APT40 အကြံပြုချက်

PRC MSS လက်ရှိ ထောက်လှမ်းမှု နည်းလမ်း

Australian Government

Australian Signals Directorate

National Cyber
Security Centre
a part of GCHQ

Communications
Security Establishment

**Canadian Centre
for Cyber Security**

Centre de la sécurité
des télécommunications

**Centre canadien
pour la cybersécurité**

မာတိကာ

အကျဉ်းချုံး

နောက်ခံအကြောင်းအရာ

ဤ အကြံပြုစာစောင်အား ဩစတြေးလျနိုင်ငံ ဆက်သွယ်ညှိနှိုင်းရေး ဌာန၏ ဩစတြေးလျနိုင်ငံ ဆိုင်ဘာလုံခြုံရေးစင်တာ (ASD's ACSC)၊ အမေရိကန်နိုင်ငံ ဆိုင်ဘာလုံခြုံရေးနှင့် အခြေခံအဆောက်အအုံ လုံခြုံရေးအေဂျင်စီ (CISA)၊ အမေရိကန်နိုင်ငံ အမျိုးသား လုံခြုံရေးအေဂျင်စီ (NSA)၊ အမေရိကန်နိုင်ငံ ဗဟိုထောက်လှမ်းဌာန (FBI)၊ ယူကေနိုင်ငံ အမျိုးသားဆိုင်ဘာ လုံခြုံရေးစင်တာ (NCSC-UK)၊ ကနေဒါနိုင်ငံ ဆိုင်ဘာလုံခြုံရေးစင်တာ (CCCS)၊ နယူးဇီလန်နိုင်ငံ အမျိုးသား ဆိုင်ဘာလုံခြုံရေးစင်တာ (NCSC-NZ)၊ ဂျာမနီနိုင်ငံ ဗဟိုထောက်လှမ်းရေးဝန်ဆောင်မှုရုံး (BND) နှင့် ဖွဲ့စည်းအုပ်ချုပ်ပုံ အခြေခံဥပဒေကို ကာကွယ်ရေး ဗဟိုရုံး (BfV)၊ တောင်ကိုရီးယားနိုင်ငံ ထောက်လှမ်းရေးဝန်ဆောင်မှုဌာန (NIS) နှင့် NIS ၏ အမျိုးသား ဆိုင်ဘာလုံခြုံရေး စင်တာ၊ ဂျပန်နိုင်ငံ အခင်းဖြစ်ပွားမှုအတွက် အသင့်ဖြစ်ခြင်းနှင့် ဆိုင်ဘာလုံခြုံရေး ဆိုင်ရာ နည်းဗျူဟာ စင်တာ (NISC) နှင့် အမျိုးသား ရဲအေဂျင်စီ (NPA) တို့မှ ပူးပေါင်း ထုတ်ဝေထားခြင်းဖြစ်ကာ - ဤနောက်ပိုင်းတွင် ၎င်းအဖွဲ့အစည်းများကို "အာဏာပိုင် အေဂျင်စီများ" ဟု သုံးနှုန်းသွားမည် - တရုတ်ပြည်သူ့ သမ္မတနိုင်ငံ (PRC) မှ ကျောထောက်နောက်ခံ ပြုထားသည့် ဆိုင်ဘာအဖွဲ့အစည်းများမှ လက်ရှိ ဩစတြေးလျ၏ ကွန်ရက်များအပေါ် ခြိမ်းခြောက်မှုများ လုပ်ဆောင်နေသည့် အကြောင်းကို ဖော်ပြထားပါသည်။ ဤ အကြံပြုချက်သည် အာဏာပိုင် အေဂျင်စီများ၏ ခြိမ်းခြောက်မှုအပေါ် ဘုံနားလည်မှုအပြင် ASD ၏ ACSC ၏ အခင်းဖြစ်ပွားမှုနှင့် ပတ်သက်ပြီး တုံ့ပြန်သည့် စုံစမ်းစစ်ဆေးမှုများအကြောင်း နားလည်ကြရန်အတွက် ရည်ရွယ်လုပ်ဆောင်ထားပါသည်။

တရုတ်ပြည်သူ့ သမ္မတနိုင်ငံ PRC မှ ကျောထောက်နောက်ခံပြုထားသည့် ဆိုင်ဘာအဖွဲ့များသည် ဩစတြေးလျ၊ အမေရိကန်အပါအဝင် နိုင်ငံအချို့မှ အဖွဲ့အစည်းများကို ပစ်မှတ်ထား တိုက်ခိုက်မှုများရှိခဲ့ပြီး အောက်တွင် ဖော်ပြထားသည့် နည်းလမ်းများမှာ PRC မှ နိုင်ငံတော် -စပွန်ဆာ ပေးထားသည့် ဆိုင်ဘာသမားများ ကမ္ဘာတလွှားတွင် တိုက်ခိုက်မှု လုပ်သည့်အခါ ပုံမှန် အသုံးပြုသည့် နည်းလမ်းအချို့ ဖြစ်ပါသည်။ ထိုကြောင့် အာဏာပိုင် အေဂျင်စီများအနေဖြင့် ထိုဆိုင်ဘာအဖွဲ့နှင့် ၎င်းတို့ အသုံးပြုသည့် နည်းလမ်းများနှင့် ဆင်တူသော တိုက်ခိုက်ရေး နည်းလမ်းများသည် အာဏာပိုင် အေဂျင်စီ နိုင်ငံများ၏ ကွန်ရက်အတွက် ခြိမ်းခြောက်မှု ရှိနေဆဲ ဖြစ်သည်ဟု ယုံကြည်ကြပါသည်။

ဤအဖွဲ့သည် တရုတ်ပြည်သူ့ သမ္မတနိုင်ငံ၏ နိုင်ငံတော် လုံခြုံရေး ဝန်ကြီးဌာန (MSS) အတွက် မသမာသည့် ဆိုင်ဘာတိုက်ခိုက်ရေးများ လုပ်နေသည်ဟု အာဏာပိုင် အေဂျင်စီများ အနေဖြင့် သုံးသပ်ထားပါသည်။ ၎င်းတို့၏ လှုပ်ရှားမှုနှင့် အသုံးပြုသည့် နည်းလမ်းများသည် Advanced Persistent Treat (APT) 40 အဖွဲ့များ (တနည်းအားဖြင့် ၎င်းတို့ကို Kryptonite Panda, GINGHAM TYPHOON၊ Leviathan and Bronze Mohawk ဟုလည်း လုပ်ငန်းဆိုင်ရာ အစီရင်ခံစာတွင် ဖော်ပြထားပါသည်) အသုံးပြုသည့် နည်းလမ်းများနှင့် ဆင်တူနေကြောင်း တွေ့ရှိရပါသည်။ ထိုအဖွဲ့သည် ဟိုင်နန်ပြည်နယ် ဟိုင်ကိုးမြို့တွင် အခြေချကာ တရုတ်ပြည်သူ့ သမ္မတနိုင်ငံနှင့် နိုင်ငံတော် လုံခြုံရေးဝန်ကြီးဌာနနှင့် ဟိုင်နန်ပြည်နယ် လုံခြုံရေးဌာန၏ ညွှန်ကြားချက်များအတိုင်း လုပ်ဆောင်ကြောင်း ယခင် ဖော်ပြချက်များအရ သိရပါသည်။[2] ဤအကြံပြုချက်သည် ၎င်းတို့ ပစ်မှတ်ထားသည့် ကွန်ရက် နှစ်ခုအား တိုက်ခိုက်ရာတွင် အသုံးပြုသည့် တိုက်ခိုက်ရေး နည်းလမ်းများကို ဖြစ်ရပ်မှန် နမူနာများဖြင့် ဖော်ပြထားပါသည်။ ဖြစ်ရပ်မှန် နမူနာများသည် ဆိုင်ဘာလုံခြုံရေး လုပ်ငန်း လုပ်ကိုင်သူများအတွက် ၎င်းတို့၏ ကွန်ရက်အား APT40 ၏ ရန်မှ ကာကွယ်ခြင်း နှင့် တိုက်ခိုက်ခံရမှုမှ ပြန်လည်ထူပြုပြင်ခြင်း ဆိုင်ရာ လုပ်ငန်းများ လုပ်ကိုင်သည့်အခါတွင် လက်ငင်း အကျိုးဖြစ်စေနိုင်သည့် နမူနာများ ဖြစ်ပါသည်။ ရွေးထုတ်ဖော်ပြထားသည် ဖြစ်ရပ်မှန် နမူနာများသည် တိုက်ခိုက်ခံရပြီးနောက် ပြန်လည်ထူထောင်ပြုပြင်ခြင်းများ ပြုလုပ်ကာ ဤ မသမာသူများ သို့မဟုတ် အခြားသော မသမာသူများမှ ထပ်မံ တိုက်ခိုက်မှု မလုပ်နိုင်ရန်အတွက် အန္တရာယ်ကို လျော့ကျစေသည့် ကာကွယ်ရေး နည်းလမ်းများကို အသုံးပြုထားသည့် ဖြစ်ရပ်မှန် နမူနာများကို အခြေခံထားပါသည်။ ထိုအတွက်ကြောင့် ဤဖြစ်ရပ်မှန် နမူနာများသည် ဖြစ်ပေါ်ပြီးသား အချိန်ကာလမှ အကြောင်းအရာဟောင်းများဖြစ်ပြီး ၎င်းတို့အနေဖြင့် တိုက်ခိုက်ခံရမှုမှ ပြန်လည်ထူထောင်ပြုပြင်မှု လုပ်ရန်အတွက် လိုအပ်သည့် အချိန်ကို ရရှိစေရန်အတွက် ဖြစ်ပါသည်။

လှုပ်ရှားမှု အကျဉ်းချုပ်

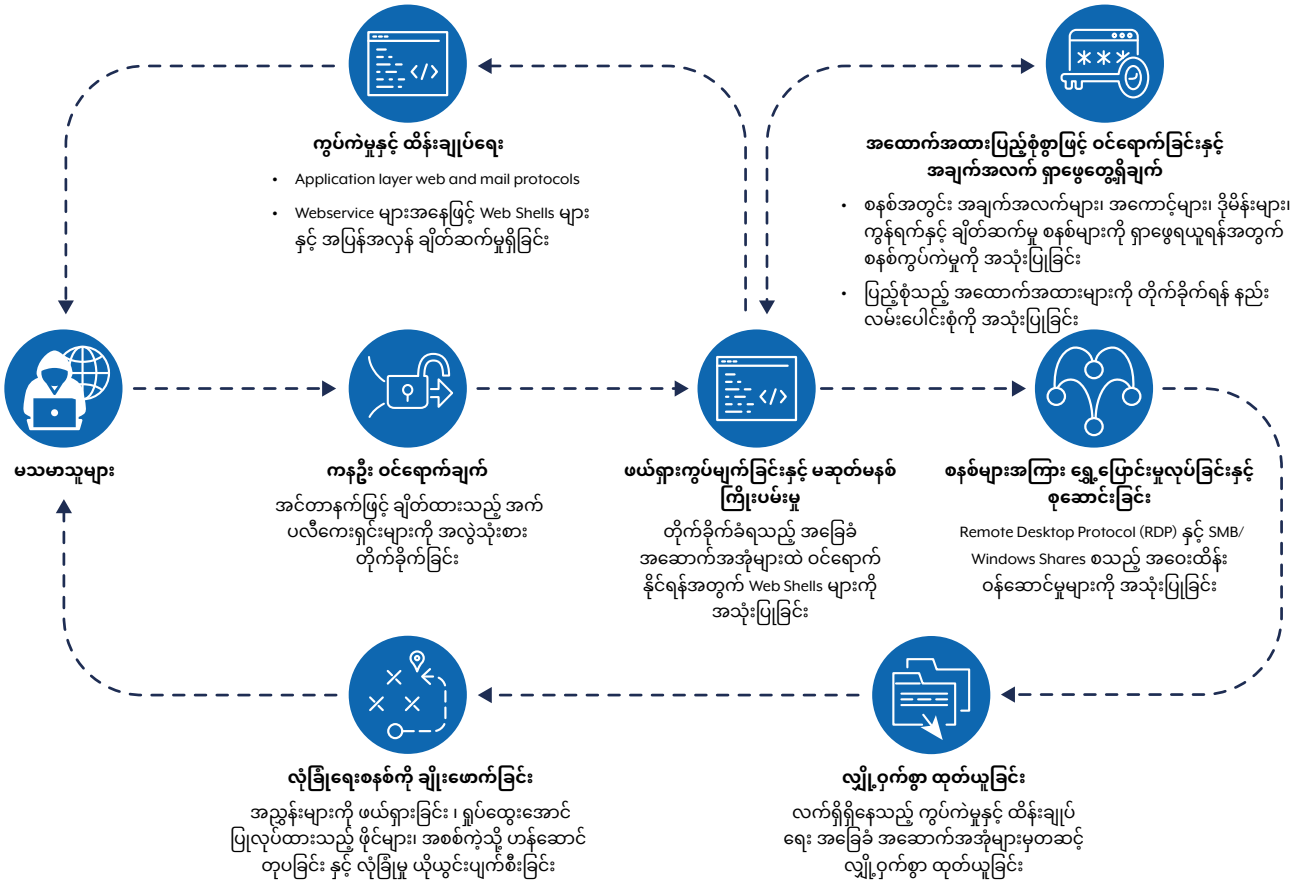
APT40 သည် ဩစတြေးလျ၏ ကွန်ရက်များကို အကြိမ်ကြိမ် တိုက်ခိုက်မှု လုပ်သက္ခဲသို့ ဒေသအတွင်းမှ အစိုးရနှင့် ပုဂ္ဂလိကပိုင် ကွန်ရက်များအား တိုက်ခိုက်မှုလုပ်ခဲ့သည့်အပြင် ကျွန်ုပ်တို့၏ ကွန်ရက်များအတွက် ခြိမ်းခြောက်မှု အန္တရာယ် ရှိနေဆဲ ဖြစ်ပါသည်။ ဤအကြံပြုချက် စာစောင်တွင် ဖော်ပြထားသည့် ထောက်လှမ်းမှု နည်းဗျူဟာများသည် ဩစတြေးလျ၏ ကွန်ရက်များကို တိုက်ခိုက်သည့်အခါတွင် အသုံးပြုလေ့ရှိသည့် နည်းဗျူဟာများ ဖြစ်ပါသည်။

သတိပြုမိသည်မှာ APT40 သည် ၎င်းတို့ ပစ်မှတ်ထားသည့် ကွန်ရက်များ၏ ပျော့ကွက်ဟာကွက်အားနည်းချက် အသစ်များကို တွေ့ရှိသည်နှင့် တပြိုင်နက် လျင်မြန်စွာ ပြောင်းလဲနိုင်စွမ်းနှင့် proof-of-concept(s) (POCs) ကို ကောင်းမွန်စွာ အလွဲသုံးစားလုပ်ကိုင်နိုင်စွမ်းကို အသုံးပြုကာ ၎င်းတို့ ပစ်မှတ်ထားသည့် ကွန်ရက်၏ အခြေခံအဆောက်အအုံကို ရယူလိုက်ခြင်းများ လုပ်သည်ကို တွေ့ရှိရပါသည်။ APT40 သည် အာဏာပိုင်အေဂျင်စီနိုင်ငံများ၏ ကွန်ရက်များအပါအဝင် ၎င်းတို့ ပစ်မှတ်ထားလိုသည့် ကွန်ရက်များအား ပုံမှန် စူးစမ်းထောက်လှမ်းမှုများပြုလုပ်ကာ ပျော့ကွက်ဟာကွက်အားနည်းချက်များကို စောင့်ကြည့်ပြီး တိုက်ခိုက်မှုလုပ်နိုင်ရန် အခွင့်ကောင်းများကို ပုံမှန် ရှာဖွေလျက် ရှိပါသည်။ ထိုကဲ့သို့ ပုံမှန်စူးစမ်းထောက်လှမ်းမှုများထဲတွင် ၎င်းတို့ ပစ်မှတ်ထားသည့် ကွန်ရက်များနှင့် ဆက်စပ်နေသော အသုံးမပြုတော့သည့်စက်ပစ္စည်း သို့မဟုတ် ပြုပြင်မွမ်းမံထိန်းသိမ်းခြင်း မရှိတော့သည့် စက်ပစ္စည်းများကိုပါ ရှာဖွေစုံစမ်းကာ မသမာမှုများ လျင်မြန်စွာ လုပ်ခွင့်ရရှိရန်အတွက် လုပ်ဆောင်လျက် ရှိပါသည်။ APT40 သည် ၂၀၁၇ ခုနှစ်မှ စတင်ကာ ၎င်းတို့ ပစ်မှတ်ထားသည့် အဖွဲ့များ၏ ပျော့ကွက်ဟာကွက် အားနည်းချက်များအပေါ် တိုက်ခိုက်မှုများ လုပ်ခဲ့ပါသည်။

APT40 သည် Log4J (CVE 2021 44228), Atlassian Confluence (CVE-2021-31207, CVE-2021-26084) နှင့် Microsoft Exchange (CVE-2021-31207; CVE-2021-34523; CVE-2021-34473) စသည့် လူအများသုံး ဆော့ဖ်ဝဲများ၏ အားနည်းချက်များကို အလွဲသုံးစားပြုကာ တိုက်ခိုက်မှုများ အလျင်အမြန် လုပ်ဆောင်လျက် ရှိပါသည်။ ASD ၏ ACSC နှင့် အာဏာပိုင် အေဂျင်စီများ အနေဖြင့် ၎င်းအုပ်စုသည် နာမည်ကြီး အားနည်းချက်များဖြစ်ပေါ်သည့် အကြောင်းကို ဖော်ပြသည့် နာရီပိုင်း သို့မဟုတ် ရက်ပိုင်းအတွင်း POCs နည်းလမ်းများကို ဆက်လက်အသုံးပြုကာ တိုက်ခိုက်မှုများ ဆက်လက်လုပ်ကိုင်မည်ဟု သုံးသပ်ထားပါသည်။

2 အမေရိကန်နိုင်ငံတရားရေးဌာန ၂၀၂၁။ တရုတ်နိုင်ငံ လုံခြုံရေးဌာနနှင့် အလုပ်လုပ်ကိုင်သည့် တရုတ်နိုင်ငံသား လေးဦးသည် ကမ္ဘာလုံးဆိုင်ရာ ကွန်ပြူတာ တိုက်ခိုက်ရေး ကမ်ပိန်းများ ပြုလုပ်ကာ ၎င်းတို့သည် ကွန်ပြူတာများထဲသို့ တရားမဝင် ဝင်ရောက်ကာ Infections Disease Research ကူးစက်ရောဂါဆိုင်ရာ သုတသန အပါအဝင် ၎င်းတို့ တိုက်ခိုက်သည့် အဖွဲ့များ၏ မူပိုင်များနှင့် လုပ်ငန်းဆိုင်ရာ အချက်အလက်များအား ခိုးယူသည့် အမှုဖြင့် တရားစွဲခံခဲ့ရပါသည်။

ပုံ ၁- APT40 လှုပ်ရှားမှုအတွက် TTP လုပ်ငန်းစဉ်အဆင့်ဆင့်ပြကားချပ်



ဤအုပ်စုသည် အစစ်အမှန်ကဲ့သို့ ဟန်ဆောင်ကာ တိုက်ခိုက်မှုလုပ်သည့် phishing ကမ်ပိန်းများကဲ့သို့သော အသုံးပြုသူများ၏ တုန့်ပြန်မှုကို ရယူသည့် နည်းလမ်းများထက် အားနည်းချက်ရှိသည့် စက်ပစ္စည်းများနှင့် အများနှင့် သက်ဆိုင်သည့် အခြေခံ အဆောက်အအုံများကို တိုက်ခိုက်မှုများ လုပ်ရန် ပို၍ အားသန်ကြောင်း တွေ့ရှိရပြီး ယုံကြည်ရသည့် အထောက်အထား များနှင့် ဝင်ရောက်ကာ နောက်နောင်တွင် တိုက်ခိုက်မှုများ လုပ်နိုင်မည့် နည်း လမ်းများကို ဦးစားပေးကြောင်း တွေ့ရပါသည်။ APT40 သည် မဆုတ်မနစ်သည့်နည်းဖြင့် တိုက်ခိုက်ရန်အတွက် web shells (T1505.003) ကို ပုံမှန်အသုံးပြုပြီး အထူးသဖြင့် အစောပိုင်း ကျူးကျော်ဝင်ရောက်သည့် ကာလတွင် ထိုနည်းလမ်းကို အသုံးပြုလေ့ရှိပါသည်။ သာမာန်အားဖြင့် ကနဦးဝင်ရောက်မှု ရရှိသည့်အခါ APT40 သည် တိုက်ခိုက်ခံရသူ၏ ဘေး ပတ်ဝန်းကျင်ထဲ ဆက်လက် ဝင်ရောက်နိုင်ရန်အတွက် မဆုတ်မနစ်သည့်နည်း ဖြင့် တိုက်ခိုက်မှုကို အခြေချနိုင်ရန် လုပ်ဆောင်ပါသည်။ သို့သော် ကနဦး ဝင်ရောက်သည့် ကာလကတည်းက ထိုမဆုတ်မနစ်သည့်နည်းဖြင့် တိုက်ခိုက် ကျူးကျော်သည့် ကာလအတွင်း လေ့လာပြီးသားဖြစ်သည့်အတွက် မည်သည့်တိုက်ခိုက်မှုဖြစ်စေ သို့မဟုတ် မည်ကဲ့သို့ တုန့်ပြန်မှု လုပ်သည်ဖြစ်စေ ၎င်းက လေ့လာပြီးသား ဖြစ်နိုင်ပါသည်။

ထူးခြားသည့် ထောက်လှမ်းမှုနည်းလမ်း

APT40 သည် ယခင်က သြစတြေးလျ၏ ဝဘ်ဆိုက်များကို ကွပ်ကဲမှုနှင့် ထိန်းချုပ်ရေး (C2) hosts ကို တိုက်ခိုက်သော်လည်း ယခုတွင် ၎င်းတို့၏ တိုက်ခိုက်မှုကို တဆင့်တိုးကာ (T1594) နည်းလမ်းဖြင့် တိုက်ခိုက်ပါသည်။

APT40 သည် တိုက်ခိုက်ခံရသည့် အသေးစားရုံး/ အိမ်၏ ရုံးမှ (SOHO) ပစ္စည်း များ အပါအဝင် ကမ္ဘာတွင် ခေတ်စားသည့် တိုက်ခိုက်ခံရသည့် စက်ပစ္စည်းများ ကို အသုံးပြုခြင်း နည်းလမ်းကို အခြေခံအဆောက်အအုံဆိုင်ရာ လုပ်ငန်းများနှင့် နောက်ဆုံးလမ်းကြောင်းအား ပြောင်းလဲပေးသည့် (T1584.008) လုပ်ငန်းများ သြစတြေးလျနိုင်ငံတွင် လုပ်ကိုင်နိုင်ရန်အတွက် အသုံးပြုပါသည်။ ဤကဲ့သို့ လုပ်ဆောင်ချက်က အာဏာပိုင်အေဂျင်စီများအား ၎င်းတို့ကို သရုပ်ဖော်ရာနှင့် ၎င်းတို့၏ လှုပ်ရှားမှုများကို ခြေရာခံနိုင်မှုတို့ ဖြစ်စေပါသည်။

အသေးစားရုံး/ အိမ်၏ ရုံးမှ (SOHO) စက်ပစ္စည်း အများအပြားသည် သက်တမ်းကုန်ဆုံးခြင်း သို့မဟုတ် ပြုပြင်မွမ်းမံခြင်းမရှိသည့် စက်ပစ္စည်း များဖြစ်သည့်အတွက် N-day တိုက်ခိုက်မှုလုပ်ရန်အတွက် ပစ်မှတ်ထားခံ ရသည့် အရာများ ဖြစ်စေပါသည်။ တိုက်ခိုက်ခံရပြီဆိုသည်နှင့် (SOHO) စက်ပစ္စည်းသည် အခြားသော ယုံကြည်ရသည့် အရာများကဲ့သို့ အရောတဝင် ပြုနိုင်အောင် အစပျိုးပေးသကဲ့သို့ ဖြစ်စေပြီး ထိုမှတစ်ဆင့် ကွန်ရက်ကို ကာ ကွယ်ပေးသည့် (T1001.003) အတွက် စိန်ခေါ်မှုများ ဖြစ်စေနိုင်ပါသည်။

ထိုနည်းလမ်းများကို အခြားသော တရုတ်ပြည်သူ့ သမ္မတနိုင်ငံမှ ကျောထောက်နောက်ခံပြုထားသည့် အုပ်စုများလည်း ကမ္ဘာတလွှားတွင် အသုံးပြုသည်ကို တွေ့ရှိရပြီး အာဏာပိုင် အေဂျင်စီများအနေဖြင့် ဤလုပ်ရပ် များကို ဘုံခြိမ်းခြောက်မှုအဖြစ် မှတ်ယူပါသည်။ အချက်အလက်ပိုများအား [တရုတ်ပြည်သူ့ သမ္မတ နိုင်ငံမှ ကျောထောက်နောက်ခံပြုထားသည့် ဆိုင်ဘာ တိုက်ခိုက်ရေး သမားများအနေဖြင့် Network Providers နှင့် စက်ပစ္စည်းများ တိုက်ခိုက်ခြင်း](#) နှင့် [တရုတ်ပြည်သူ့ သမ္မတ နိုင်ငံမှ ကျောထောက်နောက်ခံ ပြုထားသည့် ဆိုင်ဘာတိုက်ခိုက်ရေး သမားများအနေဖြင့် အမေရိကန်၏ အရေးကြီးသော အခြေခံအဆောက်အအုံတစ်ခုအား တိုက်ခိုက်ပြီး မဆုတ်မနစ်သော နည်းလမ်းဖြင့် ဝင်ရောက်ရန် ပြုလုပ်ခြင်း](#) အကြောင်းအား ပူးတွဲအကြံပြုချက်တွင် လေ့လာနိုင်ပါသည်။

APT40 သည် ၎င်းတို့၏ တိုက်ခိုက်မှုအတွင်း တခါတရံ ဝယ်ယူထားသည့် သို့မဟုတ် ငှားရမ်းထားသည့် အခြေခံ အဆောက်အအုံကို အသုံးပြုကာ victim-facing C2 နည်းဖြင့် တိုက်ခိုက်မှု လုပ်သော်လည်း ထိုထောက်လှမ်းမှု နည်းလမ်းအား အသုံးပြုမှု လျော့ကျလာသည်ကို တွေ့ရပါသည်။

လုံခြုံမှုရှိအောင် ကာကွယ်လုပ်ဆောင်ခြင်း

ASD ၏ ACSC အနေဖြင့် စုံစမ်းစစ်ဆေးမှုမှ တွေ့ရှိရသည့် မသမာသည့် ဖိုင်များကို အောက်ပါအတိုင်း မျှဝေဖော်ပြထားပါသည်။ ဤဖိုင်များအား VirusTotal တွင် တင်ထားပြီး ကွန်ရက်အား ကာကွယ်မှု ကျယ်ပြန့်စွာ လုပ်ကိုင်ရန်နှင့် ဆိုင်ဘာလုံခြုံရေး ကွန်မြူနီတီအနေဖြင့် ထိုခြိမ်းခြောက်မှုများကို ပိုမို နားလည်ပြီး ကာကွယ်မှု လုပ်နိုင်ရန်အတွက် ရည်ရွယ်ပါသည်။

ဖြစ်ရပ်မှန် နမူနာများ

ASD ၏ ACSC အနေဖြင့် အမည်မဖော်ထားသည့် စုံစမ်းစစ်ဆေးရေး အစီရင်ခံစာ နှစ်ခုကိုလည်း မျှဝေထားပြီး ထိုမသမာသူများသည် ၎င်းတို့၏ ပစ္စည်းများနှင့် စုံစမ်းထောက်လှမ်းမှု နည်းလမ်းများကို မည်ကဲ့သို့ လုပ်ဆောင်သနည်းဆိုသည်ကို လူအများသိရန် ရည်ရွယ်ထားပါသည်။

MD5	ဖိုင်နာမည်	အချက်အလက်ပိုများ
26a5a7e71a601be991073c78d513dee3	horizon.jsp	1 kB | Java Source
87c88f06a7464db2534bc78ec2b915de	Index_jsp$ProxyEndpoint$Attach.class	597 B | Java Bytecode
6a9bc68c9bc5cefaf1880ae6ffb1d0ca	Index_jsp.class	5 kB | Java Bytecode
64454645a9a21510226ab29e01e76d39	Index_jsp.java	5 kB | Java Source
e2175f91ce3da2e8d46b0639e941e13f	Index_jsp$ProxyEndpoint.class	4 kB | Java Bytecode
9f89f069466b8b5c9bf25c9374a4daf8	Index_jsp$ProxyEndpoint$1.class	3 kB | Java Bytecode
187d6f2ed2c80f805461d9119a5878ac	Index_jsp$ProxyEndpoint$2.class	1 kB | Java Bytecode
ed7178cec90ed21644e669378b3a97ec	Nova_jsp.class	7 kB | Java Bytecode
5bf7560d0a638e34035f85cd3788e258	Nova_jsp$TomcatListenerMemShellFromThread.class	8 kB | Java Bytecode
e02be0dc614523ddd7a28c9e9d500cff	Nova_jsp.java	15 kB | Java Source

ဖြစ်ရပ်မှန် နမူနာ 1

ဤအစီရင်ခံစာကို ကျယ်ပြန့်စွာ ဖြန့်ဝေရန်အတွက် ရည်ရွယ်သဖြင့် နာမည်ရင်းများကို ထိန်ချန်ထားပါသည်။ သည်နောက်ပိုင်းတွင် တိုက်ခိုက်ခံရသည့် အဖွဲ့အစည်းကို 'ထိုအဖွဲ့အစည်း' ဟု သုံးနှုန်းသွားမည် ဖြစ်သည်။ တိုက်ခိုက်ခံရသူ မည်သူမည်ဝါဖြစ်ကြောင်း ဖော်ပြနိုင်သည့် အချက်အလက် တချို့ကို ဖယ်ရှားထားသကဲ့သို့ ASD ၏ ACSC တုန့်ပြန်မှု နည်းလမ်းတချို့ကိုလည်း ဖယ်ရှားထားပါသည်။

အဓိကအကြောင်းအရာ အကျဉ်းချုပ်

ဤအစီရင်ခံစာတွင် ၂၀၂၂ ခုနှစ် ဇူလိုင်လနှင့် စက်တင်ဘာလအကြား တိုက်ခိုက်ခံရသည့် အဖွဲ့အစည်းတစ်ခု၏ ကွန်ရက်နှင့် ပတ်သက်ပြီး ASD အော်ကတွင်ရှိသည့် ACSC စုံစမ်းစစ်ဆေးမှု၏ တွေ့ရှိချက်များကို ဖော်ပြထားပါသည်။ ဤစုံစမ်းစစ်ဆေးချက် အစီရင်ခံစာအား အဖွဲ့အစည်းသို့ ပေးပို့ကာ ၎င်းအနေဖြင့် မသမာသည့် လှုပ်ရှားမှုများကို စောင့်ကြည့်ရန်နှင့် ပြန်လည် ပြုပြင်ထူထောင်မှုများ လုပ်ကိုင်နိုင်မည့် မူဘောင် အကြံပြုချက်များ ပေးပို့ခဲ့ပါသည်။ စုံစမ်းစစ်ဆေးချက်အရ APT40 မှ တိုက်ခိုက်မှုလုပ်ကြောင်း ပြသထားပါသည်။

ဩဂုတ်လလယ်ပိုင်းတွင် ASD ၏ ACSC မှ ထိုအဖွဲ့အစည်းကို ဆက်သွယ်ပြီး တိုက်ခိုက်ခံရနိုင်ခြေများသည့် ကွန်ရက်တစ်ခုအား မသမာသူများ အသုံးပြုကာ ၎င်း၏ ကွန်ရက်နှင့် ချိတ်ဆက်မှုလုပ်နေကြောင်း အသိပေးရာမှ ဩဂုတ်လနှောင်းပိုင်းတွင် ထိုအဖွဲ့အစည်း၏ ခွင့်ပြုချက်ဖြင့် ASD ၏ ACSC မှ host-based ဆင်ဆာ များ အသုံးပြုကာ အဖွဲ့အစည်း၏ ကွန်ရက်ကို တိုက်ခိုက်နိုင်သည့်လုပ်ရပ်များကို စောင့်ကြည့်ခဲ့ပါသည်။ ထိုဆင်ဆာများသည် ASD ၏ ACSC အား ဒီဂျစ်တယ်ဆိုင်ရာ စုံစမ်းစစ်ဆေးမှုများ ပြုလုပ်နိုင်စေရန်အတွက် အခင်းဖြစ်ပွားမှုကို တုန့်ပြန်သည့် အသေးစိတ် အချက်အလက်များကို ရရှိစေပါသည်။ ရရှိသည့် ဆင်ဆာ၏ ဒေတာများကို အသုံးပြုကာ ASD ၏ ACSC မှ အသေးစိတ် ခွဲခြမ်းစိတ်ဖြာမှုလုပ်ပြီး လေ့လာသည့်အခါ မသမာသူ အဖွဲ့များ၏ လှုပ်ရှားမှုကို ပုံဖော်နိုင်ပြီး ၎င်းတို့၏ လှုပ်ရှားမှု အခင်းအကျင်းများ၏ အချိန်ဇယားများကိုလည်း မှတ်သားနိုင်ခဲ့ပါသည်။

ဇူလိုင်လမှ ဩဂုတ်လအထိ ASD ၏ ACSC မှ တွေ့ရသည့် မသမာသူများ၏ အဓိက လှုပ်ရှားမှုထဲတွင် -

- မသမာသူများအနေဖြင့် ကွန်ရက်အတွင်းတွင် ၎င်းတို့၏ လှုပ်ရှားမှု မြေပုံကို ထားရှိရန်အတွက် Host အတွင်းမှ လုပ်ငန်းစဉ်ကို ဖော်ထုတ်ခြင်း
- မသမာသူများသည် ကွန်ရက်အတွင်း ကနဦး အခြေချနိုင်ရန်နှင့် ကွပ်ကဲမှု စွမ်းရည်ကို ဖျက်ဆီးရန်အတွက် web shell ကို အသုံးပြုခြင်း
- မသမာသည့် ရည်ရွယ်ချက်များဖြင့် အခြားသော ပစ္စည်းများကို အသုံးပြုခြင်းများ ပါဝင်ပါသည်။

စုံစမ်းစစ်ဆေးမှုအတွင်း တွေ့ရှိရသည်မှာ ထိလွယ်ရှလွယ်သော ဒေတာ အချက်အလက်များကို မသမာသူများ ရရှိပြီး ၎င်းတို့သည် (T1021.002) ကွန်ရက်အတွင်းရှိ စနစ်များအကြား သွားလာလှုပ်ရှားမှုများ ပြုလုပ်သည့် သက်သေအထောက်အထားများ တွေ့ခဲ့ရပါသည်။ တိုက်ခိုက်ခံရမှု အများစုသည် ကွန်ရက်အတွင်း ထိုအဖွဲ့၏ ရှိနှင့်ပြီးသား vectorများ၏ မျိုးစုံသော လှုပ်ရှားမှုကြောင့် ဖြစ်ရပါသည်၊ ကွန်ရက်သည် ပြားချပ်နေသည့် ပုံသဏ္ဌာန်ရှိပြီး ထင်ရာမြင်ရာ ဖိုင်များကို upload လုပ်ရန်အတွက် လုံခြုံမှု မရှိသည့် အတွင်းပိုင်းထုတ် ဆော့ဖ်ဝဲများ အသုံးပြုခြင်းတို့ကြောင့် ဖြစ်ပါသည်။ ဒေတာအချက်အလက်များကို လျှို့ဝှက်စွာ ထုတ်ယူရာတွင် အထူးခွင့်ပြုချက်ရမှ ဝင်ရောက်ခွင့်ရှိသည့် credentialဖြင့် ထိုအဖွဲ့အား log in ဝင်ခြင်းများ ပြုလုပ်နိုင်စေသကဲ့သို့ မူလဝင်ရောက်ခွင့် vector ပိတ်ချခံထားသော်လည်း မသမာသူများအား ခွင့်ပြုချက်ကန့်သတ်ထားသည့် အရာများကို ပြန်လည် ဝင်ရောက်ခွင့်ရရှိစေပါသည်။ စတင်အတိုက်ခိုက်ခံရသည့် စက်တွင် မသမာသည့် ပစ္စည်းပိုများကို မတွေ့ရပါ- သို့သော် ထိုအဖွဲ့သည် စစ်မှန်သည့်အကောင့်၊ အခွင့်ထူးရရှိသည့် credentials အချက်အလက်များဖြင့် ဝင်ရောက်သည့်အတွက် မသမာသည့် ပစ္စည်းများ ပိုသုံးရန်မလိုတော့ခြင်း ဖြစ်စေနိုင်ပါသည်။ စုံစမ်းစစ်ဆေးမှု၏ တွေ့ရှိချက်များအရ အားနည်းချက်များရှိကြောင်း လူအများသိရှိရာက အခွင့်အလမ်းသာ၍ တိုက်ခိုက်ခံရခြင်းမျိုးထက် ထိုအဖွဲ့အစည်းသည် တမင်တကာ APT40 ၏ ပစ်မှတ်ထားမှုကို ခံရဟန်ရှိပါသည်။

စုံစမ်းစစ်ဆေးမှု၏ တွေ့ရှိချက်များ

၂၀၂၂ ခုနှစ် ဩဂုတ်လလယ်ပိုင်းတွင် ASD ၏ ACSC က နိုင်ငံတစ်ခုမှ ကျောထောက်နောက်ခံပြုထားသည့် မသမာသော IP တစ်ခုသည် ထိုအဖွဲ့အစည်း၏ ကွန်ပြူတာ ကွန်ရက်များထဲသို့ အနည်းဆုံးဇူလိုင်လနှင့် ဩဂုတ်လထဲတွင် ဝင်ရောက်ရန် ကြိုးစားမှုရှိခဲ့ကြောင်း ထိုအဖွဲ့အစည်းအား အကြောင်းကြားခဲ့ပါသည်။ တိုက်ခိုက်ခံရသည့် စက်ပစ္စည်းတစ်ခုမှာ အသေးစား လုပ်ငန်းသုံးပစ္စည်း သို့မဟုတ် အိမ်သုံး စက်ပစ္စည်း ဖြစ်ဟန် ရှိပါသည်။

ဩဂုတ်လ နှောင်းပိုင်းတွင် ASD ၏ ACSC မှ ထိုအဖွဲ့အစည်း၏ ကွန်ရက်တွင် hosts လုပ်ရန်အတွက် host-based agent ကို အသုံးပြုခဲ့ပြီး ထိုအရာက တိုက်ခိုက်ခံရမှုအတွင်း မည်သည့်အချက်များအပေါ် သက်ရောက်မှုရှိခဲ့ကြောင်း သက်သေအထောက်အထားကို ပြသနိုင်ခဲ့ပါသည်။

စုံစမ်းစစ်ဆေးမှုများကို အထောက်အကူပြုစေမည့် တချို့သော အရာများရှိလျင် အထောက်အကူပြုနိုင်သော်လည်း logging ဖွဲ့စည်းမှုနှင့် ကွန်ရက်ဒီဇိုင်း အနေအထားကြောင့် မရနိုင်ခဲ့ပေ။ သို့သော်လည်း ထိုအဖွဲ့အစည်းအနေဖြင့် ရရှိသည့် ဒေတာအချက်အလက်များအားလုံးကို ASD ၏ ACSC အား မျဉဝေရန် အသင့်အနေအထားရှိသည့်အတွက် တုန့်ပြန်ဖြေရှင်းသူများအနေဖြင့် ထိုတိုက်ခိုက်မှု အဖြစ်အပျက်အား အသေးစိတ် ခွဲခြမ်းစိတ်ဖြာ လေ့လာမှု လုပ်နိုင်ခဲ့သကဲ့သို့ APT40 ၏ ကွန်ရက်အတွင်း လှုပ်ရှားမှုများကိုလည်း နားလည်သဘောပေါက်မှု ရရှိစေခဲ့ပါသည်။

စက်တင်ဘာလတွင် ASD ၏ ACSC နှင့် တိုင်ပင်ဆွေးနွေးမှုလုပ်ပြီးနောက်ပိုင်း ထိုအဖွဲ့အစည်းသည် အစောပိုင်းတွင် ဖော်ပြခဲ့သည့် မသမာသည့် IP ကို အပယ်စာရင်းထဲ ထည့်ရန် ဆုံးဖြတ်ခဲ့ပါသည်။ အောက်တိုဘာလအတွင် ထို အဖွဲ့အစည်းက ပြန်လည်ပြုပြင်ထူထောင်မှုများ ပြုလုပ်ခဲ့ပါသည်။

အသေးစိတ်များ

ဇူလိုင်လ အစောပိုင်းတွင် မသမာသူများက (T1190) custom web application ကို စမ်းသပ်ခြင်းနှင့် အလွဲသုံးစားမှုလုပ်နိုင်ခဲ့ပြီး `<webapp>2-ext` တွင် လည်ပတ်မှုလုပ်ခဲ့ကာ ၎င်းသည် ကွန်ရက်၏ စစ်မဲ့ဇုန် (DMZ) တွင် ခြေကုတ်မှု ရရှိစေခဲ့ပါသည်။ ထိုအရာက ကွန်ရက်အပြင် မြင်သာသည့် ဒိုမိန်းများအားလုံးကို စာရင်းသွင်းခြင်းများ လုပ်ခဲ့ပါသည်။ စက်ပစ္စည်းတချို့၏ စစ်မဲ့ဇုန် DMZ မှတဆင့် အခိုးခံရသည့် အချက်အလက် credentials (T1078.002) ကို Active Directory (T1018) အား query လုပ်ရန်နှင့် file shares (T1039) ကို စတင်ပြီး အချက်အလက်များကို ခိုးယူထုတ်ရန် အတွက် ပြင်ဆင်မှုများ လုပ်ဆောင်ခဲ့ပါသည်။ မသမာသူများသည် (T1558.003) ဆာဗာမှ ကွန်ရက်၏ credentials အချက်အလက် အစစ်အမှန်များ ရရှိရန်အတွက် Kerberoasting နည်းဖြင့် တိုက်ခိုက်မှု လုပ်ခဲ့ပါသည်။ ထိုအဖွဲ့သည် စစ်မဲ့ဇုန်နှင့် ကွန်ရက်အတွင်းတွင် မည်သည့် နေရာမှ ထပ်မံ ဝင်ရောက်မှု မရှိခဲ့ကြောင်း တွေ့ရှိရပါသည်။

မြင်သာသော ဇယား

အောက်ပါ ဇယားကွက်သည် ထိုအဖွဲ့အစည်း၏ ကွန်ရက်တိုက်ခိုက်မှုအတွင်း မသမာသူများ အသုံးပြုသည့် အဓိက အဆင့်များ၏ ယေဘုယျခြုံငုံသုံးသပ်ချက်ကို ဖော်ပြထားပါသည်။

ကနဦး ရှာဖွေတွေ့ရှိချက်

အဖွဲ့အစည်းအတွက် သီးသန့်တည်ဆောက်ပေးသည့် ဝဘ်အက်ပလီကေးရှင်းကို မသမာသူများ စမ်းသပ်ကြည့်ခြင်း

အလွဲသုံးစားခြင်း

T1190 Public-Facing Application ကို အလွဲသုံးစားခြင်း

Web application ကို အလွဲသုံးစားခြင်းနှင့် web shell ကို ဖန်တီးခြင်း

Host ကို စာရင်းမှတ်သားခြင်း

T1082 စနစ်အချက်အလက်ကို ရှာဖွေတွေ့ရှိခြင်း

Host ကို စာရင်းမှတ်သားခြင်းနှင့် မဆုတ်မနစ်မှုကို အခြေချခြင်း

အထောက်အထားပြည့်စုံစွာ အသုံးပြုကာ ဝင်ရောက်ခြင်းကို ပထမဆုံး တွေ့ရှိခြင်း

မသမာသည့် ဆက်သွယ်မှု

အဖွဲ့အစည်း၏ စက်ပစ္စည်းအား နိုင်ငံတော်၏ ကျောထောက်နောက်ခံမှု ရှိသည့် အခြေခံအဆောက်အအုံတစ်ခုမှ မသမာသည့် ဆက်သွယ်မှုလုပ်ခြင်းကို ပထမဆုံးတွေ့ရှိခြင်း

ကွန်ရက် စူးစမ်းထောက်လှမ်းမှု

T1021.002 အဝေးထိန်း ဝန်ဆောင်မှု - SMB/Windows Admin Shares

T1135 Network Share Discovery

ကွန်ရက်အခြေစိုက် စူးစမ်းထောက်လှမ်းမှုနှင့် လှုပ်ရှားမှုထဲတွင် - SMB shares ကို တပ်ဆင်ခြင်း၊ ကွန်ရက်အခြေစိုက် scanning နှင့် ဒိုမိန်းများကို စာရင်းသွင်းခြင်းတို့ ပါဝင်ပါသည်။

ချိတ်ဆက်မှု ရရှိရန် ပြန်လည်လုပ်ဆောင်ခြင်း

T1090 Proxy

မသမာသူများ ssf tool (ဇူလိုင် 28 ရက်နှင့် အချို့နေ့များတွင် ပြုလုပ်သည့် လှုပ်ရှားမှုနှင့် ဆင်တူ) နှင့် ချိတ်ဆက်မှု ရရှိရန် ပြန်လည်လုပ်ဆောင်ခြင်း

အသေးစိတ် အချိန်ဇယား

ဇူလိုင် - မသမာသူများသည် (T1102) transport layer security (TLS) ချိတ်ဆက်မှုမှတဆင့် အဖွဲ့အစည်းအတွက် သီးသန့်ဖန်တီးပေးထားသည့် web application ရှေ့စာမျက်နှာ (T1190) ဖြင့် ကနဦးချိတ်ဆက်မှုရရှိရန် ကြိုးစားခဲ့သည်။ (ဤနောက်ပိုင်း 'web application' သို့မဟုတ် '*webapp*') ဟုသာခေါ်ဆိုမည်။ တခြား သိသာမှတ်သားဖွယ်ရာ လှုပ်ရှားမှုများ မတွေ့ရပါ။

ဇူလိုင် - မသမာသူများသည် ပိုမို စုံစမ်းမှုလုပ်ရန်အတွက် အဆုံးမှတ်များ endpoints[2] ကို ရှာကြည့်သည့်အနေဖြင့် web application အား စတင်စာရင်းမှတ်သားမှုများ လုပ်ခဲ့ပါသည်။

July: သီးသန့် အဆုံးမှတ် Endpoint တစ်ခုကို အလွဲသုံးစား တိုက်ခိုက်ရန် အတွက် မသမာသူများ စတင်အာရုံစူးစိုက် လုပ်ဆောင်ခဲ့ပါသည်။

ဇူလိုင် - မသမာသူများအနေဖြင့် web server ဆီ အောင်မြင်စွာ `POST` ပို့ဆောင် နိုင်ခဲ့ပြီး တခြားစာမျက်နှာတွင်ရှိသည့် web shell မှတဆင့် ပြုလုပ်ခဲ့ဟန် ရှိသည်။ ထိုမသမာသူများ အသုံးပြုသည်ဟု ထင်ရသည့် နောက်ထပ် IP တစ်ခုလည်း ထို URL ကို တင်ခြင်းမျိုး စတင်ပြုလုပ်ခဲ့ပါသည်။ မသမာသူများက web shells များကို ဖန်တီးပြီး စမ်းသပ်မှုများ လုပ်ခဲ့သည်။

မည်သည့် အလွဲသုံးစားမှု နည်းလမ်းအား အသုံးပြုခဲ့သည်ကို အတိအကျ မသိရသော်လည်း သီးသန့် အဆုံးမှတ် endpoint တစ်ခုအား ပစ်မှတ်ထားခဲ့သည်မှာ သေခြာပြီး `<webapp>2-ext` တွင် ဖိုင်များ ဖန်တီးရန် လုပ်ဆောင်ခဲ့ပါသည်။

ဆက်သွယ်မှု ရယူရန် ကြိုးပမ်းသည့် IP လိပ်စာ နှစ်ခုစလုံးသည် တူညီသောအုပ်စုက ပိုင်ဆိုင်သည်ဟု ASD ၏ ACSC အနေဖြင့် ယုံကြည်ပြီး အကြောင်းရင်းမှာ ၎င်းတို့ နှစ်ခုစလုံးသည် လိုချင်မှုများ တူညီကြသလို ကနဦး ချိတ်ဆက်မှု ရရှိရန် ကြိုးစားလုပ်ဆောင်သည့် အချိန်သည်လည်း မိနစ်ပိုင်းလောက်သာ ကွာခြားသည့်အတွက် ဖြစ်ပါသည်။

ဇူလိုင် - ထိုမသမာသည့် အုပ်စုသည် host ကို စာရင်းမှတ်သားခြင်းများ ဆက်လက်လုပ်ဆောင်ပြီး အခွင့်ထူး ဝင်ခွင့်ရရန် အခွင့်အလမ်းကို ရှာဖွေပြီး တခြား web shells များကိုလည်း အသုံးပြုမှု လုပ်ခဲ့ပါသည်။ မသမာသူများသည် `<firstname.surname>@<organisation domain>`ထဲ ဝင်ရောက်နိုင်ရန်အတွက် အခိုးခံရသည့် credentials အထောက်အထားများကို အသုံးပြုခဲ့ပါသည်။

မသမာသူများအနေဖြင့် `<webapp>2-ext` တွင် ရရှိသည့် ခွင့်ပြုချက်ထက် အခွင့်အရေးတိုးချဲ့ ရယူခြင်း privilege escalation လုပ်ရန် ကြိုးစားခဲ့သော်လည်း အောင်မြင်ခဲ့ဟန် မရှိပါ။ ထိုအစား မသမာသူများသည် ကွန်ရက်အခြေပြု လှုပ်ရှားမှုကို အာရုံစူးစိုက်ခဲ့ကြပါသည်။

ဇူလိုင် - မသမာသူများသည်[3] ဝန်ဆောင်မှု အကောင့်အတွက် အခိုးခံရသည့် credentials အချက်အလက်များဖြင့် internally accessible binaries တွင် hardcoded များ တွေ့ရှိခဲ့ဟန် ရှိပါသည်။

ဇူလိုင် - မသမာသူများသည် open-source ပစ္စည်းဖြစ်သည့် Secure Socket Funnelling ကို အသုံးပြုပြီး ၎င်းအား မသမာသည့် အခြေခံအဆောက်အအုံများနှင့် ချိတ်ဆက်ရန်အတွက် အသုံးပြုခဲ့သည်။ ထိုချိတ်ဆက်မှုသည် မသမာသူမှ အဖွဲ့အစည်း၏ အတွင်းကွန်ရက်ထဲဒေတာ စီးဆင်းမှုရရှိရန်အတွက် လုပ်ဆောင်ခြင်းဖြစ်ပြီး ဝန်ဆောင်မှုအတွက် credentials များ အသုံးပြုရန် ကြိုးစားစဉ်အတွင်း ထိုအဖွဲ့အစည်း၏ စက်နာမည်နှင့် အဖြစ်အပျက် စာရင်းများ event logs များ ပေါက်ကြားမှု ဖြစ်ခဲ့ပါသည်။

ဩဂုတ် - မသမာသူများသည် အကန့်အသတ်ရှိသည့် လှုပ်ရှားမှုများ လုပ်ခဲ့သည်ကို တွေ့ရပြီး ထိုအထဲတွင် ဝန်ဆောင်မှုအကောင့်နှင့် ချိတ်ဆက်မှုရရှိရန် ကြိုးစားရာတွင် အောင်မြင်ခြင်းမရှိသည့် လုပ်ရပ်လည်း ပါဝင်ပါသည်။

ဩဂုတ် - မသမာသူများသည် ကွန်ရက်နှင့် Active Directory များကို စာရင်းမှတ်သားခြင်းများ သိသိသာသာ လုပ်ဆောင်ခဲ့ပါသည်။ Windows machines ထဲမှ စစ်မဲ့ဇုန်DMZ တွင် mount shares[4] ကို ပြင်ဆင်မှုများ လုပ်ပြီး အချက်အလက်များကို အောင်မြင်စွာ ခိုးယူရန်အတွက် တခြားအခိုးခံရသည့် အကောင့်တစ်ခုကို အသုံးပြုခဲ့ပါသည်။

DMZ အတွင်း ပြင်ဆင်ရေးစက်များထဲတွင် အခိုးခံရသည့် credential အချက်အလက်တစ်ခုကို အသုံးပြုရန်အတွက် အခွင့်အလမ်းရရှိခဲ့ဟန် ရှိပါသည်။ Firewalls မှ မသမာသူအား ပစ်မှတ်ထားခံရသည့် အတွင်းပိုင်းကွန်ရက်မှ အလားတူ လှုပ်ရှားမှုများ မလုပ်နိုင်အောင် ကာကွယ်ပေးခဲ့ပါသည်။

ဩဂုတ် - **စက်တင်ဘာ** SSF tool ကို ပြန်လည်အသုံးချကာ မသမာသည့် IP နှင့် ပြန်လည်ချိတ်ဆက်မှုရရန် လုပ်ဆောင်ခဲ့ပါသည်။ ထိုအဖွဲ့သည် ၎င်းတို့၏ ဝင်ရောက်မှုကို ပိတ်ပင်လိုက်သည့်အချိန်အထိ မည်သည့်လှုပ်ရှားမှုများမှ ထပ်လုပ်သည်ကို မတွေ့ရပါ။

စက်တင်ဘာ - အဖွဲ့အစည်းက ၎င်း၏ firewalls ကို အသုံးပြုကာ ထိုမသမာသည့် IP ကို စာရင်းမှ ပယ်ဖျက်ခြင်းလုပ်ကာ ပိတ်ဆို့မှု လုပ်လိုက်ပါသည်။

2 ဤအနေအထားတွင် အဆုံးမှတ် endpoint ဆိုသည်မှာ web application အတွင်းရှိ လုပ်ဆောင်ချက်တစ်ခု ဖြစ်ပါသည်။

3 ဝန်ဆောင်မှုအကောင့်သည် တစ်ဦးတစ်ယောက်နှင့် ဆက်စပ်မှုမရှိပဲ ဝန်ဆောင်မှုများနှင့် ဆက်စပ်ပါသည်။ Microsoft corporate ဒိုမိန်းတစ်ခုတည်းတွင် အကောင့်အမျိုးအစားပေါင်း များစွာ ရှိပါသည်။

4 Mounting shares ဆိုသည်မှာ ဖိုင်ဖွဲ့စည်းပုံ စနစ်တွင် အသုံးပြုသူ သို့မဟုတ် အသုံးပြုသည့် အဖွဲ့အတွက် ဖိုင်များကို ဖန်တီးလုပ်ဆောင်ပေးခြင်း ဖြစ်ပါသည်။

မသမာသူများ အသုံးပြုသည့် နည်းဗျူးဟာ နှင့် နည်းပညာများ

MITRE ATT&CK မူဘောင်ဆိုသည်မှာ ဆိုင်ဘာလောကတွင် မသမာသည့် သူများအသုံးပြုသည့် နည်းဗျူဟာနှင့် နည်းပညာများကို စုဆောင်းထားသည့် စာရွက်စာတမ်း ဖြစ်ပါသည်။ ထိုမူဘောင်ကို အမေရိကန်မှ အကျိုးအမြတ် မယူသည့် The MITRE Corporation မှ စုစည်းဖန်တီးပေးခြင်းဖြစ်ပြီး မသမာသူများ၏ အပြုအမူနှင့် ပတ်သက်ပြီး တကမ္ဘာလုံး အသုံးပြုသည့် ဘုံဘာသာစကားအဖြစ် ဆောင်ရွက်ပေးပါသည်။

ASD ၏ ACSC သည် မသမာသူများ၏ တရားမဝင် လှုပ်ရှားမှုနဲ့ သင့်တော်သည့် နည်းပညာနှင့် နည်းဗျူဟာများကို အောက်ပါအတိုင်း လေ့လာမှတ်သားထားပါသည်။

စူးစမ်းထောက်လှမ်းခြင်း

T1594 – တိုက်ခိုက်ခံရသူ ပိုင်ဆိုင်သည့် ဝဘ်ဆိုက်ကို ရှာဖွေခြင်း

မသမာသူများသည် ကွန်ရက်ထဲ ဝင်ရောက်နိုင်သည့် အခွင့်အရေး ရရှိရန် အတွက် web application ၏ ဝဘ်ဆိုက်ကို မှတ်သားထားခြင်းမျိုး လုပ်ပါသည်။

ကနဦး ဝင်ရောက်ချက်

T1190 – အများပြည်သူနှင့် သက်ဆိုင်သည့် အက်ပလီကေးရှင်းများကို အလွဲသုံးစားတိုက်ခိုက်ခြင်း (သီးသန့်ပြုလုပ်ထားသည့် web application နှင့် ပတ်သက်၍)

T1078.002 – စစ်မှန်သော အကောင့်များ - ဒိုမိန်း အကောင့်များ (အခိုးခံရသည့် ပြည့်စုံသော အထောက်အထား အချက်အလက် မှတ်တမ်းများနှင့် ပတ်သက်၍)

မသမာသူကို ကနဦး ဝင်ရောက်နိုင်စေမည့် လမ်းကြောင်းကို ထားရှိပေးရန်အတွက် အင်တာနက်နှင့် ထိတွေ့မှုရှိသည့် သီးသန့်ပြုလုပ်ထားသည့် web application ကို အလွဲသုံးစားလုပ်ခြင်း ဖြစ်ပါသည်။ မသမာသူသည် နောက်ပိုင်းတွင် ၎င်းတို့ ခိုးယူထားသည့် ပြည့်စုံသော အထောက်အထားများကို အသုံးပြုကာ ကွန်ရက်အတွင်း ထပ်မံဝင်ရောက်မှုများ လုပ်ဆောင်နိုင်ခဲ့ပါသည်။

ဖယ်ရှားကွပ်မျက်ခြင်း

T1059 – ကွပ်ကဲခြင်း နှင့် Scripting Interpreter (web shell မှတဆင့် ကွပ်ကဲခြင်းကို ဖယ်ရှားကွပ်မျက်ခြင်းနှင့် ပတ်သက်၍)

T1072 – Software ဖွံ့ဖြိုးရေး ပစ္စည်း (မသမာသူသည် IP နှင့် ချိတ်ဆက်ရန် အတွက် open-source ပစ္စည်းတစ်ခုဖြစ်သည့် Secure Socket Funnelling (SSF) ကို အသုံးပြုခြင်းနှင့် ပတ်သက်၍)

မဆုတ်မနစ် ကြိုးစားခြင်း

T1505.003 – Server Software Component - Web Shell (web shell အသုံးပြုခြင်းနှင့် ဝင်ရောက်ခွင့်ရရန် SSF ကို အသုံးပြုခြင်းနှင့် ပတ်သက်၍)

လျှို့ဝှက်အချက်အလက်များ ရယူခြင်း

T1552.001 – လျှို့ဝှက်ကုဒ် password ကို သိုလှောင်ရုံမှ ပြည့်စုံသော အထောက်အထားများ (password files နှင့် ဆက်စပ်သည့် စီမံခန့်ခွဲရေး စနစ်(BMS))ကို တည်ဆောက်ရေးနှင့် ပတ်သက်၍)

T1558.003 – Kerberos Tickets ကို ခိုးယူခြင်း သို့မဟုတ် တုပခြင်း - Kerberoasting (ကွန်ရက်ထဲ ဝင်ရောက်ခွင့် အထောက်အထားများ ရရှိရန် အတွက် ပြုလုပ်သည့် တိုက်ခိုက်မှုနှင့် ဆက်စပ်၍)

စနစ်များအကြား ရွှေ့ပြောင်းမှုလုပ်ခြင်း

T1021.002 – အဝေးထိန်း ဝန်ဆောင်မှုများ - SMB Shares (မသမာသူများမှ စက်ပစ္စည်းတချို့မှ SMB shares ကို ပြင်ဆင်ခြင်းနှင့် ပတ်သက်၍)

စုဆောင်းခြင်း

T1213 – Information Repositories မှ ဒေတာ အချက်အလက်များ (BMS server တွင် တွေ့ရသည့် လက်စွဲစာအုပ်/ စာရွက်စာတမ်းနှင့် ပတ်သက်၍)

လျှို့ဝှက်စွာ ထုတ်ယူခြင်း

T1041 – C2 Channel မှ အချက်အလက်ကို လျှို့ဝှက်စွာ ထုတ်ယူခြင်း (Active Directory နှင့် mounting shares မှ ဒေတာများကို မသမာသူ လျှို့ဝှက်စွာ ထုတ်ယူခြင်းနှင့် ပတ်သက်၍)

ဖြစ်ရပ်မှန် နမူနာ ၂

ဤအစီရင်ခံစာကို ကျယ်ပြန့်စွာ ဖြန့်ဝေရန်အတွက် ရည်ရွယ်သဖြင့် နာမည်ရင်းများကို ထိန်ချန်ထားပါသည်။ သည်နောက်ပိုင်းတွင် တိုက်ခိုက်ခံရသည့် အဖွဲ့အစည်းကို 'ထိုအဖွဲ့အစည်း' ဟု သုံးနှုန်းသွားမည် ဖြစ်သည်။ တိုက်ခိုက်ခံရသူ မည်သူမည်ဝါဖြစ်ကြောင်း ဖော်ပြနိုင်သည့် အချက်အလက် တချို့ကို ဖယ်ရှားထားသကဲ့သို့ ASD ၏ ACSC တုန့်ပြန်မှု နည်းလမ်းအချို့ကိုလည်း ဖယ်ရှားထားပါသည်။

အဓိကအကြောင်းအရာ အကျဉ်းချုပ်

ဤအစီရင်ခံစာသည် 2022 ခုနှစ် ဧပြီလအတွင်း ထိုအဖွဲ့အစည်း၏ ကွန်ရက်တိုက်ခိုက်ခံရခြင်းနှင့် ဆက်စပ်ပြီး ASD ၏ ACSCစုံစမ်းစစ်ဆေးမှု၏ တွေ့ရှိချက် အသေးစိတ်ကို ဖော်ပြထားပါသည်။ မသမာသူများ၏ လှုပ်ရှားမှု အကျဉ်းချုံးနှင့် ပြန်လည်ထူထောင်မှု လုပ်ရန်အတွက် အကြံပြုချက်များကို အကောင်အထည်ဖော်ရန်အတွက် ဤအစီရင်ခံစာအား ထိုအဖွဲ့အစည်းကို ပေးအပ်ခဲ့ပါသည်။ တိုက်ခိုက်မှုကို APT40 မှ ပြုလုပ်ခဲ့ကြောင်း စစ်ဆေးတွေ့ရှိရပါသည်။

၂၀၂၂ ခုနှစ် မေလတွင် ASD ၏ ACSC မှ ထိုအဖွဲ့အစည်းအား ၎င်း၏ ကွန်ရက်သည် ၂၀၂၂ ခုနှစ် ဧပြီလမှစ၍ သံသယဖြစ်ဖွယ်ရာ မသမာသည့် ဆိုင်ဘာလှုပ်ရှားမှု၏ ဒဏ်ကို ခံရနိုင်ကြောင်း အသိပေးမှု လုပ်ခဲ့ပါသည်။ နောက်ပိုင်းတွင် ထိုအဖွဲ့အစည်းက အင်တာနက်ဖြင့် ချိတ်ထားသည့် အဝေးမှ ဝင်ရောက်ခွင့် ၏ login portal တွင် မသမာသည့် ဆော့ဖ်ဝဲကို ရှာဖွေတွေ့ရှိခဲ့ကြောင်း ASD ၏ ACSC ကို အကြောင်းကြားခဲ့ပါသည်။ ဤ ဆာဗာသည် အဝေးမှ ဝင်ရောက်ခွင့် login နှင့် အထောက်အထား စီမံခန့်ခွဲရေး ထုတ်ကုန်ကို အသုံးပြုခဲ့ပြီး ဤအစီရင်ခံစာထဲတွင် ၎င်းကို 'တိုက်ခိုက်ခံရသည့် ကိရိယာ' ဟု ရည်ညွှန်းမည် ဖြစ်ပါသည်။ ASD ၏ ACSC ၏ စုံစမ်းစစ်ဆေးမှုကို အခြေခံကာ အဖွဲ့အစည်းအတွက် စုံစမ်းစစ်ဆေးရေး တွေ့ရှိချက်များနှင့် တိုက်ခိုက်ခံရပြီးနောက် မည်ကဲ့သို့ ပြန်လည်ထူထောင်မှုများ လုပ်နိုင်သည်ဆိုသည့် အကြံပြုချက်များကို ဖော်ပြထားပါသည်။

သက်သေများအရ အနည်းဆုံး ၂၀၂၂ ခုနှစ် ဧပြီလမှ စတင်၍ ထိုအဖွဲ့အစည်း၏ ကွန်ရက်သည် ၎င်း၏ အဝေးမှဝင်ရောက်ခွင့် login portal မှတဆင့် မသမာသူများ၏ တိုက်ခိုက်မှုကို ခံခဲ့ရကြောင်း တွေ့ရှိရပါသည်။ ဤဆာဗာသည် တစ်ဦးထက်မကသော မသမာသူများ၏ တိုက်ခိုက်မှုကို ခံရဖွယ်ရှိပြီး တိုက်ခိုက်ခံရသည့် ကာလအတွင်း ကျယ်ကျယ်ပြန့်ပြန့် သိကြသည့် remote code execution (RCE) အားနည်းချက်မှတဆင့် တိုက်ခိုက်ခံရနိုင်ဖွယ် ရှိပါသည်။

ASC ၏ ACSC မှ လေ့လာမိသည့် မသမာသူ၏ အဓိက လှုပ်ရှားမှုထဲတွင် -

- host ကို မှတ်တမ်းယူခြင်း၊ ထိုလုပ်ရပ်သည် မသမာသူကို ကွန်ရက်အတွင်း ၎င်း၏ ကိုယ်ပိုင်မြေပုံကို တည်ဆောက်ခွင့်ရရှိစေခြင်း
- အင်တာနက်နှင့် ချိတ်ဆက်မှုရှိသည့် application များကို အလွဲသုံးစားခြင်းနှင့် web shell ကို အသုံးပြုခြင်း - ထိုလုပ်ရပ်သည် မသမာသူကို ကွပ်ကဲရေးကို အကောင်အထည်ဖော်ရန်အတွက် ကွန်ရက်ထဲတွင် ခြေကုတ်ရယူစေခြင်း
- ဆော့ဖ်ဝဲ၏ အားနည်းချက်များကို အလွဲသုံးစားလုပ်ကာ ရရှိသည့် ခွင့်ပြုချက်ထက် အခွင့်အရေးတိုးချဲ့ ရယူခြင်း
- အထောက်အထားခိုင်သည့် credential အချက်အလက်များကို စုဆောင်းကာ စနစ်အတွင်း ရွှေ့လျားနိုင်အောင် လုပ်ဆောင်ခြင်း

ASD ၏ ACSC တွေ့ရှိချက်အရ မသမာသူသည် ၂၀၂၂ ခုနှစ် ဧပြီလတွင် တိုက်ခိုက်ခံရသည့် ကွန်ရက်အတွင်းမှ ထူးခြားသည့် username နှင့် password ရာနဲ့ချီကို လျှို့ဝှက်စွာ ခိုးထုတ်ခဲ့ကြောင်း တွေ့ရပြီး အချက်အလက်မျိုးစုံဖြင့် အတည်ပြုရသည့် ကုဒ်ပေါင်း ရာနှင့်ချီအပြင် အဝေးမှ ဝင်ရောက်ခွင့်ဆိုင်ရာ နည်းပညာ ပစ္စည်း၏ အချက်အလက်များကိုလည်း ခိုးထုတ်ခဲ့ပါသည်။ ထို အဖွဲ့အစည်း၏ ဆန်းစစ်မှုအရ password များသည် စစ်မှန်သည့် passwords များ ဖြစ်ကြောင်း တွေ့ရှိရပါသည်။ ASD ၏ ACSC အကဲဖြတ်မှုအရ မသမာသူသည် စစ်မှန်သည့် အသုံးပြုသူအနေဖြင့် ဝင်ရောက်ကာ နည်းပညာကိရိယာကို ခိုးယူခြင်းနှင့် အဝေးမှ ဝင်ရောက်ခွင့်ရအောင် လုပ်ဆောင်ပြီး စစ်မှန်သော user အကောင့်ဖြင့် အဖွဲ့အစည်း၏ ကွန်ရက်ထဲကို ဝင်ရောက်ခဲ့ဟန် ရှိပါသည်။

စုံစမ်းစစ်ဆေးချက်၏ တွေ့ရှိမှုများ

စုံစမ်းစစ်ဆေးချက် အကျဉ်းချုပ်

ထိုမသမာသူသည် အမှုထမ်းတစ်ဦး၏ အဝေးမှ ဝင်ရောက်ခွင့် login များကို ခိုးယူပြီး ကွန်ရက်အတွင်း တိုက်ခိုက်မှု ပိုလုပ်ရန်အတွက် ထိုအချက်အလက်ကို အသုံးပြုခဲ့သည်ဟု ASD ၏ ACSC က သုံးသပ်ထားပါသည်။ တိုက်ခိုက်မှု စတင်ခံရသည့် အရာတွင် လုပ်ငန်းတာဝန်များကို တူညီစွာ ဖြန့်ဖြူးခြင်း load-balanced hosts များ သုံးခု ပါဝင်ကြောင်း အစောဆုံး ဖမ်းယူရမိသည့် သက်သေတွင် ဖော်ပြထားပါသည်။ တိုက်ခိုက်ခံရကြောင်း ကနဦး သိရသည်နှင့် ထိုအဖွဲ့အစည်းက လုပ်ငန်းတာဝန်များကို တူညီစွာ ဖြန့်ဖြူးခြင်း load-balanced hosts သုံးခု ထဲမှ နှစ်ခုကို ပိတ်ချမှု လုပ်ခဲ့ပါသည်။ ရလဒ်အဖြစ် နောက်ပိုင်းတွင် တိုက်ခိုက်မှုများအားလုံးက host တစ်ခုတည်းတွင် ဖြစ်ပေါ်ခဲ့ပါသည်။ တိုက်ခိုက်ခံရသည့် ကိရိယာနှင့် ဆက်စပ်မှုရှိသည့် တခြားသော servers များသည်လား အလားတူ လုပ်ငန်းတာဝန်များကို တူညီစွာ ဖြန့်ဖြူးခြင်းနည်း load-balanced လုပ်မှုကို ခံခဲ့ရပါသည်။ ရှင်းရှင်းလင်းလင်းရှိစေရန်အတွက် တိုက်ခိုက်ခံရသည့် ကိရိယာများအားလုံးကို ဤအစီရင်ခံစာတွင် 'ကိရိယာ တစ်ခု' အဖြစ် ရည်ညွှန်းသွားမည် ဖြစ်ပါသည်။

မသမာသူသည် ၂၀၂၂ ခုနှစ် ဧပြီလမှ စတင်ကာ လူအများသိသည့် အားနည်းချက်များမှတဆင့် web shells များကို အသုံးပြုကာ ထိုကိရိယာကို တိုက်ခိုက်ခဲ့သည်ဟု ယူဆနိုင်ပါသည်။ ထိုမသမာသည့် အဖွဲ့မှ တိုက်ခိုက်မှု လုပ်သူများသည် ကိရိယာထဲ ဝင်ရောက်ရန်အတွက် လိုအပ်သော escalated privileges ရရှိသည့် ခွင့်ပြုချက်ထက် အခွင့်အရေးတိုးချဲ့ ရယူခြင်း ရှိခဲ့သည်ဟု သုံးသပ်ထားပါသည်။ ASD ၏ ACSC သည် logging မှတ်တမ်းဆိုင်ရာ အချက်အလက်များ လုံလောက်စွာ မရှိသည့်အတွက် ထိုအဖွဲ့၏ လှုပ်ရှားမှု အတိုင်းအတာ အပြည့်အစုံကို မသိနိုင်ပါ။ သို့သော် သက်သေများအရ မသမာသူအနေဖြင့် အောက်ပါ အရာများကို လုပ်ဆောင်နိုင်ခဲ့ကြောင်း တွေ့ရှိရပါသည် -

- စစ်မှန်သည့် username နှင့် password အတွဲပေါင်း ရာနှင့်ချီအား စုဆောင်းနိုင်ခြင်းနှင့်
- စစ်မှန်သော user ကဲ့သို့ virtual desktop infrastructure (VDI) ထဲ ဝင်ရောက်ကာ မသမာသူက နည်းပညာဆိုင်ရာ အချက်အလက်များကို စုဆောင်းနိုင်ခြင်းတို့ ဖြစ်ပါသည်။

မသမာသူသည် အဖွဲ့အစည်း၏ ကွန်ရက်ကို ထပ်မံ တိုက်ခိုက်မှုလုပ်ရန် ကြိုးစားခဲ့ကြောင်းလည်း ASD ၏ ACSC မှ သုံးသပ်ထားပါသည်။ မသမာသူများ လျှို့ဝှက်စွာ ထုတ်ယူနိုင်သည့် အချက်အလက်များက ၎င်းတို့အား စစ်မှန်သော user ကဲ့သို့ လုပ်ဆောင်ကာ virtual desktop sessions ကို ပြန်ပေးဆွဲမှု သို့မဟုတ် စတင်နိုင်မှုဖြစ်စေပြီး administrators အပါအဝင် ၎င်းတို့ သဘောရှိသည့် user ကို စိတ်ကြိုက်ရွေးချယ် အသုံးပြုခဲ့ပုံ ရပါသည်။ မသမာသူများသည် ထိုကဲ့သို့ ဝင်ရောက်မှုဖြစ်စေသည့် vector များကို အသုံးပြုကာ ရေရှည်အထိ မဆုတ်မနစ်တိုက်ခိုက်မှုနှင့် အခြားသော ရည်ရွယ်ချက်များ လုပ်ဆောင်ရန်အတွက် အဖွဲ့အစည်း၏ ဝန်ဆောင်မှုကို ပိုမိုတိုက်ခိုက်မှု လုပ်ခဲ့ပုံရပါသည်။

Hosting provider managed environment အတွင်းရှိ အဖွဲ့အစည်း၏ အခြားသော ကိရိယာများတွင် တိုက်ခိုက်မှု ခံခဲ့ရသည့် သက်သေများ မတွေ့ခဲ့ရပါ။

ဝင်ရောက်ခြင်း

VDI sessions (T1021.001) နှင့် ချိတ်ဆက်ရန်အတွက် တိုက်ခိုက်မှုခံရသည့် ကိရိယာပါဝင်သည့် host သည် Active Directory နှင့် webserver များမှတဆင့် အထောက်အထားစိစစ်မှု authentication များ ပံ့ပိုးခဲ့ပါသည်။

တည်နေရာ	တိုက်ခိုက်မှုခံရသည့် ကိရယာ၏ hostနာမည်များ (တူညီစွာ ဖြန့်ဖြူးခြင်းနည်း load-balanced)
Datacentre 1	HOST1, HOST2, HOST3

ကိရိယာဆီမှတဆင့် အထောက်အထားစိစစ်မှုအောင်မြင်ကြောင်း token လက်မှတ်နှင့် downloaded များ ရရှိသည်နှင့် တပြိုင်နက် ကိရိယာ၏ အခြေခံအဆောက်အအုံထဲတွင် အသုံးပြုသူများအတွက် VDI စီးဆင်းမှုဖြစ်စေသည့် host များအတွက် ဝင်ပေါက်တံခါးများ ရှိပါသည်။

ထို host များ တိုက်ခိုက်ခံရသည့် သက်သေအထောက်အထားများ မတွေ့ရပါ။ သို့သော် host များအတွက် ဝင်ပေါက်တံခါးဆိုင်ရာ မှတ်တမ်းများအရ host များသည် မသမာသည့် IP လိပ်စာများနှင့် အပြန်အလှန် ဆက်ဆံမှုရှိခဲ့ကြောင်း ပြသထားပါသည်။ ဤ host အတွင်း သို့မဟုတ် အခြား ကွန်ရက်တစ်ခု၏ ချိတ်ဆက်မှုများသည် ဤ host ဆီ ရောက်နိုင်သည့် မသမာသူ၏ အခြေခံအဆောက်အအုံနှင့် ချိတ်ဆက်မှုကြောင့် ထိုကဲ့သို့ ပြသခြင်း အလားအလာများပါသည်။ ရှိနေသည့် အထောက်အထားကို အသုံးပြု၍ ထို လှုပ်ရှားမှု၏ အနေအထားအား ကောက်ချက်မချနိုင်သော်လည်း မသမာသည့် အုပ်စုသည် အဖွဲ့အစည်း၏ ကွန်ရက် (TA0008) အတွင်း ရွှေ့ပြောင်းမှုများ လုပ်ခဲ့ကြောင်း ပြသနေပါသည်။

ကွန်ရက်အတွင်း hosts များ

ASD ၏ ACSC သည် အဖွဲ့အစည်း၏ ကွန်ရက်များကို သီးသန့်စီခွဲခြားထားခြင်းမှ အကန့်အသတ်ဖြင့်သာ ရရှိသော အချက်အလက်များဖြင့် စုံစမ်းစစ်ဆေးမှု လုပ်ခဲ့ပါသည်။ တိုက်ခိုက်ရန် ကြိုးစားသည့် သို့မဟုတ် တိုက်ခိုက်မှုအောင်မြင်သည့် မသမာသည့် လှုပ်ရှားမှုကြောင့် အဖွဲ့အစည်း၏ အတွင်းပိုင်းမှ သီးသန့်စီခွဲခြားထားခြင်း ကွန်ရက်များအပေါ် သက်ရောက်မှုရှိခဲ့ပြီး ထိုအထဲတွင် မသမာသူများက VDI နှင့် ဆက်စပ်သည့် အရာများကို ဝင်ရောက်နိုင်ခြင်း၊ (T1505.001) ဆိုသည့် internal SQL server ကို ဖယ်ရှားနိုင်ခြင်းနှင့် (TA0011) ကိရိယာ၏ ဝင်ပေါက်တံခါးမှတဆင့် မသမာသည့် IP လိပ်စာများ ဆီသို့ မရှင်းပြနိုင်သည့် ဒေတာစီးဆင်းမှုများ ရှိခဲ့သည်ကို သိရပါသည်။

တိုက်ခိုက်ခံရသည့် ကိရိယာအတွင်း ဝင်ရောက်နိုင်မှုကို အသုံးချကာ ထိုမသမာသည့် အုပ်စုသည် စစ်မှန်သော usernamesI passwords (T1003) နှင့် MFA token values (T1111) တို့ကို စုဆောင်းနိုင်ခဲ့ပါသည်။ ထိုအဖွဲ့သည် JSON Web Tokens (JWTs) (T1528) ကို စုဆောင်းနိုင်ခဲ့ပြီး ၎င်းကို virtual desktop login sessions ကို လုပ်ဆောင်ရန်အတွက် အသုံးပြုသည့် စစ်မှန်ကြောင်း

အထောက်အထားများအတွက် အသုံးပြုပါသည်။ မသမာသူသည် ထိုကဲ့သို့ ဝင်ရောက်နိုင်မှုကို အသုံးချကာ virtual desktop sessions (T1563.002) ကို ဖန်တီးခြင်း သို့မဟုတ် ပြန်ပေးဆွဲခြင်းနှင့် စစ်မှန်သော အသုံးပြုသူ (T1078) အဖြစ် ကွန်ရက်အတွင်း၏ သီးသန့်အကန့်များထဲ ဝင်ရောက်မှု လုပ်နိုင်ပါသည်။

မသမာသူသည် SQL server (T1505.001) ကို ပယ်ဖျက်ရန်အတွက် တိုက်ခိုက်ခံရသည့် ကိရိယာထဲ ဝင်ရောက်ပြီး ထိုအရာသည် အဖွဲ့အစည်း၏ အတွင်းပိုင်းကွန်ရက်တွင် တည်ရှိပါသည်။ ထိုဒေတာများကို မသမာသူ ရရှိရန် အလားအလာများပါသည်။

ကိရိယာဆီ ဝင်ရောက်နိုင်သည့် တံခါးပေါက်တို့မှ ရရှိသည့် သက်သေများအရ မသမာသည့် IP လိပ်စာများမှတဆင့် ဤစက်ပစ္စည်းဆီသို့ ကွန်ရက်စီး ဆင်းမှု ရှိခဲ့ကြောင်း ဖော်ပြထားပါသည်။ အထက်တွင် ဖော်ပြသည့်အတိုင်း မသမာသူသည် အတွင်းပိုင်း ကွန်ရက်ကို မဏ္ဍိုင်အဖြစ် အသုံးချကာ ဤစက်ပစ္စည်းကို ဆိုးကျိုးသက်ရောက်အောင် သို့မဟုတ် အသုံးချခံရအောင် လုပ်ခဲ့ကြောင်း ပြသပါသည်။

စုံစမ်းစစ်ဆေးရေး အချိန်ဇယား

အောက်ပါ စာရင်းသည် စုံစမ်းစစ်ဆေးမှုအတွင်း တွေ့ရသည့် အဓိက လှုပ်ရှားမှုများ၏ အချိန်ဇယားဖြစ်ပါသည်။

အချိန်	အဖြစ်အပျက်
၂၀၂၂ ဧပြီ	မသမာသည့် IP လိပ်စာများသည် HOST7 ဆိုသည့် access gateway host နှင့် အပြန်အလှန် ဆက်သွယ်မှု ရှိခဲ့သည်။ မည်ကဲ့သို့သော အပြန်အလှန် ဆက်သွယ်မှုများ ရှိခဲ့သည်ကိုတော့ မသိရပါ။
၂၀၂၂ ဧပြီ	HOST1၊ HOST2 နှင့် HOST3 များ အားလုံးသည် မသမာသူ သို့မဟုတ် မသမာသူများ၏ တိုက်ခိုက်မှုကို ခံခဲ့ရပြီး hosts များပေါ်တွင် web shells များကို ထားရှိခဲ့ပါသည်။ HOST 2 တွင် log file တစ်ခုကို ဖန်တီး သို့မဟုတ် ပြုပြင်မှုလည်း လုပ်ခဲ့ပါသည်။ ထိုဖိုင်ထဲတွင် အကောင့်ထဲ ဝင်ရောက်နိုင်သည့် အထောက်အထား credential များပါဝင်ပြီး မသမာသူဖက်မှ ထိုအချက်အလက်များကို ရရှိရန် အလားအလာများပါသည်။ HOST1 နှင့် HOST3 အတွင်းမှ /etc/security/opasswd နှင့် /etc/shadow ဖိုင်များသည် ပြုပြင်မှုခံခဲ့ရသည်ကို ကြည့်ခြင်းအားဖြင့် password များကို ပြောင်းလဲခဲ့ကြောင်း ပြသနေပါသည်။ HOST1 ပေါ်တွင် ပြသသည့် သက်သေအထောက်အထားများအရ 'sshuser' ဆိုသည့် အသုံးပြုသူ၏ password အပြောင်းခံရကြောင်း ပြသနေပါသည်။
၂၀၂၂ ဧပြီ	အဖွဲ့အစည်းမှ HOST2 ကို ပိတ်ချမှု လုပ်ခဲ့ပါသည်။ HOST1 နှင့် HOST 3 တွင် (T1505.003) web shells ပိုများ ထပ်မံ ဖန်တီးခဲ့ပါသည်။ HOST1 သည် HOST3 ထံမှ SSH brute force လုပ်ရန် ကြိုးစားမှုကို ခံခဲ့ရပါသည်။ HOST3 တွင် (T1070) မှတ်တမ်း log file တစ်ခု ပြုပြင်မွမ်းမံမှု ခံခဲ့ရသည်။ ဖိုင်ထဲတွင် မသမာသူ ရရှိသည့် (T1078) credential အထောက်အထားများ ပါဝင်ဖို့ အလားအလာ များပါသည်။ HOST3 ၏ output file တွင် (T1528) JWTs ကို ဖမ်းယူနိုင်ခဲ့ပါသည်။ အဖွဲ့အစည်းမှ HOST3 ကို ပိတ်ချခဲ့ပါသည်။ ထိုအချိန်နောက်ပိုင်း လှုပ်ရှားမှု အားလုံးသည် HOST1 တွင် ဖြစ်ပေါ်ခဲ့သည်။
၂၀၂၂ ဧပြီ	HOST1 တွင် (T1505.003)web shells ပိုများ ထပ်မံ ဖန်တီးခဲ့ပါသည်။ HOST1 ၏ output fileတွင် JWTs ကို ဖမ်းယူနိုင်ခဲ့ပါသည်။
၂၀၂၂ ဧပြီ	HOST1 တွင် (T1505.003) web shells ပိုများ ထပ်မံဖန်တီးမှုဖြစ်ခဲ့ပြီး မသမာသည့် IP လိပ်စာများသည် (TA0011) host နှင့် ဆက်သွယ်မှု လုပ်ခဲ့သည်။ HOST7 တွင် မသမာသည့် IP လိပ်စာများက access gateway host နှင့် ဆက်သွယ်မှု လုပ်ခဲ့သည်။
၂၀၂၂ မေ	မသမာသည့် IP လိပ်စာသည် HOST7 (TA0011) ၏ access gateway host နှင့် ဆက်သွယ်မှု လုပ်ခဲ့သည်။ HOST1 ၏ logs တွင် အသုံးပြုသူ တစ်ဦး၏ အထောက်အထားစိစစ်မှု အဖြစ်အပျက်တစ်ခုသည် မသမာသည့် IP လိပ်စာတစ်ခုနှင့် ဆက်စပ်မှု ရှိခဲ့ပါသည်။ ဤ host (T1505.003) တွင် web shells ပိုများ ထပ်မံ ဖန်တီးမှု ဖြစ်ခဲ့သည်။
၂၀၂၂ မေ	HOST1 ၏ script တစ်ခုအား မသမာသူ (T1543) မှ ပြုပြင်မွမ်းမံမှု လုပ်ခဲ့သည်။ Script ထဲတွင် SQL server အတွင်းပိုင်းမှ ရရှိသည့် ဒေတာ အကျွင်းအကျန်များ ပါဝင်ပါသည်။
၂၀၂၂ မေ	HOST1 ရှိ log file အပိုတစ်ခု (T1070) ပြုပြင်မွမ်းမံခဲ့ရပါသည်။ ထိုဖိုင်ထဲတွင် အဖွဲ့အစည်း ကွန်ရက်အတွင်းမှ username နှင့် password အတွဲလိုက် ပါဝင်ပြီး စစ်မှန်သည့် အချက်အလက်များ (T1078) ဖြစ်ဖို့ များပါသည်။
၂၀၂၂ မေ	Log file အပိုတစ်ခု (T1070) ပြုပြင် မွမ်းမံခဲ့ရပါသည်။ ဖိုင်ထဲတွင် HOST1 မှ စုဆောင်းထားသည့် JWTs ပါဝင်ပါသည်။
၂၀၂၂ မေ	HOST1 တွင် (web shells T1505.003) ပိုများ ထပ်မံ ဖန်တီးမှု ဖြစ်ခဲ့သည်။ ထိုနေ့တွင် အဖွဲ့အစည်းမှ ၂၀၂၂ ဧပြီတွင် web shell တစ်ခု ဖန်တီးမှု ရှိခဲ့သည်ကို တွေ့ရသည့်အကြောင်း ASD ၏ ACSC ကို အကြောင်းကြားခဲ့ပါသည်။
၂၀၂၂ မေ	HOST1 တွင် Log4jHotPatch.jar ဟု နာမည်ရသည့် script များ တီထွင်ရေးသားခဲ့ပါသည်။
၂၀၂၂ မေ	Access gateway host တွင် open port နှစ်ခု ထည့်သွင်းရန်အတွက် iptables-saye ကွပ်ကဲမှုကို အသုံးပြုခဲ့ပါသည်။ ထို port နှစ်ခုမှာ 9998 နှင့် 9999 (T1572) တို့ ဖြစ်ကြသည်။

မဿမာသူများ၏ နည်းဗျူဟာ နှင့် နည်းပညာများ

အောက်ပါ နည်းဗျူဟာနှင့် နည်းပညာများသည် စုံစမ်းစစ်ဆေးမှုအတွင်း တွေ့ခဲ့ရသည့် အဓိက လုပ်ရပ်များ ဖြစ်ပါသည်။

ကနဦး ဝင်ရောက်ချက်

T1190 လူအများသုံးစွဲသည့် အက်ပလီကေးရှင်း၏ အားနည်းချက်ကို အလွဲသုံးစားလုပ်ခြင်း

မဿမာသည့် အုပ်စုသည် RCEI privilege escalation နှင့် authentication များကို အလွဲသုံးစားမှုလုပ်ပြီး remote access login အတွင်းရှိ အားနည်းချက်များနှင့် identity mangement အဆင့်များကို ကျော်ဖြတ်ကာ ကွန်ရက်သို့ ကနဦး ဝင်ရောက်နိုင်ရန် ကြိုးစားသည့် အလားအလာများပါသည်။

အောက်ပါ အချက်များကြောင့် ကနဦးဝင်ရောက်ခြင်း နည်းလမ်းများ ဖြစ်ပေါ်ခဲ့ဖို့ များပါသည် -

- ထိုအချိန်က ဆာဗာသည် ထို CVEs များတွင် အားနည်းချက်ရှိခဲ့ခြင်း
- မဿမာသည့် အခြေခံအဆောက်အဦးများမှ ထိုအားနည်းချက်များကို အလွဲသုံးစားလုပ်ရန် ကြိုးစားခဲ့ခြင်းများနှင့်
- အလွဲသုံးစားမှုလုပ်ရန် ကြိုးပမ်းမှုအပြီး မကြာခင်အချိန်အတွင်း မဿမာသည့် လှုပ်ရှားမှုများ ကွန်ရက်အတွင်း ဖြစ်ပေါ်ခဲ့ခြင်းတို့ ဖြစ်ပါသည်။

ဖယ်ရှားကွပ်မျက်ခြင်း

T1059.004 Command and Scripting Interpreter- Unix Shell

ထိုအဖွဲ့သည် အထက်ပါ အားနည်းချက်များကို ကောင်းမွန်စွာ အလွဲသုံးစားလုပ်ခဲ့ပြီး တိုက်ခိုက်ခံရသည့် ကိရိယာတွင် ရနိုင်သည့် Unix shell ၏ ကွပ်ကဲမှုကို ရယူနိုင်ခဲ့ပါသည်။ ကိရိယာ၏ မှတ်တမ်းများ မရှိသည့်အတွက် မဿမာသူများ အသုံးပြုခဲ့သည့် ကွပ်ကဲမှုနည်းလမ်း အသေးစိတ်ကို မသိနိုင်ခဲ့ပါ။

မဆုတ်မနစ် ကြိုးပမ်းခြင်း

T1505.003 Server Software Component: Web Shell

မဿမာသူများသည် တိုက်ခိုက်ခံရသည့် ကိရိယာအပေါ် web shells မှာ အသုံးပြုခဲ့ပါသည်။ တမျိုးစီ ထူးခြားသည့် မဿမာသူများက web shells များကို အသုံးပြုမှုများ လုပ်နိုင်သော်လည်း မဿမာသူ အနည်းငယ်မျှသာလျင် ထိုweb shells များကို အသုံးပြုကာ တိုက်ခိုက်မှုများ လုပ်ပါသည်။ တိုက်ခိုက်ခံရသည့် ကိရိယာများပေါ်ရှိ web shell များကို မဿမာသူများက မတရား အမိန့်ပေး ကွပ်ကဲမှုများ ပြုလုပ်နိုင်ပါသည်။

ရရှိသည့် ခွင့်ပြုချက်ထက် အခွင့်အရေးတိုးချဲ့ ရယူခြင်း
Privilege escalation

T1068 ရရှိသည့် ခွင့်ပြုချက်ထက် အခွင့်အရေးတိုးချဲ့ ရယူကာ အလွဲသုံးစားလုပ်ခြင်း Exploitation for Privilege Escalation

ရရှိသည့် သက်သေအထောက်အထားများက မဿမာသူများအနေဖြင့် အခွင့်ထူးခံ previlege အဆင့် မည်မျှအထိ ရရှိခဲ့သည်ကို ဖော်ပြခြင်း မရှိပါ။ သို့သော် web shell များကို အသုံးပြုသည့်အတွက် မဿမာသူများသည် တိုက်ခိုက်ခံရသည့် ကိရိယာ၏ web server တွင် ရရှိသည့် အခွင့်ထူးခံ previlege လောက်များသည့် အရည်အတွက်များကို ရရှိကြောင်း ခန့်မှန်းနိုင်ပါသည်။ တိုက်ခိုက်မှု ခံရသည့် ကိရိယာအတွင်းမှ အားနည်းချက်များသည် မဿမာသူများအား အခွင့်ထူးခံ အရင်းအမြစ် root privileges များ ရယူမှု ဖြစ်စေနိုင်ပါသည်။

လျှို့ဝှက်အချက်အလက်များ ရယူခြင်း

T1056.003 Input Capture: Web Portal Capture

တိုက်ခိုက်ခံရသည့် ကိရိယာမှ ဖော်ပြသည့် သက်သေများအရ မဿမာသူများသည် စစ်မှန်သည်ဟု ယူဆရသော username-password အစုံပေါင်း ရာနှင့်ချီကို ရယူနိုင်ခဲ့ကြောင်း ဖော်ပြထားပါသည်။ စစ်မှန်သည့် authentication စစ်မှန်သော လုပ်ငန်းစဉ်ကို ပြုပြင်မှု အချို့လုပ်ရာကနေ အထောက်အထားcredential များကို ဖိုင်တစ်ခုသို့ ပို့ဆောင်တာမျိုး ဖြစ်စေနိုင်ပါသည်။

T1111 Multi-Factor Authentication Interception

မဿမာသူသည် login အစစ်အမှန်များ ဖြစ်စေနိုင်သော MFA tokens များကို လည်း ရယူနိုင်ခဲ့ပါသည်။ စစ်မှန်သည့် authentication လုပ်ငန်းစဉ်ကို ပြုပြင်မှု အချို့လုပ်ရာကနေ ထို value များကို ဖိုင်တစ်ခုသို့ ပို့ဆောင်တာမျိုး ဖြစ်စေနိုင်ပါသည်။ MFA tokens လုံခြုံရေးအတွက် တမူထူးခြားသည့် values များကို သိုလှောင်ထားသည့် 'လျှို့ဝှက် ဆာဗာ secret server' တိုက်ခိုက်ခံရသည့် သက်သေ အထောက်အထား မတွေ့ရပါ။

T1040 Network Sniffing

မဿမာသူသည် တိုက်ခိုက်ခံရသည့် ကိရိယာပေါ်မှ HTTP စီးဆင်းမှုကို ရယူပြီး ထိုမှတဆင့် JWTs ကို ရယူခဲ့သည်ဟု ယူဆရပါသည်။ တိုက်ခိုက်ခံရသည့် ကိရိယာတွင် tcpdump ကို ဖျက်ဆီးကွပ်မျက်ခဲ့သည့် သက်သေ အထောက်အထားတွေ့ရပြီး ထိုအရာက မဿမာသူအား JWTs ကို ရယူနိုင်စေခဲ့တာ ဖြစ်နိုင်ပါသည်။

T1539 Steal Web Session Cookie

အထက်တွင် ဖော်ပြသည့်အတိုင်း မဿမာသူသည် JWTs ကို ရယူနိုင်ခဲ့ပြီး ထို အရာက web session cookies နှင့် ဆင်တူရိုးမားမှု ဖြစ်စေနိုင်ပါသည်။ မဿမာသူက ထိုအရာကို ပြန်လည်အသုံးပြုကာ နောက်ထပ် ထိုးဖောက်ဝင်ရောက်မှုများ လုပ်နိုင်ပါသည်။

အချက်အလက် ရှာဖွေရေးနည်းလမ်းများ

T1046 ကွန်ရက်ဝန်ဆောင်မှုအတွင်းမှ အချက်အလက်များကို ရှာဖွေသည့်နည်းလမ်းများ

သီးသန့် ကွန်ရက်ထဲတွင် ရှိသည့် အခြားသော ကိရိယာများကိုလည်း တိုက်ခိုက်ရန်အတွက် တိုက်ခိုက်ခံရသည့် ကိရိယာကို အသုံးပြုကာ network scanning utility nmap ကို အကောင်အထည်ဖော် လုပ်ဆောင်ခဲ့သည့် သက်သေရှိပါသည်။ မသမာသူက ထိုကဲ့သို့ ဝင်ရောက်နိုင်ခြေရှိသည့် ကွန်ရက်ဝန်ဆောင်မှုကို ရှာဖွေကာ အခွင့်သာသည်နှင့် ကွန်ရက်အတွင်း လှုပ်ရှားမှုလုပ်ရန်အတွက် အသုံးပြုရန် ဖြစ်နိုင်ပါသည်။

စုဆောင်းခြင်း

မသမာသူအနေဖြင့် တိုက်ခိုက်ခံရသည့် ကိရိယာ သို့မဟုတ် အခြားသော စနစ်မှ ရရှိသည့် အချက်အလက်ကို မည်ကဲ့သို့ စုဆောင်းခဲ့သည် သို့မဟုတ် မည်သည့် အချက်များကို စုဆောင်းခဲ့သည်ဆိုသည့် သက်သေအထောက်အထားများ မရှိပါ။ သို့သော် တိုက်ခိုက်ခံရသည့် ကိရိယာမှ ဖိုင်များအား လုံးကို မသမာသူ ရယူနိုင်ရန် အလားအလာများပြီး ထိုအထဲတွင် အထက်တွင် ဖော်ပြသည့်အတိုင်း credentials (T1003)၊ MFA token values (T1111)နှင့် JWTs တို့ ပါဝင်နိုင်ပါသည်။

ကွပ်ကဲမှုနှင့် ထိန်းချုပ်ရေး

T1071.001 Application Layer Protocol- Web Protocols

မသမာသူများသည် ကွပ်ကဲမှုနှင့် ထိန်းချုပ်ရေးအတွက် web shells ကို အသုံးပြုခဲ့ပါသည်။ Web shell ကွပ်ကဲမှုသည် ကိရိယာပေါ်မှ(T1572). လက်ရှိ ရှိနေသည့် web server ကို အသုံးပြုကာ HTTPS ကို ဖြတ်ကျော်နိုင်ပါသည်။

T1001.003 Data ကို ရှုတ်ထွေးအောင် ပြုလုပ်ခြင်း - Protocol ကို တုပခြင်း

မသမာသူသည် တိုက်ခိုက်ခံရသည့် စက်ပစ္စည်းကို တိုက်ခိုက်ရေးစတင်သည့် ကိရိယာတစ်ခုကဲ့သို့ အသုံးပြုကာ စစ်မှန်သည့် ဒေတာစီးဆင်းမှုများနှင့် ရောနှောမှုပြုလုပ်ပြီး တိုက်ခိုက်ရန် ဖြစ်ပါသည်။

ဖမ်းယူရမိခြင်းနှင့် အန္တရာယ်လျော့ချရေးဆိုင်ရာ အကြံပြုမှုများ

ASD ၏ ACSC အနေဖြင့် ဆိုင်ဘာလုံခြုံရေးဆိုင်ရာ အဖျက်အပျက်များကို လျော့ချရန်အတွက် ASD Essential Eight ထိန်းချုပ်မှုနှင့် ဆက်စပ်နည်းဗျူဟာများကို အသုံးပြုရန် ခိုင်မာစွာ တိုက်တွန်းထားပါသည်။ အောက်ပါ အကြံပြုချက်များသည် APT40 ၏ ကျူးကျော်မှုကို ဖမ်းယူရမိခြင်းနှင့် ထိုရန်မှ ကာကွယ်ရန်အတွက် ကွန်ရက်လုံခြုံရေး လုပ်ဆောင်ချက်များဖြစ်ပြီး ဇယား ၁ တွင် ဖော်ပြထားသည့် အန္တရာယ်လျော့ချရေး အဓိက TTPs လေးမျိုးနှင့် တွဲသုံးရန် ဖြစ်ပါသည်။

ဖမ်းယူရမိခြင်း

အထက်တွင် ဖော်ပြခဲ့သည် ဖိုင်တချို့၏ dropped in တည်နေရာများမှာ C:\Users\Public* and C:\Windows\Temp* စသည်တို့ ဖြစ်ပါသည်။ ထို တည်နေရာများသည် writing data အချက်အလက်အတွက် သင့်တော်သည့် နေရာဖြစ်နိုင်ပြီး အကြောင်းရင်းမှာ ၎င်းတို့သည် world writable ဖြစ်ပြီး Windows တွင် မှတ်ပုံတင်သည့် user အကောင့်မှန်သမျှ ထို directories နှင့် subdirectories များကို ဝင်ရောက်နိုင်သည့် အတွက် ဖြစ်ပါသည်။ မကြာခဏ ဆိုသလို အသုံးပြုသူ မည်သူမဆို ထိုဖိုင်များထဲ ဝင်ရောက်နိုင်သည့်အတွက် ကွန်ရက်အတွင်း ရွှေ့လွှားသွားလာမှုများ၊ လုံခြုံရေး ချိုးဖောက်မှုများ၊ အခွင့်ထူးမှု အဆင့်နိမ့်သည့်တိုင် ဝင်ရောက်နိုင်မှု low-privilege execution နှင့် အချက်အလက်များကို လျှို့ဝှက်စွာ ထုတ်ယူခြင်းများ ဖြစ်ပေါ်စေနိုင်ပါသည်။

အောက်ပါ Sigma စည်းမျဉ်းသည် သံသယဖြစ်ဖွယ် တည်နေရာမှ မမှန်ကန်သည့် လှုပ်ရှားမှုကို ညွှန်ပြသည့် အရာအဖြစ် အသုံးပြုကာ အကောင်အထည်ဖော်မှု လုပ်ပါသည်။ အခြေအနေအားလုံးတွင် မသမာသည့် လှုပ်ရှားမှုများနှင့် မည်သူ့လုပ်ဆောင်ချက်များဖြစ်ကြောင်းကို အတည်ပြုရန် အတွက် နောက်ဆက်တွဲ စုံစမ်းစစ်ဆေးမှုများ ပြုလုပ်ရန် လိုအပ်ပါသည်။

ခေါင်းစဉ် - World Writable Execution - Temp

ID: d2fa2d71-fbd0-4778-9449-e13ca7d7505c

အကြောင်းအရာ ရှင်းပြချက်- Detect process execution from C:\Windows\Temp.

နောက်ခံအကြောင်း-

ဤစည်းမျဉ်းသည် C:\Windows\Temp* ကို အထူး အကောင်အထည်ဖော်ကွပ်မျက်ရန်အတွက် ဖြစ်ပါသည်။ ပိုမို ညင်သာပျော့ပြောင်းသည့် အက်ပလီကေးရှင်းဖြင့် Temp ကို ပိုမိုကျယ်ပြန့်စွာ အသုံးပြုသောကြောင့် C:\Windows တွင် မသမာမှု ဖြစ်စေသည့် ညွှန်ပြမှုသည် အခြားသော writable subdirectoris များထက် အန္တရာယ် ပိုနည်းပါသည်။

SYSTEM သို့မဟုတ် NETWORK SERVICE users မှ အကောင်အထည်ဖော်သည့် အက်ပလီကေးရှင်းများကို ဖယ်ရှားခြင်းသည် ဤစည်းမျဉ်းအတွက် ရွေးချယ်ထားသည့် ညင်သာပျော့ပြောင်းသည့် လုပ်ရပ်အရေအတွက်ကို သိသိသာသာ လျော့ကျစေနိုင်ပါသည်။

ဆိုလိုသည်မှာ ဤစည်းမျဉ်းသည် ပိုမြင့်သည့် အခွင့်ထူးခံအဆင့် privilege level တွင် မသမာမှုများကို ကွပ်မျက်ရန် မသိလိုက်တာမျိုး ဖြစ်နိုင်သော်လည်း အခြားစည်းမျဉ်းများကို အသုံးပြုရန် အကြံပြုလိုပြီး အကြောင်းရင်းမှာ အသုံးပြုသူ အနေဖြင့် SYSTEM ထဲ ဝင်နိုင်ရင် အခွင့်ထူးခံမှု previleges ကို တိုးမြင့်ခြင်း ဟုတ်မဟုတ် သိနိုင်ရန်အတွက် ဖြစ်ပါသည်။

စုံစမ်းစစ်ဆေးချက်

1. ဤဖိုင်ကွပ်မျက်ခြင်းနှင့် ဆက်စပ်သည့် အချက်အလက်များကို သေချာလေ့လာပါ- ဥပမာ မည်သည့် userက file ကို သုံးနေသနည်း၊ မည်သည့် အကောင်အထည်ဖော်မှုက မှန်ကန်မှုအဆင့်ရှိသနည်း၊ နောက်ဆက်တွဲ လုပ်ဆောင်မှုနှင့် ဖိုင်မှတင်ထားသည့် ပုံများစသည့် အရာများသည် ဖယ်ရှားကွပ်မျက်ခံရသည့်ဖိုင်နှင့် တိုက်ရိုက် ဆက်စပ်မှုရှိမရှိ ဆန်းစစ်ပါ။
2. လှုပ်ရှားမှုသည် စစ်မှန်ခြင်းရှိမရှိကို အကဲဖြတ်သည့်အခါ အထောက်အကူပြုရန်အတွက် host ပေါ်ရှိ လည်ပတ်ခြင်းဆိုင်ရာ ဆက်စပ်လုပ်ငန်းစဉ်များ၊ ကွန်ရက်များ၊ ဖိုင်နှင့် အခြားသော ပံ့ပိုးမှု ဒေတာများကို စုံစမ်းစစ်ဆေးပါ။
3. လိုအပ်ပါက ဖိုင်ကို မိတ္တူယူပြီး တရားဝင်လုပ်ရပ် ဟုတ်မဟုတ် သိနိုင်ရန် သေခြာဆန်းစစ်မှုလုပ်သည့် reverse engineering နည်းကို အသုံးပြုပါ။

ကျမ်းကိုးများ

https://www.elastic.co/guide/en/security/current/process-execution-from-an-unusual-directory.html

ရေးသားသူ - ASD ၏ ACSC

ရက်စွဲ - 2024/06/19

လက်ရှိအနေအထား - စမ်းသပ်ရေး

Tags:

- tlp.green
- classification.au.official
- attack.execution

Log Source:

category: process_creation

product: windows

ဖမ်းယူမိခြင်း-

temp:

Image|startswith: 'C:\\Windows\\Temp\\'

common_temp_path:

Image|re|ignorecase: 'C:\\Windows\\Temp\\\{[a-fA-F0-9]{8}-([a-fA-F0-9]{4}-){3}[a-fA-F0-9]{12}\}\\'

system_user:

အသုံးပြုသူ -

- စနစ်
- ကွန်ရက် ဝန်ဆောင်မှု

dismhost:

Image|endswith: 'dismhost.exe'

known_parent:

ParentImage|endswith:

- '\\esif_uf.exe'
- '\\vmtoolsd.exe'
- '\\cwainstaller.exe'
- '\\trolleyexpress.exe'

condition: temp and not (common_temp_path or system_user or dismhost or known_parent)

False positives:

- ခွင့်ပြုစာရင်းကို စစ်ဆေးသည့် အက်ပလီကေးရှင်းသည် Temp မှတဆင့် executables များ လုပ်ဆောင်သည်ကို တွေ့ခဲ့ရပါသည်။
- Temp တွင် စစ်မှန်သော setup applications အမျိုးမျိုးနှင့် launchers များ ပါဝင်ပါသည်၊ ထို့ကြောင့် ဤစည်းမျဉ်းကို အသုံးမပြုခင် စောင့်ကြည့်သည့် ကွန်ရက်တွင် (ခွင့်ပြုစာရင်းကို ၎င်းအနေဖြင့် ထားရှိနိုင်ခြင်း ရှိမရှိ) ၎င်း၏ အပြုအမူမည်သို့ရှိမည်ကို စောင့်ကြည့်လေ့လာရန် သင့်တော်မှုဖြစ်စေပါသည်။

အဆင့် - နိမ့်

ခေါင်းစဉ် World Writable Execution - Non-Temp System Subdirectory

ID - 5b187157-e892-4fc9-84fc-aa48aff9f997

အကြောင်းအရာ ရှင်းပြချက်- subdirectory တစ်ခုအတွင်းမှ world writable တည်နေရာတွင် လုပ်ငန်းစဉ်များကို **ဖမ်းယူကာ ကွပ်မျက်ခြင်း**

နောက်ခံအကြောင်း

ဤစည်းမျဉ်းသည် C:\Windows\Temp (ညှင်သာပျော့ပျောင်းသည့် အက်ပလီကေးရှင်းများကို ပိုမိုကျယ်ပြန့်စွာ အသုံးပြုသည့်အတွက် မသမာတိုက်ခိုက်မှု ခံရနိုင်ခြေပိုနည်း) မှလွဲ၍ C:\ နှင့် အထူးသဖြင့် C:\Windows* အတွင်းရှိ world writable directories များကို ကွပ်မျက်ရန်အတွက် အထူးလုပ်ဆောင်ထားပါသည်။

အကယ်၍ SYSTEM ကို ဖိုင်တစ်ခုကဲ့သို့ လည်ပတ်စေလျင် AppData folder ကို ဖယ်ရှားထားသည် - ဤကဲ့သို့လုပ်ဆောင်မှုသည် ယာယီ အက်ပလီကေးရှင်း ဖိုင်များကို ဖယ်ရှားကွပ်မျက်ရန်အတွက် အသုံးပြုသည့် ညှင်သာပျော့ပျောင်းသော နည်းလမ်း ဖြစ်ပါသည်။

ကနဦးကွန်ရက်အခြေခံလိုင်းကို ပြီးမြောက်စွာဆောင်ရွက်ခြင်းနှင့် ထိုတည်နေရာမှ ညှင်သာပျော့ပြောင်းသည့် ကွပ်မျက်မှုများကို သိရသည့်အခါ ထိုစည်းမျဉ်းသည် ရှားပါးသည့် လုပ်ဆောင်ချက် ဖြစ်ပါသည်။

စုံစမ်းစစ်ဆေးချက်

1. ဤဖိုင်ကွပ်မျက်ခြင်းနှင့် ဆက်စပ်သည့် အချက်အလက်များကို သေခြာလေ့လာပါ- ဥပမာ မည်သည် user က file ကို သုံးနေသနည်း၊ မည်သည့် ဖယ်ရှားကွပ်မျက်ခြင်း မှန်ကန်မှုအဆင့်ရှိသနည်း၊ နောက်ဆက်တွဲ လုပ်ဆောင်မှုနှင့် ဖိုင်မှတင်ထားသည့် ပုံများစသည့်အရာများသည် ဖယ်ရှားကွပ်မျက်ခံရသည့်ဖိုင်နှင့် တိုက်ရိုက်ဆက်စပ်မှုရှိမရှိ ဆန်းစစ်ပါ။
2. လှုပ်ရှားမှုသည် စစ်မှန်ခြင်းရှိမရှိကို အကဲဖြတ်သည့်အခါ အထောက်အကူပြုရန်အတွက် host ပေါ်ရှိ လည်ပတ်ခြင်းဆိုင်ရာ ဆက်စပ်လုပ်ငန်းစဉ်များ၊ ကွန်ရက်များ၊ ဖိုင်နှင့် အခြားသော ပုံပိုးမှုဒေတာများကို စုံစမ်းစစ်ဆေးပါ။
3. လိုအပ်ပါက ဖိုင်ကို မိတ္တူယူပြီး တရားဝင်လုပ်ရပ် ဟုတ်မဟုတ် သိနိုင်ရန် သေချာဆန်းစစ်မှုလုပ်သည့် reverse engineering နည်းကို အသုံးပြုပါ။

ကျမ်းကိုးများ-

https://gist.github.com/mattifestation/5f9de750470c9e0e1f9c9c33f0ec3e56

https://www.elastic.co/guide/en/security/current/process-execution-from-an-unusual-directory.html

ရေးသားသူ - ASD ၏ ACSC

ရက်စွဲ 2024/06/19

လက်ရှိအနေအထား စမ်းသပ်ရေး

Tags:

- tlp.green
- classification.au.official
- attack.execution

Log source:

category: process_creation

ကုန်ပစ္စည်း - windows

ဖမ်းယူမိခြင်း -

writable_path:

ပုံ/ ပါဝင်မှု -

- ':\\$Recycle.Bin\\'
- ':\\AMD\\Temp\\'
- ':\\Intel\\'
- ':\\PerfLogs\\'
- ':\\Windows\\addins\\'
- ':\\Windows\\appcompat\\'
- ':\\Windows\\apppatch\\'
- ':\\Windows\\AppReadiness\\'
- ':\\Windows\\bcastdvr\\'
- ':\\Windows\\Boot\\'
- ':\\Windows\\Branding\\'
- ':\\Windows\\CbsTemp\\'
- ':\\Windows\\Containers\\'
- ':\\Windows\\csc\\'
- ':\\Windows\\Cursors\\'
- ':\\Windows\\debug\\'
- ':\\Windows\\diagnostics\\'
- ':\\Windows\\DigitalLocker\\'
- ':\\Windows\\dot3svc\\'
- ':\\Windows\\en-US\\'
- ':\\Windows\\Fonts\\'
- ':\\Windows\\Globalization\\'
- ':\\Windows\\Help\\'
- ':\\Windows\\IdentityCRL\\'
- ':\\Windows\\IME\\'
- ':\\Windows\\ImmersiveControlPanel\\'
- ':\\Windows\\INF\\'
- ':\\Windows\\intel\\'
- ':\\Windows\\L2Schemas\\'

- ':\\Windows\\LiveKernelReports\\'
- ':\\Windows\\Logs\\'
- ':\\Windows\\media\\'
- ':\\Windows\\Migration\\'
- ':\\Windows\\ModemLogs\\'
- ':\\Windows\\ms\\'
- ':\\Windows\\OCR\\'
- ':\\Windows\\panther\\'
- ':\\Windows\\Performance\\'
- ':\\Windows\\PLA\\'
- ':\\Windows\\PolicyDefinitions\\'
- ':\\Windows\\Prefetch\\'
- ':\\Windows\\PrintDialog\\'
- ':\\Windows\\Provisioning\\'
- ':\\Windows\\Registration\\CRMLog\\'
- ':\\Windows\\RemotePackages\\'
- ':\\Windows\\rescache\\'
- ':\\Windows\\Resources\\'
- ':\\Windows\\SchCache\\'
- ':\\Windows\\schemas\\'
- ':\\Windows\\security\\'
- ':\\Windows\\ServiceState\\'
- ':\\Windows\\servicing\\'
- ':\\Windows\\Setup\\'
- ':\\Windows\\ShellComponents\\'
- ':\\Windows\\ShellExperiences\\'
- ':\\Windows\\SKB\\'
- ':\\Windows\\TAPI\\'
- ':\\Windows\\Tasks\\'
- ':\\Windows\\TextInput\\'
- ':\\Windows\\tracing\\'
- ':\\Windows\\Vss\\'
- ':\\Windows\\WaaS\\'
- ':\\Windows\\Web\\'
- ':\\Windows\\wlansvc\\'
- ':\\Windows\\System32\\Com\\dmp\\'
- ':\\Windows\\System32\\FxsTmp\\'
- ':\\Windows\\System32\\Microsoft\\Crypto\\RSA\\MachineKeys\\'
- ':\\Windows\\System32\\Speech\\'
- ':\\Windows\\System32\\spool\\drivers\\color\\'
- ':\\Windows\\System32\\spool\\PRINTERS\\'
- ':\\Windows\\System32\\spool\\SERVERS\\'
- ':\\Windows\\System32\\Tasks_Migrated\\Microsoft\\Windows\\PLA\\System\\'
- ':\\Windows\\System32\\Tasks\\'
- ':\\Windows\\SysWOW64\\Com\\dmp\\'
- ':\\Windows\\SysWOW64\\FxsTmp\\'
- ':\\Windows\\SysWOW64\\Tasks\\'

appdata -

Image|contains: '\\AppData\\'

အသုံးပြုသူ - 'စနစ်'

condition: writable_path and not appdata

False positives:

စစ်ဆေးရေး အက်ပလီကေးရှင်းစာရင်းကို directories များကို ထိုလမ်းညွှန်များတွင် လုပ်ဆောင်ခဲ့ကြောင်း တွေ့ရှိရသည်။

စောင့်ကြည့်ရေးဝန်းကျင်/များတွင် အသုံးပြုသည့် scripts နှင့် administrative tools များသည် ထိုလမ်းညွှန်များတွင် တည်ရှိနိုင်ပြီး တစ်ခုခြင်းစီအလိုက် အနေအထားတွင် ဖော်ထုတ်သင့်ပါသည်။

အဆင့်- မြင့်

ခေါင်းစဉ် - World Writable Execution - အသုံးပြုသူများ

ID - 6dda3843-182a-4214-9263-925a80b4c634

အကြောင်းအရာ ရှင်းပြချက်- C:\Users\Public* နှင့် Users **အတွင်းရှိ အခြားသော** world writable folders **များ၏ လုပ်ဆောင်မှုနည်းလမ်းကို လေ့လာထောက်လှမ်းပါ။**

နောက်ခံအကြောင်း-

အကယ်၍ SYSTEM ကို ဖိုင်တစ်ခုကဲ့သို့ လည်ပတ်စေလျှင် AppDate folder ကို ဖယ်ရှားထားသည် - ဤကဲ့သို့လုပ်ဆောင်မှုသည် ယာယီ အက်ပလီကေးရှင်း ဖိုင်များကို ဖယ်ရှားကွပ်မျက်ရန်အတွက် အသုံးပြုသည့် ညင်သာပျော့ပျောင်းသော နည်းလမ်း ဖြစ်ပါသည်။

စုံစမ်းစစ်ဆေးချက် -

1. ဤဖိုင်ကွပ်မျက်ခြင်းနှင့် ဆက်စပ်သည့် အချက်အလက်များကို သေချာလေ့လာပါ- ဥပမာ မည်သည် userက file ကို သုံးနေသနည်း၊ မည်သည့် ဖယ်ရှားကွပ်မျက်ခြင်း မှန်ကန်မှုအဆင့်ရှိသနည်း၊ နောက်ဆက်တွဲ လုပ်ဆောင်မှုနှင့် ဖိုင်မှတင်ထားသည့် ပုံများစသည့် အရာများသည် ဖယ်ရှားကွပ်မျက်ခံရသည့်ဖိုင်နှင့် တိုက်ရိုက် ဆက်စပ်မှုရှိမရှိ ဆန်းစစ်ပါ။
2. လှုပ်ရှားမှုသည် စစ်မှန်ခြင်းရှိမရှိကို အကဲဖြတ်သည့်အခါ အထောက်အကူပြုရန်အတွက် host ပေါ်ရှိ လည်ပတ်ခြင်းဆိုင်ရာ ဆက်စပ်လုပ်ငန်းစဉ်များ၊ ကွန်ရက်များ၊ ဖိုင်နှင့် အခြားသော ပံ့ပိုးမှုဒေတာများကို စုံစမ်းစစ်ဆေးပါ။
3. လိုအပ်ပါက ဖိုင်ကို မိတ္တူယူပြီး တရားဝင်လုပ်ရပ် ဟုတ်မဟုတ် သိနိုင်ရန် သေခြာဆန်းစစ်မှုလုပ်သည့် reverse engineering နည်းကို အသုံးပြုပါ။

ကျမ်းကိုးများ-

https://www.elastic.co/guide/en/security/current/process-execution-from-an-unusual-directory.html

စာရေးသူ - ASD ၏ ACSC

ရက်စွဲ- 2024/06/19

လက်ရှိအနေအထား- စမ်းသပ်ရေး

Tags:

- tlp.green
- classification.au.official
- attack.execution

Log source:

category: process_creation

product: windows

ဖမ်းယူမိခြင်း -

အသုံးပြုသူများ -

Image|contains:

- ':\\Users\\All Users\\'
- ':\\Users\\Contacts\\'
- ':\\Users\\Default\\'
- ':\\Users\\Public\\'
- ':\\Users\\Searches\\'

appdata:

Image|contains: '\\AppData\\'

အသုံးပြုသူ - 'စနစ်'

အခြေအနေ - users and not appdata

False positives -

- စောင့်ကြည့်ရေးဝန်းကျင်/များတွင် အသုံးပြုသည့် scripts နှင့် administrative tools များသည် အများဝင်ရောက်နိုင်သည့် လမ်းညွှန် သို့မဟုတ် လမ်းညွှန်ခွဲများတွင် တည်ရှိနိုင်ပြီး တစ်ခုခြင်းစီအလိုက် အနေအထားတွင် ဖော်ထုတ်သင့်ပါသည်။

အဆင့်- အတန်အတင့်

အန္တရာယ် လျော့ချခြင်း

Logging စာရင်းမှတ်တမ်းတင်ခြင်း

ASD၏ ACSC စုံစမ်းစစ်ဆေးမှုအတွင်း ထိရောက်မှု လျော့နည်းခြင်းနှင့် စုံစမ်းစစ်ဆေးမှု မြန်ဆန်မှုကို အနှောင့်အယှက်ဖြစ်စေသည့်အချက်မှာ ပြည့်စုံလုံလောက်သည့် မှတ်တမ်းများနှင့် logging စာရင်းမှတ်တမ်း၏ သမိုင်းအချက်အလက်များ ကဏ္ဍစုံတွင် နည်းပါးခြင်းကြောင့် ဖြစ်ရပြီး ထိုအထဲတွင် web server မှတ်တမ်းများ၊ Windows event မှတ်တမ်းများနှင့် internet proxy မှတ်တမ်းတို့ ပါဝင်ပါသည်။

ASD ၏ ACSC အနေဖြင့် Windows Event Logging နှင့် Forwarding ဆိုင်ရာ လမ်းညွှန်ချက်များကို ပြန်လည်ဆန်းစစ်ပြီး အကောင်အထည်ဖော်ရန် အကြံပြုလိုပါသည်။ ထိုအထဲတွင် Windows Event Logging Repository နှင့် အချက်အလက် လုံခြုံရေးဆိုင်ရာ လက်စွဲစာအုပ်၏ စနစ်ကို စောင့်ကြည့်ရေးဆိုင်ရာ လမ်းညွှန်ချက် များ၏ ဖိုင်နှင့် scripts များ၏ ဖွဲ့စည်းမှုတို့ ပါဝင်ပြီး သင့်တော်သည့်ကာလအတွက် ဗဟိုမှတ်တမ်းများနှင့် ထိန်းသိမ်းရေးမှတ်တမ်းများကိုပါ ထည့်သွင်းသင့်ပါသည်။

ဖာထေးပြုပြင်မွမ်းမံခြင်းဆိုင်ရာ စီမံခန့်ခွဲမှု

အင်တာနက်နှင့် ချိတ်ဆက်ထားသည့် စက်ပစ္စည်းနှင့် ဝန်ဆောင်မှုများကို ချက်ခြင်း ဖာထေးပြုပြင်မွမ်းမံမှုများလုပ်ပါ၊ ထိုအထဲတွင် web servers၊ web applications နှင့် အဝေးမှ ဝင်ရောက်ခွင့် လမ်းကြောင်းများ ပါဝင်ပါသည်။ ဖာထေးပြုပြင်မွမ်းမံမှုများကို အလိုအလျောက်လုပ်နိုင်ရန်နှင့် လျင်မြန်စွာ လုပ်ကိုင်ရန်အတွက် ဖာထေးပြုပြင်မွမ်းမံခြင်းဆိုင်ရာ ဗဟို စီမံခန့်ခွဲရေးစနစ်ကို အသုံးပြုရန် ထည့်သွင်းစဉ်းစားပါ။ ASD ၏ ACSC သည် စနစ်စီမံခန့်ခွဲရေး System Management အတွက် ISM ၏ လမ်းညွှန်ချက်ကို အကောင်အထည်ဖော်ရန် တိုက်တွန်းထားပြီး အထူးသဖြင့် ဖြစ်နိုင်သည့်အခါ စနစ်ကို ဖာထေးပြုပြင်မွမ်းမံနိုင်သည့် ထိန်းချုပ်မှုအတွက် လုပ်သင့်ပါသည်။

မသမာသူများ တိုက်ခိုက်သည့် စက်ပစ္စည်းများတွင် လူသိကြသည့် အရာများဖြစ်ပြီး ဖာထေးပြုပြင်မွမ်းမံမှုများနှင့် အန္တရာယ်လျော့ချရေးများ ရှိခဲ့သည့် စက်ပစ္စည်းများ ဖြစ်ပါသည်။ အဖွဲ့အစည်းများအနေဖြင့် အင်တာနက်နှင့် ချိတ်ဆက်ထားသည့် အခြေခံအဆောက်အအုံများအတွက် ၄၈ နာရီအတွင်း လုံခြုံရေးဆိုင်ရာ ဖာထေးပြုပြင်မွမ်းမံမှုနှင့် အန္တရာယ်လျော့ချရေးအတွက် အကောင်အထည်ဖော် လုပ်ဆောင်သည့်နည်းလမ်းကို အသုံးပြုသင့်ပြီး ဖြစ်နိုင်ပါက နောက်ဆုံးပေါ် ဆော့ဖ်ဝဲနှင့် လည်ပတ်ခြင်းဆိုင်ရာ စနစ်များကို အသုံးပြုပါ။

ကွန်ရက်များကို သီးသန့်စီခွဲခြားထားခြင်း

ကွန်ရက်များကို သီးသန့်စီခွဲခြားထားခြင်းအားဖြင့် တိုက်ခိုက်လိုသူများအား အဖွဲ့အစည်းပိုင်ဆိုင်သည့် ထိလွယ်ရှလွယ်သော အချက်အလက်များရှိသည့် နေရာကို ဝင်ရောက်ပြီး ထိုအချက်အလက်များ ရယူရန် ပို၍ ခက်ခဲစေနိုင်ပါသည်။ ကွန်ရက်များကို သီးသန့်စွဲခွဲခြားထားခြင်းသည် ဘေးတိုက်ရွှေ့လျားမှုကို ကန့်သတ်ခြင်း သို့မဟုတ် ပိတ်ပင်ထားသည့်အတွက် ကွန်ပြူတာများအကြား အချက်အလက်စီးဆင်းမှုကို တားမြစ်ထားခြင်းဖြစ်ပြီး လိုအပ်မှသာလျှင် ဖွင့်ပေးခြင်းမျိုးကို လုပ်နိုင်ပါသည်။ အရေးကြီးသည့် Active Directory နှင့် အခြားသော authentication servers ကဲ့သို့ အရေးကြီးသည့် server များအတွက် အကန့်အသတ်ရှိသည့် ကြားခံဆာဗာများ သို့မဟုတ် 'jump servers' များမှတဆင့်သာ ထိန်းချုပ်ခွင့် ရှိသင့်ပါသည်။ ထိုဆာဗာများကို အနီးကပ် စောင့်ကြည့်မှုလုပ်သင့်ပြီး ကောင်းမွန်သည့် လုံခြုံရေး ချမှတ်ကာ ဝင်ရောက်ခွင့်ရသူကို ကန့်သတ်သကဲ့သို့ ၎င်းတို့နှင့် ချိတ်ဆက်နိုင်သည့် စက်ပစ္စည်းများကိုလည်း ကန့်သတ်မှု လုပ်သင့်ပါသည်။

စနစ်များအကြား ရွှေ့လျားမှုလုပ်ခြင်းကို ပိတ်ပင်ထားသည့်တိုင် ကွန်ရက်ကို သီးသန့်စွဲခွဲထားခြင်းများ ထပ်လုပ်ထားပါက တိုက်ခိုက်ခံရသည့်အခါတွင် မသမာသူများအား ဒေတာအချက်အလက်များကို အကန့်အသတ်ဖြင့်သာ ရရှိမှု ဖြစ်စေနိုင်ပါသည်။

ပိုသာသည့် နည်းလမ်းဖြင့် အန္တရာယ် လျော့ချခြင်း

အာဏာပိုင်အေဂျင်စီများသည် APT40 နှင့် TTPs အသုံးပြုသည့် အခြားသော တိုက်ခိုက်မှု အန္တရာယ်ကို လျော့ချရန်အတွက် အောက်ပါနည်းလမ်းများကို အသုံးပြုရန် တိုက်တွန်းထားပါသည်။

- အသုံးမပြုတော့သည့် သို့မဟုတ် မလိုအပ်တော့သည့် ကွန်ရက် ဝန်ဆောင်မှုများ၊ ports များနှင့် protocols များကို အသုံးမပြုနိုင်တော့အောင် လုပ်ဆောင်ပါ။
- Web serves များနှင့် အက်ပလီကေးရှင်းများကို ကာကွယ်ရန်အတွက် ကောင်းမွန်သည့် Web application firewalls (WAFs) များကို အသုံးပြုပါ။
- ဆာဗာများ၊ ဖိုင်မျှဝေခြင်းများနှင့် အခြားသော အရင်းအမြစ်များထဲ ဝင်ရောက်မှုကို အနည်းဆုံးလိုအပ်သည့် အခွင့်ထူးအဆင့်ပြည့်မီမှ ဝင်ရောက်နိုင်သည့် နည်းလမ်းကို ကျင့်သုံးပါ။
- အချက်အလက်မျိုးစုံဖြင့် အတည်ပြုခြင်း (MFA) ကိုအသုံးပြုခြင်းနှင့် မည်သူမည်ဝါဖြစ်ကြောင်း သက်သေပြရသည့် credentials အချက်အလက်များကို ခိုးယူမှု သို့မဟုတ် ပြန်လည်အသုံးပြုမှုလုပ်ဖို့ ခက်ခဲရန်အတွက် ဝန်ဆောင်မှုအကောင့်များကို စီမံခန့်ခွဲမှု လုပ်ပါ။ အဝေးမှ အင်တာနက်ဖြင့် ချိတ်ဆက်ကာ ဝင်ရောက်နိုင်သည့် အရာများအားလုံးအတွက် MFA နည်းကို အသုံးပြုသင့်ပြီး ထိုအထဲတွင် -
  - Web နှင့် cloud-based email များ
  - Collaboration platforms များ
  - Virtual private network connections များ
  - အဝေးထိန်း desktop ဝန်ဆောင်မှုများနှင့်
- သက်တမ်းကုန်သည့် စက်ပစ္စည်းများကို အစားထိုးခြင်းတို့ ပါဝင်ပါသည်။

ဇယား ၁ - အန္တရာယ် လျှော့ချရေး နည်းဗျူဟာ/ နည်းပညာများ

TTP	Essential Eight Mitigation Strategies	ISM Controls
ကနဦး ဝင်ရောက်ချက် T1190 ဖာထေးပြုပြင်ထားသည့် အက်ပလီကေးရှင်းများ	ဖာထေးပြုပြင်ထားသည့် လည်ပတ်ရေးစနစ်များ ပြုပြင်မွမ်းမံထားသည့် အချက်အလက် မျိုးစုံဖြင့် အတည်ပြုခြင်း Multi-Factor Authentication အက်ပလီကေးရှင်းကို ထိန်းချုပ်ခြင်း	ISM-0140 ISM-1698 ISM-1701 ISM-1921 ISM-1876 ISM-1877 ISM-1905
ကွပ်မျက်ခြင်း T1059 Command and Scripting Interpreter	အက်ပလီကေးရှင်းကို ထိန်းချုပ်ခြင်း Restrict Microsoft Office macros အဆင့်မြင့် ခွင့်ပြုချက်များကို ကန့်သတ်ခြင်း	ISM-0140 ISM-1490 ISM-1622 ISM-1623 ISM-1657 ISM-1890
မဆုတ်မနစ် လုပ်ဆောင်ခြင်း T1505.003 Server Software Component: Web Shell	အက်ပလီကေးရှင်းကို ထိန်းချုပ်ခြင်း အဆင့်မြင့် ခွင့်ပြုချက်များကို ကန့်သတ်ခြင်း	ISM-0140 ISM-1246 ISM-1746 ISM-1249 ISM-1250 ISM-1490 ISM-1657 ISM-1871
ကနဦးဝင်ရောက်ချက်/ ရှိသည့် ခွင့်ပြုချက်ထက် အခွင့်အရေးတိုးချဲ့ ရယူခြင်း/ မဆုတ်မနစ် လုပ်ဆောင်ခြင်း T1078 စစ်မှန်သော အကောင့်များ -	ဖာထေးပြုပြင်ထားသည့် လည်ပတ်ရေးစနစ်များ အချက်အလက် မျိုးစုံဖြင့် အတည်ပြုခြင်း Multi-Factor Authentication အဆင့်မြင့် ခွင့်ပြုချက်များကို ကန့်သတ်ခြင်း အက်ပလီကေးရှင်းကို ထိန်းချုပ်ခြင်း အသုံးပြုသူ၏ အက်ပလီကေးရှင်းကို လုံခြုံစွာ ပြုလုပ်ခြင်း	ISM-0140 ISM-0859 ISM-1546 ISM-1504 ISM-1679

ဖမ်းယူမိခြင်းနှင့် အန္တရာယ်လျှော့ချခြင်းဆိုင်ရာ အထွေထွေအချက်အလက်များအတွက် အန္တရာယ် လျှော့ချရေးနှင့် ဖမ်းယူခြင်း ဆိုသည့် MITRE ATT&CK ၏ နည်းလမ်းဆိုင်ရာ ဝဘ်စာမျက်နှာသို့ သွားရောက်ကာ ဤအကြံပြုချက်အဆုံးတွင် ဖော်ပြထားသည့် MITRE ATT&CK အကျဉ်းချုံးတွင် နည်းလမ်းတစ်ခုခြင်းစီအတွက် ရှင်းပြချက်ကို လေ့လာနိုင်ပါသည်။

မသက်ဆိုင်ကြောင်း ရှင်းလင်းချက်

ဤအစီရင်ခံစာပါ အချက်အလက်များသည် "ဤကဲ့သို့" အချက်အလက်အသိပေးခြင်းရည်ရွယ်ချက်အနေဖြင့်သာ ဖော်ပြထားခြင်း ဖြစ်ပါသည်။ အာဏာပိုင်အေဂျင်စီများသည် ဤစာစောင်တွေ့ ပါဝင်သည့် မည်သည့်အဖွဲ့၊ မည်သည့်ထုတ်ကုန်လုပ်ငန်း၊ မည်သည့်ဝန်ဆောင်မှုကိုမှ အားပေးထောက်ခံမှု မလုပ်ထားပါ။ ကုမ္ပဏီ၏ နာမည် သို့မဟုတ် ပစ္စည်းတစ်ခု၏ နာမည်၊ သို့မဟုတ် လုပ်ငန်းစဉ် သို့မဟုတ် ဝန်ဆောင်မှု၊ ကုန်အမှတ်တံဆိပ်၏ နာမည်၊ ကုန်ထုတ်လုပ်သူ၏ နာမည်နှင့် အခြား နာမည်များကို ဖော်ပြခဲ့သည်ရှိသော် ၎င်းတို့ကို အာဏာပိုင်အေဂျင်စီများမှ ထောက်ခံချက်ပေးခြင်း၊ သုံးစွဲရန် အကြံပြုခြင်း သို့မဟုတ် မျက်နှာသာပေးခြင်း မဟုတ်ကြောင်း အသိပေးလိုပါသည်။

ဤစာစောင်သည် TLP:CLEAR စာစောင်ဖြစ်ကြောင်း သတ်မှတ်ထားပါသည်။ အကန့်အသတ်မဲ့ ထုတ်ဝေထားပါသည်။ ကိုးကားသူများအနေဖြင့် အများပြည်သူအတွက် ထုတ်ဝေချက်တွင် သတ်မှတ်ထားသည့် စည်းမျဉ်းနှင့် လုပ်ထုံးလုပ်နည်းများအတိုင်း အချက်အလက်များအား အနည်းငယ်မျှသာ သို့မဟုတ် တလွဲအသုံးပြုမှုများ မလုပ်ပဲ သုံးမည်ဆိုပါက အချက်အလက် အရင်းအမြစ်အဖြစ် TLP:CLEAR ကို ကိုးကား ဖော်ပြနိုင်ပါသည်။ မူပိုင်ခွင့်၏ စံချိန်စံညွှန်းများအတိုင်း လုပ်ဆောင်နိုင်ပြီး TLP:CLEAR အချက်အလက်များအား အကန့်အသတ်မဲ့ ဖြန့်ဝေနိုင်ပါသည်။ မည်သည့်စာစောင်မျိုးကို မည်မျှအထိ မျှဝေသုံးစွဲသင့်သည်ဟု သတ်မှတ်ပေးထားသော Traffic Light Protocol အကြောင်း ပိုသိလိုပါက cisa.gov/tlp တွင် ဝင်ရောက်ကြည့်ရှုနိုင်ပါသည်။

MITRE ATT&CK – Historical APT40 tradecraft of interest

စူးစမ်းထောက်လှမ်းမှု (TA0043)	
တိုက်ခိုက်ခံရသူများ ပိုင်ဆိုင်သည့် ဝဘ်ဆိုက်များကို ရှာရန် (T1594)	တိုက်ခိုက်ခံရသူ၏ အချက်အလက်ကို စုဆောင်းခြင်း- အထောက်အထားများ Credentials (T1589.001)
Active Scanning: Vulnerability Scanning (T1595.002)	တိုက်ခိုက်ခံရသူ၏ Host ကို စုဆောင်းခြင်း (T1592)
Open Websites/ Domains များ ရှာဖွေပါ - Search Engines (T1593.002)	တိုက်ခိုက်ခံရသူ၏ ကွန်ရက်အချက်အလက်ကို စုဆောင်းခြင်း- Domain Properties (T1590.001)
တိုက်ခိုက်ခံရသူ၏ အချက်အလက်ကို စုဆောင်းခြင်း- အီးမေးလ်လိပ်စာများ (T1589.002)	

အရင်းအမြစ် ဖွံ့ဖြိုးတိုးတက်ရေး (TA0042)	
လိုအပ်သည့် အခြေခံ အဆောက်အအုံ - ဒိုမိန်းများ (T1583.001)	လိုအပ်သည့် အခြေခံ အဆောက်အအုံ (T1583)
လိုအပ်သည့် အခြေခံ အဆောက်အအုံ- DNS Server (T1583.002)	တိုက်ခိုက်ခံရသည့် အကောင့်များ (T1586)
ဖွံ့ဖြိုးမှု စွမ်းရည်များ - Code Signing Certificates (T1587.002)	တိုက်ခိုက်ခံရသည့် အခြေခံ အဆောက်အအုံများ (T1584)
ဖွံ့ဖြိုးမှု စွမ်းရည်များ - Digital Certificates (T1587.003)	ဖွံ့ဖြိုးမှု စွမ်းရည်များ - မသမာသည့် Malware (T1587.001)
ရယူနိုင်သည့် စွမ်းရည်များ - Code Signing Certificates (T1588.003)	အတည်တကျရှိသည့် အကောင့်များ - Cloud Accounts (T1585.003)
တိုက်ခိုက်ခံရသည့် အခြေခံ အဆောက်အအုံ - ကွန်ရက် စက်ပစ္စည်းများ (T1584.008)	ရယူနိုင်သည့် စွမ်းရည်များ - Digital Certificates (T1588.004)

ကနဦး ဝင်ရောက်ချက် (TA0001)	
စစ်မှန်သော အကောင့်များ (T1078)	အတုအယောင်လုပ်ကာ ခိုးယူခြင်း (T1566)
စစ်မှန်သော အကောင့်များ - အလိုအလျောက်ပါလာသည့် အကောင့်များ (T1078.001)	အတုအယောင်လုပ်ကာ ခိုးယူခြင်း - Spearphishing Attachment (T1566.001)
စစ်မှန်သော အကောင့်များ - ဒိုမိန်း အကောင့်များ (T1078.002)	အတုအယောင်လုပ်ကာ ခိုးယူခြင်း - Spearphishing Link (T1566.002)
ပြင်ပမှ အဝေးထိန်း ဝန်ဆောင်မှု (T1133)	Exploit Public-Facing Application (T1190)
Drive-by Compromise (T1189)	

ကွပ်မျက်ခြင်း (TA0002)	
Windows Management Instrumentation (T1047)	Command and Scripting Interpreter: Python (T1059.006)
Scheduled Task/Job: At (T1053.002)	Command and Scripting Interpreter: JavaScript (T1059.007)
စီစဉ်ထားသော တာဝန်/အလုပ် - စီစဉ်ထားသော တာဝန် (T1053.005)	Native API (T1106)
Command and Scripting Interpreter (T1059)	Inter-Process Communication (T1559)
Command and Scripting Interpreter: Windows Command Shell (T1059.003)	စနစ်၏ ဝန်ဆောင်မှုများ ဝန်ဆောင်မှုကို ကွပ်မျက်ခြင်း (T1569.002)
Command and Scripting Interpreter: PowerShell (T1059.001)	Exploitation for Client Execution (T1203)
Command and Scripting Interpreter: Visual Basic (T1059.005)	အသုံးပြုသူမှ အကောင်အထည်ဖော်ခြင်း- မသမာသည့်ဖိုင် (T1204.002)
Command and Scripting Interpreter: Unix Shell (T1059.004)	Command and Scripting Interpreter: Apple Script (T1059.002)
စီစဉ်ထားသော တာဝန်/ အလုပ် - Cron (T1053.003)	Software Deployment Tools (T1072)

မဆုတ်မနစ်ခြင်း (TA0003)	
စစ်မှန်သော အကောင့်များ (T1078)	Server Software Component: Web Shell (T1505.003)
Office Application Startup: Office Template Macros (T1137.001)	Create or Modify System Process: Windows Service (T1543.003)
စီစဉ်ထားသော တာဝန်/အလုပ်- At (T1053.002)	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001)
စီစဉ်ထားသော တာဝန်/အလုပ် - စီစဉ်ထားသော တာဝန် (T1053.005)	Boot or Logon Autostart Execution: Shortcut Modification (T1547.009)
ပြင်ပ အဝေးထိန်း ဝန်ဆောင်မှု (T1133)	Hijack Execution Flow: DLL Search Order Hijacking (T1574.001)
စီစဉ်ထားသော တာဝန်/အလုပ် - Cron (T1053.003)	Hijack Execution Flow: DLL Side-Loading (T1574.002)
Account Manipulation (T1098)	စစ်မှန်သော အကောင့်များ - Cloud Accounts (T1078.004)
စစ်မှန်သော အကောင့်များ - ဒိုမိန်းအကောင့်များ (T1078.002)	

ရှိသည့် ခွင့်ပြုချက်ထက် အခွင့်အရေးတိုးချဲ့ ရယူခြင်း (TA0004)	
စီစဉ်ထားသော တာဝန်/အလုပ် - At (T1053.002)	Create or Modify System Process: Windows Service (T1543.003)
စီစဉ်ထားသော တာဝန်/အလုပ် - စီစဉ်ထားသော တာဝန် (T1053.005)	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001)
Process Injection: Thread Execution Hijacking (T1055.003)	Boot or Logon Autostart Execution: Shortcut Modification (T1547.009)
Process Injection: Process Hollowing (T1055.012)	Hijack Execution Flow: DLL Search Order Hijacking (T1574.001)

ရှိသည့် ခွင့်ပြုချက်ထက် အခွင့်အရေးတိုးချဲ့ ရယူခြင်း (TA0004)	
စစ်မှန်သော အကောင့်များ - ဒိုမိန်းအကောင့်များ (T1078.002)	ရှိသည့် ခွင့်ပြုချက်ထက် အခွင့်အရေးတိုးချဲ့ ရယူကာ အလွဲသုံးစားမှု လုပ်ခြင်း (T1068)
Access Token Manipulation: Token Impersonation/Theft (T1134.001)	Event Triggered Execution: Unix Shell Configuration Modification (T1546.004)
Process Injection: Dynamic-link Library Injection (T1055.001)	စစ်မှန်သော အကောင့်များ - ဒိုမိန်းအကောင့်များ (T1078.002)
စစ်မှန်သော အကောင့်များ - Local Accounts (T1078.003)	

လုံခြုံရေးစနစ်ကို ချိုးဖောက်ခြင်း (TA0005)	
Rootkit (T1014)	တိုက်ရိုက်မဟုတ်သည့် ကွပ်ကဲမှုကို ကွပ်မျက်ခြင်း (T1202)
ရှုပ်ထွေးအောင် ပြုလုပ်ထားသည့် ဖိုင်များ သို့မဟုတ် အချက်အလက်များ (T1027)	System Binary Proxy Execution: Mshta (T1218.005)
ရှုပ်ထွေးအောင် ပြုလုပ်ထားသည့် ဖိုင်များ သို့မဟုတ် အချက်အလက်များ - Software ထုတ်ပိုးမှု (T1027.002)	System Binary Proxy Execution: Regsvr32 (T1218.010)
ရှုပ်ထွေးအောင် ပြုလုပ်ထားသည့် ဖိုင်များ သို့မဟုတ် အချက်အလက်များ - Steganography (T1027.003)	Subvert Trust Controls: Code Signing (T1553.002)
ရှုပ်ထွေးအောင် ပြုလုပ်ထားသည့် ဖိုင်များ သို့မဟုတ် အချက်အလက်များ - Compile After Delivery (T1027.004)	File and Directory Permissions Modifications: Linux and Mac File and Directory Permissions Modification (T1222.002)
ဟန်ဆောင်လှည့်စားခြင်း - နာမည် သို့မဟုတ် တည်နေရာ ကိုက်ညီမှု (T1036.005)	Virtualisation/Sandbox Evasion: စနစ်ကို စစ်ဆေးချက်များ(T1497.001)
Process Injection: Thread Execution Hijacking (T1055.003)	ဟန်ဆောင်လှည့်စားခြင်း - (T1036)
Reflective Code Loading (T1620)	ကာကွယ်မှု ယိုယွင်းခြင်း - Disable or Modify System Firewall (T1562.004)
Process Injection: Process Hollowing (T1055.012)	Hide Artifacts: Hidden Files and Directories (T1564.001)
Indicator Removal: ဖိုင်ကို ပယ်ဖျက်ခြင်း (T1070.004)	Hide Artifacts: Hidden Window (T1564.003)
Indicator Removal: Timestomp (T1070.006)	Hijack Execution Flow: DLL Search Order Hijacking (T1574.001)
Indicator Removal: Clear Windows Event Logs (T1070.001)	Hijack Execution Flow: DLL Side-Loading (T1574.002)
Modify Registry (T1112)	Web Service (T1102)
Deobfuscate/Decode Files or Information (T1140)	ဟန်ဆောင်လှည့်စားခြင်း - ဟန်ဆောင်လှည့်စားထားသည့် တာဝန် သို့မဟုတ် ဝန်ဆောင်မှု (T1036.004)
ကာကွယ်မှု ယိုယွင်းခြင်း (T1562)	

Credential အချက်အလက် ရရှိခြင်း (TA0006)	
OS Credential Dumping: LSASS Memory (T1003.001)	လူခြုံဘေးကင်းမှု မရှိသည့် Credentials အချက်အလက် - Credentials in Files (T1552.001)
OS Credential Dumping: NTDS (T1003.003)	Brute Force: Password ကို ခန့်မှန်းခြင်း (T1110.001)
Network Sniffing (T1040)	Forced Authentication (T1187)

Credential အချက်အလက် ရရှိခြင်း (TA0006)	
Password သိုလှောင်ရေးမှ credentials များ - Keychain (T1555.001)	Kerberos Tickets ကို ခိုးယူခြင်း သို့မဟုတ် တုပခြင်း - Kerberoasting (T1558.003)
Input Capture: Keylogging (T1056.001)	Multi-Factor Authentication Interception (T1111)
Steal Web Session Cookie (T1539)	Steal Application Access Token (T1528)
Exploitation for Credential Access (T1212)	Brute Force: Password Cracking (T1110.002)
Input Capture: Web Portal Capture (T1056.003)	OS Credential Dumping: DCSync (T1003.006)
Password သိုလှောင်ရေးမှ credentials များ (T1555)	Password သိုလှောင်ရေးမှ အထောက်အထား credentials များ Credentials from Web Browsers (T1555.003)

Discovery (TA0007)	
System Service Discovery (T1007)	System Information Discovery (T1082)
Application Window Discovery (T1010)	Account Discovery: Local Account (T1087.001)
Query Registry (T1012)	System Information Discovery, Technique T1082 - Enterprise | MITRE ATT&CK®
File and Directory Discovery (T1083)	System Time Discovery (T1124)
ကွန်ရက်ဝန်ဆောင်မှုအတွင်းမှ အချက်အလက်များကို ရှာဖွေသည့်နည်းလမ်းများ (T1046)	System Owner/User Discovery (T1033)
Remote System Discovery (T1018)	Domain Trust Discovery (T1482)
Account Discovery: အီးမေးလ်အကောင့် (T1087.003)	Account Discovery: ဒိုမိန်းအကောင့် (T1087.002)
System Network Connections Discovery (T1049)	Virtualisation/Sandbox Evasion: စနစ်ကို စစ်ဆေးခြင်း (T1497.001)
Process Discovery (T1057)	Software Discovery (T1518)
Permission Groups Discovery: ဒိုမိန်း အုပ်စုများ (T1069.002)	Network Share Discovery, Technique T1135 - Enterprise | MITRE ATT&CK®
System Network Configuration Discovery: Internet Connection Discovery (T1016.001)	

Lateral Movement (TA0008)	
အဝေးထိန်း ဝန်ဆောင်မှုများ - Remote Desktop Protocol (T1021.001)	အဝေးထိန်း ဝန်ဆောင်မှုများ (T1021)
အဝေးထိန်း ဝန်ဆောင်မှုများ - SMB/Windows Admin Shares (T1021.002)	Use Alternate Authentication Material: Pass the Ticket (T1550.003)
အဝေးထိန်း ဝန်ဆောင်မှုများ - Windows Remote Management (T1021.006)	Lateral Tool Transfer (T1570)

စုဆောင်းခြင်း (TA0009)	
ဒေသစနစ်အတွင်းမှ အချက်အလက်များ (T1005)	Archive Collected Data: Archive via Library (T1560.002)
Data from Network Shared Drive (T1039)	အီးမေးလ် စုဆောင်းမှု - အဝေးထိန်း အီးမေးလ် စုဆောင်းမှု (T1114.002)

စုဆောင်းခြင်း (TA0009)	
Input Capture: Keylogging (T1056.001)	Clipboard Data (T1115)
Automated Collection (T1119)	Data from Information Repositories (T1213)
Input Capture: Web Portal Capture (T1056.003)	Data Staged: Remote Data Staging (T1074.002)
Data Staged: Local Data Staging (T1074.001)	Archive Collected Data (T1560)
အီးမေးလ် စုဆောင်းမှု (T1114)	

လျှို့ဝှက်စွာ ထုတ်ယူခြင်း (TA0010)	
C2 Channel တွင် လျှို့ဝှက်စွာ ထုတ်ယူခြင်း (T1041)	Alternative Protocol တွင် လျှို့ဝှက်စွာ ထုတ်ယူခြင်း- Exfiltration Over Asymmetric Encrypted Non-C2 Protocol (T1048.002)
Alternative Protocol တွင် လျှို့ဝှက်စွာ ထုတ်ယူခြင်း (T1048)	Web Service တွင် လျှို့ဝှက်စွာ ထုတ်ယူခြင်း - Cloud Storage တွင် လျှို့ဝှက်စွာ ထုတ်ယူခြင်း (T1567.002)

ကွပ်ကဲမှုနှင့် ထိန်းချုပ်ရေး (TA0011)	
အချက်အလက်ကို ရှုပ်ထွေးအောင် ပြုလုပ်ခြင်း - Protocol Impersonation (T1001.003)	Web Service: Dead Drop Resolver (T1102.001)
Commonly Used Port (T1043)	Web Service: One-way Communication (T1102.003)
Application Layer Protocol: Web Protocols (T1071.001)	Ingress Tool Transfer (T1105)
Application Layer Protocol: File Transfer Protocols (T1071.002)	Proxy: Internal Proxy (T1090.001)
Proxy: External Proxy (T1090.002)	Non-Standard Port (T1571)
Proxy: Multi-hop Proxy (T1090.003)	Protocol Tunnelling (T1572)
Web Service: Bidirectional Communication (T1102.002)	Encrypted Channel (T1573)
Encrypted Channel: Asymmetric Cryptography (T1573.002)	Ingress Tool Transfer (T1105)
Proxy, Technique T1090 - Enterprise | MITRE ATT&CK®	

သက်ရောက်မှု (TA0040)	
Service Stop (T1489)	Disk Wipe (T1561)
စနစ်ကို ပိတ်ချခြင်း/ ဖွင့်ပိတ်လုပ်ခြင်း (T1529)	Resource Hijacking (T1496)

မှတ်ချက်

မသက်ဆိုင်ကြောင်း ရှင်းလင်းချက်

ဤလမ်းညွှန်ချက်ပါ အကြောင်းအရာများသည် အထွေထွေအကြံပြုချက်သာဖြစ်ပြီး တရားရေးရာ အကြံပြုချက် အဖြစ် မမှတ်ယူသင့်သကဲ့သို့ အချို့အခြေအနေအတွက် အကူအညီ သို့မဟုတ် အရေးပေါ်အခြေအနေအတွက် အားထားရာ အကြံပြုချက်မဖြစ် မယူဆသင့်ပါ။ အရေးကြီးသည့်အခါ သင်ကြုံတွေ့ရသည့် အတွေ့အကြုံအတွက် သင့်တော်ပြီး သီးသန့် လွတ်လပ်မှုရှိသည့် ကျွမ်းကျင်ပညာရှင်များ၏ အကြံဉာဏ်များကို ရယူပါ။

ဤအကြံပြုချက်ပါ အချက်အလက်များအပေါ် မှီခိုရာက ပျက်စီးမှုဖြစ်ခြင်း၊ ဆုံးရှုံးရခြင်း သို့မဟုတ် ငွေကုန်ကြေးကျ ခံရပါက အစိုးရအနေဖြင့် တာဝန်ယူမည် မဟုတ်ပါ။

မူပိုင်ခွင့်

နိုင်ငံတော် အမှတ်တံဆိပ်ကို အသုံးပြုခြင်း

နိုင်ငံတော် အမှတ်တံဆိပ်အား မည်သည့်နေရာတွင် အသုံးပြုခြင်းဆိုင်ရာ အသေးစိတ်အချက်အလက်အား ဝန်ကြီးချုပ်နှင့် ဝန်ကြီးအဖွဲ့၏ ဝန်ကြီးဌာန၏ ဝဘ်ဆိုက်တွင် ဖော်ပြထားပါသည်၊ နိုင်ငံတော်၏ အမှတ်တံဆိပ် ဆိုင်ရာ အချက်အလက်နှင့် လမ်းညွှန်ချက်များ| pmc.gov.au.

အချက်အလက်ပိုများနှင့် ဆိုင်ဘာလုံခြုံရေး ချိုးဖောက်ခံရမှုအား မည်သို့ တိုင်တန်းနိုင်သနည်း အကြောင်း လေ့လာရန် နှင့် ဆက်သွယ်မှုလုပ်လိုပါက-

cyber.gov.au | 1300 CYBER1 (1300 292 371) ကို ဆက်သွယ်ပါ။

ဤနံပါတ်ကို ဩစတြေးလျနိုင်ငံအတွင်းသာ အသုံးပြုနိုင်ပါသည်။

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre