APT40 གྲོས་སྒོག།

PRC MSS ཚོང་ལས་ལག་རྩལ་ལག་ལེན་ནང་

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**

内閣サイバーセキュリティセンター

National center of Incident readiness and
Strategy for Cybersecurity

警察庁

National Police Agency

དཀར་ཆག

བསྡུད་དོན།

རྒྱབ་སྐྱོར།

འདི་ཡང་གོས་སྐྱོན་འདི་ ཨའུས་ཏེ་ལི་ཡའི་བཏ་མཚོན་བགོད་ཁྲབ་ལས་སྐྱོར་ཀྱི་ཨའུས་ཏེ་ལི་ཡའི་ཡོངས་འབྲེལ་ཉེན་སྐྱོང་སྐྱེ་བ་ (ASD's ACSC)| ཨ་མེ་རི་ཀའི་ཡོངས་འབྲེལ་ཉེན་སྐྱོང་དང་གཞི་རྟེན་སྤྱོར་མཐུད་བདེ་འཐགས་ལས་སྐྱོར་ (CISA)| ཨ་མེ་རི་ཀའི་རྒྱལ་ཡོངས་ཡོངས་འབྲེལ་ཉེན་སྐྱོང་ལས་སྐྱོར་ (NSA)| ཨ་མེ་རི་ཀའི་སྤྱི་མཐུན་ཞིབ་འཚུག་ལས་སྐྱོར་ (FBI)| ཡུ་ནའི་ཊེཊ་ཀིང་ཏམ་གྱི་རྒྱལ་ཡོངས་ཡོངས་འབྲེལ་ཉེན་སྐྱོང་སྐྱེ་བ་ (NCSC-UK)| ཀེ་ན་ཌའི་དུ་རྒྱའི་བདེ་འཐགས་སྐྱེ་བ་ (CCCS)| ནིའུ་ཛི་ལེནཌ་གྱི་རྒྱལ་ཡོངས་དུ་རྒྱའི་བདེ་འཐགས་སྐྱེ་བ་ (NCSC-NZ)| ཌར་མ་ནིའི་སྤྱི་མཐུན་གསང་བའི་ཞབས་རྟོག (BND) དང་རུ་ཁྲིམས་སྐྱང་སྤྱོད་སྤྱི་མཐུན་ཨིག་ཚང་ (BfV)| ཀོ་རི་ཡ་སྤྱི་མཐུན་རྒྱལ་ཁབ་ཀྱི་རྒྱལ་ཡོངས་གསང་བའི་ལས་ཁྲངས་ (NIS) དང་ NIS ཀྱི་རྒྱལ་ཡོངས་ཡོངས་འབྲེལ་ཉེན་སྐྱང་སྐྱེ་བ། དེ་བཟུམ་སྟེ་ ཇ་པཱན་གྱི་ཡོངས་འབྲེལ་ཉེན་སྐྱང་བྱང་ཆུབ་ཀྱི་གྲ་སྒྲིག་དང་ཐབས་བྱས་རྒྱལ་ཡོངས་སྐྱེ་བ་ (NISC) དང་རྒྱལ་ཡོངས་ཁྲིམས་སྐྱང་ལས་ཁྲངས་ (NPA) སོགས་– འདི་གི་ཤུལ་ལས་ “རྩོམ་བྱིས་ལས་སྟེ་ཚུ་” ཞེས་བརྗོད། རྒྱ་ནག་མི་སེར་སྤྱི་མཐུན་རྒྱལ་ཁབ་ (PRC) གི་རྒྱལ་ཁབ་ཀྱིས་རྒྱབ་སྐྱོར་བྱས་པའི་དྲ་རྒྱའི་སྟེ་ཚན་དང་། ཁོང་ཚུ་གི་དཔྱའི་ཞའུས་ཏེ་ལི་ཡའི་དྲ་རྒྱའི་མཐུན་ཤུན་ལུ་ཉེན་ཁ་འདི་གསལ་བཀོད་འབད་ཡོདཔ་ཨིན།

གོས་སྐྱོན་འདི་གིས་ རྩོམ་བྱིས་ལས་སྟེ་ཚུ་གིས་ ཉེན་ཁ་གི་སྐོར་ལས་ མཉམ་ཀྱི་ཉ་གོ་ ཐབས་དང་། དེ་བཞིན་ ASD གི་ ACSC གི་བྱང་རྒྱན་ལན་འདེབས་ཞིབ་འཚུག་ཚུ་ལུ་ གཞི་བཞག་སྟེ་ཨིན། རྒྱ་ནག་གཞུང་གི་ (PRC) མངའ་སྡེ་གི་རྒྱབ་སྐྱོར་འབད་མི་ཡོངས་འབྲེལ་སྟེ་ཚན་ཀྱིས་ ཉེ་མ་ ཨོསི་ཏེ་ལི་ཡ་དང་ཨ་མེ་རི་ཀ་རྩིས་ཉེ་ རྒྱལ་ཁབ་མ་འདུམ་ཚུ་ཏང་ དཔལ་གསལ་བ་ དཔལ་ཡོན་ཅན་ཚུ་ཁ་ཤས་ཀྱི་ཐབས་ལམ་ཚུ་ཏང་ ལས་སྟེ་ཚུ་ལུ་ དཔལ་གསལ་འབེན་བསྒྲིད་དེ་ཡོདཔ་ད་ གཤམ་གསལ་ཀྱི་ཐབས་ལམ་ཚུ་ འཛམ་གླིང་ནང་ རྒྱ་ནག་གཞུང་གི་རྒྱབ་སྐྱོར་འབད་མི་ཉམས་ཆུང་ཏེ་ཡོདཔ་ད་ གཤམ་གསལ་ཀྱི་ཐབས་ལམ་ཚུ་ འཛམ་གླིང་ལས་ སྟེ་ཚན་ཁག་ཅིག་ཁར་འབྲེལ་བ་ཡོདཔ་ཨིན། ཨོསི་ཏེ་ལི་ཡ་དང་ཨ་མེ་རི་ཀ་རྩིས་ཉེ་ རྒྱལ་ཁབ་ཀྱི་ཉ་གོ་ ཐབས་ལམ་ཚུ་ཏང་ ཨ་རྒྱུས་ཏེ་ལི་ཡའི་ཡོངས་འབྲེལ་ཉེན་སྐྱང་སྐྱེ་བ་ (ASD's ACSC)| ཨ་མེ་རི་ཀའི་ཡོངས་འབྲེལ་ཉེན་སྐྱང་དང་གཞི་རྟེན་སྤྱོར་མཐུད་བདེ་འཐགས་ལས་སྐྱོར་ (CISA)| ཨ་མེ་རི་ཀའི་རྒྱལ་ཡོངས་ཡོངས་འབྲེལ་ཉེན་སྐྱང་ལས་སྐྱོར་ (NSA)| ཨ་མེ་རི་ཀའི་སྤྱི་མཐུན་ཞིབ་འཚུག་ལས་སྐྱོར་ (FBI)| ཡུ་ནའི་ཊེཊ་ཀིང་ཏམ་གྱི་རྒྱལ་ཡོངས་ཡོངས་འབྲེལ་ཉེན་སྐྱང་སྐྱེ་བ་ (NCSC-UK)| ཀེ་ན་ཌའི་དུ་རྒྱའི་བདེ་འཐགས་སྐྱེ་བ་ (CCCS)| ནིའུ་ཛི་ལེནཌ་གྱི་རྒྱལ་ཡོངས་དུ་རྒྱའི་བདེ་འཐགས་སྐྱེ་བ་ (NCSC-NZ)| ཌར་མ་ནིའི་སྤྱི་མཐུན་གསང་བའི་ཞབས་རྟོག (BND) དང་རུ་ཁྲིམས་སྐྱང་སྤྱོད་སྤྱི་མཐུན་ཨིག་ཚང་ (BfV)| ཀོ་རི་ཡ་སྤྱི་མཐུན་རྒྱལ་ཁབ་ཀྱི་རྒྱལ་ཡོངས་གསང་བའི་ལས་ཁྲངས་ (NIS) དང་ NIS ཀྱི་རྒྱལ་ཡོངས་ཡོངས་འབྲེལ་ཉེན་སྐྱང་སྐྱེ་བ། དེ་བཟུམ་སྟེ་ ཇ་པཱན་གྱི་ཡོངས་འབྲེལ་ཉེན་སྐྱང་བྱང་ཆུབ་ཀྱི་གྲ་སྒྲིག་དང་ཐབས་བྱས་རྒྱལ་ཡོངས་སྐྱེ་བ་ (NISC) དང་རྒྱལ་ཡོངས་ཁྲིམས་སྐྱང་ལས་ཁྲངས་ (NPA) སོགས་– འདི་གི་ཤུལ་ལས་ “རྩོམ་བྱིས་ལས་སྟེ་ཚུ་” ཞེས་བརྗོད། རྒྱ་ནག་མི་སེར་སྤྱི་མཐུན་རྒྱལ་ཁབ་ (PRC) གི་རྒྱལ་ཁབ་ཀྱིས་རྒྱབ་སྐྱོར་བྱས་པའི་དྲ་རྒྱའི་སྟེ་ཚན་ཁག་ཅིག་ཁར་འབྲེལ་བ་ཡོདཔ་ཨིན། ཁོང་ཚུ་གི་དཔྱའི་ཞའུས་ཏེ་ལི་ཡའི་དྲ་རྒྱའི་མཐུན་ཤུན་ལུ་ཉེན་ཁ་འདི་གསལ་བཀོད་འབད་ཡོདཔ་ཨིན།

གོས་སྐྱོན་འདི་གིས་ རྩོམ་བྱིས་ལས་སྟེ་ཚུ་གིས་ ཉེན་ཁ་གི་སྐོར་ལས་ མཉམ་ཀྱི་ཉ་གོ་ ཐབས་དང་། དེ་བཞིན་ ASD གི་ ACSC གི་བྱང་རྒྱན་ལན་འདེབས་ཞིབ་འཚུག་ཚུ་ལུ་ གཞི་བཞག་སྟེ་ཨིན། རྒྱ་ནག་གཞུང་གི་ (PRC) མངའ་སྡེ་གི་རྒྱབ་སྐྱོར་འབད་མི་ཡོངས་འབྲེལ་སྟེ་ཚན་ཀྱིས་ ཉེ་མ་ ཨོསི་ཏེ་ལི་ཡ་དང་ཨ་མེ་རི་ཀ་རྩིས་ཉེ་ རྒྱལ་ཁབ་མ་འདུམ་ཚུ་ཏང་ ལས་སྟེ་ཚུ་ལུ་ དཔལ་གསལ་འབེན་བསྒྲིད་དེ་ཡོདཔ་ད་ གཤམ་གསལ་ཀྱི་ཐབས་ལམ་ཚུ་ འཛམ་གླིང་ནང་ རྒྱ་ནག་གཞུང་གི་རྒྱབ་སྐྱོར་འབད་མི་ཉམས་ཆུང་ཏེ་ཡོདཔ་ད་ གཤམ་གསལ་ཀྱི་ཐབས་ལམ་ཚུ་ འཛམ་གླིང་ལས་ སྟེ་ཚན་ཁག་ཅིག་ཁར་འབྲེལ་བ་ཡོདཔ་ཨིན།

ཇོ་མ་སྨྲིག་ལས་སྟེ་ཚུ་གིས་ སྟེ་ཚན་འདི་གིས་ རྒྱ་ནག་གཞུང་གི་ (PRC) སྤུང་སྐྱོང་ལྷན་ཁག་གི་ (MSS) དོན་ལུ་ གཞོད་དཔ་ཅན་གྱི་ཡོངས་འབྲེལ་གྱི་ལུ་ཚུ་ འགོ་འདྲེན་འཐབ་དོ་ཡོདཔ་སྟེ་ བརྒྱུད་ཞིབ་འབདཔ་ཨིན། གནས་སྐབས་དང་ཐབས་ཤེས་ཚུ་ Advanced Persistent Threat (APT) 40 ཟེར་བའི་སྟེ་ཚན་གྱི་ཐོག་ལས་རྟེས་སུ་འབྱང་སྟེ་བཟུམ་མི་ཚུ་དང་མཉམ་དུ་གཅིག་ཁར་འགོ་འདྲེ། ᔑ འདི་ཡང་ཆོང་ལས་ཀྱི་སྐབས་ཐོའི་ནང་ལུ་ Kryptonite Panda, GINGHAM TYPHOON, Leviathan དང་ Bronze Mohawk ཟེར་ཡང་སྐབ་མས།[1] སྟེ་ཚན་འདི་ གྱང་གོའི་མི་དམངས་སྤྱི་མཐུན་རྒྱལ་ཁབ་ (PRC) ཀྱི་ དཔེ་ནན་ཞིང་ཆེན་ཀྱི་ དཔེ་ཀོའུ་ལུ་ གཞི་རྟེན་བཙུགས་ཏེ་ གྱང་གོའི་མི་དམངས་སྤྱི་མཐུན་རྒྱལ་ཁབ་ (PRC) ཀྱི་ གསང་བའི་སྤུང་སྐྱོང་ལས་ཁྲངས་ དཔེ་ནན་རྒྱལ་ཁབ་བདེ་འཐགས་ལས་ཁྲངས་ནང་ལས་ ལས་འགན་ལེན་མི་སྟེ་ སྤྱན་ལྟ་ཞིབ་ཚད་ཀྱི་ ཨ་རྒྱུས་ཏེ་ལི་ཡ་དང་ཨ་མེ་རི་ཀ་རྩིས་ཉེ་ རྒྱལ་ཁབ་མ་འདུམ་ཚུ་ཏང་ ཉམས་སྐྱང་བའི་ཡོངས་འབྲེལ་ གཞི་རྟེན་ལུ་ ཉ་སྤྱོད་འབད་བའི་སྐབས་ དགུ་བོ་འདི་གི་ཐབས་ཤེས་ཚུ་གི་ གཡ་གནད་ཅན་

གོས་སྐྱོན་འདི་གིས་ རྩོམ་བྱིས་ལས་སྟེ་ཚུ་གིས་ ཉེན་ཁ་གི་སྐོར་ལས་ མཉམ་ཀྱི་ཉ་གོ་ ཐབས་དང་། དེ་བཞིན་ ASD གི་ ACSC གི་བྱང་རྒྱན་ལན་འདེབས་ཞིབ་འཚུག་ཚུ་ལུ་ གཞི་བཞག་སྟེ་ཨིན། རྒྱ་ནག་གཞུང་གི་ (PRC) མངའ་སྡེ་གི་རྒྱབ་སྐྱོར་འབད་མི་ཡོངས་འབྲེལ་སྟེ་ཚན་ཀྱིས་ ཉེ་མ་ ཨོསི་ཏེ་ལི་ཡ་དང་ཨ་མེ་རི་ཀ་རྩིས་ཉེ་ རྒྱལ་ཁབ་མ་འདུམ་ཚུ་ཏང་ ལས་སྟེ་ཚུ་ལུ་ དཔལ་གསལ་འབེན་བསྒྲིད་དེ་ཡོདཔ་ད་ གཤམ་གསལ་ཀྱི་ཐབས་ལམ་ཚུ་ འཛམ་གླིང་ལས་ སྟེ་ཚན་ཁག་ཅིག་ཁར་འབྲེལ་བ་ཡོདཔ་ཨིན།

བྱ་བའི་བསྡུད་དོན།

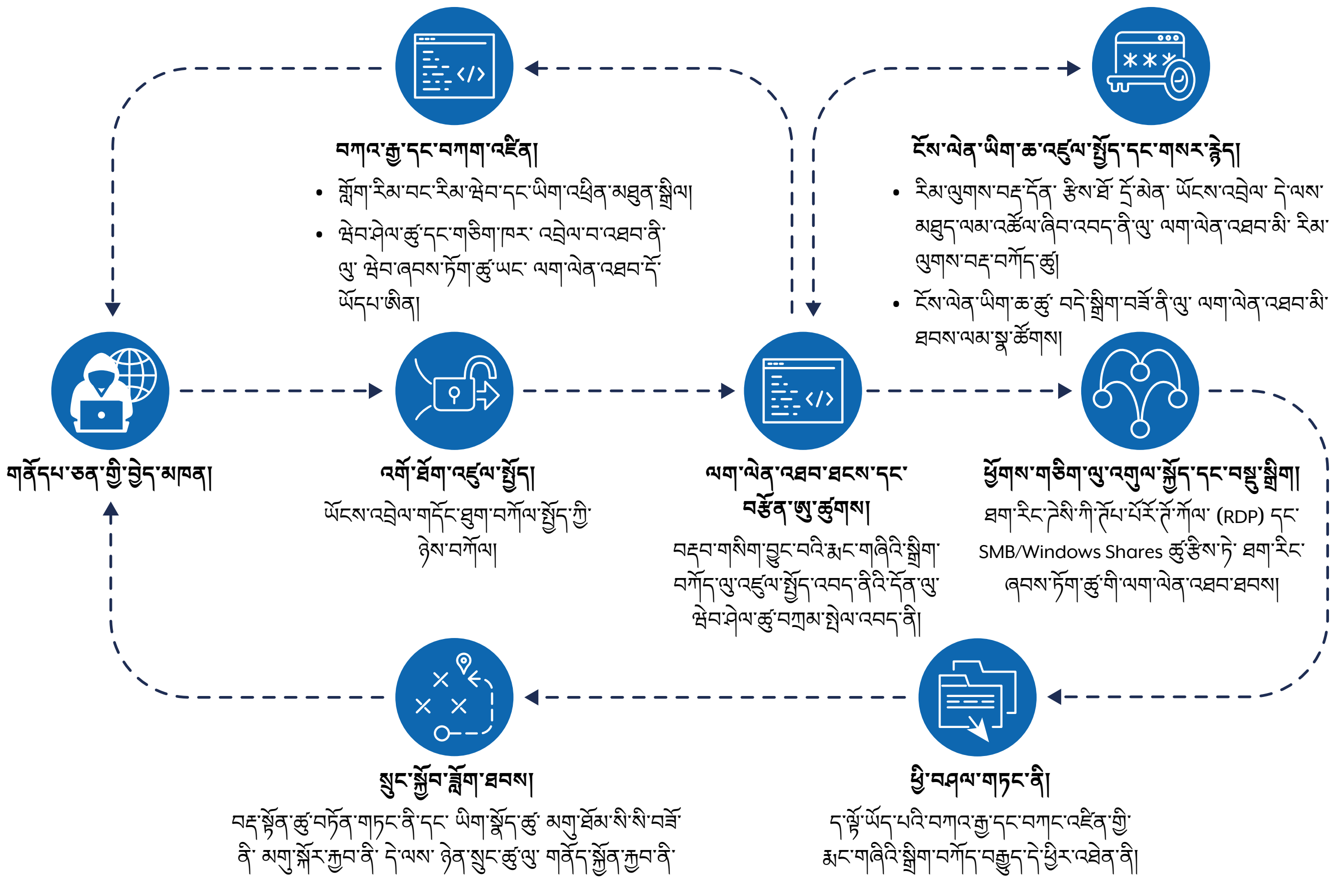
APT40 གིས་ ཨོསི་ཏེ་ལི་ཡ་གི་ཡོངས་འབྲེལ་དང་ ཡུང་ཕྱོགས་ནང་ གཞུང་དང་སྒེར་སྟེ་གི་ཡོངས་འབྲེལ་ཚུ་ལུ་ བསྒྲུར་ཡོག་དམིགས་གཏད་བསྒྲིད་དེ་ཡོདཔ་ལས་ ང་བཅས་རའི་ཡོངས་འབྲེལ་ཚུ་ལུ་ ཉེན་ཁ་བྱང་མི་འདི་ འཛོ་མཐུད་དེ་རང་ འབྱང་དོ་ཡོདཔ་ཨིན། གོས་སྐྱོན་འདི་ཡང་ ཨ་རྒྱུས་ཏེ་ལི་ཡ་དང་ཨ་མེ་རི་ཀ་རྩིས་ཉེ་ རྒྱལ་ཁབ་མ་འདུམ་ཚུ་ཡོངས་འབྲེལ་ཉེན་སྐྱང་ལས་ཀྱི་ དུས་རྒྱུན་དུ་ ཨོསི་ཏེ་ལི་ཡ་གི་ཡོངས་འབྲེལ་ཚུ་ལུ་ བསྒྲུར་ཡོག་བཏང་ཡོདཔ་ཨིན།

གཡ་ཆེ་བའི་གནད་དོན་སྟེ་ APT40 ལུ་ ཉེན་ཁ་གསར་པ་ཚུ་གི་ལག་ལེན་འཐབ་ཐབས་ཀྱི་ འཐུག་ཆ་གྲུབ་འབྲས་ (POCs) ཚུ་ མཉོགས་པར་ བསྒྲུར་བཅོས་འབད་དེ་ མཐུན་སྒྲིག་འབད་ཚུགས་པའི་སྟེང་གས་ཡོད་མ་ཚད་ འཛེལ་བའི་ཉེན་ཁ་དེ་གི་གནས་རིམ་ཡུགས་ཡོངས་ཀྱི་ ཐབས་ལམ་ཚུ་ ཉེན་ཁ་བྱང་མི་འདི་ འཛོ་མཐུད་དེ་རང་ འབྱང་དོ་ཡོདཔ་ཨིན། APT40 གིས་ དུས་རྒྱུན་དུ་ ཇོ་མ་སྨྲིག་ལས་སྟེ་ཚུ་གི་རྒྱལ་ཁབ་ཚུ་ལུ་ ཡོངས་འབྲེལ་ཉེན་སྐྱང་ལས་ཀྱི་ སྤྱི་བ་ཡོངས་འབྲེལ་ཉེན་སྐྱང་ལས་ཀྱི་ ཐབས་ལམ་ཚུ་ ཉེན་ཁ་དེ་གི་གནས་རིམ་ཡུགས་ཡོངས་ཀྱི་ ཐབས་ལམ་ཚུ་ ཉེན་ཁ་བྱང་མི་འདི་ འཛོ་མཐུད་དེ་རང་ འབྱང་དོ་ཡོདཔ་ཨིན། ད་ལྟོ་ཡོངས་ཁྱོད་ཀྱི་ བཅའ་ཁྲིམས་ཀྱི་ ཐབས་ལམ་ཚུ་ ཉེན་ཁ་བྱང་མི་འདི་ འཛོ་མཐུད་དེ་རང་ འབྱང་དོ་ཡོདཔ་ཨིན། ཨ་རྒྱུས་ཏེ་ལི་ཡ་དང་ཨ་མེ་རི་ཀ་རྩིས་ཉེ་ རྒྱལ་ཁབ་མ་འདུམ་ཚུ་ཡོངས་འབྲེལ་ཉེན་སྐྱང་ལས་ཀྱི་ ཐབས་ལམ་ཚུ་ ཉེན་ཁ་བྱང་མི་འདི་ འཛོ་མཐུད་དེ་རང་ འབྱང་དོ་ཡོདཔ་ཨིན།

APT40 གིས་ ཁྱབ་ཆེ་བའི་ལག་ལེན་འཐབ་མི་ མཉེན་ཆས་ Log4J (CVE 2021 44228) Atlassian Confluence (CVE-2021-31207, CVE-2021-26084) དང་ Microsoft Exchange (CVE-2021-31207, CVE-2021-34523, CVE-2021-34473) བཟུམ་གྱི་ནང་གི་ མི་མང་ལུ་ཤེས་རྟོགས་ཡོད་པའི་ཉེན་ཁ་གསར་པ་ཚུ་ མཉོགས་སྐྱར་དུ་ ལག་ལེན་འཐབ་ཨིན། ASD གི་ ACSC དང་ ཇོ་མ་སྨྲིག་ལས་ཁྲངས་ཚུ་ གིས་ སྟེ་ཚན་འདི་གིས་ མི་མང་ལུ་གསལ་བསྒྲགས་འབད་བའི་ཁྱབ་ལས་ ཆུ་ཚོད་ཡང་ན་ ཉེན་ཁ་གསར་ཀྱི་ ནང་ལ་ཁོད་ལུ་ མཐོ་རིམ་ཚུ་ཏང་ དེ་བཞིན་ POCs འཛོ་མཐུད་དེ་ ལག་ལེན་འཐབ་ནི་གི་རེ་བ་བསྒྲིད་པ་ཨིན།

2 ཨ་མ་རི་ཀཱའི་ཁྲིམས་འཛིན་ལས་ཁང་། 2021 གསང་བའི་སྤུང་སྐྱོང་ལས་ཁྲངས་དང་གཅིག་ཁར་ལཱ་སྟའབད་མ་ཨི་རྒྱག་གི་མི་སེར་བཙན་སེལ་དབང་ཐང་ཆོད་བཏགས་དང་ གསང་བའི་ཆོད་བཏགས་ཀྱི་ཡི་གེ། https://www.justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion-campaign-targeting

པར་རིས་ ༧ པ། APT40 ལས་འགུལ་གྱི་དོན་ལུ་ TTP འགྲོ་རིམ་ཁ་ཐུག་རེའུ་མིག།



འ་ནི་སྡེ་ཚན་འདི་གིས་ ཕི་ཤིང་སྐྱུལ་བསྒྲགས་བཟུམ་གྱི་ ལག་ལེན་པ་ཚུ་གིས་ འབྲེལ་བ་འཐབ་དགོ་པའི་ ཐབས་ལམ་ཚུ་ལས་ མི་མང་ལུ་གདོང་ལེན་འབད་ཚུགས་པའི་ ཉེན་ཁ་ཅན་གྱི་གཞི་རྟེན་རིམ་ལུགས་ཚུ་ ལག་ལེན་འཐབ་ནི་ལུ་ དགའ་འདོད་ཡོད་པ་གི་མ་ཚད་ ཤུལ་ལས་ལག་ལེན་མ་འདྲ་བ་ཚུ་ འབད་ཚུགས་ནི་གི་དོན་ལུ་ ཆ་གནས་ཅན་གྱི་ ངེས་གཏན་ཡིག་ཆ་ཚུ་ ཐོབ་ནི་ལུ་ གསོ་རིམ་སྒོམ་སྒྲེ་ བཞག་དོ་ཡོདཔ་ཨིན། APT40 གིས་ དུས་རྒྱུན་དུ་ ཕྲེབ་ཤེལ་ ([T1505.003](#)) འདི་ བརྟན་ཧྲོག་ཧོ་གི་དོན་ལུ་ ལག་ལེན་འཐབ་ཨིན་ དམིགས་བསལ་གྱིས་ བཙན་འཛུལ་གྱི་མི་ཚེ་འཁོར་རིམ་འགོ་བཙུགས་པའི་སྐབས་ལུ་ཨིན། ཕྱིར་བཏང་ལུ་ འགོ་ཐོག་འཛུལ་སྤྱོད་མཐར་འཁྱོལ་ཅན་ཅིག་འབྱུང་བའི་ཤུལ་ལས་ APT40 གིས་ ཉམས་རྒྱུདཔ་གི་མཐའ་འཁོར་གནས་སྟངས་ནང་ འཛུལ་སྤྱོད་འབད་ཚུགས་པའི་ བརྟན་ཤུགས་གཞི་བཙུགས་འབད་ནི་ལུ་ གཙོ་བོར་སྟོནམ་ཨིན། ཨིན་རུང་ བཙན་འཛུལ་གྱི་སྐབས་ལུ་ བརྟན་ཤུགས་འདི་ ཧེ་མ་ལས་རང་ འབྱུང་དོ་ཡོདཔ་ལས་ བདེ་སྲུག་དང་ བྱ་སྤྱོད་ག་དེ་ཅིག་འབད་རུང་ བཙན་འཛུལ་ག་རའི་ནང་ལུ་ མཐོང་ཚུགས་ནི་གི་འོས་འབབ་ཡོདཔ་ཨིན་མས།

གལ་ཆེ་བའི་ཚོང་ལས་ལག་རྩལ།

APT40 གིས་ ཧེ་མ་ལས་ བཀོལ་སྤྱོད་ཀྱི་དོན་ལུ་ བརྡ་བཀོད་དང་ཚད་འཛིན་ (C2) ཌོསི་ཏེ་སྦེ་ བདེ་སྲུག་བཟོ་ཡོད་པའི་ ཨསི་ཏེ་ལི་ཡ་གི་ཡོངས་འབྲེལ་འཆར་སྒོ་ཚུ་ ལག་ལེན་འཐབ་ཡོདཔ་ཨིན་རུང་ སྡེ་ཚན་འདི་གིས་ ཐབས་ལམ་འདི་ གོང་འཕེལ་བཏང་ཡོདཔ་ཨིན། ([T1594](#))

APT40 གིས་ འཛམ་གླིང་ཡོངས་ཁྱབ་ཀྱི་ ཡིག་ཚང་ཆུང་བ་/ཁྱིམ་ཡིག་ཚང་ (SOHO) ཅ་ཆས་ཚུ་རྩིས་ཏེ་ བདེ་སྲུག་བཟོ་ཡོད་པའི་ ཅ་ཆས་ཚུ་ ལག་ལེན་འཐབ་ནིའི་ གཞི་རྟེན་དང་ མཇུག་མཐའི་ ཧོབ་བསྐྱུར་ལོག་འབད་མི་ ([T1584.008](#)) ཚུ་ ཨོསི་ཊེ་ལི་ཡ་ལུ་ ལག་ལེན་འཐབ་ནིའི་དོན་ལུ་ ལག་ལེན་འཐབ་ནི་གི་ འགྲོས་ལུ་ ངོས་ལེན་འབད་ཡོདཔ་ཨིན། འདི་གིས་ རྩོམ་བྲིས་ལས་སྡེ་ཚུ་ལུ་ སྡེ་ཚན་འདི་གི་འགྱོ་སྟངས་ཚུ་ ལེགས་ཤོམ་སྦེ་ ཁྱད་ཆོས་བཏོན་ཚུགས་ནི་དང་ བརྟག་ཞིབ་འབད་ཚུགས་ནི་ལུ་ ཕན་ཐོགས་བྱུང་ཡོདཔ་ཨིན།

འ་ནི་ SOHO ཡོ་ཆས་མང་ཤོས་ཅིག་ མི་ཚེ་མཇུག་བསྡུ་ཡོད་མི་ ཡང་ན་ སྐྱོན་བཅོས་མ་འབད་མི་ཚུ་ཨིནམ་ལས་ N-day ལག་ལེན་འཐབ་ནི་གི་དོན་ལུ་ དམིགས་གཏད་འཇམ་པོ་ཅིག་ བྱིན་དོ་ཡོདཔ་ཨིན། བདེ་སྲུག་བཟོ་ཚར་བའི་ཤུལ་ལས་ SOHO ཡོ་ཆས་ཚུ་གིས་ ཁྲིམས་མཐུན་འགྱུལ་སྐྱོད་དང་ མཉམ་དུ་སླ་བསྲེ་རྐྱབ་དེ་ དྲ་རྒྱ་སྲུང་སྐྱོབ་པ་ཚུ་ལུ་ དཀའ་ངལ་བཀལ་ནི་གི་དོན་ལུ་ བཟོ་བཀོད་འབད་ཡོད་པའི་ གནོད་སྐྱོན་རྐྱབ་ནི་གི་དོན་ལུ་ འགོ་བཙུགས་སའི་ས་སྒོ་ཅིག་ བྱིན་དོ་ཡོདཔ་ཨིན། ([T1001.003](#))

འ་ནི་ཐབས་ལམ་འདི་ འཛམ་གླིང་ནང་ལུ་ གཞན་མི་པི་ཨར་སི་མངའ་སྡེ་གིས་རྒྱབ་སྐྱོར་འབད་མི་ བྱེད་མཁན་ཚུ་གིས་ཡང་ དུས་རྒྱུན་དུ་ར་ལག་ལེན་འཐབ་དོ་ཡོདཔ་དང་ རྩོམ་བྲིས་ལས་སྡེ་ཚུ་གིས་ འ་ནི་འདི་ ཉེན་ཁ་མཉམ་རུབ་ཅིག་སྦེ་བརྩི་དོ་ཡོདཔ་ཨིན། བརྡ་དོན་ཁ་སྐོང་དོན་ལུ་ མཉམ་འབྲེལ་གྱི་གྲོས་སྟོན་ཚུ་བལྟ། [རྒྱ་ནག་མི་དམངས་སྤྱི་མཐུན་རྒྱལ་ཁབ་ཀྱིས་རྒྱབ་སྐྱོར་འབད་མི་ སྤྱི་འཐུས་གློག་རིག་འཁྲབ་སྟོན་པ་ཚུ་གིས་ དྲ་རྒྱ་སྤྲིན་མཁན་དང་ ཡོ་ཆས་ཚུ་ ལག་ལེན་འཐབ་དོ་ཡོདཔ།](#) དང་ [PRC རྒྱལ་ཁབ་ཀྱིས་རྒྱབ་སྐྱོར་འབད་མི་ འཁྲབ་སྟོན་པ་ཚུ་གིས་ ཨེ་རི་གི་གལ་ཆེ་བའི་གཞི་རྟེན་རིམ་ལུགས་ལུ་ བདེ་སྲུག་བཟོ་དེ་ རྟག་བརྟན་འཛུལ་ཞུགས་ ཉར་སྲུང་འབད་དོ་ཡོདཔ།](#)

APT40 གིས་ འཕྲལ་འཕྲལ་སྐབས་ མགོ་སྐྲུན་འབད་མི་དང་ ཡང་ན་ གླ་ཁར་ལེན་ཡོད་པའི་ གཞི་རྟེན་མཐུན་རྐྱེན་ཚུ་ ཉམས་རྒྱུདཔ་ལུ་གདོང་ལེན་འབད་མི་ C2 མཐུན་རྐྱེན་སྦེ་ ལག་ལེན་འཐབ་ཨིན། ཨིན་རུང་ ཚོང་ལས་ལག་རྩལ་འདི་ མར་ཕབ་འགྱོ་དོ་བཟུམ་ཅིག་འདུག།

ལག་ཆས་བཟོ་ནི།

ASD གི་ ACSC གིས་ གཤན་གསལ་གྱི་ཞིབ་དཔྱད་ཚུ་གི་སྐབས་ལུ་ དོས་འཛིན་འབད་མི་ གནོད་པ་ཅན་གྱི་ཡིག་སྟོད་ལ་ལུ་ཅིག་ མཉམ་བགོ་འབད་དོ་ཡོདཔ་ཨིན། ཡིག་སྟོད་འདི་ཚུ་ ཐབེ་རྟསི་ཏོ་ཀལ་ནང་ སྐྱེལ་བཙུགས་འབད་དེ་ཡོདཔ་ད་ དེ་ཡང་ ཡོངས་འབྲེལ་གྱི་ ཉེན་སྐྱང་དང་ ཡོངས་འབྲེལ་གྱི་ ཉེན་སྐྱང་མི་སྟེ་ཚུ་གིས་ ཉེན་ཁ་ཚུ་ ལེགས་ཤོམ་སྟེ་ ཏ་གོ་ཚུགས་ནིའི་དོན་ལུ་ཨིན་པས།

གནད་དོན་ཞིབ་འཇུག་ཚུ།

ASD གི་ ACSC གིས་ བྱེད་མཁན་ཚུ་གིས་ ཁོང་རའི་ལག་ཆས་དང་ ཚོང་འབྲེལ་གྱི་ ལག་ཆས་ཚུ་ གཅེ་སྟེ་ལག་ལེན་འཐབ་ཨིན་ན་ གོ་བ་བརྟག་སྟེན་འབད་ནི་གི་དོན་ལུ་ མིང་མ་བགོད་པའི་ ཞིབ་དཔྱད་སྐྱན་ཞུ་གཏིས་ བརྟེས་འབད་དོ་ཡོདཔ་ཨིན།

MD5	ཡིག་སྟོད་མིང་།	བརྟ་དོན་ཁ་སྐོང་།
26a5a7e71a601be991073c78d513dee3	horizon.jsp	kB ༧ | ངོ་བ་འབྲུང་ཁུངས།
87c88f06a7464db2534bc78ec2b915de	Index_jsp$ProxyEndpoint$Attach.class	B ५৫৩ | ངོ་བ་བྱའིའི་ཀོད།
6a9bc68c9bc5cefaf1880ae6ffb1d0ca	Index_jsp.class	kB ५ | ངོ་བ་བྱའིའི་ཀོད།
64454645a9a21510226ab29e01e76d39	Index_jsp.java	kB ५ | ངོ་བ་འབྲུང་ཁུངས།
e2175f91ce3da2e8d46b0639e941e13f	Index_jsp$ProxyEndpoint.class	kB ৬ | ངོ་བ་བྱའིའི་ཀོད།
9f89f069466b8b5c9bf25c9374a4daf8	Index_jsp$ProxyEndpoint$1.class	kB ३ | ངོ་བ་བྱའིའི་ཀོད།
187d6f2ed2c80f805461d9119a5878ac	Index_jsp$ProxyEndpoint$2.class	kB ༧ | ངོ་བ་བྱའིའི་ཀོད།
ed7178cec90ed21644e669378b3a97ec	Nova_jsp.class	kB ৩ | ངོ་བ་བྱའིའི་ཀོད།
5bf7560d0a638e34035f85cd3788e258	Nova_jsp$TomcatListenerMemShellFromThread.class	kB ८ | ངོ་བ་བྱའིའི་ཀོད།
e02be0dc614523ddd7a28c9e9d500cff	Nova_jsp.java	kB ২৫ | ངོ་བ་འབྲུང་ཁུངས།

གནད་དོན་ཞིབ་འཇུག་ ༧

སྐན་ཞུ་འདི་ ཁྲབ་ཆེཤ་སྟེ་ ཁྲབ་སྟེལ་འབད་ཚུགས་ནིའི་དོན་ལུ་ མིང་མ་བཀོད་པར་ བཞག་ཡོདཔ་ཨིན། གནོད་སྐྱོན་བྱུང་མི་ལས་སྟེ་འདི་ལུ་ ན་ལས་ཨར་ ‘ལས་སྟེ’ ཟེར་གོ་འོང། ཉམས་ཐུབ་པའི་ངོ་རྟགས་དང་ ASD གི་ ACSC གིས་བྱུང་ཤུན་ལག་འདེབས་ཐབས་ལམ་ཚུ་ སྤུང་སྐྱོབ་ འབད་ནིའི་དོན་ལུ་ དམིགས་བསལ་གྱི་ཁ་གསལ་ལ་ལུ་ཅིག་ བཏོན་བཏང་ཡོདཔ་ཨིན།

བཀོད་ཁྲབ་བསྡུད་དོན།

སྐན་ཞུ་འདི་གིས་ ཀྱི་ལོ་2022 ཀྱི་བླ་ཨ་པ་ལས་ ཀྱི་བླ་ཉ་པའི་བར་ན་ ལས་སྟེ་འདི་གི་ ཡོངས་འཛིལ་ཀྱི་ མཐར་འཐུལ་ཅན་གྱི་ བདེ་སྐྱིག་བཟོ་ཡོད་པའི་སྐོར་ལས་ ASD གི་ ACSC ཞིབ་དཔྱད་ཀྱི་ གྲུབ་འབྲས་ཚུ་ ཁ་གསལ་སྟེ་ བཀོད་ཏེ་ཡོདཔ་ཨིན། ཞིབ་དཔྱད་སྐན་ཞུ་འདི་ ལས་སྟེ་ལུ་ བཙུན་རྟོགས་འབད་མི་ གནོད་པ་ཅན་གྱི་ལུ་ཚུ་ བཙུད་བསྡུ་སྟེ་ བཅོ་ཁ་ཤུབ་ནིའི་ སྒོས་འཚར་ཚུ་ བཟོ་ནིའི་དོན་ལུ་ ཀྱིན་ཡོདཔ་ཨིན་པས། ཞིབ་འཇུག་འདི་གིས་ བདེ་སྐྱིག་འདི་ APT40 གིས་འབད་ཡོདཔ་སྟེ་སྟོན་ནམ་ཨིན།

ཀྱི་བླ་ང་པའི་བར་ཁཨས་ཅིག་ཁར་ ASD གི་ ACSC གིས་ ལས་སྟེ་འདི་ལུ་ སྟེ་ཚན་གྱིས་ ཀྱི་བླ་ང་པའི་མཇུག་ཁར་ལག་ལེན་འཐབ་མི་ བདག་དབང་འོག་ལུ་སྒོང་ཡོདཔ་འདུ་བའི་ ཅ་ཚས་ཅིག་གིས་ དེ་ཚུའི་ཡོངས་འཛིལ་དང་ གནོད་སྐྱེན་སེམས་ཅན་གྱི་འཛིལ་བ་འཐབ་སྟེ་ ཡོདཔ་སྟེ་ བདག་སྒོང་ཡོདཔ་དུ། ལས་སྟེ་འདི་གི་གནང་བ་དང་འཁིལ་ཏེ་ ASD གི་ ACSC གིས་ ལས་སྟེ་གི་ཡོངས་འཛིལ་ནང་ལུ་ གནོད་ཉེན་ཚུ་ཨིན་ཞེས་ ཅ་ཚས་ཅིག་ཁར་ ASD གི་ ACSC བྱང་ཆུབ་ལས་ དཔྱད་པ་ཚུ་ ཐོག་ལས་ཀྱི་ བཀོད་པ་ཤུགས་ཆུབ་ཏུ་ ཡོདཔ་ཨིན། ཞིབ་འཇུག་ལས་ ཀྱི་བླ་ཉ་པའི་ ཟླ་ཚེས་ ཉིན་ཁ་ནས་ ཟླ་ཚེས་ ཉིན་ཁ་ཚུན་ ཀྱི་བླ་ཉ་པའི་ ཟླ་ཚེས་ ཉིན་ཁ་ཚུན་ ཡོདཔ་ཨིན།

ཀྱི་བླ་ཨཔ་ལས་ཀྱི་བླ་ཨཡ་ཚུན་ ASD གི་ ACSC གིས་བསྒྲུབ་འབད་མི་ གནོད་བའོ་ཁོའི་ ཉེད་མཁོན་ཚུ་གི་འགྲུལ་སྐྱོད་ནང་ལུ་ འདི་ཚུ་ཚུད་དེ་ཡོདཔ།:

- དོ་སིཏ་གནས་སྡུད་འདི་གིས་ ཉེད་མཁོན་ལུ་ཡོངས་འཛིལ་ཀྱི་ས་ཁྲ་རང་སོའི་ བཟོ་བསྒྲུབ་འབད་ནིའི་ གོ་སྐབས་ཀྱིན་ནི།
- ཤེབ་ཤེལ་ལག་ལེན་འཐབ་ནི་འདི་གིས་ ཉེད་མཁོན་ལུ་ཡོངས་འཛིལ་ནང་འགོ་ཐོག་གི་གནས་སྐབས་གཅིག་དང་ བཅ་བགོད་ཚུ་ལག་ལེན་འཐབ་ནིའི་ཡོ་བྱད་ གྲུབ་ཀྱིན་ཡོདཔ་ དང་
- ཉེད་མཁོན་གིས་ གནོད་པ་ཅན་གྱི་དོན་ལུ་ ལག་ལེན་འཐབ་མི་ ལག་ཆས་ གཞན་ཚུ་ བཀག་སྟེལ་འབད་ནི།

ཞིབ་དཔྱད་ནང་ ཚོར་ཐུགས་ཅན་གྱི་གནས་སྡུད་མང་ཤོས་ཅིག་ འཛུལ་སྤྱོད་འབད་ཚུགས་པའི་ སྐྱུབ་ཉེད་དང་ ཉེད་མཁོན་ཚུ་ཅིག་ ཡོངས་འཛིལ་བརྒྱུད་ནི་ ཕྱོགས་གཅིག་ལུ་ འགྲོ་བའི་ སྐྱབ་ཉེད་ཚུ་ མཐོང་ཁིའི་ (T1021.002)། བདག་དབང་འོག་ལུ་བཏང་བའི་གནད་དོན་མང་ཤོས་ཅིག་ སྟེ་ཚན་གྱིས་ཡོངས་འཛིལ་ནང་ལུ་འཛུལ་སྤྱོད་ཀྱི་ལམ་ཁ་ཅིག་གི་བཅུགས་འབད་མི་དང་། ཡོངས་འཛིལ་འདི་གཞི་བཀོད་སྟོན་ཡོད་ཀྱི་ཡིན་ལུ་ཅི་ཅིའི་ བཅུགས་འབད་ཚུགས་པའི་ཉེན་སྐྱང་མེད་པའི་ནང་འཁོད་མཉེན་ཆས་སྤྱོད་པ་འདི་ཚུ་ གིས་ཁན་ཐེགས་བྱང་ཆུག། ཕྱིར་ཐོན་གནས་སྡུད་ནང་ལུ་ སྟེ་ཚན་འདི་ནང་བསྟོད་འབད་ཚུགས་པའི་དཔང་ཤུགས་ཅན་གྱི་ངོ་རྟགས་བདེན་བཤད་ཚུ་ཚུདཔ་ཨིན་ལས་མ་ཚད། འགོ་དང་ཁོའི་འཛུལ་ལམ་འདི་བཀག་བཞག་པ་ཅིན་ ཉེད་མཁོན་ཚུ་ཡུ་གནང་བ་མེད་པའི་ འཛུལ་སྤྱོད་ལོག་སྟེ་འབད་ཚུགས་པའི་ ཡོངས་འཛིལ་བརྟེན་ཚུ་ཡང་ ཚུད་ཚུདཔ་ཨིན། འགོ་ཐོག་ལུ་ བཀོད་སྟེ་ཉེད་མི་འཛུལ་ཚས་ཚུ་ལས་ཡུག་སྟེ་ གནོད་སྐྱེན་སེམས་ཅན་གྱི་ཐབས་ལམ་ཚུ་ ཡོངས་འཛིལ་ནང་ལུ་ ཚུད་ཚུདཔ་ཨིན། ཞིབ་དཔྱད་ཀྱི་ གྲུབ་འབྲས་ཚུ་ ཐུགས་ཅན་གྱི་ཁ་གསལ་ཚུ་ ཡོངས་འཛིལ་ནང་ལུ་ ཚུད་ཚུདཔ་ཨིན། ཡོངས་འཛིལ་བརྒྱུད་དེ་ ཕྱོགས་ཅིག་ལུ་ཡོདཔ་ཨིན། (T1021.002)། བདག་དབང་འོག་ལུ་བཏང་བའི་གནད་དོན་མང་ཤོས་ཅིག་ སྟེ་ཚན་གྱིས་ཡོངས་འཛིལ་ནང་ལུ་འཛུལ་སྤྱོད་ཀྱི་ལམ་ཁ་ཅིག་གི་བཅུགས་འབད་མི་དང་། ཡོངས་འཛིལ་འདི་གཞི་བཀོད་སྟོན་ཡོད་ཀྱི་ཡིན་ལུ་ཅི་ཅིའི་ བཅུགས་འབད་ཚུགས་པའི་ཉེན་སྐྱང་མེད་པའི་ནང་འཁོད་མཉེན་ཆས་སྤྱོད་པ་འདི་ཚུ་ གིས་ཁན་ཐེགས་བྱང་ཆུག། ཕྱིར་ཐོན་གནས་སྡུད་ནང་ལུ་ སྟེ་ཚན་འདི་ནང་བསྟོད་འབད་ཚུགས་པའི་དཔང་ཤུགས་ཅན་གྱི་ངོ་རྟགས་བདེན་བཤད་ཚུ་ཚུདཔ་ཨིན། འགོ་དང་ཁོའི་འཛུལ་ལམ་འདི་བཀག་བཞག་པ་ཅིན་ ཉེད་མཁོན་ཚུ་ཡུ་གནང་བ་མེད་པའི་ འཛུལ་སྤྱོད་ལོག་སྟེ་འབད་ཚུགས་པའི་ ཡོངས་འཛིལ་བརྟེན་ཚུ་ཡང་ ཚུད་ཚུདཔ་ཨིན། ཞིབ་འཇུག་ལས་ ཀྱི་བླ་ཉ་པའི་ ཟླ་ཚེས་ ཉིན་ཁ་ནས་ ཟླ་ཚེས་ ཉིན་ཁ་ཚུན་ ཀྱི་བླ་ཉ་པའི་ ཟླ་ཚེས་ ཉིན་ཁ་ཚུན་ ཡོདཔ་ཨིན།

ཞིབ་དཔྱོད་གླུག་འབྲས།

ཁ་གསལ།

སྤྱི་ཟླ་བདུན་པ་ལས་འགོ་བཙུགས་ཏེ། ཉེད་པ་པོ་ཚུ་གིས་སྟོལ་སྒྲིག་སྒེབ་བློག་རིམ་ (T1190) བརྒྱག་དཔྱད་དང་ ལག་ལེན་འཐབ་ཚུགས་ནུག <webapp>2-ext གྱུ་གཡོག་འཐབ་མི། དེ་གིས་སྒེ་ཚན་འདི་ཡུ་ཡོངས་འབྲེལ་དམག་མེད་ས་ཁོངས་ (DMZ) ནང་ཡུ་ཀང་རྐེན་བཙུགས་ཚུགསཔ་བཟོ་སྟེ་འདུག། ཀ་ནི་འདི་ ཡོངས་འབྲེལ་དང་ མཐོང་ཚུགས་པའི་དོ་མེན་གཏིས་ཆ་ར་ རྩིས་ཏུབ་ནི་གི་དོན་ཡུ་ ལག་ལེན་འཐབ་ནུག། བདེ་སྒྲིག་འབད་ཡོད་ཨེས་འཛིན་ཡིག་ཆ་ (T1078.002) འདི་ ཤུགས་ལྡན་སྟོད་ཐོ་ (T1018) འདྲི་དཔྱད་འབད་ནི་དང་། དམག་མེད་ས་ཁོངས་ (DMZ) ནང་གི་འཕྲུལ་ཆས་སྟུ་མང་ལས་ཡིག་སྟོད་བགོ་བཤའ་ཚུ་ (T1039) སྤྱར་བརྩེགས་འབད་ཐོག་ལས་ གནད་སྡུད་ཕྱིར་འཐེན་འབད་ནི་ཡུ་ལག་ལེན་འཐབ་ཡོད་པ་ཞིན།། ཉེད་མཁན་འདི་གིས་ ས་བར་ཅིག་ལས་ ནུས་ཅན་ཡོངས་འབྲེལ་ཀྱི་ཆོག་ཐམ་ཚུ་ཐོབ་ནི་དོན་ཡུ་ ཀར་བེ་རོས་ཉིང་ (Kerberoasting)འཛབ་ཚོལ་འབད་ཡོད་པ་ཞིན། (T1558.003)། སྟེ་ཚན་འདི་གིས་ དམག་མེད་ས་ཁོངས་ (DMZ) དང་ ཡང་ན་ ནང་འགོད་ཡོངས་འབྲེལ་ག་ར་ནང་ཡུ་ ཁ་སྐོང་གནས་ས་ག་ནི་ཡང་ཐོབ་པར་མ་མཐོང་།

མཐོང་སྟངས་གི་དུས་ཡུན།

འོག་གི་དུས་ཚོད་ཐིག་ཁྲམ་འདི་གིས་ ལས་སྟེ་གི་ཡོངས་འབྲེལ་ནང་ཡུ་ བཤུར་རྐྱེགས་ འབད་མི་ གནོད་པ་ཅན་ཀྱི་ཉེད་མཁན་གི་ལས་སྟ་གི་ གནས་རིམ་གཅོ་བོ་ཚུ་གི་ བརྡ་དོན་རྒྱབ་ཀྱི་ཐོག་ལས།

ཁོས་ཏི་ཚིས་ཞིབ།

T1082 མ་ལག་བརྡ་དོན་འཚོལ་ཞིབ།

ཁོས་ཏི་ཚིས་ཞིབ་དང་རྟག་བརྟན་བཙུགས་པ།

ཁྱིམས་མཐུན་ཀྱི་ངོ་རྟགས་ཚུ་ལག་ལེན་འཐབ་སྟེ་ འགོ་དང་པ་ནང་སྒྲོག་འབད་ཡོད།

ཡོངས་འབྲེལ་བརྟག་ཞིབ།

T1021.002 ཐག་རིང་ཞབས་ཏོག SMB/ཁིན་ཏོ་བདག་སྒྲོང་འགོ་ཁཐད་

T1135 འབྲེལ་མཐུད་འགོ་ཁཐད་འཚོལ་ཞིབ་

ཡོངས་འབྲེལ་གཞི་བཞག་གི་སྟོན་འཚོལ་དང་ཉེད་པ་པོའི་ཀུ་བ་ཚུ་ནང་ལུ་ཚུད་ཡོད། SMB འགོ་ཁཐད་ཚུ་སྤྱར་བརྩེགས་འབད་བ། ཡོངས་འབྲེལ་གཞི་བཞག་གི་བཤུ་སྤུད་དང་ཁོངས་ཀར་ཀྱི་ཆོས་ཞིབ

འགོ་དང་པའི་གསར་རྩེད།

ལས་སྟེ་གི་དོན་ལུ་བཙོ་བསྒྲུབ་འབད་ཡོད། སྟོལ་སྒྲིག་རིམ་ཁ་ཤས་ཀྱི་ཐོག་ལས་ ཉེན་ཁའི་ཐོག་ལས་ ཁ་སྐོང་ཚུ་ཐོབ་ཐུབ།

བཤུ་གཞོག།

T1190 མི་མང་ལ་གདོང་ཐུག་ཉེད་པའི་ལག་ལེན་བགོལ་སྟོང།

ཡོངས་འབྲེལ་བགོལ་སྟོང་བགོལ་སྟོང་དང་ཡོངས་འབྲེལ་ཤེལ་ཡོངས་གསར་བཙོ།

གནོད་ཅན་ཀྱི་འབྲེལ་བ།

འགོ་དང་པ་མཚོང་བའི་ལས་སྟེའི་འཕྲུལ་ཆས་དང་ དོས་འཛིན་ཡོད་པའི་ཆུལ་ཁལ་ཀྱིས་ཆུབ་སྟོང་ འབད་མི་གཞི་རྟེན་མཐུན་ཆུན་ཀྱི་བར་ཀྱི་འབྲེལ་བ།

མཐུད་འབྲེལ་བསྒྲུར་འཛུགས།

T1090 དོ་ཚན

ཉེད་མཁན་ཀྱིས་ ssf ལག་ཆས་ཀྱི་མཐུད་ལམ་ཡོག་སྟེ་ གཞི་བཙུགས་འབད་ཡོད་པ་ཞིན (སྤྱི་ཟླ་༡༢ ཀྱི་བྱ་བ་དང་མཚུངས་པར་ཚོས་གཞན་ཚུ་ནང་ལུ་ཡང་)

དུས་ཡུན་ཁ་གསལ།

ཐབས་བདུན་པ།: བྱེད་མཁན་ཚོ་གིས་ ལས་སྡེ་གི་དོན་ལུ་བཟོ་ཡོད་པའི་ སྤྲོད་སྒྲིག་ཞབ་སྒྲོག་རིམ་ (T1190) གི་གནོད་ཕོག་ལུ་ འགོ་ཐོག་མཐུད་ལམ་གཞི་བཙུགས་འབད་ཡོདཔ་ཨིན། (ད་སྔོ་ལས་འགོ་བཟུང་ 'ཞབ་སྒྲོག་རིམ'' ཡང་ན་ 'webapp' ཟེར་མིང་བཏགས་ཡོད) སྐྱེལ་འདྲེན་བང་རིམ་ཉེན་སྲུང་ (TLS) མཐུད་ལམ་བརྒྱུད་དེ་ (T1102)། གཞན་ཡང་ གལ་གནད་ཅན་གྱི་ལས་རིམ་ཅིག་ ག་ནི་ཡང་\མཐོང་།

ཐབས་བདུན་པ།: བྱེད་མཁན་ཚོ་གིས་ ཞབ་སྒྲོག་རིམ་གྱི་ཞབ་སཪྦ་འདི་ལུ[2] མཐའ་སྣེ་ འཚོལ་ཞིབ་འབད་དེ་ དེ་ལས་ཞིབ་དཔྱད་འབད་ནིའི་དོན་ལུ་རྩིས་ཞིབ་འགོ་བཙུགསཔ་ཨིན།

ཐབས་བདུན་པ།: བྱེད་མཁན་ཚོ་གིས་ དམིགས་བསལ་གྱི་མཐའ་མཇུག་ཅིག་ ལག་ལེན་འཐབ་ནི་གི་དཔའ་བཅམ་མི་ལུ་ གཙོ་བོར་བསྟེནམ་ཨིན།

ཐབས་བདུན་པ།: བྱེད་མཁན་ཚོ་གིས་ ཤོག་ལེབ་གཞན་ཅིག་གུ་བཙུགས་ཡོད་པའི་ཞབ་ཤེལ་བརྒྱུད་དེ་ ཞབ་སར་བར་ལུ་ མཐར་འཁྱོལ་ཅན་སྦེ་ POST འབད་ཚུགས། བྱེད་མཁན་གཅིག་མཚུངས་ཚུ་གིས་ ལྷ་གཡོག་བྱིན་མི་ IP གཉིས་པ་འདི་གིས་ཡང་ URL གཅིག་ལུ་ བཀྲམ་སྤེལ་འབད་ནི་འགོ་བཙུགསཔ་ཨིན། བྱེད་མཁན་ཚོ་གིས་ ཡོངས་འབྲེལ་གྱི་ཤེལ་ཡོརཔ་ལེ་ཤ་ཅིག་བཟོ་སྟེ་ བརྟག་དཔྱད་འབད་ནུག།

བཀོལ་སྤྱོད་ཀྱི་ཐབས་ལམ་ངོ་མ་འདི་མ་ཤེས་རུང་། དམིགས་བསལ་མཐའ་སྣེ་འདི་ <webapp>2-ext གུ་ཡིག་སྣོད་ཚུ་གསར་བསྐྲུན་འབད་ནིའི་དོན་ལུ་དམིགས་གཏད་བསྐྱེད་ཡོདཔ་ཨིནམ་གསལ་ཏོག་ཏོ་ཨིན།

ASD གི་ ACSC གིས་ IP ཁ་བྱང་མཐུད་ལམ་གཉིས་འདི་ བར་འཇུལ་གྱི་ཆ་ཤས་ཅིག་ཨིནམ་སྦེ་ ཡིད་ཆེས་བསྐྱེདཔ་ཨིནམ་ད་ དེ་ཡང་ ཁོང་གི་སྤྱོ་བ་བརྗེ་སོར་དང་ འགོ་ཐོག་མཐུད་ལམ་ཚུ་ སྐར་མ་དག་པ་ཅིག་གི་བར་ན་ འབྱུང་མི་ལུ་བརྟེན་ཏེ་ཨིན་མས།

ཐབས་བདུན་པ།: སྡེ་ཚན་འདི་གིས་ མགོ་སྤྱོད་ཆས་རྩིས་ཞིབ་དང་། ཐོབ་དབང་ཡར་སེང་གི་གོ་སྐབས་འཚོལ་ནི། དེ་ལས་ ཞབ་ཤེལ་སོ་སོ་ཅིག་བཀྲམ་སྤེལ་འབད་ནི་ཚུ་ འཕྲོ་མཐུད་དེ་རང་འབད་དོ་ཡོདཔ་ཨིན། བྱེད་མཁན་ཚུ་གིས་ ༧ གི་དོན་ལུ་ བདེ་སྲིག་བཟོ་ཡོད་པའི་ངོ་རྟགས་ཚུ་ལག་ལེན་འཐབ་སྟེ་ ཞབ་སྒྲོག་རིམ་ནང་ ནང་བསྐྱོད་འབདཔ་ཨིན། <firstname.surname>@<organisation domain>

བྱེད་མཁན་ཚུ་གི་ལས་རིམ་འདི་ མཐར་འཁྱོལ་ཅན་ཅིག་སྦེ་ ཐོབ་དབང་ཡར་སེང་འབད་མ་ཚུགསཔ་བཟུམ་ཅིག་འདུག། <webapp>2-ext། དེ་གི་ཚབ་ལུ་ བྱེད་མཁན་ཚུ་གིས་ ཡོངས་འབྲེལ་གཞི་བཞག་པའི་ལས་སྣ་ཚུ་ལུ་ གཙོ་བོར་བསྟེནམ་ཨིན།

ཐབས་བདུན་པ།: བྱེད་མཁན་འདི་གིས་ ཞབས་ཏོག་རྩིས་ཐོ་ གི་དོན་ལུ་ བདེ་སྲིག་བཟོ[3] ཡོད་པའི་ངོ་རྟགས་ཚུ་བརྟག་དཔྱད་འབདཔ་ཨིན།

ཐབས་བདུན་པ།: བྱེད་མཁན་ཚུ་གིས་ གནོདཔ་ཅན་གྱི་གཞི་རྟེན་ཚུ་ལུ་ མཐུད་ནིའི་དོན་ལུ་ ལག་ལེན་འཐབ་མི་ ཁ་ཕྱེ་ཡོད་པའི་ཐོན་ཁུངས་ལག་ཆས་ ཉེན་སྲུང་སོ་ཀེཊ་ཕྲན་ལིང་འདི་ བཀྲམ་སྤེལ་འབདཔ་ཨིན། འ་ནི་མཐུད་ལམ་འདི་ བྱེད་པ་པོའི་གནོདཔ་བཀལ་མི་འཕྲུལ་ཆས་ཚུ་ལས་ ལས་སྡེའི་ནང་འཁོད་ཡོངས་འབྲེལ་ནང་ལུ་ འགྲུལ་སྐྱོད་འདྲུད་སྒུགས་འབད་ནིའི་དོན་ལུ་ལག་ལེན་འཐབ་ཨིན། འདི་ཚུ་གིས་ཞབས་ཏོག་རྩིས་ཁ་གི་ངོས་འཛིན་ཡིག་ཆ་ལག་ལེན་འཐབ་ནི་ལུ་འབད་རྩོལ་བསྐྱེད་པའི་སྐབས་ལུ་ འདི་ཚུ་གི་འཕྲུལ་ཆས་མིང་ཚུ་བྱུང་རིམ་ཐོ་ཡིག་ནང་ལུ་ཕྱིར་འཐོན་འགྱོ་ནུག

ཐབས་བརྒྱད་པ།: བྱེད་མཁན་ཚུ་གིས་ ཞབས་ཏོག་རྩིས་ཁྲ་དང་འབྲེལ་བའི་ མཐུད་ལམ་གཞི་བཙུགས་འབད་མ་ཚུགས་མི་ཚུ་རྩིས་ཏེ་ ལས་རིམ་ཚད་འཛིན་འབད་དེ་ འགོ་འདྲེན་འཐབ་སར་མཐོངམ་ཨིན།

ཐབས་བརྒྱད་པ།: བྱེད་མཁན་ཚུ་གིས་ གལ་གནད་ཅན་གྱི་ཡོངས་འབྲེལ་དང་ ཤུགས་ལྡན་སྡོད་པོ་གྲངས་རྩིས་ཚུ་འབདཔ་ཨིན། བདེ་སྲིག་འབད་ཡོད་པའི་རྩིས་ཁ་སོ་སོ་ཅིག་ ཤུལ་ལས་ དམག་མེད་ས་ཁོངས་ (DMZ) ནང་འཁོད་ཀྱི་ Windows འཕྲུལ་ཆས་ཚུ་ནང་ བགོ་བཤའ་སྦྲུར་བརྩེགས[4] འབད་ནི་ལུ་ ལག་ལེན་འཐབ་ཡོདཔ་ལས་ གནད་སྡུད་མཐར་འཁྱོལ་ཅན་སྦེ་ ཕྱིར་འཐེན་འབད་ཚུགསཔ་བཟོཔ་ཨིན།

འདི་ཡང་ དམག་མེད་ས་ཁོངས་ (DMZ) ནང་ལུ་ སྦྲུར་བརྩེགས་འབད་བཏུབ་པའི་འཕྲུལ་ཆས་ཚུ་གུ་ ཀུ་ཤོར་བའི་ངོས་འཛིན་ཡིག་ཆ་ གོ་སྐབས་ལྡན་པའི་ཐོག་ལས་ ལག་ལེན་འཐབ་མི་བཟུམ་ཅིག་ཨིན་མས། ཕ་ཡར་ཕྱལ་ཚུ་གིས་ བྱེད་མཁན་འདི་ ལས་རིམ་ཅིག་འཐབ་པ་དང་གཅིག་ཁར་ ནང་འཁོད་ཡོངས་འབྲེལ་ལུ་དམིགས་གཏད་བསྐྱེད་ནི་ལས་ བཀག་ཆ་འབད་ཡོདཔ་ཨིན།

སྤྱི་ཚེ་བརྒྱད་པ་ལས་ དགུ་པ་: SSF ལག་ཆས་འདི་གིས་ གནོདཔ་ཅན་གྱི་IP ཅིག་ལུ་ མཐུད་ལམ་ལོག་སྟེ་གཞི་བཙུགས་འབད་ནུག། སྡེ་ཚན་འདི་གིས་ ཁོང་ཚུ་གི་འཇུལ་ཞུགས་བཀག་ཆ་མ་འབད་ཚུན་ཚོད་ ལས་རིམ་ཁ་སྐོང་ག་ནི་ཡང་ འབད་མི་མཐོང་།

ཐབས་དགུ་པ།: ལས་སྡེ་གིས་ གནོདཔ་ཅན་གྱི་IP འདི་ ཁོང་རའི་ཕ་ཡར་ཕྱོལ་ཚུ་ནང་ ཐོ་བཀོད་བཀག་ཆ་འབད་དེ་ བཀག་བཞགཔ་ཨིན།

2 སབྐྲུས་དགོ་འདའི་ཞིང་ལ་ ༼མཐའ་སནྣེར་མ་འིད་ ཕྲབ་གསྒྲ་རམི་གཡྲིས་འབག་གཅགི་ཨནི།
3 ཞབས་ཏགོ་རྩསི་ཁ་ཚ་ ༼ལགཨ་ལནེ་པ་ར་རེ་དིང་མཐདུ་ད་མེདཔ་ལས་ ཞབས་ཏགོ་ཚ་དུང་མཐདུ་ད་ཡདོཔ་ཨནི། མའ་ཀརོ་སོཕཊ་ཡིས་འཛནི་གཏྲི་སྦྲོན་ནང་ རྩསི་ཐ་སོ་རྐྒོས་ཡདོཔ་ཨནི།
4 བག་པོཤའ་ཚ་སྦྲུ་བརསྩེིས་འབད་ན་འདིད་ ཡགི་སནྡེ་རམི་ལགྱུས་གཞ་བགིད་ནང་ག་ཡགི་སནྡེ་ཚ་ ༼ལགཨ་ལནེ་པ་ཡང་ན་ ལགཨ་ལནེ་པ་སྒྲོན་ལ་ ༽འཛལུ་ཞགུས་འབད་ཚུགས་པ་བཟ་ོའདི་ཐ་ོརམི་ཅགི་ཨནི།

བྱེད་མཁན་པའི་གནས་སྐབས་དང་ཐབས་ཤེས།

MITRE ATT&CK གཞི་བཀོད་འདི་ ཡོངས་འཛིལ་ནང་ ཉེན་ཁ་ཅན་གྱི་བྱེད་མཁན་ཚུ་གིས་ ལག་ལེན་འཐབ་མི་ གནས་སྐབས་དང་ ཐབས་ཤེས་ཚུ་ ཡིག་ཐོག་ལུ་བཀོད་དེ་ བསྒྲུམ་བྱིག་འབད་མི་ ཅིག་ཁྱེན། གཞི་བཀོད་འདི་ ཡུ་ཨེས་ཀྱི་ཁེ་ སང་ཨེད་པའི་ MITRE ལས་འཛིན་གྱིས་ བཟོ་ཡོདཔ་ད་ འདི་གིས་ཉེན་ཁ་ཅན་བྱེད་པ་པོའི་སྤྱོད་ལམ་གྱི་སྐོར་ལས་ འཛམ་གླིང་ཡོངས་ཀྱི་དཔྱད་གཅིག་སྐད་ཡིག་གི་ཐོག་ལུ་ལུ་འབདཔ་ཨིན།

ASD གི་ ACSC གིས་ བྱེད་མཁན་གྱི་ གཞོདཔ་ཅན་གྱི་ལས་སྣ་ཚུ་དང་ འབྲེལ་བ་ཡོད་པའི་ གཞན་གསལ་གྱི་གནས་སྐབས་དང་ ཐབས་ཤེས་ཚུ་ དབྱེ་ཞིབ་འབདཔ་ཨིན།

འཚོལ་ཞིབ།

T1594 – ཉམས་རྒུད་པའི་བདག་དབང་ཡོད་པའི་ཡོངས་འབྲེལ་འཚར་སྒོ་འཚོལ།

བྱེད་མཁན་གིས་ ཡོངས་འབྲེལ་ནང་འཛུལ་སྤྱོད་འབད་ནི་ གི་གོ་སྐབས་ངོས་འཛིན་འབད་ནི་དོན་ལུ་ སྔོལ་སྒྲིག་ཁེབ་ལག་ལེན་ གྱི་ཡོངས་འབྲེལ་འཚར་སྒོ་འདི་ རྩིས་རྒྱབ་ཡོདཔ་ཨིན།

འགོ་ཐོག་འཛུལ་སྤྱོད།

T1190 – མི་མང་ལུ་གདོང་ཐུག་འབད་མི་ ལག་ལེན་བཀོལ་སྤྱོད་འབད་ནི་ (སྔོལ་སྒྲིག་ཁེབ་ལག་ལེན་བཀོལ་སྤྱོད་འབད་ནི་དང་འབྲེལ་བའི་)

T1078.002 – ནུས་ལྡན་རྩིས་ཁྲི་ དེ་མེན་རྩིས་ཐོ་ཚུ་ (བསྟེམས་རྩིས་ཡིག་ཚ་ཚུ་དང་ གཅིག་ཁར་ ཁང་བསྒྲིད་འབད་ནི་དང་འབྲེལ་བའི་)

ཡོངས་འབྲེལ་ཐོག་ལས་ གསལ་སྟོན་འབད་མི་ སྔོལ་སྒྲིག་ཁེབ་ལག་ལེན་ཚུ་ ལག་ལེན་འཐབ་མི་འདི་གིས་ བྱེད་མཁན་འདི་ལུ་ འགོ་ཐོག་འཛུལ་སྤྱོད་ཀྱི་ས་སྒོ་ཅིག་ཏིན་ཡོངས་ཤེན། བྱེད་མཁན་འདི་གིས་ ཤུལ་ལས་ ཁོང་གིས་ ཡོངས་འབྲེལ་ཁང་ལུ་ འཛུལ་སྤྱོད་འབད་ནི་གི་དོན་ལུ་ བདེ་སྒྲིག་བཟོ་ཡོད་པའི་ ངོས་ལེན་ཡིག་ཆ་ཚུ་ ལག་ལེན་འཐབ་ཚུགས་ཀྱག།

ལག་ལེན།

T1059 – བཏ་བཀོད་དང་ཡིག་གཟུགས་སྐད་སྒྲུར་པ་ (ཤེའུ་ཤེལ་བརྒྱུད་དེ་བཏ་བཀོད་ ལག་ལེན་འཐབ་ནིའི་སྐོར་ལས་)

T1072 – མཉེན་ཆས་བཀག་སྡེལ་གྱི་ལག་ཆས་ (IP ལུ་མཐུད་ནིའི་དོན་ལུ་ ཁ་ཕྱེ་ཡོད་པའི་ཐོན་ཁྲངས་ལག་ཆས་ Secure Socket Funneling (SSF) ལག་ལེན་འཐབ་མི་ བྱེད་མཁན་ལུ་བཙུགས།)

ཚུ་ཚུགས།

T1505.003 – ཁར་བར་མཉེན་ཆས་ཆ་ཤས།: ཤེའུ་ཤེལ་ (འཛུལ་སྤྱོད་གཞི་བཙུགས་ འབད་ནིའི་དོན་ལུ་ ཤེའུ་ཤེལ་དང་ཚེའི་ཚེའི་ལག་ལེན་འཐབ་ནིའི་སྐོར་ལས་)

དོ་རྟགས་འཛུལ་སྤྱོད།

T1552.001 – གསང་ཡིག་མཇོད་ཁང་ཚུ་ལས་ དོས་ལེན་ཡིག་ཆ་ (སྤྱིང་ཁྱིམ་འཛིན་སྐྱོང་རིམ་ལུགས་ (BMS) དང་འབྲེལ་བའི་ཚོགས་ཡིག་ཡིག་སྤྱོད་ཚུ་གི་སྐོར་ལས་)

T1558.003 – ཀར་ལེ་རོསི་གི་ཨོག་བྱང་ཚར་ཁ་བཀྲ་ནི་ཡང་ན་རྩུབ་བཟོ་ནི། Kerberoasting (ཡོངས་འབྲེལ་གྱི་ཚོགས་ཐབས་ཐོབ་ནིའི་དོན་ལུ་ གཞོད་དཔའ་བཀལ་ནིའི་ སྐོར་ལས་)

ཕྱོགས་གཅིག་གི་འགུལ་སྤྱོད།

T1021.002 – ཐག་རིང་ཞབས་ཏེའུ། SMB བགོ་བཤའ་ཚུ་ (ཐབས་འཕྲུལ་སྤྱ་ཚོགས་ ལས་ SMB བགོ་བཤའ་ཚུ་ བྱེད་མཁན་གིས་ བཙུགས་མི་དང་འབྲེལ་བའི་)

བསྡུ་ལེན།

T1213 – བཏ་དོན་མཇོད་ཁང་ལས་ གནད་སྡུད་ (BMS ས་བར་ནང་མཐོང་མི་ ལག་དེབ་/ཡིག་ཚ་ཚུ་གི་སྐོར་ལས་)

ཕྱི་བཤལ་གཏང་ནི།

T1041 – C2 རྒྱུན་ལམ་ཐོག་ལས་ ཕྱིར་འཐེན་འབད་ནི། (བྱེད་མཁན་གྱི་གནས་སྡུད་ཚུ་ Active Directory དང་ བགོ་བཤའ་ཚུ་ བཙུགས་ནི་ལས་ ཕྱིར་འཐེན་འབད་ནི་དང་ འབྲེལ་བ་ཡོདཔ་ཨིན།)

གནད་དོན་ཞིབ་འཇུག་ 2

སྙན་ཞུ་འདི་ ཁྲབ་ཆེཕ་སྒྲེ་ ཁྲབ་སྒྲེལ་འབབ་ཚུགས་ནིའི་དོན་ལུ་ མིང་མ་བཀོད་པར་ བཞག་ཡོདཔ་ཨིན། གནོད་སྐྱོན་བྱུང་མི་ལས་སྡེ་འདི་ལུ་ ན་ལས་ཕར་ ‘ལས་སྡེ་’ ཟེར་གོ་འོང་། ཉམས་རྒྱུད་པའི་ངོ་རྟགས་དང་ ASD གི་ ACSC གིས་བྱུང་རྐྱེན་ལན་འདེབས་ཐབས་ལམ་ཚུ་ སྒྲུང་སྐྱོབ་འབད་ནིའི་དོན་ལུ་ དམིགས་བསལ་གྱི་ཁ་གསལ་ལ་ལུ་ཅིག་ བརྗོད་བཏང་ཡོདཔ་ཨིན།

བཀོད་ཁྲབ་བཅུད་དོན།

འ་ནི་སྙན་ཞུ་འདི་གིས་ སྤྱི་ལོ་༢༠༢༢སྤྱི་ཟླ་༦པའི་ནང་ ལས་སྡེ་གི་ཡོངས་འབྲེལ་ནང་ལུ་མཐར་འཁྱོལ་ཅན་གྱི་བདེ་སྲུག་བཟོ་ཡོད་པའི་སྐོར་ལས་ ASD གི་ ACSC ཞིབ་དཔྱད་ཀྱི་གྲུབ་འབྲས་ཚུ་ ཁ་གསལ་སྦེ་བཀོད་དེ་ཡོདཔ་ཨིན། ཞིབ་དཔྱད་སྙན་ཞུ་འདི་ ལས་སྡེ་ལུ་ མཐོང་མི་གནོད་སྐྱོན་ལྟ་ཚུ་ བསྡུས་དོན་བཟོ་ནི་དང་ བཙོས་སྲུག་གི་གྲོས་འཆར་ཚུ་གཞི་བཞག་འབད་ནིའི་དོན་ལུ་ བྱིན་ཡོདཔ་ཨིན། ཞིབ་འཇུག་འདི་གིས་ བདེ་སྲུག་འདི་ APT40 གིས་འབད་ཡོདཔ་སྦེ་སྟོནམ་ཨིན།

སྤྱི་ལོ་༢༠༢༢ སྤྱི་ཟླ་༥ པའི་ནང་ ASD གི་ ACSC གིས་ སྤྱི་ལོ་༢༠༢༢ སྤྱི་ཟླ་༦ པ་ལས་ ལས་སྡེ་གི་ཡོངས་འབྲེལ་ལུ་ གནོད་པ་ཡོད་པའི་ དོགས་པ་ཡོད་པའི་ ལས་སྡེ་ཅིག་ལུ་བརྡ་དོན་སྤྲོད་ཡོདཔ་ཨིན། དེ་གི་ཞུལ་ལས་ ལས་སྡེ་གིས་ ASD གི་ ACSC ལུ་ ཁོང་གི་ལས་སྡེའི་ལས་འཛིན་ཐག་རིང་འཇུལ་སྤྱོད་ཐབས་ལམ་གྱི་ ནང་བསྐྱོད་སྒོ་ཁྱང་ བྱིན་མི་ཡོངས་འབྲེལ་དྲ་རྒྱར་གདོང་ཐུག་འབད་མི་ སར་བར་ནང་ལུ་ གནོད་སྐྱོན་ཅན་གྱི་མཉེན་ཆས་ རྙེད་ཡོདཔ་སྦེ་ བརྡ་སྤྲོད་ཡོདཔ་ཨིན། སར་བར་འདི་གིས་ ཐག་རིང་འཇུལ་སྤྱོད་ནང་བསྐྱོད་དང་ངོ་རྟགས་འཛིན་སྐྱོང་གི་ཐོན་སྐྱེད་ལག་ལེན་འཐབ་ཡོདཔ་ལས་ སྙན་ཞུ་འདི་ནང་ ‘བདེ་སྲུག་བཟོ་ཡོད་པའི་འཕྲུལ་ཆས་’ ཟེར་སླབ་འོང་། སྙན་ཞུ་འདི་ནང་ ASD གི་ ACSC གིས་འཐབ་མི་ཞིབ་དཔྱད་ཀྱི་ལན་དུ་ འཚོགས་སྡེ་གི་དོན་ལུ་བཟོ་མི་ ཞིབ་དཔྱད་གྲུབ་འབྲས་དང་ བཙོས་སྲུག་གི་བློ་སྟོན་ཚུ་ ཞིབ་ཕྲ་སྦེ་ བཀོད་དེ་ཡོདཔ་ཨིན།

སྤྱི་ལོ་༢༠༢༢ སྤྱི་ཟླ་༦ པ་ལས་ ལས་སྡེ་གི་ཡོངས་འབྲེལ་ཆ་ཤེས་ཅིག་ ཡོངས་འབྲེལ་གྱི་ བྱེད་མཁན་ཚུ་གིས་ ཐག་རིང་ལས་ འཇུལ་སྤྱོད་འབད་ཚུགས་པའི་ ནང་བསྐྱོད་ཀྱི་ཡོངས་འབྲེལ་བརྒྱུད་དེ་ གནོད་སྐྱོན་རྐྱབ་ཡོདཔ་སྦེ་ སྒྲུབ་བྱེད་བཀོད་ནུག། སར་བར་འདི་བྱེད་པོ་ལེ་ཤ་ཅིག་གིས་ བདེ་སྲུག་འཕྲོག་ཡོདཔ་སྲིད་པ་དང་། བདེ་སྲུག་འཕྲོག་པའི་དུས་ཚོད་དེ་སྐབས་སུ་ ཁྲབ་ཆེ་བའི་སྒོ་ལས་ཁྲབ་བསྒྲུགས་འབད་མི་ ཐག་རིང་ལས་གསང་ཡིག་ལག་ལེན་འཐབ་ནི་ (RCE) གི་ཉེན་ཁ་དེ་གིས་ གནོད་སྐྱོན་རྐྱབ་ཡོདཔ་བཟུམ་ཅིག་རེད།

ASD's ACSC གིས་བལྟ་རྟོགས་འབད་མི་ བྱེད་མཁན་གཙོ་བོ་གི་ལས་སྣ་ཚུ་ཡང་ འདི་ནང་ལུ་ཚུདཔ་ཨིན།:

- ཧོསིཊ་གནས་སྡུད་འདི་གིས་ བྱེད་མཁན་ལུ་ཡོངས་འབྲེལ་གྱི་ས་ཁྲ་རང་སོའི་བཟོ་བསྐྲུན་འབད་ནིའི་གོ་སྐབས་བྱིན་ནི།
- ཡོངས་འབྲེལ་གྱི་ལག་ལེན་དང་ ཞབ་ཞྭལ་ལག་ལེན་འཐབ་མི་ཚུ་ ལག་ལེན་འཐབ་ཐོག་ལས་ བྱེད་མཁན་ལུ་ ཡོངས་འབྲེལ་ནང་ འགོ་ཐོག་གཞི་བཙུགས་དང་ བརྟ་བཀོད་ཚུ་ ལག་ལེན་འཐབ་ཚུགས་པའི་ ལྷོགས་གྲུབ་བྱིནམ་ཨིན།
- ཐོབ་དབང་ཡར་སེང་འབད་ནིའི་དོན་ལུ་ མཉེན་ཆས་ཀྱི་ཉེན་ཁ་ཚུ་ ལག་ལེན་འཐབ་ནི། དང་
- ཕྱོགས་གཅིག་ལུ་འགྱོ་ཚུགསཔ་བཟོ་ནི་ལུ་ ངོ་རྟགས་བསྡུ་ལེན།

ASD གི་ ACSC གིས་ སྤྱི་ལོ་༢༠༢༢ སྤྱི་ཟླ་༦ པའི་ནང་ གནོད་སྐྱོན་ཅན་གྱི་བྱེད་པོ་ཅིག་གིས་ བདེ་སྲུག་འཕྲོག་པའི་ཡོ་ཆས་ནང་ལས་ ལག་ལེན་པའི་མིང་དང་ཚིག་ཡིག་ ཐ་དད་པ་བརྒྱ་ལས་བཅད་པ་དང་། ཆ་རྐྱེན་མང་པོའི་བདེན་བཤད་གསང་ཨང་དང་ ཐག་རིང་འཇུལ་སྤྱོད་ལྷ་ཡུན་དང་འབྲེལ་བའི་ འཕྲུལ་རིག་གི་རྟགས་རིས་ཚུ་ ཕྱིར་འཐེན་འབད་ཡོདཔ་ ཧྲེད་སོང་ནུག ལས་སྡེ་གིས་ བསྐྱར་ཞིབ་འབད་བའི་སྐབས་ ཚིག་ཡིག་ཚུ་ ཁྲིམས་མཐུན་སྦེ་ མཐོང་ཡོདཔ་ཨིན་པས། ASD གི་ ACSC གིས་ བྱེད་མཁན་འདིས་འཕྲུལ་རིག་གི་རྟགས་རིས་འདི་ཚུ་ ཁྲིམས་མཐུན་ལག་ལེན་པ་ཅིག་འདྲ་སྦེ་ ཐག་རིང་ནང་བསྐྱོད་ལྷ་ཡུན་ བཀྲ་འཕྲོག་འབད་ནི་ཡང་ན་གསར་བཟོ་འབད་ནི་དང་། ཁྲིམས་མཐུན་ལག་ལེན་པའི་རྩིས་ཐོ་ལག་ལེན་འཐབ་སྟེ་ ལས་སྡེའི་ནང་འཁོར་གྱི་ལས་འཛིན་ཡོངས་འབྲེལ་ལུ་ འཇུལ་སྤྱོད་འབད་ནིའི་དོན་ལུ་ བསྡུ་སྒྲིག་འབད་ཡོདཔ་སྲིད་པའི་ལྟ་རྟོག་འབདཔ་ཨིན།

ཞིབ་དཔྱོད་གྲུབ་འབྲས།

ཞིབ་དཔྱོད་བསྡུད་དོན།

ASDགི་ ACSCགིས་ བྱེད་མཁན་འདི་གིས་ ལས་སྒོ་གི་ལས་བྱེདཔ་ཚུ་ལུ་ ཐག་རིང་ས་ལས་ ནང་བསྐྱོད་འབད་ནི་གི་དུས་ཚོད་བྱིན་མི་ ཅ་ཆས་ཚུ་ བདེ་སྲུང་བཟོ་ཡོདཔ་སྦེ་ཐག་བཅད་དེ་ བདེ་སྲུང་འདི་ ལས་རིམ་གཞན་ཚུ་ འགོ་འདྲེན་འཐབ་ནི་གི་དོན་ལུ་ ལག་ལེན་འཐབ་ནུག ཡོ་ཆས་འདི་ཚུ་ནང་ བདེ་སྲུང་འཕྲོག་པའི་སྒྲུབ་བྱེད་སྔ་ཤོས་ མཐོང་བའི་ལྡེད་ཚད་འདྲ་མཉམ་གྱི་གཙོ་འཛིན་གསུམ་ཡོདཔ་ཨིན། ལས་སྒོ་འདི་གིས་ འགོ་ཐོག་བདེ་སྲུང་བཟོ་བའི་ཤུལ་ལས་ མགྱོགས་པ་རང་ ལྡེད་ཚད་འདྲ་མཉམ་གྱི་ གཙོ་འཛིན་གསུམ་གྱི་གྲལ་ལས་ གཉིས་ སྒོ་བསྡམས་ཡོདཔ་ཨིན། དེ་ལས་བརྟེན་ཏེ་ ཤུལ་མའི་ལས་སྣ་ཚ་མཉམ་ ཧོསིཊི་གཅིག་གུ་བྱུང་ཡོདཔ་ཨིན། གཞན་ཡང་ བདེ་སྲུང་བཟོ་ཡོད་པའི་འཕྲུལ་ཆས་དང་འབྲེལ་བའི་ སར་བར་ཚུ་ཡང་ དེ་བཟུམ་སྦེ་ མངོན་གསལ་འབད་ཡོདཔ་ཨིན་པས། ལྷག་ཚུགསཔ་སྦེ་བཟོ་ནི་གི་དོན་ལས་ བདེ་སྲུང་བཟོ་ཡོད་པའི་ཅ་ཆས་ཚུ་ག་ར་ སྣན་ཞུ་འདི་ནང་ལུ་ ཅ་ཆས་གཅིག་སྦེ་བཀོད་དེ་ཡོདཔ་ཨིན།

བྱེད་མཁན་འདི་གིས་ སྤྱི་ལོ་༢༠༢༢ སྤྱི་ཟླ་༩ པ་ལས་ མི་མང་ལུ་ཤེས་རྟོགས་ཡོད་པའི་ ཉེན་ཁ་ཅན་ཚུ་ ལག་ལེན་འཐབ་སྟེ་ བདེ་སྲུང་བཟོ་ཡོད་པའི་ འཕྲུལ་ཆས་ཚུ་ལུ་ ཕྱེབ་ཞིལ་ཚུ་ བཀྲམ་སྤེལ་འབད་ཡོདཔ་སྦེ་ ཡིད་ཆེས་བསྐྱེདཔ་ཨིན་མས། སྡེ་ཚན་འདི་ནང་ལས་ ཉེན་ཁ་ཅན་གྱི་བྱེད་མཁན་ཚུ་གིས་ འཕྲུལ་ཆས་འདི་གི་ཐོག་ལུ་ ཐོབ་དབང་ཡར་སེང་འགྱོ་སྟེ་ཡོདཔ་སྦེ་ དཔྱེ་ཞིབ་འབད་ཡོདཔ་ཨིན། དྲན་ཐོ་བཀོད་ནིའི་ མཐུན་རྐྱེན་མེད་མི་ལུ་བརྟེན་ ཨེ་ཨེསི་ཊི་གི་ ཨེ་སི་ཨེསི་སི་གིས་ ལས་རིམ་གྱི་ ཁྲབ་ཚད་ཆ་ཚང་ གཏན་འབེབས་བཟོ་མ་ཚུགས། དེ་འབདཝ་ད་ ཐབས་འཕྲུལ་འདི་གུ་ཡོད་པའི་སྒྲུབ་བྱེད་ཚུ་གིས་ བྱེད་མཁན་ཅིག་གིས་ གཞམ་གསལ་གྱི་གྲུབ་འབྲས་ཚུ་ ཐོབ་ཡོདཔ་སྦེ་སྟོནམ་ཨིན།

- ལག་ལེན་པའི་མིང་དང་ཚིག་ཡིག་ཆ་གཅིག་ངོ་མ་བརྒྱ་ལས་བཅད་དེ་བསྡུ་སྒྲིག་འབད་ནི། དང་
- འཕྲུལ་རིག་ཅ་ཆས་བསྡུ་གསོག་འབད་མི་འདི་གིས་ གནོདཔ་ཅན་གྱི་བྱེད་མཁན་ཅིག་ལུ་ ཁྲིམས་མཐུན་ལག་ལེན་པ་ཅིག་སྦེ་ བརྫ་དོན་ཊེཀ་སི་ཊོཔ་གཞི་རྟེན་ (VDI) ལཱ་ཡུན་ནང་ འཛུལ་སྤྱོད་འབད་བཅུག་སྟེ་ཡོདཔ་ཨིན།

ASD གི་ ACSC གིས་ བྱེད་པོ་འདིས་ འཚོགས་སྡེའི་དྲ་རྒྱའི་བདེ་སྲུང་འཕྲོག་ནི་ དེ་ལས་རྒྱ་ཆེ་རུ་གཏང་ནིའི་འབད་རྩོལ་འབད་འོང་ཟེར་ ལྷ་རྟོག་འབདཝ་ཨིན། བྱེད་མཁན་གིས་ བརྟོན་བཏང་མི་ ཅ་རྙིང་ཚུ་གིས་ ཁོང་ལུ་ བདག་སྐྱོང་པ་ཚུ་རྩིས་ཏེ་ ཁོང་རའི་གདམ་ཁ་གི་ལག་ལེན་པ་ཅིག་སྦེ་ ཁྲིམས་མཐུན་གྱི་ལག་ལེན་པ་ཅིག་སྦེ་ བཀྲུ་འཕྲོག་འབད་ནི་དང་ ཡང་ན་ བརྫ་དོན་གྱི་ཊེཀ་སི་ཊོཔ་ལཱ་ཡུན་ཚུ་ འགོ་བཙུགས་བཅུག་སྟེ་ཡོདཔ་ཨིན། བྱེད་མཁན་འདི་གིས་ འ་ནི་ཐབས་ལམ་འདི་ ལས་སྒོ་གི་ཞབས་ཏོག་ཚུ་ བརྟན་ཏོག་ཏོ་དང་ གཞན་མི་དམིགས་ཡུལ་ཚུ་གྲུབ་ཐབས་ལུ་ བདེ་སྲུང་བཟོ་ནི་ལུ་ ལག་ལེན་འཐབ་ཡོདཔ་འོང་།

གཞན་མི་ལས་སྒོ་གི་ཅ་ཆས་ཚུ་གིས་ གཙོ་བོར་བརྟེན་མི་གིས་ འཛིན་སྐྱོང་འཐབ་མི་ མཐའ་འཁོར་ནང་ བདེ་སྲུང་བཟོ་བའི་ སྒྲུབ་བྱེད་མ་སྟོནམ་ཨིན་པས།

འཛུལ་སྤྱོད།

བདེ་སྲུང་འཕྲོག་ཡོད་པའི་ཡོ་ཆས་དང་ལྡན་པའི་གཙོ་འཛིན་གྱིས་ VDI ལཱ་ཡུན་ཚུ་ལུ་ མཐུད་མི་ལག་ལེན་པ་ཚུ་གི་དོན་ལུ་ Active Directory དང་ཕྱེབ་སར་བར་བརྒྱུད་དེ་ བདེན་བཤད་བྱིན་ཡོདཔ་ཨིན། (T1021.001)

ས་གནས།	བདེ་སྲུང་བཟོ་ཡོད་པའི་ཐབས་འཕྲུལ་ཧོསིཊི་མིང་ཚུ་ (མངོན་གསལ་ཚད་སྙོམས་)
གནད་སྡུད་ལྟེ་བ་ ༡	HOST1, HOST2, HOST3

ཡོ་ཆས་གཞི་རྟེན་ནང་ ལག་ལེན་པས་ཡོ་ཆས་ནང་ལས་བཟོ་བསྐྲུན་འབད་དེ་ཕབ་ལེན་འབད་མི་བདེན་བཤད་བརྡ་རྟགས་ཐོབ་པའི་ཤུལ་ལས་ VDI ལུ་ཕུག་ལམ་བྱིན་མི་འཛུལ་སྤྱོད་སྒོ་སྲུང་གཙོ་འཛིན་ཚུ་ཡང་ཚུད་དེ་ཡོདཔ་ཨིན།

འ་ནི་གཙོ་འཛིན་ཚུ་གི་གྲལ་ལས་ ག་ཡང་ བདེ་སྲུང་བཟོ་བའི་ སྒྲུབ་བྱེད་མེདཔ་ཨིན་པས། ཨིན་རུང་ འཛུལ་སྤྱོད་སྒོ་སྲུང་ཧོསིཊི་དྲན་ཐོ་ཚུ་གིས་ ཤེས་རྟོགས་ཡོད་པའི་ གནོདཔ་ཅན་གྱི་IP ཁ་བྱང་ཚུ་དང་གཅིག་ཁར་ གལ་གནད་ཅན་གྱི་འབྲེལ་བ་འཐབ་ཡོད་པའི་སྒྲུབ་བྱེད་སྟོན་ཡོདཔ་ཨིན། འདི་གིས་ ཧོསིཊི་འདི་གུ་བྱུང་མི་ ལས་སྣ་འདི་ ཡང་ན་ ཧོསིཊི་འདི་ལུ་ལྡོད་མི་ ཉེན་ཁ་ཅན་གྱི་བྱེད་མཁན་གཞི་རྟེན་དང་གཅིག་ཁར་ ཡོངས་འབྲེལ་མཐུད་ལམ་ཚུ་ བརྡ་སྟོན་འབད་ཡོདཔ་བཟུམ་ཅིག་ཨིན། ལས་རིམ་འདི་གི་རང་གཤིས་འདི་ ཐོབ་ཡོད་པའི་སྒྲུབ་བྱེད་ཚུ་ལག་ལེན་འཐབ་སྟེ་ གཏན་འབེབས་བཟོ་མ་ཚུགས་རུང་ སྡེ་ཚན་འདི་གིས་ ལས་སྒོ་གི་ཡོངས་འབྲེལ་ནང་ལུ་ ཕྱོགས་གཅིག་ལས་ འགྱོ་ནི་གི་རྩིས་རྐྱབ་ཡོདཔ་སྦེ་ བརྡ་སྟོནམ་ཨིན། (TA0008)

ནང་འཁོད་ཧོསིཊི་ཚུ།

ASD གི་ ACSC གིས་ ནང་འཁོད་ལས་སྒོ་གི་ཡོངས་འབྲེལ་ཆ་ཤས་ནང་ལས་ གནས་སྡུད་ཚད་འཛིན་འབད་དེ་ཡོདཔ་སྦེ་ ཞིབ་དཔྱད་འབད་ནུག ནང་འཁོད་ལས་སྒོ་གི་ཡོངས་འབྲེལ་ཆ་ཤས་ལུ་ གནོད་སྐྱོན་བྱུང་ཡོད་པའི་ དཔའ་བཅམ་མི་དང་ ཡང་ན་ མཐར་འཁྱོལ་ཅན་གྱི་ གནོདཔ་ཅན་གྱི་ལས་སྣ་ཚུ་གིས་ ཕྱི་ཊི་ཨའི་དང་འབྲེལ་བའི་ ཅ་རྙིང་ཚུ་ལུ་ བྱེད་མཁན་འཛུལ་སྤྱོད་འབད་ནི་དང་ ནང་འཁོད་ཀྱི་ཨེསི་ཀིའུ་ཨེལ་སར་བར་ (T1505.001) དེ་ལས་ འགྲེལ་བཤད་མ་རྐྱབ་པའི་འགྱུལ་སྐྱོད་ཚུ་ ཤེས་རྟོགས་བྱུང་མི་ གླ་ཕྱི་ཨའི་པི་ཁ་བྱང་བརྒྱུད་དེ་ འཛུལ་སྤྱོད་འབད་མི་ཚུ་ ཚུདཔ་ཨིན། (TA0011)

བདེ་སྲུང་བཟོ་ཡོད་པའི་ཐབས་འཕྲུལ་ལུ་ ཁོང་གི་འཛུལ་སྤྱོད་ལག་ལེན་འཐབ་སྟེ་ སྡེ་ཚན་གྱིས་ ལག་ལེན་པའི་མིང་ངོ་མ་དང་ གསང་ཡིག་ཡིག་ (T1003) དེ་ལས་ ཨེམ་ཨེཕ་ཨེ་ཊོ་ཀེན་གནས་གོང་ཚུ་ (T1111) བསྡུ་ལེན་འབད་ཡོདཔ་ཨིན། སྡེ་ཚན་འདི་གིས་ JSON Web Tokens (JWTs) (T1528) ཡང་བསྡུ་ལེན་འབད་ཡོདཔ་ད་ འདི་ཡང་ བར་ཅུ་ཡལ་ཊེཀ་སི་ཊོཔ་ནང་བསྐྱོད་ལཱ་ཡུན་ཚུ་གསར་བསྐྲུན་འབད་ནི་ལུ་ལག་ལེན་འཐབ་མི་བདེན་བཤད་ཀྱི་ བརྡ་མཚོན་ཅིག་ཨིན། བྱེད་མཁན་འདི་གིས་ འདི་ཚུ་ལག་ལེན་འཐབ་སྟེ་ རྟོག་བཟོ་ཊེསིཀ་ཊོཔ་ལཱ་ཡུན་ཚུ་ གསར་བཟོ་འབད་ནི་ཡང་ན་བཀྲུ་འཕྲོག་འབད་ནི་

(T1563.002) དང་ ཁྲིམས་མཐུན་ལག་ལེན་པ་ཅིག་སྣེ་ འཚོགས་སྡེའི་ནང་འཁོར་དྲ་རྒྱའི་ཆ་ཤས་ལུ་ འཛུལ་སྤྱོད་འབད་ནི་ (T1078) ལུ་ རྩུགས་ཡོདཔ་སྦེད།

བྱེད་མཁན་འདི་ཡང་ ལས་སྡེའི་ནང་འཁོར་དྲ་རྒྱ་ནང་ཡོད་པའི་ SQL སར་བར་ (T1505.001) འདི་ བཏུབ་སྐྱུད་འབད་ནིའི་དོན་ལུ་ བདེ་སྲིག་འཕྲོག་ཡོད་པའི་ཡོ་ཆས་ལུ་ འཛུལ་སྤྱོད་འབད་ནུག། བྱེད་མཁན་འདི་གིས་ གནས་སྟུད་འདི་རྩུ་ འཐོབ་རྩུགསཔ་བཟུམ་ཅིག་འདུག།

འཛུལ་སྤྱོད་སྔོ་སྲིག་ཐབས་འཕྲུལ་ལས་ཐོབ་པའི་སྒྲུབ་བྱེད་རྩུ་གིས་ ཡོངས་འབྲེལ་འགྲུལ་སྐྱོད་འདི་ ཤེས་རྟོགས་ཡོད་པའི་ གནོདཔ་ཅན་གྱི་ IP ཁ་བྱང་རྩུ་ལས་ ཡང་ན་ ཐབས་འཕྲུལ་འདི་ནང་ལས་ འབྱུང་ཡོདཔ་སྦེ་ གསལ་སྟོན་འབད་ཡོདཔ་ཨིན། གོང་ལས་བཤད་དོ་བཟུམ་སྦེ་ འདི་གིས་ གནོདཔ་བཀལ་མི་ ཡོངས་འབྲེལ་གྱི་ བྱེད་མཁན་རྩུ་གིས་ ཐབས་འཕྲུལ་འདི་ལུ་ གནོད་སྐྱོན་རྐྱབ་ཡོདཔ་སྦེ་ བརྟ་སྟོནམ་ཨིནམ་མ་ཚད་ ནང་འཁོད་ཡོངས་འབྲེལ་ནང་ལུ་ འགྱོ་ནི་གི་ འོས་འབབ་ཡོདཔ་ཨིན།

ཞིབ་དཔྱོད་དུས་ཡུན།

འོག་གི་ཐོ་ཡིག་འདི་གིས་ ཞིབ་དཔྱད་འབད་བའི་སྐབས་ མཐོང་ཡོད་པའི་ ལཱ་གཙོ་བོ་རྩུ་གི་དུས་ཚོད་བཀོད་ཡོདཔ་ཨིན།

དུས་ཚོད།	ལས་དོན།
སྤྱི་ལོ་༢༠༢༢ སྤྱི་ཟླ་༩ པ།	ཤེས་རྟོགས་ཡོད་པའི་ གནོདཔ་ཅན་གྱི་ IP ཁ་བྱང་རྩུ་གིས་ འཛུལ་སྤྱོད་སྔོ་སྲིག་ཧོསིཊི་ HOST7 དང་ཅིག་ཁར་ འབྲེལ་བ་འཐབ་ཨིན། འབྲེལ་འཐབ་ཀྱི་རང་གཞིས་འདི་ གཏན་འབེབས་བཟོ་མ་ཚུགས།
སྤྱི་ལོ་༢༠༢༢ སྤྱི་ཟླ་༩ པ།	ཧོསིཊི་ཆ་མཉམ་ HOST1, HOST2 དང་ HOST3 རྩུ་ གནོདཔ་ཅན་གྱི་བྱེད་མཁན་ཡང་ན་ བྱེད་མཁན་རྩུ་གིས་ བརྟལ་བཤིག་གཏང་ཡོདཔ་ལས་ ཧོསིཊི་རྩུ་གུ་ཤེལ་ཤེལ་རྩུ་བཙུགས་ཡོདཔ་ཨིན། དྲན་དེབ་ཡིག་སྣོད་ཅིག་ HOST2 གུ་གསར་བསྐྲུན་ཡང་ན་ལེགས་བཅོས་འབད་ཡོདཔ་ཨིན། ཡིག་སྣོད་འདི་ནང་ གནོདཔ་ཅན་གྱི་བྱེད་མཁན་གྱིས་ འཛིན་བཟུང་འབད་ཡོདཔ་བཟུམ་ཅིག་ཡོད་པའི་ ངོས་ལེན་རྒྱུ་ཆ་རྩུ་ཡོདཔ་ཨིན། /etc/security/opasswd དང་ /etc/shadow ཡིག་སྣོད་རྩུ་ HOST1 དང་ HOST3 གུ་བསྒྱུར་བཅོས་འབད་ཡོདཔ་ལས་ གསང་ཡིག་རྩུ་བསྒྱུར་བཅོས་འབད་ཡོད་པའི་བདེན་རྟོནམ་ཨིན། HOST1 གུ་ཡོད་པའི་སྒྲུབ་བྱེད་རྩུ་གིས་ ལག་ལེན་པ་ 'sshuser' གི་གསང་ཡིག་འདི་བསྒྱུར་བཅོས་འབད་ཡོདཔ་སྦེ་ བསམ་འཆར་བཀོདཔ་ཨིན།
སྤྱི་ལོ་༢༠༢༢ སྤྱི་ཟླ་༩ པ།	HOST2 འདི་ ལས་སྡེ་གིས་ སྒོ་བསྡམ་ཡོདཔ་ཨིན། ཁ་སྐོང་ཕྱེབ་ཤེལ་ (T1505.003) རྩུ་ HOST1 དང་ HOST3 གུ་གསར་བསྐྲུན་འབད་ཡོདཔ་ཨིན། HOST1 གིས་ HOST3 ལས་ SSH བརྡུངས་ཤུགས་དཔའ་བཅམ་མི་ཉམས་མྱོང་ཐོབ་ཡོདཔ། དྲན་དེབ་ཡིག་སྣོད་ཅིག་ HOST3 གུ་ལེགས་བཅོས་འབད་ཡོདཔ་ཨིན་ (T1070)། ཡིག་སྣོད་འདི་ནང་ ངོས་ལེན་རྒྱུ་ཆ་ (T1078) གནོདཔ་ཅན་གྱི་བྱེད་མཁན་ཅིག་གིས་ འཛིན་བཟུང་འབད་ཡོདཔ་འོང་། JWTs རྩུ་ བཟུང་ཡོདཔ་ཨིན་ (T1528) དེ་ལས་ HOST3 གུ་ཡོད་པའི་ཡིག་སྣོད་ཅིག་ལུ་ ཐོན་འབྲས་བཏོན་ཡོདཔ་ཨིན། HOST3 འདི་ ལས་སྡེ་གིས་ སྒོ་བསྡམ་ཡོདཔ་ཨིན། དུས་ཚོད་འདི་གི་ཤུལ་ལས་ ལས་དོན་ཆ་མཉམ་ HOST1 གུ་འབྱུངམ་ཨིན།
སྤྱི་ལོ་༢༠༢༢ སྤྱི་ཟླ་༩ པ།	HOST1 ནང་ ཁ་སྐོང་གི་ཕྱེབ་ཤེལ་རྩུ་ གསར་བཟོ་འབད་ཡོདཔ་ཨིན། (T1505.003) JWTs རྩུ་ HOST1 གུ་ཡོད་པའི་ཡིག་སྣོད་ཅིག་ལུ་ འཛིན་བཟུང་འབད་དེ་ ཐོན་འབྲས་བཏོན་ཡོདཔ་ཨིན།
སྤྱི་ལོ་༢༠༢༢ སྤྱི་ཟླ་༩ པ།	ཁ་སྐོང་ཕྱེབ་ཤེལ་རྩུ་ HOST1 (T1505.003) གུ་གསར་བསྐྲུན་འབད་ཡོདཔ་དང་ ཤེས་རྟོགས་ཡོད་པའི་ གནོདཔ་ཅན་གྱི་ IP ཁ་བྱང་ཅིག་གིས་ ཧོསིཊི་ (TA0011) དང་ཅིག་ཁར་ འབྲེལ་བ་འཐབ་ཨིན། ཤེས་རྟོགས་ཡོད་པའི་ གནོདཔ་ཅན་གྱི་ IP ཁ་བྱང་ཅིག་གིས་ འཛུལ་སྤྱོད་སྔོ་སྲིག་ཧོསིཊི་ HOST7 དང་ཅིག་ཁར་ འབྲེལ་བ་འཐབ་ཨིན།
སྤྱི་ལོ་༢༠༢༢ ཟླ་༥ པ།	ཤེས་རྟོགས་ཡོད་པའི་ གནོདཔ་ཅན་གྱི་ IP ཁ་བྱང་ཅིག་གིས་ འཛུལ་སྤྱོད་སྔོ་སྲིག་ཧོསིཊི་ HOST7 (TA0011) དང་ཅིག་ཁར་ འབྲེལ་བ་འཐབ་ཡོདཔ་ཨིན། ལག་ལེན་པ་ཅིག་གི་དོན་ལུ་ བདེན་བཤད་བྱུང་ལས་ཅིག་ HOST1 གུ་ཡོད་པའི་དྲན་ཐོ་རྩུ་ནང་ ཤེས་རྟོགས་ཡོད་པའི་ གནོདཔ་ཅན་གྱི་ IP ཁ་བྱང་ཅིག་ལུ་འབྲེལ་མཐུད་འབད་ཡོདཔ་ཨིན། ཧོསིཊི་འདི་གུ་ ཕྱེབ་ཤེལ་ཁ་སྐོང་ཅིག་གསར་བསྐྲུན་འབད་ཡོདཔ་ཨིན་ (T1505.003)།
སྤྱི་ལོ་༢༠༢༢ ཟླ་༥ པ།	HOST1 གུ་ཡོད་པའི་ཡིག་ཆ་འདི་ བྱེད་མཁན་ཅིག་གིས་ ལེགས་བཅོས་འབད་ཡོདཔ་ཨིན་ (T1543)། ཡིག་རྩུགས་འདི་ནང་ ནང་འཁོད་ཨེསི་ཀིའུ་ཨེལ་སར་བར་ལས་ གནད་སྡུད་བཏོན་བཏང་ཡོད་པའི་ལས་འགན་རྩུ་ཡོདཔ་ཨིན།
སྤྱི་ལོ་༢༠༢༢ ཟླ་༥ པ།	HOST1 གུ་ཡོད་པའི་ དྲན་ཐོ་ཡིག་སྣོད་ཁ་སྐོང་ཅིག་ མཐའ་མཇུག་ལུ་ ལེགས་བཅོས་འབད་ཡོདཔ་ཨིན་ (T1070). ཡིག་སྣོད་འདི་ནང་ ལས་སྡེའི་ཡོངས་འབྲེལ་གྱི་དོན་ལུ་ ལག་ལེན་པའི་མིང་དང་ ཚིག་ཡིག་ཆ་གཅིག་ཡོདཔ་ད་ དེ་རྩུ་ ཁྲིམས་མཐུན་ཨིནམ་སྦེ་ ཡིད་ཆེས་བསྐྱེདཔ་ཨིན་ (T1078)།
སྤྱི་ལོ་༢༠༢༢ ཟླ་༥ པ།	ཁ་སྐོང་གི་དྲན་དེབ་ཡིག་སྣོད་ཅིག་ མཐའ་མཇུག་ལུ་ བསྒྱུར་བཅོས་འབད་ཡོདཔ་ཨིན། (T1070)། ཡིག་སྣོད་འདི་ནང་ HOST1 ལས་བསྡུ་ལེན་འབད་ཡོད་པའི་ JWTs རྩུ་ཡོདཔ་ཨིན།
སྤྱི་ལོ་༢༠༢༢ ཟླ་༥ པ།	HOST1 ནང་ ཁ་སྐོང་གི་ཕྱེབ་ཤེལ་རྩུ་ གསར་བཟོ་འབད་ཡོདཔ་ཨིན། (T1505.003)། ཚེས་གྲངས་འདི་ལུ་ འཚོགས་སྡེ་གིས་ སྤྱི་ལོ་༢༠༢༢ སྤྱི་ཟླ་༩ པའི་ནང་ བཟོ་བསྐྲུན་ཚེས་གྲངས་ཡོད་པའི་ ཕྱེབ་ཤེལ་ཅིག་ རྙེད་པའི་སྐོར་ལས་ ASD གི་ ACSC ལུ་ སྙན་སེང་འབད་ནུག
སྤྱི་ལོ་༢༠༢༢ ཟླ་༥ པ།	HOST1 ནང་ ཡིག་རྩུགས་གྲངས་ཁ་ཤས་གསར་བཟོ་འབད་ཡོདཔ་ད་ དེ་ནང་ Log4jHotPatch.jar ཟེར་མིང་བཏགས་མི་གཅིག་ཡང་རྩུད་དེ་ཡོདཔ་ཨིན།
སྤྱི་ལོ་༢༠༢༢ ཟླ་༥ པ།	iptables-save བརྡ་བཀོད་འདི་ འཛུལ་སྤྱོད་སྔོ་སྲིག་ཧོསིཊི་ལུ་ ཁ་ཕྱེ་ཡོད་པའི་འདྲེན་ལམ་གཉིས་ཁ་སྐོང་འབད་ནི་ལུ་ལག་ལེན་འཐབ་ཡོདཔ་ཨིན། འདྲེན་ལམ་རྩུ་ ༡༡༡༨ དང་ ༡༡༡༡ (T1572) ཨིན་པས།

བྱེད་མཁན་པའི་གནས་སྐབས་དང་ཐབས་ཤེས།

ཞིབ་དཔྱད་འབད་བའི་སྐབས་ དོས་འཛིན་འབད་མི་ གནས་སྐབས་དང་ ཐབས་ཤེས་ལེ་ཤ་ཅིག་ གཤམ་གསལ་ལྟར་ཡིན།

འགོ་ཐོག་འཛུལ་སྤྱོད།

T1190 མི་མང་ལ་གདོང་གཏད་པའི་ཡག་ལེན་སྒོག་སྤྱོད།

སྟེ་ཚན་འདི་གིས་ ཡོངས་འཛིལ་ནང་ལུ་ འགོ་ཐོག་འཛུལ་སྤྱོད་འབད་ནི་ གི་དོན་ལས་ ཐག་རིང་ལས་ ནང་བསྒྲིད་དང་ དོ་རྟགས་འཛིན་སྒྲིང་ གི་ཐོན་སྒྲིད་ནང་ལུ་ RCEདང་ ཐོན་དབང་ཡར་སེང་ དེ་ལས་ བདེན་བཤད་ཀྱི་ཉེན་ཁ་ཚུ་ ཡག་ལེན་འཐབ་ཡོད་པ་བཟུམ་ཅིག་ འདུག

འདི་འགོ་ཐོག་འཛུལ་སྤྱོད་ཐབས་ལམ་འདི་ གཤམ་གསལ་ཀྱི་དབང་གིས་ མངའ་ཤོས་འབྱུང་ཐིད་པ་སྟེ་བཅིངམ་ཨིན།:

- དེ་སྐབས་ སར་བར་འདི་ CVE འདི་ཚུ་ལུ་ ཉེན་ཁ་ཅན་ཅིག་ཨིན་པས།
- ཤེས་རྟོགས་ཡོད་པའི་བྱེད་མཁན་གཞི་རྟེན་ལས་ ཉེན་ཁ་འདི་ཚུ་ ཡག་ལེན་འཐབ་ནི་གི་དཔའ་བཅམ་ནི། དང་
- ཤེས་རྟོགས་བྱང་བའི་ནང་འཁོད་ཀྱི་གནོད་འཚེ་ཅན་ཀྱི་ལས་སྣ་འགོ་དང་པ་ འདི་ བགོལ་སྤྱོད་འབད་ནི་གི་དཔའ་བཅམ་པའི་ཤུལ་ལས་ འབྱུང་ཡོདཔ་ཨིན།

ལག་ལེན།

T1059.004 བཏ་བགོད་དང་ཡིག་གཟུགས་སྒྲུང་མཁན།: ཡུ་ནིགས་ཤེལ་

སྟེ་ཚན་གྱིས་ གོང་འཁོད་ཀྱི་ཉེན་ཁ་ཚུ་ མཐར་འགྱོལ་ཅན་སྟེ་ ལག་ལེན་འཐབ་ཡོདཔ་ལས་ གནོད་སྐྱོན་བྱུང་མི་ འཛུལ་ཚན་ཚུ་ ཡིག་ཆ་ཚང་ཡོད་པའི་ ཡུ་ནིགས་ཤེལ་ནང་ བཏ་བགོད་ཚུ་ གཡོག་ཡིག་ཚུགས་པའོང་། བྱེད་མཁན་ཚུ་གིས་ ཁྱབ་གཡོག་འཐབ་ཡོདཔ་ལས་ བགོད་ཀྱི་ཉེན་ཁ་ཚུ་ ཐབས་ཤེས་ལེ་ཤ་ཅིག་ཡོདཔ་ཨིན། བྱེད་མཁན་ཚུ་གིས་ ཁྱབ་གཡོག་ཐོག་ལས་ ཡུ་ནིགས་ཤེལ་ནང་ བཏ་བགོད་ཚུ་ གཡོག་ཐོག་ཚུགས་པ་འོང་། བྱེད་མཁན་ཚུ་གིས་ ཁྱབ་གཡོག་ཐོག་ལས་ ཡུ་ནིགས་ཤེལ་ལེ་ཤ་ཅིག་ ཐོན་སྐྱེད་ཀྱི་ཉེན་ཁ་ཚུ་ ཡག་ལེན་འཐབ་ཡོདཔ་ཨིན། ཡུ་ནིགས་ཤེལ་ནང་ བཏ་བགོད་ཚུ་ གཡོག་ཐོག་ཚུགས་པ་འོང་། བྱེད་མཁན་ཚུ་གིས་ ཁྱབ་གཡོག་ཐོག་ལས་ ཡུ་ནིགས་ཤེལ་ལེ་ཤ་ཅིག་ ཐོན་སྐྱེད་ཀྱི་ཉེན་ཁ་ཚུ་ ཡག་ལེན་འཐབ་ཡོདཔ་ཨིན། ཡུ་ནིགས་ཤེལ་ནང་ བཏ་བགོད་ཚུ་ གཡོག་ཐོག་ཚུགས་པ་འོང་། བྱེད་མཁན་ཚུ་གིས་ ཁྱབ་གཡོག་ཐོག་ལས་ ཡུ་ནིགས་ཤེལ་ལེ་ཤ་ཅིག་ ཐོན་སྐྱེད་ཀྱི་ཉེན་ཁ་ཚུ་ ཡག་ལེན་འཐབ་ཡོདཔ་ཨིན།

ཡུ་ཚུགས།

T1505.003 སར་བར་མཉེན་ཆས་ཆ་ཤས། ཤེལ་ཤེལ་

བྱེད་མཁན་ཚུ་གིས་ གནོད་སྐྱོན་བྱུང་མི་ ཅ་ཆས་གུང་ ཤེལ་ཤེལ་ལེ་ཤ་ཅིག་ བཀྲམ་སྤེལ་འབད་ནུག། བྱེད་མཁན་མ་འདྲ་བ་ལེ་ཤ་ཅིག་གིས་ཤེལ་ཤེལ་ཚུ་བཀྲམ་སྤེལ་འབད་ཡོདཔ་འདི་སྤྱིད་ཨིན་རྒྱུ་། བྱེད་མཁན་ཁྱང་སུ་ཅིག་གིས་ཆུང་ཤས་ཅིག་ཤེལ་ཤེལ་འདི་ཚུ་ ཡག་ལེན་འཐབ་སྟེ་ཁྱོད་རིམ་ཚུ་འགོ་འདྲེན་འབད་ཡོདཔ་ཨིན། ཤེལ་ཤེལ་ཚུ་གིས་ནང་ འཁོད་བྱེད་མཁན་ལུ་ བཅོན་ཐབས་ཀྱིས་བཟུང་ཡོད་པའི་ཅ་ཆས་ཚུ་གུ་ལུ་ རང་དབང་ངང་བཏ་བགོད་ལག་ལེན་འཐབ་ཚུགས་པའི་གོ་སྐབས་བྱིན་ཡོདཔ་ཨིན།

ཁེ་དབང་གི་འཐར་བ།

T1068 ཁེ་དབང་གི་འཐར་བ་གི་ཆེད་དུ་བགོལ་སྤྱོད།

ཐོབ་པའི་སྐྱབ་བྱེད་ཚུ་གིས་ བྱེད་མཁན་ཚུ་གིས་ ཐོབ་དབང་གི་གནས་ཚད་འདི་ འགྲེལ་བཤད་ཀྱི་མི་ཚུགས། ཨིན་རུང་ ཤེས་ཤེལ་ཚུ་ཡག་ལེན་འཐབ་སྟེ་ བྱེད་མཁན་ཚུ་གིས་ བདེ་སྐྱིག་ཡོད་པའི་ ཅ་ཆས་གྱ་ཡོད་པའི་ ཤེལ་སར་བར་དང་ གཏན་འཁེལ་ཡོད་པའི་ ཐོབ་དབང་ཐོག་ནས་ ཁྱོད་ཀྱིས་ ཅ་ཆས་ཀྱི་ནང་ལུ་ ཡོདཔ་སྟེ་ཡིད་ཆེས་འབད་ཡོད་པའི་ཉེན་ཁ་ཚུ་ ཐོབ་ཚུགས་ཡོད་ཅེཏ་ཡིན་ན། ཐོབ་དབང་ཐོག་ཚུགས་པའི་གོ་སྐབས་སྤྱིན་ཡོདཔ་ཨིན།

དོ་རྟགས་འཛུལ་སྤྱོད།

T1056.003 ནང་འཇུག་འཛིན་བཟུང་། ཤེལ་ཡོངས་འབྲེལ་འཛིན་བཟུང་

བདེ་སྐྱིག་བཟོ་ཡོད་པའི་ འཕྲུལ་ཆས་འདི་གི་སྐྱུབ་བྱེད་ཚུ་གིས་ བྱེད་མཁན་འདི་གིས་ ལག་ལེན་པའི་མིང་དང་ཚོག་ཡིག་ཆ་བརྒྱ་ལས་བཅད་དེ་ ཁྲིམས་མཐུན་སྤྱི་ ཡིད་ཆེས་བསྒྲིད་མི་ ཚིག་ཡིག་གསལ་ཀྱོག་ཀྱོ་ནང་ བཟུང་ཡོདཔ་སྤྱི་ཨིན་མས། འདི་ཚུ་ཡིག་སྟོད་ཅིག་ཤོས་ལས་ ཡིག་ཆ་ཚུ་ཐོབ་ནི་མི་ བདེན་བཤད་བྱ་རིམ་ངོ་མ་འདི་ ལེགས་བཅོས་འབད་དེ་ བཟུང་ཡོདཔ་བཟུམ་ཅིག་ཨིན། MFA ཉོ་ཀེན་ཚུ་གི་ རིན་ཐང་ཡང་ལེན་ཉེ་ཁ་བཞག་ཡོདཔ་ཨིན། འདི་ཚུ་ ཡིག་སྟོད་ཅིག་ཤོས་ལས་ ཁྲིམས་མཐུན་ནང་བསྒྲིད་ཚུ་དང་འབྲེལ་བའི་ MFA ཉོ་ཀེན་ཚུ་གི་ཉེན་སྐྱང་བྱིན་མི་ ཁྱད་པར་ཅན་གྱི་ གནས་གོང་ཚུ་ གསོག་འཇོག་འབདཝ་མི་ ‹གསང་བའི་སར་བར་› གི་བདེ་སྐྱིག་བཟོ་བའི་ སྐྱབ་བྱེད་མེདཔ་ཨིན།

T1040 ཡོངས་འབྲེལ་ཚོར་བ།

བྱེད་མཁན་འདི་གིས་ བཅོན་ཐབས་ཀྱིས་བཟུང་ཡོད་པའི་ ཅ་ཆས་གུར་ HTTP འགྲུལ་སྐྱོད་ཚུ་འཛིན་བཟུང་འབད་ཐོག་ལས་JWTs ཚུ་བཟུང་ཡོདཔ་སྟེ་ཡིད་ཆེས་སྐྱེད་ཡོདཔ་ཨིན། འདི་ཡང་ མཐུན་ཤུན་ tcpdump འདི་ བདེ་སྐྱིག་བཟོ་ཡོད་པའི་ ཅ་ཆས་གུར་ ལག་ལེན་འཐབ་ཡོད་པའི་ སྐྱབ་བྱེད་ཡོདཔ་ལས་ བྱེད་མཁན་འདི་གིས་ འ་ནི་ JWTs ཚུ་ག་དེ་སྟེ་ བཟུང་ཡོདཔ་ཨིན་ན་ འོང་སྟིད་ནི་ཨིན་མས།

T1539 ཤེལ་ལས་རིམ་ཀྱི་ཀུ་ཀི་ཞར་ཟ་བཀུ།

གོང་ལུ་འགེལ་བཤད་ཀྱབ་ཡོད་དོ་བཟུམ་སྟེ་ བྱེད་མཁན་གིས་ ཤེལ་ལྟ་ཡུན་ཀུ་ཀི་ཚུ་ དང་ རིགས་མཚུངས་ཡོད་མི་ JWTs ཚུ་ བཟུང་ཡོདཔ་ཨིན། འ་ནི་ཚུ་ བྱེད་མཁན་གིས་ འཛུལ་སྤྱོད་འབད་ནི་ཁ་ཏོན་ཡོད་པ་ཨིན། འ་ནི་ཚུ་ ཡག་ལེན་འཐབ་ཚུགས་ནི་ཨིན་པས།

གསར་རྩེད།

T1046 ཡོངས་འཛེལ་ཞབས་ཏོགས་གསར་རྩེད།

ཡོངས་འཛེལ་གྱི་ཚ་ཤས་གཅིག་ནང་ གཞན་མི་ཅ་ཚས་ཚུ་ པར་ལོག་བཏབ་ནིའི་དོན་ལུ་ བདེ་སྒྲིག་བཟོ་ཡོད་པའི་ ཅ་ཚས་གྱང་ ཡོངས་འཛེལ་པར་ལོག་བཏབ་ནི་གི་ མཐུན་རྐྱེན་ nmap འདི་ ལག་ལེན་འཐབ་ཡོད་པའི་ སྒྲུབ་བྱེད་ཡོདཔ་ཨིན། འདི་ བྱེད་མཁན་གྱིས་ འཛེལ་མཐུད་ཚུགས་པའི་ དྲན་རྐྱེའི་ཞབས་ཏོག་གཞན་ཚུ་ གཏོར་བཤད་འབདཝ་ནི་ལུ་ ལག་ལེན་འཐབ་ཡོདཔ་སྟེད། དེ་ཚུ་གིས་ ཡོག་སྤྱང་སྤོ་ལོག་གི་གོ་སྐབས་ཚུ་སྤྱི་ཚུགསཔ་ཨིན།

བསྟུ་ལེན།

ཐོབ་ཚུགས་པའི་སྒྲུབ་བྱེད་ཚུ་གིས་ བྱེད་མཁན་ཚུ་གིས་ གཞས་སྤྱད་ག་དེ་སྤྲེ་བསྟུ་ལེན་ འབད་ཡི་ག་དང་ ཡང་ན་ བདེ་སྒྲིག་བཟོ་ཡོད་པའི་ ཅ་ཚས་དང་ ཡང་ན་ གཞན་མི་ཡམ་ ཡུགས་ཚུ་ལས་ ག་ཅི་བསྟུ་ལེན་འབད་ཡི་ག་ གསལ་སྟོན་མི་འབད། ཨིན་རུང་ བྱེད་མཁན་ ཚུ་གིས་ བཀག་འཛིན་འབད་ཡོད་པའི་ ངོས་ལེན་ཡིག་ཚ་ (T1003) དང་ ཨེམ་ཨེཕ་ཨེ་ ཏེ་ཀེན་གནས་གོང་ (T1111) དེ་ལས་ གོང་ལས་འགེལ་བཤད་ཀྱབ་ཡོད་པའི་ JWTs ཚུ་ ཅིས་ཏེ་ བདེ་སྒྲིག་བཟོ་ཡོད་པའི་ འཕྲུལ་ཆས་གྱ་ཡིག་སྟོད་ཚ་མཉམ་ལུ་ འཛུལ་སྤྱོད་འབད་ ཚུགསཔ་བཟུམ་ཅིག་འདུག།

བཀའ་རྒྱ་དང་བཀག་འཛིན།

T1071.001 གློག་རིམ་བང་རིམ་མཐུན་སྒྲིལ། ཤེབ་མཐུན་འཛེལ་ཚུ།

བྱེད་མཁན་ཚུ་གིས་ བཏ་བཀོད་དང་ཚད་འཛིན་གྱི་དོན་ལུ་ ཤེབ་ཤེལ་ཚུ་ལས་ལག་ལེན་འཐབ་ ནུག། ཤེབ་ཤེལ་གྱི་བཏ་བཀོད་ཚུ་ འཕྲུལ་ཆས། (T1572) གྱ་ཡོད་པའི་ ད་ལྟོ་ཡོད་པའི་ཤེབ་ སར་བར་ལག་ལེན་འཐབ་སྟེ་ ཨེཆ་ཏེ་ཏེ་པི་ཨེསི་ཐོག་ལས་ བརྒྱུད་སྤྲོད་འབད་འོང་།

T1001.003 གཞས་སྤྱད་མག་ཐོམ་སི་སི། མཐུན་སྒྲིག ཇུས་བཟོ།

བྱེད་མཁན་ཚུ་གིས་ ཁྱིམས་མཐུན་འགྲུལ་སྤྱོད་དང་གཅིག་ཁར་ སྒ་བསྡེ་ཀྱབ་ནིའི་དོན་ལུ་ བཟོ་བཀོད་འབད་དེ་ཡོད་མི་ གནོད་དཔ་བཀལ་ནི་གི་དོན་ལུ་ བདེ་སྒྲིག་བཟོ་ཡོད་པའི་ཅ་ཚས་ ཚུ་ལག་ལེན་འཐབ་ནུག།

བརྟག་ཞིབ་དང་ཉེན་ཁ་སེལ་ཐབས་ཀྱི་ངོས་སྤྲོར།

ASD's ACSC གསལ་བསྒྲགས་བྱས་པ་ཡིན་པ་ནི། ཨས་ཏི་ཨེས་ཏི་ཨིའི་ [ཉེར་མཁོ་བརྒྱུད་དང་](#) འབེལ་བའི་ [བདེན་འཛིན་སྐྱོང་བའི་བཀོལ་སྤྱོད་བསྒྲུར་འཛུགས་ཐབས་ལམ་ཚུ་](#) ལག་ལེན་བྱ་དགོས་པ་ཡིན་དོ། འོག་ལུ་ APT40 གིས་ བཅོན་འཛུལ་འབད་མི་ཚུ་ བརྟག་དཔྱད་འབད་ནི་དང་ བཀག་ཐབས་འབད་ནི་གི་དོན་ལུ་ ཡོངས་འབྲེལ་ཉེན་སྐྱང་གི་ བྱ་སྤྱོད་ཚུ་ འབད་དགོ་པའི་ སྔོས་འཚར་ཚུ་ བཀོད་དེ་ཡོདཔ་དང་ དེ་གི་ཐུན་ལས་ ཐེག་ཁན་ ༧ པའི་ནང་ བསྡུས་གཏང་དེ་ཡོད་མི་ གཅོ་ཚོ་ TTPs བཞེ་གི་དོན་ལུ་ དམིགས་བསལ་གྱི་ མར་ཡག་འབད་དགོཔ་ཨིན།

ཤེས་རྟོགས།

གོང་ལུ་ངོས་འཛིན་འབད་ཡོད་པའི་ཡིག་སྒྲོད་ལ་ལུ་ ཅིག་ C:\Users\Public* དང་ C:\Windows\Temp* བཟུམ་གྱི་གནས་ཚོངས་ཚུ་ནང་བཀོཐག་བཞག་ཡོདཔ་ཨིན། འ་ནི་གནས་ཚོངས་ཚུ་ ཐྲིན་བཀང་འཛམ་གླིང་འབྱི་ཚུགསཔ་ལས་ གནད་སྡུད་འཕྲི་ནི་ལུ་ སྤྱབས་བའི་བའི་ས་ཚོངས་ཅིག་འོང་ནི་ཨིན། དེ་ཡང་ ཕྱིན་ཅོས་ནང་ ཐོ་བཀོད་འབད་ཡོད་པའི་ ལག་ལེན་པའི་རྩིས་ཐོ་ཚ་མཉམ་ལུ་ སྒྲོད་ཐོ་འདི་ཚུ་དང་ དེ་ཚུ་གི་ཡན་ལག་ སྒྲོད་ཐོ་ཚུ་ འཛུལ་སྤྱོད་འབད་ཚུགས། འཕྲལ་འཕྲལ་སྐབས་ ལག་ལེན་པ་ག་ར་གིས་ ཕྲུལ་ལས་ ཡིག་སྒྲོད་འདི་ཚུ་ འཛུལ་སྤྱོད་འབད་ཚུགས་ནི་ཨིན་མས་ ཡོུགས་གཅིག་ལུ་འཚུ་ནི་དང་ ཉེན་སྐྱང་འབད་ནི་ དེ་ལས་ ཐོན་རྫས་ཀྱི་ཁང་ཚུ་ནང་ ཁྱད་ཆོས་ཚུ་ དེས་གཏན་བཟོ་ནི་ལུ་ ཕྲུལ་མའི་ཞིབ་དཔྱད་འབད་དགོཔ་ཨིན།

འོག་གི་སིག་མ་ལམ་ལུགས་ཚུ་གིས་ དོགས་པ་ཅན་གྱི་ས་གནས་ཚུ་ནང་ལས་ ལག་ལེན་འཐབ་ནི་འདི་ མ་འདུ་བའི་ལས་སྣ་གི་བརྡ་མཚོན་ཅིག་སྟེ། འཚོལ་ཞིབ་ཨིན། གནས་སྤྱངས་ཆ་མཉམ་ནང་ གནོད་པ་ཅན་གྱི་ལས་སྣ་དང་ ཁྱད་ཆོས་ཚུ་ དེས་གཏན་བཟོ་ནི་ལུ་ ཕྲུལ་ལས་ཀྱི་ཨེ་ཕི་ཀེ་ཤནསི་ཚུ་ ཞིབ་དཔྱད་འབད་ནི་ དེ་ལས་ ཕྱི་ཁར་ཐོན་ནི་གི་གོ་སྐབས་ཚུ་ བྱིན་མ་ཚུགས།

མིང: འཛམ་གླིང་འབྲི་བཀུབ་པའི་ལག་བསྟར། - གནས་སྐབས།

ངོ་རྟགས: d2fa2d71-fbd0-4778-9449-e13ca7d7505c

འགྲེལ་བཤད: C:\Windows\Temp. ལས་བྱ་རིམ་ལག་ལེན་འཐབ་ནི་ཤེས་རྟོགས་འབད།

རྒྱབ་ཁྱད:

ལམ་ལུགས་འདི་གིས་ དཔེགས་བསལ་གྱིས་ C:\Windows\Temp* ནང་ལས་ ལག་ལེན་འཐབ་ནི་དོན་ལུ་བསྟུན་ཞིན། གནས་སྐབས་ཀྱི་ཐོ་འཛིན་འདི་ ཁན་ཐོག་ས་ཚུ་གིས་ ཡོངས་གྲགས་སུ་ལག་ལེན་འཐབ་སྟེ་ཡོདཔ་ལས་ C:\Windows ནང་གི་ འཛིག་རྟེན་ཡོངས་ཀྱིས་འབྲི་ཆོག་པའི་ཡན་ལག་ཐོ་འཛིན་གཞན་ལུ་ཆུ་ནང་ལས་སྟེལ་བ་ལས་ གནོད་སྐྱོན་ཅན་ཁ་ཚད་ཀྱི་ཅ་རྙིང་ཚུ་ བཏོན་ཏེ་ཡོདཔ་ཨིན།

རིམ་ལུགས་ཡང་ན་ཡོངས་འབྲེལ་ཞབས་རྟོག་ལག་ལེན་པ་ཚུ་གིས་ ལག་ལེན་འཐབ་མི་ སྒོག་རིམ་ཚུ་བརྟེན་གཏང་མི་འདི་གིས་ ལམ་ལུགས་འདི་གིས་ སེལ་འཐུ་འབད་ཡོད་པའི་ བའེ་རྟོག་ཏོ་གི་ལས་སྣ་གི་འབོར་ཚད་འདི་ གནམ་མེད་ས་མེད་མར་ཕབ་འབདཔ་ཨིན།

འདི་གི་དོན་དག་ ལམ་ལུགས་འདི་གིས་ ཐོན་དབང་གནས་རིམ་མཐོ་བའི་ནང་ གཏོང་ཚད་ཀྱི་སྒེལ་བ་ཚུ་ མ་ཐོན་པར་འགྱོ་གི་ཡིན། དེ་འབདཔ་ལུ་ ལམ་ལུགས་འདི་གིས་ ཐོན་དབང་གནས་རིམ་མཐོ་བའི་ནང་ གཏོང་ཚད་ཀྱི་སྒེལ་བ་ཚུ་ ལག་ལེན་པ་ཚུ་ ཡོངས་ཀྱི་ SYSTEMལུ་ཐུར་འཕེལ་འབད་ནི་ལུ་ འབད་རྩོལ་བསྐྱེད་དོ་ཡོདཔ་ཨིན་ན་མེན་ན་ གཏན་འབེལ་བས་བཟོ་ནི་ལུ་ ལམ་ལུགས་གཞན་ཚུ་ལག་ལེན་འཐབ་དགོཔ་སྟེ་ འོས་སྤྱོར་འབད་ཡོདཔ་ཨིན།

ཞིབ་དཔྱད:

1. ལག་ལེན་པའི་སྐབས་དོན་དང་ ལག་ལེན་འཐབ་ནིའི་ཚིག་སྒྲིལ་གནས་རིམ་དེ་འཕྲོ་ལས་ རྩེས་འཇུག་ལས་རིམ་དང་ ཡིག་སྒྲོད་ཀྱིས་མངོན་གསལ་འབད་ཡོད་པའི་ གཟུགས་བརྙན་ཚུ་བཟུམ་གྱི་ ཡིག་སྒྲོད་ལག་ལེན་འཐབ་ནི་འདི་ དང་ ཐད་ཀར་དུ་འབྲེལ་བ་ཡོད་པའི་བཏང་དོན་ཚུ་ བརྟག་ཞིབ་འབད།
2. ལས་རིམ་འདི་ གནོད་པ་ཅན་ཞེན་ན་མེན་ན་ བརྟག་ཞིབ་འབད་ནི་ལུ་ སྤོགས་རམ་འབད་ནི་ལུ་ ཉོས་ཤིའི་གླ་ཡོད་པའི་ སྐབས་དོན་བྱ་རིམ་དང་ ཡོངས་འབྲེལ་ཡིག་སྒྲོད་ དེ་ལས་ གཞན་མི་རྣམ་སྐྱོར་གནས་སྤྱད་ཚུ་ ཞིབ་དཔྱད་འབད།
3. དགོས་མཁོ་ཡོད་པ་ཅིན་ ཁྲིམས་མཐུན་ཞེན་ན་མེན་ན་ གཏན་འབེལ་བས་བཟོ་ནི་ལུ་ ལོག་བཟོ་རིག་གི་དོན་ལུ་ ཡིག་སྒྲོད་ཀྱི་འདུ་བཤུས་བསྡུ་ལེན་འབད་ནི་ལུ་ དཔའ་བཅམ་དགོ།

སྐུལ་གཏུགས།:

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

རྩོམ་སྒྲིག་པ: ASD's ACSC

ཐྱི་ཚེས: ২০২৩/০৬/৶৫

གནས་ཚད: ཚོད་ལྟའི་

Tags:

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

དབྱ་ཐོའི་འབྱུང་ཁུངས།:

དབྱེ་རིམ: བྱ་རིམ_གསར་བཟོ

ཐོན་སྐྱེད: ཕིན་ཅོས།

ཤེས་རྟོགས།:

temp:

གཟུགས་བརྙན།འགོ་ཚུགས།: 'C:\\Windows\\Temp\\'

ཐྲིན་བཀང་_གནས་སྐབས་_འགྲོལ་ལམ:

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

རིམ་ལུགས་_ལག་ལེན་པ།:

ལག་ལེན་པ།:

- 'རིམ་ལུགས'
- 'ཡོངས་འབྲེལ་ཞབས་རྟོག'

dismhost:

གཟུགས་བརྟན་|མཇུག་བསྡུ:'dismhost.exe'

known_parent:

ཡམ་གཟུགས་བརྟན་|མཇུག་བསྡུ:

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

གནས་སྟངས: ཉེམ་པི་དང་མེན་ (སྤྱིར་བཏང་_ཉེམ་པི་_འགྲུལ་ལམ་ ཡང་ན་ རིམ་ལུགས་_ལག་ལེན་པ་ ཡང་ན་ ཇིས་ཏོ་སྟེ་ ཡང་ན་ ཤེས་རྟོགས་_ཡམ་)

རྩུབ་མའི་ངེས་གཏན་ཚུ།

- ཚོག་ཐམ་རྩིས་ཞིབ་བློག་རིམ་ཚུ་ ཉེམ་པི་ལས་ ལག་ལེན་འཐབ་བཏུབ་མི་ཚུ་ གལ་ཆེག་བཀོལ་བའི་བསྒང་ཡོད་པ་སྟེ་ བསྟུ་ཡོད་པ་ཞིན།
- ཉེམཔི་ནང་ ཁྱིམས་མཐུན་ཐོག་ལས་ གཞི་སྒྲིག་བློག་རིམ་དང་ འགོ་བཙུགས་མི་ཚུ་གི་ ཚེ་རེ་ཚུ་འོང་ནི་ཞིན་ལས་ ལམ་ལུགས་འདི་ བཀྲམ་སྤེལ་མ་འབད་བའི་ཉེ་མ་ ལྟ་རྟོག་འབད་ཡོད་པའི་ཡོངས་འཛིལ་ནང་ སྤྱོད་ལམ་འདི་ གཅེ་སྟེ་ ཁྱབ་ཚེཕ་ཞིན་ན་ བསྟུ་དགོས་ཞིན།

རིམ་པ: དམའ་བ།

མིང: འཛིག་རྟེན་ཡོངས་ཀྱི་འབྲི་ཚོག་སྒེལ་བ། - གནས་སྐབས་མིན་པའི་-རིམ་ལུགས་ཡན་ལག་ཐོ་འཛིན།

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

འགྲེལ་བཤད: ཁིན་ཇོ་ཙོ་ཚེའི་གཞི་བཙུགས་གནས་ཁོངས་ཀྱི་ཡན་ལག་སྤྱོད་ཐོ་ནང་ འཛམ་གླིང་འཛི་བཏུབ་པའི་གནས་ཁོངས་ལས་བྱ་རིམ་ལག་ལེན་འཐབ་ནི་ཤེས་རྟོགས་འབད།

རྒྱབ་སྐྱོར:

ལམ་ལུགས་འདི་གིས་ དཔེགས་བསལ་དུ་ C:\ ནང་དང་ ལྷག་པར་དུ་ C:\Windows* ནང་གི་ འཛིག་རྟེན་ཡོངས་ཀྱིས་འཛི་ཚོག་པའི་ཐོ་འཛིན་ཚུ་ལས་ སྤེལ་བ་ཚུ་འཚོལ་ཞིབ་འབདཔ་ཨིན། C:\Windows\Temp འདི་བར་ཆོད་ཨིན། (འདི་ ཐབ་ཐོགས་ཅན་གྱི་ སྒྲིག་རིམ་ཚུ་གིས་ ཡོངས་གྲགས་སུ་ལག་ལེན་འཐབ་སྟེ་ཡོད་པ་ལས་ གཞོད་སྐྱོན་ཅན་གྱི་ བརྡ་རྟགས་ཡིད་ཆེས་ཀྱི་གནས་ཚད་དམའ་བ་ཅིག་ཨིན།)།

ཡིག་སྒྲོད་ཅིག་ SYSTEM སྤེ་གཡོག་བཀོལ་བ་ཅིན་ AppData སྒྲོད་འཛིན་ཚུ་ ཕྱིར་བཏོན་འབདཔ་ཨིན་ - འདི་ གནས་སྐབས་ཀྱི་སྒྲིག་རིམ་ཡིག་སྒྲོད་ལེ་ཤ་ཅིག་ ལག་ལེན་འཐབ་མི་ བདེ་ཏོག་ཏོ་གི་ཐབས་ལམ་ཅིག་ཨིན།

འགོ་ཐོག་དུ་རྒྱུའི་གཞི་རྟེན་འདི་ མཇུག་བསྡུ་ཞིནམ་ལས་ ས་གནས་འདི་ཚུ་ནང་ལས་ ཤེས་རྟོགས་ཡོད་པའི་ བདེ་ཏོག་ཏོ་སྟེ་ ལག་ལེན་འཐབ་མི་ཚུ་ངོས་འཛིན་འབདཝ་བའི་ཐུལ་ལས་ ལམ་ལུགས་འདི་ དགོཝ་དགོས་སྟེ་ ཝེ་བཏང་དགོས་ཨིན།

ཞིབ་དཔྱད:

1. ལག་ལེན་པའི་སྐབས་དོན་དང་ ལག་ལེན་འཐབ་ནི་ཅི་ཚེག་སྒྲིལ་གནས་རིམ་དེ་འཛོལ་ལས་ རྟེས་འཇུག་ལས་རིམ་དང་ ཡིག་སྒྲོད་ཀྱིས་མངོན་གསལ་འབད་ཡོད་པའི་ གཟུགས་བརྟན་ཚུ་བཟུམ་གྱི་ ཡིག་སྒྲོད་ལག་ལེན་འཐབ་ནི་འདི་དང་ ཐད་ཀར་དུ་འབྲེལ་བ་ཡོད་པའི་བཅུ་དོན་ཚུ་ བརྟག་ཞིབ་འབདཝ་ཨིན།
2. ལས་རིམ་འདི་ གཅོད་པ་ཅན་ཚེན་ན་མེན་ན་ བརྟག་ཞིབ་འབད་ནི་ཡུ་ གོགས་རམ་འབད་ནི་ཡུ་ དོ་སིའེ་ཀུ་ཡོད་པའི་ སྐབས་དོན་བྱ་རིམ་དང་ ཡོངས་འབྲེལ་ ཡིག་སྒྲོད་ དེ་ལས་ གཞན་མི་ཚུ་ལ་སྐྱོར་གནས་སྟུད་ཚུ་ ཞིབ་དཔྱད་འབད།

3. དགོས་མཁོ་ཡོད་པ་ཅིན་ ཁྱིམས་མཐུན་ཚེན་ན་མེན་ན་ གཏན་འབེབས་བཟོ་ནི་དེ་ན་ཡུ་ ལོག་བཟོ་རིག་གི་དོན་ཡུ་ ཡིག་སྒྲོད་ཀྱི་འདུ་བཏུས་བསྡུ་ལེན་ འབད་ནི་ཡུ་ དཔའ་བཅམ་དགོ།

སྐྱེས་གཏུགས།:

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

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

རྩོམ་སྒྲིག་པ: ASD's ACSC

ཟླ་ཚེས: ২০২৩/০৬/১৮

གནས་ཚད: ཚོང་ལྷའི་

Tags:

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

དབྱ་ཐོའི་འཐུང་སྐྱེས།:

དབྱེ་རིམ: བྱ་རིམ_གསར་བཟོ

ཐོག་སྐྱེད: ཕིན་ཏོསི།

ཤེས་རྟོགས།:

འབྲི་བཏུབ་_འགྲུལ་ལམ:

གཟུགས་བརྟན་|ནང་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\\'

appdata:

གཟུགས་བརྙན་|ནང་ཡོད། '\\AppData\\'

ལག་ལེན་པ། 'རིམ་ལུགས'

condition: writable_path and not appdata

རྩྭ་མའི་དེས་གཏན་ཚུན།:

ཆོག་ཐམ་ཐོ་ཡིག་རྩིས་ཞིབ་གླེག་རིམ་ཚུ་ སྟོང་ཐོ་འདི་ཚུ་ལས་ བགོལ་སྟོང་འབད་བཏུབ་མི་ཚུ་ གལོག་བགོལ་བའི་བསྟུང་ཡོདཔ་སྟེ་ བཤུ་ཡོདཔ་ཞིན།

ཤུ་རྐོག་འབད་ཡོད་པའི་མཐའ་འཁོར་ནང་ལག་ལེན་འཐབ་མི་ ཡིག་ཆ་དང་བདག་སྐྱོང་ལག་ཆས་ཚུ་ སྟོང་ཐོ་འདི་ཚུ་གི་གླལ་ལས་གཅིག་ནང་ ཡོདཔ་བོང་ནི་ཞིནམ་ལས་ གནད་དོན་རེ་རེ་བཞིན་དུ་ ཁ་བྱང་བགོད་དགོཔ་ཞིན།

གནས་རིམ: མཐོ།

མིང: འཛམ་གླིང་འབྲེལ་བཏུབ་པའི་ལག་བསྟར། - ལག་ལེན་པ་ཚུ།

ངོ་རྟགས: 6ddd3843-182a-4214-9263-925a80b4c634

འགྲེལ་བཤད: ལག་ལེན་པ་ཚུ་གི་ནང་འགོད་ལུ་ C:\Users\Public* དང་གཞན་འཛམ་གླིང་འབྲེལ་བཏུབ་པའི་སྟོང་འཛིན་ཚུ་ལས་ ལས་སྟོན་ལག་ལེན་འཐབ་ནི་ཤེས་རྟོགས་འབད།

རྒྱབ་ཁྲངས:

ཡིག་སྟོང་ཅིག་ SYSTEM སྤེ་གཡོག་བགོལ་བ་ཅིན་ AppData སྟོང་འཛིན་ཚུ་ ཕྱིར་བཏོན་འབདཝ་ཞིན། - འདི་ གནས་སྐབས་ཀྱི་གླེག་རིམ་ཡིག་སྟོང་ལེ་ཤ་ཅིག་ ལག་ལེན་འཐབ་མི་ བདེ་ཏོག་ཏོ་གི་ཐབས་ལམ་ཅིག་ཞིན།

ཞིབ་དཔྱད།:

1. ལག་ལེན་པའི་སྐབས་དོན་དང་ ལག་ལེན་འཐབ་ནི་ཉིག་གླེལ་གནས་རིམ་དེ་འཕྲོ་ལས་ རྩེས་འཇུག་ལས་རིམ་དང་ ཡིག་སྟོང་ཀྱིས་མངོན་གསལ་འབད་ཡོད་པའི་ གཟུགས་བརྙན་ཚུ་བཟུམ་གྱི་ ཡིག་སྟོང་ལག་ལེན་འཐབ་ནི་འདི་ དང་ ཐད་ཀར་དུ་འབྲེལ་བ་ཡོད་པའི་བརྟེན་ཚུ་ བརྟག་ཞིབ་འབད།
2. ལས་རིམ་འདི་ གནོད་པ་ཅན་ཞིན་ན་མེན་ན་ བརྟག་ཞིབ་འབད་ནི་ལུ་ གོགས་རམ་འབད་ནི་ལུ་ ཉོསཱིའེ་གུ་ཡོད་པའི་ སྐབས་དོན་བྱ་རིམ་དང་ ཡོངས་འབྲེལ་ཡིག་སྟོང་ དེ་ལས་ གཞན་མི་རྒྱབ་སྟོར་གནས་སྤྱད་ཚུ་ ཞིབ་དཔྱད་འབད།
3. དགོས་མཁོ་ཡོད་པ་ཅིན་ ཁྲིམས་མཐུན་ཞིན་ན་མེན་ན་ གཏན་འབེབས་བཟོ་ནིའི་དོན་ལུ་ ལོག་བཟོ་རིག་གི་དོན་ལུ་ ཡིག་སྟོང་ཀྱི་འདུ་བཏུས་བསྡུ་ལེན་ འབད་ནི་ལུ་ དཔའ་བཅམ་དགོ།

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

རྩོམ་སྒྲིག་པ: ASD's ACSC

ཐྱི་ཚེས: ২০২৯/০৬/১৮

གནས་ཚད: ཚོད་ལྟའི་

Tags:

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

དབྱ་ཐོའི་འབྱུང་ཁྲངས།:

དབྱེ་རིམ་: བྱ་རིམ་_གསར་བཟོ།
ཐོན་སྐྱེད: ཕིན་ཏོས།

ཞིབ་རྟོགས།:

ལག་ལེན་པ་ཚུ་:

གཟུགས་བརྙན་ཁ་ཤོད།:

- ‘:\\ལག་ལེན་པ་ཚུ\\ལག་ལེན་པ་ཆ་མཉམ།\\’
- ‘:\\ལག་ལེན་པ་ཚུ་\\འབྲེལ་བ་འཐབ་མི་ཚུ་\\’
- ‘:\\ལག་ལེན་པ་ཚུ\\སྔོན་སྒྲིག\\’
- ‘:\\ལག་ལེན་པ་ཚུ་\\སྤྱི་དམངས།\\’
- ‘:\\ལག་ལེན་པ་ཚུ\\འཚོལ་ཞིབ་ཚུ་\\’

appdata:

གཟུགས་བརྙན་ཁ་ཤོད།’\\AppData\\’

ལག་ལེན་པ།: ‘རིམ་ལུགས’

གནས་སྟངས་: ལག་ལེན་པ་ཚུ་དང་ ཨེཔ་ཊ་ཏ་མེད།

ཛུན་མའི་ངེས་གཏན་ཚུ།:

- ལྷ་རྟོག་འབད་ཡོད་པའི་མཐའ་འཁོར་ནང་ལག་ལེན་འཐབ་མི་ ཡིག་ཆ་དང་བདག་སྐྱོང་ལག་ཆས་ཚུ་ མི་མང་ཡང་ན་ ཡན་ལག་སྡོད་ཐོ་ནང་ཡོདཔ་ལས་ གནད་དོན་རེ་རེ་བཞིན་དུ་ ཁ་གསལ་འབད་དགོཔ་འདི་འོས་འབབ་ཅན་ཅིག་ཨིན།

རིམ་པ: འཕྲིང་།

ཉེན་ཁ་སེལ་ཐབས།

ནང་བསྐྱོད་འབད་དོ།

ASD གི་ ACSC ཞིབ་དཔྱད་ཀྱི་སྐབས་ལུ་ ཞིབ་དཔྱད་ཀྱི་ནུས་པ་དང་མགྱོགས་ཚད་མར་ཕབ་འབད་མི་ སྤྱིར་བཏང་གི་གནད་དོན་གཅིག་འདི་ ཕྱིབ་སར་བར་གྱི་ཞུ་བ་ལོག་ཐོ་དང་ | ཕྱིན་ཊོསི་བྱུང་བའི་གནད་ཀ་ལོག་ཐོ། དེ་ལས་ཨིན་ཊར་ནེཊི་པོརོག་སི་ལོག་ཐོ་ཚུ་བཅིས་ཏེ་ ཁོངས་ཁ་གསུམ་ནང་ རྒྱས་པའི་བརྡ་དོན་ཐོ་འགོད་དང་ལོ་རྒྱུས་ཀྱི་བརྡ་དོན་ཐོ་འགོད་མ་ཐོབ་པ་འདི་ཨིན།

ASD གི་ ACSC གིས་ ཕྱིན་ཊོསི་འབྱུང་ལས་དྲན་ཐོ་དང་གཏོང་ལེན [གི་ཐད་ལུ་ཁོང་གི་ལམ་སྟོན་བསྐྱར་ཞིབ་དང་ལག་ལེན་འཐབ་དགོ་པའི་གྲོས་འཆར་ཞུ་ནུག།] འདི་ནང་ ཕྱིན་ཊོསི་འབྱུང་ལས་དྲན་ཐོ་མཇོད་ཁང་ [གི་རིམ་སྒྲིག་ཡིག་ཆ་དང་སྐད་ཡིག་ཚུ་དང་།] བརྡ་དོན་བདེ་སྐྱོབ་ལག་དེབ་ཀྱི་ [རིམ་ལུགས་ལྟ་རྟོག་གི་ལམ་སྟོན་ ཚུ་འདུས་དེ།] དྲན་ཐོ་ཚུ་དབུས་སྒྲིག་འབད་ནི་དང་འོས་འབབ་ཀྱི་དུས་ཚོད་རིང་ལུ་དྲན་ཐོ་ཚུ་ཉར་ཚགས་འཐབ་ནི་ཚུ་ཚུད་དགོཔ་ཨིན།

ཐིག་ཁྲམ་འཛིན་སྐྱོང་།

ཕྱིབ་སར་བར་དང་ ཕྱིབ་གློག་རིམ་ དེ་ལས་ ཐག་རིང་འཛུལ་སྤྱོད་ཀྱི་སྒོ་སྒྲིག་ཚུ་རྩིས་ཏེ་ ཡོངས་འབྲེལ་གྱི་ ཕྱིར་བཏོན་འབད་ཡོད་པའི་ ཐབས་འཕྲུལ་དང་ཞབས་ཏོག་ཚུ་ཆ་མཉམ་དུས་འཕྲལ་ལས་ ཐབས་ཤེས་བཟོ། བྱ་རིམ་འདི་རང་བཞིན་དང་མགྱོགས་དྲགས་བཟོ་ནི་ལུ་ དབུས་སྒྲིག་ཐིག་ཁྲམ་འཛིན་སྐྱོང་ལམ་ལུགས་ཅིག་ ལག་ལེན་འཐབ་ནི་ལུ་བསམ་ཞིབ་འབད། ASD’s ACSC གིས་ ISM’s [གི་རིམ་ལུགས་འཛིན་སྐྱོང་གི་ལམ་སྟོན་ ལག་ལེན་འཐབ་དགོ་པའི་གྲོས་འཆར་ཞུ་ནུག།] དམིགས་བསལ་དུ་འཇུག་སྤྱོད་ཆོག་པའི་ས་གནས་ཚུ་ནང་རིམ་ལུགས་རྒྱབ་སྐྱོང་ཚད་འཛིན་ཚུ་ཨིན།

བྱེད་མཁན་གིས་ ལག་ལེན་འཐབ་མི་ ལོག་སྤྱོད་མང་ཤོས་རང་ མི་མང་གིས་ཤེས་ཡོདཔ་དང་ འདི་ནང་ལུ་ ཐབས་ཤེས་དང་ ཡང་ན་ མར་ཕབ་འབད་ནི་གི་ཐབས་ལམ་ཚུ་ཡོདཔ་ཨིན་པས། ལས་སྡེ་ཚུ་གིས་ཨིན་ཊར་ནེཊ་ཐད་ཀར་འབྲེལ་བའི་གཞི་རྟེན་འཕྲུལ་རིག་ཚུ་ལུ་ཚོད་༩༨ གི་ནང་འཁོད་ལུ་བདེ་སྲུང་རྒྱབ་སྐྱོང་ཡང་ན་སྲུང་སྐྱོབ་ཐབས་ཤེས་ཚུ་བཏབ་དགོ་པ་དང་། ཚོགས་པ་ཅིན་མཉེན་ཆས་དང་བཀོལ་སྤྱོད་རིམ་ལུགས་ཀྱི་མཐའ་མའི་འཐོན་རིམ་ཚུ་ལག་ལེན་འཐབ་དགོ་པའི་ཁེངས་ཡོད་གཏང་དགོཔ་ཨིན།

ཡོངས་འབྲེལ་ཆ་ཤས་བཟོ་ནི།

ཡོངས་འབྲེལ་དབྱེ་འབྱེད་འདི་གིས་མི་བཟང་ཚུ་ལུ་ལས་སྡེ་གི་གསང་བའི་གནས་སྡུད་ཚུ་འཚོལ་ཞིབ་འབད་ནི་དང་ཞུགས་འཛོབ་ཚུགས་ནི་ལུ་ལག་འདེབས་ངེས་པར་དུ་ཁག་སྦོམ་བཟོ་འོང་། དགོས་མཁོ་མེད་པ་ཅིན་ གློག་རིག་ཚུ་གི་བར་ན་ འགྲུལ་སྐྱོད་བཀག་ཆ་འབད་དེ་ ཟུར་ཁའི་འགྲུལ་སྐྱོད་ཚད་འཛིན་ཡང་ན་ བཀག་ཆ་འབད་ནི་ལུ་ ཡོངས་འབྲེལ་ཚུ་ཆ་ཤས་བཟོ། ཁག་ཆེ་བའི་སར་བར་ཚུ་ དཔེར་ན་ ཤུགས་ལྡན་སྡོད་ཐོ་དང་ གཞན་མི་བདེན་བཤད་སར་བར་ཚུ་ བར་མཚམས་སར་བར་གྱུངས་ཁ་ཚད་ཅིག་ལས་ ཡང་ན་ ‘མཆོང་སར་བར་ཚུ’ ལས་རྐྱངམ་ཅིག་ བདག་སྐྱོང་འབད་ཚུགས་དགོ། སར་བར་འདི་ཚུ་ ལེགས་ཤོམ་སྦེ་ བལྟ་རྟོག་འབད་དགོཔ་མ་ཚད་ ལེགས་ཤོམ་སྦེ་ ཉེན་སྲུང་འབད་དགོཔ་མ་ཚད་ ལག་ལེན་པ་དང་ ཐབས་འཕྲུལ་ག་ཚུ་གིས་ མཐུད་ཚུགསཔ་ཨིན་ན་ ཚད་འཛིན་འབད་དགོཔ་ཨིན།

ཕྱོགས་འགྱུར་གྱི་སྒོ་བ་བཀག་ཐབས་འབད་ཡོད་མི་གནས་སྟངས་ཚུ་ངོས་འཛིན་འབད་ཟང་། ཁ་སྐོང་གི་ཡོངས་འབྲེལ་དབྱེ་འབྱེད་འདི་གིས་བྱེད་མཁན་ཚུ་གིས་གནས་སྡུད་འཐོབ་ནི་དང་ཕྱིར་འདོན་འབད་ཚུགས་མི་གི་ཚད་གཞི་དེ་ད་ལྟོ་ལས་འང་ཚད་འཛིན་འབད་ཚུགས་ནུག

ཁ་སྐོང་གི་ཉེན་ཁ་སེལ་ཐབས།

རྩོམ་བྲིས་ལས་སྡེ་ཚུ་གིས་ APT40 དང་ གཞན་མི་ཚུ་གིས་ གཞམ་གསལ་གྱི་ TTPs ལག་ལེན་འཐབ་མི་ཚུ་ལུ་ གདོང་ལེན་འབད་ནི་གི་དོན་ལུ་ གཞམ་གསལ་གྱི་ ཉེན་སྲུང་ཚུ་ གྲོས་འཆར་བཀོད་ནུག།

- ལག་ལེན་མ་འཐབ་མི་དང་ ཡང་ན་ དགོས་མཁོ་མེད་པའི་ཡོངས་འབྲེལ་ཞབས་ཏོག་ཚུ་དང་ འདྲེན་ལམ་ཚུ་ དེ་ལས་ མཐུན་འབྲེལ་ཚུ་ ལྕོགས་མིན་བཟོ།
- ཕྱིབ་སར་བར་དང་གློག་རིམ་ཚུ་ཉེན་སྲུང་འབད་ནི་ལུ་ ལེགས་ཤོམ་སྦེ་བསྒྱུར་བཅོས་འབད་ཡོད་པའི་ཕྱིབ་གློག་རིམ་ཕ་ཡར་ཝོལ་ཚུ་ (WAFs) ལག་ལེན་འཐབ།
- སར་བར་དང་ཡིག་སྣོད་བགོ་བཤའ་ དེ་ལས་ ཐོན་ཁུངས་གཞན་ཚུ་ལུ་འཛུལ་སྤྱོད་ཚད་འཛིན་འབད་ནི་ལུ་ ཐོབ་དབང་ཉུང་ཤོས་བཀག་དམ་འབད།
- ངོས་ལེན་ཡིག་ཆ་ཚུ་ བཟུང་ནི་དང་ ལོག་སྤྱོ་ལག་ལེན་འཐབ་ནི་ལུ་ ལྷ་ཁག་བཟོ་ནི་ལུ་ སྣ་མང་རྒྱུ་རྐྱེན་བདེན་བཤད་ (MFA) དང་ འཛིན་སྐྱོང་འཐབ་ཡོད་པའི་ཞབས་ཏོག་རྩིས་ཐོ་ཚུ་ལག་ལེན་འཐབ། MFA འདི་ ཡོངས་འབྲེལ་འཛུལ་སྤྱོད་འབད་ཚུགས་པའི་ ཐག་རིང་འཛུལ་སྤྱོད་ཞབས་ཏོག་ཚུ་ག་ར་ལུ་ ལག་ལེན་འཐབ་དགོཔ་ཨིན།
    - ཕྱིབ་དང་ཀླད་ཀོར་གྱི་གློག་འཕྲིན།
    - མཉམ་ལས་སྟེགས་བྱ།
    - བཟོ་བཀོད་གསང་བའི་ཡོངས་འབྲེལ་སྦྲེལ་མཐུད།
    - ཐག་རིང་གི་ཊེཀསི་ཊོཔ་ཞབས་ཏོག་ཚུ།
- མི་ཚེ་མཇུག་བསྡུ་བའི་ཅ་ཆས་ཚུ་ཚབ་བཙུགས།

རེའུ་མིག ༧: ཉེན་ཁ་སེལ་ཐབས་ཀྱི་བྱ་ཐབས་/ཐབས་ཤེས།

TTP	གལ་ཆེ་བའི་ཉེན་ཁ་སེལ་བའི་ཐབས་བྱས་བརྒྱད།	ISM ཚད་འཛིན་ཚུ།
འགོ་ཐོག་འཛུལ་སྤྱོད། T1190 མི་མང་ལུ་ཐད་ཀར་འབྲེལ་བའི་ཉེར་སྤྱོད་ཀྱི་གནོད་འཚེ་སྤྱོད་ལེན།	ཐབས་འཕྲུལ་བྱོག་རིམ་ཚུ། ཐབས་འཕྲུལ་བགོལ་སྤྱོད་རིམ་ལུགས་ཚུ། སྣ་མང་རྒྱུ་ཆུན་བདེན་དཔང་། གཉེར་སྤྱོད་ཚད་འཛིན།	ISM-0140 ISM-1698 ISM-1701 ISM-1921 ISM-1876 ISM-1877 ISM-1905
ལག་ལེན། T1059 བཏང་བགོད་དང་ཡིག་གཟུགས་སྒྲིག་སྒྲུབ་པ།	གཉེར་སྤྱོད་ཚད་འཛིན། མའི་ཀོ་རོ་སོཕ་ཀེ་ཡིག་ཚང་མེ་ཀོ་རོ་ཚུ་ཚད་འཛིན་འབད།། བདག་སྐྱོང་ཐོབ་དབང་ཚད་འཛིན་འབད་ནི།	ISM-0140 ISM-1490 ISM-1622 ISM-1623 ISM-1657 ISM-1890
ཞུ་ཚུགས། T1505.003 ཁར་བར་མཉེན་ཆས་ཆ་ཤས།: ཤེབ་ཤེལ།	གཉེར་སྤྱོད་ཚད་འཛིན། བདག་སྐྱོང་ཐོབ་དབང་ཚད་འཛིན་འབད་ནི།	ISM-0140 ISM-1246 ISM-1746 ISM-1249 ISM-1250 ISM-1490 ISM-1657 ISM-1871
འགོ་ཐོག་འཛུལ་སྤྱོད་ / ཐོབ་དབང་ཡར་འཕར་ / ཞུ་ཚུགས T1078 ནུས་ཅན་རྩིས་ཁྲ།	ཐབས་འཕྲུལ་བགོལ་སྤྱོད་རིམ་ལུགས་ཚུ། སྣ་མང་རྒྱུ་ཆུན་བདེན་དཔང་། བདག་སྐྱོང་ཐོབ་དབང་ཚད་འཛིན་འབད་ནི། གཉེར་སྤྱོད་ཚད་འཛིན། ལག་ལེན་པའི་སྒོག་རིམ་སྤ་བརྟན་བཟོ་ནི།	ISM-0140 ISM-0859 ISM-1546 ISM-1504 ISM-1679

སྤྱིར་བཏང་རྟགས་འཛིན་དང་སྤུང་སྐྱོབ་ཐབས་ཤེས་ཀྱི་གོོས་སྤྱོན་ཁ་སྐོང་གི་དོན་ལུ་ གོོས་སྤྱོན་འདི་གི་མཇུག་ཏུ་ཡོད་པའི་MITRE ATT&CK བཟུང་བསྡུས་ནང་ངོས་འཛིན་འབད་ཡོད་པའི་ཐབས་ལམ་རེ་རེའི་དོན་ལུ་MITRE ATT&CK ཐབས་ལམ་གྱི་ཡོངས་འབྲེལ་ཨོག་ལེབ་ནང་ཡོད་པའི་ སྤུང་སྐྱོབ་ཐབས་ཤེས་དང་རྟགས་འཛིན་ ཚ་ཤས་ཚུ་ཁྱོ་གནང་ཞུ།

བཀག་འགོག།

སྤྱན་ཞུ་འདི་ནང་ བརྡ་དོན་ཚུ་ བརྡ་དོན་གྱི་དོན་ལུ་རྒྱུངས་ཅིག་ “དེ་སྤེ་ཡོངས་ཚིན།” ཟེར་ ཁྱིན་དོ་ཡོངས་ཚིན། རྩོམ་སྤྱིག་ལས་སྤེ་ཚུ་ཤིས་ཡིག་ཚ་འདི་ནང་འབྲེལ་མཐུད་འབད་ཡོད་མི་ཚུ་ རྩིས་ཀྱ་ཚོང་འབྲེལ་གྱི་ཁྱིམ་སྤེ། ཐོག་སྐྱེད། ལས་ཁུངས་ཡང་ན་ཞབས་ཏོག་གང་རུང་ལུ་རྒྱབ་སྐྱོར་མི་འབད། དམིགས་བསལ་གྱི་ཚོང་འབྲེལ་གྱི་གནས་སྤེ་དང་། ཐོག་སྐྱེད། བྱ་རིམ། ཡང་ན་ཞབས་ཏོག་ཚུ་ལུ་ཞབས་ཏོག་མཚོན་རྟགས། ཚོང་འབྲེལ་མཚོན་རྟགས། བཟོ་བསྐྲུན་པ། ཡང་ན་གཞན་གྱི་ཐོག་ནས་ཐད་ཀར་གཞི་བཞག་པ་འདི་གིས་རྩོམ་བྱིས་འབད་མི་ལས་སྤེ་ཚུ་གི་ངོས་ལེན་དང་། གོོས་འཚར། ཡང་ན་རྒྱབ་སྐྱོར་གྱི་རྟགས་མཚན་མ་ཡིན་པ་མ་ཟད། དེ་ཤར་བསམ་པའི་རྒྱུ་མཚན་ཡང་མིན།

ཡིག་ཚ་འདི་ TLP:CLEAR རྟགས་བགོད་ཡོད། ཁ་གསལ་འབད་ནི་ལུ་ཚད་འཛིན་མེད། བརྡ་དོན་འདི་ཚུ་ མི་མང་ལུ་གསལ་བསྒྲགས་འབད་ནི་དེའི་ཤུལ་ལུ་ འབྲེལ་ཡོད་ལམ་ལུགས་དང་བྱ་རིམ་ཚུ་ཤང་འཁྲིལ་ཏེ་ གོག་སྤྱོད་འབད་ནི་གི་ཉེན་ཁ་ཉུང་སུ་ཅིག་དང་ ཡང་ན་ མངོན་གསལ་མེད་པ་སྤེ་ཡོད་པའི་སྐབས་ འབྱུང་ཁྲལ་ཚུ་གིས་ TLP:CLEAR ལག་ལེན་འཐབ་བཏུབ། ཚད་ལྡན་པར་དབང་ལམ་ལུགས་དང་འཁྲིལ་ཏེ་ TLP:CLEAR བརྡ་དོན་འདི་བཀག་ཆ་མེད་པར་བཏུམ་ཤེལ་བཏང་བཏུབ། འབྲིམ་འགྱལ་སྤོག་སྤྱོན་ཚུ་གོོས་མཐུན་སྐོར་གྱི་གནས་ཚུལ་ཁ་གསལ་གྱི་དོན་ལུ་ cisa.gov/tlp ལུ་གཟིགས།

MITRE ATT&CK – གལ་ཆེ་བའི་ལོ་རྒྱུས་ཀྱི་ APT40 ཚོང་ལས་ལག་རྟལ།

བརྒྱ་ཁིབ་ (TA0043)

ཉམས་རྒྱད་པའི་བདག་དབང་ཡོད་པའི་ཡོངས་འཛེལ་འཚར་སྒོ་འཚོལ་ཁིབ་འབད། (T1594)	ཉམས་རྒྱད་པའི་ངོ་རྟགས་བརྟ་དོན་བསྡུ་ལེན་འབད། ངོས་འཛིན་ཡིག་ཚ། (T1589.001)
ཤུགས་ལྡན་པར་བཟློས་འབད་ནི། ཉེན་ཁ་ཅན་ཀྱི་པར་བཟློས། (T1595.002)	ཉམས་རྒྱད་པ་གཙོ་བོ་གི་བརྟ་དོན་བསྡུ་ལེན་འབད། (T1592)
ཁ་ཕྱེ་ཡོངས་འཛེལ་དྲྭ་མེན་འཚོལ་ཁིབ: འཚོལ་ཁིབ་འཕྲུལ་ཆས། (T1593.002)	ཉམས་རྒྱད་པའི་ཡོངས་འཛེལ་བརྟ་དོན་བསྡུ་ལེན་འབད། དྲྭ་མེན་རྒྱུ་དངོས་ (T1590.001)
ཉམས་རྒྱད་པའི་ངོ་རྟགས་བརྟ་དོན་བསྡུ་ལེན་འབད། སྒོག་འཕྲིན་ཁ་བྱང་། (T1589.002)	

ཐོན་སྐྱངས་གོང་འཕེལ། (TA0042)

གཞི་རྟེན་མཐུན་རྐྱེན་ཚུ་ལེན་ནི། དྲྭ་མེན་ཚུ་ (T1583.001)	གཞི་རྟེན་མཐུན་རྐྱེན་ལེན་ནི། (T1583)
གཞི་རྟེན་མཐུན་རྐྱེན་ཚུ་ལེན་ནི། DNS སར་བར། (T1583.002)	བདེ་སྒྲིག་རྩིས་ཁྲ་ཚུ། (T1586)
སྐྱོགས་གྲུབ་གོང་འཕེལ་གཏང་ནི། གསང་གྲངས་མིང་རྟགས་བགོད་པའི་ལག་ལྟེ། (T1587.002)	གཞི་རྟེན་འཕྲུལ་རིག་ལུ་གཞོད་སྐྱོན་བཏང་ནི། (T1584)
སྐྱོགས་གྲུབ་གོང་འཕེལ་གཏང་ནི། ཡོངས་འཛེལ་ལག་ལྟེར། (T1587.003)	སྐྱོགས་གྲུབ་གོང་འཕེལ་གཏང་ནི། མཉེན་ཆས་ངན་པ། (T1587.001)
སྐྱོགས་གྲུབ་ལེན་ནི། གསང་གྲངས་མིང་རྟགས་བགོད་པའི་ལག་ལྟེ། (T1588.003)	རྩིས་ཁྲ་གཞི་བཙུགས། སྤྱིན་པའི་རྩིས་ཁྲ་ (T1585.003)
གཞི་རྟེན་འཕྲུལ་རིག་ལུ་གཞོད་སྐྱོན་བཏང་ནི། ཡོངས་འཛེལ་འཕྲུལ་ཆས་ཚུ་ (T1584.008)	སྐྱོགས་གྲུབ་ལེན་ནི། ཡོངས་འཛེལ་ལག་ལྟེར། (T1588.004)

འགོ་ཐོག་འཛུལ་སྤྱོད། (TA0001)

ནུས་ཅན་རྩིས་ཁྲ། (T1078)	ཡི་ཤིང་ (T1566)
ནུས་ཅན་རྩིས་ཁྲ། སྡོད་སྒྲིག་རྩིས་ཐོ་ཚུ། (T1078.001)	ཡི་ཤིང་: ཨིས་པེར་ཡི་ཤིང་མཉམ་སྒྲིག། (T1566.001)
ནུས་ཅན་རྩིས་ཁྲ། དྲྭ་མེན་རྩིས་ཁྲ། (T1078.002)	ཡི་ཤིང་: ཨིས་པེར་ཡི་ཤིང་འཛེལ་མཐུད་ (T1566.002)
ཕྱི་ཡི་ཐག་རིང་ཞབས་ཏོག། (T1133)	མི་མང་ལུ་གདོང་ལན་འབད་མི་ སྒོག་རིམ་ (T1190) ལག་ལེན་འཐབ།
བཏང་བའི་བདེ་སྒྲིག། (T1189)	

ལག་ལེན། (TA0002)

ཕྱིན་ཅིས་འཛིན་སྐྱོང་ལག་ཆས། (T1047)	བརྡ་བཀོད་དང་ཡིག་གཟུགས་སྐད་སྒྱུར་པ་: པའི་ཐོན་ (T1059.006)
དུས་ཚོད་བཀོད་ཡོད་པའི་ལས་ཀ/ལྟ: At (T1053.002)	བརྡ་བཀོད་དང་ཡིག་གཟུགས་སྐད་སྒྱུར་པ་: ཇ་བ་ཚིས་ཀིར་པཊི་ (T1059.007)
དུས་ཚོད་བཀོད་ཡོད་པའི་ལས་ཀ/ལྟ: དུས་ཚོད་བཀོད་ཡོད་པའི་ལས་ཀ། (T1053.005)	རང་བཞིན་API (T1106)
བརྡ་བཀོད་དང་ཡིག་གཟུགས་སྐད་སྒྱུར། (T1059)	བྱ་རིམ་བར་ཐྲི་བརྡ་སྤྲོད། (T1559)
བརྡ་བཀོད་དང་ཡིག་གཟུགས་སྐད་སྒྱུར་པ་: ཕྱིན་ཅིས་བརྡ་བཀོད་ཤེལ། (T1059.003)	རིམ་ལུགས་ཞབས་ཏོག: ཞབས་ཏོག་ལག་ལེན། (T1569.002)
བརྡ་བཀོད་དང་ཡིག་གཟུགས་སྐད་སྒྱུར་པ་: པྱ་ཐར་ཤེལ། (T1059.001)	མགོ་སྤྲོད་འབད་མི་ལག་ལེན་འཐབ་ཏིའི་དོན་ལུ་ བཀོལ་སྤྱོད། (T1203)
བརྡ་བཀོད་དང་ཡིག་གཟུགས་སྐད་སྒྱུར་པ་: གཞི་རྟེན་མཐོང་སྒང་། (T1059.005)	ལག་ལེན་པའི་ལག་བསྟུན: གཏོད་པ་ཅན་ཐྲི་ཡིག་སྤྲོད། (T1204.002)
བརྡ་བཀོད་དང་ཡིག་གཟུགས་སྐད་སྒྱུར་པ་: ཡུ་ནི་གཱི་ཤེལ། (T1059.004)	བརྡ་བཀོད་དང་ཡིག་གཟུགས་སྐད་སྒྱུར་པ་: ཚེ་པུལ་ཡིག་གཟུགས། (T1059.002)
དུས་ཚོད་བཀོད་ཡོད་པའི་ལས་ཀ/ལྟ: Cron (T1053.003)	མཉེན་ཆས་བཀྲམ་སྒེལ་ཐྲི་ལག་ཆས། (T1072)

ཡུ་ཚུགས། (TA0003)

ནུས་ཅན་རྩིས་ཁྲ། (T1078)	ས་བར་མཉེན་ཆས་ཆ་ཤས: ཤེབ་ཤེལ། (T1505.003)
ཨོ་ཡིས་གཉེར་སྤྱོད་འགོ་བཙུགས། ཨོ་ཡིས་ལྕེམ་ཝེལ་ཀེག་རོས་ (T1137.001)	རིམ་ལུགས་བྱ་རིམ་གསར་བསྒྲུན་ཡང་ན་ལེགས་བཅོས་འབད། ཕྱིན་ཅིས་ཞབས་ཏོག (T1543.003)
དུས་ཚོད་བཀོད་ཡོད་པའི་ལས་ཀ/ལྟ: At (T1053.002)	མགོ་འཛུགས་སམ་ཞུགས་རིམ་རང་བཞིན་མགོ་བརྩམས་ལག་བསྟར། ཐོ་བཀོད་གཡོག་བཀོལ་ལྟེ་མིག་ཚུ་ / འགོ་བཙུགས་སྤྲོད་འཛིན། (T1547.001)
དུས་ཚོད་བཀོད་ཡོད་པའི་ལས་ཀ/ལྟ: དུས་ཚོད་བཀོད་ཡོད་པའི་ལས་ཀ། (T1053.005)	མགོ་འཛུགས་སམ་ཞུགས་རིམ་རང་བཞིན་མགོ་བརྩམས་ལག་བསྟར། མཉོགས་ཐབས་བསྒྱུར་བཅོས། (T1547.009)
ཕྱིའི་ཐག་རིང་ཞུགས་ཀྱི། (T1133)	Hijack ལག་ལེན་འཐབ་ཐངས་རྒྱུན་རིམ། DLL འཚོལ་ཞིབ་བཀའ་རྒྱ་བཅན་འཕྲོ། (T1574.001)
དུས་ཚོད་བཀོད་ཡོད་པའི་ལས་ཀ/ལྟ: Cron (T1053.003)	Hijack ལག་ལེན་འཐབ་ཐངས་རྒྱུན་རིམ། DLLཕྱོགས་མངོན་གསལ་འབད་དོ། (T1574.002)
རྩིས་ཁྲ་གཡོ་སྒྱུ། (T1098)	ནུས་ཅན་རྩིས་ཁྲ། སྤྱིན་པའི་རྩིས་ཁྲ་ (T1078.004)
ནུས་ཅན་རྩིས་ཁྲ། དྲྭ་མེན་རྩིས་ཁྲ། (T1078.002)	

ཐོན་དབང་ཡར་འཕར། (TA0004)

དུས་ཚོད་བཀོད་ཡོད་པའི་ལས་ཀ/ལྟ: At (T1053.002)	རིམ་ལུགས་བྱ་རིམ་གསར་བསྒྲུན་ཡང་ན་ལེགས་བཅོས་འབད། ཕྱིན་ཅིས་ཞབས་ཏོག (T1543.003)
དུས་ཚོད་བཀོད་ཡོད་པའི་ལས་ཀ/ལྟ: དུས་ཚོད་བཀོད་ཡོད་པའི་ལས་ཀ། (T1053.005)	མགོ་འཛུགས་སམ་ཞུགས་རིམ་རང་བཞིན་མགོ་བརྩམས་ལག་བསྟར། ཐོ་བཀོད་གཡོག་བཀོལ་ལྟེ་མིག་ཚུ་ / འགོ་བཙུགས་སྤྲོད་འཛིན། (T1547.001)
བྱ་རིམ་བཙུགས་: ཐགས་པ་ལག་ལེན་འཐབ་ཐོག་བཙན་འཕྲོག་འབད་ནི་ (T1055.003)	མགོ་འཛུགས་སམ་ཞུགས་རིམ་རང་བཞིན་མགོ་བརྩམས་ལག་བསྟར། མཉོགས་ཐབས་བསྒྱུར་བཅོས། (T1547.009)
བྱ་རིམ་བཙུགས་: བྱ་རིམ་ཁོག་སྟོང་། (T1055.012)	Hijack ལག་ལེན་འཐབ་ཐངས་རྒྱུན་རིམ། DLL འཚོལ་ཞིབ་བཀའ་རྒྱ་བཅན་འཕྲོ། (T1574.001)

ཐོབ་དབང་ཡར་འཕར། (TA0004)

ནུས་ཅན་རྩིས་ཁྲི: དྲྭ་ཐེག་རྩིས་ཁྲི (T1078.002)	ཐོབ་དབང་ཡར་སེང་གི་དོན་ལུ་ བཀོལ་སྤྱོད། (T1068)
འཛུལ་སྤྱོད་བརྒྱ་མཚོན་གཡོ་སྒྲུ: དོ་ཀེན་རྫུས་མ་/ཙར་ཁ་ཀྱ་བ། (T1134.001)	བྱུང་ལས་འགོ་བཙུགས་པའི་ལག་ལེན། ཡུ་ནི་གཞི་ཤེལ་རིམ་སྒྲིག་ལེགས་བཅོས། (T1546.004)
བྱ་རིམ་བཙུགས་: Dynamic-link དཔེ་མཛོད་བཙུགས། (T1055.001)	ནུས་ཅན་རྩིས་ཁྲི: དྲྭ་ཐེག་རྩིས་ཁྲི (T1078.002)
ནུས་ཅན་རྩིས་ཁྲི: ས་གནས་རྩིས་ཁྲི (T1078.003)	

བཀག་སྡོམ་གཡོལ་ཐབས། (TA0005)

Rootkit (T1014)	ཐད་ཀར་མིན་པའི་བརྒྱབ་ཀོད་ལག་བསྟུན། (T1202)
མགུ་ཐོམ་སི་སི་གི་ཡིག་སྒྲོད་ཡང་ན་བརྡ་དོན། (T1027)	རིམ་ཡུགས་གཞིས་ལྡན་དོ་ཚབ་ལག་ལེན་འཐབ་ནི: Mshta (T1218.005)
མགུ་ཐོམ་སི་སི་གི་ཡིག་སྒྲོད་ཡང་ན་བརྡ་དོན། མཉེན་ཆས་ཐུམ་སྒྲིལ། (T1027.002)	རིམ་ཡུགས་གཞིས་ལྡན་དོ་ཚབ་ལག་ལེན་འཐབ་ནི: Regsvr32 (T1218.010)
མགུ་ཐོམ་སི་སི་གི་ཡིག་སྒྲོད་ཡང་ན་བརྡ་དོན། སྒེད་ཡིག་རིག་པ། (T1027.003)	བློ་གཏད་ཚད་འཛིན་ཆུ་ མར་ཕབ་འབད། གསང་གྲངས་འཛུལ་སྤྱོད། (T1553.002)
མགུ་ཐོམ་སི་སི་གི་ཡིག་སྒྲོད་ཡང་ན་བརྡ་དོན། བཀྲམ་སྤེལ་འབད་བའི་ཤུལ་ལས་ བསྟུ་སྒྲིག་འབད། (T1027.004)	ཡིག་སྒྲོད་དང་སྒྲོད་ཐོའི་གནང་བ་བསྒྲུར་བཅོས་ཆུ། ཚི་ནག་སི་དང་མེཀ་ཡིག་སྒྲོད་དང་སྒྲོད་ཐོ་གནང་བ་བསྒྲུར་བཅོས། (T1222.002)
གཡོ་སྒྲུ: ཁྲིམས་མཐུན་མིང་ཡང་ན་ས་གནས་མཐུན་སྒྲིག་འབད། (T1036.005)	བར་ཆུའལ་བཙོ་ནི་/སེནཊ་བོགས་ སྤོ་ནི། རིམ་ཡུགས་ཞིབ་དཔྱད། (T1497.001)
བྱ་རིམ་བཙུགས་: ཐགས་པ་ལག་ལེན་འཐབ་ཐོག་བཙན་འཕྲོག་འབད་ནི་ (T1055.003)	གཡོ་སྒྲུ (T1036)
བསམ་ཞིབ་ཚང་རྟགས་མངོན་གསལ་འབད་ནི། (T1620)	ཉེན་སྐྱང་ཡུ་གནོད་སྐྱེན་བརྒྱབ་ནི། རིམ་ཡུགས་ཁ་ཡར་ཁོལ་མ་བཏུབ་བཙོ་ནི་ཡང་ན་ལེགས་བཅོས་འབད་ནི། (T1562.004)
བྱ་རིམ་བཙུགས་: བྱ་རིམ་ཁོག་སྡོང་། (T1055.012)	ཅ་རྟེང་ཚུ་སྦྱ་བཞག: སྦྱ་ཡོད་པའི་ཡིག་སྒྲོད་དང་སྒྲོད་ཐོ་ཚུ། (T1564.001)
བརྡ་སྡོན་བཏོན་གཏང་ནི། ཡིག་སྒྲོད་བཏོན་གཏང་ནི། (T1070.004)	ཅ་རྟེང་ཚུ་སྦྱ་བཞག: སྦྱ་ཡོད་པའི་ཤེན་ཀོས། (T1564.003)
བརྡ་སྡོན་བཏོན་གཏང་ནི། དུས་ཚོད་མཐའ་གཅིག (T1070.006)	Hijack ལག་ལེན་འཐབ་ཐངས་རྒྱུན་རིམ། DLL འཚོལ་ཞིབ་བཀའ་རྒྱ་བཅན་འཛོག (T1574.001)
བརྡ་སྡོན་བཏོན་གཏང་ནི། ཤེན་ཀོས་བྱང་ལས་དུན་ཐོ་ཚུ་བསལ་ (T1070.001)	Hijack ལག་ལེན་འཐབ་ཐངས་རྒྱུན་རིམ། DLLཕྱོགས་མཚོན་གསལ་འབད་དོ། (T1574.002)
ཐོ་བཀོད་ལེགས་བཅོས་འབད། (T1112)	ཤེབ་ཞབས་ཀྱོག (T1102)
ཀྱི་ཚོབ་ཕུས་ཀྱི་/ཀྱི་ཀོཀྱི་ཡིག་སྒྲོད་ཆུ་ཡང་ན་བརྡ་དོན་ (T1140)	གཡོ་སྒྲུ: གཡོ་སྒྲུ་རྒྱབ་པའི་ལས་འགན་ཡང་ན་ཞབས་ཀྱོག (T1036.004)
ཉམས་རྒྱུད་འགོག་སྲུང་། (T1562)	

དོས་ལེན་ཡིག་ཆ་འཛུལ་སྤྱོད། (TA0006)

OS དོ་རྟགས་བཏོན་གཏང་ནི། LSASS དྲན་གསོག (T1003.001)	ཉེན་སྐྱང་ཝེད་པའི་དོ་རྟགས་ཚུ། ཡིག་སྒྲོད་ཆུ་ནང་ འཛུལ་སྤྱོད་དོ་རྟགས། (T1552.001)
OS དོ་རྟགས་བཏོན་གཏང་ནི། NTDS (T1003.003)	བྱུའ་ཡོངས་: གསང་ཡིག་ཚོད་དཔག་འབད། (T1110.001)
ཡོངས་འཛིལ་ཚོར་བ། (T1040)	བཙན་ཤེད་ཀྱི་བདེན་བཤད། (T1187)

དོས་ལེན་ཡིག་ཆ་འཛུལ་སྤྱོད། (TA0006)

གསང་ཡིག་གསོག་ཁང་ཚུ་ནང་གི་དོ་རྒྱས་ཚུ། ཀེའི་ཅེན། (T1555.001)	ཨར་ཁ་བཀུ་ནི་ཡང་ན་Kerberos གི་ཨོག་འཛིན་ རྩུས་མ་བཟོ་ནི་: Kerberoasting (T1558.003)
ནང་འཇུག་འཛིན་བཟུང་། ཕྲེ་མིག་ནང་བསྒྲིད་ (T1056.001)	སྣ་མང་རྒྱུ་རྐྱེན་བདེན་བཤད་བར་ཆད། (T1111)
ཁེབ་ལྟ་ཡུན་ཀུ་ཀི་ཨར་ཁ་བཀུ། (T1539)	ལག་ལེན་འཇུལ་སྤྱོད་བརྟག་ཨར་ཁ་བཀུ་བ། (T1528)
དོས་ལེན་ཡིག་ཆ་འཛུལ་སྤྱོད་ཀྱི་དོན་ལུ་ བཀོལ་སྤྱོད། (T1212)	བྱུང་ཚོར་སི་: གསང་ཡིག་བརྡབ་གསིག་ (T1110.002)
ནང་འཇུག་འཛིན་བཟུང་། ཁེབ་དྲྭ་ཚིགས་འཛིན་བཟུང་། (T1056.003)	OS དོ་རྒྱས་བཏོན་གཏང་ནི། DCSync (T1003.006)
གསང་ཡིག་གསོག་ཁང་ཚུ་ནང་གི་དོ་རྒྱས་ཚུ། (T1555)	གསང་ཡིག་གསོག་ཁང་ཚུ་ནང་གི་དོ་རྒྱས་ཚུ། ཁེབ་བར་འུ་ཟར་ཚུ་ལས་ དོ་རྒྱས་ཚུ། (T1555.003)

གསར་རྩེད། (TA0007)

རིམ་ལུགས་ཞབས་ཏོག་འཚོལ་ཞིབ། (T1007)	རིམ་ལུགས་བརྟ་དོན་འཚོལ་ཞི། (T1082)
ལག་ལེན་སྒོ་སྒྲིག་འཚོལ་ཞིབ། (T1010)	རྩིས་ཁྲ་གསར་རྩེད། ས་གནས་ཀྱི་རྩིས་ཁྲ། (T1087.001)
འབྲི་དཔྱད་ཐོ་བཀོད། (T1012)	ལམ་ལུགས་བརྟ་དོན་འཚོལ་ཞིབ། ཐབས་ཤེས། T1082 - Enterprise | MITRE ATT&CK®
ཡིག་སྒོང་དང་སྒོང་ཐོ་འཚོལ་ཞིབ། (T1083)	རིམ་ལུགས་དུས་ཚོད་འཚོལ་ཞིབ། (T1124)
ཡོངས་འབྲེལ་ཞབས་ཏོག་འཚོལ་ཞིབ། (T1046)	རིམ་ལུགས་ཇོ་བདག་/ལག་ལེན་པ་གསར་རྩེད། (T1033)
ཐག་རིང་རིམ་ལུགས་འཚོལ་ཞིབ། (T1018)	དྲ་ཤེན་བྱོ་གཏད་འཚོལ་ཞིབ། (T1482)
རྩིས་ཁྲ་གསར་རྩེད། སྒོག་འཛིན་རྩིས་ཁྲ། (T1087.003)	རྩིས་ཁྲ་གསར་རྩེད། དྲ་ཤེན་རྩིས་ཐོ། (T1087.002)
རིམ་ལུགས་ཡོངས་འབྲེལ་མཐུད་ལམ་འཚོལ་ཞིབ། (T1049)	བར་ཆུའལ་བཟོ་ནི་/ཤེནྟ་བོགས་ སྒོ་ནི། རིམ་ལུགས་ཞིབ་དཔྱད། (T1497.001)
བྱ་རིམ་གསར་རྩེད། (T1057)	མཉེན་ཆས་འཚོལ་ཞིབ། (T1518)
གནང་བའི་སྤེ་ཚན་འཚོལ་ཞིབ་: དྲ་ཤེན་སྤེ་ཚན་ཚུ། (T1069.002)	ཡོངས་འབྲེལ་བགོ་བཤའ་འཚོལ་ཞིབ་, ཐབས་ཤེས་ T1135 - Enterprise | MITRE ATT&CK®
རིམ་ལུགས་ཡོངས་འབྲེལ་རིམ་སྒྲིག་གསར་རྩེད། ཡོངས་འབྲེལ་མཐུད་ལམ་འཚོལ་ཞི། (T1016.001)	

ཕྱོགས་གཅིག་གི་གཡོ་འགུལ་ (TA0008)

ཐག་རིང་ཞབས་ཏོག་ཚུ། ཐག་རིང་ཉེགས་ཏོལ་མཐུན་འབྲེལ། (T1021.001)	ཐག་རིང་ཞབས་ཏོག། (T1021)
ཐག་རིང་ཞབས་ཏོག་ཚུ། SMB/ཞིན་ཇོས་བདག་སྐྱོང་བགོ་བཤའ། (T1021.002)	བདེན་བཤད་རྩུ་ཆ་གཞན་ལག་ལེན་འཐབ། ཨོག་འཛིན་སྒོག (T1550.003)
ཐག་རིང་ཞབས་ཏོག་ཚུ། ཞིན་ཇོས་ཐག་རིང་འཛིན་སྐྱོང་། (T1021.006)	ཕྱོགས་ལག་ཆས་སྒོ་བཤྱོག (T1570)

བསྡུ་སྒྲིག (TA0009)

ས་གནས་རིམ་ལུགས་ལས་ གནད་སྡུག (T1005)	ཡིག་མཛོད་བསྡུ་ལེན་འབད་ཡོད་པའི་གནས་སྡུག་: དཔེ་མཛོད་བརྒྱུད་དེ་གཏན་མཛོད། (T1560.002)
ཡོངས་འབྲེལ་རྒྱབ་སྐྱོང་འདེན་འཕྲུལ་ལས་ གནད་སྡུག (T1039)	སྒོག་འཛིན་བསྡུ་སྒྲིག་ ཐག་རིང་སྒོག་འཛིན་བསྡུ་སྒྲིག (T1114.002)

བསྡུ་ཐུའི་གཅ (TA0009)

ནང་འཇུག་འཛིན་བཟུང་། ཤེ་མིག་ནང་བསྐྱོད་ (T1056.001)	བཏུད་ཕ་གནད་སྡུག (T1115)
རང་འགྱལ་བསྡུ་སྒྲིག (T1119)	བཙུ་དོན་མཛོད་ཁང་ཚུ་ལས་ གནད་སྡུག (T1213)
ནང་འཇུག་འཛིན་བཟུང་། ཤེབ་དུ་ཆོགས་འཛིན་བཟུང་། (T1056.003)	གནད་སྡུད་གནས་རིམ། ཐག་རིང་གནས་སྡུད་གནས་རིམ། (T1074.002)
གནད་སྡུད་གནས་རིམ། ས་གནས་ཀྱི་གནས་སྡུད་གནས་རིམ། (T1074.001)	ཡིག་མཛོད་བསྡུ་སྒྲིག་འབད་ཡོད་པའི་གནས་སྡུག (T1560)
སྒོག་འཛིན་བསྡུ་སྒྲིག (T1114)	

ཕྱིར་འཐེན། (TA0010)

C2 རྒྱུན་ལམ་ཐོག་ལས་ ཕྱིར་འཐེན་འབད་ནི། (T1041)	གདམ་ཁ་ཅན་ཀྱི་མཐུན་སྒོས་ཀུ་ལས་ ཕྱིར་འཐོན་འབད་ནི། མ་འདྲ་བའི་གསང་བཟོ་འབད་ཡོད་པའི་ C2 མེན་པའི་མཐུན་སྒོས་ (T1048.002) ཀུ་ལས་ ཕྱིར་འཐོན་འབད་ནི།
གདམ་ཁ་ཅན་ཀྱི་མཐུན་སྒོས་ཐོག་ལས་ ཕྱིར་འཐེན་འབད་ནི། (T1048)	ཤེབ་ཞབས་ཀྱག་ཐོག་ལས་ ཕྱི་ཁར་ཐོན་ནི། ཕྱིན་གསོག་འཇོག་ལ་ཡུ་ཕྱིར་འཐེན་འབད་ནི། (T1567.002)

བཀའ་རྒྱ་དང་ཚད་འཛིན། (TA0011)

གནད་སྡུད་མཐུ་ཐོམ་སི་སི། མཐུན་སྒྲིག རྟུས་བཟོ། (T1001.003)	ཡོངས་འབྲེལ་ཞབས་ཀྱག་ ཤི་བའི་བརྡབ་གསིག་སེལ་བྱེད། (T1102.001)
ཕྱིར་བཏང་ལག་ལེན་འཐབ་མི་འདྲེན་ལམ། (T1043)	ཡོངས་འབྲེལ་ཞབས་ཀྱག་ ཕྱོགས་གཅིག་བརྒྱུད་འབྲེལ། (T1102.003)
སྒོག་རིམ་བང་རིམ་མཐུན་སྒྲིག་ ཤེབ་མཐུན་འབྲེལ་ཚུ། (T1071.001)	ནང་འཇུལ་ལག་ཆས་སྒོ་བཏུད། (T1105)
སྒོག་རིམ་བང་རིམ་མཐུན་སྒྲིག་ ཡིག་སྡོད་སྒོ་བཏུད་མཐུན་འབྲེལ་ཚུ། (T1071.002)	ངོ་ཚབ་: ནང་འགོད་ངོ་ཚབ། (T1090.001)
ངོ་ཚབ་: ཕྱིའི་ངོ་ཚབ། (T1090.002)	ཚད་ལྡན་མིན་པའི་འབྲེལ་ལམ། (T1571)
ངོ་ཚབ་: སྐ་མང་ཉོར་ངོ་ཚབ་ (T1090.003)	མཐུན་སྒོས་ཕྱག་ལམ། (T1572)
ཡོངས་འབྲེལ་ཞབས་ཀྱག་ ཕྱོགས་གཅིས་ཀྱི་བརྡ་སྤྲོད། (T1102.002)	གསང་བཟོ་འབད་ཡོད་པའི་རྒྱུ་ལམ། (T1573)
གསང་བཟོ་འབད་ཡོད་པའི་རྒྱུ་ལམ། འབྲ་མཉམ་མེད་པའི་གསང་ཡིག་རིག་པ། (T1573.002)	ནང་འཇུལ་ལག་ཆས་སྒོ་བཏུད། (T1105)
ངོ་ཚབ་ ཐབས་ཤེས་ T1090 - Enterprise | MITRE ATT&CK®	

ཤུགས་རྒྱེན། (TA0040)

ཞབས་ཀྱག་བཀག་ཆ། (T1489)	ཉེཀསི་བསྒྲལ། (T1561)
རིམ་ཡུགས་སྒོ་བསྡམ/ལོག་འགོ་བསྒྱགས། (T1529)	ཐོན་ཁྲངས་བཙན་འཕྲོག། (T1496)

དྲན་ཐོ།

བཀག་འགོག།

ལམ་སྟོན་འདི་ནང་ལུ་ཡོད་པའི་རྒྱུ་ཆ་ཚུ་ སྤྱིར་བཏང་གི་རང་བཞིན་ཅིག་ཚིགས་ལས་ ཁྲིམས་དོན་གྱི་སྒོས་སྟོན་སྟེ་ བཅོ་དགོཔ་མ་ཚད་ དཔེགས་བསལ་གྱི་གནས་སྟངས་ ཡང་ན་ སྤྱི་བྱར་གྱི་གནས་སྟངས་ནང་ སྒོགས་རམ་གྱི་དོན་ལུ་ བློ་གཏད་མེ་བཏུབ། ཁག་ཆེ་བའི་གནད་དོན་གང་རུང་ཅིག་ནང་ ལྟོད་རའི་གནས་སྟངས་ དང་འབྲེལ་བའི་ ཉོས་འཐབ་ཅན་གྱི་ རང་དབང་ཅན་གྱི་མཁས་རིགས་བསྒྲབ་བྱ་ཚུ་ འཚོལ་དགོ།

ལམ་སྟོན་འདི་ནང་ བརྟོན་ཚུལ་བརྟེན་ཏེ་ གནོན་སྐྱོན་དང་ སྤྱོང་རྒྱུ་ དེ་ལས་ ཟད་འགྲོ་ཚུ་ འབྱུང་མི་ལུ་ རྒྱུ་མཐུན་གཞུང་གིས་ འགན་ལྷང་དང་ འགན་འཁྱི་གཏི་ཡང་ ངོས་ལེན་མི་འབད།

པར་དབང་།

© ཨོསི་ཊེ་ལི་ཡའི་སྤྱི་མཐུན་རྒྱལ་ཁབ་ 2024

མཚོན་རྟགས་དང་ དེ་མེན་པ་ཅིན་ དཔེ་སྐུན་འདི་ནང་ གསལ་བཀོད་འབད་མི་ ཡིག་ཆ་ཚ་མཉམ་ Creative Commons Attribution 4.0 International license | creativecommons.org གསར་གཏོད་ཀྱི་སྤྱིར་བཏང་དྲ་ཚིགས།

དོགས་པ་བཀག་ཐབས་ལུ་ འདི་གིས་ ཆོག་ཐམ་འདི་ ཡིག་ཆ་འདི་ནང་ བཀོད་དེ་ཡོད་མི་བཀོད་སྤྲིག་ཚུ་རྒྱངས་ཅིག་ལུ་ འཛུག་སྤྱོད་འབདཝ་ཨིན།

འབྲེལ་ཡོད་ཆོག་མཆན་གྱི་གནས་སྟངས་ཀྱི་ཞིབ་ཚགས་ཚུ་ Creative Commons ཡོངས་འབྲེལ་ནང་ལུ་ཡོད་དོ། དེ་བཞིན་དུ་ CC BY 4.0 ཆོག་མཆན་གྱི་ཁྲིམས་ཀྱི་ཚད་རྟགས་ཡང་ཡོད། | creativecommons.org.

རྒྱལ་རྟགས་ལག་ལེན།

རྒྱལ་རྟགས་འདི་ ལག་ལེན་འཐབ་ཆོག་པའི་ ཐ་སྙད་ཚུ་ བློན་ཆེན་ལས་ཁུངས་དང་ ལྷན་རྒྱས་གཞུང་ཆོགས་ཀྱི་ ཡོངས་འབྲེལ་འཚར་སྐྱོ་ནང་ ཁ་གསལ་སྟེ་ བཀོད་དེ་ཡོདཔ་ཨིན། དབྱིན་ཇིའི་རྒྱལ་རྟགས་བརྟན་འཕེན་དང་ལམ་སྟོན། | pmc.gov.au.

བརྟན་དོན་ཁ་གསལ་གྱི་དོན་ལུ་ ཡང་ན་ ཡོངས་འབྲེལ་ཉེན་སྐྱོང་གི་ བྱུང་རྐྱེན་ཅིག་ སྐན་ཞུ་འབད་ནིའི་དོན་ལུ་ ང་བཅས་དང་གཅིག་ཁར་འབྲེལ་བ་འཐབ།

cyber.gov.au | 1300 CYBER1 (1300 292 371)

འདི་ཨང་ཨས་ལ་ལུས་ཀྱི་ནང་ཡང་བརྒྱུད་སྤྱོད་ལུ་ཡོད་རེད།

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre