APT40 བསྒྲབ་སྦྱོན།

PRC MSS གྱི་ལག་རྩལ་བེད་སྤྱོད་བྱེད་པ།

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**

དཀར་ཆག

ཀློ་བསྡོམས།

རྒྱབ་སྐྱོར།

འདི་ནི་ཨོ་སི་ཀླུ་ལི་ཡའི་བརྡ་རྟགས་འགན་འཛིན་གྱི་ཨོ་སི་ཀླུ་ལི་ཡའི་དྲ་རྒྱའི་བདེ་འཇགས་ཚེ་གནས་ (ASD's ACSC)དང་། ཨ་རིའི་དྲ་རྒྱའི་བདེ་འཇགས་དང་རྩིང་གཞིའི་བདེ་འཇགས་ལས་ཁུངས་ (CISA)། ཨ་རིའི་རྒྱལ་ཡོངས་བདེ་འཇགས་ལས་ཁུངས་ (NSA)། ཨ་རིའི་སྤྱི་མཐུན་ཞིབ་བཤེར་ལས་ཁུངས་ (FBI)། ཡིང་གི་རྒྱལ་ཡོངས་དྲྭ་རྒྱའི་བདེ་འཇགས་ཚེ་གནས་ (NCSC-UK)། ཀེ་ན་ཊའི་དྲ་རྒྱའི་བདེ་འཇགས་ཚེ་གནས་ (CCCS)། ནེའུ་ཛི་ལན་གྱི་རྒྱལ་ཡོངས་དྲྭ་རྒྱའི་བདེ་འཇགས་ཚེ་གནས་ (NCSC-NZ)། འཇར་མན་གྱི་སྤྱི་མཐུན་མཁས་སྒྲུལ་ལས་ཁུངས་ (BND) དང་རྩ་ཁྲིམས་སྡུང་སྐྱོབ་སྤྱི་མཐུན་ལས་ཁང་ (BfV)། ཚྭ་ཀོ་རི་ཡའི་རྒྱལ་ཡོངས་མཁས་སྒྲུལ་ལས་ཁུངས་ (NIS) དང་རྒྱལ་ཡོངས་དྲྭ་རྒྱའི་བདེ་འཇགས་ཚེ་གནས། ཉི་ཧོང་གི་རྒྱལ་ཡོངས་གནོད་འཚེ་ཐབས་ཤེས་དང་ཐབས་རྩལ་གྱི་དྲ་རྒྱའི་བདེ་འཇགས་ཚེ་གནས་ (NISC) དང་རྒྱལ་ཡོངས་ཉེན་རྐྱེ་གལ་ལས་ཁུངས་ (NPA) བཅས་ཀྱིས་ – རྩེས་སུ་”རྩོམ་སྒྲིག་ལས་ཁུངས་ཚོ་”ཞེས་འབོད་པ་དེས་ཀྱང་གོ་མི་དམངས་སྤྱི་མཐུན་རྒྱལ་ཁབ་ (PRC) ཀྱི་རྒྱལ་ཁབ་ཀྱིས་རྒྱབ་སྐྱོར་བྱེད་པའི་དྲྭ་རྒྱའི་ཚོགས་པ་ཞིག་དང་། དེ་ཚོས་ཨོ་སི་ཀླུ་ལི་ཡའི་དྲ་རྒྱ་ལ་ཉེན་ཁ་གང་འདུ་ཞིག་བཟོ་བསྒྲུབ་བྱེད་ཀྱི་ཡོད་པའི་སྐོར་གསལ་སྟོན་བྱས་ཡོད། བསྒབ་སྟོན་འཛིན་སྡེ་”རྩོམ་སྒྲིག་ལས་ཁུངས་ཚོའི་ཉེན་ཁ་དེའི་སྐོར་ཀྱི་མཐའ་སྐྱོང་གོ་རྐྱེན་པ་དང་། དེ་བཞིན་ ASD ཡི་ ACSC ཀྱི་དོན་ཆུབ་ལ་ཡན་འདེའས་བྱེད་ཞིང་ཡིན་ཞེས་ཁས་ལེན་ཡོད། བསྒྲུབ་སྟོན།

ཀྲུང་གོ་མི་དམངས་སྤྱི་མཐུན་རྒྱལ་ཁབ་ཀྱི་གཞུང་གིས་རྒྱབ་སྐྱོར་བྱེད་པའི་དྲྭ་རྒྱའི་ཚོགས་པས་སྤྱོད་ཚད་ཨོ་སི་ཀླུ་ལི་ཡ་དང་ཨ་རི་སོགས་རྒྱལ་ཁབ་སོ་སོའི་ཚོགས་པ་ཁག་ལ་དམིགས་འབེབ་བཟུང་ཡོད་པ་དང་། གཞན་དུ་གསལ་བྱས་པའི་ལག་རྟོགས་དེ་དག་ནི་འཛམ་གླིང་ཡོངས་ལ་ཀྲུང་གོ་གཞུང་གིས་རྒྱབ་སྐྱོར་བྱེད་པའི་གཞན་པའི་བྱེད་སྒོ་ཚོས་ཏྲག་པར་བེད་སྤྱོད་གཏོང་གི་ཡོད། དེར་བརྟེན་ཚོས་སྤྲིག་ལས་ཁུངས་ཚོས་ཚོགས་པ་དེ་དང་དེ་དང་འབྲེལ་བའི་ལག་རྟོང་ཚོའི་རྒྱལ་ཁབ་ཀྱི་ཁྱད་དེ་ཁོ་ནས་ཁོང་ཚོའི་རྒྱལ་ཁབ་ཀྱི་ཡོད། དེར་བརྟེན་ཚོས་སྤྲིག་ལས་ཁུངས་ཚོས་ཚོགས་པ་དེ་དང་དེ་དང་འབྲེལ་བའི་ལག་རྟོང་ཚོའི་རྒྱལ་ཁབ་ཀྱི་ཁྱད་དེ་ཁོ་ནས་ཁོང་ཚོའི་རྒྱལ་ཡོངས་ཉེན་ཁ་ཡིན་པར་ཡིད་ཆེས་བྱེད་ཀྱི་ཡོད།

ཚོས་པ་པོ་ལས་ཁུངས་ཁག་གིས། ཚོགས་པ་འདིས་རྒྱ་རྒྱ་རྒྱལ་ཁབ་ཀྱི་བདེ་འཇགས་ཤུན་ཁང་ (MSS) ལ་དྲག་རྒྱའི་ལས་དོན་ངན་པ་སྤེལ་བཞིན་ཡོད་ཀྱི་ཚོད་དཔག་བྱེད་ཀྱི་ཡོད། ལས་རིམ་དང་ལག་རྩལ་དེ་ཚོ་གོང་འཕེལ་ཅན་གྱི་རྒྱུན་གཏན་ཀྱི་ཉེན་ཁ་ (APT) ༤༠ ཞེས་རྩེས་འབྲང་བྱེད་པའི་ཚོགས་པ་ཚོ་དང་མཐུན་པ་ཡོད། (བཅོ་གྲའི་སྐྱན་ཁྲའི་ནང་ Kryptonite Panda དང་། GINGHAM TYPHOON| Leviathan| Bronze Mohawk ཞེས་ཀྱང་ཟེས་པ།) ཚོགས་པ་འདི་སྟོན་ཚད་ཀྲུང་གོ་མི་དམངས་སྤྱི་མཐུན་རྒྱལ་ཁབ་ཀྱི་ཉའི་ནན་ཚེ་གྲུབ་ཡོད་པ་དང་། PRC MSS ཉའི་ནན་མངའ་སྡེའི་རྒྱལ་ཁབ་བདེ་འཇགས་ལས་ཁུངས་ནས་ལས་འགན་ལེན་བཞིན་ཡོད་པའི་སྐྱན་ཁྲ་ཐོན་ཡོད། གཤན་གྱི་བསྒབ་སྟོན་འདིས་འཚེ་བ་ཡོག་པའི་དྲྭ་གཉིས་ལ་དམིགས་ནས་དགུ་བོ་འདིས་བེད་སྤྱོད་གཏོང་བའི་ལག་རྩལ་གྱི་གལ་ཆེའི་དབེ་ཞིབ་ཤིག་ཡིན།

ལས་དོན་བསྡུས་དོན།

APT40 ཡིས་ཨོ་སི་ཀླུ་ལི་ཡའི་དྲྭ་དང་ས་ཁུལ་དེའི་གཞུང་དང་སྤེར་གྱི་དྲྭ་ལ་ཡང་ཡང་དམིགས་འབེབ་བཟུང་ཡོད་པ་དང་། དེ་དག་གིས་ད་ཚོའི་དྲྭ་རྒྱ་ལ་ཉེན་ཁ་ བཟོ་བཞིན་པ་དེ་སུ་མཐུད་ནས་གནས་བཞིན་ཡོད། བསྒབ་སྟོན་འདིའི་ནང་དུ་བཤད་པའི་ལག་རྩལ་ཚང་ཐབས་ཤེས་དེ་ཨོ་སི་ཀླུ་ལི་ཡའི་དྲྭ་རྒྱའི་ཐོན་རྫས་ (POCs)མཁྱོགས་སྡུར་དུ་སྡུར་བཅོས་དང་བསྟུན་སྤོང་བྱེད་ཐུབ་པའི་ནུས་པ་ཡོད་པ་དང་། དེ་མཚུངས་རྣམ་སྐྱོན་དང་འབྲེལ་བའི་གཞི་རིམ་ཅན་གྱི་དམིགས་ཡུལ་དྲྭ་རྒྱའི་ཐོག་ལ་མཚམས་མེད་དུ་བེད་སྤྱོད་བྱེད་ཐུབ་པ་རེད། APT40 ཡིས་དུས་རྒྱུན་དུ་རྩོམ་སྒྲིག་ལས་ཁུངས་ཀྱི་རྒྱལ་ཁབ་ཀྱི་དྲྭ་རྒྱ་ཚུད་པའི་ཁེ་ཕན་ཡོད་པའི་དྲྭ་རྒྱ་ལ་སར་ཉེན་ཁ་དེ་ཚོའི་ཐོག་ལ་ཡིད་ཆེས་བྱེད་ཀྱི་ཡོད་པ་དང་། དེ་ཡང་དམིགས་ཡུལ་ལ་སྐྱོན་ཞུགས་པའི་གོ་སྐབས་འཚོལ་བ་ཡིན། དུས་རྒྱུན་གྱི་བརྟག་དཔྱད་འདིས་ཚོགས་པ་དེ་ལ་རྣམ་སྐྱོན་ཡོག་པའི་འཕྲུལ་ཆས་དང་། ཚུལ་གསར་མེད་པ། དངོས་སྟོབ་བྱས་ཚར་བའི་འཕྲུལ་ཆས་ཚུ་སྐོར་ལ་རིགས་སྤགས་མང་བའི་ ཡོངས་འཛིན་གྱི་དོན་ལས་དོས་འཛིན་བྱེད་པ་དང་། སྡུར་དུག་སྐྱོར་བྱས་པར་བཙུག་པ་ཡིན། APT40ཡིས་2017ལོ་ནས་བཟུང་རྣམ་སྐྱོན་བགོལ་སྟོང་བྱེད་པར་སྡུ་མཐུད་དུ་གྲུབ་འབྲས་ཐོབ་ཡོད།

APT40 ཡིས་ཁྱབ་ཚར་བེད་སྟོང་བྱེད་བཞིན་པའི་མཉེན་ཆས་ཀྱི་ཁྱབ་ཁྱོངས་ཀྱི་རྣམ་སྐྱོན་གསར་པ་ཚུར་མཁོགས་པར་བེད་སྟོང་བྱེད་ཀྱི་ཡོད། དཔེར་ན་ Log4j (CVE 2021 44228) དང་། Atlassian Confluence (CVE-2021-31207, CVE-2021-26084) དང་། Microsoft Exchange (CVE-2021-31207; CVE-2021-34523; CVE-2021-34473) སོགས་ཡིན། ASDཡི་ACSCདང་ཚོས་སྤེལ་གྲུབ་ཀྱིས་ཚོགས་པ་དེས་ནི་མང་ལ་གསལ་བསྒགས་བྱས་པའི་ཚུ་ཚོད་དང་ཉེན་ཁ་ཤས་ནང་མཐོ་རིམ་གྱི་རྣམ་སྐྱོན་གསར་པའི་ཚེད་ཀྱུ་ POCs མ་མཐུད་ནས་བེད་སྟོང་གཏོང་ཚུའི་ཨ་བ་བྱེད་ཀྱི་ཡོད།

2 ཨ་རིའི་ཁྲིམས་ཞིབ་ལས་ཁུངས། ༢༠༢༡ རྒྱལ་ཁབ་བདེ་འཇགས་ལས་ཁུངས་དང་མཉམ་དུ་ལས་ཀ་བྱེད་བཞིན་པའི་རྒྱ་མི་ཕེར་བཞི་ལ་ཤེས་ཡོན་རྒྱ་ཚོད་ཟིན་དང་གསང་བའི་ཚོང་དོན་གནས་ཚུལ། དེ་ནང་ནས་ཡིག་ཆའི་ཤོག་གྲངས་ཀྱི་ཐོག་ནས་ཞིབ་ཕྲའི་ཆ་འཕྲིན་ཚུ་ཡོད།

དཔེ་རིས ༧། APT40 བྱ་འགྱུལ་གྱི་ TTPཚུན་རིམ་རི་མོ།

ཚོགས་པ་འདིས་ཡི་ཤིང་ལས་འགྱལ་ལྟ་བུའི་སྤྱོད་མཁན་གྱི་འབེལ་བ་དགོས་པའི་ལག་རྩལ་ལས་རྣམ་སྤྱོད་ཡོག་པའི་སྤྱི་དམངས་ལ་ཁ་ཡོག་པའི་གཞི་རིམ་སྤྱིག་ཆས་བེད་སྤྱོད་གཏོང་རྒྱུ་དགའ་ཡོ་བྱེད་ཀྱི་ཡོད་པ་མ་རེད། ཕྱི་མའི་ལས་གཞི་སྣ་ཚོགས་ལག་བསྟར་བྱེད་པའི་ཚེད་དུ་ཡང་དག་པའི་ཐོབ་ཐང་ལས་པར་བཞེས་པ་ལ་གནད་འགག་ཚེན་པོ་སྤུང་ཀྱི་ཡོད།། APT40 ཡིས་རྒྱུན་དུ་དྲ་རྒྱའི་ཁོག་སྟོང་ (T1505.003) བརྟན་གནས་ཀྱི་ཚེད་དུ་བེད་སྤྱོད་བྱེད་ཀྱི་ཡོད་པ་དང་། སྐག་པར་དུ་ཞུགས་འཇུལ་ཀྱི་འཛེལ་རིམ་གྱི་ཐོག་མར་དེ་སྐར་བྱེད་ཀྱི་ཡོད། ཕྱིར་བཏང་དུ་ཐོག་མའི་ཐོབ་ཐང་ལེགས་འགྲུབ་བྱང་རྩེས་APT40ཡིས་གནོད་འཚེ་ཡོག་མཁན་གྱི་ཁོར་ཡུག་ལ་ཐོབ་ཐང་རྒྱུན་འགྱོངས་བྱེད་པར་བརྩོན་འགྲུས་བཏང་བས་གཙོ་བོར་བཤུ་དགོས། ཡིན་ནའང་། བརྟན་གནས་ནི་ཞུགས་འཇུལ་ཀྱི་ཐོག་མར་བྱེད་ཀྱི་ཚད་གཞི་ཡང་ན་ཕྱི་མའི་བྱ་གཞག་ལ་མ་སྤྱོས་པར། ཞུགས་འཇུལ་ཚང་མའི་ནང་བཤོད་རྒྱུའི་ཐོ་སྐབས་ཚེ་བ་ཡོད།

མངོན་གསལ་དོད་པའི་ཚོང་ལས་ལག་རྩལ།

APT40 ཡིས་སྤོན་ལས་ཙོསི་ཏོ་ལི་ཡའི་དྲ་ཚིགས་ཚུ་སྒོ་འབྱེད་བྱས་པའི་བརྒྱུད་སྒོང་དང་ཚོད་འཛིན་ (C2) གྱི་བཀའ་བཀོད་ལུ་ཅེད་སྤྱོད་བྱས་པ་ཡིན་ཀྱང་། དེ་ཚུ་ཚོགས་པ་དེས་ཐབས་ལམ་དེ་རིམ་པ་བསྒྲུར་ཞིབ་དང་མཐོང་སྐལ་བྱས་འདུག (T1594)

APT40 ཡིས་ཙོ་སི་ཁྲུ་ལི་ཡའི་ལས་དོན་ཚེད་དུ་ཡིག་ཚང་ཆུང་ཆུང་/ཁྱིམ་ཚང་གི་ཡིག་ཚང་(SOHO) བཅས་བཀོལ་སྤྱོད་བྱེད་པའི་རྩང་གཞིའི་སྤྱིག་བཀོད་དང་མཐའ་མའི་བསྒྲུབ་ལེས་ཀྱི་ཡོད་པ་ཨིན། (T1584.008) བཀོལ་སྤྱོད་བྱེད་པའི་གོ་ལ་དེའ་པོའི་འགོ་ཕྱོགས་ལ་དང་ལེན་བྱས། འདིས་རྩོམ་པ་པོའི་ལས་ཁྲངས་ལ་ཚོགས་པ་འདིའི་འགྱལ་སྤྱོད་ལ་ཁྲད་ཚོས་ཡག་པོ་བསྒྲུབ་ཐུབ་པ་དང་རྗེས་འབེད་གཏོང་ཐུབ་པ་བྱས་ཡོད།

SOHO ཡོ་ཚས་འདི་དག་མང་ཆེ་བ་ཚོ་སྡོག་མཐུག་སྤྱིལ་ཟིན་པ་དང་། ཡང་ན་བསྒྲུར་བཅོས་མ་བྱས་པ་ཡིན་པས། དེ་ལས་འདས་པའི་དུན་དེབ་བགོལ་སྤྱོད་ཀྱི་ཐབས་ལམ་ལ་དམིགས་ནས་གནས་སྐབས་བསམ་འཆར་བྱས་པའི་གནས་སུ་འགྲོ་བའི་ཡོད་ཚད་ཅན་ཡིན། གལ་ཏེ་SOHO ཡོ་ཚས་དེ་ཚོས་ཁེམས་མཐུན་ཀྱི་འགྲིམ་འགྲུལ་དང་འགན་སྤོང་དུ་རྒྱའི་འགོག་སྡུང་བ་དང་མཉམ་དུ་བསྟེན་ནས་བཟོས་པའི་འཛབ་ཚོལ་ཀྱི་འགོ་འཛུགས་ས་ཞིག་སྤྱོད་ཀྱི་ཡོད། (T1001.003)

ཐབས་ཤེས་འདི་འཛམ་གླིང་ཡོངས་ཀྱི་རྒྱ་ནག་གཞུང་གིས་རྒྱབ་རྟེན་སྤྱོར་བྱས་པའི་འཁབ་སྟོན་པ་གཞན་དག་གིས་ཀྱང་དུ་བེད་སྤྱོད་བྱེད་སྐུག་ཡོད་དང་། མཚོན་འབྱེད་བྱས་པའི་ལས་ཁྲངས་གཞན་དག་གིས་ཡང་ཁ་ཤེས་དུ་བཤུ་དེ་ཡིན་པས་གཞི་རིམ་སྤྱིག་ཆས་ཀྱི་ཚད་གཞི་ཡང་ན་ཕྱི་མའི་བྱ་གཞག་ལ་མ་སྟོས་པར། ཞུགས་འཇུལ་ཚང་མའི་ནང་བཅོས་བཟོས་ཡོད་ཟེར་བ་ཡིན་ནའང་། ཁྱད་པར་ཅན་གྱི་ཐབས་ལམ་ཚུ་ནི་ཁོང་ཚུའི་ཐོག་ཁོ་ནར་ཡོད་པ་ཨིན།

འཛབ་སྟོན་པ་ཚུས་དྲ་རྒྱའི་མཁོ་སྤྲོད་བྱེད་མཁན་དང་འཕྲུལ་ཆས་ཚུ་ཡུ་བཀོལ་སྤྱོད་བྱས་པ་ དང་། རྒྱ་ནག་གཞུང་གིས་རྒྱུ་བཤུ་ཡོད་པའི་ཐབས་ལམ་ལ་འཇུག་འབྲས་ཆེ་ཤོས་ཡོད་པའི་ཁྱད་པར་ཅན་གྱི་འཇུག་སྤྱོད་ཀྱི་ཐབས་ལམ་ཚུ་ཨིན།

APT40 ཡིས་སྐབས་རེ་ཉོ་སྤྱད་བྱས་པའམ་ཡང་ན་གྲ་གཅོད་བྱས་པའི་རྩང་གཞིའི་སྤྱིག་བཀོད་དེ་ཁོང་གི་ལས་དོན་ནང་གཞོད་འཚེ་ཡོག་མཁན་ལ་གཏོང་ལེན་བྱེད་པའི་C2 རྩང་གཞིའི་སྤྱིག་བཀོད་ཉར་བེད་སྤྱོད་བྱེད་ཀྱི་ཡོད། ཡིན་ནའང་ཚོང་ལས་ལག་རྩལ་འདི་ཤུད་དུ་འགྲོ་བཞིན་ཡོད་པ་ཉུ་བུ་རེད།

ལག་ཆ།

གཤན་གསལ་གྱི་ཞིབ་བཤེར་སྐབས་སུ་ངོས་འཛིན་བྱས་པའི་ཡིག་ཆ་དང་པ་ཤས་ ASD ཡི་ ACSC གིས་མཉམ་སྦྱོང་བྱེད་བཞིན་ཡོད། ཡིག་ཆ་འདི་དག་ VirusTotal ལ་ཕབ་ལེན་བྱས་པ་དེས་ དྲ་རྒྱའི་འགོག་སྡུང་དང་དྲ་རྒྱའི་བའེ་འཛགས་ཚོགས་པ་རྣམས་ཆེ་བ་ཚུ་གིས་བའེ་སྤྱངས་བསམ་ཚུལ་ཅན་དུ་ཞིན་ཁ་ཚུ་ཤེས་དགོས་པ་དེ་ལ་གོ་བ་ལེན་ཐུབ་པ་བྱེད་པའི་དོན་ལུ་ཡིན།

དཔེ་མཚོན་ཞིབ་འཇུག།

ASD གི་ ACSC ཡིས་བྱེད་མཁན་ཚོས་ཁོང་ཚོའི་ལག་ཆ་དང་ལག་རྩལ་ཐུམ་ཉོད་སྤྱོད་བྱེད་ཀྱི་ཡོད་པའི་ཤེས་རྟོགས་སྤྲོད་པའི་ཚེད་དུ་མིང་མ་བཀོད་པའི་ཞིབ་འཇུག་སྤྱན་ཁྱབ་མཉམ་སྦྱོང་བྱེད་བཞིན་ཡོད།

MD5	ཡིག་ཆའི་མིང་།	ཁ་སྐོན་གྱི་ཆ་འཕྲིན།
26a5a7e71a601be991073c78d513dee3	horizon.jsp	1 kB | Java འབྱུང་ཁུངས།
87c88f06a7464db2534bc78ec2b915de	Index_jsp$ProxyEndpoint$Attach.class	597 B | ཇ་བ་གླེའུ་ཀོད།
6a9bc68c9bc5cefaf1880ae6ffb1d0ca	Index_jsp.class	5 kB | ཇ་བ་གླེའུ་ཀོད།
64454645a9a21510226ab29e01e76d39	Index_jsp.java	5 kB | Java འབྱུང་ཁུངས།
e2175f91ce3da2e8d46b0639e941e13f	Index_jsp$ProxyEndpoint.class	4 kB | ཇ་བ་གླེའུ་ཀོད།
9f89f069466b8b5c9bf25c9374a4daf8	Index_jsp$ProxyEndpoint$1.class	3 kB | ཇ་བ་གླེའུ་ཀོད།
187d6f2ed2c80f805461d9119a5878ac	Index_jsp$ProxyEndpoint$2.class	1 kB | ཇ་བ་གླེའུ་ཀོད།
ed7178cec90ed21644e669378b3a97ec	Nova_jsp.class	7 kB | ཇ་བ་གླེའུ་ཀོད།
5bf7560d0a638e34035f85cd3788e258	Nova_jsp$TomcatListenerMemShellFromThread.class	8 kB | ཇ་བ་གླེའུ་ཀོད།
e02be0dc614523ddd7a28c9e9d500cff	Nova_jsp.java	15 kB | Java འབྱུང་ཁུངས།

དཔེ་མཚོན་ཞིབ་འཇུག་དང་པ།

སྤྱན་ཐོ་འདི་ཁྱབ་བསྒྲགས་རྒྱ་ཆེ་རུ་གཏོང་ཆེད་མིང་མ་བཀོད་པར་བཟོས་ཡོད། ཤུགས་རྐྱེན་ཐེབས་པའི་ཚོགས་པ་དེ་ཕྱི་མ་ནས་,ཚོགས་པ་དེ་,ཞེས་བརྗོད་པར་བྱའོ། ཚོར་བའི་མི་དང་ ASD གི་ ACSC ཡི་གནས་ཚུལ་ལན་འདེབས་ཐབས་ལམ་གྱི་ངོ་བོ་སྣང་སྐྱོབ་བྱེད་པའི་ཆེད་དུ་དམིགས་བསལ་གྱི་ཞིབ་ཕྲའི་གནས་ཚུལ་འགའ་ཤས་བསྡུ་བའོ།

འཆར་གཞི་བདག་པོའི་བསྟུས་དོན།

སྤྱན་ཐོ་འདིས་ 2022 ལོའི་ཟླ་ བདུན་པ་ནས་ཟླ་ དགུ་པའི་བར་ཚོགས་པའི་དྲུམ་སྒྲིག་འཛུགས་ལ་ལོངས་བཅམ་བྱས་པའི་ལས་དོན་དང་འབྲས་བུ་ལ་སྐྱོན་པའི་ ASD ཡི་ ACSC ཞིབ་བཤེར་གྱི་གནས་ཚུལ་ཞིབ་ཕྲ་བགོད་ཡོད། ཞིབ་བཤེར་སྤྱན་ཞུ་འདི་ཚོགས་པ་དེ་ལ་སྤུང་པ་ཡིན། དེའི་དོན་ནི་ དོ་སྣང་བྱང་བའི་གཞོད་འཚོ་ཅན་གྱི་བྱ་སྤྱོད་སྤྱིང་བསྡུས་དང་། བཅོས་སྒྲིག་བྱ་རྒྱའི་སྟོས་འཚར་བཟོ་ཆེད་ཡིན། ཞིབ་བཤེར་གྱི་འབྲས་བུ་ཡྱར་ན་ བདེ་འཇགས་དེ་ APT40 ཡིས་ལོངས་བཅམ་བྱས་པ་ཡིན།

སྒྲིག་འཛུགས་ཀྱིས་ནེད་སྤྱོད་བྱེད་བཞིན་པའི་ཡོ་ཆས་ཤིག་ལས་འབྱང་བ་དེ་དཔྱད་བཤེར་བྱས་ནས་རྒྱན་དུ་གསལ་བར་བཏང་ཡོད། དེ་མཉམ་སྒྲིག་བྱས་ནས་ཚོགས་པའི་དྲུམ་སྒྲིག་འཛུགས་གཞོད་འཛེ་བྱང་བའི་ཡོ་ཆས་ཚུ་གནས་སྐྱངས་ལ་གཟིགས་སྐྱོང་བྱེད་པའི་ཐབས་ལམ་བཅད་ཚུ་འཛུགས་དུ་ ASD ཡི་ ACSC གིས་ཡོ་ཆས་གཞན་ལ་མངོན་སྐྱོན་བྱང་བའི་འཛུགས་སྒྲིག་བྱེད་བཞིན་པའི་ཁ་ཤས་ASDཡི་ ACSC དོན་རྒྱེན་ལན་འདེབས་དབྱེ་ཞིབ་པ་ཚོར་དུ་རྒྱའི་ཁྲིམས་ལུགས་ཞིབ་བཤེར་གཏིང་ཟབ་བྱེད་ཐུབ་པ་བྱས། མཐོང་ཐུབ་པའི་ཚོར་ཤེས་ཀྱི་གནས་ཚུལ་བགོལ་ནས་ ASD ཡི་ ACSC དབྱེ་ཞིབ་པ་ཚོས་ཚོགས་པའི་བྱེད་སྒོ་མཐར་ཕྱིན་དང་ས་ཁྲ་བཟོས་ནས་བརྟག་དཔྱད་བྱས་པའི་སྐྱང་རིམ་གྱི་དུས་ཚོད་ཞིབ་ཕྲ་བཟོས་ཡོད།

ཟླ་ བདུན་པ་ནས་ཟླ་ བརྒྱད་པའི་བར་གྱས། ASD ཡི་ ACSC གིས་དོ་སྣང་བྱས་པའི་འཁབ་སྐྱོན་པ་གཙོ་བོའི་བྱེད་སྒོ་ཚུ་ནི།

- ཡོ་ཆས་གྲངས་འབོར་བྱས་པ། དེས་འཁབ་སྐྱོན་པ་ཞིག་ལ་དྲུའི་ས་ཁྲ་རང་ཉིད་གསར་བཟོ་བྱེད་ཐུབ།
- དྲུའི་ཁོག་སྐྱོང་ཝེད་སྤྱོད་བྱེད་པ་དེས་འཁབ་སྐྱོན་པ་ལ་དྲུའི་ཐོག་ལ་འགོ་འཛུགས་ཀྱི་ཤུང་པ་འཛུགས་ས་དང་བཀག་ཆོག་ལག་བསྟར་བྱེད་པའི་ནུས་པ་སྤྱོད་ཀྱི་ཡོད། དང་
- གནོད་འཚེ་བྱེད་པས་གནོད་འཚེ་དོན་ལུ་བགོལ་སྤྱོད་བྱེད་པའི་ལག་ཆ་གཞན་པ་ཕྱོགས་སུ་འཛུག་བྱས་པ།

ཞིབ་བཤེར་གྱིས་ཚོར་ཐུགས་ཆེ་བའི་གནས་ཚུལ་མང་པོ་ཞིག་ལ་འཛུལ་ཞུགས་བྱེད་པའི་དཔང་རྟགས་དང་འཁྲབ་སྐྱོན་པ་ཚོས་དྲུ་ཆུ་བརྒྱུད་ནས་ཕྱོགས་གཅིག་ཏུ་སྤོ་བའི་དཔང་རྟགས་ཤེས་རྟོགས་བྱང་ཡོད། (T1021.002) བདེ་འཇགས་ལོངས་སྤྱོད་ཀྱི་གནད་དོན་ཀྱི་ཚེ་ཤོས་ནི་ཚོགས་པ་དེས་དྲུ་ཆུ་ནང་དུ་ཞུགས་ཐབས་ཀྱི་ལམ་ཁ་མང་པོ་གཏན་འབེབས་བྱས་པ་དང་། དྲུ་ཆུ་དེ་ལ་རིམ་པ་མེད་པའི་བཀོད་པ་ཡོད་པ། དེ་མ་ཟད་ནང་ཁུལ་དུ་སྐྱན་པའི་བདེ་འཇགས་མེད་པའི་མཉེན་ཆས་ཤིག་བསྒྲིད་བྱས་པ་སྟེ། དེ་ལ་བརྟེན་ནས་ཡིག་ཆ་གང་རུང་གི་ར་དང་དཔང་གིས་ཁྲར་བླུག་ཏེད་ཐུབ་པ་ཡྱར་བ་རེད། ཕྱིར་འདྲེན་བྱས་པའི་གནས་ཚུལ་ཀྱི་ནང་དུ་ཚོགས་པ་དེ་ལ་ནང་འཛུལ་ཏེད་ཐུབ་པའི་ཁྱད་པར་ཅན་ཀྱི་ངོས་འཛིན་ཡང་དག་ཡིག་ཆ་དང་། དེ་བཞིན་དུ་རྒྱའི་ཆ་འཕྲིན་ཚུད་ཡོད་དེ། གལ་ཏེ་ཐོག་མའི་འཛུལ་ཞུགས་ཀྱི་བརྒྱུད་ལམ་བཀག་ཡོད་ན། ཏེད་མཁའ་རྣམས་ལ་ཚོག་མཚན་མེད་པའི་འཛུལ་ཞུགས་སྒར་ཐོབ་ཐུབ་པའི་གོ་སྐབས་སྤྱད་ཡོད། ཐོག་མར་བཀོལ་སྤྱོད་བྱས་པའི་འཕྲུལ་ཆས་ཐོག་ཡོད་པ་ལས་གཞན་ཡང་ཁ་ཤས་ཀྱི་ཐོག་ཏུ་སྐྱོན་སྤྱད་ཡོད་ཀྱི་ཡག་ཆ་ཁ་སྐོང་ཡོད་ཚེ་ཡང་ཁ་ཤས་ཀྱི་ཡོད་ཚད་ཆ་ཤས་ཙམ་ཁོ་ནས་ཡོད་ཚུལ་ཞིབ་ཕྲ་ཐོག་ཏུ་ཡོད་ཚུལ་ཁོངས་ནས་ཤེས་ཡོན་ཡོད་པ་ཡིན། ཕྱིར་བཏང་ཐུབ་པའི་ཡིག་ཆ་ཚུ་ནང་ཁུལ་ཁྱབ་ཀྱི་ཡིག་ཆ་ཁ་ཤས་ཀྱང་ཡོད་ཅིང་། ཁོང་ཚོས་ཡིག་ཆ་ཚུ་ཁྱབ་ཁོངས་ནས་ཕྱིར་བཏོན་བྱས་ཡོད་ཚུལ་ཡང་ཞིབ་ཕྲ་ཞིབ་བཤེར་བྱས་ཡོད།

ཞིབ་བཤེར་གྱིས་ཚོར་ཐུགས་ཆེ་བའི་གནས་ཚུལ་མང་པོ་ཞིག་ལ་འཛུལ་ཞུགས་བྱེད་པའི་དཔང་རྟགས་དང་འཁྲབ་སྐྱོན་པ་ཚོས་དྲུ་ཆུ་བརྒྱུད་ནས་ཕྱོགས་གཅིག་ཏུ་སྤོ་བའི་དཔང་རྟགས་ཤེས་རྟོགས་བྱང་ཡོད། (T1021.002) བདེ་འཇགས་ལོངས་སྤྱོད་ཀྱི་གནད་དོན་ཀྱི་ཚེ་ཤོས་ནི་ཚོགས་པ་དེས་དྲུ་ཆུ་ནང་དུ་ཞུགས་ཐབས་ཀྱི་ལམ་ཁ་མང་པོ་ཞིག་ལ་འཛུལ་ཞུགས་བྱེད་པའི་ཆེད་དུ་ཞུགས་ཐབས་ཀྱི་ལམ་ཁ་མང་པོ་ཡོད་པ། དེ་མ་ཟད་ནང་ཁུལ་དུ་སྐྱན་པའི་བདེ་འཇགས་མེད་པའི་མཉེན་ཆས་ཤིག་བསྒྲིད་བྱས་པ་སྟེ། དེ་ལ་བརྟེན་ནས་ཡིག་ཆ་ཚུ་ནང་ཁུལ་ཁྱབ་ཀྱི་ཡིག་ཆ་ཁ་ཤས་ཀྱང་ཡོད་ཅིང་། ཕྱིར་འདྲེན་བྱས་ཡོད་ཚུལ་ཡང་ཞིབ་ཕྲ་ཞིབ་བཤེར་བྱས་ཡོད།

ཞིབ་བཤེར་གྲུབ་འབྲས།

༢༠༢༢ ལོའི་ནུབ་བཀྲའ་པའི་དཀྱིལ་ཙམ་ལ། ASD ཡི་ ACSC ཡིས་ཚོགས་པ་དེ་ལ་བརྟལ་བ་བཏང་སྟེ། གཞུང་གིས་རྒྱབ་སྐྱོར་བྱེད་པའི་དྲྭའི་ཚོགས་པ་ཞིག་དང་ འབྲེལ་བ་ཡོད་པར་དེས་པའི་གནོད་སྐྱེན་ཞུས་པའི་ IP གནས་སོ་ཞིག་གིས། ཀུང་མཐར་ཡང་ནུས་བའི་བྱུན་པ་ནས་བརྒྱའ་པའི་བར་དུ་ཚོགས་པ་དེའི་སྒོག་ཐུག་དྲུག་དང་འབྲེལ་བ་བྱས་ཡོད་པར་རེད། གཏོར་བརླག་ཞེབས་པའི་ཡོ་ཆས་དེ་ཡལ་ཚེར་ཚོད་ལས་རྒྱང་རྒྱང་ཞིག་ཡིན་ཡང་ཁྱེད་ཀྱིས་ཚང་གི་སྤྱོད་མཁན་ཞིག་ཡིན་པ་དང་བ་རེད།

ནུ་བ་བཀྲའ་པའི་ནུ་མཇུག་ཀུ་ASDཡི་ ACSC ཡིས་ཚོགས་པའི་དྲྭའི་ཞོག་ལ་གཙོ་སྤྱོད་ཀྱིས་མཁན་ཚོར་གཙོ་བདག་ལ་གཞི་བཅོལ་བའི་ལས་ཀྱིས་ཅིག་ བཏོད་སྤྱིས་མོལ་གྱིས་ཤུགས་རྐྱེན་ཞེབས་པའི་མངོན་གསལ་སྟོན་གྱི་ཡོད།

ཞིབ་བཤེར་གྱི་ལས་དོན་ལ་རྒྱབ་སྐྱོར་ཀྱིས་ཐུབ་པའི་དཔང་རྟགས་ཁ་ཤས་དུན་ཞིའི་སྒྲིག་ བཏོད་དམ་དྲྭའི་བཙོ་བཏོད་ཀྱི་རྐྱེན་གྱིས་ཞོན་ཐུབ་མ་སོང་། དེ་ཤུར་ཡིན་ནའང་། ཚོགས་པ་དེས་ཞོབ་ཚུབས་པའི་གནས་ཚུལ་ཡོད་ཚད་མགོ་སྒོང་ཀྱེད་ཀྱི་ཐུབ་པ་ཏ་སྒྲིག་ཀྱས་པ་དེས། ASD ཡི་ ACSC དོན་རྐྱེན་ལག་འདེབས་པ་ཚོར་ཕྱོགས་ཡོངས་ཀྱི་དབྱེ་ཞིབ་ཀྱེད་ཐུབ་པ་དང་། དྲྭའི་ཞོག་ལ་ APT40 གྱི་བྱ་སྤྱོད་འབྱུང་སྲིད་པའི་སྐོར་ལ་གཏོ་རྐོགས་ཐུབ་པ་ལྟུང་།

ཟླ་བ་དགུ་པའི་ནང་། ASD ཡི་ ACSC དང་གློས་བསྡུར་བྱས་རྗེས། ཚོགས་པ་དེས་ཞོག་ཚའི་བརྡ་ཞོའི་ནང་དོར་འཛིན་བྱས་པའི་ IP གནས་སོ་དེ་ཁས་མི་ལེན་པའི་ཞོ་ཡིག་ནང་འཇུག་པའི་ཐག་གཅོད་བྱས། ཟླ་བཅུ་པའི་ནང་ཚོགས་པ་དེས་བཅོས་སྒྲིག་བྱེད་འགོ་ཚུགས་པ་རེད།

ཞིབ་ཚ།

ཟླ་བ་བདུན་པ་ནས་བཟུང་། བྱེད་མཁན་ཚོས་ <webapp>2-ext ཞོག་ཏུ་འགོར་སྐྱོད་བྱེད་བཞིན་པའི་སྒེར་སྐུ་དྲྭའི་ཉེར་སྤྱོད་ (T1190) ཚོད་ལྟ་དང་བགོལ་སྤྱོད་བྱེད་ཐུབ་པ་རེད། དེས་ཚོགས་པ་དེ་ལ་དྲྭའི་དམག་མེད་ས་ཁུལ་ (DMZ) ནང་ཞབས་འདེགས་བཙུགས་ཐུབ་པའི་གོ་སྐབས་སྤྲད་ཡོད། འདི་དྲྭ་དང་མཐོང་ཐུབ་པའི་ཁྱབ་ཁོངས་ཚང་མ་རྩིས་རྐྱག་པར་བེད་སྤྱོད་བཏང་ཡོད། བའེ་འཛགས་ལོངས་སྤྱོད་བྱུང་བའི་ཚོག་མཚན་ཡིག་ཚ་ (T1078.002) དེ་བགོལ་སྤྱོད་བཏང་སྟེ་ཤུགས་ལྟབ་སྟོང་ཞོ་ (T1018) ལ་འདྲི་རྩད་བྱས་པ་དང་། DMZ ནང་གི་འཕྲལ་ཚས་མང་པོ་ནས་ཡིག་ཚའི་མཉམ་སྤྱོད་ (T1039) སྤྱོང་བ་བརྒྱབ་ནས་གནས་ཚུལ་ཕྱིར་འདེབ་བྱས་ཡོད། བྱེད་མཁན་གྱིས་ཞབས་ཞུ་འཕྲལ་ཚས་ནས་ཚོག་ཆེད་ཡོད་པའི་དྲྭའི་ཚོག་མཚན་ཡིག་ཚ་ཞོང་པའི་ཆེད་དུ་ Kerberoasting འཛིགས་སྐྱལ་བྱས། (T1558.003) སྟེ་ཚན་དེས་ DMZ དང་ནང་ཁུལ་གྱི་དྲྭ་གང་རུང་གི་ནང་དུ་གནས་ས་ཁ་སྤྱོད་ཞོང་པ་མཞོང་མ་སོང་།

མཚན་ཉིད་འདུས་རྒྱུག

གཤམ་གྱི་མཚན་ཉིད་འདུས་རྒྱུད་ཀྱིས་ཚོགས་པའི་དྲྭའི་ཞོག་ཏུ་མཞོང་བའི་གནོད་ཅན་གྱི་བྱེད་མཁན་གྱི་བྱ་སྤྱོད་ཀྱི་རིམ་པ་གཙོ་བོའི་སྐོར་ལ་ཡྱི་བསྟོམས་རྒྱ་ཆེ་བ་ཞིག་སྟོངས་ཡོད།

ཞོག་མའི་གསར་རྟེའུ།

ཐེབ་ཀའི་ཁྱིས་ཚོགས་པའི་ཚེད་དུ་བཙོས་པའི་ཐེབ་ཀ་ཞིག་ཡིན་པ་ཞིག་ཡིན།

གཙོ་བདག་གྲངས་སྟོན།

T1082 མ་ལག་ཚ་འཕྲིན་གསར་རྟེའུ།

གཙོ་བདག་གྲངས་སྟོན་དང་བརྟན་རྩུགས་འཇུག་པ།

ཞོག་མར་དོ་སྣང་ཐུས་པའི་ནང་འཇུལ་དེ་ཁིམས་མཐུན་གྱི་ཚོག་མཚན་ལག་ཁྱེར་ཐུབ་དེ་

དུ་བའི་རྟོག་ཞིབ།

T1021.002 ཐག་རིང་ཞབས་ཀྱ SMB/ཕེན་ཅོ་འཛིན་སྤྱོང་བགོ་བཤའ།

T1135 དྲྭའི་བགོ་བཤའ་གསར་རྟེའུ།

དྲྭར་གཞི་བཅོལ་བའི་སྤྱོན་འཚོལ་དང་ཁྱེད་མཁན་གྱི་ཐུབ་སྤྱོད་དེའི་ནང་དུ་ SMB མཉམ་སྤྱོད་སྤྱོར་བ། དྲྭར་གཞི་བཅོལ་བའི་བརྟག་དཔྱད་དང་ས་ཁྱལ་གྱི་གྲངས་སྟོན་བཅས་འདུས།

བཤུ་གཞོག

T1190 སྤྱི་དམངས་ལ་ཁ་གཏད་པའི་མཉེན་ཆས་བགོལ་སྤྱོལ།

དྲྭའི་ཉེར་སྤྱོད་བགོལ་སྤྱོད་དང་དྲྭའི་ཤེལ་སྒྲབས་གསར་སྐྱན།

གནོད་འཚེའི་འབེལ་འདྲིས།

རྒྱལ་ཁབ་ཀྱིས་རོགས་སྐྱོར་ཁྱེད་པའི་རྣང་གཞིའི་སྒྲིག་བགོད་དང་སྒྲིག་འཇུག་གཤམ་ཀྱི་འབེལ་བ་ཚོག་མར་དོ་སྣང་ཐུས།

འབེལ་མཐུད་སྒང་གསོ་ཁྱེད་པ།

T1090 བར་སྤྱོད་པ

ཁྱེད་མཁན་ཀྱིས་ ssf ལག་ཆའི་མཐུད་ལམ་སྒང་གསོ་ཐུས། (ཚོས་ཀྱངས་གཞན་ཁག་དང་མཉམ་དུ་བརྟན་པའི་ཚོས་ ২২ ཉིན་ཀྱི་ཐུ་སྤྱོད་དང་འདུ་ག།

ཞིབ་ཕྲའི་མཚན་ཉིན་འདུས་རྒྱུད།

ཟླ་བདུན་པ།: བྱེད་མཁན་ཚོས་ཚོགས་པའི་ཆེད་དུ་བཟོས་པའི་སྣེར་སྐྱ་དྲ་རྒྱའི་ཉེར་སྤྱོད་ (T1190) ཡི་མདུན་ཤོག་ལ་ཐོག་མའི་མཐུད་ལམ་བཙུགས་ཡོད། (ཕྱི་མར་'དྲ་རྒྱའི་ཉེར་སྤྱོད།' ཡང་ན་ 'webapp' ཞེས་འབོད།) སྐྱེལ་འདྲེན་བང་རིམ་བདེ་འཇགས་ (TLS) མཐུད་ལམ་ (T1102) བརྒྱུད་ནས། གཞན་ཡང་དོ་སྣང་བྱེད་འོས་པའི་བྱེད་སྒོ་གང་ཡང་མཐོང་མ་བྱུང་།

ཟླ་བདུན་པ།: བྱེད་མཁན་ཚོས་དྲ་རྒྱའི་ཉེར་སྤྱོད་ཀྱི་དྲ་ཚིགས་གྲངས་སྟོན་འགོ་ཚུགས་ཏེ་ཞིབ་འཇུག་འཕར་མ་བྱེད་རྒྱུའི་མཐར་སྣེ་འཚོལ་བཞིན་ཡོད།

ཟླ་བདུན་པ།: བྱེད་མཁན་ཚོས་མཐའ་མཚམས་དམིགས་བསལ་ཞིག་བཀོལ་སྤྱོད་བྱེད་པའི་ཐབས་ལ་ཡིད་དོ་སྣང་བྱེད་ཀྱི་ཡོད།

ཟླ་བདུན་པ།: བྱེད་མཁན་ཚོས་དྲ་རྒྱའི་ཞབས་ཞུ་འཕྲུལ་ཆས་ལ་ལེགས་འགྲུབ་དང་ POSTབཏང་ཐུབ་ཀྱི་ཡོད། འདི་ནི་ཤོག་ངོས་གཞན་ཞིག་ལ་བཞག་པའི་དྲ་རྒྱའི་སྦྲུབས་ཤིག་བརྒྱུད་ནས་ཡིན་སྲིད། IP གཉིས་པ་དེ་བྱེད་མཁན་གཅིག་པ་ཚོས་བཀོལ་སྤྱོད་བྱེད་སྲིད་པ་དེས་ཀྱང་ URL གཅིག་པ་ལ་སྤྲེལ་བ་འགོ་ཚུགས་པ་རེད། བྱེད་མཁན་ཚོས་དྲ་རྒྱའི་སྦྲུབས་ཡིན་སྲིད་པ་མང་པོ་བཟོས་ནས་ཚོད་ལྟ་བྱས།

བེད་སྤྱོད་ཉེས་པའི་ཐབས་ལམ་ངོས་འཛིན་ཐུབ་ཀྱི་མེད་ཀྱང་། དམིགས་བསལ་གྱི་མཐའ་སྣེ་དེ་ལ་ <webapp>2-extསྙིང་ལ་ཡིག་ཆ་གསར་བསྐྲུན་བྱེད་པར་དམིགས་གཏད་བཏང་ཡོད་པ་གསལ་པོ་རེད།

ASD ཡི་ ACSC ཡིས་ IP ཁ་བྱང་མཐུད་ལམ་གཉིས་དེ་དག་གི་དོ་སྣང་མཉམ་སྤྱོད་དང་དང་པོའི་མཐུད་ལམ་སྐར་མ་ཁ་ཤས་ཀྱི་བར་ཐེབས་ལ་བརྟེན་ནས་བཙན་འཛུལ་གཅིག་པའི་ཆ་ཤས་ཤིག་ཡིན་པར་ཡིད་ཆེས་བྱེད་ཀྱི་ཡོད།

ཟླ་བདུན་པ།: སྔེ་ཚན་དེས་མུ་མཐུད་དུ་གཙོ་བདག་གྲངས་འབོར་བྱེད་པ་དང་། ཐོབ་ཐང་འཕར་མའི་གོ་སྐབས་འཚོལ་བ། དྲ་རྒྱའི་སྦྲུབས་གཞན་པ་བཀོལ་སྤྱོད་བྱེད་བཞིན་ཡོད།

བྱེད་མཁན་ཚོས་ཉམས་ཞིབ་བྱས་པའི་ངོས་འཛིན་གསང་ཨང་ <firstname.surname>@<organisation domain> བེད་སྤྱོད་གཏོང་སྟེ་དྲ་རྒྱའི་ཉེར་སྤྱོད་མཉེན་ཆས་ནང་ལ་ཞུགས་པ་རེད།

བྱེད་མཁན་ཚོའི་བྱེད་སྒོ་དེས་ <webapp>2-ext ལ་ཐོབ་ཐང་འཕར་མ་ལེགས་འགྲུབ་བྱུང་མེད་པ་འདྲ། དེའི་ཚབ་ཏུ་བྱེད་མཁན་ཚོས་དྲ་རྒྱའི་ཐོག་བརྟེན་པའི་བྱེད་སྒོ་ལ་གཙོ་བོར་བཏོན་ཡོད།

ཟླ་བདུན་པ།: བྱེད་མཁན་གྱིས་ཞབས་ཞུའི་རྩིས་ཁྲའི་ཆེད་དུ་ཉམས་ཞིབ་བྱས་པའི་ངོས་འཛིན་གསང་ཨང་ཚོད་ལྟ་བྱེད་ཀྱི་ཡོད། དེ་ནི་ནང་ཁུལ་དུ་སྤྱོད་ཚོག་གི་ཀྲུར་ཁ་ གཉིས་སྐར་ནང་དུ་རྩ་བ་ནས་བྲིས་འགོད་བྱས་པ་རག་ལས་པ་ཡིན་སྲིད།

ཟླ་བདུན་པ།: བྱེད་མཁན་ཚོས་ཁ་ཕྱེ་བའི་ཐོན་ཁུངས་ལག་ཆ་ Secure Socket Funnelling བཀོལ་སྤྱོད་བྱེད་ཀྱི་ཡོད། དེ་ནི་གནོད་སྐྱེད་ཀྱི་གཞི་རྟེན་ཆ་འཕྲིན་ལ་ཕྱི་ལོགས་སུ་འབྲེལ་མཐུད་བྱེད་པའི་ཆེད་དུ་བེད་སྤྱོད་བྱས་པ་ཡིན། འབྲེལ་མཐུད་འདི་བྱེད་མཁན་གྱི་འཇིགས་སྐུལ་འཕྲུལ་ཆས་ནས་ལས་ཁུངས་ཀྱི་ནང་ཁུལ་དྲ་རྒྱ་ནང་དུ་འགྲུལ་བཞུད་སྦྲིན་པར་བེད་སྤྱོད་གཏོང་གི་ཡོད། ཁོང་ཚོས་ཞབས་ཞུའི་རྩིས་ཁྲའི་ངོས་འཛིན་གསང་ཨང་བེད་སྤྱོད་བྱེད་འབད་རྩོལ་སྐབས་འཕྲུལ་ཆས་ཀྱི་མིང་ཚོ་གཏམ་བྱུང་བོ་འགོད་ནང་མངོན་གསལ་དུ་ཐོན་འདུག

ཟླ་བརྒྱད་པ།: བྱེད་མཁན་ཚོས་ཞབས་ཞུའི་རྩིས་ཁྲ་དང་འབྲེལ་བའི་འབྲེལ་མཐུད་འཛུགས་མ་ཐུབ་པ་སོགས་ཚད་འཛིན་ཅན་གྱི་བྱེད་སྒོ་སྤེལ་བཞིན་པ་མཐོང་རྒྱུ་ཡོད།

ཟླ་བརྒྱད་པ།: བྱེད་མཁན་ཚོས་དྲ་རྒྱ་དང་ Active Directory གྱི་གྲངས་འབོར་གལ་ཆེན་པོ་སྒྲུབ་ཀྱི་ཡོད། དེ་རྗེས་DMZནང་ཁུལ་གྱི་ཕྱིན་ཊོ་འཕྲུལ་ཆས་སྟེང་ལ་བགོ་བཤའ་བཙུགས་པར་བརྟབ་གསིག་ཐེབས་པའི་རྩིས་ཁྲ་གཞན་ ཞིག་བཀོལ་སྤྱོད་བྱེད་པ་དེས་གནས་ཚུལ་མཐར་ཕྱིན་པ་བཤེར་ཐུབ་པ་བྱས།

འདི་ནི་DMZནང་དུ་སྒྲིག་ཐུབ་པའི་འཕྲུལ་ཆས་ཐོག་ལ་རྐྱ་འཕྲོག་བྱས་པའི་ཚོག་མཆན་ཐོབ་པའི་གོ་སྐབས་ལྡན་པའི་བེད་སྤྱོད་ཅིག་ཡིན་པ་འདྲ། མི་གྲུང་གིས་བྱེད་མཁན་གྱིས་ནང་ཁུལ་གྱི་དྲ་རྒྱ་ལ་དེ་འདྲའི་བྱེད་སྒོ་མཚུངས་པས་དམིགས་འབེན་བཟོ་བར་བཀག་འགོག་བྱས།

ཟླ་བརྒྱད་པ་ནས་དགུ་པ་བར། SSF ལག་ཆས་ཀྱིས་གནོད་སྐྱེད་ཀྱི་ IP ལ་འབྲེལ་མཐུད་ཡང་བསྐྱར་འཛུགས་པ་རེད། ཚོགས་པ་དེས་ཁོང་ཚོའི་འཛུལ་ཞུགས་བཀག་འགོག་མ་བྱས་བར་དུ་ཁ་སྟོན་གྱི་བྱ་འགུལ་གང་ཡང་བསྒྲུབ་བཞིན་ཡོད་པར་དོ་སྣང་བྱེད་ཀྱི་མེད།

ཟླ་དགུ་པ།: ལས་ཁུངས་ཀྱིས་ཁོང་ཚོའི་མི་གྲུང་ཐོག་ལ་འགོག་ཐོའི་ནང་བཙུག་སྟེ་གནོད་སྐྱེད་ཀྱི་ IP དེ་བཀག་འགོག་བྱེད་ཀྱི་ཡོད།

2 འདི་ལྟའི་གནད་དོན་ནང་ལ་མཐའ་མཚམས་ཞེས་པ་ནི་དྲ་རྒྱའི་ཉེར་སྤྱོད་མཉེན་ཆས་ཀྱི་ལས་འགན་ཞིག་རེད།

3 ཞབས་ཞུའི་རྩིས་ཁྲ་དེ་སྤྱོད་མཁན་རེ་རེ་ལ་འབྲེལ་བ་མེད་པར་ཞབས་ཞུ་ལ་འབྲེལ་བ་ཡོད། མའི་ཀྲོ་སོ་སོཕཊ་ཚོང་ལས་ཁྱབ་ཁོངས་ནང་ལ་རྩིས་ཁྲ་སྣ་ཚོགས་ཡོད།

4 བགོ་བཤའ་སྒྲིག་སྦྱོར་བྱེད་པ་ནི་ཡིག་ཆ་མ་ལག་གི་བཀོད་སྒྲིག་ཐོག་གི་ཡིག་ཆ་ཚོ་སྤྱོད་མཁན་ཡང་ན་སྤྱོད་མཁན་སྡེ་ཚན་ལ་སྤྱོད་ཚོག་པར་བཟོ་བའི་བྱ་རིམ་ཞིག་ཡིན།

བྱེད་མཁན་གྱི་བྱེད་སྤྱད་དང་ཐབས་ཤེས།

MITRE ATT&CK གཞི་སྒོམ་ནི་དྲ་རྒྱའི་བར་སྐང་ནང་འཛིགས་སྐུལ་བྱེད་མཁན་གྱིས་བཀོལ་སྤྱོད་བྱེད་པའི་བྱེད་སྤྱངས་དང་ཐབས་ཤེས་ཀྱི་ཡིག་ཆོག་ཏུ་བཀོད་པའི་བསྡུ་རྩྭ་ཅིག་རེད། གཞི་སྒོམ་དེ་ཚ་རིའི་ཁེ་ལས་མ་ཡིན་པའི་ཚོགས་པ་ MITRE Corporation གིས་བཟོས་པ་དང་། འཛིགས་སྐུལ་བྱེད་མཁན་གྱི་སྤྱོད་ལམ་སྐོར་འཛམ་གླིང་ཡོངས་ལ་མཉམ་སྤྱོད་བྱེད་པའི་སྐད་རིགས་ཞིག་གི་བྱེད་ལས་སྒྲུབ་ཀྱི་ཡོད།

ASD ཡི་ ACSC ཡིས་གཤམ་གསལ་གྱི་ཐབས་ཤེས་དང་བྱེད་སྤྱངས་དེ་དག་བྱེད་མཁན་གྱི་གཞོད་སྐྱེད་ཀྱི་བྱ་སྤྱོད་དང་འབྲེལ་བ་ཡོད་པར་དབྱེ་ཞིབ་བྱེད་ཀྱི་ཡོད།

རྟོག་ཞིབ།

T1594 – གཞོད་འཚེ་ཡོག་མཁན་གྱིས་བདག་གཞེར་བྱེད་པའི་དྲ་ཚིགས་འཚོལ་ཞིབ།

བྱེད་མཁན་གྱིས་དྲ་རྒྱ་ལ་འཚུལ་ཞུགས་བྱེད་པའི་གོ་སྐབས་ངོས་འཛིན་བྱེད་ཆད་སྤྲིག་བཅོས་དྲ་རྒྱའི་ཉེར་སྤྱོད་མཉེན་ཆས་ཀྱི་དྲ་ཚིགས་དེ་གང་འབོར་བྱས།

ཐོག་མའི་ཚོག་མཆན།

T1190 – སྤྱི་དམངས་ལ་ཁ་གཏད་པའི་མཉེན་ཆས་བེད་སྤྱོད་གཏོང་བ (སྒྲིག་བཅོས་དྲ་རྒྱའི་ཉར་སྤྱོད་མཉེན་ཆས་བེད་སྤྱོད་གཏོང་བ་དང་འབྲེལ།)

T1078.002 – ནུས་ལྡན་ཅིས་ཐུབ། ཁྱབ་ཁོངས་ཀྱི་ཅིས་ཐུབ (ཉེས་པ་ཅན་གྱི་ཐོ་འཇུག་ཡིག་ཆ་སྤྱད་དེ་ཞུགས་པའི་སྐོར།)

དྲ་རྒྱའི་ཐོག་ལ་མཐོན་པའི་སྟོལ་རྒྱུན་གྱི་དྲ་རྒྱའི་མཉེན་ཆས་བཀོལ་སྤྱོད་བྱེད་པ་དེས་འཁབ་སྐྱེན་པ་ལ་འགོ་འཛུགས་ཀྱི་འཛུལ་ཞུགས་བྱེད་ས་འི་ས་ཚོགས་ཤིག་མཁོ་སྤྱོད་བྱས། རྒྱུད་སྐུལ་བ་དེས་ཕྱིས་སུ་ཁོང་ཚོས་ཉེས་པར་བཤད་བའི་ཐོ་འཇུག་ཡིག་ཆ་དེ་དག་བེད་སྤྱད་ཀྱིས་དྲ་རྒྱའི་ནང་དུ་ཁོང་ཚོའི་འཚང་འབྲེན་དེ་ཐུར་ལས་རྒྱ་ཆེར་གཏོང་ཐུབ་སོང་།

ལག་བསྟར།

T1059 – བཀའ་ཚོག་དང་ཡིག་ཆའི་སྐད་སྒྲུར་བྱེད་མཁན། (དྲ་རྒྱའི་ཁབ་ལེན་བརྒྱུད་ནས་བཀའ་ཚོག་ལག་བསྟར་བྱེད་པའི་སྐོར་)

T1072 – མཉེན་ཆས་བཀོལ་སྤྱོད་ལག་ཆ། (IP ལ་མཐུད་པའི་ཆེད་དུ་ཁ་ཕྱེ་བའི་ཐོན་སྒྲུབ་ལག་ཆ་ Secure Socket Funneling (SSF) བེད་སྤྱོད་བྱེད་མཁན་གྱི་འཁྲབ་སྟོན་པ་ལ་འབྲེལ་བ།)

བརྟན་པོར་གནས་པ

T1505.003 – ཞབས་ཞུའི་མཉེན་ཆས་ཆ་ཤས། དྲ་རྒྱའི་ཁོག་ལེན། (དྲ་རྒྱའི་ཁོག་ཁོག་དང་SSFབེད་སྤྱོད་བྱས་ནས་འཛུལ་སྤྱོད་བྱེད་པའི་སྐོར།)

ཚོག་མཆན་ཐོབ་ཐང་།

T1552.001 – གསང་ཚང་མཇོད་ཁང་ནས་ཐོབ་ཐང་ཡིག་ཚ། (ཁང་པའི་འཛིན་སྐྱོང་མ་ལག་(BMS)དང་འབྲེལ་བའི་གསང་ཚང་ཡིག་ཆའི་སྐོར།)

T1558.003 – ཀར་ཉེ་རོས་ཀྱི་འཛིན་བྱང་ཀུ་བའམ་རྩྭ་བཟོ་བྱེད་པ། ཀེར་བེ་རོས་ཏིང་། (དྲ་རྒྱའི་ཐོབ་ཐང་ཡིག་ཆ་ཐོབ་པའི་ཚེད་དུ་བྱས་པའི་འཐབ་རྩོད་ཀྱི་སྐོར།)

ཕྱོགས་གཅིག་ཏུ་འགུལ་སྐྱོད་བྱེད་པ།

T1021.002 – ཐག་རིང་ཞབས་ཞུ། SMB བཀོ་བཤད། (རྒྱུད་སྐུལ་བས་ཡོ་བྱད་མང་པོ་ནས་SMB བཀོ་བཤད་འཇུག་པའི་སྐོར།)

སོར་སྟུག

T1213 – བརྡ་འཕྲིན་མཐོ་ཁང་ནས་གནས་རྒྱུས་ཚུལ། (BMS ཞབས་ཞུ་འཕྲུལ་ཆས་ཐོག་ནས་རྩེད་པའི་ལག་དེབ་/ཡིག་ཆ་ཁག་གི་སྐོར།)

ཕྱིར་འཐེན་བྱེད་པ།

T1041 – C2 བརྒྱུད་ལམ་བརྒྱུད་ནས་ཕྱིར་འཐེན་བྱེད་པ་ (འཁྲབ་སྟོན་པའི་གནས་ཚུལ་དེ་Active Directory ནས་ཕྱིར་འཐེན་བྱེད་པ་དང་བཀོ་བཤད་སྒྲིག་པའི་སྐོར་ལ་)

དཔེ་མཚོན་ཞིབ་འཇུག་གཉིས་པ།

སྙན་ཐོ་འདི་ཁྱབ་བསྒྲགས་རྒྱ་ཆེ་རུ་གཏོང་ཆེད་མིང་མ་བཀོད་པར་བཟོས་ཡོད། ཤུགས་རྐྱེན་ཐེབས་པའི་ཚོགས་པ་དེ་ཕྱི་མ་ནས་'ཚོགས་པ་དེ་'ཞེས་བརྗོད་པར་བྱའོ། ཚོར་བའི་མི་དང་ ASD གི་ ACSC ཡི་གནས་ཚུལ་ལན་འདེབས་ཐབས་ལམ་གྱི་ངོ་བོ་སྲུང་སྐྱོབ་བྱེད་པའི་ཆེད་དུ་དམིགས་བསལ་གྱི་ཞིབ་ཕྲའི་གནས་ཚུལ་འགའ་ཤས་བསུབ་ཡོད།

འཆར་གཞི་བདག་པོའི་བསྡུས་དོན།

སྙན་ཐོ་འདིས་ ༢༠༢༢ ལོའི་ཟླ་ ༩ པར་ཚོགས་པ་དེའི་དྲ་རྒྱ་ལ་མཐར་ཕྱིན་པའི་ཉེས་འཆར་བཏང་བ་ལ་ ASD ཡི་ ACSC གིས་ཞིབ་འཇུག་བྱས་པའི་མཐའ་འབྲས་ཞིབ་ཕྲ་བཀོད་ཡོད། བརྟག་དཔྱད་སྙན་ཞུ་འདི་ཚོགས་པ་དེ་ལ་དོ་སྣང་བྱུང་བའི་གནོད་འཚེ་ཅན་གྱི་བྱ་སྤྱོད་སྟེང་བསྡུས་དང་བཅོས་སྒྲིག་གི་གྲོས་འཆར་བཟོ་ཆེད་དུ་སྤྲད་ཡོད། ཞིབ་བཤེར་གྱི་འབྲས་བུ་ལྟར་ན་ བདེ་འཇགས་དེ་ APT40 ཡིས་ལོངས་བཅམ་བྱས་པ་ཡིན།

༢༠༢༢ ལོའི་ཟླ་ ༥ པར་ ASD ཡི་ ACSC གིས་ཚོགས་པ་ཞིག་ལ་ ༢༠༢༢ ལོའི་ཟླ་ ༩ པ་ནས་བཟུང་ཚོགས་པ་དེའི་དྲ་རྒྱ་ལ་ ཤུགས་རྐྱེན་སྤྲད་པའི་ཐེ་ཚོམ་ཅན་གྱི་གནོད་འཚེ་ཅན་གྱི་བྱ་སྤྱོད་ཀྱི་སྐོར་བརྡ་སྤྲོད་ཞུས། དེ་རྗེས་ཚོགས་པ་དེས་ ASD ཡི་ ACSC ལ་ཁོང་ཚོས་དྲ་རྒྱའི་ཐོག་ལ་ཁ་གཏད་པའི་ཞབས་ཞུ་འཕྲུལ་ཆས་ཤིག་གི་སྟེང་དུ་གནོད་འཚེ་ཅན་གྱི་མཉེན་ཆས་རྙེད་ཡོད་པ་དང་། ཞབས་ཞུ་འཕྲུལ་ཆས་དེས་ཚོགས་པ་དེའི་ཁང་པའི་རྒྱུང་རིང་འཚང་འདྲེན་གྱི་ཐབས་ལམ་གྱི་ཐོ་འཇུག་སྒོ་འཕྲུལ་ཁྱུང་མགོ་སྤྲོད་བྱེད་ཀྱི་ཡོད་པའི་གནས་ཚུལ་བརྗོད་ཡོད། ཞབས་ཞུ་འཕྲུལ་ཆས་འདིས་རྒྱང་རིང་འཚང་འདྲེན་ཐོ་འཇུག་དང་ངོ་བོ་འཛིན་སྐྱོང་གི་ཐོན་རྫས་བེད་སྤྱོད་བྱས་ཡོད་ལ། སྙན་ཐོ་འདིའི་ནང་དུ་འདི་ལ་'ཉེས་པར་བཏང་བའི་ཡོ་བྱད་'ཞེས་བརྗོད་རྒྱུ་ཡིན། སྙན་ཐོ་འདིས་ASDཡི་ACSCཡིས་སྤེལ་བའི་ཞིབ་བཤེར་ལ་ལན་འདེབས་བྱེད་པའི་ཆེད་དུ་སྒྲིག་འཛུགས་ལ་ཞིབ་བཤེར་གྱི་ཤེས་རྟོགས་དང་བཅོས་སྒྲིག་བྱེད་པའི་བསླབ་བྱ་ཞིབ་ཕྲ་བཀོད་ཡོད།

དཔང་རྟགས་ཀྱིས་སྒྲིག་འཛུགས་ཀྱི་དྲ་རྒྱའི་ཆ་ཤས་ཤིག་ཉུང་མཐར་ཡང་༢༠༢༢ལོའི་ཟླ་བ་བཞི་པ་ནས་བཟུང་སྒྲིག་འཛུགས་ཀྱི་ཐག་རིང་ནས་འཛུལ་ཞུགས་བྱེད་པའི་ནང་འཛུལ་དུ་ཚིགས་བརྒྱུད་ནས་དྲ་རྒྱའི་བྱེད་པོ་ངན་པ་ཚོས་གཏོར་བརླག་བཏང་ཡོད་པའི་བརྡ་སྟོན་གྱི་ཡོད། ཞབས་ཞུ་འཕྲུལ་ཆས་འདི་ལ་རྒྱུད་སྐྱུལ་བ་མང་པོས་ཉེས་འཆར་བཏང་ཡོད་སྲིད་ལ། ཉེས་འཆར་བཏང་བའི་དུས་ཚོད་དེའི་སྐབས་ལ་ཁྱབ་བསྒྲགས་ཆེན་པོ་བྱས་པའི་རྒྱང་རིང་ནས་བཀོད་རིས་ལག་བསྟར་བྱེད་པའི་ (RCE) སྐྱོན་ཆ་དེས་ཤུགས་རྐྱེན་ཐེབས་ཡོད་ངེས་ཅན་ཆགས་ཡོད།

ASD ཡི་ ACSC ཡིས་དོ་སྣང་བྱས་པའི་རྒྱུད་སྐྱུལ་བ་གཙོ་བོའི་བྱེད་སྒོ་ནང་དུ།

- ཡོ་ཆས་གྲངས་འགོར་བྱས་པ། དེས་འཁྲབ་སྟོན་པ་ཞིག་ལ་དྲ་རྒྱའི་ས་ཁྲ་རང་ཉིད་གསར་བཟོ་བྱེད་ཐུབ།
- དྲ་རྒྱའི་ཐོག་ལ་ཁ་གཏད་པའི་གློག་ཀླད་ཉེར་སྤྱོད་དང་དྲ་རྒྱའི་ཁབ་ལེན་བེད་སྤྱད་བྱས་པས་རྒྱུད་སྐྱུལ་བ་ལ་དྲ་རྒྱའི་ནང་དུ་ཐོག་མའི་ཀ་རྟེན་དང་བཀའ་ཚིག་ལག་བསྟར་བྱེད་པའི་ནུས་པ་སྤྲད་ཡོད།
- མཉེན་ཆས་ཀྱི་སྐྱོན་ཆ་བེད་སྤྱད་ཀྱིས་དབང་ཆ་མཐོར་སྤོ་བ། དེ་བཞིན།
- ཕྱོགས་གཅིག་ནས་འགུལ་སྐྱོད་བྱེད་ཐུབ་པའི་ཡིག་ཆ་བསྡུ་རུབ།

༢༠༢༢ ལོའི་ཟླ་ ༩ པར་ ASD ཡི་ ACSC ཡིས་གནོད་འཚེ་ཅན་གྱི་རྒྱུད་སྐྱུལ་བ་ཞིག་གིས་ཉེས་པར་བཏང་བའི་ཡོ་བྱད་ཐོག་ནས་སྤྱོད་མཁན་གྱི་མིང་དང་གསང་ཨང་གྱི་ཆ་གཅིག་མི་འདྲ་བ་བརྒྱ་ཕྲག་མང་པོ་ཕྱིར་འཐེན་བྱས་པ་དང་། དེ་བཞིན་རྣམ་གྲངས་མང་པོའི་ངེས་འདེམས་ལམ་ཁ་ཤས་ཀྱི་གསང་ཨང་དང་རྒྱང་རིང་འཚང་འདྲེན་གྱི་ཐེངས་དང་འབྲེལ་བའི་རིག་གནས་ལོ་རྒྱུས་ཀྱི་དངོས་པོ་ཁ་ཤས་ཀྱང་ཤེས་རྟོགས་བྱུང་བ་རེད། ཚོགས་པ་དེས་བསྐྱར་ཞིབ་བྱས་རྗེས་གསང་ཨང་དེ་དག་ཁྲིམས་མཐུན་ཡིན་པ་ཤེས་རྟོགས་བྱུང་ཡོད། ASD ཡི་ ACSC ཡིས་རྒྱུད་སྐྱུལ་བ་དེས་ཁྲིམས་མཐུན་སྤྱོད་མཁན་ཞིག་ལྟར་རྒྱང་རིང་ཐོ་འཇུག་གི་ཐེངས་འཕྲོག་པའམ་གསར་བཟོ་བྱེད་ཆེད་དང་། ཁྲིམས་མཐུན་སྤྱོད་མཁན་གྱི་རྩིས་ཁྲ་བེད་སྤྱད་ཀྱིས་ཚོགས་པ་དེའི་ནང་ཁུལ་གྱི་ལས་ཁུངས་དྲ་རྒྱ་ལ་འཚང་འདྲེན་བྱེད་ཆེད་དུ་རིག་གནས་ལོ་རྒྱུས་ཀྱི་དངོས་པོ་དེ་དག་བསྡུ་རུབ་བྱས་ཡོད་སྲིད་པའི་དཔྱད་པ་བྱས་ཡོད།

ཞིབ་བཤེར་གྲུབ་འབྲས།

ཞིབ་བཤེར་གནད་བསྡུས།

ASD ཡི་ ACSC ཡིས་རྒྱུད་སྐྱེལ་བ་དེས་ཚོགས་པའི་ལས་བྱེད་པ་ཚོར་རྒྱང་རིང་ཐོ་འཇུག་གི་ཐེངས་མཐོ་སྤྱོད་བྱེད་པའི་ཡོ་བྱད་ལ་ཉེས་འཆར་བཏང་ཡོད་པ་གཏན་འཁེལ་བྱས་ཡོད་ལ། ཉེས་འཆར་འདི་བེད་སྤྱད་ཀྱིས་མུ་མཐུད་དུ་བྱ་གཞག་གཞན་སྒྲུབ་པའི་རྩོལ་བ་བྱས་ཡོད། འཕྲུལ་ཆས་འདི་དག་ལ་ལྡེད་ཚད་འདྲ་མཉམ་གྱི་མགྲོན་ཁང་གསུམ་ཡོད་ཅིང་། དེ་དག་ལ་བདེ་འཇགས་ཀྱི་དཔང་རྟགས་སྔ་ཤོས་ཤེས་རྟོགས་བྱུང་ཡོད། ལས་ཁུངས་དེས་ཐོག་མའི་ཉེས་འཆར་བྱུང་རྗེས་མགྱོགས་པོ་ཁུར་སྒྲིལ་སྒོམས་པོ་བྱས་པའི་གཙོ་འཁྲིད་འཕྲུལ་ཆས་གསུམ་གྱི་ནང་ནས་གཉིས་སྒོ་རྒྱག་ཡོད། དེའི་གྲུབ་འབྲས་སུ་རྗེས་མའི་བྱེད་སྒོ་ཚང་མ་གཙོ་བདག་གཅིག་གི་སྟེང་དུ་བྱུང་ཡོད། བཙུབ་གསིག་ཐེབས་པའི་ཡོ་ཆས་དང་འབྲེལ་བའི་སར་བར་གཞན་པ་རྣམས་ཀྱང་དེ་དང་འདྲ་བའི་ཐོག་ནས་ལྡེད་ཚད་འདྲ་མཉམ་བཟོས་ཡོད། ཀློག་བདེ་བའི་ཆེད་དུ་སྙན་ཐོ་འདིའི་ཆ་ཤས་ཕལ་ཆེ་བའི་ནང་དུ་ཉེས་པར་བཏང་བའི་ཡོ་བྱད་ཚང་མ་ལ་‘ཡོ་བྱད་གཅིག་པུ’ཞེས་བརྗོད་ཡོད།

བྱེད་པོ་དེས་2022 ལོའི་ཟླ་བ་བཞི་པ་ནས་བཟུང་། ཉམས་ཆགས་འགྱུར་བའི་ལག་ཆ་དེའི་ནང་དུ་དྲ་རྒྱའི་ཤེལ་སྒྲུབས་འཇོག་པར་མི་མང་ལ་ཤེས་རྟོགས་ཡོད་པའི་རྨས་སྐྱོན་བེད་སྤྱོད་བྱས་པར་ཡིད་ཆེས་བྱེད་ཀྱི་ཡོད། སྡེ་ཚན་དེའི་ནང་ནས་འཛིགས་སྐུལ་བྱེད་མཁན་ཚོས་འཕྲུལ་ཆས་དེའི་ཐོག་ལ་ཐོབ་ཐང་ཆེ་རུ་བཏང་ཡོད་པར་བརྟག་དཔྱད་བྱེད་ཀྱི་ཡོད། ASD ཡི་ ACSC གིས་ཟིན་ཐོ་འདེབས་སྐུལ་མེད་པའི་རྒྱུ་མཚན་གྱིས་བྱ་བའི་ཁྱབ་ཁོངས་ཆ་ཚང་གཏན་འབེབས་བྱེད་ཐུབ་མེད། གང་ལྟར་ཡང་ཡོ་ཆས་དེའི་ཐོག་གི་དཔང་རྟགས་ཀྱིས་བྱེད་པོ་ཞིག་གིས་གཤམ་གསལ་གྱི་གྲུབ་འབྲས་ཐོབ་ཡོད་པའི་བརྡ་སྟོན་གྱི་ཡོད།

- དངོས་གནས་སྤྱོད་མཁན་གྱི་མིང་དང་གསང་ཨང་ཟུང་འབྲེལ་བརྒྱ་ཕྲག་མང་པོ་བསྡུ་ལེན། དང་
- ལག་རྩལ་གྱི་དངོས་པོ་བསྡུ་རུབ་བྱས་པ་དེས་གནོད་འཚེ་ཅན་གྱི་འཁྲབ་སྟོན་པ་ཞིག་ལ་ཁྲིམས་མཐུན་གྱི་སྤྱོད་མཁན་ཞིག་ཡིན་པའི་ཆ་ནས་གཟུགས་བརྙན་གྱི་ཡིག་ཆའི་རྨང་གཞིའི་སྒྲིག་བཀོད་(VDI)ཀྱི་ཚོགས་འདུ་ལ་འཛུལ་ཐུབ་པ་བྱས་ཡོད་སྲིད།

ASD ཡི་ ACSC གིས་བྱེད་པོ་དེས་སྒྲིག་འཛུགས་ཀྱི་དྲ་རྒྱའི་མཐུན་རྐྱེན་ལ་དམ་འདུམ་ཇེ་ཆེར་གཏོང་རྒྱུ་ཡིན་པར་བརྟག་དཔྱད་བྱེད་ཀྱི་ཡོད། བྱེད་པོས་ཕྱིར་འདོན་བྱས་པའི་དངོས་རྫས་དེ་དག་གིས་ཁོང་ཚོར་ཁྲིམས་མཐུན་སྤྱོད་མཁན་ཞིག་གི་ཆ་ནས་རྟོག་བྲལ་ཅོག་ངོས་ཀྱི་ལས་ཚན་བཅན་འཕྲོག་བྱེད་པའམ་འགོ་འཛུགས་བྱེད་པའི་གོ་སྐབས་སྤྲད་ཡོད་སྲིད། དེ་ཡང་ཁོང་ཚོས་འདེམས་པའི་སྤྱོད་མཁན་ཞིག་གི་ཆ་ནས་ཏེ། འཛིན་སྐྱོང་བ་ཚུད་པ་རེད། བྱེད་པོས་འཛུལ་ཞུགས་བྱེད་ཐབས་འདི་བེད་སྤྱད་དེ་སྒྲིག་འཛུགས་ཀྱི་ཞབས་ཞུ་ལ་སྔར་ལས་ལྷག་པའི་དམ་འདུམ་གཏོང་ནས་རིང་པོར་གནས་ཐུབ་པ་དང་དམིགས་ཡུལ་གཞན་དག་སྒྲུབ་ཐུབ་ཀྱི་རེད།

མགྲོན་ཁང་མཐོ་སྤྱོད་བྱེད་མཁན་གྱིས་དོ་དམ་བྱེད་པའི་ཁོར་ཡུག་ནང་དུ་སྒྲིག་འཛུགས་ཀྱི་འཕྲུལ་ཆས་གཞན་པས་དམ་འདུམ་ཞུགས་པའི་དཔང་རྟགས་སྟོན་མེད།

ལྟ་སྤྱོད།

དམ་འདུམ་ཞུགས་པའི་འཕྲུལ་ཆས་ཡོད་པའི་མགྲོན་འཁྱེར་དེས། VDI ལས་ཚན་དང་འབྲེལ་བ་འཁྲིག་བཞིན་པའི་སྤྱོད་མཁན་རྣམས་ལ་ Active Directory དང་དྲ་རྒྱའི་ཞབས་འདེགས་བརྒྱུད་ནས་ངོས་འཛིན་ཞིབ་བཤེར་སྤྲད་ཡོད། (T1021.001)

གནས་ཡུལ།	བཙུབ་གསིག་ཐེབས་པའི་ཡོ་ཆས་གཙོ་གཉེར་མིང་། (ལྡེད་ཚད་འདྲ་མཉམ།)
གཞི་གྲངས་ལྟེ་གནས་1	HOST1, HOST2, HOST3

འཕྲུལ་ཆས་ཀྱི་རྨང་གཞིའི་སྒྲིག་བཀོད་ནང་ལ་འཛུལ་སྒོའི་སྒོ་ཕྱེ་སའི་མགྲོན་འཁྱེར་ཡང་ཚུད་ཡོད། དེས་སྤྱོད་མཁན་གྱིས་འཕྲུལ་ཆས་ནས་བཟོས་ཏེ་ཕབ་ལེན་བྱས་པའི་ངོས་འཛིན་རྟགས་བུ་ཐོབ་པའི་རྗེས། ཁོང་ཚོར་VDI ལ་ཕྱུག་ལམ་མཐོ་སྤྱོད་བྱེད་ཀྱི་ཡོད།

གཙོ་སྐྱོང་པ་དེ་དག་ལས་གང་རུང་གིས་བདེ་འཇགས་བཟོས་པའི་དཔང་རྟགས་གང་ཡང་མེད། ཡིན་ནའང་། འཛུལ་སྒོའི་སྒོ་སྒྲིག་གཙོ་བོའི་དྲན་ཐོ་དེས་ཤེས་རྟོགས་བྱུང་བའི་IPཁ་བྱང་ངན་པ་དང་འབྲེལ་བ་གལ་ཆེན་པོ་ཡོད་པའི་དཔང་རྟགས་སྟོན་ཡོད། འདིས་གཙོ་བདག་འདིའི་སྟེང་དུ་བྱུང་བའི་བྱ་འགུལ་དེ་བསྟན་ཡོད་སྲིད། ཡང་ན་གཙོ་བདག་འདི་ལ་སླེབས་པའི་འཇིགས་སྐུལ་བྱེད་མཁན་གྱི་རྨང་གཞིའི་སྒྲིག་བཀོད་དང་དྲ་རྒྱའི་འབྲེལ་བ་དེ་བསྟན་ཡོད་སྲིད། བྱ་གཞག་འདིའི་རང་བཞིན་དེ་ཡོད་པའི་དཔང་རྟགས་བཀོལ་ནས་གཏན་འབེབས་བྱེད་ཐུབ་ཀྱི་མེད། འོན་ཀྱང་ཚོགས་སྡེ་དེས་སྒྲིག་འཛུགས་ཀྱི་དྲ་རྒྱའི་ནང་ངོས་ཕྱོགས་སུ་སྒོ་བར་འབད་བརྩོན་བྱེད་ཀྱི་ཡོད་པའི་བརྡ་སྟོན་གྱི་ཡོད། (TA0008)

ནང་ཁུལ་གྱི་གཙོ་སྐྱོང་པ།

ASD ཡི་ ACSC གིས་ནང་ཁུལ་གྱི་སྒྲིག་འཛུགས་ཀྱི་དྲ་རྒྱའི་ཆ་ཤས་ནས་ཚད་གཞི་ཆུང་བའི་གནས་ཚུལ་ཞིབ་འཇུག་བྱས། ནང་ཁུལ་གྱི་སྒྲིག་འཛུགས་ཀྱི་དྲ་རྒྱའི་ཆ་ཤས་ལ་ཤུགས་རྐྱེན་ཐེབས་པར་ཤེས་པའི་གནོད་འཚེ་ཅན་གྱི་བྱ་སྤྱོད་ལ་འབད་བརྩོན་བྱས་པའམ་གྲུབ་འབྲས་ཐོབ་པ་དེའི་ནང་། བྱེད་པོས་VDI དང་འབྲེལ་བའི་དངོས་རྫས་ལ་འཛུལ་ཞུགས་བྱེད་པ་དང་། ནང་ཁུལ་གྱི་SQL ཞབས་འདེགས་པ་ལ་གཏུབ་རི་བྱེད་པ། (T1505.001) དེ་བཞིན་གནོད་འཚེ་ཅན་གྱི་IP ཁ་བྱང་ནས་འཛུལ་སྒོའི་སྒོ་ཕྱེ་སའི་འཕྲུལ་ཆས་བརྒྱུད་དེ་འགྲོ་བཞིན་པའི་བཤད་མེད་པའི་འགྲུལ་བཞུད། (TA0011) བཅས་ཚུད་ཡོད།

དམ་འདུམ་ཞུགས་པའི་འཕྲུལ་ཆས་ལ་འཛུལ་ཞུགས་བྱེད་ཐབས་བེད་སྤྱོད་བྱས་ནས། ཚོགས་སྡེ་དེས་དངོས་གནས་སྤྱོད་མཁན་གྱི་མིང་དང་གསང་ཨང (T1003)། དེ་བཞིན་MFA རྟགས་བུའི་རིན་ཐང་ (T1111) བཅས་བསྡུ་ལེན་བྱས། ཚོགས་སྡེ་དེས་JSON དྲ་རྒྱའི་རྟགས་བུ་ (JWTs) (T1528) ཡང་བསྡུ་ལེན་བྱས། འདི་ནི་རྟོག་བྲལ་ཅོག་ངོས་ཀྱི་ནང་འཛུལ་ལས་ཚན་གསར་འཛུགས་བྱེད་པར་བེད་སྤྱོད་བྱེད་པའི་ངོས་འཛིན་དངོས་རྫས་ཞིག་རེད། བྱེད་པོ་དེས་འདི་དག་བེད་སྤྱོད་བྱས་ནས་རྟོག་བྲལ་ཅོག་ངོས་ཀྱི་ལས་

ཚན་ (T1563.002) བཟོ་བའམ་བཙན་འཕྲོག་བྱེད་ཐུབ་པ་དང་། ཁྱིམས་མཐུན་སྤྱོད་མཁན་ཞིག་གི་ཚ་ནས་ནང་ལྷུམ་གྱི་སྒིག་འཇུག་དུ་རྒྱའི་ཚ་ཤས་ལ་འཇུལ་ཞུགས་བྱེད་ཐུབ་པ་ཡིན་སྲིད། (T1078)

དེ་བཞིན་འཁྲབ་སྟོན་པ་དེས་སྒིག་འཇུག་ལུལ་དུ་རྒྱའི་ནང་དུ་ཡོད་པའི་ SQL ཉར་བར་(T1505.001) བཀོག་པར་བརྟབ་གཞིག་ཐེབས་པའི་ཡོ་ཚས་དེ་ལ་འཇུལ་ཞུགས་བྱས། བྱེད་པོ་དེས་གནས་ཚུལ་འདི་ལ་འཇུལ་ཞུགས་བྱེད་ཐུབ་པ་ཆེ།

འཇུལ་སྒོའི་སྒོ་ཕྱེ་འཕྲུལ་ཚས་ནས་ཐོབ་པའི་དཔང་རྟགས་ནི། དྲ་རྒྱའི་འགྲུལ་བཞུད་ཀྱི་སྐབས་ལ། འཕྲུལ་ཚས་འདི་བརྒྱུད་པ་དང་ ཡང་ན་འཕྲུལ་ཚས་འདི་ལ་ཕྱི་ཕྱག་གི་བྱུང་བའི་ཐོག་ནས་ཡིན་ཐུབ་པ་ཅིའི་ཕྱིར་ཞེ་ན། ཁོང་ཚོས་ཐོག་མར་ IP ཁ་བྱང་ནས་འགྲོ་བའི་གནས་ཚུལ་གསལ་སྟོན་བྱས་ཡོད། འདིས་དྲ་རྒྱའི་ཐོག་གི་བྱ་སྤྱོད་དབ་པ་ཚོས་འཕྲུལ་ཚས་འདི་ལ་ཤུགས་རྒྱུན་ཞུན་ཐེབས་པ་དང་ཡང་ན་ཅེད་སྤྱོད་བྱས་པ། འདིའི་ཐོག་ལས་ཕྱི་ཕྱག་ལས་ནང་གི་དྲ་བ་ནང་འཇུག་བྱེད་པའི་ཁོངས་འགོག་བྱས་པའམ། ཡང་ན་རྒྱུ་མཚན་ཡོད་པའི་སྟོན་རྟགས་སྟོན་པའི་ཉིན་རིམ་ཀྱི་སྒོ་ནོར་ཡིན་སྲིད།

ཞིབ་བཟེར་དུས་ཚོད།

གཤམ་ཀྱི་ཐོ་གཞུང་འདིས་ཞིབ་བཟེར་བྱེད་སྐབས་ཤེས་རྟོགས་བྱུང་བའི་གལ་ཆེའི་བྱེད་སྒོ་ཁག་གི་དུས་ཚོད་བགོད་ཡོད།

དུས་ཚོད།	དོན་ཚིག།
༢༠༢༢ ལྷ་ ༥	ཤེས་རྟོགས་བྱང་བའི་གནོད་བཚོ་ཅན་ཀྱི་IP ཁ་བྱང་རྒྱ་ནས་འཇུལ་སྒོའི་གཙོ་བའག HOST7 དང་འབྲེལ་བ་བྱས་པའི་གནས་རྒྱལ་ཡོད། འབྲེལ་འབྲིས་ཀྱི་རང་བཞིན་གཏན་འབེབས་བྱེད་ཐུབ་ཀྱི་ཞེད།
༢༠༢༢ ལྷ་ ༥	གཙོ་བའག་ཚང་མ་— HOST1, HOST2 དང་ HOST3 — ལ་གནོད་བཚོ་ཅན་ཀྱི་འཁྲབ་སྟོན་པ་ཡང་ན་འཁྲབ་སྟོན་པ་ཚོས་ཤུགས་ཉེན་ཐེབས་པ་དང་། དྲ་སྒོགས་ཤལ་རྒྱ་གཙོ་བའག་དེར་བཙུགས་པའི་གནས་རྒྱལ་ཡོད། HOST2 ཐོག་ལ་དྲན་ཐོ་ཡིག་ཆ་ཞིག་གསར་བཟོ་བྱས་པའམ་ཡང་ན་བསྒྱར་བཅོས་བྱས། ཡིག་ཆ་འདིའི་ནང་དུ་བྱ་སྤྱོད་དན་པ་ཞིག་གིས་འཛིན་བཟུང་བྱས་པའི་ཚོག་མཆན་འབྲི་ཡིག་ཡོད་པའི་ཉིན་རིམ་ཀྱི་སྒོ་ནོར་ཡིན། /etc/security/opasswd དང་ /etc/shadow ཡིག་ཆ་དེ་ཚོ་ HOST1 དང་ HOST3 ཐོག་བསྒྱར་བཅོས་བྱས་པ་དེས་གསང་ཚང་བསྒྱར་བཅོས་བྱས་ཡོད་པའི་བཟོ་སྒོ་ཀྱི་ཡོད། HOST1 ཐོག་ཡོད་པའི་དཔང་རྟགས་ཀྱིས་སྤྱོད་མཁན་ 'sshuser' ཀྱི་གསང་ཚང་བསྒྱར་བཅོས་བྱས་ཡོད་པའི་བཟོ་སྒོ་ཀྱི་ཡོད།
༢༠༢༢ ལྷ་ ༥	HOST2 ནི་ཚོགས་པ་དེས་སྒོ་བརྒྱབ་པ་རེད། དྲ་རྒྱའི་ཁབ་ལེན་ཁ་སྒོན་ (T1505.003) HOST1 དང་ HOST3 ཐོག་ལ་བཅོས་ཡོད། HOST1 ལ་HOST3 ནས་SSH བཙན་ཤེད་ཀྱི་ཚོད་ལྟ་སྤྱོང་ཚོར་བྱུང་ཡོད། HOST3 ཐོག་ལ་དྲན་ཐོ་ཡིག་ཆ་ཞིག་བསྒྱར་བཅོས་བྱས། (T1070) ཡིག་ཆ་འདིའི་ནང་དུ་ཡིག་ཆའི་རྒྱུ་ཆ་ (T1078) གཤོད་བའཆོ་ཀྱི་འཁྲབ་སྟོན་པས་འཛིན་བཟུང་བྱས་ཡོད་སྲིད། JWTs བཟུང་བ་ (T1528) དང་ HOST3 ཐོག་གི་ཡིག་ཆ་ཞིག་ཀུ་ཡིར་འདོན་བྱས། HOST3 ནི་ཚོགས་པ་དེས་སྒོ་བརྒྱབ་པ་རེད། དུས་ཚོད་འདིའི་རྗེས་ཀྱི་ཉེད་སྒོ་ཚང་མ་HOST1 ཐོག་ལ་འབྱུང་བ་རེད།
༢༠༢༢ ལྷ་ ༥	HOST1 (T1505.003) ཐོག་དྲ་རྒྱའི་ཁ་སྒོན་ཁ་སྒོན་བྱས། JWTs བཟུང་ནས་ HOST1 ཐོག་གི་ཡིག་ཆ་ཞིག་ཀུ་ཡིར་འདོན་བྱས།
༢༠༢༢ ལྷ་ ༥	ཁ་སྒོན་དྲ་རྒྱའི་ཤེལ་སྤུབས་ HOST1 (T1505.003) ཐོག་ལ་གསར་འཛུགས་བྱས་པ་དང་། ཤེས་རྟོགས་ཡོད་པའི་གནོད་འཚེ་ཅན་གྱི་ IP ཁ་བྱང་གིས་མཁོན་འཕྲེར་དེ་དང་འཐེལ་འབྲེས་ཉེད་ཀྱི་ཡོད། (TA0011) ཤེས་རྟོགས་བྱང་བའི་གནོད་འཚེ་ཅན་གྱི་IPཁ་བྱང་ཞིག་གིས་འཛུལ་སྒོའི་སྒོ་ཕྱེ་གཙོ་བོHOST7དང་འཐེལ་བ་ཉེད་ཀྱི་ཡོད།
ཕྱི་ལོ་ ༢༠༢༢ ལྷ་ ༤	ཤེས་རྟོགས་བྱང་བའི་གནོད་འཚེ་ཅན་ཀྱི་IPཁ་བྱང་ཞིག་གིས་འཛུལ་སྤྱོད་སྒོ་ཕྱེ་གའི་གཙོ་བའག་HOST7 (TA0011) དང་འཐེལ་བ་བྱས། འེད་སྤྱོད་པ་ཞིག་གི་བཅེན་དཔང་བྱང་རིམ་དེ་HOST1 ཐོག་གི་དྲན་ཐོའི་ནང་དུ་ཡོད་པའི་IPཁ་བྱང་ངན་པ་ཤེས་རྟོགས་བྱང་བ་དང་འཐེལ་བ་ཡོད། གཙོ་བའག་འདིའི་སྐྱེང་དུ་རྒྱའི་ཁབ་ལེན་ཁ་སྒོན་ཞིག་གསར་འཛུགས་བྱས་ཡོད། (T1505.003)
ཕྱི་ལོ་ ༢༠༢༢ ལྷ་ ༤	HOST1 ལ་ཡོད་པའི་སྒིཔ་ཀི་ཞིག་ཉེད་ཡོ་གཅིག་གིས་བཅོས་བསྒྱར་བྱས་པ་རེད། (T1543) ཡིག་ཆ་འདི་ལ་ནང་སྒུལ་གྱི་SQL ཉར་བར་ནས་གནས་རྒྱལ་བསྒྱུར་ཐུབ་ཉེད་པའི་ལས་ཀ་ཡོད།
ཕྱི་ལོ་ ༢༠༢༢ ལྷ་ ༤	HOST1 ཐོག་གི་དྲན་ཐོ་ཡིག་ཆ་ཁ་སྒོན་ཞིག་མཐའ་མར་བསྒྱར་བཅོས་བྱས། (T1070) ཡིག་ཆ་འདིའི་ནང་དུ་སྒིག་འཇུལ་སྤྱོད་མཁན་གྱི་མིང་དང་གསང་ཚང་ཆ་གཅིག་ཡོད་པ་དེ་དག་ཁྲིམས་མཐུན་ཡིན་པར་ཡིད་ཆེས་ཉེད་ཀྱི་ཡོད། (T1078)
ཕྱི་ལོ་ ༢༠༢༢ ལྷ་ ༤	ཁ་སྒོན་དྲན་ཐོ་ཡིག་ཆ་ཞིག་མཐའ་མར་བསྒྱར་བཅོས་བྱས། (T1070) ཡིག་ཆ་འདིའི་ནང་HOST1ནས་བསྒུ་རྒྱ་བྱས་པའི་JWTsཡོད།
ཕྱི་ལོ་ ༢༠༢༢ ལྷ་ ༤	HOST1 (T1505.003) ཐོག་དྲ་རྒྱའི་ཁ་སྒོན་ཁ་སྒོན་བྱས། ཚེས་གྲངས་འདིར་ཚོགས་པ་དེས་༢༠༢༢ ལོའི་ལྷ་བ་ཅཊི་པར་བཅོས་པའི་ཚེས་གྲངས་དང་བཅས་པའི་དྲ་རྒྱའི་ཁོག་སྟོང་ཞིག་རྟེན་པའི་སྐོར་ ASD ཡི་ ACSC ལ་སྦྱན་ཞུ་ཡུལ་ཡོད།
ཕྱི་ལོ་ ༢༠༢༢ ལྷ་ ༤	HOST1 ལ་ཡིག་ཆ་མང་པོ་བཅོས་ཡོད་ལ། དེའི་ནང་ནས་ Log4jHotPatch.jar ཞེས་མིང་བཏགས་པ་ཞིག་ཀྱང་ཡོད།
ཕྱི་ལོ་ ༢༠༢༢ ལྷ་ ༤	iptables-save བད་བགོད་དེ་འཇུལ་ཞུགས་སྒོ་ཕྱེ་ཐའི་གཙོ་བའག་ལ་ཁ་ཕྱེ་བའི་མཐུད་ཁ་གཉིས་ཁ་སྒོན་ཉེད་པར་ཅེད་ཕྱོད་བྱས། མཐུད་ཁ་དེ་དག་ནི་ཨཨཨ དང་ཨཨཨཨ ཡིན། (T1572)

བྱེད་མཁན་གྱི་བྱེད་སྟངས་དང་ཐབས་ཤེས།

གཤམ་དུ་ཞིབ་བཤེར་བྱེད་སྐབས་ཤེས་རྟོགས་བྱུང་བའི་ཐབས་ཤེས་དང་ལག་རྩལ་འགའ་ཤས་གསལ་པོ་བསྟན་ཡོད།

ཐོག་མའི་ཚོག་མཚན།

[T1190](#) སྤྱི་དམངས་ལ་ཁ་གཏད་པའི་མཉེན་ཆས་བཀོལ་སྤྱོད།

ཚོགས་པ་དེས་ཐག་རིང་ནས་འཛུལ་ཞུགས་བྱེད་པའི་ནང་འཛུལ་དང་དོས་འཛིན་འཛིན་སྐྱོང་ཐོན་རྫས་ནང་གི་RCE དང་དབང་ཆ་མཐོ་རུ་འདེགས་པ། དོས་འཛིན་བྱས་ཚད་འཚོལ་བའི་ཉེས་སྐྱོན་རྣམས་བེད་སྤྱོད་གཏོང་སྟེ་དྲ་རྒྱར་དང་པོའི་འཛུལ་ཞུགས་ཐོབ་པ་ཡིན་སྲིད།

ཐོག་མའི་ཐོབ་ཐང་ཐབས་ལམ་འདི་གཤམ་གསལ་གྱི་རྐྱེན་གྱིས་ཆེས་འབྱུང་སྲིད་པར་བརྩི་བཞིན་ཡོད།

- ད་ལྟའི་དུས་ཚོད་དེར་ CVEs འདི་དག་ལ་དྲ་གནས་བདེ་འཇགས་ཞན་པོ་འདུག
- ཤེས་རྟོགས་བྱུང་བའི་འཕྲབ་སྟོན་པ་རྨང་གཞིའི་སྒྲིག་བཀོད་ནས་རྨས་སྐྱོན་འདི་དག་བཀོལ་སྤྱོད་བྱེད་པར་འབད་བརྩོན་བྱེད། དང་
- ཤེས་རྟོགས་བྱུང་བའི་ནང་ཁུལ་གྱི་གནོད་འཚེ་ཅན་གྱི་བྱ་སྤྱོད་ཐོག་མ་དེ་བཀོལ་སྤྱོད་བྱེད་པའི་ཚོད་ལྟ་བྱས་པའི་རྗེས་སུ་བྱུང་བ་རེད།

ལག་བསྟར།

[T1059.004](#) བཀའ་ཚིག་དང་ཡིག་གཟུགས་སྒྱུར་མཁན། Unix བརྡ་བཀོད་ཁོག་སྟོང་

གོང་འཁོད་ཀྱི་སྐྱོན་ཆ་དེ་དག་ལ་མཐར་ཕྱིན་དང་བེད་སྤྱོད་བཏང་བའི་སྒེ་ཚན་གྱིས་གནོད་སྐྱོན་ཕོག་པའི་ཡོ་ཆས་སྟེང་ལ་ཡོད་པའི་ཡུ་ནི་ཀ་སི་ཁབ་ལེན་ནང་དུ་བཀའ་ཚིག་བཀོལ་སྤྱོད་བྱེད་ཐུབ་སྲིད་པ་རེད། བྱེད་པོ་རྣམས་ཀྱིས་བཀོལ་སྤྱོད་བྱས་པའི་བརྡ་བཀོད་ཀྱི་ཞིབ་ཚགས་ཆ་ཚང་སྤྲོད་མི་ཐུབ། གང་ཡིན་ཟེར་ན་སྒྲིག་ཆས་དེས་དེ་དག་ཟིན་ཐོ་བྱས་མེད།

བརྟན་པོར་གནས་པ

[T1505.003](#) སར་བར་མཉེན་ཆས་ཀྱི་ཆ་ཤས། དྲ་རྒྱའི་ཤེལ།

བྱེད་པོ་རྣམས་ཀྱིས་ཤུགས་རྐྱེན་ཐེབས་པའི་སྒྲིག་ཆས་དེར་དྲ་རྒྱའི་ཁོག་སྟོང་མང་པོ་བཀོད་སྒྲིག་བྱས། བྱེད་པོ་མི་འདྲ་བ་མང་པོས་དྲ་རྒྱའི་ཁོག་སྟོང་བཀོད་སྒྲིག་བྱེད་སྲིད་པ་རེད། འོན་ཀྱང་འཕྲབ་སྟོན་པ་ཉུང་ཤས་ཤིག་གིས་མ་ཟད་དྲ་རྒྱའི་ཁོག་སྟོང་འདི་དག་བཀོལ་སྤྱོད་བྱེད་པའི་བྱེད་སྒོ་སྤེལ་ཡོད། དྲ་རྒྱའི་ཁོག་སྟོང་དེ་དག་གིས་བྱེད་པོས་གནོད་འཚེ་ཐེབས་པའི་སྒྲིག་ཆས་རྣམས་ལ་བར་མེད་བརྡ་བཀོད་སྤེལ་བའི་གོ་སྐབས་སྤྲད་སྲིད།

ཐོབ་ཐང་ཆེ་རུ་གཏོང་བ།

[T1068](#) ཐོབ་ཐང་ཆེ་རུ་གཏོང་བའི་བཀོལ་སྤྱོད།

ཡོད་པའི་དབང་རྟགས་ཀྱིས་འཕྲབ་སྟོན་པ་ཚོས་ཐོབ་པའི་ཐོབ་ཐང་གི་གནས་ཚད་བརྗོད་མི་ཐུབ། འོན་ཀྱང་དྲ་རྒྱའི་ཁོག་སྟོང་བཀོལ་སྤྱོད་བྱས་ན། བྱེད་པོ་རྣམས་ཀྱིས་གནོད་འཚེ་ཐེབས་པའི་སྒྲིག་ཆས་དེའི་སྟེང་གི་དྲ་རྒྱའི་ཞབས་ཞུ་འདེབས་ཆས་ལ་ཡོད་པ་དང་འདྲ་བའི་དབང་ཆའི་རིམ་པ་ཐོབ་སྲིད། གནོད་འཚེ་ཐེབས་པའི་སྒྲིག་ཆས་དེར་ཡོད་པར་ཡིད་ཆེས་བྱེད་པའི་ཉེས་སྐྱོན་རྣམས་ཀྱིས་བྱེད་པོ་རྣམས་ལ་རྩ་བའི་དབང་ཆ་ཐོབ་པའི་གོ་སྐབས་སྤྲད་སྲིད།

ཚོག་མཚན་ཐོབ་ཐང་།

[T1056.003](#) ནང་འཇུག་འཛིན་བཟུང་། དྲ་རྒྱའི་སྒོ་འབྱེད་འཛིན་བཟུང་

བརྡབ་གསིག་བཏང་བའི་ཡོ་ཆས་དེའི་ཐོག་གི་མངོན་གསལ་གྱིས་འཕྲབ་སྟོན་པས་སྤྱོད་མཁན་གྱི་མིང་དང་གསང་ཨང་ཆ་གཅིག་བརྒྱ་ཕྲག་འགའ་ཤས་ཡིག་ཆ་གསལ་པོའི་ནང་བླངས་ཡོད་པ་དང་། དེ་དག་ཁྲིམས་མཐུན་ཡིན་པར་ཡིད་ཆེས་བྱེད་ཀྱི་ཡོད། དེ་དག་ངོ་མའི་ངོས་འཛིན་བྱ་རིམ་ལ་བསྒྱུར་བཅོས་འགའ་ཤས་བཏང་སྟེ་ཡིག་ཐོབ་རྩལ་ཡིག་ཆར་ཐོན་པར་བཟོ་བའི་ཐབས་ལམ་གྱིས་བླངས་པ་ཡིན་སྲིད།

[T1111](#) རྐྱེན་གྲངས་མང་པོའི་ངོས་འཛིན་ "བཀག་འགོག་

བྱེད་པོ་དེས་ཆ་འཛོག་གི་ནང་འཛུལ་དང་འབྲེལ་བའི་MFA ལག་ཆའི་རིན་ཐང་ཡང་བཟུང་བ་རེད། འདི་དག་ངོ་མའི་ངོས་འཛིན་བྱ་རིམ་ལ་བསྒྱུར་བཅོས་བཏང་སྟེ་རིན་ཐང་འདི་དག་ཡིག་ཆར་ཐོན་པར་བཟོ་བའི་ཐབས་ལམ་གྱིས་འཛིན་བཟུང་བྱས་པ་ཡིན་སྲིད། MFA ལག་ཆའི་བདེ་འཇགས་སྲུང་སྐྱོབ་ལ་མགོ་སྐོར་བྱེད་པའི་ཁྱད་པར་བའི་རིན་ཐང་དེ་དག་གསོག་འཛོག་བྱེད་མཁན་གྱི་"གསང་བའི་ཞབས་ཞུ་འདེབས་ཆས་"དེ་ལ་གནོད་འཚེ་ཐེབས་པའི་དཔང་རྟགས་མེད།

[T1040](#) དྲ་རྒྱའི་ཚོར་ལེན།

བྱེད་པོ་དེས་གནོད་འཚེ་ཐེབས་པའི་སྒྲིག་ཆས་སྟེང་དུ་HTTP འགྲུལ་བཞུད་འཛིན་བཟུང་བྱས་ནས་ JWTs རྣམས་བླངས་པར་ཡིད་ཆེས་བྱེད་ཀྱི་ཡོད། བེད་སྤྱོད་ཡོ་ཆས་ tcpdump དེ་གནོད་འཚེ་ཐེབས་པའི་སྒྲིག་ཆས་སྟེང་དུ་ལག་བསྟར་བྱས་པའི་དཔང་རྟགས་ཡོད་ལ། འདི་ནི་བྱེད་པོས་JWTs དེ་དག་འཛིན་བཟུང་བྱས་པའི་ཐབས་ལམ་ཡིན་སྲིད།

[T1539](#) དྲ་རྒྱའི་ཞབས་འདེགས་མཚོད་སྦྱིན་རྐུ་བ

གོང་དུ་བཤད་པ་ལྟར། བྱེད་པོ་དེས་JWTs རྣམས་འཛིན་བཟུང་བྱས་ཡོད་ལ། དེ་དག་ནི་དྲ་རྒྱའི་ཞབས་འདེགས་མཚོད་སྦྱིན་དང་འདྲ་བ་རེད། འདི་དག་འཕྲབ་སྟོན་པས་བསྐྱར་དུ་བེད་སྤྱོད་བཏང་ནས་ཐོབ་ཐང་སྔར་ལས་ལྷག་པ་བཙུགས་ཐུབ་ཀྱི་ཡོད།

གསར་རྙེད།

T1046 དྲ་རྒྱའི་ཞབས་ཞུའི་གསར་རྙེད།

དྲ་རྒྱ་བརྟག་དཔྱད་ཀྱི་ནེད་སྤྱོད་ཡོ་ཆས་nmap དེ་གཞོད་འཚོ་ཐེབས་པའི་སྒྲིག་ཆས་སྟེང་དུ་ལག་བསྟར་བྱས་ཏེ། དྲ་རྒྱའི་ཆ་ཤས་གཅིག་པ་དེའི་ནང་གི་སྒྲིག་ཆས་གཞན་དག་བརྟག་དཔྱད་བྱས་པའི་དཔང་རྟགས་ཡོད། འདི་ནི་ཁྱད་ཐོས་ཕྱོགས་ཀྱི་འགྱལ་སྐྱོད་ཀྱི་གོ་སྐབས་སྤྲད་ཐུབ་པའི་ཁྲབ་ཚད་ཡོད་པའི་དྲ་རྒྱའི་ཞབས་ཞུ་གཞན་དག་རྟེད་པའི་ཚེད་དུ་ནེད་སྤྱོད་བརྟང་ཡོད་སྲིད།

སོར་སྤྱུད།

དཔྱ་ཡོད་པའི་དཔང་རྟགས་ཀྱིས་ཁྱེད་པོ་རྟམས་ཀྱིས་གནས་ཚུལ་རྗེ་ཐྱར་བསྡུ་རྒྱབ་བྱས་པ་དང་། གཞོད་འཚོ་ཐེབས་པའི་སྒྲིག་ཆས་དང་རིམ་པ་གཞན་ནས་ཅི་ཞིག་བསྡུ་རྒྱབ་བྱས་མིན་གསལ་པོར་སྟོན་མི་ཐུབ། ཡིན་ནའང་། འཁྲབ་སྟོན་པ་ཚོས་གཏོར་བརླག་ཐེབས་པའི་ཡོ་ཆས་སྟེང་གི་ཡིག་ཆ་ཚང་མར་འཛུལ་ཐུབ་པ་འདུ། དེའི་ནང་དུ་འཛིན་བཟུང་བྱས་པའི་ཡོ་ཆས་ཚད་ལེན་ (T1003) དང་། MFA རྟགས་མཚན་རིན་ཐང་ (T1111) ། གོང་དུ་བཤད་པའི་ JWTs ཚོ་བཅས་ལ་ཡང་ཐུབ་པ་རེད།

བཀའ་སྩོལ་དང་ཚོད་འཛིན།

T1071.001 ཉེར་སྤྱོད་རིམ་པའི་གནད་སྟེལ་ཀྱི་གཞི་རིམ།: དྲ་རྒྱའི་གློས་མཐུན།

ཁྱེད་པ་ཚོས་བཀའ་སྒྲིག་དང་ཚོད་འཛིན་ཁྱེད་པར་དྲ་རྒྱའི་སྐུབས་སྐོགས་ལེད་སྤྱོད་བྱས། དྲ་རྒྱའི་ཁབ་ལེན་བཀའ་ཚོགས་དེ་ཚོ་འཕྲལ་ཆས་སྟེང་ཡོད་པའི་དྲ་རྒྱའི་ཞབས་ཞུ་འཕྲལ་ཆས་བཀོལ་ནས་HTTPSབརྒྱུད་ནས་སྤྲོད་ཡོད་སྲིད། (T1572).

T1001.003 གཞི་གྲངས་སྐུན་ནག་བཙོ་བ། གློས་མཐུན་རྫུན་བཙོ།

ཁྱེད་པ་ཚོས་གཏོར་བརླག་ཐེབས་པའི་ཡོ་ཆས་ཚོ་ཁྲིམས་མཐུན་གྱི་འགྲིམ་འགྱལ་དང་འབྲེས་ནས་གནས་ཐུབ་པའི་འཇིགས་སྐུལ་འགོ་འཛུགས་ས་ཚོགས་སུ་བེད་སྤྱོད་བྱས།

ཤེས་རྟོགས་ཐུབ་པ་དང་ཉུང་འཕྲི་བྱེད་དགོས་པའི་སློང་བྱ་བའོ་།

ASD ཡི་ ACSC ནས་ ASD གཙོ་བོའི་བརྒྱུད་ ཚོད་འཛིན་དང་འབྲེལ་བའི་དྲྭ་རྒྱའི་བདེ་འཇགས་དཀའ་ངལ་སེལ་བའི་ཐབས་ཤེས་ ལག་བསྟར་བྱེད་པར་ཤུགས་ཆེན་འདེམ་བསྐྱལ་ཞུ། གཤམ་དུ་APT40 ཡི་བཙན་འཛུལ་ཤེས་རྟོགས་དང་སྟོན་འགོག་བྱེད་པའི་དྲྭ་རྒྱའི་བདེ་འཇགས་ལས་དོན་གྱི་བསམ་འཆར་དང་། དེའི་རྗེས་སུ་རེའུ་མིག་དང་བོའི་ནང་བསྡུས་པའི་གཙོ་བོའི་TTPs བཞིའི་ཁྲད་པར་ཅན་གྱི་སྟོན་འགོག་ཐབས་ཚུལ་སྤྲད་ཡོག།

ཤེས་རྟོགས་བྱེད་པ།

གོང་དུ་རོས་འཛིན་བྱས་པའི་ཡིག་ཆ་ཁ་ཤས་C:\Users\Public* དང་C:\Windows\Temp* སྐྱ་བུའི་གནས་ཡུལ་དུ་བཞག་ཡོད། དེ་དག་ལ་གནས་ཚུལ་འབྲི་སའི་ས་ཆ་སྐབས་བའི་ཞིག་ཡིན། དེ་དག་ནི་སྤྱིར་བཏང་འཛམ་གླིང་ནང་བྱིས་ཐུབ་པ་ཡིན། དེ་ཡང་ཤིན་ཅོ་ནང་ཐོ་འགོད་བྱས་པའི་བགོལ་སྤྱོད་པའི་ཚེས་ཁ་ཙམ་ཚང་མར་སྟོད་ཐོ་འབྲི་དག་དང་དེ་དག་གི་སྟོད་ཐོ་ཚུང་བ་ལ་འཛུལ་ཐུབ་ཀྱི་ཡོད། མང་ཆེ་བ་སྤྱོད་མཁན་གང་རུང་གིས་རྟེན་ཅིང་འབྲེལ་བའི་ཡིག་ཆ་དེ་དག་ལ་འཛུལ་ཐུབ་པ་དེས་ཕྱོགས་གཅིག་ཏུ་འགྱུལ་སྐྱོད་དང་། བཀག་འགོག་བྱོས་བྱེད་པ། ཐག་བཅད་བའི་ལག་ལེན་འཁྲུལ་བའི་ཚེ་ཡང་ཤིན་ཅོ་ནང་ཐོ་འགོད་བྱས་པའི་ཚེས་ཁ་ཙམ་ཚང་མར་སྟོད་ཐོ་འབྲི་དག་དང་དེ་དག་གི་སྟོད་ཐོ་ཚུང་བ་ལ་འཛུལ་ཐུབ་པ་དེས་ཕྱོགས་གཅིག་ཏུ་འགྱུལ་སྐྱོད་བྱེད་པ་ཡིན། ཐག་ཆོད་ཀྱི་ཡོད།

གཤམ་གྱི་ Sigma གཞི་རིམ་ཚོས་ཐེ་ཚོམ་ཅན་གྱི་གནས་ས་ནས་འཐབ་སྟོན་བྱེད་པ་མི་རྣམས་པའི་བྱ་སྤྱོད་ཀྱི་རྟགས་མཚན་དུ་ཚོལ་ཞིབ་བྱེད། གནས་སྐངས་ཚང་མའི་ནང་དུ་གཙོ་བོ་འཆའ་ཞིག་ཡོད་དེས་གཤདས་ཞིབ་འཚུགས་ཁོ་ནས་ཡོད་པ་ཡིན།

མིང་བྱང: འཛམ་གླིང་ཀྱིས་འབྱི་ཐུབ་པའི་འཐབ་སྟོན་ - གནས་སྐབས།

ངོ་མ།: d2fa2d71-fbd0-4778-9449-e13ca7d7505c

ཞིབ་བརྗོད: C:\Windows\Temp ནས་བྱ་རིམ་འཐབ་སྟོན་ཤེས་རྟོགས་བྱེད།

རྒྱུ་སྐྱོངས:

ཁྲིམས་ལུགས་འདི་C:\Windows\Temp* ནང་ནས་ལག་བསྟར་བྱེད་པར་དམིགས་བསལ་གྱིས་སྐྱ་བཞིན་ཡོད། ཤེམ་པི་ནི་བདེ་ཐང་ཅན་གྱི་བགོལ་སྤྱོད་ཀྱིས་ཁྲབ་ཆེ་བ་ཤེད་སྤྱོད་བྱེད་ཀྱི་ཡོད། དེར་བརྟེན་C:\Windowsནང་དུ་འཛམ་གླིང་གཞན་གྱི་ཡིག་འབྲི་ཐུབ་པའི་སྟོད་ཐོ་ཚུང་བ་ལས་ལག་བསྟར་བྱེད་པ་ལས་ཡིད་ཆེས་ཀྱི་གནོད་འཚེ་ཅན་གྱི་བཏང་སྟོན་དུ་བཏང་ཡོད།

མ་ལག་ཡང་ན་དྲྭ་རྒྱའི་ཞབས་ཞུའི་སྤྱོད་མཁན་གྱིས་ལག་བསྟར་བྱས་པའི་མཉེན་ཆས་མེད་པར་བཟོས་པ་དེས་ཁྲིམས་འདིས་འདེམས་སྒྲུག་བྱས་པའི་བའི་ཐང་གི་བྱེད་སྤོའི་ཚད་གཞི་མངོན་གསལ་དོད་པོས་ཤུང་དུ་བཏང་ཡོག།

དེའི་དོན་ནི་གཞི་རིམ་དེས་སྟོབ་ཐང་མཐོ་བའི་རིམ་པར་གཏོང་འཚོ་ཅན་གྱི་འཁྲབ་སྟོན་མ་ཤེས་ཐུབ་སྲིད་ཀྱང་། བགོལ་སྤྱོད་པས་སྟོབ་ཐང་ SYSTEM ལ་མཚོ་རྒྱ་གཏོང་བར་འབད་བརྩོན་བྱེད་ཀྱི་ཡོད་མེད་གཏན་འབེབས་བྱེད་པར་གཞི་རིམ་གཞན་པ་བེད་སྤྱོད་བྱེད་པར་འདེམ་བསྐྱལ་ཞུ།

ཞིབ་བཤེར།

1. ཡིག་ཆ་འདི་ལག་བསྟར་དང་ཐད་ཀར་འབྲེལ་བ་ཡོད་པའི་གནས་ཚུལ་ལ་ཞིབ་བཤེར་བྱེད་དགོས། དཔེར་ན་སྤྱོད་མཁན་གྱི་སྐབས་དེན་བྱས་པ། ལག་བསྟར་གྱི་བདེ་འཇགས་གནས་ཚད། འཕུལ་མར་རྩེས་འདེད་བྱེད་ཐྲོ་དང་ཡིག་ཆ་དེས་མངོན་པའི་པར་རིས་བཅས་ཡིན།
2. འབྲེལ་ཡོད་བྱ་རིམ་དང་། དྲྭ་ཐུ། ཡིག་ཆ། དེ་བཞིན་གཙོ་ཡོ་ཆས་སྟེང་གི་ཚུབ་སྐྱོར་གནས་ཚུལ་གཞན་དག་ལ་ཞིབ་འཇུག་བྱས་ནས་བྱ་སྤྱོད་དེ་གནོད་ཐུབ་ཀྱི་ཡོད་མེད་ཀྱི་ཞིབ་བཤེར་བྱེད་དགོས།
3. དགོས་དེས་ཡིན་ན་ཡིག་ཆ་དེའི་འདུ་ཤུགས་ཤིག་བསྡུ་ལེན་བྱས་ནས་ཁྲིམས་མཐུན་ཡིན་མིན་གཏན་འབེབས་བྱེད་པར་ཚུབ་ཚོག་འཕྲལ་རིག་སྤྱད་དེ་ཞིབ་འཇུག་བྱེད་པར་འབད་བརྩོན་བྱེད་དགོས།

དཔྱད་གཞི།:

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

རྩོམ་པ་པོ།: ASD ཡི་ ACSC

ཚོས་གྲངས།: ২০২৩/০৬/৶৮

གནས་བབས།: ཚོད་ཟྱེའི་

རྟགས་མཚན།:

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

དྲན་ཐོའི་འབྱུང་ཁུངས།:

དབྱེ་ཁག: བྱ་རིམ་_གསར་བཟོ

ཐོན་སྐྱེད: windows

བརྟག་དཔྱད།:

གནས་སྐབས།:

པར་རིས།|འདི་ནས་འགོ་འཛུགས།: 'C:\\ཆེའུ་ཁྲང་\\དུས་ཚོད|\\'

སྤྱིར་བཏང་_གནས་སྐབས་_ལམ་ཐེག:

པར་རིས།|བསྒྲུར་།སྒང་ནེད།: 'C:\\ཤིན་ཅོ་\\གནས་སྐབས་\\\{[a-fA-F0-9]{8}-([a-fA-F0-9]{4}-){3}[a-fA-F0-9]{12}\}\\'

མ་ལག་སྤྱོད་མཁན།

སྤྱོད་མཁན།:

- 'མ་ལག'
- དྲྭ་རྒྱའི་ཞབས་ཞུ།

དྲིམ་ཉོས་ཤ།
ཡར་རིས།|མཇུག་སྦྱིལ།:'dismhost.exe'
གསལ་བའི་རྟ་བ།:
རྟ་བའི་གཟུགས་བརྟན།|མཇུག་སྡུང་:
- '\\esif_uf.exe'
- '\\vmtoolsd.exe'
- '\\cwainstaller.exe'
- '\\trolleyexpress.exe'

ཀློན་: temp དང་མེན་པ་ (common_temp_path ཡང་ན་ system_user ཡང་ན་ dismhost ཡང་ན་ known_parent)

བདེན་པ་མེད་པ།

- ཆོག་མཆན་ཐོ་གཞུང་ཚིས་ཞིབ་ཀྱི་མཉེན་ཆས་དེ་ཆོ་ཤེམ་པི་ནས་ལག་བསྟར་བྱེད་སྤྱད་པའི་ཡིག་ཆ་བགོལ་སྤྱོད་བྱེད་བཞིན་ཡོད་པར་བརྟག་དཔྱད་བྱས།
- ཤེམ་པི་ཡི་ནང་ལ་ཁྲིམས་མཐུན་པའི་སྒོ་ནས་སྤྱིག་འཇུག་པ་དང་འགོ་འཇུག་བྱེད་པའི་མཉེན་ཆས་རིགས་མང་པོ་ཡོད་པས། འདི་ལྟར་གྱུབ་འབྲས་དེ་བསྟུས་ནས་དྲྭ་བ་ལ་ལྟ་བའི་སྒོ་ནས་སྤྱོད་ལམ་འདི་གང་འདྲ་ཞུབ་ཡོད་མེད་དང་། ཡང་ན་དེར་གཞོན་ཐུབ་གཟུགས་ཐོ་ལག་བགོལ་ཆོག་མི་རེད་ལག་ལེན་བྱ་རྒྱུ་ཡོད་མེད་གཅོད་བྱས་ནས་ཁྲིམས་ལུགས་འདི་བཟོ་བཅོས་བྱ་དགོས།

རིམ་པ།: དམའ་

མིང་བྱང: འཛམ་གླིང་འབྲི་ཐུབ་པའི་ལག་བསྟར། - མ་ཡིན་པའི་-གནས་སྐབས་མ་ལག་གི་སྟོད་ཐོ།

ངོ་བོ།: 5b187157-e892-4fc9-84fc-aa48aff9f997

ཞིབ་བརྗོད།: Windows OS སྒྲིག་སྒྲིར་གནས་ས་ཡི་ཡན་ལག་དཀར་ཆག་ནང་གི་འཛིག་རྟེན་ཡོངས་ཀྱིས་འབྲི་ཐུབ་པའི་གནས་ས་ནས་བྱ་རིམ་འཕྲབ་སྟོན་ཤེས་རྟོགས་བྱེད།

རྒྱབ་སྟོངས:

གཞི་རིམ་འདི་དམིགས་བསལ་གྱིས་C:\ དང་བྱེ་བྲག་ཏུ་C:\Windows* ནང་གི་འཛིག་རྟེན་ཡོངས་ཀྱིས་འབྲི་ཐུབ་པའི་དཀར་ཆག་ནས་འཕྲབ་སྟོན་བྱེད་པ་ཚོས་བཞིན་ཡོད་པའི་C:\Windows\Temp མ་གཏོགས་ཏེ་དེ་ནི་ཕན་ཚུན་མེད་པའི་ཉར་སྟོངས་ཚོས་ཡོངས་གྲགས་སུ་སྟོད་པ་དང་དེ་བཞིན་གཞོན་ནུར་ཁྱབ་ཅིང་ཤོག་ཡིག་ཆ་མང་བ་ཡིན་པའི་རྒྱུ་མཚན་གྱིས་སོ།

གལ་ཏེ་ཡིག་ཆ་ཞིག་SYSTEM ཤུར་གཡོག་བགོལ་ན་AppData སྟོད་ཐོ་དེ་དག་ཐྱིར་འཕེན་བྱེད། འདི་ནི་གནས་སྐབས་བགོལ་སྤྱོད་ཡིག་ཆ་མང་པོ་ལག་བསྟར་བྱེད་པའི་ཐབས་ཤེས་བཟང་པོ་ཞིག་ཡིན།

དྲྭ་རྒྱའི་གཞི་རྩའི་ཐོག་མའི་ཚད་གཞི་མཇུག་སྡིལ་རྩེས་དང་ས་ཁུལ་དེ་དག་ནས་ཤེས་རྟོགས་བྱུང་བའི་བདེ་ཐབས་ཐོ་ལག་ཁྲིམས་དོས་འཛིན་བྱས་རྩེས། ཁྲིམས་ལུགས་འདི་དགོན་པོ་ཆགས་དགོས།

ཞིབ་བཤེར།

1. ཡིག་ཆ་འདི་ལག་བསྟར་དང་ཐད་གར་འབེལ་བ་ཡོད་པའི་གནས་ཚུལ་ལ་ཞིབ་བཤེར་བྱེད་དགོས། དཔེར་ན་སྤྱོད་མཁན་གྱི་སྐབས་དོན་དང་། ལག་བསྟར་གྱི་བདེ་འཇགས་གནས་ཚད། འཕྲལ་མར་རྩེས་འདེད་བྱེད་སྟོང་དང་ཡིག་ཆ་དེས་མངོན་པའི་པར་རིས་བཅས་ཡིན།
2. འབེལ་ཡོད་བྱ་རིམ་དང་། དྲྭ་ཐུ། ཡིག་ཆ། དེ་བཞིན་གཙོ་ཡོ་ཆས་སྟེང་གི་རྒྱབ་སྐྱོར་གནས་ཚུལ་གཞན་དག་ལ་ཞིབ་འཇུག་བྱས་ནས་བྱ་སྤྱོད་དེ་གནོད་འཚེ་ཅན་ཡིན་མིན་ལ་ཐག་གཅོད་པར་རོགས་རམ་བྱེད་དགོས།
3. དགོས་དེས་ཡིན་ན་ཡིག་ཆ་དེའི་འདྲ་བཤུས་ཤིག་བསྡུ་ལེན་བྱས་ནས་ཁྲིམས་མཐུན་ཡིན་མིན་གཏན་འབེལས་བྱེད་པར་རྒྱབ་ལོག་ཤུལ་རིག་སྤྱད་དེ་ཞིབ་འཇུག་བྱེད་པར་འབད་བརྩོན་བྱེད་དགོས།

དཔྱད་གཞི།:

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

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

རྩོམ་པ་པོ།: ASD ཡི་ ACSC

ཚེས་གྲངས།: ২০২৩/০৬/৭৫

གནས་བབས།: ཚོད་ལྟའི་

རྟགས་མཚན།:
- tlp.green
- classification.au.official
- attack.execution

དྲན་ཐོའི་འབྱུང་ཁུངས།:
དཔྱ་ཁག: བྱ་རིམ་_གསར་བཟོ
ཐོན་སྐྱེད: windows

བརྟག་དཔྱད།:
འབྲི་ཐུབ་པའི་_འགྲོ་ལམ།:
ཡར་རིས།|འདུས་ཡོད།:
- ':\\$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\\'

མཉེན་ཆས་གྲངས་ཀ།:
པར་རིས།|འདྲུས་ཡོད།:'\\མཉེན་ཆས་གྲངས་ཀ\\'
སྒྲིད་མཁན། 'མ་ལག'
ཆེན། འཛི་ཐུབ་པའི་ལམ་གྱ་དང་མཉེན་ཆས་གྲངས་ཀ་མིན་པ།

བདེན་པ་མེད་པ།

ཚོག་མཆན་ཞིབ་བཤེར་ཉེར་སྒྲིད་ཁག་གིས་དཀར་ཆག་འདི་དག་ནས་འགོར་སྐྱོད་ཐུབ་པའི་ཡིག་ཆ་རྣམས་འགོར་སྒྲིད་བྱེད་པར་མཐོང་བ་རེད།

ཚོག་མཆན་ཀ་གཞུང་རྩིས་ཞིབ་ཀྱི་མཉེན་ཆས་དེ་དག་གིས་སྒོ་ཀ་འདི་དག་ནས་ལག་བསྟར་བྱེད་ཐུབ་པའི་ཡིག་ཆ་བགོལ་སྒྲིད་བྱེད་བཞིན་ཡོད་པར་བརྟག་དཔྱད་ཐུས།ལྟ་རྟོག་བྱེད་པའི་ཁོར་ཡུག་ནང་སྒྲིད་བྱེད་པའི་གཙོ་སྤྱིའི་ཡིག་ཆ་དང་འཛིན་སྒྲིད་ལག་ཆ་དེ་དག་དཀར་ཆག་འདི་དག་གི་ནང་དུ་གནས་ཡོད་སྲིད་པས་གནས་ཚུལ་རེ་རེ་བཞིན་དུ་ཐག་གཅོད་བྱེད་དགོས།

རིམ་པ་: མཐོ་པོ་

མིང་བྱང: འཛམ་གླིང་འབྲི་ཐུབ་པའི་ལག་བསྟར། - བགོལ་སྒྲིད་པ།

ངོ་བོ།: 6dda3843-182a-4214-9263-925a80b4c634

ཞིབ་བརྟེད: སྒྲིད་མཁན་ནང་ཁུལ་གྱི་C:\Users\Public* དང་འཛམ་གླིང་གི་འབྲི་ཐུབ་པའི་སྒྲིད་གཞན་དག་ནས་བྱ་རིམ་ལག་བསྟར་བྱེད་པ་ཤེས་རྟོགས་བྱེད།

རྒྱབ་སྟྲོངས:

གལ་ཏེ་ཡིག་ཆ་ཞིག་SYSTEM ཁྱར་གཡོག་བགོལ་ན་ AppData སྒྲིད་ཐོ་དེ་དག་ཕྱིར་འཐེན་བྱེད། འདི་ནི་གནས་སྐབས་བགོལ་སྒྲིད་ཡིག་ཆ་མང་པོ་ལག་བསྟར་བྱེད་པའི་ཐབས་ཤེས་བཟང་པོ་ཞིག་ཡིན།

ཞིབ་བཤེར།

1. ཡིག་ཆ་འདི་ལག་བསྟར་དང་ཐད་ཀར་འཛེལ་བ་ཡོད་པའི་གནས་ཚུལ་ལ་ཞིབ་བཤེར་བྱེད་དགོས། དཔེར་ན་སྒྲིད་མཁན་གྱི་སྐབས་དེན་དང་། ལག་བསྟར་གྱི་བདེ་འཇགས་གནས་ཚད། འཕྲལ་མར་རྗེས་འདེད་བྱེད་སྒོ་དང་ཡིག་ཆ་དེས་མངོན་པའི་པར་རིས་བཅས་ཡིན།
2. འཛེལ་ཡོད་བྱ་རིམ་དང་། དྲ་རྒྱ། ཡིག་ཆ། དེ་བཞིན་གཙོ་ཡོ་ཆས་སྐྱེད་གི་རྒྱབ་སྐྱོར་གནས་ཚུལ་གཞན་དག་ལ་ཞིབ་འཇུག་བྱས་ནས་བྱ་སྒྲིད་དེ་གནོད་འཚེ་ཅན་ཡིན་མིན་ལ་ཐག་གཅོད་པར་རོགས་རམ་བྱེད་དགོས།
3. དགོས་ངེས་ཡིན་ན་ཡིག་ཆ་དེའི་འདུ་བཤུས་ཤིག་བསྡུ་ལེན་བྱས་ནས་ཁྱིམས་མཐུན་ཡིན་མིན་གཏན་འབེབས་བྱེད་པར་རྒྱབ་ཡོག་འཕྲུལ་རིག་སྤྱད་དེ་ཞིབ་འཇུག་བྱེད་པར་འབད་བརྩོན་བྱེད་དགོས།

དཔྱད་གཞི:

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

རྩོམ་པ་པོ།: ASD ཡི་ ACSC
ཚེས་གྲངས།: ২০২৩/০৬/১৫
གནས་བབས།: ཚོད་ལྟའི་
རྟགས་མཚན།:

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

དུན་ཐོའི་འབྱུང་ཁུངས།:

དབྱེ།ཁག: བྱ་རིམ་_གསར་བཟོ།
ཐོན་སྐྱེད: windows

བརྟག་དཔྱད།:

སྤྱོད་མཁན།:

ཕར་རིས།འདུས་ཡོད།:

- ‘:\\སྤྱོད་མཁན་\\སྤྱོད་མཁན་ཚང་མ\\’
- ‘:\\སྤྱོད་མཁན\\འབྲེལ་གཏུག\\’
- ‘:\\སྤྱོད་མཁན\\སྔོན་སྒྲིག\\’
- ‘:\\སྤྱོད་མཁན\\སྤྱི་བ\\’།
- ‘:\\སྤྱོད་མཁན\\འཚོལ་ཞིབ་བྱེད་མཁན\\’

མཉེན་ཆས་གྲངས་ཐོ།:

ཕར་རིས།འདུས་ཡོད།:’\\མཉེན་ཆས་གྲངས་ཐོ\\’

སྤྱོད་མཁན།: ‘མ་ལག’

ཆ་རྐྱེན། སྤྱོད་མཁན་དང་མཉེན་ཆས་གྲངས་ཐོ་མིན་པ།

བདེ་ན་པ་མི་ད་པ།:

– བལྟ་རྟོགས་བྱེད་པའི་ཁོར་ཡུག་ནང་བེད་སྤྱོད་བྱེད་པའི་ཡིག་ཆ་དང་འཛིན་སྐྱོང་ལག་ཆ་དེ་ཚོ་སྤྱི་དམངས་ཡང་ན་སྟོད་པོ་ཆུང་བ་ཞིག་གི་ནང་དུ་གནས་ཡོད་སྲིད་པས་གནས་ཚུལ་རེ་རེ་བཞིན་ཐག་གཅོད་བྱེད་དགོས།

རིམ་པ།: འཕྲིང་

ཞི་འཇམ།

ཐོ་འགོད་པ།

ASD གི་ ACSC ཞིབ་བཤེར་སྐབས་སུ། ཞིབ་བཤེར་གྱི་ནུས་པ་དང་མགྱོགས་ཚད་ཉུང་དུ་གཏོང་བའི་ཕྱིར་བཏང་གི་གནད་དོན་ཞིག་ནི་དྲ་རྒྱའི་ཞབས་ཞུ་བའི་རེ་འདུན་ཐོ་འགོད་དང་། ཕྱིན་ཉོ་བྱུང་རིམ་ཐོ་འགོད། དྲ་རྒྱའི་ཚབ་མཚོན་ཐོ་འགོད་སོགས་ས་ཁུལ་མང་པོའི་ནང་ཁྱབ་ཆེ་ཞིང་ལོ་རྒྱུས་ཀྱི་ཐོ་འགོད་ཆ་འཕྲིན་མེད་པ་དེ་རེད།

ASD གི་ ACSC ནས་ཁོང་ཚོའི་ཕྱིན་ཉོ་བྱུང་རིམ་ཐོ་འགོད་དང་སྒོ་གཏོང་གྲོས་འདེབས་དེ་བལྟ་ཞིབ་དང་བསྟར་སྤྱོད་བྱེད་པ་སྣན་འདེབས་བྱེད་ཡོད། འདིའི་ནང་ཕྱིན་ཉོ་བྱུང་རིམ་ཐོ་འགོད་མཛོད་ཁང་གི་སྒྲིག་བཀོད་ཡིག་ཆ་དང་ཡིག་ཆ་རྣམས། ཆ་འཕྲིན་བདེ་འཇགས་ལག་དེབ་ཀྱི་མ་ལག་བལྟ་རྟོག་གི་འདྲིས་སྟོན་བཅས་ཚུད་ཡོད་ཅིང་། དེའི་ནང་ཐོ་འགོད་དབུས་སུ་སྒྲིག་པ་དང་དུས་ཚོད་འོས་པ་ཞིག་གི་རིང་ཐོ་འགོད་གསོག་ཉར་བྱེད་པ་བཅས་ཚུད།

ཞུས་དག་འཛིན་སྐྱོང་།

དྲ་རྒྱའི་ཐོག་ལ་འཕྲད་པའི་ཡོ་ཆས་དང་ཞབས་ཞུ་ཚང་མ་མྱུར་དུ་བསྐྱར་བཅོས་བྱེད་དགོས། དེའི་ནང་དྲ་རྒྱའི་ཞབས་ཞུ་འཕྲུལ་ཆས་དང་། དྲ་རྒྱའི་མཉེན་ཆས། བྱ་རིམ་དེ་རང་འགྱུལ་ཅན་དང་མགྱོགས་སུ་གཏོང་བར་དབུས་གཙང་གི་ཐིག་ལེ་འཛིན་སྐྱོང་མ་ལག་ལག་བསྟར་བྱེད་པར་བསམ་གཞིག་བྱོས། ASD གི་ ACSC ནས་ ISM གི་མ་ལག་འཛིན་སྐྱོང་གི་འདྲིས་སྟོན་བསྟར་སྤྱོད་བྱེད་པ་སྣན་འདེབས་བྱེད་ཡོད། བྱེ་བྲག་ཏུ་འཚམས་པའི་མ་ལག་ཞུས་དག་ཚོད་འཛིན་ཞེས་པ་དེ་རེད།

བྱེད་མཁན་གྱིས་བེད་སྤྱོད་བྱས་པའི་བརྟན་འཇུག་ཕལ་ཆེ་བ་ནི་མི་མང་ལ་ཤེས་གསལ་ཡིན་ཞིང་ཞུས་དག་གམ་སྐྱོབ་བཅོས་ཐབས་ལམ་ཡོད་པ་ཞིག་རེད། མཐུན་ཚོགས་ཁག་གིས་ཆུ་ཚོད་༤༨ ནང་དྲ་རྒྱའི་ཐོག་ལ་ཁ་གཏད་པའི་རྨང་གཞིའི་སྒྲིག་བཀོད་ལ་བདེ་འཇགས་ཞུས་དག་གམ་སྐྱོབ་བཅོས་ཐབས་ལམ་སྤྱོད་དགོས་པ་དང་། ཐུབ་ན་མཉེན་ཆས་དང་བདག་སྐྱོང་མ་ལག་གི་གསར་པའི་འདོན་ཐེངས་བེད་སྤྱོད་བྱེད་དགོས།

དྲ་རྒྱའི་ཆ་ཤས་དབྱེ་འབྱེད།

དྲ་རྒྱའི་ཆ་བགོས་འབྱེད་པ་དེས་དགྲ་བོ་ཚོར་ཚོགས་པའི་ཚོར་ཤུགས་ཆེ་བའི་གནས་ཚུལ་འཚོལ་ཞིབ་དང་ཐོབ་ཐང་ཐོབ་པར་དཀའ་ངལ་ཆེ་རུ་གཏོང་ཐུབ། དགོས་མཁོ་མེད་ན་གློག་ཀླད་བར་གྱི་འགྲོ་འོང་བཀག་འགོག་བྱས་ནས་ཕྱོགས་གཅིག་གི་འགྱུལ་སྐྱོད་ཚད་བཀག་བྱེད་པའམ་ཡང་ན་བཀག་འགོག་བྱེད་པའི་དྲ་རྒྱ་ཆ་ཤས་བཟོས། གལ་ཆེའི་སར་བར་ཁག་ཅིག དཔེར་ན། Active Directory དང་བདེན་དཔང་སར་བར་གཞན་པ་དེ་ཚོ་བར་མའི་སར་བར་ཚད་གཞི་ཆུང་བ་ཞིག་གམ་ཡང་ན་"མཚོང་སར་བར"ནས་ཁོ་ནར་འཛིན་སྐྱོང་བྱེད་ཐུབ་དགོས། དེ་དག་ལ་ལྟ་རྟོག་ནན་པོ་བྱེད་དགོས་པ་དང་། བདེ་འཇགས་ཡག་པོ་ཡོད་དགོས། དེ་བཞིན་སྤྱོད་མཁན་དང་འཕྲུལ་ཆས་གང་ཞིག་དེ་དག་ལ་མཐུད་ཐུབ་མིན་ཚད་གཞི་བཟོ་དགོས།

ཕྱོགས་ངོས་སྔོ་བའི་འགྱུལ་སྐྱོད་འགོག་པའི་གནས་ཚུལ་ངོས་འཛིན་བྱས་པ་ལ་མ་ལྟོས་པར། དྲ་རྒྱའི་ཆ་བགོས་འབྱེད་པ་ཁ་སྣོན་བྱས་ན་བྱེད་མཁན་གྱིས་འཇུལ་ཞུགས་དང་འདོན་ལེན་བྱེད་ཐུབ་པའི་གནས་ཚུལ་གྱི་ཚད་གཞི་དེ་བས་ཀྱང་ཚད་བཀག་ཐུབ་ངེས།

ཁ་སྣོན་སྐྱོབ་བཅོས་ཐབས་ལམ།

རྩོམ་སྒྲིག་ལས་ཁུངས་ཁག་གིས་ APT40 དང་གཞན་པ་ཚོས་གཤམ་གྱི་ TTPs བེད་སྤྱོད་བྱེད་པར་ཁ་གཏད་པའི་ཆེད་དུ་གཤམ་གསལ་གྱི་སྐྱོབ་བཅོས་ཐབས་ལམ་ཁག་སྣན་འདེབས་བྱེད་ཀྱི་ཡོད།

- བེད་སྤྱོད་མ་བཏང་བའམ་ཡང་ན་དགོས་མཁོ་མེད་པའི་དྲ་རྒྱའི་ཞབས་ཞུ་དང་། སྒོ་ཆ། གཏོང་ལེན་གྲོས་གཞི་བཅས་མི་ལས་པ་བཟོ་དགོས།
- དྲ་རྒྱའི་ཞབས་ཞུ་འཕྲུལ་ཆས་དང་མཉེན་ཆས་ལ་སྲུང་སྐྱོབ་བྱེད་པར་དྲ་རྒྱའི་མཉེན་ཆས་ཀྱི་མེ་གྱང་(WAFs)ལེགས་པར་བསྒྲིགས་ནས་བེད་སྤྱོད་བྱེད་དགོས།
- གསབ་ལེན་དང་ཡིག་ཆ་མཉམ་སྤྱོད་དང་ཐོན་ཁུངས་གཞན་དག་ལ་འཛུལ་ཞུགས་ཚད་བཀག་བྱེད་པའི་ཐོབ་ཐང་ཉུང་ཤོས་ལག་བསྟར་བྱེད་དགོས།
- ཆ་རྐྱེན་སྣ་ཚོགས་ཀྱི་བདེན་དཔང་(MFA)དང་དོ་དམ་བྱེད་པའི་ཞབས་ཞུའི་རྗེས་ཁྲ་བེད་སྤྱད་དེ་ཡིག་ཆ་དེ་ཚོ་གཏོར་བརླག་གཏོང་བ་དང་བསྒྱུར་དུ་བེད་སྤྱོད་གཏོང་བར་དཀའ་ངལ་བཟོ་ཐུབ། དྲ་རྒྱའི་ཐོག་ནས་འཛུལ་ཞུགས་ཐུབ་པའི་ཐག་རིང་འཛུལ་ཞུགས་ཞབས་ཞུ་ཚང་མར་MFA ལག་བསྟར་བྱེད་དགོས་པ་དང་། དེའི་ནང་འདི་དག་ཚུད།
  - དྲ་རྒྱ་དང་སྤྲིན་ལ་བརྟེན་པའི་གློག་འཕྲིན།
  - མཉམ་ལས་སྟེགས་བུ།
  - གཟུགས་བརྙན་སྒེར་གྱི་དྲ་རྒྱའི་སྦྲེལ་མཐུད།
  - ཐག་རིང་ཅོག་སྟེགས་ཞབས་ཞུ།
- བེད་སྤྱོད་མཇུག་རྫོགས་པའི་སྒྲིག་ཆས་བརྗེ་དགོས།

རེའུ་མིག 1. སྒྲིབ་བཅོས་ཐབས་ལམ་/ལག་རྟལ།

TTP	གལ་ཆེའི་བརྒྱུད་ཀྱི་སྒྲིབ་བཅོས་ཐབས་ལམ།	ISM ཚོད་འཛིན།
ཐོག་མའི་ཚོག་མཚན། T1190 སྤྱི་དམངས་ལ་ཁ་གཏད་པའི་ཞུ་ཡིག་བཀོལ་སྤྱོད།	ཕིག་ཁམ་བཀོལ་སྤྱོད། བདག་སྐྱོང་མ་ཡག་ལ་ཞུས་དག་བཏང་བ། ཚ་ཀྱེན་མང་སྟེའི་བདེན་དཔང་། ཉེར་སྤྱོད་ཚོད་འཛིན།	ISM-0140 ISM-1698 ISM-1701 ISM-1921 ISM-1876 ISM-1877 ISM-1905
ལག་བསྟར། T1059 བཀའ་བཀོད་དང་ཡིག་གཟུགས་སྒྲུར་མཁན།	ཉེར་སྤྱོད་ཚོད་འཛིན། མའི་ཀོ་རོ་སོཕཏ་གི་མེ་ཀ་རོ་ཚད་འཛིན་བྱེད་པ། སྲིད་འཛིན་ཁེ་དབང་ལ་ཚོད་འཛིན་བྱེད་པ།	ISM-0140 ISM-1490 ISM-1622 ISM-1623 ISM-1657 ISM-1890
བརྟན་པོར་གནས་པ T1505.003 གསབ་ལེན་མཉེན་ཆས་ཀྱི་ཆ་འགས། དྲ་རྒྱའི་ཤེལ་ལ།	ཉེར་སྤྱོད་ཚོད་འཛིན། སྲིད་འཛིན་ཁེ་དབང་ལ་ཚོད་འཛིན་བྱེད་པ།	ISM-0140 ISM-1246 ISM-1746 ISM-1249 ISM-1250 ISM-1490 ISM-1657 ISM-1871
ཐོག་མའི་ཚོག་མཚན། ཐོབ་ཐང་འཕེལ་རྒྱས། བརྟན་བཟློང་།	བདག་སྐྱོང་མ་ཡག་ལ་ཞུས་དག་བཏང་བ། ཚ་ཀྱེན་མང་སྟེའི་བདེན་དཔང་། སྲིད་འཛིན་ཁེ་དབང་ལ་ཚོད་འཛིན་བྱེད་པ། ཉེར་སྤྱོད་ཚོད་འཛིན། སྤྱོད་མཁན་ཀྱི་ཉེར་སྤྱོད་སྐ་མཁེགས་བཟོ་བ།	ISM-0140 ISM-0859 ISM-1546 ISM-1504 ISM-1679
T1078 ནུས་སྟན་རྩིས་ཁྲ།		

སྤྱིར་བཏང་གི་རྩོགས་པ་དང་སྒྲིབ་བཅོས་ཀྱི་བསྟབ་བྱ་ཁ་སྟོན་ཆེད་དུ། བསྟབ་བྱ་འདི་ཉིད་མཇུག་ཏུ་MITRE ATT&CK [སྐྱིང་བསྡུས་ནང་དོས་འཛིན་བྱས་པའི་ཐབས་ཤེས་རེ་རེའི་ཚེད་དུ་](#) MITRE ATT&CK ཐབས་ཤེས་དྲ་ཚིགས་སྐྱང་གི་Mitigations and Detection ཞེས་པའི་སྟེ་ཚན་ལ་གཟིགས་རོགས་གནང་།

ངོས་མི་ལེན་པ།

སྐན་ཞུ་འདིའི་ནང་གི་ཚ་འཕྲིན་དེ་ཚོ་ཚ་འཕྲིན་སྤྱོད་པའི་དམིགས་ཡུལ་ཅན་ལ་"གང་ཡོད་ཁྱར་"སྤྱོད་བཞིན་ཡོད། རྩོམ་སྒྲིག་ལས་ཁུངས་ཁག་གིས་ཚོང་འཛིལ་ཚོགས་སྟེ་གང་ཡང་རུང་བ། ཐོབ་སྐྱེད། ཚོང་ལས། ཞབས་ཞུ་གང་ཡང་རུང་བ་ལ་རྒྱབ་སྐྱོར་མི་བྱེད། དེའི་ནང་དུ་ཡིག་ཚ་འདིའི་ནང་སྤྲལ་མཐུད་བྱས་པའི་ཚོགས་སྟེ། ཐོན་སྐྱེད། ཞབས་ཞུ་གང་ཡང་ཚུད། ཚོང་དོན་ཀྱི་སྟེ་ཚན་དང་། ཐོབ་རྩལ། བྱ་རིམ། ཡང་ན་ཞབས་ཞུའི་སྐོར་ལ་ཞབས་ཞུའི་མཚོན་རྟགས་དང་། ཚོང་རྟགས། བཟོ་མཁན། ཡང་ན་གཞན་པའི་ཐོག་ནས་བརྩོད་པ་གང་རུང་ཞིག་གིས་རྩོམ་སྒྲིག་ལས་ཁུངས་ཀྱིས་རྒྱབ་སྐྱོར་དང་། བསྟན་འདེབས། ཡང་ན་དགའ་ཞེན་བྱས་པར་གྱུབ་པའམ་སྟོན་པ་མ་རེད།

ཡིག་ཚ་འདི་ལ་TLP:CLEARཞེས་རྟགས་བཀོད་ཡོད། གསལ་སྟོན་ལ་བཀག་ཚ་མེད། བརྟ་འཕྲིན་གྱི་ནང་དོན་ལ་ཡོག་སྤྱོད་ཀྱི་ཉེན་ཁ་ཉང་ཤོས་ཡོད་པ་དང་ཡང་ནས་སྟོན་བཏང་བ་ཐང་རས་མེད་པའི་ཉེན་ཁ་ཡོད་པའི་སྣབས་ལ། བསྒྲགས་སྤྱོད་དང་བྱི་སྤྱོད་གཏོང་ཚུལ་ཁྱར་སྤྱོད་མཁན་གྱིས་TLP:CLEAR བེད་སྤྱོད་བྱས་ཚོག་སྟིད། སྲིད་འཛིན་དང་མཐུན་པའི་དྲན་བྱེད་ཁ་ཐུག་ནས། TLP:CLEAR བརྟ་འཕྲིན་དེ་ལ་ཚབས་མེད་ཀྱི་སྤྱོད་སྒོ་བཟོ་ཚོག་སྟིད། འགྲེམ་འགྱུལ་སྒོག་སྒྲོན་སྒྲིག་གཞིའི་སྐོར་ཀྱི་གནས་ཚུལ་མང་པོ་ཤེས་འདོད་ན། cisa.gov/tlp ལ་གཟིགས།

MITRE ATT&CK –

པོ་རྒྱུས་དྲས་རབས་ཀྱི་ APT40 གྱི་ཕྱོགས་རྒྱུན་ལག་རྩལ་དོ་སྣང་།

རྟོག་ཞིབ། (TA0043)

གཞོད་འཚེ་པོག་མཁན་གྱིས་བདག་གཉེར་བྱེད་པའི་དྲ་ཚིགས་འཚོལ་ཞིབ། (T1594)	ཡན་ཆུན་དང་འབྲེལ་བའི་ངོས་འཛིན་གྱི་བརྡ་དོན་བསྡུ་ལེན། ཚོག་མཚན་བརྡ་དོན། (T1589.001)
ཕྱིར་འཚོལ་སྐྱོན་ལེན་བྱེད་པ། ཟས་སྐྱོན་ཞིབ་བཤེར་(T1595.002)	གཞོད་འཚེ་པོག་མཁན་གྱི་གཙོ་བདག་ཚ་འཕེན་བསྡུ་རྒྱབ་བྱས། (T1592)
འཚོལ་ཞིབ་ཁ་ཕྱེ་བའི་དྲ་ཚིགས/ཁྱབ་ཁོངས་: འཚོལ་ཞིབ་འཕྲལ་ཚས་(T1593.002)	གཡན་ཆུན་གྱི་དྲ་བའི་ཚ་འཕེན་བསྡུ་ལེན། ཁོངས་ཁྱབ་ཁྱད་ཚོས། (T1590.001)
ཡན་ཆུན་དང་འབྲེལ་བའི་ངོས་འཛིན་གྱི་བརྡ་དོན་བསྡུ་ལེན། སྒོག་འཕེན་ཁ་བྱང་། (T1589.002)	

ཐོན་ཁུངས་གསར་སྤེལ། (TA0042)

རྩང་གཞིའི་སྤྱིག་བཀོད་ཀྱི་སྐྱབ་བྱེད་པ། ཁྱབ་ཁོངས་ (T1583.001)	རྩང་གཞིའི་སྤྱིག་བཀོད་ཀྱི་སྐྱབ་བྱས། (T1583)
རྩང་གཞིའི་སྤྱིག་བཀོད་ཀྱི་སྐྱབ་བྱེད་པ། ཉི་ཞེན་ཞེས་སར་བར་ (T1583.002)	ཚོག་མཚན་གྲངས་འཛིན་བཀག་བྱས་པ། (T1586)
ནུས་པ་འཛེལ་རྒྱས་གཏོང་བ། གསང་ཞང་མིང་རྟགས་བཀོད་པའི་ལག་ཆེད། (T1587.002)	གཞི་རྟེན་བཀག་བྱས་པ། (T1584)
ནུས་པ་འཛེལ་རྒྱས་གཏོང་བ། དྲ་རྒྱའི་ལག་ཆེད། (T1587.003)	ནུས་པ་འཛེལ་རྒྱས་གཏོང་བ། མཉེན་ཆས་ངན་པ། (T1587.001)
ནུས་པ་ཐོབ། གསང་ཞང་མིང་རྟགས་བཀོད་པའི་ལག་ཆེད། (T1588.003)	རྩིས་ཁྲ་བཙུགས་པ། སྤྱིན་རྩིས་ཁྲ། (T1585.003)
གཞི་རྟེན་བཀག་བྱས་པ། དྲ་རྒྱའི་སྤྱིག་ཆས། (T1584.008)	ནུས་པ་ཐོབ། དྲ་རྒྱའི་ལག་ཆེད། (T1588.004)

ཐོག་མའི་མཆོག་ཆན། (TA0001)

ནུས་ལྡན་གྱི་རྩིས་ཁྲ། (T1078)	པི་ཤེང་། (T1566)
ནུས་ལྡན་རྩིས་ཁྲ། སྡོད་སྤྱིག་རྩིས་ཁྲ། (T1078.001)	པི་ཤེང་། དཔེགས་བསལ་ཀ་འཛིན་སྤེལ་ཡིག (T1566.001)
ནུས་ལྡན་རྩིས་ཁྲ། ཁྱབ་ཁོངས་རྩིས་ཁྲ། (T1078.002)	པི་ཤེང་། དཔེགས་བསལ་ཀ་འཛིན་སྤེལ་མཐུད། (T1566.002)
ཕྱི་རོལ་གྱི་ཐག་རིང་ཞབས་ཞུ། (T1133)	སྤྱི་དམངས་ལ་ཁ་གཏད་པའི་མཉེན་ཆས་བཀོལ་སྤྱོད། (T1190)
འགྲོ་སྐབས་བཅོམ་པ། (T1189)	

ལག་བསྟར། (TA0002)

ཕྱིན་ཅི་འཛིན་སྒྲོང་ལག་ཆ། (T1047)	བཀའ་བཀོད་དང་ཡིག་གཟུགས་སྐད་སྒྱུར་མཁན། ཁའི་ཐོན་ (T1059.006)
དུས་ཚོད་གཏན་འཁེལ་བྱས་པའི་ལས་འགན། (T1053.002) ལ།	བཀའ་བཀོད་དང་ཡིག་གཟུགས་སྐད་སྒྱུར་མཁན། རྡ་བ་སི་ཁི་རིཔ་ཏི་ (T1059.007)
དུས་ཚོད་གཏན་འཁེལ་བྱས་པའི་ལས་འགན། དུས་ཚོད་བཀོད་པའི་ལས་ཀ། (T1053.005)	ས་གནས་ཀྱི་API(T1106)
བཀའ་བཀོད་དང་ཡིག་གཟུགས་སྐད་སྒྱུར་ཚས་(T1059)	བྱ་རིམ་བར་ཀྱི་བཅད་སྒྲིག (T1559)
བཀའ་བཀོད་དང་ཡིག་གཟུགས་སྐད་སྒྱུར་མཁན། ཕྱིན་ཅི་བཀའ་ཆོག་ཤེལ་ (T1059.003)	མ་ལག་གི་ཞབས་ཀྱུ། ཞབས་ཀྱ་ལག་བསྟར། (T1569.002)
བཀའ་བཀོད་དང་ཡིག་གཟུགས་སྐད་སྒྱུར་མཁན། པྲ་ཁར་ཤེལ་ (T1059.001)	མགོ་སྒྲིད་ཌེད་མཁན་ཀྱི་ལག་བསྟར་ཆེད་དུ་བཀོལ་སྒྲིག (T1203)
བཀའ་བཀོད་དང་ཡིག་གཟུགས་སྐད་སྒྱུར་མཁན། མཐོང་ཐོས་གཞི་རྟ (T1059.005)	བཀོལ་སྒྲིད་པའི་ལག་བསྟར། གཤོད་བཙོ་ཅན་ཀྱི་ཡིག་ཆ་(T1204.002)
བཀའ་བཀོད་དང་ཡིག་གཟུགས་སྐད་སྒྱུར་མཁན། ཡུ་ནི་ཀ་ཤེལ་ (T1059.004)	བཀའ་བཀོད་དང་ཡིག་གཟུགས་སྐད་སྒྱུར་མཁན། ཀུ་ཤུའི་ཡིག་ཆ། (T1059.002)
དུས་ཚོད་གཏན་འཁེལ་བྱས་པའི་ལས་འགན། Cron (T1053.003)	མཉེན་ཆས་བཀོལ་སྒྲིད་ལག་ཆ། (T1072)

བརྒྱུད་འགྲུལ་(TA0003)

ནུས་ལྡན་ཀྱི་རྩིས་ཁྲ་(T1078)	གསང་ལེན་མཉེན་ཆས་ཀྱི་ཆ་ཤས། དྲ་རྒྱའི་ཤྲུལ། (T1505.003)
ཡིག་ཚང་གི་མཉེན་ཆས་འགོ་འཛུགས། ཡིག་ཚང་གི་དཔེ་སྒྲོམ་མེཀ་རོ་ (T1137.001)	མ་ལག་གི་བྱ་རིམ་གསར་འཛུགས་ཡང་ན་སྒྱུར་བཅོས། ཕྱིན་ཅི་ཞབས་ཀྱ (T1543.003)
དུས་ཚོད་གཏན་འཁེལ་བྱས་པའི་ལས་འགན། (T1053.002) ལ།	འགོ་འཛུགས་ཡང་ན་ནང་འཛུལ་རང་འགུལ་འགོ་འཛུགས་ལག་བསྟར། ཐོ་འགོད་བཀོལ་སྒྲིད་ཉེ་མིག་/འགོ་འཛུགས་སྒོའི་ཐོ (T1547.001)
དུས་ཚོད་གཏན་འཁེལ་བྱས་པའི་ལས་འགན། དུས་ཚོད་བཀོད་པའི་ལས་ཀ། (T1053.005)	འགོ་འཛུགས་ཡང་ན་ནང་འཛུལ་རང་འགུལ་འགོ་འཛུགས་ལག་བསྟར། མཁྱོགས་ཐབས་བསྒྱུར་བཅོས་ (T1547.009)
ཕྱི་རོལ་གྱི་ཐག་རིང་ཞབས་ཀྱ། (T1133)	བཀུ་འཕྲོག་ལག་བསྟར་གྱི་བཀྲ་རྒྱུན། DLL འཚོལ་རིམ་འཕྲོག་པ། (T1574.001)
དུས་ཚོད་གཏན་འཁེལ་བྱས་པའི་ལས་འགན། Cron (T1053.003)	བཀུ་འཕྲོག་ལག་བསྟར་གྱི་བཀྲ་རྒྱུན། DLL ཕྱོགས་འཇུག (T1574.002)
རྩིས་ཁྲ་གཡོ་ཐབས་(T1098)	ནུས་ལྡན་རྩིས་ཁྲ། སྤྱིན་རྩིས་ཁྲ། (T1078.004)
ནུས་ལྡན་རྩིས་ཁྲ། ཁྲབ་ཁོངས་རྩིས་ཁྲ་(T1078.002)	

ཐོབ་ཐང་ཚེ་རྩ་གཏོང་བ། (TA0004)

དུས་ཚོད་གཏན་འཁེལ་བྱས་པའི་ལས་འགན། (T1053.002) ལ།	མ་ལག་གི་བྱ་རིམ་གསར་འཛུགས་ཡང་ན་སྒྱུར་བཅོས། ཕྱིན་ཅི་ཞབས་ཀྱ (T1543.003)
དུས་ཚོད་གཏན་འཁེལ་བྱས་པའི་ལས་འགན། དུས་ཚོད་བཀོད་པའི་ལས་ཀ། (T1053.005)	འགོ་འཛུགས་ཡང་ན་ནང་འཛུལ་རང་འགུལ་འགོ་འཛུགས་ལག་བསྟར། ཐོ་འགོད་བཀོལ་སྒྲིད་ཉེ་མིག་/འགོ་འཛུགས་སྒོའི་ཐོ (T1547.001)
བྱ་རིམ་འཛུག་པ། སྐྱད་པ་ལག་བསྟར་བཙན་འཕྲོག (T1055.003)	འགོ་འཛུགས་ཡང་ན་ནང་འཛུལ་རང་འགུལ་འགོ་འཛུགས་ལག་བསྟར། མཁྱོགས་ཐབས་བསྒྱུར་བཅོས་ (T1547.009)
བྱ་རིམ་འཛུག་པ། བྱ་རིམ་ཁོག་སྒོང་བཟོ་བ། (T1055.012)	བཀུ་འཕྲོག་ལག་བསྟར་གྱི་བཀྲ་རྒྱུན། DLL འཚོལ་རིམ་འཕྲོག་པ། (T1574.001)

ཐོབ་ཐང་ཆེ་རུ་གཏོང་བ། (TA0004)

ནུས་ལྡན་རྩིས་ཁྲི: ཁྲུབ་ཁོངས་རྩིས་ཁྲ་(T1078.002)	ཐོབ་ཐང་ཆེ་རུ་གཏོང་བའི་བཀོལ་སྤྱོད། (T1068)
འཇུག་སྤྱོད་བརྟག་གཞི་སྣུ། བརྟག་མཉམ་རྩིན་རྩུན་བཟོ་/རྒྱག་མ། (T1134.001)	བྱུང་རིམ་ཀྱིས་ལག་བསྟར: Unix སྣུབས་རིག་སྤྲིག་འདེམས་བཟོ་བཅོས།(T1546.004)
བྱ་རིམ་འཇུག་པ། འཐུར་ལྡན་འབེལ་རིས་ཁང་འཇུག་པ། (T1055.001)	ནུས་ལྡན་རྩིས་ཁྲི: ཁྲུབ་ཁོངས་རྩིས་ཁྲ་(T1078.002)
ནུས་ལྡན་རྩིས་ཁྲི: ས་གནས་རྩིས་ཁྲ་ (T1078.003)	

འགོག་སྐུང་བོས་བྱོལ། (TA0005)

རྩ་བའི་ལག་ཚ། (T1014)	ཐད་ཀར་མིན་པའི་བཀའ་བཀོད་ལག་བསྟར། (T1202)
སྐུན་ནག་གི་ཡིག་ཚའམ་ཚ་འཕྲིན་(T1027)	མ་ལག་གཞིས་ལྡན་གྱི་དོ་ཚབ་ལག་བསྟར: Mshta (T1218.005)
སྐུན་ནག་གི་ཡིག་ཚའམ་ཚ་འཕྲིན།: མཉེན་ཆས་ཐུམ་སྒྲིལ། (T1027.002)	མ་ལག་གཞིས་ལྡན་གྱི་དོ་ཚབ་ལག་བསྟར: Regsvr32 (T1218.010)
སྐུན་ནག་གི་ཡིག་ཚའམ་ཚ་འཕྲིན།: སྒེས་པའི་ཡི་གེ་རིག་པ། (T1027.003)	ཡིད་ཆེས་ཚོད་འཛིན་གཏོར་བརླག་གཏོང་བ།: ཞང་རྒྱས་བགོད་པ།(T1553.002)
སྐུན་ནག་གི་ཡིག་ཚའམ་ཚ་འཕྲིན།: སྐྱེལ་འདེབ་བྱེས་རྩེས་ཡྱོགས་བསྒྲིགས། (T1027.004)	ཡིག་ཚ་དང་སྡོད་ཐོའི་ཚོག་མཚན་བསྒྱར་བཅོས།: Linux དང་ Mac ཡིག་ཚ་དང་སྡོད་ཐོའི་ཚོག་མཚན་བསྒྱར་བཅོས། (T1222.002)
རྐྱ་འཕྲུལ།: ཁྱིམས་མཐུན་མིང་ཡང་ན་གནས་ས་དང་མཐུན་པ། (T1036.005)	མངོན་སུམ་ཅན་དུ་བསྒྱར་བ། ཉེ་སྐམ་གྱི་བོོས་བྱོལ།: མ་ལག་ཞིབ་བཤེར་(T1497.001)
བྱ་རིམ་འཇུག་པ།: སྐུད་པ་ལག་བསྟར་བཅན་འཕྲོག (T1055.003)	རྐྱ་འཕྲུལ (T1036)
བོད་འཚོར་བའི་ཚང་རྒྱས་མངོན་པ། (T1620)	འགོག་སྐུང་ལ་གནོད་སྐྱོན་གཏོང་བ། རིམ་པའི་མེ་སྤར་མི་ནུས་པར་བཟོ་བའམ་བསྒྱར་བཅོས། (T1562.004)
བྱ་རིམ་འཇུག་པ།: བྱ་རིམ་ཁོག་སྡོང་བཟོ་བ། (T1055.012)	ལུས་རྩལ་སྤས་པ།: གསང་བའི་ཡིག་ཚ་དང་སྡོད་ཐོ། (T1564.001)
བརྟ་སྡོན་མེད་པར་བཟོ་བ།: ཡིག་ཚ་བསུབས་པ། (T1070.004)	ལུས་རྩལ་སྤས་པ།: གསང་བའི་སྤེའུ་ཁུང་། (T1564.003)
བརྟ་སྡོན་མེད་པར་བཟོ་བ།: དུས་ཚོད་འདེམས་པ། (T1070.006)	བཀུ་འཕྲོག་ལག་བསྟར་གྱི་བཞུར་རྒྱུན།: DLL འཚོལ་རིམ་འཕྲོག་པ། (T1574.001)
བརྟ་སྡོན་མེད་པར་བཟོ་བ།: Windows འབྲུང་རིམ་ལོ་རྒྱུས་སེལ་བ། (T1070.001)	བཀུ་འཕྲོག་ལག་བསྟར་གྱི་བཞུར་རྒྱུན།: DLL ཡྱོགས་འཇུག (T1574.002)
ཐོ་འགོད་སྒྱར་བཅོས། (T1112)	དྲྭ་རྒྱའི་ཞབས་ཞུ (T1102)
ཡིག་ཚའམ་ཚ་འཕྲིན་གསལ་བ་/ཞང་སྒྱར་འདོན་པ། (T1140)	རྐྱ་འཕྲུལ།: མགོ་སྐོར་གཏོང་བའི་ལས་འགན་ཡང་ན་ཞབས་ཞུ (T1036.004)
འགོག་སྐུང་ལ་གནོད་སྐྱོན་གཏོང་བ། (T1562)	

ཚོག་མཚན་ཐོབ་ཐང་། (TA0006)

བགོལ་སྤྱོད་རིམ་ལུགས་ཡིད་ཆེས་ཡིག་ཚ་འདོན་པ།: LSASS ནང་གསོག (T1003.001)	བའེ་འཇགས་མེད་པའི་ཚོག་མཚན་ཡིག་ཚ།: ཡིག་ཚ་ནང་གི་ཚོག་མཚན་ཡིག་ཚ། (T1552.001)
བགོལ་སྤྱོད་རིམ་ལུགས་ཡིད་ཆེས་ཡིག་ཚ་འདོན་པ།: NTDS (T1003.003)	སྡོམས་ཁྲག་བཐབ་རྩོད།: གསང་ཚང་ཚོད་དཔག (T1110.001)
དྲྭ་ཚོར་ལེན། (T1040)	བཅན་ཤེད་ཀྱིས་བདེན་དཔང་བྱེད་པ། (T1187)

ཚོག་མཚན་ཐོབ་ཐང་། (TA0006)

གསང་ཨང་མཇོད་ཁང་ནས་ཚོག་མཚན། ལྷ་མིག་ཕྱེང་བ། (T1555.001)	Kerberos འཐབ་དེབ་ཀུ་བའམ་རྩྭ་བཙོ། ཀེར་བེ་རོས་ཏིང་། (T1558.003)
ནང་འཛུག་འཛིན་བཟུང་། མཐེབ་གཡོན་ཐོ་འགོག (T1056.001)	ཚ་རྒྱུན་མང་པོའི་བདེན་དཔང་བར་འཛིན། (T1111)
དྲ་རྒྱའི་དུས་ཚོད་ཀྱི་ཀུ་ཀི་རྒྱ་འཕྲོག (T1539)	རྒྱ་འཕྲོག་བྱེད་པའི་མཉེན་ཚས་འཛུལ་སྤྱོད་ཀྱི་རྟགས་མཚན། (T1528)
ཚོག་མཚན་ཐོབ་ཐབས་སུ་སྤྱོན་ཆ་བགོལ་སྤྱོད། (T1212)	སྟོབས་ཤུགས་འཐབ་ཅོར། གསང་ཨང་གཏོར་བརླག་གཏོང་བ། (T1110.002)
ནང་འཛུག་འཛིན་བཟུང་། དྲ་རྒྱའི་སྒོ་འབྱེད་འཛིན་བཟུང་། (T1056.003)	བགོལ་སྤྱོད་རིམ་ཡུགས་ཡིད་ཆེས་ཡིག་ཆ་འདོན་པ། DCSync (T1003.006)
གསང་ཨང་མཇོད་ཁང་ནས་ཚོག་མཚན། (T1555)	གསང་ཨང་མཇོད་ཁང་ནས་ཚོག་མཚན། དྲ་རྒྱའི་འཕར་ཚས་ནས་ཚོག་མཚན། (T1555.003)

གསར་རྩེད། (TA0007)

མ་ཡག་ཞབས་ཞུའི་གསར་རྩེད། (T1007)	མ་ཡག་གི་ཆ་འཕྲིན་གསར་རྩེད། (T1082)
བགོལ་སྤྱོད་སྒེའུ་ཁུང་འཆོལ་ཞིབ། (T1010)	རྩིས་ཁྲའི་གསར་རྩེད། ས་གནས་རྩིས་ཁྲ་ (T1087.001)
ཐོ་འགོད་མཇོད་འདྲི་རྩད། (T1012)	རིམ་ཡུགས་ཆ་འཕྲིན་རྩེད་པ། ཐབས་ལམ་ T1082 - འཛིན་སྐྱོང་	MITRE ATT&CK®
ཡིག་ཆ་དང་སྡོད་ཐོ་གསར་རྩེད། (T1083)	མ་ཡག་གི་དུས་ཚོད་གསར་རྩེད། (T1124)
དྲ་རྒྱའི་ཞབས་ཞུའི་གསར་རྩེད། (T1046)	མ་ཡག་གི་བདག་པོ/སྤྱོད་མཁན་གྱི་གསར་རྩེད། (T1033)
ཐག་རིང་མ་ཡག་གསར་རྩེད། (T1018)	ཁྲབ་ཁོངས་ཡིད་ཆེས་གསར་རྩེད། (T1482)
རྩིས་ཁྲའི་གསར་རྩེད། སྒོག་འཕྲིན་ཁ་བྱང་། (T1087.003)	རྩིས་ཁྲའི་གསར་རྩེད། དྲ་རྒྱའི་རྩིས་ཁྲ། (T1087.002)
མ་ཡག་དྲ་རྒྱའི་འབྲེལ་མཐུད་གསར་རྩེད། (T1049)	མངོན་སུམ་ཅན་དུ་བསྡུར་བ། ཉེ་སྐབས་ཀྱི་དོས་ཤུལ། མ་ཡག་ཞིབ་བཤེར་(T1497.001)
བྱ་རིམ་གསར་རྩེད། (T1057)	མཉེན་ཚས་གསར་རྩེད། (T1518)
ཚོག་མཚན་སྤེ་ཚན་གསར་རྩེད། ཁྲབ་ཁོངས་སྤེ་ཚན། (T1069.002)	དྲ་རྒྱ་མཉམ་སྤྱོད་རྩེད་པ། ཐབས་ལམ་ T1135 - འཛིན་སྐྱོང་	MITRE ATT&CK®
མ་ཡག་དྲ་རྒྱའི་སྒྲིག་བགོད་གསར་རྩེད། དྲ་རྒྱའི་འབྲེལ་མཐུད་གསར་རྩེད། (T1016.001)	

ཕྱོགས་གཅིག་གི་འགྲུལ་སྐྱོད། (TA0008)

ཐག་རིང་གི་ཞབས་ཞུ། ཐག་རིང་གི་ཡིག་ཆའི་ཐོག་མཐུན། (T1021.001)	ཐག་རིང་གི་ཞབས་ཞུ (T1021)
ཐག་རིང་གི་ཞབས་ཞུ། SMB/ཞིན་ཏོ་འཛིན་སྐྱོང་བགོ་བཤའ། (T1021.002)	གཞན་ཀྱི་དོས་འཛིན་རྒྱུ་ཆ་བགོལ་སྤྱོད། འཛིན་བྱང་སྤྱོད་དགོས། (T1550.003)
ཐག་རིང་གི་ཞབས་ཞུ། ཞིན་ཏོ་ཐག་རིང་འཛིན་སྐྱོང་། (T1021.006)	ཕྱོགས་གཅིག་གི་ལག་ཆ་སྤོ་བསྡུར། (T1570)

བསྡུ་སྒྲིག (TA0009)

ས་གནས་མ་ཡག་ནས་གྲངས་ཐོ། (T1005)	ཡིག་ཚགས་བསྡུ་རུབ་བྱས་པའི་གཞི་གྲངས། དཔེ་མཇོད་བརྒྱུད་ནས་ཡིག་ཚགས། (T1560.002)
དྲ་རྒྱའི་མཉམ་སྤྱོད་སྐུལ་ཚས་ནས་གྲངས་ཐོ། (T1039)	སྒོག་འཕྲིན་བསྡུ་རུབ། ཐག་རིང་སྒོག་འཕྲིན་བསྡུ་རུབ། (T1114.002)

བསྡུ་ཐུའི་གཅ (TA0009)

ནང་འཇུག་འཛིན་བཟུང་། མཐེབ་གཅོད་ཐོ་འགོད། (T1056.001)	བཏུད་སྐྱོམ་གྱི་གཞི་གྲངས། (T1115)
རང་འགྱུལ་བསྡུ་རྒྱག (T1119)	ཚ་འཕྲིན་མཛོད་ཁང་ནས་གཞི་གྲངས། (T1213)
ནང་འཇུག་འཛིན་བཟུང་། དྲ་རྒྱའི་སྐོར་འབྱེད་འཛིན་བཟུང་། (T1056.003)	གཞི་གྲངས་རིམ་པ། རྒྱང་རིང་གཞི་གྲངས་སྐྱིག་འགོད། (T1074.002)
གཞི་གྲངས་རིམ་པ། ས་གནས་གཞི་གྲངས་སྐྱིག་འགོད། (T1074.001)	བསགས་པའི་གཞི་གྲངས་མཛོད་གསོག (T1560)
སྐོག་འཕྲིན་བསྡུ་རྒྱག (T1114)	

ཕྱིར་འཐེན་བྱེད་པ། (TA0010)

C2 རྒྱུད་ལམ་བརྒྱུད་ནས་ཕྱིར་འཐེན་བྱེད་པ། (T1041)	གཞན་གྱི་སྒོས་ལམ་བརྒྱུད་ཕྱིར་འདོན། མཚུངས་པར་མེན་པའི་གསང་སྐྱོར་C2མ་ཡིན་པའི་སྒོས་ལམ་བརྒྱུད་ནས་གཞི་རྒྱུ་ཕྱིར་འདྲེན། (T1048.002)
ཐབས་གཞན་གྱི་སྒོས་མཐུན་ཐོག་ནས་ཕྱིར་འཐེན་བྱེད་པ། (T1048)	དྲ་རྒྱའི་ཞབས་ཞུའི་ཐོག་ནས་ཕྱིར་འཐེན་བྱེད་པ། སྤྲིན་པའི་གསོག་འཇོག་ལ་ཕྱིར་འཐེན་བྱེད་པ། (T1567.002)

བཀའ་འདེབས་དང་ཚོད་འཛིན་(TA0011)

གཞི་གྲངས་མྱུན་ནག་བཟོ་བ། སྒོས་ལམ་མིང་བརྗེན་བཟོ་བ། (T1001.003)	དྲ་རྒྱ་ཞབས་ཞུ། འཚི་གནས་མཉན་སྐྱོང་བ། (T1102.001)
སྤྱིར་བཏང་ཞེད་སྤྱོད་བྱེད་པའི་མཐུད་པ། (T1043)	དྲ་རྒྱ་ཞབས་ཞུ། ཕྱོགས་གཅིག་གི་འཛིལ་གཏུག། (T1102.003)
བཀོལ་སྤྱོད་བང་རིམ་སྒོས་མཐུན། དྲ་རྒྱ་སྒོས་ལམ། (T1071.001)	ནང་འཇུལ་ལག་ཆ་སྤོ་སྐྱར། (T1105)
བཀོལ་སྤྱོད་བང་རིམ་སྒོས་མཐུན། ཡིག་ཆ་སྤོ་བསྐྱར་སྒོས་མཐུན། (T1071.002)	ལས་ཚབ། ནང་ཁུལ་གྱི་ལས་ཚབ། (T1090.001)
ལས་ཚབ། ཕྱི་རོལ་གྱི་ལས་ཚབ། (T1090.002)	ཚད་ལྡན་མིན་པའི་མཐུད་ཁ། (T1571)
ལས་ཚབ། སྐ་མང་འཕྲུར་སྐྱོང་ཀྱི་ལས་ཚབ། (T1090.003)	སྒོས་མཐུན་ཕྲག་ལམ། (T1572)
དྲ་རྒྱ་ཞབས་ཞུ། ཕྱོགས་གཅིས་ཀྱི་བཅ་སྤྱོད། (T1102.002)	གསང་སྤྱོར་རྒྱུ་ལམ། (T1573)
གསང་སྤྱོར་རྒྱུ་ལམ། : འདུ་མཉམ་མེད་པའི་གསང་ཡིག་རི་མོ། (T1573.002)	ནང་འཇུལ་ལག་ཆ་སྤོ་སྐྱར། (T1105)
ཚབ་བྱེད། ཐབས་རྩལ་ T1090 - ཚོང་ལས། | MITRE ATT&CK®	

ཤུགས་རྐྱེན། (TA0040)

ཞབས་ཞུ་མཚམས་འཇོག་ཁང་། (T1489)	སྤྱབ་འགོར་སྐུབ་པ། (T1561)
མ་ཡག་ཁ་བསྟམས།/བསྐྱར་དུ་འགོ་བཙུགས། (T1529)	ཐོན་ཁྲངས་བཙན་འཕྲོག (T1496)

མཆན་འགྲེལ།

དོས་མི་ལེན་པ།

ལམ་སྟོན་འདིའི་ནང་དུ་ཡོད་པའི་རྒྱུ་ཚ་དེ་སྤྱིར་བཏང་གི་རང་བཞིན་ཡིན་པས། ཁྱིམས་ལུགས་ཀྱི་བསླབ་བྱ་ཡང་ན་གནས་སྟངས་གང་རུང་ཞིག་ལ་རོགས་རམ་བྱེད་པའི་དོན་ལ་བརྟེན་ནས་བསམ་དགོས་མི་རེད། གལ་ཆེའི་གནད་དོན་གང་རུང་ཞིག་ལ་ཁྱེད་རང་གི་གནས་སྟངས་དང་མཐུན་པའི་རང་དབང་ཅན་གྱི་ཚེད་ལས་ཀྱི་བསླབ་བྱ་འོས་འཚམ་ཞིག་ལེན་དགོས།

ཡུལ་སྤྱི་མཐུན་གྱིས་ལམ་སྟོན་འདིའི་ནང་གི་གནས་ཚུལ་ལ་བརྟེན་ནས་བྱང་བའི་གཏོང་སྐྱོན་དང་རྒྱང་ཤོར། ཚད་འཛལ་གང་རུང་ལ་འགན་ལྡོར་རམ་དབང་འདེགས་གང་ཡང་ལེན་གྱི་མེད།

པར་དབང་།

© ཨོ་སི་ཏྲེ་ལི་ཡའི་སྤྱི་མཐུན་རྒྱལ་ཁབ། 2025

རྒྱལ་ཁབ་ཀྱི་རྒྱལ་དར་དང་གཞན་དུ་བརྗོད་པའི་གནས་ཚུལ་མ་གཏོགས། དེའི་སྐུན་འདིའི་ནང་དུ་བཀོད་པའི་རྒྱུ་ཆ་ཚང་མ་ Creative Commons Attribution 4.0 International license | གསར་གཏོད་ཀྱི་སྤྱི་མཐུན་དུ་ཚོགས།

དོགས་པ་མེད་པར་བཟོ་བའི་དོན་ལས། ཚོག་མཆན་འདི་ནི་ཡིག་ཆ་འདིའི་ནང་བཀོད་པའི་དངོས་པོ་ལ་རྒྱབ་སྐྱོར་གཅིག་རེག་གནང་བའི་ཚོག་མཆན་ཡིན།

འབྲེལ་ཡོད་ཚོག་མཆན་གྱི་ཆ་རྐྱེན་གྱི་ཞིབ་ཕྲའི་གནས་ཚུལ་དེ་Creative Commons དྲ་ཚིགས་ཐོག་ཡོད། དེ་བཞིན་ CC BY 4.0 ཚོག་མཆན་གྱི་ཁྱིམས་ལུགས་སྤྱིག་གཞི | གསར་གཏོད་ཀྱི་སྤྱི་མཐུན་དུ་ཚོགས།

རྒྱལ་རྟགས་བེད་སྤྱོད།

རྒྱལ་དར་དེ་བེད་སྤྱོད་གཏོང་ཚོག་པའི་ཐ་སྙད་དེ་སྤྱི་བྱོན་དང་བཀའ་ཤག་ལས་ཁུངས་ཀྱི་དྲ་ཚིགས་ཐོག་ཞིབ་ཕྲ་བཀོད་ཡོད། སྤྱི་མཐུན་རྒྱལ་ཁབ་རྒྱལ་རྟགས་ཀྱི་ཆ་འཕྲིན་དང་ལམ་སྟོན། | pmc.gov.au.

ཞིབ་ཕྲའི་ཆ་འཕྲིན་དགོས་ན་ཡང་ན་སྐར་ཆ་བདེ་འཇགས་ཀྱི་དཀའ་ངལ་ཞིག་སྐྱན་སེང་བྱེད་དགོས་ན་ང་ཚོ་དང་འབྲེལ་བ་འདྲིས་པར་བྱོས།

cyber.gov.au | ༡༣༠༠ CYBER1 (༡༣༠༠ ༢༩༣ ༣༧༡)

དེའི་ཚང་མི་རྐྱ་པར་ཚོས་ཏེ་ལི་ཡན་གྱི་ནང་མི་ལྟར་འགྱུར་ཚུལ་ལུ་ཡོད།

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre