင်ပါသည်။

၄။ ကူးစက်ပျံ့ပွားခြင်းခံရပြီးနောက် လုပ်ဆောင်ပုံ

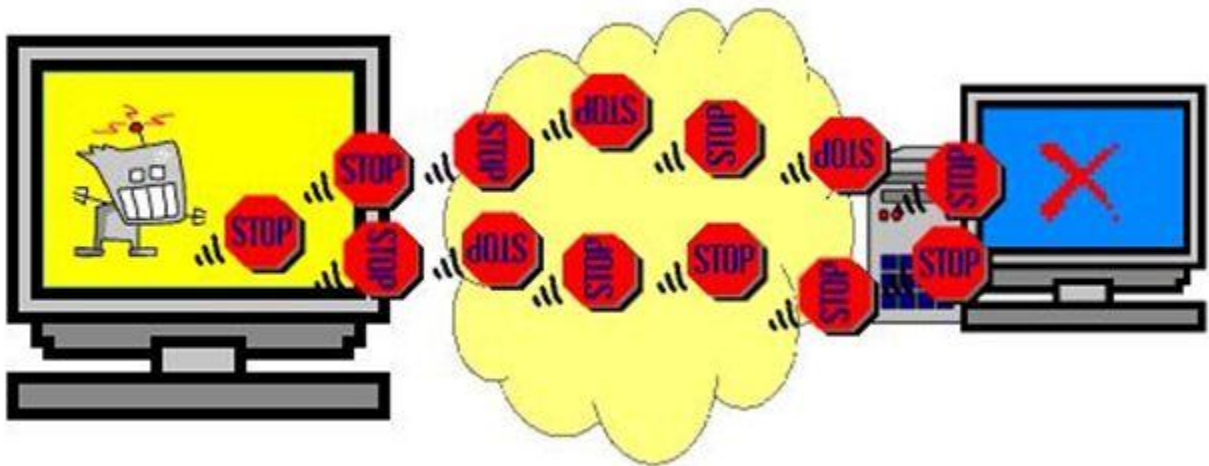
ကူးစက်ပျံ့ပွားခြင်းခံရလျှင် Network မှတစ်ဆင့် အပြင်မှ Server ၏ညွှန်ကြားချက်များအတိုင်း (Bot အများစုသည် IRC (Internet Relay Chat) (*7) ကိုအသုံးပြုသည်) (Spam မေးလ်များပေးပို့ခြင်း၊ DoS တိုက်ခိုက်မှု (*3) စသဖြင့် network မှတစ်ဆင့် ကူးစက်ပျံ့ပွားခြင်း၊ Network Scanning (*8) စသည်တို့ကိုဖြစ်ပေါ်စေပါသည်။ ထို့အပြင် မိမိကွန်ပျူတာ၏ Version up နှင့် Server ၏ညွှန်ကြားချက်များတွင်လည်း ပြောင်းလဲမှုများကို ဖြစ်ပေါ်စေပါသည်။ သို့သော် ၎င်းဗိုင်းရပ်များ၏ ကူးစက်ပျံ့ပွားမှုများသည် မိမိတို့သတိမပြုမိချိန်အတွင်း အလိုအလျောက် ဝင်ရောက်တိုက်ခိုက်တတ်သောကြောင့် ကွန်ပျူတာအသုံးပြုသူများအတွက် အလွန်အန္တရာယ်ပေးသောအရာဖြစ်ပါသည်။



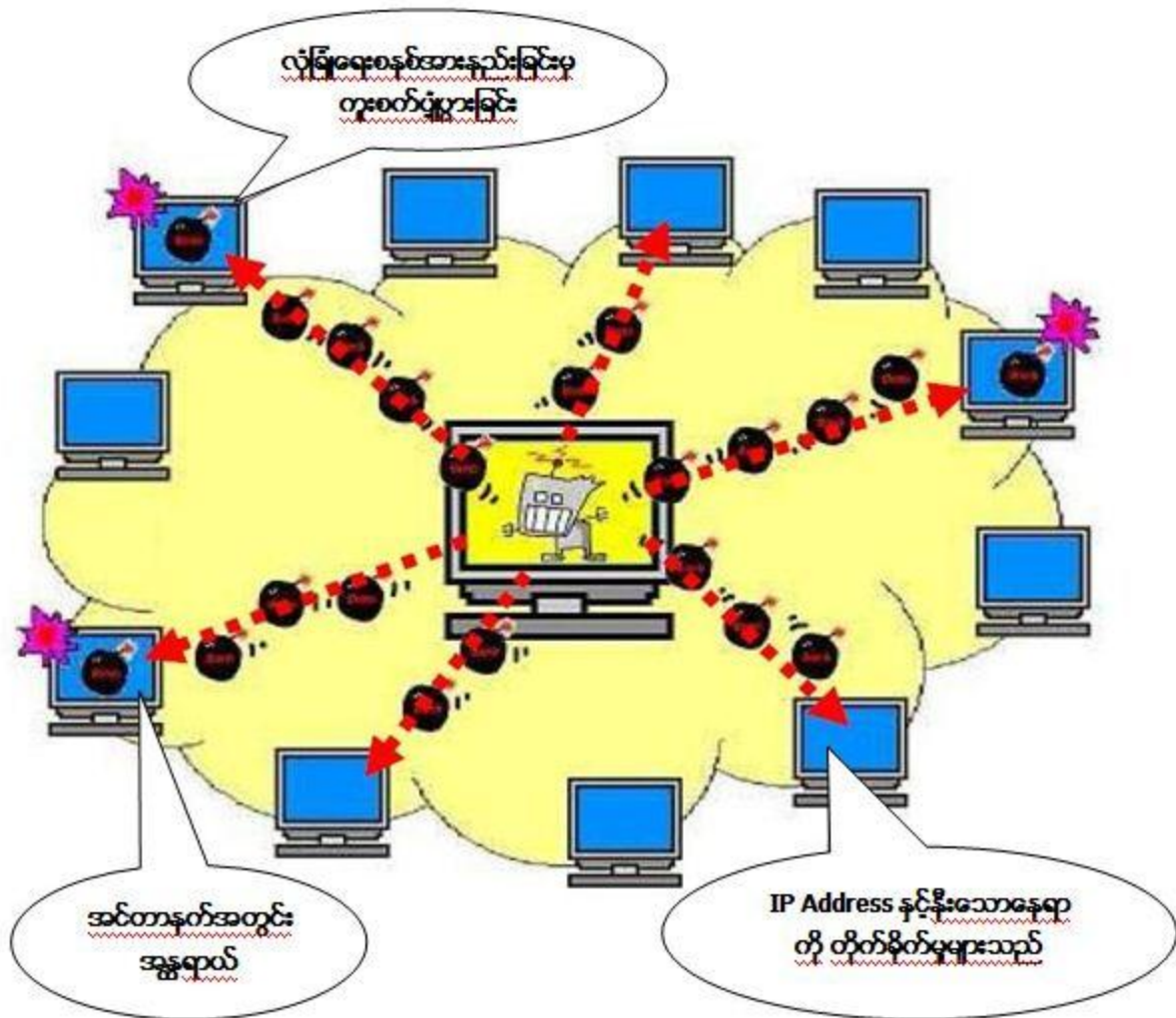
1) Spam mails များပေးပို့ခြင်း (မြောက်များစွာသော Spam မေးလ် (*2) များပေးပို့ခြင်း)



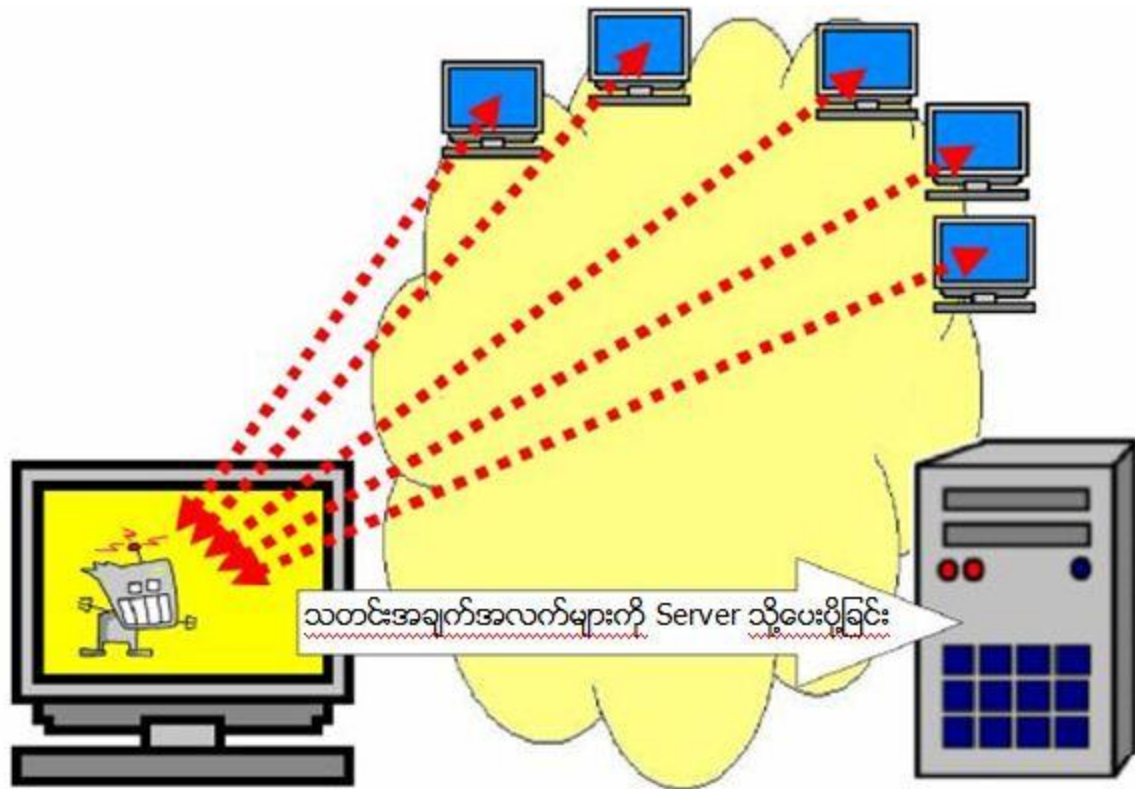
2) DoS စသည်တို့၏တိုက်ခိုက်မှုများ (သတ်မှတ်ထားသောဆိုဒ်များသို့ ဝင်ရောက်ရာတွင် နှောင့်ယှက်တိုက်ခိုက်မှု များပြုလုပ်ခြင်း)



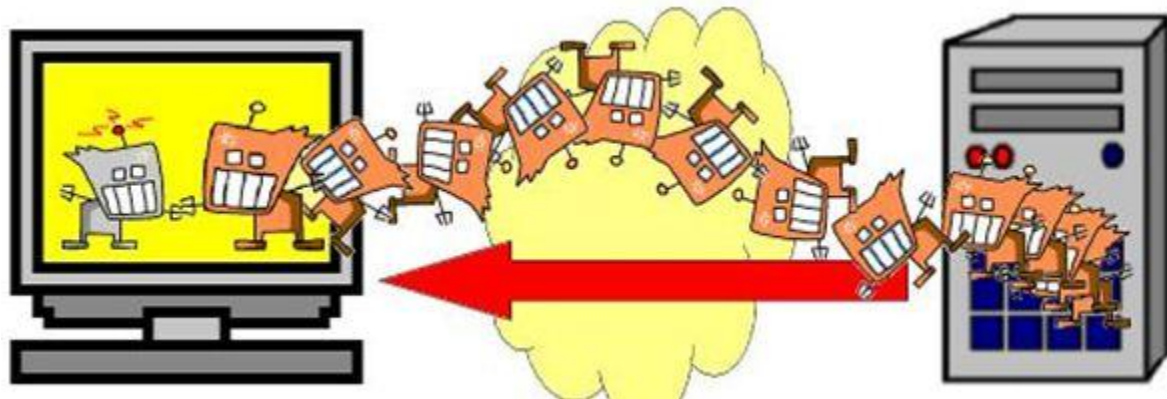
3) Network မှတစ်ဆင့် ကူးစက်ပျံ့ပွားခြင်း (ကွန်ပျူတာ၏ လုံခြုံရေးစနစ်အားနည်းခြင်းမှတစ်ဆင့် ဝိုင်းရပ်များ ကူးစက်ပျံ့ပွားခြင်း)



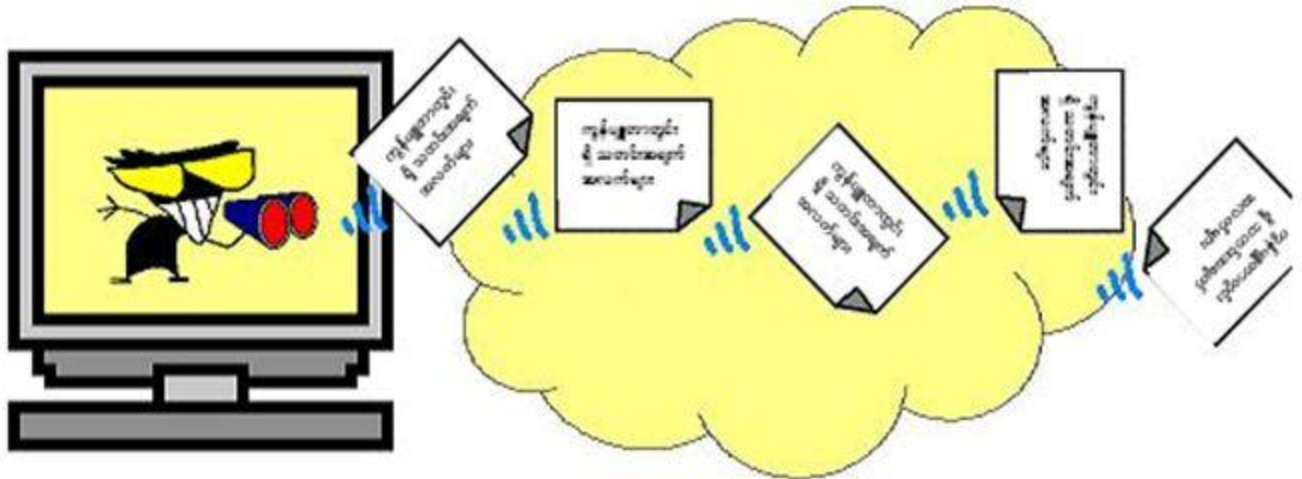
4) Network Scan ပြုလုပ်ခြင်း (ကူးစက်ပျံ့နှံ့ခြင်းပုံများနှင့် လုံခြုံရေးစနစ်အားနည်းသော ကွန်ပျူတာ၏ သတင်းအချက် အလက်များကို စုဆောင်းခြင်း)



5) မိမိကွန်ပျူတာ၏ Version up နှင့် Server ညွှန်ကြားချက်များ၏ ပြောင်းလဲမှုများကို ဖြစ်ပေါ်စေခြင်း။



6) Spy ပြုလုပ်ခြင်း။ (ကူးစက်ခံရသောကွန်ပျူတာအတွင်းမှသတင်းအချက်အလက်များကို ပြင်ပသို့ပေးပို့ခြင်း)



1. Bot ၏ကူးစက်ပျံ့ပွားခြင်းကို စစ်ဆေးပြီးဖယ်ရှားပေးသည့်နည်းလမ်းများ

(Windows ကိုအသုံးပြုသောအခါ)

လက်တလောတွင် Bot ဗိုင်းရပ်စ်များသည် အသုံးပြုသူသတိမပြုမိချိန်အတွင်း အမျိုးမျိုးသော နည်းလမ်းများကိုအသုံးပြု၍ ကူးစက်ပျံ့ပွားပါသည်။ ဥပမာ၊ ဗိုင်းရပ်စ်နိမ်နင်းရေး ဆော့ဝဲလ် (Antivirus) ကိုအသုံးပြုသောအခါ Bot ဗိုင်းရပ်စ်များ သည် ထိုဆော့ဝဲလ်၏ ဗိုင်းရပ်စ်ဖိုင် (Virus Definition file) များကို ဝင်ရောက်နှောက်ယှက်ခြင်း၊ ဆော့ဝဲလ်စနစ်ကို ရပ်တန့်စေခြင်း စသည်တို့ကိုပြုလုပ်ပါသည်။ ထို့အပြင် ကွန်ပျူတာအသုံးပြုနေစဉ်အတွင်း အသုံးပြုသူသတိ မပြုမိနိုင်သော ကွန်ပျူတာစနစ်၏မူရင်းလုပ်ဆောင်နေသောအမည်များကို အသုံးပြု၍ ကွန်ပျူတာ အတွင်း ဝင်ရောက်ကူးစက် တတ်ပါသည်။ အဆိုးရွားဆုံးအခြေအနေတွင် ကွန်ပျူတာစနစ်ကို ဖွင့်၍မရနိုင်သည့်အခြေအနေအထိ ဖြစ်တတ်ပါသည်။

သင်၏ကွန်ပျူတာတွင် သံသယဖြစ်ဖွယ်တွေ့ရှိပါက အောက်ဖော်ပြပါနည်းလမ်းများကိုအသုံးပြု၍ Bot ဗိုင်းရပ်စ်၏ ကူးစက်ပျံ့ပွားမှုကို ရှာဖွေစစ်ဆေးပါ။

1) မိမိ၏ကွန်ပျူတာကို Update ပြုလုပ်ပါ။

Microsoft Update ပြုလုပ်ပါ။

ထိုသို့ပြုလုပ်ရန် Microsoft ၏ ဆိုဒ်သို့ မဝင်ရောက်နိုင်လျှင် Bot (သို့မဟုတ် ဗိုင်းရပ်စ်)များ၏ တားဆီးနှောက်ယှက်ခြင်းကို ခံနေရနိုင်သော ကြောင့် 3) အတိုင်းပြုလုပ်ပါ။ ၎င်းနောက် မမှန်ကန်သော ညွှန်ကြားမှုများ ခံနေရပါက Microsoft Update ကိုနှောက်တစ်ကြိမ်ထပ်မံပြုလုပ်ပါ။



◆ Microsoft Update

<http://www.update.microsoft.com/microsoftupdate/v6/default.aspx>

◆ Microsoft Update ၏အသုံးပြုပုံ

<http://www.microsoft.com/en-us/windows/help/windows-update>

Microsoft Update ကိုပြုလုပ်နေစဉ်တွင် “မလိုလားသောဆော့ဝဲလ်များကိုဖယ်ရှားခြင်း Tool” သည်လည်းလုပ်ဆောင်နေပါသည်။ ထို Tool သည် အမျိုးအစားမြောက်များစွာသော Bot ပရိုဂရမ်များကိုရှာဖွေ၍ တွေ့ရှိပါက ဖယ်ရှားပေးပါသည်။ တနည်းအားဖြင့် အခမဲ့နှိမ်နင်းပေးသော ဆော့ဝဲလ်ဟု ခေါ်ဆိုနိုင်သောလည်း Microsoft Update ကို ပြုလုပ်နေစဉ်အတွင်းသာလျှင် လုပ်ဆောင်ပေးသည့်အတွက် လိုအပ်ပါက မိမိကိုယ်တိုင် Microsoft Download မှ ထို Tool ကိုဒေါင်းလုပ်ရယူပါ။ ဒေါင်းလုတ်လုပ်ထားသော Tool ရှိပါကအချိန်မရွေးဆောင်ရွက်နိုင်ပါသည်။

◆ မလိုလားသောဆော့ဝဲလ်များကိုဖယ်ရှားခြင်း Tool

<http://www.microsoft.com/security/pc-security/malware-removal.aspx>

2) ဗိုင်းရပ်စ်နှိမ်နင်းရေးဆော့ဝဲလ်ကို Update ပြုလုပ်၍ ဗိုင်းရပ်စ်စစ်ဆေးခြင်းကိုပြု လုပ်ပါ။



ပိုင်းရပ်စ်နှိမ်နင်းရေးဆော့ဝဲလ်ကို အသုံးပြုသူသည် အွန်လိုင်းမှ တဆင့် အခမဲ့ပိုင်းရပ်စ် စစ်ဆေးနှိမ်နင်းနည်းများကို အသုံးပြုနိုင်သည့်အတွက် ၎င်း တို့ကို အသုံးပြုပါ။

အကယ်၍ အခမဲ့ပိုင်းရပ်စ် စစ်ဆေးနှိမ်နင်းရေးဆိုဒ်များသို့ ဝင်ရောက်သုံး စွဲခြင်းမပြုနိုင်ပါက Bot (သို့မဟုတ် ပိုင်းရပ်စ်) များ၏ တားစီးနှောင့်ယှက် ခြင်းကို ခံနေရနိုင်သောကြောင့် 3) အတိုင်းပြုလုပ်ပါ။ မမှန်ကန်သော ညွှန်ကြားမှုများ ခံနေရပါက နောက်တစ်ကြိမ် ပိုင်းရပ်စ်နှိမ်နင်းရေးဆော့ဝဲလ်ကို Update ထပ်မံပြုလုပ်၍ ပိုင်းရပ်စ်စစ်ဆေးခြင်းကိုပြုလုပ်ပါ။ သို့မဟုတ် အွန်လိုင်း Scan ကိုပြုလုပ်ပါ။

(သတိပြု: အွန်လိုင်း Scan သည် တခါတရံ ပိုင်းရပ်စ်များကို ဖယ်ရှား မပေးနိုင်ပါ။ ရှာဖွေတွေ့ရှိသော ပိုင်းရပ်စ်များကို သက်ဆိုင်ရာ ပိုင်းရပ်စ်ဖယ်ရှားရေးနည်းလမ်းများအတိုင်း ဖယ်ရှားပါ။)

လတ်တလော ပိုင်းရပ်စ်နှိမ်နင်းရေး ဆော့ဝဲလ်များသည် ဘက်ပေါင်းစုံလုံခြုံမှုစနစ် ကာကွယ်ခြင်း ဆော့ဝဲလ် အသွင်သို့ ကူးပြောင်းနေပါသည်။ ဘက်ပေါင်းစုံ လုံခြုံမှုစနစ် ကာကွယ်ခြင်းဆော့ဝဲလ်တွင် Firewall စနစ်ပါဝင်သောကြောင့် Network မှတဆင့် ကူးစက်ပျံ့ပွားခြင်းကိုကာကွယ်ပေးနိုင်ပါသည်။

ထို့အပြင် ကွန်ပျူတာတွင် Bot ၏ကူးစက်ခံနေရသောအချိန်တွင်လည်း အသုံးပြုသူ ညွှန်ကြားချက်မပါဘဲ လုပ်ဆောင် ခြင်းများကို သိရှိ/တားမြစ်နိုင်သည့်အတွက် Bot ၏ ကူးစက်ခံနေရသည်ကို အလွယ်တကူသတိပြုမိနိုင်ပါသည်။ ထိုကဲ့သို့ ဘက်ပေါင်းစုံ လုံခြုံမှုစနစ် ကာကွယ်ခြင်းဆော့ဝဲလ်ကို အသုံးပြုခြင်းသည် အရေးကြီးသော အစီအမံတစ်ခုဖြစ်ပါသည်။

3) အောက်ဖော်ပြပါ ဖိုင်များကို စစ်ဆေးပါ။

• HOSTSファイル

Windows NT,2000の場合は、

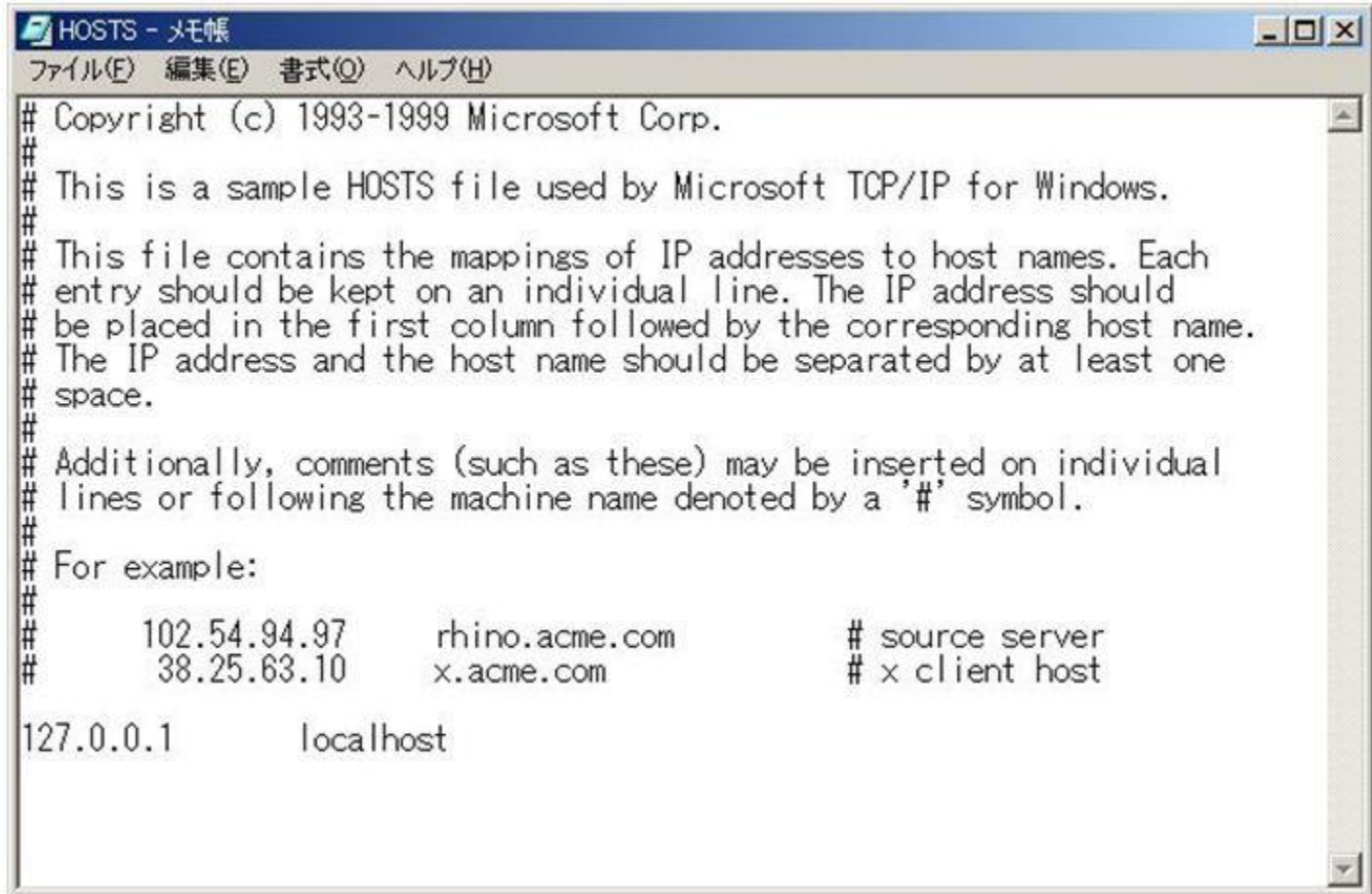
C:\WINNT\SYSTEM32\DRIVERS\ETCのフォルダにあるHOSTSファイル

Windows XP,Vistaの場合は、

C:\WINDOWS\SYSTEM32\DRIVERS\ETCのフォルダにあるHOSTSファイル

★ ပါဝင်သည့်အကြောင်းအရာများကို စစ်ဆေးသည့်အခါ Notepad (notepad.exe) ကိုအသုံးပြုပါ။

ထိုစိုင်းများသည် Network နှင့်ဆက်သွယ်သောအခါတွင် သတ်မှတ်ထားသော စိုင်းများဖြစ်သည်။
မမှန်ကန်သောစနစ် ကို ပြုလုပ်ထားပါက သတ်မှတ်ထားဆိုင်၏ URL သို့ဆက်သွယ်လိုသောအခါတွင် အခြား
IP Address သို့ ဆက်သွယ်စေ ခြင်း ကိုဖြစ်စေပါသည်။



```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com           # source server
#       38.25.63.10       x.acme.com               # x client host
#
127.0.0.1       localhost
```

ထိုစိုင်းကို ပြုပြင်ပြောင်းလဲခြင်းမပြုလုပ်နိုင်ပါက အောက်ပါစနစ် (Localhost) သာလျှင်
မှတ်ပုံတင်ထားခြင်းဖြစ်ပြီး အခြားသောစနစ်များတွင် အောက်ပါအကြောင်းအရာများကိုစစ်ဆေးပါ။
ထိုစိုင်းတွင် Microsoft Website ၏ URL ပါဝင်လျှင် (သို့) ဗိုင်းရပ်စ်နီမန်းရေး Website ပါဝင်လျှင်
၎င်းတို့ကိုဖယ်ရှား ရန်လိုအပ်ပါသည်။ (127.0.0.1 သည် မိမိ၏ကွန်ပျူတာကို ရည်ညွှန်းပါသည်)

127.0.0.1 localhost

အောက်ပါတို့သည် မမှန်ကန်သောစနစ်၏ ဥပမာများဖြစ်သည်။

127.0.0.1 www.microsoft.com
127.0.0.1 www.nai.com
127.0.0.1 trendmicro.com
127.0.0.1 update.symantec.com
127.0.0.1 updates.symantec.com

သို့သော်စာကြောင်းအစတွင်ဤသင်္ကေတ (#) ပါရှိပါက Comment ဖြစ်သည့်အတွက် စိတ်ပူစရာမလိုပါ။

၆။ ယေဘုယျအသုံးပြုသူများ သတိပြုရမည့်အချက်များ။

ယေဘုယျအသုံးပြုသူများသည် အင်တာနက်အသုံးပြုသောအခါ Bot ဗိုင်းရပ်စ်များ၏ကူးစက်ခြင်း မခံရစေရန် အောက်ဖော်ပြပါကာကွယ်နည်းများကို ပြုလုပ်ရန်လိုအပ်ပါသည်။

(1) လုံခြုံမှုစနစ်ကာကွယ်ခြင်း ဆော့ဝဲလ် ကိုထည့်သွင်းပါ။

ဗိုင်းရပ်စ်ကာကွယ်ခြင်းဆော့ဝဲလ်၊ Spyware ကာကွယ်ခြင်းဆော့ဝဲလ် (သို့မဟုတ် ဘက်ပေါင်းစုံလုံခြုံမှု စနစ်ကာကွယ်ခြင်းဆော့ဝဲလ်) ကိုထည့်သွင်းပါ။ ထို ဆော့ဝဲလ်များသည် ဗိုင်းရပ်စ်ဖိုင် (Virus Definition File) များ၏ Update နှင့် ဗိုင်းရပ်စ် စစ်ဆေးခြင်းများကိုပြုလုပ်ပါသည်။

(2) အီးမေးလ်နှင့် တွဲဆက်နေသော ဖိုင်များကိုဂရုပြုပါ။ မိမိနှင့်မသိသောသူများထံမှ မေးလ်များနှင့် တွဲဆက်ဖိုင်များကို မဖွင့်ပါနှင့်။ အထူးသဖြင့် ခိုင်မာစွာဖွဲ့စည်းထားသော တွဲဆက်ဖိုင်များကို အထူးဂရုပြုရပါမည်။



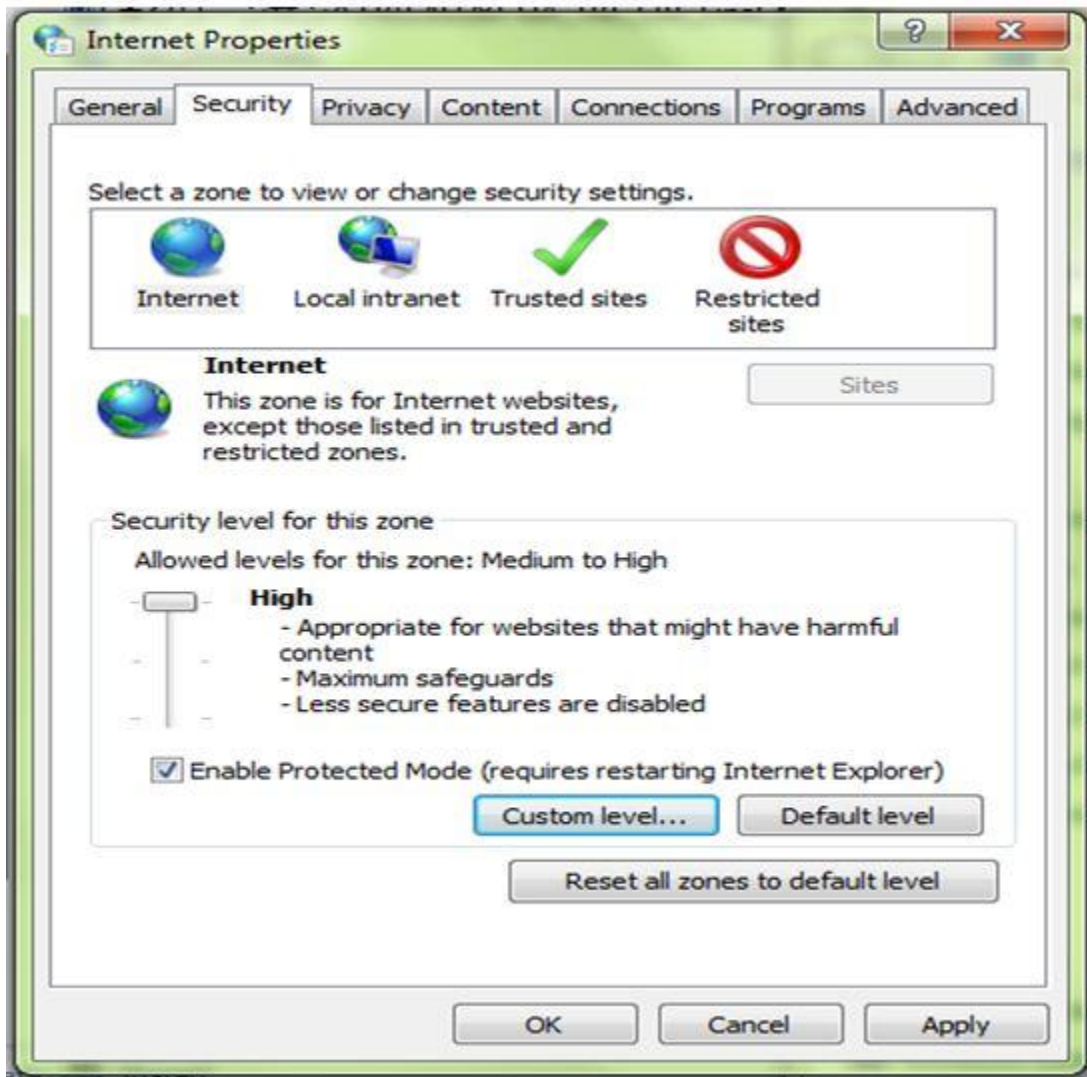
(3) သံသယဖြစ်ဖွယ် ဆိုဒ်များသို့ဝင်ရောက်ခြင်းကိုရှောင်ကြဉ်ပါ။

သင့်ကွန်ပျူတာအတွင်းသို့ မမှန်ကန်သော ပရိုဂရမ်များ ဝင်ရောက် စေရန် ရည်ရွယ်ထားသော ဝဘ်ဆိုဒ်များရှိပါသည်။ သင့်ကွန်ပျူတာ အတွင်း လုံခြုံရေးစနစ်ကာကွယ်မှု မလုံလောက်ပါက ထိုဝဘ်ဆိုဒ်များ သို့ ဝင်ရောက်ခြင်းသည် အန္တရာယ်ရှိပါသည်။



(4) Browser ၏ Internet Options (Security Options) ကိုထိရောက်စွာအသုံးပြုခြင်း

ယုံကြည်စိတ်ချရသောဝဘ်ဆိုဒ်များနှင့် မယုံကြည်ရသောဝဘ်ဆိုဒ်များကို အမျိုးအစားခွဲခြားပြီး မယုံကြည်ရသောဝဘ်ဆိုဒ်များသို့ ဝင်ရောက်မိသောအခါ ကွန်ပျူတာ၏လုံခြုံရေးစနစ်အဆင့်ကို High တွင်ထားရှိပါ။ (အောက်ပါပုံသည် Internet Explorer 7၏ the Internet Options ဖြစ်သည်)



Internet Explorer တွင်လုံခြုံမှုစနစ်ကိုသေချာစေရမည်။

http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/zone_ovr.msp?mfr=true

(5) Spam မေးလ် စသည်တို့ပါဝင်သော ဖြားယောင်းဖိတ်ခေါ်ထားသော လင့်ခ်များကို မဖွင့်ပါနှင့်။

Spam မေးလ် စသည်တို့ပါဝင်သော ဖြားယောင်းဖိတ်ခေါ်ထားသော လင့်ခ်များကို အထူးဂရုပြုရန် လိုအပ်ပါသည်။ (3) တွင်ဖော်ပြထားသည့်အတိုင်း သံသယဖြစ်ဖွယ် ဆိုဒ်များသို့ ဝင်ရောက်စေခြင်းဖြစ်ပါသည်။

Present?



(6) အင်တာနက်စနစ်ကို လုံခြုံစေရန်ဆက်သွယ်ထားသော Router (သို့) ကိုယ်ပိုင် Firewall ကို ကွန်ပျူတာအတွင်းထည့်သွင်းပြီး မှန်ကန်သောညွှန်ကြားမှုများပြုလုပ်ခြင်း။
သင့်ကွန်ပျူတာနှင့် Network ကိုအင်တာနက်မှတစ်ဆင့် ဝိုင်းရပ်စ်ကူးစက်ခြင်းကို ကာကွယ်နိုင်ရန် Router (သို့) ကိုယ်ပိုင် Firewall ကိုဝယ်ယူထည့်သွင်းခြင်းပြုလုပ်ရန် အကြံပြုပါသည်။
အကယ်၍ ဝိုင်းရပ်စ် ကူးစက်ခြင်း ခံရပါကလည်း မိမိကွန်ပျူတာ (သို့) Network အတွင်းမှ အချက်အလက်များ အင်တာနက်မှတစ်ဆင့် ပြင်ပသို့ ပျံ့ပွားခြင်းကို ကာကွယ်ပေးနိုင်ပါသည်။

(7) မိမိကွန်ပျူတာ၏ OS နှင့် Application များကိုအမြဲ Update လုပ်ပါ။ (Microsoft Update လုပ်ပါ။)

Web လုပ်ဆောင်သူများလိုက်နာရမည့် Bot ကာကွယ်ရေးအချက်များ

Web လုပ်ဆောင်သူများ၊ အင်တာနက်မှသတင်းအချက်အလက်များကို အသုံးပြုသူများသည် Bot ဝိုင်းရပ်စ်များ ၏ ကူးစက်ခြင်းကို မခံရစေရန် အောက်ပါကာကွယ်နည်းလမ်းများကို ပြုလုပ်သင့်ပါသည်။

- (1) အင်တာနက်မှတစ်ဆင့် Bot ဝိုင်းရပ်စ်များ ကူးစက်ပျံ့ပွားနိုင်သဖြင့်မိမိ၏ Web ကိုမကူးစက်စေရန် ဂရုပြုပါ။
- (2) မိမိကွန်ပျူတာ၏ OS နှင့် Application များကိုအမြဲ Update ပြုလုပ်ပါ။
- (3) မသင်္ကာစရာတွေ့ရှိပါက ဝင်ရောက်ကြည့်ရှုနေသော Web ကိုပိတ်၍ လုပ်ဆောင်သင့်သော ကာကွယ်နည်းများကို ပြုလုပ်ပါ။

ကိုးကားချက်

အောက်ဖော်ပြပါဆိုင်များသို့ ဝင်ရောက်လေ့လာပါ။

♦ IT Security White Paper 2007—အဓိကအန္တရာယ် 10ချက်။(မမြင်နိုင်သော အန္တရာယ်များ)

http://www.ipa.go.jp/security/vuln/20070309_ISwhitepaper.html

♦ ကွန်ပျူတာလုံခြုံမှုစနစ် 2004ခုနှစ်၏ကာကွယ်ခြင်းနည်းလမ်းများ

http://www.ipa.go.jp/security/vuln/20050331_trend2004.html

♦ မလိုအပ်သောဆော့ဝဲလ်များပယ်ဖျက်ခြင်း Tool

<http://www.microsoft.com/japan/security/malwareremove/>

- ◆ Cyber Clean Center (CCC) Ministry of Internal Affairs and Communications နှင့် Ministry of Economy, Trade and Industry တို့၏ပူးပေါင်းဆောင်ရွက်မှု။

<https://www.ccc.go.jp/>

အွန်လိုင်း Scan (ပိုင်းရပ်စ် စစ်ဆေးခြင်း)

- ◆ Cyber Clean Center ၏ Bot ဖယ်ရှားခြင်းနည်းလမ်းများ

<https://www.ccc.go.jp/flow/>

- ◆ Symantec လုံခြုံမှုစနစ် စစ်ဆေးခြင်း

<http://security.symantec.com/sscv6/home.asp>

- ◆ Trendmicro အွန်လိုင်း Scan

<http://www.trendflexsecurity.jp/housecall/>

- ◆ McAfee အခမဲ့ Scan

<http://www.mcafee.com/japan/mcafee/home/freescan.asp>

ဝေါဟာရ ရှင်းလင်းချက်

(*1) Phishing

တရားဝင် ဘဏ္ဍာရေးအဖွဲ့အစည်းများ (ဘဏ်၊ Credit ကဒ် ကုမ္ပဏီစသည်) အနေဖြင့် အယောင်ဆောင် အီးမေးလ်များပေးပို့၍ ဝယ်ယူသူ၏ကိုယ်ပိုင်အချက်အလက်များ (အမည်၊ လိပ်စာ၊ ဘဏ်စာရင်းနံပါတ်၊ Credit ကဒ်နံပါတ်စသည်) ကိုခိုးယူလိမ့်လည်ခြင်းဖြစ်သည်။ Phishing သည် Fishing ဆိုသည့်စကားလုံးမှ ဆင်းသက်လာပြီး ရှုပ်ထွေးသောလိမ်လည်မှုဖြစ်သည်။

(*2) Spam mail

UBE (သို့) unsolicited bulk Email ဟုခေါ်သော သံသယဖြစ်ဖွယ် မေးလ်များသည် ဝါဒဖြန့်ခြင်း၊ အနှောက်အယှက် ပေးခြင်းစသည့် ရည်ရွယ်ချက် အမျိုးမျိုးဖြင့်ရောက်ရှိလာသော အီးမေးလ်များဖြစ်သည်။

(*3) DoS တိုက်ခိုက်မှု/DDoS တိုက်ခိုက်မှု

ဝန်ဆောင်မှုကိုနှောင့်ယှက်တိုက်ခိုက်ခြင်း (DoS တိုက်ခိုက်မှု) ဆိုသည်မှာ အင်တာနက် အချက်အလက်များကို ဖျက်စီးခြင်း၊ အင်တာနက်နှင့်ချိတ်ဆက်ထားသော ကွန်ပျူတာ၏စနစ်များကို လွန်ကဲစွာ တာဝန်ထမ်းဆောင်စေခြင်းများဖြင့် ဝင်ဆောင်မှုများကို ပျက် စီးစေရန် နှောင့်ယှက်တိုက်ခိုက်ခြင်းဖြစ်သည်။ ထိုကဲ့သို့သော DoS ပေါင်းများစွာမှ ကွန်ပျူတာတစ်လုံးကို ဝင်ရောက်တိုက်ခိုက်သောအခါ ကွန်ပျူတာ၏စနစ်များကို ပို၍လွန်ကဲစွာ တာဝန်ထမ်းဆောင်စေ ပါသည်။ ထိုကဲ့သို့တိုက်ခိုက်မှုများကို DDoS (Distributed Denial of Service: ဝန်ဆောင်မှုကို ပြန့်ကျဲစွာ နှောင့်ယှက်တိုက်ခိုက်ခြင်း) ဟုခေါ်ပါသည်။

DoS တိုက်ခိုက်မှုများ၏ မူရင်းသည် တိုက်ခိုက်သူအသုံးပြုသော Website ဖြစ်သည်။ တိုက်ခိုက်သူသည် တစ်ချို့သော Website များအတွင်း ခိုင်မြဲစွာနေရာယူထားပြီး အဝေးမှတစ်ဆင့် တိုက်ခိုက်မှုများကို ပြုလုပ်ထိန်းချုပ်နေခြင်းဖြစ်သည်။

(*4) စနစ်အားနည်းခြင်း

လုံခြုံမှုစနစ်အားနည်းခြင်းသည် အခြားစနစ်များ network များ၊ Application များ၊ protocols များ၏ လုံခြုံရေး စနစ်ကိုပါ အဆင့်နိမ့်ကျစေပါသည်။ ထိုမှတစ်ဆင့် မလိုလားအပ်သော အဖြစ်အပျက်များဖြစ်ပေါ်လာစေပြီး လုပ်ဆောင် ချက်များ၊ အမှားများကို ဖြစ်ပေါ်စေပါသည်။ Operating စနစ်အားနည်းခြင်း၊ Application စနစ်အားနည်းခြင်း စသည်ဖြစ်ရှိပါသည်။ ထို့ပြင် ဆော့ဝဲလ် အားနည်းခြင်း အပြင် လုံခြုံမှုစနစ် မလုံလောက်လျှင်လည်း စနစ် အားနည်းခြင်း ဖြစ်နိုင်ပါသည်။ ၎င်းကို အများ အားဖြင့် Security hole ဟုခေါ်ဆိုပါသည်။

(*5) Backdoor

ကွန်ပျူတာအတွင်းသို့ မမှန်မကန်နည်းဖြင့် ဝင်ရောက်နိုင်ရန် ရည်ရွယ်ထားသော ပရိုဂရမ် ဖြစ်သည်။ သတ်မှတ်ထားသော Port ကိုဖွင့်ပြီး ၎င်းကိုအသုံးပြု၍ပရိုဂရမ်ကို လုပ်ဆောင်သည်။ ထိုစနစ်ကြောင့် အပြင်အင်တာနက်မှတစ်ဆင့် ကွန်ပျူတာအတွင်းသို့ ဝင်ရောက်နိုင်ပါသည်။

(*6) IM (instant messenger)

အင်တာနက်နှင့်ဆက်သွယ်ထားသော ကွန်ပျူတာအချင်းချင်း Chat များနှင့် ဖိုင်များ အပြန်အလှန် ဖလှယ်နိုင်သော ဆော့ဝဲလ်ဖြစ်သည်။ ထိုဆော့ဝဲလ်ကိုအသုံးပြု၍ မိတ်ဆွေအချင်းချင်း အင်တာနက် မှတစ်ဆင့် အချိန်နှင့်တပြေးညီ သတင်းများပေးပို့နိုင်ပါသည်။ လူသုံးအများဆုံးမှာ AOL Instant Messaging နှင့် MSN Messenger တို့ဖြစ်သည်။

(*7) IRC (Internet Relay Chat)

စကားပြောစနစ်ဖြစ်သည်။ သတ်မှတ်ထားသော ဆော့ဝဲလ်ကိုအသုံးပြု၍ IRC Server မှတစ်ဆင့် အင်တာနက် အသုံးပြုသူများအချင်းချင်း သတင်းများပေးပို့ဖလှယ်နိုင်ပါသည်။

(*8) Network Scanning

Port Scan စနစ်ကိုအသုံးပြု၍ကွန်ပျူတာအတွင်းရှိ Port များ၏အခြေအနေကို စစ်ဆေးခြင်းဖြစ်သည်။ အခြားသော ဗိုင်းရပ်စ်များ ပါဝင်သည့် Backdoor စသည်တို့ ဝင်ရောက်နေခြင်းရှိမရှိကိုလည်း စစ်ဆေးပေးနိုင်ပါသည်။

ဤအစီအမံစာအုပ်ကို အောက်ပါအဖွဲ့အစည်းများ၏ ပူးပေါင်းဆောင်ရွက်မှုဖြင့် ထုတ်ဝေပါသည်။

♦ Ahnlabo ကုမ္ပဏီ

<http://www.ahnlab.co.jp/>

♦ Kaspersky Labs Japan ကုမ္ပဏီ

<http://www.kaspersky.co.jp/>

♦ Symantec ကုမ္ပဏီ

<http://www.symantec.com/ja/jp/>

♦ Sourcenext ကုမ္ပဏီ

<http://www.sourcenext.com/>

♦ Trendmicro ကုမ္ပဏီ

<http://jp.trendmicro.com/>

♦ Microsoft ကုမ္ပဏီ

<http://www.microsoft.com/ja/jp/>

♦ McAfee ကုမ္ပဏီ

<http://www.mcafee.com/japan/>



※ဤစာအုပ်သည် ကွန်ပျူတာသတင်းအချက်အလက်များ ကာကွယ်ဆောင်ရွက်မှုအဖွဲ့အစည်း (IPA) ၏ ကွန်ပျူတာကွန်ရက် လုံခြုံရေးစင်တာမှ ပြဌာန်း ထုတ်ဝေပါသည်။ ဂျပန်အစိုးရ၏ဘာသာပြန်မှုဖြင့် အရှေ့တောင်အာရှနိုင်ငံများသို့ အခမဲ့ဖြန့်ဝေပေးမည်ဖြစ်ပါသည်။ ထို့ပြင် ဤစာအုပ်သည် ဂျပန်အစိုးရ၏ ခွင့်ပြုချက်မရဘဲ စီးပွားဖြစ်ကူးယူအသုံးပြုခြင်း၊ လွှဲပြောင်းပေးခြင်း၊ ထုတ်လွှင့်ပြသခြင်းများ မပြုလုပ်ရ။ (ဆက်သွယ်ရန်: အစိုးရ၏ ကွန်ပျူတာသတင်းအချက်အလက်များ၏ကွန်ရက်လုံခြုံရေးစင်တာ (NISC) 〒100-0014 တိုကျိုမြို့ချိုရောအရပ်ကွက် နဂတမြို့နယ်2-4-12 poc@nisc.go.jp)