Obtain Capabilities: Tool, Sub-technique T1588.002 - Enterprise

Archived: 2026-04-05 15:27:39 UTC

G1007 Aoqin Dragon

Aoqin Dragon obtained the Heyoka open source exfiltration tool and subsequently modified it for their operations.[4]

G0099 APT-C-36

APT-C-36 obtained and used a modified variant of Imminent Monitor.[5]

G0006 APT1

APT1 has used various open-source tools for privilege escalation purposes.[6]

G0073 APT19

APT19 has obtained and used publicly-available tools like Empire.[7][8]

G0007 APT28

APT28 has obtained and used open-source tools like Koadic, Mimikatz, and Responder.[9][10][11]

G0016 APT29

APT29 has obtained and used a variety of tools including Mimikatz, SDelete, Tor, meek, and Cobalt Strike.[12][13][14]

G0050 APT32

APT32 has obtained and used tools such as Mimikatz and Cobalt Strike, and a variety of other open-source tools from GitHub.[15][16]

G0064 APT33

APT33 has obtained and leveraged publicly-available tools for early intrusion activities.[17][18]

G0082 APT38

APT38 has obtained and used open-source tools such as Mimikatz.[19]

G0087 APT39

APT39 has modified and used customized versions of publicly-available tools like PLINK and Mimikatz.[20][21]

G0096 APT41

APT41 has obtained and used tools such as Mimikatz, pwdump, PowerSploit, and Windows Credential Editor.[22]

G1044 APT42

APT42 has used built-in features in the Microsoft 365 environment and publicly available tools to avoid detection.[23]

G0143 Aquatic Panda

Aquatic Panda has acquired and used Cobalt Strike in its operations.[24]

G0135 BackdoorDiplomacy

BackdoorDiplomacy has obtained a variety of open-source reconnaissance and red team tools for discovery and lateral movement.[25]

G1002 BITTER

BITTER has obtained tools such as PuTTY for use in their operations.[26]

G0098 BlackTech

BlackTech has obtained and used tools such as Putty, SNScan, and PsExec for its operations.[27]

G0108 Blue Mockingbird

Blue Mockingbird has obtained and used tools such as Mimikatz.[28]

G0060 BRONZE BUTLER

BRONZE BUTLER has obtained and used open-source tools such as Mimikatz, gsecdump, and Windows Credential Editor.[29]

C0010 C0010

For C0010, UNC3890 actors obtained multiple publicly-available tools, including METASPLOIT, UNICORN, and NorthStar C2.[30]

C0015 C0015

For C0015, the threat actors obtained a variety of tools, including AdFind, AnyDesk, and Process Hacker.[31]

C0017 C0017

For C0017, APT41 obtained publicly available tools such as YSoSerial.NET, ConfuserEx, and BadPotato.[32]

C0018 C0018

For C0018, the threat actors acquired a variety of open source tools, including Mimikatz, Sliver, SoftPerfect Network Scanner, AnyDesk, and PDQ Deploy.[33][34]

C0021 C0021

For C0021, the threat actors used Cobalt Strike configured with a modified variation of the publicly available Pandora Malleable C2 Profile.[35][36]

C0027 C0027

During C0027, Scattered Spider obtained and used multiple tools including the LINpeas privilege escalation utility, aws_consoler, rsocx reverse proxy, Level RMM tool, and RustScan port scanner.[37]

C0032 C0032

During the C0032 campaign, TEMP.Veles obtained and used tools such as Mimikatz and PsExec.[38]

G0008 Carbanak

Carbanak has obtained and used open-source tools such as PsExec and Mimikatz.[39]

G0114 Chimera

Chimera has obtained and used tools such as BloodHound, Cobalt Strike, Mimikatz, and PsExec.[40][41]

G1021 Cinnamon Tempest

Cinnamon Tempest has used open-source tools including customized versions of the Iox proxy tool, NPS tunneling tool, Meterpreter, and a keylogger that uploads data to Alibaba cloud storage.[42][43]

G0003 Cleaver

Cleaver has obtained and used open-source tools such as PsExec, Windows Credential Editor, and Mimikatz.[44]

G0080 Cobalt Group

Cobalt Group has obtained and used a variety of tools including Mimikatz, PsExec, Cobalt Strike, and SDelete.[45]

G1052 Contagious Interview

Contagious Interview has used remote management and monitoring software such as "AnyDesk".[46][47][48][49][50]

G0052 CopyKittens

CopyKittens has used Metasploit, Empire, and AirVPN for post-exploitation activities.[51][52]

C0004 CostaRicto

During CostaRicto, the threat actors obtained open source tools to use in their operations.[53]

C0029 Cutting Edge

During Cutting Edge, threat actors leveraged tools including Interactsh to identify vulnerable targets, PySoxy to simultaneously dispatch traffic between multiple endpoints, BusyBox to enable post exploitation activities, and Kubo Injector to inject shared objects into process memory.[54][55]

G0079 DarkHydrus

DarkHydrus has obtained and used tools such as Mimikatz, Empire, and Cobalt Strike.[56]

G0105 DarkVishnya

DarkVishnya has obtained and used tools such as Impacket, Winexe, and PsExec.[57]

G0035 Dragonfly

Dragonfly has obtained and used tools such as Mimikatz, CrackMapExec, and PsExec.[58]

G1006 Earth Lusca

Earth Lusca has acquired and used a variety of open source tools.[59]

G0137 Ferocious Kitten

Ferocious Kitten has obtained open source tools for its operations, including JsonCPP and Psiphon.[60]

G0051 FIN10

FIN10 has relied on publicly-available software to gain footholds and establish persistence in victim environments.[61]

G1016 FIN13

FIN13 has utilized publicly available tools such as Mimikatz, Impacket, PWdump7, ProcDump, Nmap, and Incognito V2 for targeting efforts.[62]

G0053 FIN5

FIN5 has obtained and used a customized version of PsExec, as well as use other tools such as pwdump, SDelete, and Windows Credential Editor.[63]

G0037 FIN6

FIN6 has obtained and used tools such as Mimikatz, Cobalt Strike, and AdFind.[64][65]

G0046 FIN7

FIN7 has utilized a variety of tools such as Cobalt Strike, PowerSploit, and the remote management tool, Atera for targeting efforts.[66]

G0061 FIN8

FIN8 has used open-source tools such as Impacket for targeting efforts.[67]

C0001 Frankenstein

For Frankenstein, the threat actors obtained and used Empire.[68]

C0007 FunnyDream

For FunnyDream, the threat actors used a modified version of the open source PcShare remote administration tool.[69]

G0093 GALLIUM

GALLIUM has used a variety of widely-available tools, which in some cases they modified to add functionality and/or subvert antimalware solutions.[70]

G0047 Gamaredon Group

Gamaredon Group has used various legitimate tools, such as `mshta.exe` and Reg, and services during operations.[71][72]

G0078 Gorgon Group

Gorgon Group has obtained and used tools such as QuasarRAT and Remcos.[73]

G1001 HEXANE

HEXANE has acquired, and sometimes customized, open source tools such as Mimikatz, Empire, VNC remote access software, and DIG.net.[74][75][76]

C0038 HomeLand Justice

During HomeLand Justice, threat actors used tools including Advanced Port Scanner, Mimikatz, and Impacket.[77][78]

G1032 INC Ransom

INC Ransom has acquired and used several tools including MegaSync, AnyDesk, esentutl and PsExec.[79][80][81][82][83]

G0100 Inception

Inception has obtained and used open-source tools such as LaZagne.[84]

G0136 IndigoZebra

IndigoZebra has acquired open source tools such as NBTscan and Meterpreter for their operations.[85][86]

G0004 Ke3chang

Ke3chang has obtained and used tools such as Mimikatz.[87]

G0094 Kimsuky

Kimsuky has obtained and used tools such as Nirsoft WebBrowserPassVIew, Mimikatz, and PsExec.[88][89][90]

G1004 LAPSUS$

LAPSUS$ has obtained tools such as RVTools and AD Explorer for their operations.[91][92]

G0032 Lazarus Group

Lazarus Group has obtained a variety of tools for their operations, including Responder and PuTTy PSCP.[93]

G0077 Leafminer

Leafminer has obtained and used tools such as LaZagne, Mimikatz, PsExec, and MailSniper.[94]

S0681 Lizar

FIN7 has obtained and used tools such as Impacket, Mimikatz, and PsExec.[95]

G0030 Lotus Blossom

Lotus Blossom has used publicly-available tools such as a Python-based cookie stealer for Chrome browsers, Impacket, and the Venom proxy tool.[96]

G1014 LuminousMoth

LuminousMoth has obtained an ARP spoofing tool from GitHub.[97]

G0059 Magic Hound

Magic Hound has obtained and used tools like Havij, sqlmap, Metasploit, Mimikatz, and Plink.[98][99][100][101][102]

G1051 Medusa Group

Medusa Group has obtained and leveraged numerous RMM services, along with publicly available tools used for scanning.[103][104][105] Medusa Group has utilized tools such as Advanced IP Scanner and SoftPerfect Network scanner for user, system and network discovery.[104] Medusa Group has also acquired tools for command and control and defense evasion which include tunneling tools Ligolo and Cloudflared.[104]

G0045 menuPass

menuPass has used and modified open-source tools like Impacket, Mimikatz, and pwdump.[106]

G1013 Metador

Metador has used Microsoft's Console Debugger in some of their operations.[107]

G1009 Moses Staff

Moses Staff has used the commercial tool DiskCryptor.[108]

G0069 MuddyWater

MuddyWater has used legitimate tools ConnectWise, RemoteUtilities, and SimpleHelp to gain access to the target environment.[109][110]

G0129 Mustang Panda

Mustang Panda has obtained and leveraged publicly-available tools for intrusion activities.[111][112]

C0002 Night Dragon

During Night Dragon, threat actors obtained and used tools such as gsecdump.[113]

G0049 OilRig

OilRig has made use of the publicly available tools including Plink and Mimikatz.[114][115]

C0012 Operation CuckooBees

For Operation CuckooBees, the threat actors obtained publicly-available JSP code that was used to deploy a webshell onto a compromised server.[116]

C0022 Operation Dream Job

For Operation Dream Job, Lazarus Group obtained tools such as Wake-On-Lan, Responder, ChromePass, and dbxcli.[117][118]

C0048 Operation MidnightEclipse

During Operation MidnightEclipse, threat actors used the GO Simple Tunnel (GOST) reverse proxy tool.[119]

C0005 Operation Spalax

For Operation Spalax, the threat actors obtained packers such as CyaX.[120]

C0014 Operation Wocao

For Operation Wocao, the threat actors obtained a variety of open source tools, including JexBoss, KeeThief, and BloodHound.[121]

G0040 Patchwork

Patchwork has obtained and used open-source tools such as QuasarRAT.[122]

G0011 PittyTiger

PittyTiger has obtained and used tools such as Mimikatz and gsecdump.[123]

G1040 Play

Play has used multiple tools for discovery and defense evasion purposes on compromised hosts.[124]

G1005 POLONIUM

POLONIUM has obtained and used tools such as AirVPN and plink in their operations.[52]

C0059 Salesforce Data Exfiltration

During Salesforce Data Exfiltration, threat actors initially relied on the legitimate Salesforce Data Loader app for data exfiltration.[125][126]

G1045 Salt Typhoon

Salt Typhoon has used publicly available tooling to exploit vulnerabilities.[127]

G0034 Sandworm Team

Sandworm Team has acquired open-source tools for their operations, including Invoke-PSImage, which was used to establish an encrypted channel from a compromised host to Sandworm Team's C2 server in preparation for the 2018 Winter Olympics attack, as well as Impacket and RemoteExec, which were used in their 2022 Prestige operations.[128][129] Additionally, Sandworm Team has used Empire, Cobalt Strike and PoshC2.[130]

G1015 Scattered Spider

Scattered Spider has obtained tools for use throughout the attack lifecycle to include remote access software, protocol tunneling and proxy tools, exploitation frameworks, and reconnaissance tools.[131][132][133][134]

G1041 Sea Turtle

Sea Turtle has used tools such as Adminer during intrusions.[135]

C0045 ShadowRay

During ShadowRay, threat actors used tools including the XMRig miner and Interactsh.[136]

C0058 SharePoint ToolShell Exploitation

During SharePoint ToolShell Exploitation, threat actors leveraged tools including Impacket, PsExec, and Mimikatz.[137]

G0091 Silence

Silence has obtained and modified versions of publicly-available tools like Empire and PsExec.[138] [139]

G0122 Silent Librarian

Silent Librarian has obtained free and publicly available tools including SingleFile and HTTrack to copy login pages of targeted organizations.[140][141]

C0052 SPACEHOP Activity

SPACEHOP Activity leverages a C2 framework sourced from a publicly-available Github repository for administration of relay nodes.[142]

G1033 Star Blizzard

Star Blizzard has incorporated the open-source EvilGinx framework into their spearphishing activity.[143][144]

G1046 Storm-1811

Storm-1811 acquired various legitimate and malicious tools, such as RMM software and commodity malware packages, for operations.[145][146]

G1018 TA2541

TA2541 has used commodity remote access tools.[147]

G0092 TA505

TA505 has used a variety of tools in their operations, including AdFind, BloodHound, Mimikatz, and PowerSploit.[148]

G0027 Threat Group-3390

Threat Group-3390 has obtained and used tools such as Impacket, pwdump, Mimikatz, gsecdump, NBTscan, and Windows Credential Editor.[149][150]

G0076 Thrip

Thrip has obtained and used tools such as Mimikatz and PsExec.[151]

C0030 Triton Safety Instrumented System Attack

In the Triton Safety Instrumented System Attack, TEMP.Veles used tools such as Mimikatz and other open-source software.[152]

G0010 Turla

Turla has obtained and customized publicly-available tools like Mimikatz.[153]

G1017 Volt Typhoon

Volt Typhoon has used legitimate network and forensic tools and customized versions of open-source tools for C2.[154][155]

G0107 Whitefly

Whitefly has obtained and used tools such as Mimikatz.[156]

G0090 WIRTE

WIRTE has obtained and used Empire for post-exploitation activities.[157]

G0102 Wizard Spider

Wizard Spider has utilized tools such as Empire, Cobalt Strike, Cobalt Strike, Rubeus, AdFind, BloodHound, Metasploit, Advanced IP Scanner, Nirsoft PingInfoView, and SoftPerfect Network Scanner for targeting efforts.[158][159]
