Lookup Hash	Rating	Comment	Positives	Virus	File Names	First Submitted	Last Submitted	File Type	MD5	SHA1	SHA256	Imphash	Matching Rule	Harmless	Revoked	Expired	Trusted	Signed	Signer	Hybrid Analysis S	MalShare Sample	VirusBay Sample	MISP	MISP Events	URLhaus	AnyRun	CAPE	VALHALLA	User Comments	Microsoft	Kaspersky	McAfee	CrowdStrike	TrendMicro	ESET-NOD32	Symantec	F-Secure	Sophos	GData
0acb884f2f4cfa75	malicious	APT_APT29_NOBELIUM_BoomBox_May21_1	41	Microsoft: TrojanDownloader:W	BOOM.exe, BOOI	#############	#############	Win32 EXE	e9594890e33b65	5fb5074d103624	0acb884f2f4cfa75	f34d5f2d4577ed6	-	FALSE	FALSE	FALSE	FALSE	FALSE	-	TRUE	FALSE	FALSE	FALSE		FALSE	FALSE	FALSE	[]	['-']	TrojanDownloade	-	Downloader-FCEI	win/malicious_cor	TROJ_GEN.R002	a variant of MSIL/	Trojan Horse	-	Mal/Generic-S	Trojan.GenericKD.46332476
60e20576b08a24	malicious	APT_APT29_NOBELIUM_BoomBox_May21_1	21	Microsoft: TrojanDownloader:W	Attachment.img	#############	#############	Macintosh Disk In	a879889bc011f0f	f48026a143a8b4	60e20576b08a24	-	-	FALSE	FALSE	FALSE	FALSE	FALSE	-	FALSE	FALSE	FALSE	FALSE		FALSE	FALSE	FALSE	[{'positives': 2, 'rul	['thor']	TrojanDownloade	HEUR:Trojan.MSI	Downloader-FCEI	-	-	multiple detection	-	-	-	Trojan.GenericKD.46332476
749bf48a22ca161	malicious	APT_APT29_NOBELIUM_BoomBox_May21_1	25	Microsoft: TrojanDownloader:W	NV.img	#############	#############	Macintosh Disk In	5c37d66e0a02ee	de8b0031ac9e00	749bf48a22ca161	-	-	FALSE	FALSE	FALSE	FALSE	FALSE	-	FALSE	FALSE	FALSE	FALSE		FALSE	FALSE	FALSE	[{'positives': 22, 'r	['thor']	TrojanDownloade	HEUR:Trojan.MSI	Downloader-FCEI	-	-	multiple detection	-	-	Mal/Generic-S	Trojan.GenericKD.46331359
8199f309478e8ec	malicious	APT_APT29_NOBELIUM_BoomBox_May21_1	44	Microsoft: TrojanDownloader:W	BOOM.exe, BOOI	#############	#############	Win32 EXE	bd7734d9ee4a6d	fc60899c6d0468a	8199f309478e8ec	f34d5f2d4577ed6	-	FALSE	FALSE	FALSE	FALSE	FALSE	-	TRUE	FALSE	FALSE	FALSE		FALSE	FALSE	FALSE	[]	['-']	TrojanDownloade	HEUR:Trojan.MSI	Downloader-FCEI	win/malicious_cor	TROJ_GEN.R002	a variant of MSIL/	Trojan Horse	-	-	Trojan.GenericKD.46334963
85d44977f6fc4e7	malicious	APT_APT29_NOBELIUM_BoomBox_May21_1	11	Microsoft: TrojanDownloader:W	BOOM.exe, NV.p	#############	#############	Win32 EXE	9efc878ac530357	78ea2c679d3a41	85d44977f6fc4e7	f34d5f2d4577ed6	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	-	FALSE	FALSE	FALSE	FALSE		FALSE	FALSE	FALSE	[]	['-']	TrojanDownloade	-	-	-	-	a variant of MSIL/	-	-	-	-
cf1d992f776421f7	malicious	APT_APT29_NOBELIUM_BoomBox_May21_1	42	Microsoft: TrojanDownloader:W	BOOM.exe, BOOI	#############	#############	Win32 EXE	a3369c4bf67cdb3	9ec1ce776d13c2	cf1d992f776421f7	f34d5f2d4577ed6	-	FALSE	FALSE	FALSE	FALSE	FALSE	-	TRUE	FALSE	FALSE	FALSE		FALSE	TRUE	FALSE	[]	['-']	TrojanDownloade	HEUR:Trojan.MSI	Downloader-FCEI	win/malicious_cor	TROJ_GEN.R002	a variant of MSIL/	-	-	-	Trojan.GenericKD.46331359
e41a7616a3919d	malicious	APT_APT29_NOBELIUM_BoomBox_May21_1	23	Microsoft: TrojanDownloader:W	NV.img	#############	#############	Macintosh Disk In	2e3b4221697bc2	2d17a7533da3d6	e41a7616a3919d	-	-	FALSE	FALSE	FALSE	FALSE	FALSE	-	FALSE	FALSE	FALSE	FALSE		FALSE	TRUE	FALSE	[{'positives': 3, 'rul	['thor', 'thor']	TrojanDownloade	HEUR:Trojan.MSI	Downloader-FCEI	-	-	multiple detection	-	-	Mal/Generic-S	Trojan.GenericKD.46334963
0acb884f2f4cfa75	malicious	APT_APT29_NOBELIUM_BoomBox_May21_2	41	Microsoft: TrojanDownloader:W	BOOM.exe, BOOI	#############	#############	Win32 EXE	e9594890e33b65	5fb5074d103624	0acb884f2f4cfa75	f34d5f2d4577ed6	-	FALSE	FALSE	FALSE	FALSE	FALSE	-	TRUE	FALSE	FALSE	FALSE		FALSE	FALSE	FALSE	[]	['-']	TrojanDownloade	-	Downloader-FCEI	win/malicious_cor	TROJ_GEN.R002	a variant of MSIL/	Trojan Horse	-	Mal/Generic-S	Trojan.GenericKD.46332476
60e20576b08a24	malicious	APT_APT29_NOBELIUM_BoomBox_May21_2	21	Microsoft: TrojanDownloader:W	Attachment.img	#############	#############	Macintosh Disk In	a879889bc011f0f	f48026a143a8b4	60e20576b08a24	-	-	FALSE	FALSE	FALSE	FALSE	FALSE	-	FALSE	FALSE	FALSE	FALSE		FALSE	FALSE	FALSE	[{'positives': 2, 'rul	['thor']	TrojanDownloade	HEUR:Trojan.MSI	Downloader-FCEI	-	-	multiple detection	-	-	-	Trojan.GenericKD.46332476
749bf48a22ca161	malicious	APT_APT29_NOBELIUM_BoomBox_May21_2	25	Microsoft: TrojanDownloader:W	NV.img	#############	#############	Macintosh Disk In	5c37d66e0a02ee	de8b0031ac9e00	749bf48a22ca161	-	-	FALSE	FALSE	FALSE	FALSE	FALSE	-	FALSE	FALSE	FALSE	FALSE		FALSE	FALSE	FALSE	[{'positives': 22, 'r	['thor']	TrojanDownloade	HEUR:Trojan.MSI	Downloader-FCEI	-	-	multiple detection	-	-	Mal/Generic-S	Trojan.GenericKD.46331359
8199f309478e8ec	malicious	APT_APT29_NOBELIUM_BoomBox_May21_2	44	Microsoft: TrojanDownloader:W	BOOM.exe, BOOI	#############	#############	Win32 EXE	bd7734d9ee4a6d	fc60899c6d0468a	8199f309478e8ec	f34d5f2d4577ed6	-	FALSE	FALSE	FALSE	FALSE	FALSE	-	TRUE	FALSE	FALSE	FALSE		FALSE	FALSE	FALSE	[]	['-']	TrojanDownloade	HEUR:Trojan.MSI	Downloader-FCEI	win/malicious_cor	TROJ_GEN.R002	a variant of MSIL/	Trojan Horse	-	-	Trojan.GenericKD.46334963
85d44977f6fc4e7	malicious	APT_APT29_NOBELIUM_BoomBox_May21_2	11	Microsoft: TrojanDownloader:W	BOOM.exe, NV.p	#############	#############	Win32 EXE	9efc878ac530357	78ea2c679d3a41	85d44977f6fc4e7	f34d5f2d4577ed6	-	FALSE	FALSE	FALSE	FALSE	FALSE	-	FALSE	FALSE	FALSE	FALSE		FALSE	FALSE	FALSE	[]	['-']	TrojanDownloade	-	-	-	-	a variant of MSIL/	-	-	-	-
cf1d992f776421f7	malicious	APT_APT29_NOBELIUM_BoomBox_May21_2	42	Microsoft: TrojanDownloader:W	BOOM.exe, BOOI	#############	#############	Win32 EXE	a3369c4bf67cdb3	9ec1ce776d13c2	cf1d992f776421f7	f34d5f2d4577ed6	-	FALSE	FALSE	FALSE	FALSE	FALSE	-	TRUE	FALSE	FALSE	FALSE		FALSE	TRUE	FALSE	[]	['-']	TrojanDownloade	HEUR:Trojan.MSI	Downloader-FCEI	win/malicious_cor	TROJ_GEN.R002	a variant of MSIL/	-	-	-	Trojan.GenericKD.46331359
e41a7616a3919d	malicious	APT_APT29_NOBELIUM_BoomBox_May21_2	23	Microsoft: TrojanDownloader:W	NV.img	#############	#############	Macintosh Disk In	2e3b4221697bc2	2d17a7533da3d6	e41a7616a3919d	-	-	FALSE	FALSE	FALSE	FALSE	FALSE	-	FALSE	FALSE	FALSE	FALSE		FALSE	TRUE	FALSE	[{'positives': 3, 'rul	['thor', 'thor']	TrojanDownloade	HEUR:Trojan.MSI	Downloader-FCEI	-	-	multiple detection	-	-	Mal/Generic-S	Trojan.GenericKD.46334963
656384c4e5f9fe4	suspicious	APT_APT29_NOBELIUM_BoomBox_PDF_Masq_May2	1	Microsoft: Trojan:Win32/Casde	manual.pdf	#############	#############	PDF	c59d65430e090f3	88f009eb0d68024	656384c4e5f9fe4	-	-	FALSE	FALSE	FALSE	FALSE	FALSE	-	FALSE	FALSE	FALSE	FALSE		FALSE	FALSE	FALSE	[]	['-']	Trojan:Win32/Cas	-	-	-	-	-	-	-	-	-
076b5eab4b6a2b	suspicious	APT_APT29_NOBELIUM_JS_EnvyScout_May21_1	3	Microsoft: TrojanDropper:JS/Er	076b5eab4b6a2b	#############	#############	Text	59b583645978f9	d464bc03fe20c78	076b5eab4b6a2b	-	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	-	FALSE	FALSE	FALSE	FALSE		FALSE	FALSE	FALSE	[]	['-']	TrojanDropper:JS	-	-	-	-	JS/TrojanDropper	-	-	-	-
541d3868c3f75bb	suspicious	APT_APT29_NOBELIUM_JS_EnvyScout_May21_1	2	Microsoft: TrojanDropper:JS/Er	071d5c44d21c36	#############	#############	Text	2ea5aea76bfa9df	d6ce559645b043	541d3868c3f75bb	-	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	-	FALSE	FALSE	FALSE	FALSE		FALSE	FALSE	FALSE	[]	['-']	TrojanDropper:JS	-	-	-	-	JS/TrojanDropper	-	-	-	-
72ecba53877d57	suspicious	APT_APT29_NOBELIUM_JS_EnvyScout_May21_1	3	Microsoft: TrojanDropper:JS/Er	071d5c44d21c36	#############	#############	Text	8a620ca09cd6f2c	91f722376257ff37	72ecba53877d57	-	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	-	FALSE	FALSE	FALSE	FALSE		FALSE	FALSE	FALSE	[]	['-']	TrojanDropper:JS	-	-	-	-	JS/TrojanDropper	-	-	-	-
8df6ba945aee768	suspicious	APT_APT29_NOBELIUM_JS_EnvyScout_May21_1	3	Microsoft: TrojanDropper:JS/Er	8df6ba945aee768	#############	#############	Text	9625d2daa24391	16a993cce7920f0	8df6ba945aee768	-	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	-	FALSE	FALSE	FALSE	FALSE		FALSE	FALSE	FALSE	[]	['-']	TrojanDropper:JS	-	-	-	-	JS/TrojanDropper	-	-	-	-
9059c5b46dce85	suspicious	APT_APT29_NOBELIUM_JS_EnvyScout_May21_1	4	Microsoft: TrojanDropper:JS/Er	Attachment.html	#############	#############	HTML	44011659d6f589	aa5589fe1e149ef	9059c5b46dce85	-	-	FALSE	FALSE	FALSE	FALSE	FALSE	-	FALSE	FALSE	FALSE	FALSE		FALSE	FALSE	FALSE	[]	['-']	TrojanDropper:JS	-	-	-	-	JS/TrojanDropper	-	-	-	HTML.Trojan.Agent.SQ1U23
9301e48ea3fa7d3	suspicious	APT_APT29_NOBELIUM_JS_EnvyScout_May21_1	3	Microsoft: TrojanDropper:JS/Er	_NOSUBMIT_NV.	#############	#############	HTML	e405285f73ddb8	ae2a555cf0d0cb1	9301e48ea3fa7d3	-	-	FALSE	FALSE	FALSE	FALSE	FALSE	-	TRUE	FALSE	FALSE	FALSE		FALSE	TRUE	FALSE	[]	['-']	TrojanDropper:JS	-	-	-	-	JS/TrojanDropper	-	-	-	-
0585ed374f47d82	suspicious	APT_APT29_NOBELIUM_LNK_NV_Link_May21_2	4	ESET-NOD32: LNK/Agent.KT	NV.LNK	#############	#############	Windows shortcut	736d58bf1d28bf9	182a7a2a0f84d11	0585ed374f47d82	-	-	FALSE	FALSE	FALSE	FALSE	FALSE	-	FALSE	FALSE	FALSE	FALSE		FALSE	FALSE	FALSE	[]	['-']	-	-	-	-	-	LNK/Agent.KT	-	-	-	-
e41a7616a3919d	malicious	APT_APT29_NOBELIUM_LNK_NV_Link_May21_2	23	Microsoft: TrojanDownloader:W	NV.img	#############	#############	Macintosh Disk In	2e3b4221697bc2	2d17a7533da3d6	e41a7616a3919d	-	-	FALSE	FALSE	FALSE	FALSE	FALSE	-	FALSE	FALSE	FALSE	FALSE		FALSE	TRUE	FALSE	[{'positives': 3, 'rul	['thor', 'thor']	TrojanDownloade	HEUR:Trojan.MSI	Downloader-FCEI	-	-	multiple detection	-	-	Mal/Generic-S	Trojan.GenericKD.46334963
69f0d85119123f3	suspicious	APT_APT29_NOBELIUM_LNK_Samples_May21_1	3	ESET-NOD32: LNK/Agent.KT	AKTUALIZ.LNK	#############	#############	Windows shortcut	ed24b708a0abb9	6e45cc934336d7	69f0d85119123f3	-	-	FALSE	FALSE	FALSE	FALSE	FALSE	-	FALSE	FALSE	FALSE	FALSE		FALSE	TRUE	FALSE	[]	['-']	-	-	-	-	-	LNK/Agent.KT	-	-	-	-
f88530bc87cf2c1	suspicious	APT_APT29_NOBELIUM_LNK_Samples_May21_1	1	ESET-NOD32: LNK/Agent.KT	REPLY_SL.LNK	#############	#############	Windows shortcut	1d059c2645ebac	5c6ec94ef0c56f1	f88530bc87cf2c1	-	-	FALSE	FALSE	FALSE	FALSE	FALSE	-	FALSE	FALSE	FALSE	FALSE		FALSE	FALSE	FALSE	[]	['-']	-	-	-	-	-	LNK/Agent.KT	-	-	-	-
776014a63bf3cc7	suspicious	APT_APT29_NOBELIUM_Malware_May21_2	7	Microsoft: Trojan:Win32/Native	diassvcs.dll, DIAS	#############	#############	Win32 DLL	e55d9f6300fa324	247a32ebee0595	776014a63bf3cc7	f09dc86f464ce61	-	FALSE	FALSE	FALSE	FALSE	FALSE	-	FALSE	FALSE	FALSE	FALSE		FALSE	TRUE	FALSE	[]	['-']	Trojan:Win32/Nati	-	-	win/malicious_cor	-	a variant of Win64	-	-	-	-
89016b87e97a07	suspicious	APT_APT29_NOBELIUM_Malware_May21_2	3	Microsoft: Trojan:Win32/Native	AktualizC!ciu.img	#############	#############	Macintosh Disk In	bd05e95b88b41c	6de2eb459ea442	89016b87e97a07	-	-	FALSE	FALSE	FALSE	FALSE	FALSE	-	FALSE	FALSE	FALSE	FALSE		FALSE	TRUE	FALSE	[{'positives': 1, 'rul	['thor']	Trojan:Win32/Nati	-	-	-	-	multiple detection	-	-	-	-
2a352380d61e89	malicious	APT_APT29_NOBELIUM_Malware_May21_3	28	Microsoft: Program:Win32/Wac	MsDiskMountServ	#############	#############	Win32 DLL	77605aa6bd6fb8	6114655cf8ddfd1	2a352380d61e89	4c87e913f89b91a	-	FALSE	FALSE	FALSE	FALSE	FALSE	-	TRUE	FALSE	FALSE	FALSE		FALSE	FALSE	FALSE	[]	['-']	Program:Win32/W	-	Artemis!77605AA	win/malicious_cor	-	a variant of Win32	ML.Attribute.High	-	ML/PE-A	Trojan.GenericKD.46094142
f006af714379fdd6	malicious	APT_APT29_NOBELIUM_Malware_May21_3	23	Microsoft: Program:Win32/Wac	Reply slip.iso	#############	#############	Macintosh Disk In	c689d925ea3b4e	01abab121bf50d	f006af714379fdd6	-	-	FALSE	FALSE	FALSE	FALSE	FALSE	-	FALSE	FALSE	FALSE	FALSE		FALSE	FALSE	FALSE	[{'positives': 6, 'rul	['thor']	Program:Win32/W	-	Trojan-FTND!776	-	-	multiple detection	-	-	Generic PUA GB	Trojan.GenericKD.46094142
3b94cc71c325f90	malicious	APT_APT29_NOBELIUM_Malware_May21_4	39	Microsoft: Trojan:Win32/Native	KM.FileSystem.dll	#############	#############	Win32 DLL	66534e53d8751a	fc781887fd05790	3b94cc71c325f90	a3e5fd5218aa8a	-	FALSE	FALSE	FALSE	FALSE	FALSE	-	TRUE	FALSE	FALSE	FALSE		FALSE	TRUE	FALSE	[]	['joesecurity', 'joes	Trojan:Win32/Nati	UDS:Trojan.Multi.	Artemis!66534E5	win/malicious_cor	TROJ_GEN.R011	a variant of Win32	ML.Attribute.High	-	Mal/Generic-R	Trojan.GenericKD.36928994
136f4083b67bc8d	malicious	APT_APT29_NOBELIUM_NativeZone_Loader_May21_	31	Microsoft: Trojan:Win32/Native	NativeCacheSvc.I	#############	#############	Win32 DLL	a707f6bd9c96423	91f9ee61662317	136f4083b67bc8d	f200d189ba41ff2	-	FALSE	FALSE	FALSE	FALSE	FALSE	-	TRUE	FALSE	FALSE	FALSE		FALSE	FALSE	FALSE	[]	['-']	Trojan:Win32/Nati	-	Artemis!A707F6B	win/malicious_cor	TROJ_GEN.R002	a variant of Win32	Trojan.Gen.2	-	-	Trojan.GenericKD.46329626