System Service Discovery, Technique T1007 - Enterprise

Archived: 2026-04-05 13:28:12 UTC

G0018 admin@338

admin@338 actors used the following command following exploitation of a machine with LOWBALL malware to obtain information about services: `net start >> %temp%\download` [5]

G0006 APT1

APT1 used the commands `net start` and `tasklist` to get a listing of the services on the system.[6]

G0143 Aquatic Panda

Aquatic Panda has attempted to discover services for third party EDR products.[7]

S0638 Babuk

Babuk can enumerate all services running on a compromised host.[8]

S0127 BBSRAT

BBSRAT can query service configuration information.[9]

S0570 BitPaymer

BitPaymer can enumerate existing Windows services on the host that are configured to run as LocalSystem.[10]

S1070 Black Basta

Black Basta can check whether the service name `FAX` is present.[11]

G0060 BRONZE BUTLER

BRONZE BUTLER has used TROJ_GETVERSION to discover system services.[12]

S0572 Caterpillar WebShell

Caterpillar WebShell can obtain a list of the services from a system.[13]

G0114 Chimera

Chimera has used `net start` and `net use` for system service discovery.[14]

S0154 Cobalt Strike

Cobalt Strike can enumerate services on compromised hosts.[15]

S0244 Comnie

Comnie runs the command: `net start >> %TEMP%\info.dat` on a victim.[16]

S0625 Cuba

Cuba can query service status using `QueryServiceStatusEx` function.[17]

S1066 DarkTortilla

DarkTortilla can retrieve information about a compromised system's running services.[18]

S0024 Dyre

Dyre has the ability to identify running services on a compromised host.[19]

G1006 Earth Lusca

Earth Lusca has used Tasklist to obtain information from a compromised host.[20]

S0081 Elise

Elise executes `net start` after initial communication is made to the remote server.[21]

S1247 Embargo

Embargo has obtained active services running on the victim’s system through the functions `OpenSCManagerW()` and `EnumServicesStatusExW()`.[22]

S0082 Emissary

Emissary has the capability to execute the command `net start` to interact with services.[23]

S0091 Epic

Epic uses the `tasklist /svc` command to list the services on the system.[24]

S0049 GeminiDuke

GeminiDuke collects information on programs and services on the victim that are configured to automatically run at startup.[25]

S0237 GravityRAT

GravityRAT has a feature to list the available services on the system.[26]

S0342 GreyEnergy

GreyEnergy enumerates all Windows services.[27]

S1027 Heyoka Backdoor

Heyoka Backdoor can check if it is running as a service on a compromised host.[28]

S0431 HotCroissant

HotCroissant has the ability to retrieve a list of services on the infected host.[29]

S0203 Hydraq

Hydraq creates a backdoor through which remote attackers can monitor services.[30][31]

S0398 HyperBro

HyperBro can list all services and their configurations.[32]

G0119 Indrik Spider

Indrik Spider has used the win32_service WMI class to retrieve a list of services from the system.[33]

S0260 InvisiMole

InvisiMole can obtain running services on the victim.[34]

S0015 Ixeshe

Ixeshe can list running services.[35]

S0201 JPIN

JPIN can list running services.[36]

S0283 jRAT

jRAT can list local services.[37]

G0004 Ke3chang

Ke3chang performs service discovery using `net start` commands.[38]

G0094 Kimsuky

Kimsuky has used an instrumentor script to gather the names of all services running on a victim's system.[39]

S0236 Kwampirs

Kwampirs collects a list of running services with the command `tasklist /svc`.[40]

S0582 LookBack

LookBack can enumerate services on the victim machine.[41]

S1244 Medusa Ransomware

Medusa Ransomware has leveraged an encoded list of services that it designates for termination.[42][43][44]

S0039 Net

The `net start` command can be used in Net to find information about Windows services.[45]

G0049 OilRig

OilRig has used `sc query` on a victim to gather information about services.[46]

C0012 Operation CuckooBees

During Operation CuckooBees, the threat actors used the `net start` command as part of their initial reconnaissance.[47]

C0014 Operation Wocao

During Operation Wocao, threat actors used the `tasklist` command to search for one of its backdoors.[48]

G0033 Poseidon Group

After compromising a victim, Poseidon Group discovers all running services.[49]

S0378 PoshC2

PoshC2 can enumerate service and service permission information.[50]

S1228 PUBLOAD

PUBLOAD has leveraged `tasklist` to gather running services on victim host.[51]

S1242 Qilin

Qilin can identify specific services for termination or to be left running at execution.[52][53][54]

S0629 RainyDay

RainyDay can create and register a service for execution.[55]

S0241 RATANKBA

RATANKBA uses `tasklist /svc` to display running tasks.[56]

S0496 REvil

REvil can enumerate active services.[57]

S0085 S-Type

S-Type runs the command `net start` on a victim.[58]

S1085 Sardonic

Sardonic has the ability to execute the `net start` command.[59]

S0692 SILENTTRINITY

SILENTTRINITY can search for modifiable services that could be used for privilege escalation.[60]

S0533 SLOTHFULMEDIA

SLOTHFULMEDIA has the capability to enumerate services.[61]

S0615 SombRAT

SombRAT can enumerate services on a victim machine.[62]

S0559 SUNBURST

SUNBURST collected a list of service names that were hashed using a FNV-1a + XOR algorithm to check against similarly-hashed hardcoded blocklists.[63]

S0018 Sykipot

Sykipot may use `net start` to display running services.[64]

S0242 SynAck

SynAck enumerates all running services.[65][66]

S0663 SysUpdate

SysUpdate can collect a list of services on a victim machine.[67]

S0057 Tasklist

Tasklist can be used to discover services running on a system.[68]

G0139 TeamTNT

TeamTNT has searched for services such as Alibaba Cloud Security's aliyun service and BMC Helix Cloud Security's bmc-agent service in order to disable them.[69]

S0266 TrickBot

TrickBot collects a list of install programs and services on the system's machine.[70]

G0010 Turla

Turla surveys a system upon check-in to discover running services and associated processes using the `tasklist /svc` command.[24]

S0386 Ursnif

Ursnif has gathered information about running services.[71]

S0180 Volgmer

Volgmer queries the system to identify existing services.[72]

G1017 Volt Typhoon

Volt Typhoon has used `net start` to list running services.[73]

S0219 WINERACK

WINERACK can enumerate services.[74]

S0086 ZLib

ZLib has the ability to discover and manipulate Windows services.[58]

S0412 ZxShell

ZxShell can check the services on the system.[75]
