GROUPS
Overview
admin@338
APT1
APT12
APT16
APT17
APT18
APT19
APT28
APT29
APT3
APT30
APT32
APT33
APT37
APT38
APT39
APT41
Axiom
BlackOasis
BRONZE BUTLER
Carbanak
Charming Kitten
Cleaver
Cobalt Group
CopyKittens
Dark Caracal
Darkhotel
DarkHydrus
Deep Panda
Dragonfly
Dragonfly 2.0
DragonOK
Dust Storm
Elderwood
Equation
FIN10
FIN4
FIN5
FIN6
FIN7
FIN8
Gallmaker
Gamaredon Group
GCMAN
Gorgon Group
Group5
Honeybee
Ke3chang
Kimsuky
Lazarus Group
Leafminer
Leviathan
Lotus Blossom
Machete
Magic Hound
menuPass
Moafee
Molerats
MuddyWater
Naikon
NEODYMIUM
Night Dragon
OilRig
Orangeworm
Patchwork
PittyTiger
PLATINUM
Poseidon Group
PROMETHIUM
Putter Panda
Rancor
RTM
Sandworm Team
Scarlet Mimic
Silence
SilverTerrier
Soft Cell
Sowbug
Stealth Falcon
Stolen Pencil
Strider
Suckfly
TA459
TA505
Taidoor
TEMP.Veles
The White Company
Threat Group-1314
Threat Group-3390
Thrip
Tropic Trooper
Turla
WIRTE

TA459

TA459 is a threat group believed to operate out of China that has targeted countries including Russia, Belarus, Mongolia, and others. [1]

ID: G0062
Contributors: Valerii Marchuk, Cybersecurity Help s.r.o.
Version: 1.0
Created: 18 April 2018
Last Modified: 25 March 2019

Techniques Used

ATT&CK® Navigator Layers

Domain	ID	Name	Use
Enterprise	T1203	Exploitation for Client Execution	TA459 has exploited Microsoft Word vulnerability CVE-2017-0199 for execution.[1]
Enterprise	T1086	PowerShell	TA459 has used PowerShell for execution of a payload.[1]
Enterprise	T1064	Scripting	TA459 has a VBScript for execution.[1]
Enterprise	T1193	Spearphishing Attachment	TA459 has targeted victims using spearphishing emails with malicious Microsoft Word attachments.[1]
Enterprise	T1204	User Execution	TA459 has attempted to get victims to open malicious Microsoft Word attachment sent via spearphishing.[1]

Software

ID	Name	References	Techniques
S0032	gh0st RAT	TA459 has used a Gh0st variant known as PCrat/Gh0st.[1]	Command-Line Interface, Commonly Used Port, DLL Side-Loading, File Deletion, Indicator Removal on Host, Input Capture, New Service, Process Discovery, Registry Run Keys / Startup Folder, Remote File Copy, Rundll32, Screen Capture, Standard Cryptographic Protocol
S0033	NetTraveler	[1]	Application Window Discovery, Input Capture
S0013	PlugX	[1]	Command-Line Interface, Commonly Used Port, Custom Command and Control Protocol, Deobfuscate/Decode Files or Information, DLL Side-Loading, Execution through API, File and Directory Discovery, Input Capture, Masquerading, Modify Existing Service, Modify Registry, Multiband Communication, Network Share Discovery, New Service, Process Discovery, Query Registry, Registry Run Keys / Startup Folder, Remote File Copy, Screen Capture, Standard Application Layer Protocol, Standard Non-Application Layer Protocol, System Network Connections Discovery, Trusted Developer Utilities, Virtualization/Sandbox Evasion, Web Service
S0230	ZeroT	[1]	Binary Padding, Bypass User Account Control, Data Obfuscation, Deobfuscate/Decode Files or Information, DLL Side-Loading, New Service, Obfuscated Files or Information, Remote File Copy, Software Packing, Standard Application Layer Protocol, Standard Cryptographic Protocol, System Information Discovery, System Network Configuration Discovery

References

1. Axel F. (2017, April 27). APT Targets Financial Analysts with CVE-2017-0199. Retrieved February 15, 2018.