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
Winnti Group
WIRTE

Home
> Groups
> Tropic Trooper

Tropic Trooper

Tropic Trooper is an unaffiliated threat group that has led targeted campaigns against targets in Taiwan, the Philippines, and Hong Kong. Tropic Trooper focuses on targeting government, healthcare, transportation, and high-tech industries and has been active since 2011.[1][2]

ID: G0081
Associated Groups: KeyBoy
Contributors: Edward Millington, Bart Parys
Version: 1.2
Created: 29 January 2019
Last Modified: 14 October 2019

Associated Group Descriptions

Name	Description
KeyBoy	[2][1]

Techniques Used

ATT&CK® Navigator Layers

Domain	ID	Name	Use
Enterprise	T1043	Commonly Used Port	Tropic Trooper can use ports 443 and 53 for C2 communications via malware called TClient.[1]
Enterprise	T1140	Deobfuscate/Decode Files or Information	Tropic Trooper used shellcode with an XOR algorithm to decrypt a payload.[2]
Enterprise	T1073	DLL Side-Loading	Tropic Trooper has been known to side-load DLLs using a valid version of Windows Address Book executable with one of their tools.[5]
Enterprise	T1203	Exploitation for Client Execution	Tropic Trooper has executed commands through Microsoft security vulnerabilities, including CVE-2017-11882, CVE-2018-0802, and CVE-2012-0158.[1][2]
Enterprise	T1158	Hidden Files and Directories	Tropic Trooper has created a hidden directory under `C:\ProgramData\Apple\Updates\`.[1]
Enterprise	T1046	Network Service Scanning	Tropic Trooper used `pr` to scan for open ports on target systems.[3]
Enterprise	T1135	Network Share Discovery	Tropic Trooper used `netview` to scan target systems for shared resources.[3]
Enterprise	T1050	New Service	Tropic Trooper installs a service pointing to a malicious DLL dropped to disk.[6]
Enterprise	T1027	Obfuscated Files or Information	Tropic Trooper has encrypted configuration files.[1]
Enterprise	T1057	Process Discovery	Tropic Trooper enumerates the running processes on the system.[2]
Enterprise	T1055	Process Injection	Tropic Trooper has injected a DLL backdoor into a file dllhost.exe.[1]
Enterprise	T1063	Security Software Discovery	Tropic Trooper searches for anti-virus software running on the system.[2]
Enterprise	T1193	Spearphishing Attachment	Tropic Trooper sent spearphishing emails that contained malicious Microsoft Office attachments.[2][3][4]
Enterprise	T1032	Standard Cryptographic Protocol	Tropic Trooper uses SSL to connect to C2 servers.[1]
Enterprise	T1082	System Information Discovery	Tropic Trooper has detected a target system's OS version.[3]
Enterprise	T1033	System Owner/User Discovery	Tropic Trooper used `letmein` to scan for saved usernames on the target system.[3]
Enterprise	T1221	Template Injection	Tropic Trooper delivered malicious documents with the XLSX extension, typically used by OpenXML documents, but the file itself was actually an OLE (XLS) document.[2]
Enterprise	T1004	Winlogon Helper DLL	Tropic Trooper creates the Registry key `HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell` and sets the value to establish persistence.[2]

Software

ID	Name	References	Techniques
S0190	BITSAdmin	[1]	BITS Jobs, Exfiltration Over Alternative Protocol, Remote File Copy
S0387	KeyBoy	[2] [4]	Command-Line Interface, Commonly Used Port, Credentials from Web Browsers, Custom Cryptographic Protocol, Dynamic Data Exchange, Exploitation for Client Execution, File and Directory Discovery, Hidden Window, Input Capture, New Service, Obfuscated Files or Information, PowerShell, Remote File Copy, Screen Capture, Scripting, System Information Discovery, System Network Configuration Discovery, Timestomp, Winlogon Helper DLL
S0012	PoisonIvy	[2]	Application Window Discovery, Command-Line Interface, Data from Local System, Data Staged, Input Capture, Modify Existing Service, Modify Registry, New Service, Obfuscated Files or Information, Process Injection, Registry Run Keys / Startup Folder, Remote File Copy, Rootkit, Standard Cryptographic Protocol, Uncommonly Used Port
S0388	Yahoyah	[3]	Deobfuscate/Decode Files or Information, Obfuscated Files or Information, Remote File Copy, Security Software Discovery, Standard Application Layer Protocol, System Information Discovery

References

1. Horejsi, J., et al. (2018, March 14). Tropic Trooper's New Strategy. Retrieved November 9, 2018.
2. Ray, V. (2016, November 22). Tropic Trooper Targets Taiwanese Government and Fossil Fuel Provider With Poison Ivy. Retrieved November 9, 2018.
3. Alintanahin, K. (2015). Operation Tropic Trooper: Relying on Tried-and-Tested Flaws to Infiltrate Secret Keepers. Retrieved June 14, 2019.
4. Alexander, G., et al. (2018, August 8). Familiar Feeling: A Malware Campaign Targeting the Tibetan Diaspora Resurfaces. Retrieved June 17, 2019.
5. Hulcoop, A., et al. (2016, November 17). It's Parliamentary KeyBoy and the targeting of the Tibetan Community. Retrieved June 13, 2019.
6. Parys, B. (2017, February 11). The KeyBoys are back in town. Retrieved June 13, 2019.