PRACTICAL 5

DATE: 17-04-2025

AIM: To learn about CTI and threat hunting operations and incident response planning.

Steps;-

- Open the hash file
- Analyze the type of hash
- Scan the hash in Virus total
- Prepare a Report in chart format

SR. No	Properties	04eda293e486872c3ad9353b5bde5bae	04ef876b2ba1a6836641dc875f1cf52a
1	**Type of hash**	MD5	MD5
2	**Analysis Date**	2025-03-16 11:46:47 UTC	2024-06-05 14:49:45 UTC
3	**Creation Time**	2013-04-09 15:54:09 UTC	2016-10-06 14:33:38 UTC
4	**Name**	amstream.dll	sys.dll
5	**Target Machine**	Intel 386 or later processors and compatible processors	Intel 386 or later processors and compatible processors
6	**Security Vendor Analysis**	AhnLab-V3-Trojan/Win32.Banker.R56908 Alibaba-TrojanSpy:Win32/Banker.117f3d7f AliCloud - Backdoor:Win/Bradop.A ALYacGen :-Trojan.Heur.bnSfremII5DU Antiy-AVL - Trojan/Win32.BHO	AlibabaTrojanBanker:Win32/Ghoul.054e2f69 Antiy-AVLTrojan/Win32.SGeneric AvastWin32:AgentBanker-A [Bank] AVGWin32:AgentBanker-A [Bank] Avira (no cloud)HEUR/AGEN.1328858
7	**Type of Attack**	Trojan	Trojan
8	**IP**	-	-
9	**Behaviour**	-	-
10	**Modules Involved**	-	-

SR. No	Properties	04f48c7dad83b583eaff571af1149473	04f4d2915c4125570df7bb2640f543da
1	Type of hash	MD5	MD5
2	Analysis Date	2021-01-26 18:39:27 UTC	2021-02-05 04:12:32 UTC
3	Creation Time	2013-10-31 10:10:49 UTC	1992-06-19 22:22:17 UTC
4	Name	siswin32.exe	Boleto_Numero_472390574343.cpl
5	Target Machine	Intel 386 or later processors and compatible processors	Intel 386 or later processors and compatible processors
6	Security Vendor Analysis	Ad-AwareGen:Variant.Johnnie.18512 AlibabaTrojan:Win32/BANKER.6d0c4efb ALYacGen:Variant.Johnnie.18512 ArcabitTrojan.Johnnie.D4850 AvastWin32:Malware-gen	Ad-AwareGen:Variant.Graftor.184869 AhnLab-V3Trojan/Win32.ChePro.R139734 AlibabaTrojanDownloader:Win32/Banload.8feaaf21 ALYacGen:Variant.Graftor.184869 Antiy-AVLTrojan[Banker]/Win32.ChePro
7	Type of Attack	Trojan	Trojan
8	IP	-	-
9	Behaviour	Modify registry of startup	-
10	Modules Involved	C:\WINDOWS\system32\MSCTF.dll C:\WINDOWS\system32\kernel32.dll C:\WINDOWS\system32\msctfime.ime	-

SR. No	Properties	04f9615f20a930c85391ec6432ec899f	04faf3609b7f1739fa006d97dc54b03d
1	Type of hash	MD5	MD5
2	Analysis Date	2025-03-22 00:50:55 UTC	2021-02-14 13:59:26 UTC
3	Creation Time	1992-06-19 22:22:17 UTC	2017-06-16 17:46:42 UTC
4	Name	index.php.exe.vir	CodigodeRastreio_CJ463077332BR.exe
5	Target Machine	Intel 386 or later processors and compatible processors	Intel 386 or later processors and compatible processors
6	Security Vendor Analysis	AlibabaTrojanDownloader:Win32/Banload.0773dd28 AliCloudTrojan[downloader]:Win/Banload.QML ALYacTrojan.Crypt.Delf.AG Antiy-AVLTrojan/Win32.Agent ArcabitTrojan.Crypt.Delf.AG	Ad-AwareTrojan.GenericKD.5377634 AegisLabTrojan.Win32.Generic.4!c AhnLab-V3Trojan/Win32.Banload.C2031854 AlibabaTrojanDownloader:MSIL/Banload.68cc93f8 ALYacTrojan.GenericKD.5377634
7	Type of Attack	Trojan	Trojan
8	IP	-	-
9	Behaviour	Modify registry of UAC	Access CPU clock directly
10	Modules Involved	ADVAPI32.dll C:\WINDOWS\System32\wshtcpip.dll C:\WINDOWS\system32\MSCTF.dll C:\WINDOWS\system32\Msctf.dll	ADVAPI32.dll AdvApi32.dll C:\WINDOWS\System32\wshtcpip.dll

SR. No	Properties	04fe98b96a00e739a7fc0e4804c641f0	04fea0b448de8c6e2ea592efa90056d0
1	Type of hash	MD5	MD5
2	Analysis Date	2021-02-14 11:07:21 UTC	2021-02-05 09:03:04 UTC
3	Creation Time	2008-04-13 18:31:55 UTC	2017-01-19 20:44:00 UTC
4	Name	sndrec32.exe	mtav.exe
5	Target Machine	Intel 386 or later processors and compatible processors	Intel 386 or later processors and compatible processors
6	Security Vendor Analysis	Ad-AwareWin32.Valhalla.2048 AhnLab-V3Win32/Valla.2048 AlibabaVirus:Win32/Xorala.9306e3f1 ALYacWin32.Valhalla.2048 Antiy-AVLVirus/Win32.Xorala.b	Ad-AwareTrojan.GenericKD.45131452 AegisLabTrojan.Win32.Bandra.7!c AlibabaTrojanBanker:Win32/Bandra.e3f4270e ALYacTrojan.GenericKD.45131452 Antiy-AVLTrojan[Banker]/Win32.Bandra
7	Type of Attack	Virus	Trojan
8	IP	-	-
9	Behaviour	Modify existing executable file	Access CPU clock directly
10	Modules Involved	comctl32.dll imm32.dll rpcrt4.dll version.dll	cryptbase.dll dwmapi.dll executer.exe gdi32.dll

SR. No	Properties	04fecd302a792283461c57da9f57f98a	04ffefaac4db4191aa9613798a1c232a
1	Type of hash	MD5	MD5
2	Analysis Date	2025-03-24 10:39:56 UTC	2021-02-01 17:47:59 UTC
3	Creation Time	1992-06-19 22:22:17 UTC	2015-07-07 01:16:34 UTC
4	Name	any.EXE	HnPFQNyhtEf.exe
5	Target Machine	Intel 386 or later processors and compatible processors	Intel 386 or later processors and compatible processors
6	Security Vendor Analysis	AhnLab-V3Trojan/Win32.Inject.R27213 AlibabaTrojanDropper:Win32/Dorifel.1e3463f9 AliCloudTrojan[downloader]:Win/Waldek.gen ALYacTrojan.Generic.KD.648583 Antiy-AVLTrojan[Dropper]/Win32.Dorifel	Ad-AwareTrojan.GenericKD.2548349 AlibabaTrojan:Win32/Predator.ali2000022 ALYacTrojan.GenericKD.2548349 ArcabitTrojan.Generic.D26E27D AvastWin32:GenMalicious-LTF [Trj]
7	Type of Attack	Trojan	Trojan
8	IP	-	-
9	Behaviour	-	Modify registry of startup
10	Modules Involved	-	C:\Program Files\Common Files\System\wab32.dll C:\Program Files\Common Files\System\wab32res.dll C:\WINDOWS\System32\wshtcpip.dll

Conclusion:-

Understanding Cyber Threat Intelligence (CTI), threat hunting operations, and incident response planning is essential for building a robust cybersecurity posture. CTI provides actionable insights into potential threats, helping organizations proactively defend against attacks. Threat hunting complements this by actively seeking out hidden threats within systems, going beyond traditional reactive security measures. Meanwhile, a well-structured incident response plan ensures that when incidents occur, organizations can contain, mitigate, and recover efficiently. Together, these elements form a proactive, layered defense strategy that significantly enhances an organization's ability to detect, respond to, and prevent cyber threats.