# Two Factor Authentication ကိုအသုံးပြုသူများ သတိပြုရမည့် New Spear Phishing Attack အကြောင်း

အဆိုပါ တိုက်ခိုက်မှုသည် နဂိုတိုက်ခိုက်လေ့ရှိသော Spear Phishing တိုက်ခိုက်မှုထက်ပိုမို လွယ်ကူရိုးရှင်းသော်လည်း ထိခိုက်မှုအန္တရာယ်မှာ ပိုမိုများပြားစေနိုင်ပါသည်။

Mobile အသုံးပြုသူများကို ရည်ရွယ်၍ ပစ်မှတ်ထားသော Two Factor Authentication ကိုကျော်လွှားသွားနိုင်ပြီး Victims ၏ e-mail accounts ကိုပါယူဆောင်သွားနိုင်သည့် Spear Phishing တိုက်ခိုက်မှု အသစ်အကြောင်းကို Symantec မှ Reseracher များမှ သတိပေးချက်များ ထုတ်ပြန်ခဲ့ပါသည်။

တိုက်ခိုက်မှုကို စတင်ရန်အတွက် ပစ်မှတ်၏ အီးမေးလ် လိပ်စာနှင့် ဖုန်းနံပါတ် ကို သိရှိရန်တော့ လိုအပ်ပါသည်။

Attacker က User များအသုံးပြုလေ့ရှိသော password မေ့သွားလျှင် ၎င်း၏ Mobile ဖုန်းသို့ Verification code ပြန်လည်ပေးပို့ပေးသည့် e-mail password recovery feature ကိုအသုံးပြုပြီး ရိုးရှင်းစွာဖြင့် တိုက်ခိုက်ခြင်း ဖြစ်ပါသည်။

E-mail ပိုင်ရှင်မှ "forgot password" နှင့် "verification code" တောင်းခံသည့် link ကို နှိပ်မိခြင်းဖြင့် Attacker မှ victim ၏ mobile phone သို့ code ကို SMS message ပေးပို့မည် ဖြစ်ပါသည်။

Attacker မှ victim ဆီသို့ "Google has detected unusual activity on your account. Please respond with the code sent to your mobile device to stop unauthorized activity." ကဲ့သို့သော SMS Message ထပ်မံပေးပို့ခြင်းဖြင့် code ကိုပြန်လည် ရရှိစေရန် လုပ်ဆောင်မည် ဖြစ်ပါသည်။

ထိုအခါတွင် Victim မှ code ကို ပြန်လည်ပေးပို့လိုက်သောအခါတွင် attacker မှ victim ၏ email account ကို access လုပ်ခွင့်ရရှိသွားမည် ဖြစ်ပါသည်။

Symantec မှ Principal Research Engineer တစ်ဦးဖြစ်သော Grzonkowski ၏မှတ်စုအရဆိုလျှင် အကောင့်၏ password ကို restart ချပြီးသည့်နောက်တွင်လည်း Attacker မှ "Thank you for verifying your Google account. Your temporary password is [TEMPORARY PASSWORD." ကဲ့သို့သော SMS မျိုးကို victim သို့ ထပ်မံပေးပို့နိုင်ပါသည်။

Victim မှ ၄င်း၏ အကောင့်သည် တိုက်ခိုက်ခံနေရပြီဟု မသိရှိပဲ ယခုအချိန်တွင် တရားဝင်နှင့် ပိုမိုလုံခြုံစိတ်ချပြီဟု တွေးထင် နေမည် ဖြစ်ပါသည်။ ထိုကဲ့သို့ တိုက်ခိုက်ခြင်းဖြင့် phishing attack ဖြစ်နေသည်ကို victim မှမသိပဲ ယုံကြည်နေမည် ဖြစ်ပါသည်ဟု Symantec မှ Principal Research Engineer တစ်ဦးဖြစ်သော Grzonkowski မှရေးသားထားခဲ့ပါသည်။

Symantec မှလေ့လာချက်များအရ အများအားဖြင့် Gmail, Hotmail နှင့် Yahoo Mail အသုံးပြုသူများ တွင် ၄င်း တိုက်ခိုက်မှုအဖြစ်များကြောင်း တွေ့ရှိရပါသည်။

တိုက်ခိုက်မှု၏ အဓိကရည်ရွယ်ချက်မှာ ငွေရေးကြေးရေးထိခိုက်မှုမျိုး ကို ရည်ရွယ်၍ တိုက်ခိုက်ခြင်းခြင်းမျိုး မဟုတ်ပဲ သတင်းအချက်အလက်များ ရရှိစေရန်ကိုသာ ဦးတည်၍ တိုက်ခိုက်ခြင်းမျိုး ဖြစ်ကြောင်း Symantec မှ Principal Research Engineer တစ်ဦးဖြစ်သော Grzonkowski မှပြောကြားခဲ့ပါသည်။

ယခုကဲ့သို့ ရိုးရှင်းထိရောက်သော တိုက်ခိုက်မှုနည်းလမ်းအသစ်သည် နဂိုပြုလုပ်လေ့ရှိသော Spear Phishing တိုက်ခိုက်မှုဖြစ်သော Attacker အနေဖြင့် Domain တစ်ခုကို register ပြုလုပ်ခြင်းနှင့် Phishing site တခုကိုပြုလုပ်ရန် လိုအပ်သည် ထက်ပို၍ ကုန်ကျစရိတ် သက်သာစေပါသည်။ ယခုကဲ့သို့ အခြေအနေတွင် SMS message ပို့သည့် ကုန်ကျစရိတ်သာ ရှိပြီး user's mobile software (သို့) by the mobile carrier တို့ဖြင့်ပြုလုပ်ခြင်း ဖြစ်သောကြောင့်လည်း detect လုပ်ရန်မှာ ခက်ခဲမည် ဖြစ်ပါသည်။

Victim ဖြစ်ခြင်းမှ ကာကွယ်ရှောင်ရှားရန်အတွက် verification codes ကိုမေးမြန်းသော SMS message မျိုးသည် သံသယဖြစ်ဖွယ် ကောင်းသည့်အတွက် သတိပြုသင့်သည်ဟု အကြံပြုထားပါသည်။ Password recovery services မှ တရားဝင် message ဆိုလျှင် verification codes ကို ရိုးရှင်းစွာဖြင့် ပြောကြားမည် ဖြစ်ပြီး မည်သည့်တုံ့ပြန်မှုများမှ ပြန်လည်မေးမြန်းလိမ့်မည် မဟုတ်ဟု Grzonkowski မှရေးသားထားခဲ့ပါသည်။

အထက်တွင် ဖော်ပြထားခဲ့သော အကြောင်းအရာများသည် မိမိ၏ အကောင့်ကို လုံခြုံမှုရှိစေရန် အတွက် Two Factor Authentication ကိုအသုံးပြုထားသော်လည်း ယခုကဲ့သို့ New Spear Phishing တိုက်ခိုက်မှုများ ရှိနေသည်ကို သိရှိစေရန် ရည်ရွယ်၍ ဒီဆောင်းပါးလေးကို ရေးသားရခြင်းဖြစ်ပါသည်။

http://www.esecurityplanet.com/network-security/new-spear-phishing-attack-bypasses-two-factor-authentication.html