Part I. Russian APT - APT28 collection of samples including OSX XAgent

contagiodump.blogspot.de/2017/02/russian-apt-apt28-collection-of-samples.html

This post is for all of you, Russian malware lovers/haters. Analyze it all to your heart's content. Prove or disprove Russian hacking in general or DNC hacking in particular, or find that "400 lb hacker" or nail another country altogether. You can also have fun and exercise your malware analysis skills without any political agenda.

The post contains malware samples analyzed in the APT28 reports linked below. I will post APT29 and others later.

Read about groups and types of targeted threats here: Mitre ATT&CK

List of References (and samples mentioned) listed from oldest to newest:

Download

Download sets (matching research listed above). Email me if you need the password

Download all files/folders listed (72MB)

Sample list

Parent Folder	File Name (SHA1)
APT28	APT28_2011-09_Telus_Trojan.Win32.Sofacy.A
APT28_2011-09_Telus_Trojan.Win32.Sofacy.A	28F21E96E0722DD6FC7D6E1275F352BD060ADE0D
APT28_2011-09_Telus_Trojan.Win32.Sofacy.A	72CFD996957BDE06A02B0ADB2D66D8AA9C25BF37
APT28_2011-09_Telus_Trojan.Win32.Sofacy.A	AC6B465A13370F87CF57929B7CFD1E45C3694585
APT28_2011-09_Telus_Trojan.Win32.Sofacy.A	C01B02CCC86ACBD9B266B09D2B693CB39A2C6809
APT28	APT28_2014-08_MhtMS12-27_Prevenity
APT28_2014-08_MhtMS12-27_Prevenity	33EEC0D1AE550FB33874EDCE0138F485538BB21B__.mht_
APT28_2014-08_MhtMS12-27_Prevenity	8DEF0A554F19134A5DB3D2AE949F9500CE3DD2CE_filee.dll_
APT28_2014-08_MhtMS12-27_Prevenity	A8551397E1F1A2C0148E6EADCB56FA35EE6009CA_coreshell.dll_
APT28_2014-08_MhtMS12-27_Prevenity	E338A57C35A4732BBB5F738E2387C1671A002BCB_advstorshell.dll_
APT28	APT28_2014-10_Fireeye_A_Window_into_Russia_Cyber_Esp.Operations
APT28_2014-10_Fireeye_A_Window_into_Russia_Cyber_Esp.Operations	367D40465FD1633C435B966FA9B289188AA444BC__tmp64.dat_
APT28_2014-10_Fireeye_A_Window_into_Russia_Cyber_Esp.Operations	6316258CA5BA2D85134AD7427F24A8A51CE4815B_coreshell.dll_
APT28_2014-10_Fireeye_A_Window_into_Russia_Cyber_Esp.Operations	682E49EFA6D2549147A21993D64291BFA40D815A_coreshell.dll_
APT28_2014-10_Fireeye_A_Window_into_Russia_Cyber_Esp.Operations	85522190958C82589FA290C0835805F3D9A2F8D6_coreshell.dll_
APT28_2014-10_Fireeye_A_Window_into_Russia_Cyber_Esp.Operations	A8551397E1F1A2C0148E6EADCB56FA35EE6009CA_coreshell.dll_
APT28_2014-10_Fireeye_A_Window_into_Russia_Cyber_Esp.Operations	CF3220C867B81949D1CE2B36446642DE7894C6DC_coreshell.dll_
APT28_2014-10_Fireeye_A_Window_into_Russia_Cyber_Esp.Operations	D87B310AA81AE6254FFF27B7D57F76035F544073_coreshell.dll_
APT28_2014-10_Fireeye_A_Window_into_Russia_Cyber_Esp.Operations	D9C53ADCE8C35EC3B1E015EC8011078902E6800B_coreshell.dll_
APT28_2014-10_Fireeye_A_Window_into_Russia_Cyber_Esp.Operations	E2450DFFA675C61AA43077B25B12851A910EEEB6_ coreshell.dll_
APT28_2014-10_Fireeye_A_Window_into_Russia_Cyber_Esp.Operations	ED48EF531D96E8C7360701DA1C57E2FF13F12405_coreshell.dll_
APT28_2014-10_Fireeye_A_Window_into_Russia_Cyber_Esp.Operations	F5B3E98C6B5D65807DA66D50BD5730D35692174D_asdfasdf.dat_
APT28	APT28_2014-10_Telus_Coreshell.A
APT28_2014-10_Telus_Coreshell.A	D87B310AA81AE6254FFF27B7D57F76035F544073_coreshell.dll_
APT28	APT28_2014-10_TrendMicro Operation Pawn Storm
APT28_2014-10_TrendMicro Operation Pawn Storm	0A3E6607D5E9C59C712106C355962B11DA2902FC_Case2_S.vbs_exe_
APT28_2014-10_TrendMicro Operation Pawn Storm	0E12C8AB9B89B6EB6BAF16C4B3BBF9530067963F_Case2_Military Coopera
APT28_2014-10_TrendMicro Operation Pawn Storm	14BEEB0FC5C8C887D0435009730B6370BF94BC93_Case5Payload2_netids.
APT28_2014-10_TrendMicro Operation Pawn Storm	3814EEC8C45FC4313A9C7F65CE882A7899CF0405_Case4_NetIds.dll_
APT28_2014-10_TrendMicro Operation Pawn Storm	4B8806FE8E0CB49E4AA5D8F87766415A2DB1E9A9_Case2dropper_cryptmo

Parent Folder	File Name (SHA1)
APT28_2014-10_TrendMicro Operation Pawn Storm	550ABD71650BAEA05A0071C4E084A803CB413C31_Case2_skype.exe_
APT28_2014-10_TrendMicro Operation Pawn Storm	55318328511961EC339DFDDCA0443068DCCE9CD2_Case3_conhost.dll_
APT28_2014-10_TrendMicro Operation Pawn Storm	5A452E7248A8D3745EF53CF2B1F3D7D8479546B9_Case3_netui.dll_keylog
APT28_2014-10_TrendMicro Operation Pawn Storm	6ADA11C71A5176A82A8898680ED1EAA4E79B9BC3_Case1_Letter to IAEA.p
APT28_2014-10_TrendMicro Operation Pawn Storm	6B875661A74C4673AE6EE89ACC5CB6927CA5FD0D_Case2Payload2_ netids
APT28_2014-10_TrendMicro Operation Pawn Storm	72CFD996957BDE06A02B0ADB2D66D8AA9C25BF37_Case1_saver.scr_
APT28_2014-10_TrendMicro Operation Pawn Storm	78D28072FDABF0B5AAC5E8F337DC768D07B63E1E_Case5_IDF_Spokesper
APT28_2014-10_TrendMicro Operation Pawn Storm	7FBB5A2E46FACD3EE0C945F324414210C2199FFB_Case5payload_saver.sc
APT28_2014-10_TrendMicro Operation Pawn Storm	88F7E271E54C127912DB4DB49E37D93AEA8A49C9_Case3_download_msmv
APT28_2014-10_TrendMicro Operation Pawn Storm	8DEF0A554F19134A5DB3D2AE949F9500CE3DD2CE_Case6_dropper_filee.dl
APT28_2014-10_TrendMicro Operation Pawn Storm	956D1A36055C903CB570890DA69DEABAACB5A18A_Case2_International Mi
APT28_2014-10_TrendMicro Operation Pawn Storm	9C622B39521183DD71ED2A174031CA159BEB6479_Case3_conhost.dll__
APT28_2014-10_TrendMicro Operation Pawn Storm	A8551397E1F1A2C0148E6EADCB56FA35EE6009CA_Case6_Coreshell.dll_
APT28_2014-10_TrendMicro Operation Pawn Storm	A90921C182CB90807102EF402719EE8060910345_Case4_APEC Media list 2
APT28_2014-10_TrendMicro Operation Pawn Storm	AC6B465A13370F87CF57929B7CFD1E45C3694585_Case4Payload_dw20.t_
APT28_2014-10_TrendMicro Operation Pawn Storm	B3098F99DB1F80E27AEC0C9A5A625AEDAAB5899A_APEC Media list 2013 F
APT28_2014-10_TrendMicro Operation Pawn Storm	BC58A8550C53689C8148B021C917FB4AEEC62AC1_Case5Payload_install.e
APT28_2014-10_TrendMicro Operation Pawn Storm	C5CE5B7D10ACCB04A4E45C3A4DCF10D16B192E2F_Case1Payload_netids.
APT28_2014-10_TrendMicro Operation Pawn Storm	D0AA4F3229FCD9A57E9E4F08860F3CC48C983ADDml.rtf
APT28_2014-10_TrendMicro Operation Pawn Storm	DAE7FAA1725DB8192AD711D759B13F8195A18821_Case6_MH17.doc_decoy
APT28_2014-10_TrendMicro Operation Pawn Storm	E338A57C35A4732BBB5F738E2387C1671A002BCB_Case6_advstoreshell.dll_
APT28_2014-10_TrendMicro Operation Pawn Storm	F542C5F9259274D94360013D14FFBECC43AAE552_Case5Decoy_IDF_Spoke
APT28_2014-10_TrendMicro Operation Pawn Storm	wp-operation-pawn-storm.pdf
APT28	APT28_2015-07_Digital Attack on German Parliament
APT28_2015-07_Digital Attack on German Parliament	0450AAF8ED309CA6BAF303837701B5B23AAC6F05_servicehost.dll_
APT28_2015-07_Digital Attack on German Parliament	CDEEA936331FCDD8158C876E9D23539F8976C305_exe_
APT28_2015-07_Digital Attack on German Parliament	Digital Attack on German Parliament_ Investigative Report on the Hack of the Le netzpolitik.pdf
APT28_2015-07_Digital Attack on German Parliament	F46F84E53263A33E266AAE520CB2C1BD0A73354E_winexesvc.exe_
APT28	APT28_2015-07_ESET_Sednit_meet_Hacking
APT28_2015-07_ESET_Sednit_meet_Hacking	51B0E3CD6360D50424BF776B3CD673DD45FD0F97.exe_
APT28_2015-07_ESET_Sednit_meet_Hacking	B8B3F53CA2CD64BD101CB59C6553F6289A72D9BBdll_
APT28_2015-07_ESET_Sednit_meet_Hacking	D43FD6579AB8B9C40524CC8E4B7BD05BE6674F6C_warfsgfdydcikf.mkv.swf_
APT28	APT28_2015-07_Telus_Trojan-Downloader.Win32.Sofacy.B
APT28_2015-07_Telus_Trojan-Downloader.Win32.Sofacy.B	B8B3F53CA2CD64BD101CB59C6553F6289A72D9BB.dll_
APT28	APT28_2015-09_Root9_APT28_Technical_Followup
APT28_2015-09_Root9_APT28_Technical_Followup	0450AAF8ED309CA6BAF303837701B5B23AAC6F05_servicehost.dll_
APT28_2015-09_Root9_APT28_Technical_Followup	CDEEA936331FCDD8158C876E9D23539F8976C305_exe_
APT28_2015-09_Root9_APT28_Technical_Followup	F46F84E53263A33E266AAE520CB2C1BD0A73354E_winexesvc.exe_

Parent Folder	File Name (SHA1)
APT28	APT28_2015-09_SFecure_Sofacy-recycles-carberp-and-metasploit-code
APT28_2015-09_SFecure_Sofacy-recycles-carberp-and-metasploit-code	Dlls
Dlls	21835AAFE6D46840BB697E8B0D4AAC06DEC44F5B
Dlls	3B52046DD7E1D5684EABBD9038B651726714AB69
Dlls	5C3E709517F41FEBF03109FA9D597F2CCC495956
Dlls	7319A2751BD13B2364031F1E69035ACFC4FD4D18
Dlls	9FC43E32C887B7697BF6D6933E9859D29581EAD0
Dlls	AC61A299F81D1CFF4EA857AFD1B323724AAC3F04
Dlls	B8B3F53CA2CD64BD101CB59C6553F6289A72D9BB
Dlls	D3AA282B390A5CB29D15A97E0A046305038DBEFE
Dlls	D85E44D386315B0258847495BE1711450AC02D9F
Dlls	ED9F3E5E889D281437B945993C6C2A80C60FDEDC
Dlls	F7608EF62A45822E9300D390064E667028B75DEA
APT28_2015-09_SFecure_Sofacy-recycles-carberp-and-metasploit-code	Droppers
Droppers	015425010BD4CF9D511F7FCD0FC17FC17C23EEC1
Droppers	4FAE67D3988DA117608A7548D9029CADDBFB3EBF
Droppers	51B0E3CD6360D50424BF776B3CD673DD45FD0F97
Droppers	63D1D33E7418DAF200DC4660FC9A59492DDD50D9
Droppers	B4A515EF9DE037F18D96B9B0E48271180F5725B7
Droppers	B7788AF2EF073D7B3FB84086496896E7404E625E
Droppers	B8AABE12502F7D55AE332905ACEE80A10E3BC399
Droppers	F3D50C1F7D5F322C1A1F9A72FF122CAC990881EE
APT28	APT28_2015-10_New Adobe Flash Zero-Day Used in Pawn Storm
APT28_2015-10_New Adobe Flash Zero-Day Used in Pawn Storm	2DF498F32D8BAD89D0D6D30275C19127763D5568763D5568.swf_
APT28_2015-10_New Adobe Flash Zero-Day Used in Pawn Storm	A5FCA59A2FAE0A12512336CA1B78F857AFC06445AFC06445_ mgswizap.dll
APT28	APT28_2015-10_Root9_APT28_targets Financial Markets
APT28_2015-10_Root9_APT28_targets Financial Markets	0450AAF8ED309CA6BAF303837701B5B23AAC6F05_servicehost.dll_
APT28_2015-10_Root9_APT28_targets Financial Markets	F325970FD24BB088F1BEFDAE5788152329E26BF3_SupUpNvidia.exe_
APT28	APT28_2015-12_Bitdefender_In-depth_analysis_of_APT28â€"The_Political_Cy
APT28_2015-12_Bitdefender_In-depth_analysis_of_APT28â€"The_Political_Cyber-Espionage	Bitdefender_In-depth_analysis_of_APT28â€"The_Political_Cyber-Espionage.pd
APT28_2015-12_Bitdefender_In-depth_analysis_of_APT28â€"The_Political_Cyber-Espionage	CB796F2986700DF9CE7D8F8D7A3F47F2EB4DF682_xp.exe_APT28
APT28_2015-12_Bitdefender_In-depth_analysis_of_APT28â€"The_Political_Cyber-Espionage	F080E509C988A9578862665B4FCF1E4BF8D77C3E_Linux.Fysbis.A_ksysdefd
APT28_2015-12_Bitdefender_In-depth_analysis_of_APT28â€"The_Political_Cyber-Espionage	SIMILAR
SIMILAR	356d03f6975f443d6db6c5069d778af9_exe_
SIMILAR	78450806e56b1f224d00455efcd04ce3_xp.exe_APT28

Parent Folder	File Name (SHA1)
SIMILAR	e49bce75070a7a3c63a7cebb699342b3_CVE-2014-4076_tan.exe_
APT28	APT28_2015-12_Kaspersky_Sofacy APT hits high profile targets
APT28_2015-12_Kaspersky_Sofacy APT hits high profile targets	1A4F39C0262822B0623213B8ED3F56DEE0117CD59_tf394kv.dll_
APT28_2015-12_Kaspersky_Sofacy APT hits high profile targets	1A4F39C0262822B0623213B8ED3F56DEE0117CD5_tf394kv.dll_
APT28_2015-12_Kaspersky_Sofacy APT hits high profile targets	314EF7909CA0ED3A744D2F59AB5AC8B8AE259319.dll_(4.3)AZZYimplants-U
APT28_2015-12_Kaspersky_Sofacy APT hits high profile targets	3E2E245B635B04F006A0044388BD968DF9C3238C_IGFSRVC.dll_USBSteale
APT28_2015-12_Kaspersky_Sofacy APT hits high profile targets	776C04A10BDEEC9C10F51632A589E2C52AABDF48_USBGuard.exe_
APT28_2015-12_Kaspersky_Sofacy APT hits high profile targets	AF86743852CC9DF557B62485715AF4C6D73644D3_AZZY4.3installer
APT28_2015-12_Kaspersky_Sofacy APT hits high profile targets	C78FCAE030A66F388BF8CEA569422F5A79B7B96C_tmpdt.tmp_(4.3)AZZYim
APT28_2015-12_Kaspersky_Sofacy APT hits high profile targets	C78FCAE030A66F388BF8CEA569422F5A79B7B96C_tmpdt.tmp__
APT28_2015-12_Kaspersky_Sofacy APT hits high profile targets	E251B3EB1449F7016DF78D113571BEA57F92FC36c_servicehost.dll_USBSte
APT28_2015-12_Kaspersky_Sofacy APT hits high profile targets	E3B7704D4C887B40A9802E0695BAE379358F3BA0_Stand-aloneAZZYbackdo
APT28_2015-12_Kaspersky_Sofacy APT hits high profile targets	F325970FD24BB088F1BEFDAE5788152329E26BF3_SupUpNvidia.exe_USBS
APT28	APT28_2015_06_Microsoft_Security_Intelligence_Report_V19
APT28_2015_06_Microsoft_Security_Intelligence_Report_V19	0450AAF8ED309CA6BAF303837701B5B23AAC6F05_servicehost.dll_
APT28_2015_06_Microsoft_Security_Intelligence_Report_V19	1535D85BEE8A9ADB52E8179AF20983FB0558CCB3.exe_
APT28	APT28_2016-02_PaloAlto_Fysbis Sofacy Linux Backdoor
APT28_2016-02_PaloAlto_Fysbis Sofacy Linux Backdoor	9444D2B29C6401BC7C2D14F071B11EC9014AE040_Fysbis_elf_
APT28_2016-02_PaloAlto_Fysbis Sofacy Linux Backdoor	A Look Into Fysbis_ Sofacyâ€™s Linux Backdoor - Palo Alto Networks Blog.pdf
APT28_2016-02_PaloAlto_Fysbis Sofacy Linux Backdoor	ECDDA7ACA5C805E5BE6E0AB2017592439DE7E32C_ksysdefd_elf
APT28_2016-02_PaloAlto_Fysbis Sofacy Linux Backdoor	F080E509C988A9578862665B4FCF1E4BF8D77C3E
APT29	APT29_2016-06_Crowdstrike_Bears in the Midst Intrusion into the Democratic N
APT29_2016-06_Crowdstrike_Bears in the Midst Intrusion into the Democratic National Committee	0B3852AE641DF8ADA629E245747062F889B26659.exe_
APT29_2016-06_Crowdstrike_Bears in the Midst Intrusion into the Democratic National Committee	74C190CD0C42304720C686D50F8184AC3FADDBE9.exe_
APT29_2016-06_Crowdstrike_Bears in the Midst Intrusion into the Democratic National Committee	Bears in the Midst_ Intrusion into the Democratic National Committee Â».pdf
APT29_2016-06_Crowdstrike_Bears in the Midst Intrusion into the Democratic National Committee	CB872EDD1F532C10D0167C99530A65C4D4532A1E.exe_
APT29_2016-06_Crowdstrike_Bears in the Midst Intrusion into the Democratic National Committee	E2B98C594961AAE731B0CCEE5F9607080EC57197_pagemgr.exe_
APT29_2016-06_Crowdstrike_Bears in the Midst Intrusion into the Democratic National Committee	F09780BA9EB7F7426F93126BC198292F5106424B_VmUpgradeHelper.exe_
APT28	APT28_2016-07_Invincea_Tunnel of Gov DNC Hack and the Russian XTunnel
APT28_2016-07_Invincea_Tunnel of Gov DNC Hack and the Russian XTunnel	E2101519714F8A4056A9DE18443BC6E8A1F1B977_PortMapClient.exe_

Parent Folder	File Name (SHA1)
APT28_2016-07_Invincea_Tunnel of Gov DNC Hack and the Russian XTunnel	F09780BA9EB7F7426F93126BC198292F5106424B_VmUpgradeHelper.exe_
APT28_2016-07_Invincea_Tunnel of Gov DNC Hack and the Russian XTunnel	Tunnel of Gov_ DNC Hack and the Russian XTunnel _ Invincea.pdf
APT28	APT28_2016-10_ESET_Observing the Comings and Goings
APT28_2016-10_ESET_Observing the Comings and Goings	eset-sednit-part-2.pdf
APT28_2016-10_ESET_Observing the Comings and Goings	Sedreco-dropper
Sedreco-dropper	4F895DB287062A4EE1A2C5415900B56E2CF15842
Sedreco-dropper	87F45E82EDD63EF05C41D18AEDDEAC00C49F1AEE
Sedreco-dropper	8EE6CEC34070F20FD8AD4BB202A5B08AEA22ABFA
Sedreco-dropper	9E779C8B68780AC860920FCB4A8E700D97F084EF
Sedreco-dropper	C23F18DE9779C4F14A3655823F235F8E221D0F6A
Sedreco-dropper	E034E0D9AD069BAB5A6E68C1517C15665ABE67C9
Sedreco-dropper	E17615331BDCE4AFA45E4912BDCC989EACF284BC
APT28_2016-10_ESET_Observing the Comings and Goings	Sedreco_payload
Sedreco_payload	04301B59C6EB71DB2F701086B617A98C6E026872
Sedreco_payload	11AF174294EE970AC7FD177746D23CDC8FFB92D7
Sedreco_payload	E3B7704D4C887B40A9802E0695BAE379358F3BA0
APT28_2016-10_ESET_Observing the Comings and Goings	XAgent-LIN
XAgent-LIN	7E33A52E53E85DDB1DC8DC300E6558735ACF10CE
XAgent-LIN	9444D2B29C6401BC7C2D14F071B11EC9014AE040
XAgent-LIN	ECDDA7ACA5C805E5BE6E0AB2017592439DE7E32C
XAgent-LIN	F080E509C988A9578862665B4FCF1E4BF8D77C3E
APT28_2016-10_ESET_Observing the Comings and Goings	XAgent-WIN
XAgent-WIN	072933FA35B585511003F36E3885563E1B55D55A
XAgent-WIN	082141F1C24FB49981CC70A9ED50CDA582EE04DD
XAgent-WIN	08C4D755F14FD6DF76EC86DA6EAB1B5574DFBAFD
XAgent-WIN	0F04DAD5194F97BB4F1808DF19196B04B4AEE1B8
XAgent-WIN	3403519FA3EDE4D07FB4C05D422A9F8C026CEDBF
XAgent-WIN	499FF777C88AEACBBAA47EDDE183C944AC7E91D2
XAgent-WIN	4B74C90C9D9CE7668AA9EB09978C1D8D4DFDA24A
XAgent-WIN	4BC32A3894F64B4BE931FF20390712B4EC605488
XAgent-WIN	5F05A8CB6FEF24A91B3BD6C137B23AB3166F39AE
XAgent-WIN	71636E025FA308FC5B8065136F3DD692870CB8A4
XAgent-WIN	780AA72F0397CB6C2A78536201BD9DB4818FA02A
XAgent-WIN	A70ED3AE0BC3521E743191259753BE945972118B
XAgent-WIN	BAA4C177A53CFA5CC103296B07B62565E1C7799F
XAgent-WIN	C18EDCBA2C31533B7CDB6649A970DCE397F4B13C
XAgent-WIN	C2E8C584D5401952AF4F1DB08CF4B6016874DDAC
XAgent-WIN	D00AC5498D0735D5AE0DEA42A1F477CF8B8B0826

Parent Folder	File Name (SHA1)
XAgent-WIN	D0DB619A7A160949528D46D20FC0151BF9775C32
XAgent-WIN	E816EC78462B5925A1F3EF3CDB3CAC6267222E72
XAgent-WIN	F1EE563D44E2B1020B7A556E080159F64F3FD699
APT28_2016-10_ESET_Observing the Comings and Goings	Xtunnel
Xtunnel	0450AAF8ED309CA6BAF303837701B5B23AAC6F05
Xtunnel	067913B28840E926BF3B4BFAC95291C9114D3787
Xtunnel	1535D85BEE8A9ADB52E8179AF20983FB0558CCB3
Xtunnel	42DEE38929A93DFD45C39045708C57DA15D7586C
Xtunnel	8F4F0EDD5FB3737914180FF28ED0E9CCA25BF4CC
Xtunnel	982D9241147AAACF795174A9DAB0E645CF56B922
Xtunnel	99B454262DC26B081600E844371982A49D334E5E
Xtunnel	C637E01F50F5FBD2160B191F6371C5DE2AC56DE4
Xtunnel	C91B192F4CD47BA0C8E49BE438D035790FF85E70
Xtunnel	CDEEA936331FCDD8158C876E9D23539F8976C305
Xtunnel	DB731119FCA496064F8045061033A5976301770D
Xtunnel	DE3946B83411489797232560DB838A802370EA71
Xtunnel	E945DE27EBFD1BAF8E8D2A81F4FB0D4523D85D6A
APT28	APT28_2016-10_ESET_Sednit A Mysterious Downloader
APT28_2016-10_ESET_Sednit A Mysterious Downloader	1CC2B6B208B7687763659AEB5DCB76C5C2FBBF26.scr_
APT28_2016-10_ESET_Sednit A Mysterious Downloader	49ACBA812894444C634B034962D46F986E0257CF.exe_
APT28_2016-10_ESET_Sednit A Mysterious Downloader	4C9C7C4FD83EDAF7EC80687A7A957826DE038DD7.exe_
APT28_2016-10_ESET_Sednit A Mysterious Downloader	4F92D364CE871C1AEBBF3C5D2445C296EF535632.exe_
APT28_2016-10_ESET_Sednit A Mysterious Downloader	516EC3584073A1C05C0D909B8B6C15ECB10933F1.exe_
APT28_2016-10_ESET_Sednit A Mysterious Downloader	593D0EB95227E41D299659842395E76B55AA048D.exe_
APT28_2016-10_ESET_Sednit A Mysterious Downloader	593D0EB95227E41D299659842395E76B55AA048D_dll_
APT28_2016-10_ESET_Sednit A Mysterious Downloader	5C132AE63E3B41F7B2385740B9109B473856A6A5.dll_
APT28_2016-10_ESET_Sednit A Mysterious Downloader	5FC4D555CA7E0536D18043977602D421A6FD65F9.exe_
APT28_2016-10_ESET_Sednit A Mysterious Downloader	669A02E330F5AFC55A3775C4C6959B3F9E9965CF.exe_
APT28_2016-10_ESET_Sednit A Mysterious Downloader	6CAA48CD9532DA4CABD6994F62B8211AB9672D9E_bk.exe_
APT28_2016-10_ESET_Sednit A Mysterious Downloader	7394EA20C3D510C938EF83A2D0195B767CD99ED7_x32.dll_
APT28_2016-10_ESET_Sednit A Mysterious Downloader	9F3AB8779F2B81CAE83F62245AFB124266765939.exe_
APT28_2016-10_ESET_Sednit A Mysterious Downloader	E8ACA4B0CFE509783A34FF908287F98CAB968D9E.exe_
APT28_2016-10_ESET_Sednit A Mysterious Downloader	EE788901CD804965F1CD00A0AFC713C8623430C4.exe_
APT28_2016-10_ESET_Sednit A Mysterious Downloader	EE788901CD804965F1CD00A0AFC713C8623430C46.exe_
APT28_2016-10_ESET_Sednit A Mysterious Downloader	eset-sednit-part3.pdf
APT28	APT28_2016-10_ESET_Sednit Approaching the Target
APT28_2016-10_ESET_Sednit Approaching the Target	015425010BD4CF9D511F7FCD0FC17FC17C23EEC1
APT28_2016-10_ESET_Sednit Approaching the Target	0F7893E2647A7204DBF4B72E50678545573C3A10
APT28_2016-10_ESET_Sednit Approaching the Target	10686CC4E46CF3FFBDEB71DD565329A80787C439

Parent Folder	File Name (SHA1)
APT28_2016-10_ESET_Sednit Approaching the Target	17661A04B4B150A6F70AFDABE3FD9839CC56BEE8
APT28_2016-10_ESET_Sednit Approaching the Target	21835AAFE6D46840BB697E8B0D4AAC06DEC44F5B
APT28_2016-10_ESET_Sednit Approaching the Target	2663EB655918C598BE1B2231D7C018D8350A0EF9
APT28_2016-10_ESET_Sednit Approaching the Target	2C86A6D6E9915A7F38D119888EDE60B38AB1D69D
APT28_2016-10_ESET_Sednit Approaching the Target	351C3762BE9948D01034C69ACED97628099A90B0
APT28_2016-10_ESET_Sednit Approaching the Target	3956CFE34566BA8805F9B1FE0D2639606A404CD4
APT28_2016-10_ESET_Sednit Approaching the Target	4D5E923351F52A9D5C94EE90E6A00E6FCED733EF
APT28_2016-10_ESET_Sednit Approaching the Target	4FAE67D3988DA117608A7548D9029CADDBFB3EBF
APT28_2016-10_ESET_Sednit Approaching the Target	51B0E3CD6360D50424BF776B3CD673DD45FD0F97
APT28_2016-10_ESET_Sednit Approaching the Target	51E42368639D593D0AE2968BD2849DC20735C071
APT28_2016-10_ESET_Sednit Approaching the Target	5C3E709517F41FEBF03109FA9D597F2CCC495956
APT28_2016-10_ESET_Sednit Approaching the Target	63D1D33E7418DAF200DC4660FC9A59492DDD50D9
APT28_2016-10_ESET_Sednit Approaching the Target	69D8CA2A02241A1F88A525617CF18971C99FB63B
APT28_2016-10_ESET_Sednit Approaching the Target	6FB3FD8C2580C84314B14510944700144A9E31DF
APT28_2016-10_ESET_Sednit Approaching the Target	80DCA565807FA69A75A7DD278CEF1DAAEE34236E
APT28_2016-10_ESET_Sednit Approaching the Target	842B0759B5796979877A2BAC82A33500163DED67
APT28_2016-10_ESET_Sednit Approaching the Target	8F99774926B2E0BF85E5147AACA8BBBBCC5F1D48
APT28_2016-10_ESET_Sednit Approaching the Target	90C3B756B1BB849CBA80994D445E96A9872D0CF5
APT28_2016-10_ESET_Sednit Approaching the Target	99F927F97838EB47C1D59500EE9155ADB55B806A
APT28_2016-10_ESET_Sednit Approaching the Target	9FC43E32C887B7697BF6D6933E9859D29581EAD0
APT28_2016-10_ESET_Sednit Approaching the Target	A43EF43F3C3DB76A4A9CA8F40F7B2C89888F0399
APT28_2016-10_ESET_Sednit Approaching the Target	A5FCA59A2FAE0A12512336CA1B78F857AFC06445
APT28_2016-10_ESET_Sednit Approaching the Target	A857BCCF4CC5C15B60667ECD865112999E1E56BA
APT28_2016-10_ESET_Sednit Approaching the Target	B4A515EF9DE037F18D96B9B0E48271180F5725B7
APT28_2016-10_ESET_Sednit Approaching the Target	B7788AF2EF073D7B3FB84086496896E7404E625E
APT28_2016-10_ESET_Sednit Approaching the Target	B8AABE12502F7D55AE332905ACEE80A10E3BC399
APT28_2016-10_ESET_Sednit Approaching the Target	C1EAE93785C9CB917CFB260D3ABF6432C6FDAF4D
APT28_2016-10_ESET_Sednit Approaching the Target	C2E8C584D5401952AF4F1DB08CF4B6016874DDAC
APT28_2016-10_ESET_Sednit Approaching the Target	C345A85C01360F2833752A253A5094FF421FC839
APT28_2016-10_ESET_Sednit Approaching the Target	D3AA282B390A5CB29D15A97E0A046305038DBEFE
APT28_2016-10_ESET_Sednit Approaching the Target	D85E44D386315B0258847495BE1711450AC02D9F
APT28_2016-10_ESET_Sednit Approaching the Target	D9989A46D590EBC792F14AA6FEC30560DFE931B1
APT28_2016-10_ESET_Sednit Approaching the Target	E5FB715A1C70402774EE2C518FB0E4E9CD3FDCFF
APT28_2016-10_ESET_Sednit Approaching the Target	E742B917D3EF41992E67389CD2FE2AAB0F9ACE5B
APT28_2016-10_ESET_Sednit Approaching the Target	ED9F3E5E889D281437B945993C6C2A80C60FDEDC
APT28_2016-10_ESET_Sednit Approaching the Target	F024DBAB65198467C2B832DE9724CB70E24AF0DD
APT28_2016-10_ESET_Sednit Approaching the Target	F3D50C1F7D5F322C1A1F9A72FF122CAC990881EE
APT28_2016-10_ESET_Sednit Approaching the Target	F7608EF62A45822E9300D390064E667028B75DEA
APT28_2016-10_ESET_Sednit Approaching the Target	eset-sednit-part1.pdf

Parent Folder	File Name (SHA1)
APT28	APT28_2016-10_Sekoia_Rootkit analysisUse case on HideDRV
APT28_2016-10_Sekoia_Rootkit analysisUse case on HideDRV	83E54CB97644DE7084126E702937F8C3A2486A2F_fsflt.sys_
APT28_2016-10_Sekoia_Rootkit analysisUse case on HideDRV	9F3AB8779F2B81CAE83F62245AFB124266765939_fsflt.1
APT28	APT28_2017-02_Bitdefender_OSX_XAgent
APT28_2017-02_Bitdefender_OSX_XAgent	70A1C4ED3A09A44A41D54C4FD4B409A5FC3159F6_XAgent_OSX