Presentation As a Malware

Description

Can ppt file be malware?

Research Objectives

1. What was the general name/category of the malicious file in the analyzed ppt file?

2. Which is the url adresses it communicates with has been detected as harmful by sandboxes?

3. What is the name of the htm file that drops to disk?

4. Which process is running to persistent under mshta.exe after relevant malware runs?

5. If there was a short IDS in the environment at the time of the incident, which rules would it match?

Walkthrough

File hashsum

Firstly, need to get hash of the malware sample. And you too, if you want to examine sample closely through VirusTotal, AnyRun or, exctactly, `download` it from the Bazaar.

- powershell.exe `Get-FileHash .\filename.extension`
  Here it is:
  `md5sum PO#00187.ppt`
  `1dadb4c3fe45566d28b7156be2e2aa6b PO#00187.ppt`

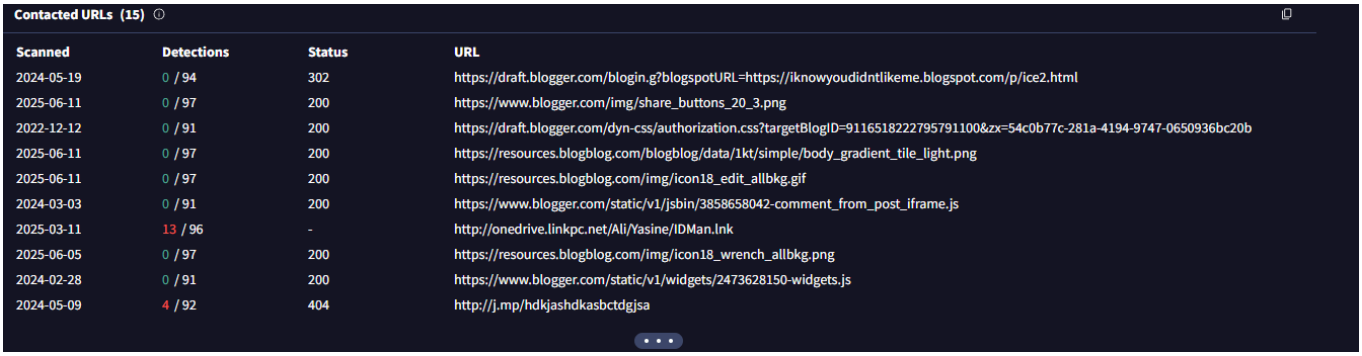
Examining with VirusTotal

Our objectives refer to malware activities when it was executed. So, if the run malware on our environment, we will infect our own machine. Also i think we cant oversee full behaviour analysis when run it on labstand cause it is isolated.

Security vendors' analysis			Do you want to automate checks?
Acronis (Static ML)	Suspicious	AhnLab-V3	Downloader/PPT.Generic.S1397
AliCloud	Trojan[downloader]:MSOffice/Obfuse.P…	ALYac	VB:Trojan.VBA.Agent.BJR
Antiy-AVL	Trojan[Downloader]/MSOffice.Agent	Arcabit	VB:Trojan.VBA.Agent.BJR
Avast	MO97:Downloader-VH [Trj]	AVG	MO97:Downloader-VH [Trj]
BitDefender	VB:Trojan.VBA.Agent.BJR	CTX	Ppt.trojan.generic
DrWeb	P98M.Downloader.5	Elastic	Malicious (high Confidence)
Emsisoft	VB:Trojan.VBA.Agent.BJR (B)	eScan	VB:Trojan.VBA.Agent.BJR
ESET-NOD32	A Variant Of VBA/TrojanDownloader.Age…	Fortinet	VBA/Agent.BJQ!tr
GData	VB:Trojan.VBA.Agent.BJR	Google	Highly Suspicious
Huorong	HEUR:TrojanDownloader/VBS.Agent.hf	Ikarus	Trojan.VB
Kaspersky	HEUR:Trojan.MSOffice.SAgent.gen	Lionic	Trojan.MSPPoint.SAgent.4!c
Microsoft	TrojanDownloader:O97M/Obfuse.PKT!MTB	NANO-Antivirus	Trojan.Ole2.Vbs-heuristic.druvzi
QuickHeal	O97M.Trojan.Agent.41693	Rising	Downloader.Agent/VBA!8.109E7 (TOPIS:…
Sangfor Engine Zero	VBA.Sus.Obf	SentinelOne (Static ML)	Static AI - Malicious OLE
Skyhigh (SWG)	BehavesLike.OLE2.Suspicious.cr	Symantec	Trojan.Gen.NPE
Tencent	Heur.Macro.Generic.h.8242c1d3	Trellix ENS	W97M/Downloader.dlt
TrendMicro	Trojan.P97M.POWLOAD.AN	TrendMicro-HouseCall	Trojan.P97M.POWLOAD.AN
Varist	VBA/ABTrojan.INPC-	VIPRE	VB:Trojan.VBA.Agent.BJR
VirIT	P97M.Aggah.CTR	Xcitium	Malware@#2t8qyyq4s9guw

So the category is the `VB:Trojan` - first goal

To see the contacted URLs, we need go to relations page and examine that

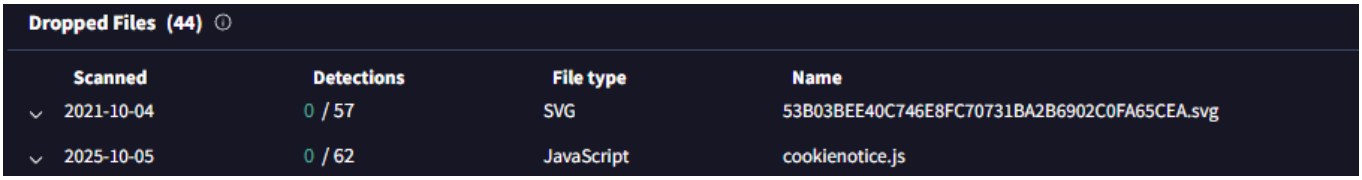


Contacted URLs (15)

Scanned	Detections	Status	URL
2024-05-19	0 / 94	302	https://draft.blogger.com/blogin.g?blogspotURL=https://iknowyoudidntlikeme.blogspot.com/p/ice2.html
2025-06-11	0 / 97	200	https://www.blogger.com/img/share_buttons_20_3.png
2022-12-12	0 / 91	200	https://draft.blogger.com/dyn-css/authorization.css?targetBlogID=9116518222795791100&zx=54c0b77c-281a-4194-9747-0650936bc20b
2025-06-11	0 / 97	200	https://resources.blogblog.com/blogblog/data/1kt/simple/body_gradient_tile_light.png
2025-06-11	0 / 97	200	https://resources.blogblog.com/img/icon18_edit_allbkg.gif
2024-03-03	0 / 91	200	https://www.blogger.com/static/v1/jsbin/3858658042-comment_from_post_iframe.js
2025-03-11	13 / 96	-	http://onedrive.linkpc.net/Ali/Yasine/IDMan.lnk
2025-06-05	0 / 97	200	https://resources.blogblog.com/img/icon18_wrench_allbkg.png
2024-02-28	0 / 91	200	https://www.blogger.com/static/v1/widgets/2473628150-widgets.js
2024-05-09	4 / 92	404	http://j.mp/hdkjashdkasbctdgjsa

One of them have the bigger detections rate - it is our second goal

To overview dropped files go to same segment



Dropped Files (44)

Scanned	Detections	File type	Name
2021-10-04	0 / 57	SVG	53B03BEE40C746E8FC70731BA2B6902C0FA65CEA.svg
2025-10-05	0 / 62	JavaScript	cookienotice.js

And look for .htm document:

`[hdkjashdkasbctdgjsa[1].htm] The next step we need to examine part of process tree: ![[Pasted image 20251118000236.png]]` schtasks.exe `used to persist To examine the IDS rules: ![[Pasted image 20251118000421.png]]` EVENT_CTE_HEADER` is our goal

Let's summarize

1. `VB:Trojan`
2. `http[://]onedrive[.]linkpc[.]net[/]ali[/]yasine[/]idman[.]lnk`
3. `[hdkjashdkasbctdgjsa[1].htm]`
4. `schtasks.exe`
5. `EVENT_CTE_HEADER`