System Owner/User Discovery, Technique T1033 - Enterprise

Archived: 2026-04-05 14:50:05 UTC

S1028 Action RAT

Action RAT has the ability to collect the username from an infected host.[3]

S0331 Agent Tesla

Agent Tesla can collect the username from the victim’s machine.[4][5][6]

S0092 Agent.btz

Agent.btz obtains the victim username and saves it to a file.[7]

S1025 Amadey

Amadey has collected the user name from a compromised host using `GetUserNameA`.[8]

G0073 APT19

APT19 used an HTTP malware variant and a Port 22 malware variant to collect the victim’s username.[9]

G0022 APT3

An APT3 downloader uses the Windows command `"cmd.exe" /C whoami` to verify that it is running with the elevated privileges of "System."[10]

G0050 APT32

APT32 collected the victim's username and executed the `whoami` command on the victim's machine. APT32 executed shellcode to collect the username on the victim's machine. [11][12][13]

G0067 APT37

APT37 identifies the victim username.[14]

G0082 APT38

APT38 has identified primary users, currently logged in users, sets of users that commonly use a system, or inactive users.[15]

G0087 APT39

APT39 used Remexi to collect usernames from the system.[16]

G0096 APT41

APT41 has executed `whoami` commands, including using the WMIEXEC utility to execute this on remote machines.[17][18]

G0143 Aquatic Panda

Aquatic Panda gathers information on recently logged-in users on victim devices.[19]

S0456 Aria-body

Aria-body has the ability to identify the username on a compromised host.[20]

S1087 AsyncRAT

AsyncRAT can check if the current user of a compromised system is an administrator. [21]

S1029 AuTo Stealer

AuTo Stealer has the ability to collect the username from an infected host.[3]

S0344 Azorult

Azorult can collect the username from the victim’s machine.[22]

S0414 BabyShark

BabyShark has executed the `whoami` command.[23]

S0093 Backdoor.Oldrea

Backdoor.Oldrea collects the current username from the victim.[24]

S1081 BADHATCH

BADHATCH can obtain logged user information from a compromised machine and can execute the command `whoami.exe`.[25]

S0534 Bazar

Bazar can identify the username of the infected user.[26]

S0017 BISCUIT

BISCUIT has a command to gather the username from the system.[27]

S1068 BlackCat

BlackCat can utilize `net use` commands to discover the user name on a compromised host.[28]

S0521 BloodHound

BloodHound can collect information on user sessions.[29]

S0657 BLUELIGHT

BLUELIGHT can collect the username on a compromised host.[30]

S0486 Bonadan

Bonadan has discovered the username of the user running the backdoor.[31]

S1226 BOOKWORM

BOOKWORM has obtained the username from an infected host. [32]

S0635 BoomBox

BoomBox can enumerate the username on a compromised host.[33]

S1039 Bumblebee

Bumblebee has the ability to identify the user name.[34]

C0017 C0017

During C0017, APT41 used `whoami` to gather information from victim machines.[35]

C0018 C0018

During C0018, the threat actors collected `whoami` information via PowerShell scripts.[36]

S0351 Cannon

Cannon can gather the username from the system.[37]

S0348 Cardinal RAT

Cardinal RAT can collect the username from a victim machine.[38]

S0572 Caterpillar WebShell

Caterpillar WebShell can obtain a list of user accounts from a victim's machine.[39]

S0631 Chaes

Chaes has collected the username and UID from the infected machine.[40]

G0114 Chimera

Chimera has used the `quser` command to show currently logged on users.[41]

S1149 CHIMNEYSWEEP

CHIMNEYSWEEP has included the victim's computer name and username in C2 messages sent to actor-owned infrastructure.[42]

S0667 Chrommme

Chrommme can retrieve the username from a targeted system.[43]

S0660 Clambling

Clambling can identify the username on a compromised host.[44][45]

S1024 CreepySnail

CreepySnail can execute `getUsername` on compromised systems.[46]

S0115 Crimson

Crimson can identify the user on a targeted system.[47][48][49]

S0498 Cryptoistic

Cryptoistic can gather data on the user of a compromised host.[50]

S1153 Cuckoo Stealer

Cuckoo Stealer can discover and send the username from a compromised host to C2.[51]

S0334 DarkComet

DarkComet gathers the username from the victim’s machine.[52]

S0673 DarkWatchman

DarkWatchman has collected the username from a victim machine.[53]

S0354 Denis

Denis enumerates and collects the username from the victim’s machine.[54][13]

S0021 Derusbi

A Linux version of Derusbi checks if the victim user ID is anything other than zero (normally used for root), and the malware will not execute if it does not have root privileges. Derusbi also gathers the username of the victim.[55]

S0659 Diavol

Diavol can collect the username from a compromised host.[56]

S1021 DnsSystem

DnsSystem can use the Windows user name to create a unique identification for infected users and systems.[57]

S0186 DownPaper

DownPaper collects the victim username and sends it to the C2 server.[58]

G0035 Dragonfly

Dragonfly used the command `query user` on victim hosts.[59]

S0694 DRATzarus

DRATzarus can obtain a list of users from an infected machine.[60]

S0024 Dyre

Dyre has the ability to identify the users on a compromised host.[61]

G1006 Earth Lusca

Earth Lusca collected information on user accounts via the `whoami` command.[62]

S0554 Egregor

Egregor has used tools to gather information about users.[63]

S0367 Emotet

Emotet has enumerated all users connected to network shares.

S0363 Empire

Empire can enumerate the username on targeted hosts.[64]

S0091 Epic

Epic collects the user name from the victim’s machine.[65]

S0568 EVILNUM

EVILNUM can obtain the username from the victim's machine.[66]

S0401 Exaramel for Linux

Exaramel for Linux can run `whoami` to identify the system owner.[67]

S0569 Explosive

Explosive has collected the username from the infected host.[68]

S0171 Felismus

Felismus collects the current username and sends it to the C2 server.[69]

S0267 FELIXROOT

FELIXROOT collects the username from the victim's machine.[70][71]

G0051 FIN10

FIN10 has used Meterpreter to enumerate users on remote systems.[72]

G0046 FIN7

FIN7 has used the command `cmd.exe /C quser` to collect user session information.[73]

G0061 FIN8

FIN8 has executed the command `quser` to display the session details of a compromised machine.[74]

S0696 Flagpro

Flagpro has been used to run the `whoami` command on the system.[75]

S0381 FlawedAmmyy

FlawedAmmyy enumerates the current user during the initial infection.[76][77]

C0001 Frankenstein

During Frankenstein, the threat actors used Empire to enumerate hosts and gather username, machine name, and administrative permissions information.[64]

S1044 FunnyDream

FunnyDream has the ability to gather user information from the targeted system using `whoami/upn&whoami/fqdn&whoami/logonid&whoami/all`.[78]

G0093 GALLIUM

GALLIUM used `whoami` and `query user` to obtain information about the victim user.[79]

G0047 Gamaredon Group

A Gamaredon Group file stealer can gather the victim's username to send to a C2 server.[80]

S0168 Gazer

Gazer obtains the current user's security identifier.[81]

S0666 Gelsemium

Gelsemium has the ability to distinguish between a standard user and an administrator on a compromised host.[43]

S0460 Get2

Get2 has the ability to identify the current username of an infected host.[82]

S0249 Gold Dragon

Gold Dragon collects the endpoint victim's username and uses it as a basis for downloading additional components from the C2 server.[83]

S0477 Goopy

Goopy has the ability to enumerate the infected system's user name.[13]

S0531 Grandoreiro

Grandoreiro can collect the username from the victim's machine.[84]

S0237 GravityRAT

GravityRAT collects the victim username along with other account information (account type, description, full name, SID and status).[85]

S0632 GrimAgent

GrimAgent can identify the user id on a target machine.[86]

G0125 HAFNIUM

HAFNIUM has used `whoami` to gather user information.[87]

S0214 HAPPYWORK

can collect the victim user name.[88]

S1229 Havoc

Havoc can trigger exection of `whoami` on the target host to display the current user.[89][90]

S0391 HAWKBALL

HAWKBALL can collect the user name of the system.[91]

G1001 HEXANE

HEXANE has run `whoami` on compromised machines to identify the current user.[92]

S1249 HexEval Loader

HexEval Loader has collected the username from the victim host.[93]

S0431 HotCroissant

HotCroissant has the ability to collect the username on the infected host.[94]

S1245 InvisibleFerret

InvisibleFerret has identified the user's UUID and username through the "pay" module.[95][96][97]

S0260 InvisiMole

InvisiMole lists local users and session information.[98]

S0015 Ixeshe

Ixeshe collects the username from the victim's machine.[99]

S0201 JPIN

JPIN can obtain the victim user name.[100]

S0265 Kazuar

Kazuar gathers information on users.[101]

G0004 Ke3chang

Ke3chang has used implants capable of collecting the signed-in username.[102]

S0250 Koadic

Koadic can identify logged in users across the domain and views user sessions.[103][104]

S0162 Komplex

The OsInfo function in Komplex collects the current running username.[105]

S0356 KONNI

KONNI can collect the username from the victim's machine.[106]

S1075 KOPILUWAK

KOPILUWAK can conduct basic network reconnaissance on the victim machine with `whoami`, to get user details. [107]

S0236 Kwampirs

Kwampirs collects registered owner details by using the commands `systeminfo` and `net config workstation`. [108]

S1160 Latrodectus

Latrodectus can discover the username of an infected host.[109]

G0032 Lazarus Group

Various Lazarus Group malware enumerates logged-on users.[110][111][112][113][114][50][115]

S0362 Linux Rabbit

Linux Rabbit opens a socket on port 22 and if it receives a response it attempts to obtain the machine's hostname and Top-Level Domain. [116]

S0513 LiteDuke

LiteDuke can enumerate the account name on a targeted system.[117]

S0680 LitePower

LitePower can determine if the current user has admin privileges.[118]

S0681 Lizar

Lizar can collect the username from the system.[119][120]

S0447 Lokibot

Lokibot has the ability to discover the username on the infected host.[121]

S0532 Lucifer

Lucifer has the ability to identify the username on a compromised host.[122]

G1014 LuminousMoth

LuminousMoth has used a malicious DLL to collect the username from compromised hosts.[123]

S1141 LunarWeb

LunarWeb can collect user information from the targeted host.[124]

S1016 MacMa

MacMa can collect the username from the compromised machine.[125]

S1060 Mafalda

Mafalda can collect the username from a compromised host.[126]

G0059 Magic Hound

Magic Hound malware has obtained the victim username and sent it to the C2 server.[127][128][129]

S1169 Mango

Mango can collect the user name from a compromised system which is used to create a unique victim identifier.[130]

S0652 MarkiRAT

MarkiRAT can retrieve the victim’s username.[131]

S0459 MechaFlounder

MechaFlounder has the ability to identify the username and hostname on a compromised host.[132]

G1051 Medusa Group

Medusa Group has utilized PsExec to execute `quser` to discover the user session information.[133]

S1059 metaMain

metaMain can collect the username from a compromised host.[126]

S0455 Metamorfo

Metamorfo has collected the username from the victim's machine.[134]

S1146 MgBot

MgBot includes modules for identifying local users and administrators on victim machines.[135]

S0339 Micropsia

Micropsia collects the username from the victim’s machine.[136]

S1015 Milan

Milan can identify users registered to a targeted machine.[137]

S0280 MirageFox

MirageFox can gather the username from the victim’s machine.[138]

S0084 Mis-Type

Mis-Type runs tests to determine the privilege level of the compromised user.[139]

G1036 Moonstone Sleet

Moonstone Sleet deployed various malware such as YouieLoader that can perform system user discovery actions.[140]

S0149 MoonWind

MoonWind obtains the victim username.[141]

S0284 More_eggs

More_eggs has the capability to gather the username from the victim's machine.[142][143]

S0256 Mosquito

Mosquito runs `whoami` on the victim’s machine.[144]

G0069 MuddyWater

MuddyWater has used malware that can collect the victim’s username.[145][146]

S0228 NanHaiShu

NanHaiShu collects the username from the victim.[147]

S0590 NBTscan

NBTscan can list active users on the system.[148][149]

S0272 NDiskMonitor

NDiskMonitor obtains the victim username and encrypts the information to send over its C2 channel.[150]

S0691 Neoichor

Neoichor can collect the user name from a victim's machine.[102]

S1106 NGLite

NGLite will run the `whoami` command to gather system information and return this to the command and control server.[151]

C0002 Night Dragon

During Night Dragon, threat actors used password cracking and pass-the-hash tools to discover usernames and passwords.[152]

S1147 Nightdoor

Nightdoor gathers information on victim system users and usernames.[153]

S0385 njRAT

njRAT enumerates the current user during the initial infection.[154]

S0353 NOKKI

NOKKI can collect the username from the victim’s machine.[155]

S0644 ObliqueRAT

ObliqueRAT can check for blocklisted usernames on infected endpoints.[156]

S0340 Octopus

Octopus can collect the username from the victim’s machine.[157]

S1172 OilBooster

OilBooster can identify the compromised system's username which is then used as part of a unique identifier.[158]

G0049 OilRig

OilRig has run `whoami` on a victim.[159][160][161]

S0439 Okrum

Okrum can collect the victim username.[162]

C0012 Operation CuckooBees

During Operation CuckooBees, the threat actors used the `query user` and `whoami` commands as part of their advanced reconnaissance.[163]

C0014 Operation Wocao

During Operation Wocao, threat actors enumerated sessions and users on a remote host, and identified privileged users logged into a targeted system.[164]

G0040 Patchwork

Patchwork collected the victim username and whether it was running as admin, then sent the information to its C2 server.[165][150]

S0013 PlugX

PlugX has the ability to gather the username from the victim’s machine.[166]

S0428 PoetRAT

PoetRAT sent username, computer name, and the previously generated UUID in reply to a "who" command from C2.[167]

S0139 PowerDuke

PowerDuke has commands to get the current user's name and SID.[168]

S0441 PowerShower

PowerShower has the ability to identify the current user on the infected host.[169]

S0223 POWERSTATS

POWERSTATS has the ability to identify the username on the compromised host.[170]

S0184 POWRUNER

POWRUNER may collect information about the currently logged in user by running `whoami` on a victim.[171]

S0113 Prikormka

A module in Prikormka collects information from the victim about the current user name.[172]

S1228 PUBLOAD

PUBLOAD has obtained the username from an infected host.[173][174][175][176]

S0192 Pupy

Pupy can enumerate local information for Linux hosts and find currently logged on users for Windows hosts.[177]

S1032 PyDCrypt

PyDCrypt has probed victim machines with `whoami` and has collected the username from the machine.[178]

S0650 QakBot

QakBot can identify the user name on a compromised system.[179][180]

S0269 QUADAGENT

QUADAGENT gathers the victim username.[181]

S0262 QuasarRAT

QuasarRAT can enumerate the username and account type.[182]

S1148 Raccoon Stealer

Raccoon Stealer gathers information on the infected system owner and user.[183][184][185]

S1130 Raspberry Robin

Raspberry Robin determines whether it is successfully running on a victim system by querying the running account information to determine if it is running in Session 0, indicating running with elevated privileges.[186]

S0241 RATANKBA

RATANKBA runs the `whoami` and `query user` commands.[187]

S0662 RCSession

RCSession can gather system owner information, including user and administrator privileges.[188]

S0172 Reaver

Reaver collects the victim's username.[189]

S0153 RedLeaves

RedLeaves can obtain information about the logged on user both locally and for Remote Desktop sessions.[190]

S1240 RedLine Stealer

RedLine Stealer has obtained the username from the victim’s machine.[191][192][193]

S0125 Remsec

Remsec can obtain information about the current user.[194]

S0379 Revenge RAT

Revenge RAT gathers the username from the system.[195]

S0258 RGDoor

RGDoor executes the `whoami` on the victim’s machine.[196]

S0433 Rifdoor

Rifdoor has the ability to identify the username on the compromised host.[94]

S0448 Rising Sun

Rising Sun can detect the username of the infected host.[197]

S0270 RogueRobin

RogueRobin collects the victim's username and whether that user is an admin.[198]

S0240 ROKRAT

ROKRAT can collect the username from a compromised host.[199]

S0148 RTM

RTM can obtain the victim username and permissions.[200]

S0085 S-Type

S-Type has run tests to determine the privilege level of the compromised user.[139]

S1018 Saint Bot

Saint Bot can collect the username from a compromised host.[201]

G0034 Sandworm Team

Sandworm Team has collected the username from a compromised host.[202]

S0461 SDBbot

SDBbot has the ability to identify the user on a compromised host.[82]

S0382 ServHelper

ServHelper will attempt to enumerate the username of the victim.[203]

S0596 ShadowPad

ShadowPad has collected the username of the victim system.[204]

C0058 SharePoint ToolShell Exploitation

During SharePoint ToolShell Exploitation, threat actors executed `whoami` on victim machines to enumerate user context and validate privilege levels.[205][206]

S0450 SHARPSTATS

SHARPSTATS has the ability to identify the username on the compromised host.[170]

S0610 SideTwist

SideTwist can collect the username on a targeted system.[161]

G0121 Sidewinder

Sidewinder has used tools to identify the user of a compromised host.[207]

S0692 SILENTTRINITY

SILENTTRINITY can gather a list of logged on users.[208]

S0533 SLOTHFULMEDIA

SLOTHFULMEDIA has collected the username from a victim machine.[209]

S1035 Small Sieve

Small Sieve can obtain the id of a logged in user.[210]

S0649 SMOKEDHAM

SMOKEDHAM has used `whoami` commands to identify system owners.[211]

S1124 SocGholish

SocGholish can use `whoami` to obtain the username from a compromised host.[212][213][214]

S0627 SodaMaster

SodaMaster can identify the username on a compromised host.[215]

S0615 SombRAT

SombRAT can execute `getinfo` to identify the username on a compromised host.[216][217]

S0543 Spark

Spark has run the whoami command and has a built-in command to identify the user logged in.[218]

S0374 SpeakUp

SpeakUp uses the `whoami` command. [219]

S1030 Squirrelwaffle

Squirrelwaffle can collect the user name from a compromised host.[220]

S0058 SslMM

SslMM sends the logged-on username to its hard-coded C2.[221]

S1037 STARWHALE

STARWHALE can gather the username from an infected host.[222][223]

G0038 Stealth Falcon

Stealth Falcon malware gathers the registered user and primary owner name via WMI.[224]

G1046 Storm-1811

Storm-1811 has used `whoami.exe` to determine if the active user on a compromised system is an administrator.[225]

S1034 StrifeWater

StrifeWater can collect the user name from the victim's machine.[226]

S0559 SUNBURST

SUNBURST collected the username from a compromised host.[227][228]

S1064 SVCReady

SVCReady can collect the username from an infected host.[229]

S0242 SynAck

SynAck gathers user names from infected hosts.[230]

S0060 Sys10

Sys10 collects the account name of the logged-in user and sends it to the C2.[221]

S0663 SysUpdate

SysUpdate can collect the username from a compromised host.[231]

S0098 T9000

T9000 gathers and beacons the username of the logged in account during installation. It will also gather the username of running processes to determine if it is running as SYSTEM.[232]

G0027 Threat Group-3390

Threat Group-3390 has used `whoami` to collect system user information.[44]

S1239 TONESHELL

TONESHELL has obtained the username from an infected host.[176]

S0266 TrickBot

TrickBot can identify the user and groups the user belongs to on a compromised host.[233]

S0094 Trojan.Karagany

Trojan.Karagany can gather information about the user on a compromised host.[234]

G0081 Tropic Trooper

Tropic Trooper used `letmein` to scan for saved usernames on the target system.[235]

S0647 Turian

Turian can retrieve usernames.[236]

S0130 Unknown Logger

Unknown Logger can obtain information about the victim usernames.[237]

S0275 UPPERCUT

UPPERCUT has the capability to collect the current logged on user's username from a machine.[238]

S0476 Valak

Valak can gather information regarding the user.[239]

S0257 VERMIN

VERMIN gathers the username from the victim's machine.[240]

G1017 Volt Typhoon

Volt Typhoon has used public tools and executed the PowerShell command `Get-EventLog security -instanceid 4624` to identify associated user and computer account names.[241][242][243]

S0515 WellMail

WellMail can identify the current username on the victim system.[244]

S0514 WellMess

WellMess can collect the username on the victim machine to send to C2.[245]

S0155 WINDSHIELD

WINDSHIELD can gather the victim user name.[246]

G0112 Windshift

Windshift has used malware to identify the username on a compromised host.[247]

S0219 WINERACK

WINERACK can gather information on the victim username.[88]

S0059 WinMM

WinMM uses NetUser-GetInfo to identify that it is running under an "Admin" account on the local system.[221]

G1035 Winter Vivern

Winter Vivern PowerShell scripts execute `whoami` to identify the executing user.[248]

G0102 Wizard Spider

Wizard Spider has used "whoami" to identify the local user and their privileges.[249]

S1065 Woody RAT

Woody RAT can retrieve a list of user accounts and usernames from an infected machine.[250]

S0161 XAgentOSX

XAgentOSX contains the getInfoOSX function to return the OS X version as well as the current user.[251]

S1207 XLoader

XLoader can identify the username from a victim machine.[252]

S1248 XORIndex Loader

XORIndex Loader has collected the username from the victim host.[253]

S0248 yty

yty collects the victim’s username.[254]

S0251 Zebrocy

Zebrocy gets the username from the system.[255][256]

G0128 ZIRCONIUM

ZIRCONIUM has used a tool to capture the username on a compromised host in order to register it with C2.[257]

S0350 zwShell

zwShell can obtain the name of the logged-in user on the victim.[152]

S0412 ZxShell

ZxShell can collect the owner and organization information from the target workstation.[258]

S1013 ZxxZ

ZxxZ can collect the username from a compromised host.[259]
