Thinking in SideWinder

Author: 2ero

Sun Tzu once said in his Art of War: "Know the enemy and know yourself; in a hundred battles you will never be in peril". So we hunt with the adversary's TTPs.

Firstly, we need to extract SideWinder's TTPs. Here, we will use ATT&CK Enterprise Matrix.

Reconnaissance	T1591 Gather Victim Org Information
	T1598 Phishing for Information
Resource Development	T1583 Acquire Infrastructure
Initial Access	T1566 Phishing
Execution	T1204 User Execution
	T1203 Exploitation for Client Execution
Persistence	T1547 Boot or Logon Autostart Execution
	T1053 Scheduled Task/Job
Privilege Escalation	T1068 Exploitation for Privilege Escalation
Defense Evasion	T1036 Masquerading
	T1027 Obfuscated Files or Information
Discovery	T1518 Software Discovery
Collection	T1005 Data from Local System
Command and Control	T1071 Application Layer Protocol
	T1008 Fallback Channels
Exfiltration	T1041 Exfiltration Over C2 Channel

Table 1. SideWinder's ATT&CK Enterprise Matrix

Secondly, we transform SideWinder's TTPs.

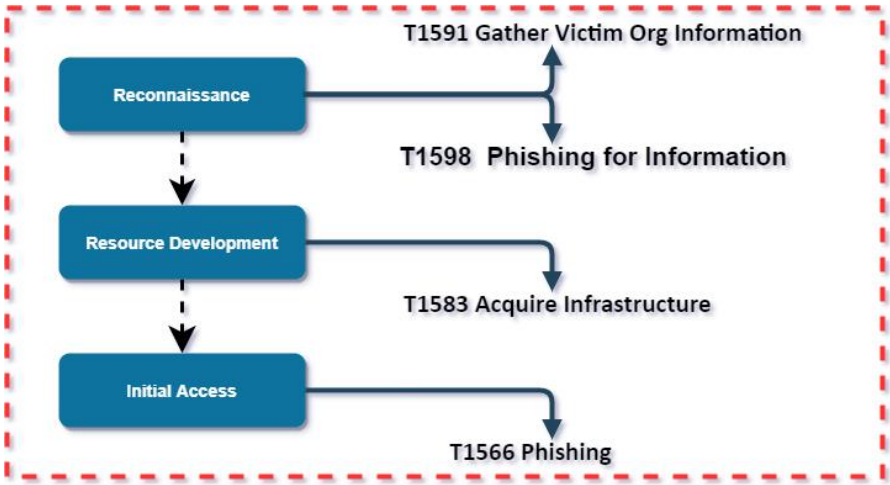


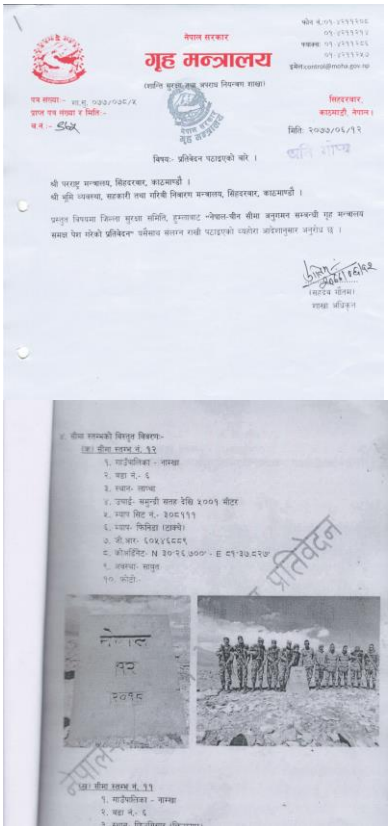
Figure 1. The first stage of hunting

Think as SideWinder

Technique	SideWinder's question(s)	SideWinder's practice
T1591 Gather Victim Org Information	Who do we need to attack? Who are our targets?	Target: Nepal, Pakistan, India Special Population, China and Bahrain Victim: Government, Military, Energy, Diplomacy, University and Finance
T1598 Phishing for Information	What are our targets meta-information?	Such as: Nepal Police, Nepal Army, Islamabad, Tsinghua, Central Bank of Bahrain, Nepal-China Border, Punjab Police, etc.
T1583 Acquire Infrastructure	How to register confusing domain?	Using meta-info combination
T1598 Phishing for Information	What are data sources we need?	Email gateway, Mail server, Social media monitoring. Such as: Faisalabad Regional Office | Govt of Punjab email address, Gujranwala Regional Office | Govt of Punjab email address, Lahore Regional Office | Govt of Punjab email address, Multan Regional Office | Govt of Punjab email address, Rawalpindi Regional Office | Govt of Punjab email address, Sahiwal Regional Office | Govt of Punjab email address.

Table 2. Think as SideWinder

Ok, we will use T1591, T1598, T1583 and T1583 to hunt. Base on meta info, I will show some "prey".

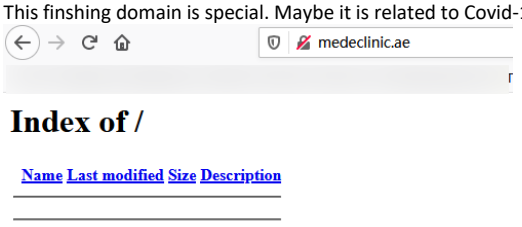
Technique	Hunt threat
T1591 Gather Victim Org Information	https://email-nepalarmy-mil-np-owa.netlify[.]app/Nepal-China%20Border%20Humla%20Field%20Inspection%20Report.zip Name: Nepal-China Border Humla Field Inspection Report.zip Sha256: fb63a33dbb48a09fb2571fd3d26742321e3ea50553d6325856a8e30bc6112dda 

नेपाल सरकार
गृह मन्त्रालय
(सशस्त्र सुरक्षा तथा आपत्कालीन नियन्त्रण शाखा)
पत्र संख्या:- गृ.मं. २७७/०७८/२
जावा पत्र संख्या र मिति:-
च.नं.:- 5Sx
सिंहदरबार,
काठमाण्डौं, नेपाल।
मिति: २०७७/०६/१२
प्रति गोप्य
विषय:- प्रतिवेदन पठाइएको बारे ।
श्री परराष्ट्र मन्त्रालय, सिंहदरबार, काठमाण्डौं ।
श्री भूमि व्यवस्था, सहकारी तथा गरिबी निवारण मन्त्रालय, सिंहदरबार, काठमाण्डौं ।
प्रस्तुत विषयमा जिल्ला सुरक्षा समिति, हुम्लाबाट "नेपाल-चीन सीमा अनुगमन सम्बन्धी गृह मन्त्रालय समक्ष पेश गरेको प्रतिवेदन" यसैसाथ संलग्न राखी पठाइएको व्यहोरा आदेशानुसार अनुरोध छ ।
(सटिक सीमा)
शाखा अधिकृत

हेभि ईक्युपमेन्ट प्राप्त भएको सम्बन्धमा.pdf
English: Regarding receiving heavy equipment.pdf
Sha256: 0db65702d705e547c7b9373cc641b90357f4762687cb0e65b01d1efa5f22a59a
Embedded fishing domain:
https://mail-nepalarmy-mil-np-view.netlify[.]app/

https://dgmi-share-folder-nepalarmy-mil-np-coas-sambodhan-pdf.netlify[.]app/Sambodhan.pdf
Name: Sambodhan.pdf
English: Address.pdf
sha256: ba87dc684c92ae53b996c41c47c356ef0b750bfb88d01d9e87598029caae6a33

http://imail.aop.gov.af.egateway.nsc-gov[.]com/call%20pages.zip
Name: call pages.zip
Sha256: de14262e933cebc5df89e725df6fea08c971aff092621bbbb462b105716d1c8a

T1598 Phishing for Information T1583 Acquire Infrastructure	Fishing domain mail-ntmail-ntcnetnp.serveftp.comcnetnp.serveftp[.]com mail-nepalpolice-gov-np-loginn.herokuapp[.]com nsc-gov[.]net medeclinic[.]ae mail-nscaf.hopto[.]org mail-nepalarmy-mil-np-fsdafjsd.herokuapp[.]com mail-nepalarmy-mil-np-login-download.netlify[.]app mail-nepalarmy-mil-np-view.netlify[.]app nepalarmy.trans-del[.]net polyinc-global.trans-del[.]net mod-cn.trans-del[.]net mil-pk[.]net mofagov-pk.naatlibrary[.]com mofagov-pk[.]online webmail.mofagov-pk[.]online autodiscover.mofagov-pk[.]online cpcalendars.mofagov-pk[.]online webdisk.mofagov-pk[.]online cpcontacts.mofagov-pk[.]online mail.mofagov-pk[.]online www.mofagov-pk[.]online cpanel.mofagov-pk[.]online mofagov-pk.naatlibrary[.]com www.mofagov-pk.naatlibrary[.]com www-punjabpolice-gov-pk-sopforsecurityofforeignersandchinese.trans-aws[.]net This finshing domain is special. Maybe it is related to Covid-19 in Southeast Asia 

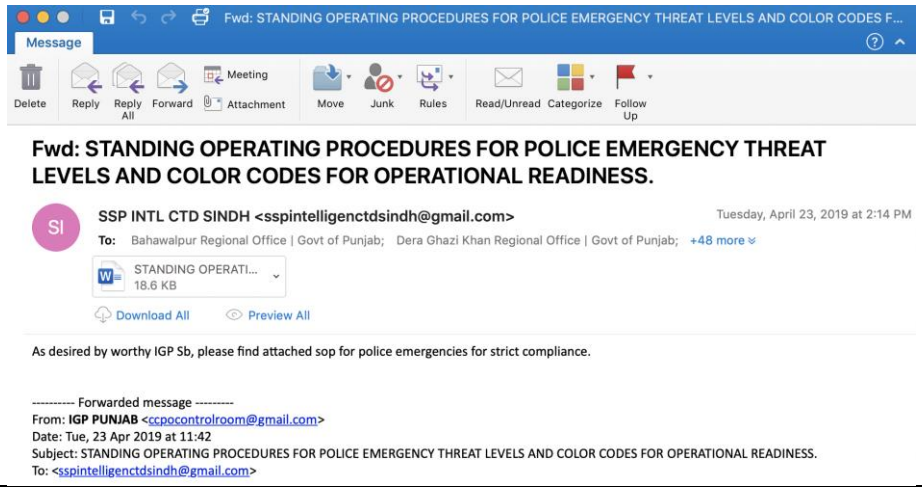
T1598 Phishing for Information	Fishing email 

Table 3. some “prey”

Execution

Technique	Hunt threat
T1204 User Execution T1203 Exploitation for Client Execution	

Sha256/URL	CVE	File Type
14a1e413881ceeb4cd25a12f74aa6caafdb9cf396092ed81d78d8b06b3d60c7f	CVE-2017-11882	RFT
121648be6641269d626d4d2ad79d234c99b121e0e0588909c05ba870308d9bc9	CVE-2017-0199	Docx
https://mp.weixin.qq.com/s/5mBqxf_v6G006EnjECoTHw	CVE-2020-0674	HTML

SideWinder uses CVE-2017-11882 and CVE-2017-0199. You can write YARA rule to detect it.

https://github.com/s0wr0b1ndef/YARA-Rules/blob/master/Malicious_Documents/Maldoc_CVE-2017-0199.yar
https://github.com/Yara-Rules/rules/blob/master/cve_rules/CVE-2017-11882.yar
https://github.com/maxpl0it/CVE-2020-0674-Exploit, you can write yara rule to detect CVE-2020-0674

Table 4. The execution stage of hunting

Persistence:

Technique	Hunt threat

T1547 Boot or Logon Autostart Execution	Sha256: 7238f4e5edbe0e5a2242d8780fb58c47e7d32bf2c4f860c88c511c30675d0857
	Auto start: HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
	Query “HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run”, check if “C:\ProgramData*\rekeywiz.exe” exists.
	`PS C:\Users> $key = Get-Item "HKCU:\Software\Microsoft\Windows\CurrentVersion\Run"`
	`PS C:\Users> Get-ItemProperty $key.PSPath`
	`sildewinder : C:\ProgramData\AtlasFilesMap1\rekeywiz.exe`
	`PSPath : Microsoft.PowerShell.Core\Registry::HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run`
	`PSParentPath : Microsoft.PowerShell.Core\Registry::HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion`
	`PSChildName : Run`
	`PSProvider : Microsoft.PowerShell.Core\Registry`

T1053 Scheduled Task/Job	Sha256: 7238f4e5edbe0e5a2242d8780fb58c47e7d32bf2c4f860c88c511c30675d0857 How to hunt? Please check schtasks.exe run more times, and commands contain“C:\ProgramData*\rekeywiz.exe” **Shell Commands** "C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE" /t /q C:\Users\Lucas\Documents\7238f4e5edbe0e5a2242d8780fb58cc511c30675d0857.rtf "C:\Program Files (x86)\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding schtasks.exe /create /tn UpdateService /sc once /tr C:\ProgramData\AtlasFilesMap1\rekeywiz.exe /st 03:48 C:\Windows\splwow64.exe 8192 C:\ProgramData\AtlasFilesMap1\rekeywiz.exe schtasks.exe /create /tn UpdateService /sc once /tr C:\ProgramData\AtlasFilesMap1\rekeywiz.exe /st 16:48 schtasks.exe /create /tn UpdateService /sc once /tr C:\ProgramData\AtlasFilesMap1\rekeywiz.exe /st 16:46 "C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE" /t /q C:\Users\Lucas\Documents\e24e51ec170b2341ef90321640fef7nalysis_subject.rtf schtasks.exe /create /tn UpdateService /sc once /tr C:\ProgramData\AtlasFilesMap1\rekeywiz.exe /st 17:04
Privilege Escalation: T1068 Exploitation for Privilege Escalation	Please view T1203 Exploitation for Client Execution

Table 5. The persistence stage of hunting

Defense Evasion:

Technique	Hunt threat
T1036 Masquerading	This technique needs many keywords, such as: Nepal Police, Nepal Army, Islamabad, Tsinghua, Central Bank of Bahrain, Nepal-China Border, Punjab Police.

T1027 Obfuscated Files or Information	SideWinder has the unique decryption algorithm
	Sha256: 2548a819e4c597ba5958d2d18baa544452948e5b00271570192ccd79abe88e8d
	`b = b64.indexOf(str.charAt(i++)) << 18`
	`b64.indexOf(str.charAt(i++)) << 12`
	`(r1 = b64.indexOf(str.charAt(i++))) << 6`
	`(r2 = b64.indexOf(str.charAt(i++)))`
	`result += r1 === 64`
	You can use opcode[62203d206236342e696e6465784f66287374722e63686172417428692b2b2929203c3c203138] to detect it. In addition, you can research its algorithm for decrypting CVE Exploit, which is also very unique.

Table 6. The defense evasion stage of hunting

Discovery:

Technique	Hunt threat

T1518 Software Discovery	Sha256: 2548a819e4c597ba5958d2d18baa544452948e5b00271570192ccd79abe88e8d
	`var objWMIService = GetObject(ELqNusUz("sstuMqZvq"+"OEEEGbcVt"+"TpGnFz5KO"+"QOHEosHtW"+"SqiUddFT"))`
	`var colItems = objWMIService.ExecQuery(ELqNusUz("Zs4FSqoU"+"stD9uHZv"+"MdEbG4Fq"+"E6HGOHFz"+"OgEgOqoU"), null, 48)`
	`var objItem = new Enumerator(colItems)`
	This technique is difficult to transform rule.

Table 7. The discovery stage of hunting

Collection, Command, Control and Exfiltration:

Technique	Hunt threat

T1005 Data from Local System
 	
T1071 Application Layer Protocol
 	
T1008 Fallback Channels The techniques are difficult to transform rule.
 	
T1041 Exfiltration Over C2 Channel
	Please use Suricata or Snort to detect it. It seems very simple.
	{
	"privileges": {
	"IsInAdminGroup": "Yes",
	"IsAdminPrivilege": "No"
	},
	"sysInfo": {
	"userAccount": [{
	"name": "Administrator"
	}, {
	"name": "[redacted]"
	}, {
	"name": "Guest"
	}],
	"computerSystem": [{
	"Caption": "WIN[redacted]",
	"UserName": "WIN-[redacted]",
	"Manufacturer": "VMware, Inc.",
	"Model": "VMware Virtual Platform",
	"PrimaryOwnerName": "Windows ....",
	"TotalPhysicalMemory": "2146951168"
	}],
	"networkAdapter": [{
	"ServiceName": "RasSstp",
	"MACAddress": "na",
	"AdapterType": "na",
	"Name": "WAN Miniport (SSTP)"
	}, {
	"ServiceName": "RasAgileVpn",
	"MACAddress": "na",
	"AdapterType": "na",
	"Name": "WAN Miniport (IKEv2)"
	}, {
	"ServiceName": "Rasl2tp",
	"MACAddress": "na",
	"AdapterType": "na",
	"Name": "WAN Miniport (L2TP)"
	}, {
	"ServiceName": "PptpMiniport",
	"MACAddress": "na",
	"AdapterType": "na",
	"Name": "WAN Miniport (PPTP)"
	}, {
	"ServiceName": "RasPppoe",
	"MACAddress": "na",
	"AdapterType": "na",
	"Name": "WAN Miniport (PPPOE)"
	}, {
	"ServiceName": "NdisWan",
	"MACAddress": "na",
	"AdapterType": "na",
	"Name": "WAN Miniport (IPv6)"
	}, {
	https://www.antiy.com/response/20190508.html

Table 7. The last stage of hunting

Ref

[1] https://www.antiy.com/response/20190508[.]html

[2] https://mp.weixin.qq[.]com/s/5mBqxf_v6G006EnjECoTHw

[3] https://www.trendmicro[.]com/en_us/research/20/l/sidewinder-leverages-south-asian-territorial-issues-for-spear-ph.html