VALKYRIE COMODO

Summary

File Name: 1.exe

File Type: PE32 executable (GUI) Intel 80386, for MS Windows

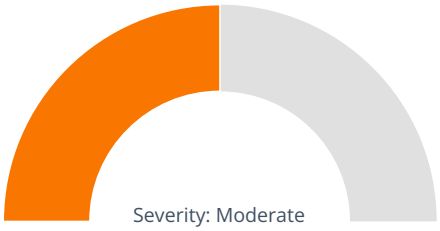
SHA1: fb608457bdf2def8455bdba2909496290fd25234

MD5: 6d46d6311c2c3abcea5de4288c4fcef5

MALWARE

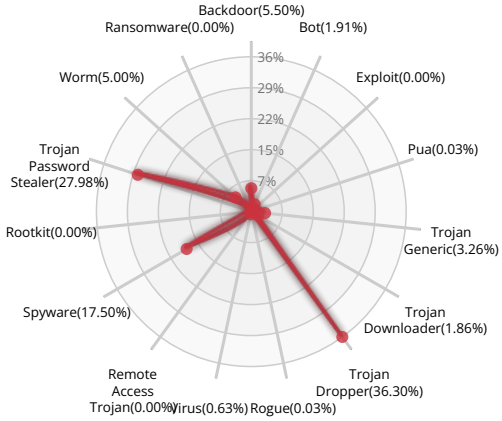
Valkyrie Final Verdict

DETECTION SECTION

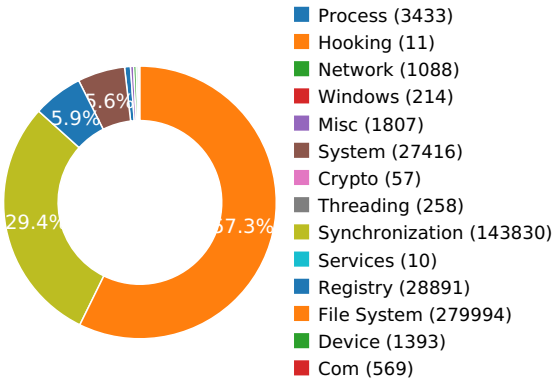


Verdict: Malware

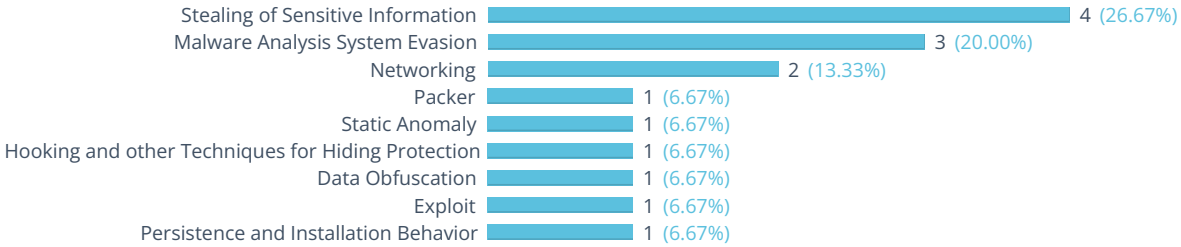
CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW



VALKYRIE COMODO

Activity Details

NETWORKING

- Attempts to connect to a dead IP:Port (12 unique times) — Show sources
- Network activity contains more than one unique useragent. — Show sources

PACKER

- The binary likely contains encrypted or compressed data. — Show sources

STEALING OF SENSITIVE INFORMATION

- Attempts to modify Internet Explorer's start page
- Sniffs keystrokes — Show sources
- Collects information to fingerprint the system
- Attempts to modify proxy settings

STATIC ANOMALY

- Anomalous binary characteristics — Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

- Creates RWX memory

DATA OBFUSCATION

- Drops a binary and executes it — Show sources

EXPLOIT

- A potential decoy document was displayed to the user — Show sources

PERSISTENCE AND INSTALLATION BEHAVIOR

Installs itself for autorun at Windows startup — Show sources

MALWARE ANALYSIS SYSTEM EVASION

A process created a hidden window — Show sources

Installs an hook procedure to monitor for mouse events

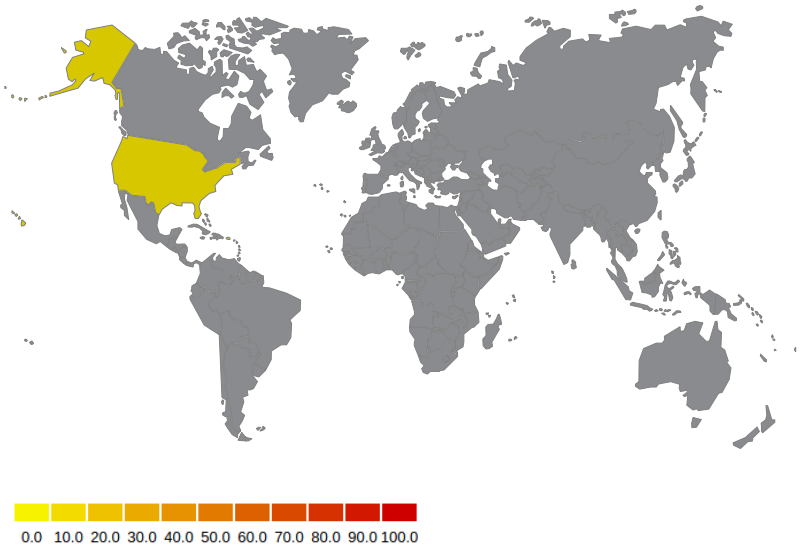
Creates a hidden or system file — Show sources

Behavior Graph

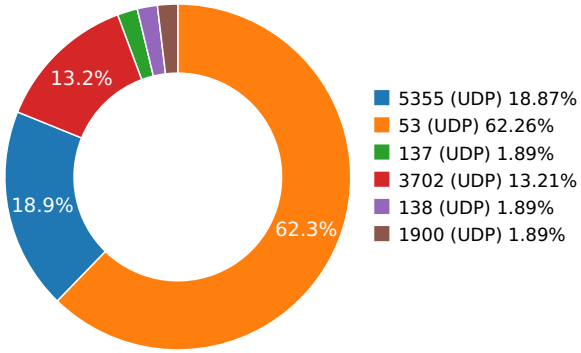
Behavior Summary

Network Behavior

CONTACTED IPS



NETWORK PORT DISTRIBUTION



Name	IP	Country	ASN	ASN Name	Trigger Process Type
assets.adobedtm.com	23.193.53.212	United States	20940	Akamai Technologies, Inc.	Malware Process
www.microsoft.com	23.192.42.35	United States	20940	Akamai Technologies, Inc.	Malware Process
api.bing.com	13.107.5.80	United States	8068	Microsoft Corporation	Malware Process
go.microsoft.com	23.199.12.142	United States	16625	Akamai Technologies, Inc.	Malware Process
crl.microsoft.com	204.2.211.8	United States	35994	NTT America, Inc.	Malware Process
www.adobe.com	23.208.39.244	United States	3257	Akamai Technologies, Inc.	Malware Process
query.prod.cms.rt.microsoft.com	23.208.52.148	United States	3257	Akamai Technologies, Inc.	Malware Process
ipv6.msftncsi.com					Malware Process
mail.vfemail.net	199.16.11.151	United States	53264	Continuum Data Centers, L...	Malware Process
teredo.ipv6.microsoft.com					Malware Process
dns.msftncsi.com	131.107.255.255	United States	3598	Microsoft Corporation	Malware Process
www.bing.com	13.107.21.200	United States	8068	Microsoft Corporation	Malware Process
ctldl.windowsupdate.com	165.254.0.24	United States	2914	NTT America, Inc.	Malware Process
wwwimages.adobe.com	23.193.53.160	United States	20940	Akamai Technologies, Inc.	Malware Process
7536585869444.comuf.com	31.170.163.130	United States	47583	Main Hosting Servers	Malware Process
ocsp.msocsp.com	198.41.214.186	United States	13335	Cloudflare, Inc.	Malware Process
mscrl.microsoft.com	72.21.81.200	United States	15133	MCI Communications Servi...	Malware Process
ocsp.omniroot.com	72.21.91.8	United States	15133	MCI Communications Servi...	Malware Process
ieonline.microsoft.com	204.79.197.200	United States	8068	Microsoft Corporation	Malware Process

DNS QUERIES

Request	Type
teredo.ipv6.microsoft.com	A
dns.msftncsi.com	A
ipv6.msftncsi.com	A
www.microsoft.com	A
crl.microsoft.com	A
ctldl.windowsupdate.com	A
go.microsoft.com	A
api.bing.com	A
www.bing.com	A
7536585869444.comuf.com	A
ocsp.omniroot.com	A
ocsp.msocsp.com	A
mscrl.microsoft.com	A
query.prod.cms.rt.microsoft.com	A
www.adobe.com	A
wwwimages.adobe.com	A
ieonline.microsoft.com	A
assets.adobedtm.com	A
mail.vfemail.net	A

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
0.791882038116	Sandbox	239.255.255.250	3702
0.818961143494	Sandbox	239.255.255.250	3702
0.824480056763	Sandbox	224.0.0.252	5355
0.868231058121	Sandbox	239.255.255.250	3702
0.876621007919	Sandbox	224.0.0.252	5355
0.897186994553	Sandbox	224.0.0.252	5355
0.920604944229	Sandbox	224.0.0.252	5355
0.939716100693	Sandbox	239.255.255.250	3702
1.07288312912	Sandbox	224.0.0.252	5355
1.14214396477	Sandbox	239.255.255.250	1900
1.91714000702	Sandbox	239.255.255.250	3702
1.91926813126	Sandbox	224.0.0.252	5355
3.11460494995	Sandbox	224.0.0.252	5355

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.16198515892	Sandbox	192.168.56.255	137
3.16295409203	Sandbox	224.0.0.252	5355
3.21122908592	Sandbox	192.168.56.1	53
3.30160212517	Sandbox	224.0.0.252	5355
3.35501503944	Sandbox	192.168.56.1	53
5.33537006378	Sandbox	192.168.56.1	53
5.33670806885	Sandbox	192.168.56.1	53
5.35143709183	Sandbox	192.168.56.1	53
5.48583197594	Sandbox	224.0.0.252	5355
6.3046040535	Sandbox	239.255.255.250	3702
6.37855315208	Sandbox	239.255.255.250	3702
7.54732394218	Sandbox	192.168.56.1	53
9.26640605927	Sandbox	192.168.56.255	138
69.7508039474	Sandbox	192.168.56.1	53
73.2168741226	Sandbox	192.168.56.1	53
77.6543991566	Sandbox	192.168.56.1	53
77.8148269653	Sandbox	192.168.56.1	53
81.0362761021	Sandbox	192.168.56.1	53
159.280334949	Sandbox	192.168.56.1	53
173.634742975	Sandbox	192.168.56.1	53
173.648213148	Sandbox	192.168.56.1	53
187.145159006	Sandbox	192.168.56.1	53
190.004589081	Sandbox	192.168.56.1	53
190.2076931	Sandbox	192.168.56.1	53
192.56351614	Sandbox	192.168.56.1	53
192.672772169	Sandbox	192.168.56.1	53
192.673316956	Sandbox	192.168.56.1	53
192.86086607	Sandbox	192.168.56.1	53
198.559213161	Sandbox	192.168.56.1	53
220.009303093	Sandbox	192.168.56.1	53
222.377439976	Sandbox	192.168.56.1	53
223.916692019	Sandbox	192.168.56.1	53
227.337568045	Sandbox	192.168.56.1	53
227.45797205	Sandbox	192.168.56.1	53
227.458213091	Sandbox	192.168.56.1	53
227.458995104	Sandbox	192.168.56.1	53
229.93740201	Sandbox	192.168.56.1	53

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
234.281342983	Sandbox	192.168.56.1	53
236.157850981	Sandbox	192.168.56.1	53
289.759227991	Sandbox	192.168.56.1	53

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Users\Win7\AppData\Local\Temp\Temp1030.Tmp	**Type :** ASCII text, with CRLF line terminators **MD5 :** d11c6ac375b1d8c287a336de516616f4 **SHA-1 :** a11e43b06bad8f4771b725a921e044473413f78a **SHA-256 :** b4069cf04022a48c3a8586ee882c0664aef7dc06 **SHA-512 :** 531941bb6baee70fe90bc501024265cd6338f262 **Size :** 0.055 Kilobytes.
C:\Users\Win7\AppData\Local\Temp\V1843453.Pdf	**Type :** PDF document, version 1.5 **MD5 :** 5ca089449a75e46616e8d91b752e9744 **SHA-1 :** 1cb3c8d178af11b3ba20ee808e0df723a2976f03 **SHA-256 :** 7a3b87fb25cfed9c7e5e5dbc8891679df962a678 **SHA-512 :** 83cdee8b65ea4b18efc1c905105d5add71690d3 **Size :** 7.458 Kilobytes.
C:\Users\Win7\AppData\Local\Temp\~DF51A559EC05334A87.TMP	**Type :** Composite Document File V2 Document, No summary info **MD5 :** 489e50aa404516847f63429711411119 **SHA-1 :** 2fde96e1efd0c0573c4efe5708e6b807476b0aa4 **SHA-256 :** df31c06be4cfe8db9bf6f997479abfaf775db88f65 **SHA-512 :** 94071ec91a413af393580c123185ce52332b3210 **Size :** 16.384 Kilobytes.
C:\Users\Win7\AppData\Local\Temp\Temp1080.Tmp	**Type :** ASCII text, with CRLF line terminators **MD5 :** b84caf896adc3e32a894c44cf9d0a99c **SHA-1 :** 8742101a6dc9be1036a991472f11e430fe9523ff **SHA-256 :** 7c7f8a38de2fcc084c2b621f3e3494489135aa29a **SHA-512 :** 920e3f00c5d242191b7baac7052e7c5df78126b6 **Size :** 0.138 Kilobytes.
C:\Users\Win7\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\RGC5OOPI\Customized.Min.Fp-6adc3ea48ebc04a48b31c002f512a6e1[1].Css	**Type :** ASCII text, with very long lines **MD5 :** 374ee2cf562a6b1001bec293347efeff **SHA-1 :** e40f7f3555b862b0af46348867e335854e8e8945 **SHA-256 :** da8845dbdf612b7d251f1ea3f8a617ac06b2cf38 **SHA-512 :** 2eb2fe800382bc87b349db4d40e5112c9a610a6f **Size :** 193.836 Kilobytes.
C:\Users\Win7\AppData\Local\Microsoft\Windows\WebCache\V01.Chk	**Type :** data **MD5 :** 7d12f3180a8fc80845c13a58be9ae6d0 **SHA-1 :** 5b7dddabe4d50822ae52119236bf39c3a94a0223 **SHA-256 :** 9beedc7cfee5b92c388eff0aaf9d7e3fa3f997c256 **SHA-512 :** e63acaa503c9d58d674efb11a5db368b005433c0 **Size :** 8.192 Kilobytes.
C:\Users\Win7\AppData\Local\Temp\Temp1001.Tmp	**Type :** ASCII text, with CRLF line terminators **MD5 :** 5867864996fe03426905fc7b09c565c1 **SHA-1 :** a0525054675e66c1c4da384bb937d80c4d5a55ef **SHA-256 :** 23772fac859f7332f4bdb52ed047e0c5965cd2f9b **SHA-512 :** 020a3e20a5081ad2dcad451012cc36f0239f61b6 **Size :** 0.068 Kilobytes.
C:\Users\Win7\AppData\Local\Temp\Temp1009.Tmp	**Type :** Message Sequence Chart (chart) **MD5 :** fba874ccb15f9a5995292ab195a9c289 **SHA-1 :** 63bcb85cdc154158ff925c570843d4dc22e4b9cd **SHA-256 :** 1fb14ec18da75945002ad97840314a36753452d2 **SHA-512 :** 662c9eb2fa8da8059795996cd59bbd1d17ea79f7 **Size :** 0.02 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\Win7\AppData\Local\Temp\Temp777	**Type :** locale data table **MD5 :** 487c7b519dc40f24fd6891a883159813 **SHA-1 :** c965eb4e0c7567f98671fdfcedf319116a8cfe22 **SHA-256 :** be5095f18a9229c910ed9775c867bfd934dd7641 **SHA-512 :** d37c81c9f2a730d0a7281886eb5bc2e95f2d64fb **Size :** 91.419 Kilobytes.
C:\Users\Win7\AppData\Local\Temp\Temp1040.Tmp	**Type :** ASCII text, with CRLF line terminators **MD5 :** 2c5001067856ba2cc2f6cd075a0a1297 **SHA-1 :** 2348a56d75f1f2e3d4562c7c047d367bb2455709 **SHA-256 :** aa80022d2e65ff626008ebb93250efab39c02b97 **SHA-512 :** 25c220df688e1c5da1170ffef26ac43f98155a39f8 **Size :** 0.055 Kilobytes.
C:\Users\Win7\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.Dat	**Type :** data **MD5 :** e67eadd6db4fa3497f868e08f2aeda37 **SHA-1 :** b2fb6881d7385533b01f1c6ca41dafeb879771e3 **SHA-256 :** fc4be2d2a25b6d07a3bddd340cb89c34705f47b9 **SHA-512 :** c3150d2f1cfff45ba33c6443335421f25dff623567 **Size :** 21037.056 Kilobytes.
C:\Users\Win7\AppData\Local\Temp\Temp1005.Tmp	**Type :** ASCII text, with CRLF line terminators **MD5 :** 4404a1dbd4c1a594ec8618e38128f1b9 **SHA-1 :** 83a34971eee368e5ebad68d951cec88e53ac95de **SHA-256 :** a6be451a181c1661608b41bd7ef1bbce90e54fab **SHA-512 :** 5e2b24d762c13550ec292eda635f18316e9b4dd2 **Size :** 1.283 Kilobytes.
C:\Users\Win7\AppData\Local\Temp\Temp1120.Tmp	**Type :** ASCII text, with CRLF line terminators **MD5 :** 8fd4faca98c903dff2858f71790109cd **SHA-1 :** 9f2f8b6ff76061af897c2e8501f5df939e1c7aa0 **SHA-256 :** cff183a9f04dacd9284d31e60892b11ed6244182 **SHA-512 :** dc5679d0065075d4788e50f02dfdb7bdf84411dc **Size :** 0.055 Kilobytes.
C:\Users\Win7\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\RGC5OOPI\SatelliteLib-46e65db5bb0c375f8f64619be31cc9b29acf4867[1].Js	**Type :** ASCII text, with very long lines **MD5 :** 7077450f5184f72ef5f922b269bb9057 **SHA-1 :** cd955a236d3b64484d2f6a464b0214cf86f6a932 **SHA-256 :** 5572144e982849fa509a6f18535896e8c6dd1f26 **SHA-512 :** 9e7ff2e09ce1a3d67d837c829669059dfebb5804 **Size :** 554.37 Kilobytes.
C:\Users\Win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\40E450F7CE13419A2CCC2A5445035A0A_06F02B1F13AB4B11B8FC669BDE565AF1	**Type :** data **MD5 :** 58ce3cc3e7816acd912adceb14db443f **SHA-1 :** a977c2eb5b744cf4593d5efc12da050250825173 **SHA-256 :** c4e7ba2cfb8bb7aa115655ae9ecd1854ed5d86eb **SHA-512 :** d5bbf7b6232e33e285b611c9b9a1c4c4192f911f3 **Size :** 0.4 Kilobytes.
C:\Users\Win7\AppData\Roaming\Microsoft\Windows\Cookies\XZ0FQL3L.Txt	**Type :** ASCII text **MD5 :** dbe97b1b432f6adc3493d0c157fdcc56 **SHA-1 :** ec8339d3578c219323d41c6a21183bed0dc4bc22 **SHA-256 :** d572d6d9d6ac5a2efb41ece8fa105a073ada00e9 **SHA-512 :** f6fbebcc58793dd52e4f0c5d2aa868f2eadc69a2c **Size :** 0.121 Kilobytes.
C:\Users\Win7\AppData\Local\Temp\FBE.ZIP:Zone.Identifier	**Type :** ASCII text, with CRLF line terminators **MD5 :** fbccf14d504b7b2dbcb5a5bda75bd93b **SHA-1 :** d59fc84cdd5217c6cf74785703655f78da6b582b **SHA-256 :** eacd09517ce90d34ba562171d15ac40d302f0e69 **SHA-512 :** aa1d2b1ea3c9de3ccadb319d4e3e3276a2f27dd1 **Size :** 0.026 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\Win7\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{0AA4135F-EF05-11E6-83DC-08002748697D}.Dat	**Type :** Composite Document File V2 Document, No summary info **MD5 :** f36edd063c75c88c60875b3fc40ab924 **SHA-1 :** eefd62909024cb568c3aafb4656ba76205f733d9 **SHA-256 :** c11e10e7c481a6f6038bb8a58cfdb4125da71cd4 **SHA-512 :** c4d2d9a52a4e998e1316377890b216f790cf6598 **Size :** 5.632 Kilobytes.
C:\Users\Win7\AppData\Local\Microsoft\Windows\Temporary Internet Files\Counters.Dat	**Type :** data **MD5 :** 578f4544ee22e649e53566fd31420f2a **SHA-1 :** d904ac8cb6bbba8f53cc1026b69b147caf919e74 **SHA-256 :** 7dc0115a55acd1e67dd587d30e4749e5abd836d **SHA-512 :** 0628d2a8f986bdeb2346222a1aedaf43af4edcd4 **Size :** 0.128 Kilobytes.
C:\Users\Win7\AppData\Local\Temp\~DF34F0BF39205F46E9.TMP **C:\Users\Win7\AppData\Local\Temp\~DF4A077BF69D4CF608.TMP** **C:\Users\Win7\AppData\Local\Temp\~DFBC78CC6BEA712B6F.TMP**	**Type :** Composite Document File V2 Document, No summary info **MD5 :** 4c93c63cd7523b5b15da8581ac483000 **SHA-1 :** b17e104f164bfc1d42271db0611367ab1bca8897 **SHA-256 :** 684b1eb121871c36787d9608c9499358d78c3c6 **SHA-512 :** ac09b59fc751593457635c2151b12cff672c56822 **Size :** 16.384 Kilobytes.
C:\Users\Win7\AppData\Local\Temp\Temp1005.Tmp	**Type :** ASCII text, with very long lines, with CRLF line terminators **MD5 :** f1a3421bb5497d9b275e2b8ca1d17d21 **SHA-1 :** 331da308f196ace6caf89e860320ae2ea59356ca **SHA-256 :** 343b47a9d7f892b35c8f610a64e0bf0700842a8b **SHA-512 :** 222d2f6efccea72dd3e97342bb356ec2e2093c23 **Size :** 1.922 Kilobytes.
C:\Users\Win7\AppData\Local\Temp\Temp1004.Tmp	**Type :** ASCII text, with CRLF line terminators **MD5 :** 22920780aa0dc077f82aa8f865f39910 **SHA-1 :** 40783b98d0183a52d33a431120a3f8fbd9cda48c **SHA-256 :** f7c4f4cc6c99f0e5d21986eaf4e0ee5170b03b05b **SHA-512 :** 0dba13c193143d5c13a3eeedf88ffb1a3e94b5d6 **Size :** 0.004 Kilobytes.
C:\Users\Win7\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\89Q863BS\Suggestions[1].En-US **C:\Users\Win7\AppData\Local\Microsoft\Internet Explorer\DomainSuggestions\En-US.2**	**Type :** data **MD5 :** 5a34cb996293fde2cb7a4ac89587393a **SHA-1 :** 3c96c993500690d1a77873cd62bc639b3a10653f **SHA-256 :** c6a5377cbc07eece33790cfc70572e12c7a48ad82 **SHA-512 :** e1b7d0107733f81937415104e70f68b1be6fd0ca **Size :** 18.176 Kilobytes.
C:\Users\Win7\AppData\Local\Temp\Temp1090.Tmp	**Type :** ASCII text, with CRLF line terminators **MD5 :** 1093f673276be441db9e281c0c038236 **SHA-1 :** 9f1757875f890537cf66a10d5d73b0fe8c8e5438 **SHA-256 :** eab085f8031658a858a61d9fa025ee6a4e493d8b **SHA-512 :** 20e7935c15fe00d24536ad58450f451824aa9e72 **Size :** 0.109 Kilobytes.
C:\Users\Win7\AppData\Local\Temp\Msavhost.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 38489fea73599f23b3abd8168ac3e9d0 **SHA-1 :** d8eb6aa56476f921b81d2b428ffed84bb08677b9 **SHA-256 :** 6848ac63649274eb2ab2d93bb48924b685ea90d **SHA-512 :** ed96d53eb1e26cdcb8627dedebeaa6e714bfeba **Size :** 32.768 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\Win7\AppData\Local\Microsoft\Windows\WebCache\V010001A.Log	**Type :** data **MD5 :** d10eb4865d376258fdcb4964af76df67 **SHA-1 :** 220943dda4293e3ca768194e18e76280d5187b44 **SHA-256 :** c7dc6789f166d28b67631e7f55e81666f1bedf4b6 **SHA-512 :** b2f7b2171d3bc303216f90e90cd6431a5c710d9e **Size :** 524.288 Kilobytes.
C:\Users\Win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\B912B2C6928A18B8CD7D50CF08BEA95B_F85B8279FA54A31CEEC2563F5A8F73E8	**Type :** data **MD5 :** 38e2936ccf3daf9b60c56cb15fed6bdb **SHA-1 :** 748f196121d3eabb10e0868b0c6c1e7faa871cd8 **SHA-256 :** dea1e73c83a38e06c4a8097c130b797c29d4883(**SHA-512 :** 1cf19f226db4b05cc17b8627edabbf332b7b9f811 **Size :** 1.82 Kilobytes.
C:\Users\Win7\AppData\Local\Microsoft\Windows\WebCache\V010001B.Log	**Type :** data **MD5 :** 1c25d8a220bf0c16a3aed97f97fbc925 **SHA-1 :** 8cd8f463482f6f956a76b1bcf92be4a939d3820d **SHA-256 :** 3d933e2ba47b67dba5b1bdc43db34f874b633ba **SHA-512 :** 4325368287a42b6fe6b205ba4b14785af133f098 **Size :** 524.288 Kilobytes.
C:\Users\Win7\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\RGC5OOPI\Thirdparty-New.Min.Fp-C24078be2ad301563ba7d6eb90204ef3[1].Css	**Type :** ASCII text **MD5 :** 1e426576474b356877191024ef5df065 **SHA-1 :** 76fdf71455681d1a2dc684783a6e841e82fd654a **SHA-256 :** 7deaae6889260ab6abe16c1dcfc485e2dddd4472 **SHA-512 :** 3c8b1c58d31c31a48a9d91590492bc113443fc91 **Size :** 0.793 Kilobytes.
C:\Users\Win7\AppData\Local\Temp\~DFD57A45D883C60F3E.TMP	**Type :** Composite Document File V2 Document, No summary info **MD5 :** 32ad42b2778e3da30228694c0f7b50ed **SHA-1 :** eeb9e8e94881bb4ffef3f2317c1e5f3cabfd18e6 **SHA-256 :** cd53c19a9843bcfe11348e16a6ee328d16f611ff8 **SHA-512 :** 9f0b4c38e49c5049ea7bd01b9342c811e9c87f30 **Size :** 114.688 Kilobytes.
C:\Users\Win7\AppData\Local\Temp\Temp1010.Tmp	**Type :** ASCII text, with CRLF line terminators **MD5 :** 8137323aa1bbef916333b0e97535d0b9 **SHA-1 :** 450452d38a0fc5620d327db32538a2a261121151 **SHA-256 :** 439ee5082c97f4f890eb4d233212eacb73807655 **SHA-512 :** 5a5f40284ae11857cd70b55da9331fc8bc2ef553(**Size :** 0.116 Kilobytes.
C:\Users\Win7\AppData\Local\Temp\Mscvhost.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** be1dbc241b0f896af1a11dce2de70720 **SHA-1 :** 8bc461717aa99a401d96e16c379d0c520bcd5ed0 **SHA-256 :** 879226bc5f8159e06bbb7a8c37258b81b07c13c5 **SHA-512 :** fa1391cf214a9be3a297ebc40879f3381cdd1945 **Size :** 118.784 Kilobytes.
C:\Users\Win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\CAEDF689AA6DC9642B833051B2B77D1A **C:\Users\Win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\0D704203BDA0CEEDCD2BBB4ACE02F586**	**Type :** data **MD5 :** ae0d9e894fcab61d793bf0c67e43917b **SHA-1 :** ae46496a87ce220af8950d844b1c04210b4bfca8 **SHA-256 :** ce3c1314985fc2617310ebfff6b558b2dbe282f2c **SHA-512 :** b7ec278f4658178be992cb6d4e7316c722b7edaf **Size :** 198.591 Kilobytes.
C:\Users\Win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\B912B2C6928A18B8CD7D50CF08BEA95B_F85B8279FA54A31CEEC2563F5A8F73E8	**Type :** data **MD5 :** 9198f199b256681657bfe5dde78560e4 **SHA-1 :** 6a0286ca55f1e7455af195772e67a5e5f8e1c24f **SHA-256 :** 380b29a879eaf940acd415b1f278e0cf800146f37 **SHA-512 :** 6ad6d748a8375ecf43e033b36a1597d8b3238d8 **Size :** 0.486 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\Win7\AppData\Local\Temp\Temp1130.Tmp	**Type :** ASCII text, with CRLF line terminators **MD5 :** 39dca5d49b07256be07dfddb8c76c325 **SHA-1 :** 7c35c9538a63759791f345c4373f7ec7bffb24ce **SHA-256 :** 3c687df53689c1afbbc3b6440543cddbe27d5a29 **SHA-512 :** 6c7cce6c6f2100e8850ac9d4b271b450ead3680a **Size :** 0.127 Kilobytes.
C:\Users\Win7\AppData\Local\Temp\Temp1002.Tmp	**Type :** Non-ISO extended-ASCII text, with CRLF line terminators **MD5 :** 223e3e58aae4ca375e5f8dff8f0b5a53 **SHA-1 :** 04bc7118a00f00de54a7f51e136be4e7671d57a2 **SHA-256 :** b3e50dd689e5e50387278395f809bd85d5c2d42 **SHA-512 :** bb7a109fa0117963dfdd5850014f0f38b08ef65a0 **Size :** 0.264 Kilobytes.
C:\Users\Win7\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\H0G27RVV\Adobe.Min.Fp-F0eb85c1a739a56d2bf759368083f70b[1].Css	**Type :** ASCII text **MD5 :** 9a91f3358c8bc51738a8dc7bb31ba7b1 **SHA-1 :** 201087feaeecc57099a62e402904462e6327c94f **SHA-256 :** 2ac2e18398ce0709d06effb1eb20799a14032561 **SHA-512 :** 4ac7403d8bdbe5674307279150fc8d871f3292f4 **Size :** 1.816 Kilobytes.
C:\Users\Win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\CAEDF689AA6DC9642B833051B2B77D1A	**Type :** data **MD5 :** 5edd76f59e9d7c704baaac0de4b32c65 **SHA-1 :** 0b9403ac6a43cbc5ba2cf3c82295c1c454867aec **SHA-256 :** 7cab8ebbec5fb21f6ea5f4ecc879c01c45bf3e738 **SHA-512 :** 53293b5484126e8907a83bf4f969d9347f4506b1 **Size :** 0.266 Kilobytes.
C:\Users\Win7\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\RGC5OOPI\Htmlselectionconfig-2_2-Win7[1].Xml **C:\Users\Win7\AppData\Local\Microsoft\Internet Explorer\EUPP\HTMLSelectionConfig.Xml**	**Type :** XML document text **MD5 :** 92bb55734dae8fbafd70a64b23e58a8e **SHA-1 :** 79b7067a38413605f5bf7e9c61d24bc4bd4b4c3a **SHA-256 :** 1a4d81fd258ec9669bf53b015230fca510855e3b **SHA-512 :** 0352c8d7626b287dcc8e3e1f33fa995617069b7b **Size :** 7.297 Kilobytes.
C:\Users\Win7\AppData\Local\Temp\Temp1111.Tmp	**Type :** HTML document, Non-ISO extended-ASCII text, with very long lines, with CRLF, LF line terminators **MD5 :** 131585c0a504a689a921283ac4e4bc36 **SHA-1 :** 871b349d17903f8804e032929d4e471c69ea2a1d **SHA-256 :** 0bcb3af552c32e540c42177cc36ede950a42431e **SHA-512 :** cb4ab1a1b3c36c9c57f27fa5ef247cbfebaef7ed0c **Size :** 2.559 Kilobytes.
C:\Users\Win7\AppData\Local\Temp\Temp1003.Tmp	**Type :** Non-ISO extended-ASCII text, with CRLF line terminators **MD5 :** 48e97051bf9198dce0bc94282bb4b1fc **SHA-1 :** 6ddc2329a2a5cca7f1b318e251bc82fb7f3b6093 **SHA-256 :** acd1d6889151ea65a5e83ffb468632c41a27bf14 **SHA-512 :** 5c9c2f6d8cdf0d99c50e72728f53724b52101e6e8 **Size :** 0.293 Kilobytes.
C:\Users\Win7\AppData\Local\Temp\FBE.ZIP	**Type :** Zip archive data, at least v2.0 to extract **MD5 :** 4e110ffd5437152b851f7bf02974c6ad **SHA-1 :** 0007578cb6ab31cf5394ca9caa308da3d8a7356f **SHA-256 :** ad67d1aa37a709d2917de37aa48ccec67e87f22f **SHA-512 :** a85d9f5671fef471c821deb45644eb7e1deb1cbb **Size :** 91.092 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\Win7\AppData\Local\Temp\Temp1140.Tmp	**Type :** ASCII text, with CRLF line terminators **MD5 :** 69f8f295ff90974af544d1d93286c43f **SHA-1 :** d84ed3a52c429b73611c38d97c8fe0509fb2c76b **SHA-256 :** c20c1aa1db225e464c03d66589ef55bcff15f029c **SHA-512 :** ca59fb74d2c14d244e9bdec15dc55c5b38960851 **Size :** 0.055 Kilobytes.
C:\Users\Win7\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{0AA41361-EF05-11E6-83DC-08002748697D}.Dat	**Type :** Composite Document File V2 Document, No summary info **MD5 :** b47c599fc05e086dc882a353e8bda660 **SHA-1 :** ab2242b5fc01deed0d92d63e2db049408375cd2a **SHA-256 :** 1a31fd1e4a0e0413ff78166a4b389c63db8d3b56 **SHA-512 :** ddc00bb8dbff65140c67c10722f842dd7ba18045 **Size :** 4.096 Kilobytes.
C:\Users\Win7\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Windows 10 Updater.Lnk	**Type :** MS Windows shortcut, Item id list present, Has Relative path, ctime=Sun Dec 31 21:00:00 1600, mtime=Sun Dec 31 21:00:00 1600, atime=Sun Dec 31 21:00:00 1600, length=0, window=hide **MD5 :** 93748299d76482007d476695f2d54992 **SHA-1 :** 8654b4cdb246f0955be64aa756f2d6c81128b694 **SHA-256 :** 2afb88388fa44c1f0b0cdc18a92dc128aa5e3f586 **SHA-512 :** af30bbf32e0270e3ca89906eb94dfb02404b7b02 **Size :** 0.884 Kilobytes.
C:\Users\Win7\AppData\Local\Temp\Temp1100.Tmp	**Type :** ASCII text, with CRLF line terminators **MD5 :** 515bd02c465d6da62c140be013c67dab **SHA-1 :** 83e3fa712ba0a1286dfcb8abc3fcc8b53811ff2a **SHA-256 :** eb1ec8fe8866133b436596796ca804fc5196c9ce **SHA-512 :** 17f6e99f1bbb71fd7e355ce8339723fa02bd6518 **Size :** 0.065 Kilobytes.
C:\Users\Win7\AppData\Local\Microsoft\Windows\WebCache\V01.Log	**Type :** data **MD5 :** e24d76b4d48d4bec4f26a57d4ff7fa0e **SHA-1 :** 20d19484ba80d679616c13281f128a73a1910e88 **SHA-256 :** 431337abd2575946af7ba619474233e8f44282c6 **SHA-512 :** ea8535c418ce9d666aa0aff94e5712404958f81f5 **Size :** 524.288 Kilobytes.
C:\Users\Win7\AppData\Local\Temp\Temp1020.Tmp	**Type :** ASCII text, with CRLF line terminators **MD5 :** e27e030e0a4c32d1bfcd268b12b8079a **SHA-1 :** 62fe94ddd2844ba231f48b14944a3f2059510e57 **SHA-256 :** 753b58df3311b10430da026eb8c6155a9c19c172 **SHA-512 :** fcb71591d9a0a993684b14e5f5c2007f72039d9c **Size :** 0.126 Kilobytes.
C:\Users\Win7\AppData\Local\Temp\Temp1050.Tmp **C:\Users\Win7\AppData\Local\Temp\Temp1060.Tmp**	**Type :** ASCII text, with CRLF line terminators **MD5 :** 4c1a79e4a210f2e4644a37449f62a7b3 **SHA-1 :** c59196233cd866412ba4732140e3b723035521fe **SHA-256 :** 5c1126e951fc894a91d18d9598994f232ce8c49b **SHA-512 :** 985eb75be2ebbfad76ef55f010778159cdc9875a **Size :** 0.111 Kilobytes.
C:\Users\Win7\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\RGC5OOPI\Aceui-Reimagine.Min.Css.Fps.Fp-87b61d14d6b29950b34d3e4e493b9c47[1].Css	**Type :** ASCII text, with very long lines **MD5 :** 87b61d14d6b29950b34d3e4e493b9c47 **SHA-1 :** 4dfb0459e32c51048e4101471e3b38f35eed1cfe **SHA-256 :** 317e136411768a86c84bb5a72ddedc0fbf021a33 **SHA-512 :** 190c652b21fd9e079bc214e64d9583511fd239df **Size :** 858.47 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\Win7\AppData\Local\Temp\Temp1070.Tmp	**Type :** ASCII text, with CRLF line terminators **MD5 :** dfd27357c710e2e1aa7ffb250a5521c9 **SHA-1 :** 5939c1c42dda9737b77ca042e5805ade142efc87 **SHA-256 :** 1f105bfa4c155022b16244455f70e0ecd1ba232ef **SHA-512 :** 880a9afc5e4fa835dfef9d5ed51476b0ae5b52abc **Size :** 0.116 Kilobytes.
C:\Users\Win7\AppData\Local\Temp\Temp1000.Tmp	**Type :** ASCII text, with CRLF line terminators **MD5 :** 74cb26f4f4ecc9673646190bdc4c8290 **SHA-1 :** c017971c31bdcc9ba13a283764972dde1f5fd2c2 **SHA-256 :** 1530547f0e7b57bbc2c76fdd44bce977d8909d60 **SHA-512 :** 120feb60d98ddff9b7ef874b4d8008d174c9ccd39 **Size :** 0.076 Kilobytes.
C:\Users\Win7\AppData\Local\Microsoft\Windows\WebCache\V010001C.Log	**Type :** data **MD5 :** 5950d2ec33af8ce6e816b3212dd48fc6 **SHA-1 :** 14833eeaf9c6d126117809acaeebb94ebe4b2b08 **SHA-256 :** 1a0481aa630a7160af54d0e5650b4b27cd985b53 **SHA-512 :** 906b2675232b7d5de67561036976846a3c9a678 **Size :** 524.288 Kilobytes.
C:\Users\Win7\AppData\Local\Temp\Temp1110.Tmp	**Type :** ASCII text, with CRLF line terminators **MD5 :** 13942f0086e50168462f4c5dee166d46 **SHA-1 :** 5264c0427503a58e0a632de7ea6e08a7080f1b1a **SHA-256 :** ad369e516f03fa929bb0699564a27c548066da15 **SHA-512 :** 2ec4f78ddec74c24ca58538638197c949fc98b24c **Size :** 0.119 Kilobytes.
C:\Users\Win7\AppData\Local\Temp\Files.Zip **C:\Users\Win7\AppData\Local\Temp\Temp1998.Zip**	**Type :** Zip archive data, at least v2.0 to extract **MD5 :** e141527d6f07150b8f35615bf896e60e **SHA-1 :** 221664001c3216b99b43ce3ef34ccdf617bc9270 **SHA-256 :** 8ea2d8fdda26ab659fdcb807f96c3b02eca62b01 **SHA-512 :** 26e2b22024cade12305deaabda91827bb1b3988 **Size :** 91.093 Kilobytes.
C:\Users\Win7\AppData\Local\Temp\Taskmgr.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 4e915fbe54c3fa26d9a188cbe770f39d **SHA-1 :** 43556ba6ed14c6a430999126f0d775c1bc2756da **SHA-256 :** f1ef59570bada74723878f764146370e9e92ffe54 **SHA-512 :** 33088c3adfc5bdd5c4255c8695203ef77571e127 **Size :** 139.264 Kilobytes.
C:\Users\Win7\AppData\Local\Microsoft\Windows\WebCache\V0100017.Log	**Type :** data **MD5 :** 17001e7faf54159d6e17c9c79fda2cd2 **SHA-1 :** bc17b484501e3283d548dd0f85c60f0ca014f31d **SHA-256 :** 129111ed31810cbcff3c3f0316359a43164d85134 **SHA-512 :** c3360287aab98c48deae9aa97e2f77d4eb89f27e **Size :** 524.288 Kilobytes.
C:\Users\Win7\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{0AA41362-EF05-11E6-83DC-08002748697D}.Dat	**Type :** Composite Document File V2 Document, No summary info **MD5 :** 895bfb5654a645c35670d0aa14a0c911 **SHA-1 :** 0ffa8555b7aa8a6b3d0b717dfc24a42afeaee217 **SHA-256 :** 0275334539d65da8ea14fc0d69a90165924b0f57 **SHA-512 :** 2ab3778776940dd474f1b192715484a564ad87c **Size :** 3.584 Kilobytes.

FILE PATH	TYPE AND HASHES

C:\Users\Win7\AppData\Local\Temp\~DF0271C9A74CD3FBC6.TMP	**Type :** Composite Document File V2 Document, No summary info
	MD5 : 0e3f307845cbe4f30c680427c681313c
	SHA-1 : 22dc624a1381aaa8e8885de690faa3119334a67b
	SHA-256 : 1cd9f96e1a40c84ebc642f955b0a2aebe1e8f241{
	SHA-512 : 4fb661513190b27f3f96fb44591e1243bfdf7bb4f{
	Size : 94.455 Kilobytes.

C:\Users\Win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\40E450F7CE13419A2CCC2A5445035A0A_06F02B1F13AB4B11B8FC669BDE565AF1	**Type :** data **MD5 :** 6f1e29ce6189fb0eddc56ac3b5821533 **SHA-1 :** b9e863132e8c9d354e2917507d934ede9448a8b7 **SHA-256 :** 2c4296707358eb99deef947e8b7f017cd5ee6a9a **SHA-512 :** 0060bbba0ab529fde5723b9cb29da175c579705{ **Size :** 2.92 Kilobytes.
C:\Users\Win7\AppData\Local\Temp\Temp1006.Tmp	**Type :** ASCII text, with CRLF line terminators **MD5 :** 04bf2421ec29f2a03c671afe159d6c94 **SHA-1 :** f1805f0de17c0d2b5c89e0ec1460e01096c3df78 **SHA-256 :** 576e1c3b79198943583e280c5749279a25a2429{ **SHA-512 :** 6ce4e7e7e8288979daac324cdc10ea15dce2ae3c **Size :** 0.29 Kilobytes.
C:\Users\Win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\0D704203BDA0CEEDCD2BBB4ACE02F586	**Type :** data **MD5 :** 6e22ad9cfc1bdab8c8b48ba9b07438f7 **SHA-1 :** 335e24db8a411dcb6902654d38366809bb1c6521 **SHA-256 :** 86f190ead7d351e0aa1c3fa776f00586a3c1730b4 **SHA-512 :** 6d50c9cbac5ff39243ff4e5ff6157e51f0e7fa461b6 **Size :** 0.262 Kilobytes.
C:\Users\Win7\AppData\Local\Microsoft\Windows\WebCache\V0100018.Log	**Type :** data **MD5 :** 54850995815c54af3357b8d46a16191b **SHA-1 :** 1d15553ca6878522263d33556107b4e5a64cc039 **SHA-256 :** 053523597e230010370965376698b4ee59555f3{ **SHA-512 :** 1c119322490a71dfcee67c8eb0447523ffc72a773 **Size :** 524.288 Kilobytes.

C:\Users\Win7\AppData\Local\Temp\Temp1111.Tmp	**Type :** Non-ISO extended-ASCII text, with very long lines, with CRLF line terminators
	MD5 : d58bcce44b96c1799d28df2080d53573
	SHA-1 : 210335f7058316e7f5903341bfe29858f30c217c
	SHA-256 : 9a93933881b2a623a13f08949162b2852152761{
	SHA-512 : 4f1998e96dc3fa232ada502425f681b104435810{
	Size : 2.24 Kilobytes.

C:\Users\Win7\AppData\Local\Microsoft\Windows\WebCache\V0100019.Log	**Type :** data **MD5 :** 2d449769d0ca91d4fbd06c74a94309d7 **SHA-1 :** 589cc8535ed3a99016fb868f975ec1b207fc23f6 **SHA-256 :** 7da16bb8c5a22a07fcf98036efcce25f4869e63de{ **SHA-512 :** 05e4e28fb4832bc280c4d54792e9d747ee237904 **Size :** 524.288 Kilobytes.

C:\Users\Win7\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\89Q863BS\BS23H4EQ.Htm	**Type :** HTML document, ASCII text, with very long lines
	MD5 : 9b539154a07531fb05e2ae4bed444aeb
	SHA-1 : 5d19a3beeb8495ff59c09de2be39c032f46ed581
	SHA-256 : cd7cf002d560c4828b4dcc745bc5cd27c3a06b76{
	SHA-512 : 5967bb5b9a45db31322bc4c2cd5f8c83d229079{
	Size : 135.229 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	1.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	fb608457bdf2def8455bdba2909496290fd25234
MD5:	6d46d6311c2c3abcea5de4288c4fcef5
First Seen Date:	2016-09-10 22:37:28.375940 (8 years ago)
Number Of Clients Seen:	5
Last Analysis Date:	2017-02-07 17:01:34.428663 (7 years ago)
Human Expert Analysis Date:	2017-01-19 12:16:30.260349 (7 years ago)
Human Expert Analysis Result:	Malware

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Number Of Sections	3
Compilation Time Stamp	0x57C4219E [Mon Aug 29 11:50:54 2016 UTC]
Translation	0x0409 0x04b0
InternalName	13.3.be.doc
FileVersion	1.00
CompanyName	oa
ProductName	PDFree
ProductVersion	1.00
OriginalFilename	13.3.be.doc.scr
Entry Point	0x4015f0 (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	131073
Sha256	bd78f34c238d0026657fb44dac52c426d0f00a4b7462563b00cc0b3d0ba8f6d5
Mime Type	application/x-dosexec

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x1c898	0x1d000	7.621576[SUSPICIOUS]	-
.data	0x1e000	0xa74	0x1000	0.000000	-
.rsrc	0x1f000	0x764	0x1000	1.858267	-

PE Imports

- MSVBVM60.DLL
  - __vbaStrI2
  - _CIcos
  - _adj_fptan
  - __vbaFreeVar
  - __vbaStrVarMove
  - __vbaEnd
  - __vbaFreeVarList
  - __vbaPut3
  - _adj_fdiv_m64
  - __vbaNextEachVar
  - _adj_fprem1
  - None
  - __vbaResume
  - __vbaStrCat
  - __vbaSetSystemError
  - __vbaHresultCheckObj
  - __vbaNameFile
  - _adj_fdiv_m32

- None
- __vbaLateMemSt
- __vbaExitProc
- None
- __vbaOnError
- __vbaObjSet
- _adj_fdiv_m16i
- __vbaObjSetAddref
- _adj_fdivr_m16i
- None
- _CIsin
- __vbaVarZero
- __vbaChkstk
- __vbaFileClose
- EVENT_SINK_AddRef
- None
- __vbaStrCmp
- __vbaVarTstEq
- __vbaGet4
- __vbaObjVar
- DllFunctionCall
- _adj_fpatan
- EVENT_SINK_Release
- None
- _CIsqrt
- EVENT_SINK_QueryInterface
- __vbaExceptHandler
- __vbaPrintFile
- _adj_fprem
- _adj_fdivr_m64
- None
- None
- __vbaFPException
- None
- None
- None
- _CIlog
- __vbaErrorOverflow
- __vbaFileOpen
- __vbaNew2
- __vbaVarLateMemCallLdRf
- None
- _adj_fdiv_m32i
- _adj_fdivr_m32i
- __vbaStrCopy
- __vbaFreeStrList
- None
- _adj_fdivr_m32
- _adj_fdiv_r
- None
- None
- None
- None
- __vbaLateMemCall
- __vbaVarDup
- __vbaStrToAnsi
- __vbaVarLateMemCallLd
- __vbaLateMemCallLd
- _CIatan
- __vbaStrMove
- __vbaForEachVar
- __vbaPutFxStr4
- _allmul
- _CItan
- None
- __vbaAryUnlock
- _CIexp
- __vbaMidStmtBstr
- __vbaFreeObj
- __vbaFreeStr

PE Resources

RT_ICON
RT_GROUP_ICON

RT_VERSION

CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

SCREENSHOTS