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

Archived: 2026-04-05 20:36:22 UTC

APT28APT28_2011-09_Telus_Trojan.Win32.Sofacy.A APT28_2011-09_Telus_Trojan.Win32.Sofacy.A28F21E96E0722DD6FC7D6E1275F352BD060ADE0D1e217668d89b480ad42e230e8c2c4d971feb41c4a64a7588d1e8e APT28_2011-09_Telus_Trojan.Win32.Sofacy.A72CFD996957BDE06A02B0ADB2D66D8AA9C25BF37ed7f6260dec470e81dafb0e63bafb5ae7313eaf95a8a8b4c206b9 APT28_2011-09_Telus_Trojan.Win32.Sofacy.AAC6B465A13370F87CF57929B7CFD1E45C3694585e1554b931affb3cd2edc90bc580280785ab8ef93fdeaac9af258845a APT28_2011-09_Telus_Trojan.Win32.Sofacy.AC01B02CCC86ACBD9B266B09D2B693CB39A2C68099e4817f7bf36a61b363e0911cc0f08b931a0906b0d8b0716712 APT28APT28_2014-08_MhtMS12-27_Prevenity APT28_2014-08_MhtMS12-27_Prevenity33EEC0D1AE550FB33874EDCE0138F485538BB21B__.mht_d3de5b8500453107d6d152b3c850693555038c4326964f480fd2160b6b2a7af APT28_2014-08_MhtMS12-27_Prevenity8DEF0A554F19134A5DB3D2AE949F9500CE3DD2CE_filee.dll_16a6c56ba458ec718b4e9bc8f9f10785ce554d57333bdbccebb5e2e8d16a3 APT28_2014-08_MhtMS12-27_PrevenityA8551397E1F1A2C0148E6EADCB56FA35EE6009CA_coreshell.dll_48656a93f9ba39410763a2196aabc67fc8087186a215553d2f95c68c03 APT28_2014-08_MhtMS12-27_PrevenityE338A57C35A4732BBB5F738E2387C1671A002BCB_advstorshell.dll_d7a625779df56d874871bb632f3e310611097a7a3336e0ab124fa921 APT28APT28_2014-10_Fireeye_A_Window_into_Russia_Cyber_Esp.Operations APT28_2014-10_Fireeye_A_Window_into_Russia_Cyber_Esp.Operations367D40465FD1633C435B966FA9B289188AA444BC__tmp64.dat_791428601ad12b9230b9 APT28_2014-10_Fireeye_A_Window_into_Russia_Cyber_Esp.Operations6316258CA5BA2D85134AD7427F24A8A51CE4815B_coreshell.dll_da2a657dc69d7320f2f APT28_2014-10_Fireeye_A_Window_into_Russia_Cyber_Esp.Operations682E49EFA6D2549147A21993D64291BFA40D815A_coreshell.dll_3b0ecd011500f61237c2 APT28_2014-10_Fireeye_A_Window_into_Russia_Cyber_Esp.Operations85522190958C82589FA290C0835805F3D9A2F8D6_coreshell.dll_8b92fe86c5b7a9e34f433 APT28_2014-10_Fireeye_A_Window_into_Russia_Cyber_Esp.OperationsA8551397E1F1A2C0148E6EADCB56FA35EE6009CA_coreshell.dll_48656a93f9ba394107 APT28_2014-10_Fireeye_A_Window_into_Russia_Cyber_Esp.OperationsCF3220C867B81949D1CE2B36446642DE7894C6DC_coreshell.dll_5882fda97fdf78b47081 APT28_2014-10_Fireeye_A_Window_into_Russia_Cyber_Esp.OperationsD87B310AA81AE6254FFF27B7D57F76035F544073_coreshell.dll_272f0fde35dbdfccbca1e APT28_2014-10_Fireeye_A_Window_into_Russia_Cyber_Esp.OperationsD9C53ADCE8C35EC3B1E015EC8011078902E6800B_coreshell.dll_1259c4fe5efd9bf07fc4 APT28_2014-10_Fireeye_A_Window_into_Russia_Cyber_Esp.OperationsE2450DFFA675C61AA43077B25B12851A910EEEB6_coreshell.dll_9eebfebe3987fec3c395594dc57a0c4ce6d09ce32cc62b6f17279204fac1771a6eb35077bb79471115e8dfed2c86cd75 APT28_2014-10_Fireeye_A_Window_into_Russia_Cyber_Esp.OperationsED48EF531D96E8C7360701DA1C57E2FF13F12405_coreshell.dll_ead4ec18ebce6890d207 APT28_2014-10_Fireeye_A_Window_into_Russia_Cyber_Esp.OperationsF5B3E98C6B5D65807DA66D50BD5730D35692174D_asdfasdf.dat_8c4fa713c5e2b009114 APT28APT28_2014-10_Telus_Coreshell.A APT28_2014-10_Telus_Coreshell.AD87B310AA81AE6254FFF27B7D57F76035F544073_coreshell.dll_272f0fde35dbdfccbca1e33373b3570d423a0799efe41b28a8b7(APT28APT28_2014-10_TrendMicro Operation Pawn Storm APT28_2014-10_TrendMicro Operation Pawn Storm0A3E6607D5E9C59C712106C355962B11DA2902FC_Case2_S.vbs_exe_db9edafbadd71c7a3a0f0aec1b216a92b3d624c4287795a7fbddd617f5770 APT28_2014-10_TrendMicro Operation Pawn Storm0E12C8AB9B89B6EB6BAF16C4B3BBF9530067963F_Case2_MilitaryCooperationDecoy.doc_7fcf20302404f644fb07fe9d4fe9ac8477166146463b9124e075f3a7925075f969974e32746c78d022ba99f578b9f0bb APT28_2014-10_TrendMicro Operation Pawn Storm14BEEB0FC5C8C887D0435009730B6370BF94BC93_Case5Payload2_netids.dll_35717cd78ce713067a5037286cf91c3e1b3dd8aaafd750aa85185c APT28_2014-10_TrendMicro Operation Pawn Storm3814EEC8C45FC4313A9C7F65CE882A7899CF0405_Case4_NetIds.dll_a24552843b9fedd7d0084e1eb1dd6e35966660738c9e3ec103c2f8fe361c8 APT28_2014-10_TrendMicro Operation Pawn Storm4B8806FE8E0CB49E4AA5D8F87766415A2DB1E9A9_Case2dropper_cryptmodule.exe_41e14894f4ad9494e0359ee5bb3d9745684f4b9ea61e14a1 APT28_2014-10_TrendMicro Operation Pawn Storm550ABD71650BAEA05A0071C4E084A803CB413C31_Case2_skype.exe_7276d1dab1125f59604252159e0c529c81f0f5fcb3cb8a63e8a3713b4107 APT28_2014-10_TrendMicro Operation Pawn Storm55318328511961EC339DFDDCA0443068DCCE9CD2_Case3_conhost.dll_f1704aaf08cd66a2ac6cf8810c9e07c274bdd9c250b0f4f27c0ecfeca967f APT28_2014-10_TrendMicro Operation Pawn

Storm5A452E7248A8D3745EF53CF2B1F3D7D8479546B9_Case3_netui.dll_keylogaa3e6af90c144112a1ad0c19bdf873ff4536650c9c5e5e1bb57d9bedf7
APT28_2014-10_TrendMicro Operation Pawn
Storm6ADA11C71A5176A82A8898680ED1EAA4E79B9BC3_Case1_Letter to
IAEA.pdf_decoy76d3eb8c2bed4f2588e22b8d0984af86b0f1f553a847f3244f434541edbf26904e2de18cca8db8f861ea33bb70942b61
APT28_2014-10_TrendMicro Operation Pawn
Storm6B875661A74C4673AE6EE89ACC5CB6927CA5FD0D_Case2Payload2_
netids.dll_42bc93c0caddf07fce919d126a6e378f9392776d6d8e697468ab671b43dce2b7baf97057b53bd3517ecd77a081eff67d
APT28_2014-10_TrendMicro Operation Pawn
Storm72CFD996957BDE06A02B0ADB2D66D8AA9C25BF37_Case1_saver.scr_ed7f6260dec470e81dafb0e63bafb5ae7313eaf95a8a8b4c206b9afe306e7
APT28_2014-10_TrendMicro Operation Pawn
Storm78D28072FDABF0B5AAC5E8F337DC768D07B63E1E_Case5_IDF_Spokesperson_Terror_Attack_011012.doc_1ac15db72e6d4440f0b4f710a516
APT28_2014-10_TrendMicro Operation Pawn
Storm7FBB5A2E46FACD3EE0C945F324414210C2199FFB_Case5payload_saver.scr_c16b07f7590a8620a8f0f687b0bd8bd8cb630234494f2424d8e158c
APT28_2014-10_TrendMicro Operation Pawn
Storm88F7E271E54C127912DB4DB49E37D93AEA8A49C9_Case3_download_msmvs.exe_66f368cab3d5e64475a91f636c87af15e8ac9acc6fa3283276b
APT28_2014-10_TrendMicro Operation Pawn
Storm8DEF0A554F19134A5DB3D2AE949F9500CE3DD2CE_Case6_dropper_filee.dll_16a6c56ba458ec718b4e9bc8f9f10785ce554d57333bdbccebb5e2
APT28_2014-10_TrendMicro Operation Pawn
Storm956D1A36055C903CB570890DA69DEABAACB5A18A_Case2_International
Military.rtf_d994b9780b69f611284e22033e435edb342e1f591ab45fcca6cee7f5da118a99dce463e222c03511c3f1288ac2cf82c8
APT28_2014-10_TrendMicro Operation Pawn
Storm9C622B39521183DD71ED2A174031CA159BEB6479_Case3_conhost.dll__d4e99548832b6999f00e8d223c6fabbdd5debe5d88e76a409b9bc3f69a(
APT28_2014-10_TrendMicro Operation Pawn
StormA8551397E1F1A2C0148E6EADCB56FA35EE6009CA_Case6_Coreshell.dll_48656a93f9ba39410763a2196aabc67fc8087186a215553d2f95c68c0
APT28_2014-10_TrendMicro Operation Pawn StormA90921C182CB90807102EF402719EE8060910345_Case4_APEC
Media list 2013
Part1.xls_aeebfc9eb9031e423797a5af1985242de8d3f1e4e0d7c19e195d92be5cb6b3617a0496554c892e93b66a75c411745c05
APT28_2014-10_TrendMicro Operation Pawn
StormAC6B465A13370F87CF57929B7CFD1E45C3694585_Case4Payload_dw20.t_e1554b931affb3cd2edc90bc580280785ab8ef93fdeaac9af258845ab5
APT28_2014-10_TrendMicro Operation Pawn StormB3098F99DB1F80E27AEC0C9A5A625AEDAAB5899A_APEC
Media list 2013
Part2.xls_decoybebb3675cfa4adaba7822cc8c39f55bf8fc4fe966ef4e7ecf635283a6fa6bacd8586ee8f0d4d39c6faffd49d60b01cb9
APT28_2014-10_TrendMicro Operation Pawn
StormBC58A8550C53689C8148B021C917FB4AEEC62AC1_Case5Payload_install.exe_c43edb579e43aaeb6f0c0703f84e43f77dd063acdfb00509b3b067
APT28_2014-10_TrendMicro Operation Pawn
StormC5CE5B7D10ACCB04A4E45C3A4DCF10D16B192E2F_Case1Payload_netids.dll_85c80d01661f88ec556579e772a5a3db461f5340f9ea47344f86b
APT28_2014-10_TrendMicro Operation Pawn
StormD0AA4F3229FCD9A57E9E4F08860F3CC48C983ADDml.rtfa24d2f5258f8a0c3bddd1b5636b0ec57992caa9e8de503fb304f97d1ab0b92202d2efb0
APT28_2014-10_TrendMicro Operation Pawn
StormDAE7FAA1725DB8192AD711D759B13F8195A18821_Case6_MH17.doc_decoy388594cd1bef96121be291880b22041aadf344f12633ab0738d25e
APT28_2014-10_TrendMicro Operation Pawn
StormE338A57C35A4732BBB5F738E2387C1671A002BCB_Case6_advstoreshell.dll_d7a625779df56d874871bb632f3e310611097a7a3336e0ab124fa92
APT28_2014-10_TrendMicro Operation Pawn
StormF542C5F9259274D94360013D14FFBECC43AAE552_Case5Decoy_IDF_Spokesperson_Terror_Attack_011012.doc_77aa465744061b4b725f7384
APT28_2014-10_TrendMicro Operation Pawn Stormwp-operation-pawn-
storm.pdfce254486b02be740488c0ab3278956fd9b8495ff1d023e3ae7aed799f02d9cf24422a38dfb9ed37c0bdc65da55b4ee42
APT28APT28_2015-07_Digital Attack on German Parliament APT28_2015-07_Digital Attack on German
Parliament0450AAF8ED309CA6BAF303837701B5B23AAC6F05_servicehost.dll_800af1c9d341b846a856a1e686be6a3e566ab945f61be016bfd9e83cc1
APT28_2015-07_Digital Attack on German
ParliamentCDEEA936331FCDD8158C876E9D23539F8976C305_exe_5e70a5c47c6b59dae7faf0f2d62b28b3730a0e3daf0b54f065bdd2ca427fbe10e8d4e
APT28_2015-07_Digital Attack on German ParliamentDigital Attack on German Parliament_ Investigative Report on the
Hack of the Left Party Infrastructure in Bundestag _
netzpolitik.pdf28d4cc2a378633e0ad6f3306cc067c43e83e2185f9e1a5dbc550914dcbc7a4d0f8b30a577ddb4cd8a0f36ac024a68aa0
APT28_2015-07_Digital Attack on German
ParliamentF46F84E53263A33E266AAE520CB2C1BD0A73354E_winexesvc.exe_77e7fb6b56c3ece4ef4e93b6dc608be05130f600cd9a9cdc82d4bad938b
APT28APT28_2015-07_ESET_Sednit_meet_Hacking APT28_2015-
07_ESET_Sednit_meet_Hacking51B0E3CD6360D50424BF776B3CD673DD45FD0F97.exe_973e0c922eb07aad530d8a1de19c77557c4101caf833aa902
APT28_2015-
07_ESET_Sednit_meet_HackingB8B3F53CA2CD64BD101CB59C6553F6289A72D9BBdll_dcf6906a9a0c970bcd93f451b9b7932a9a527274f99865a7d7
APT28_2015-
07_ESET_Sednit_meet_HackingD43FD6579AB8B9C40524CC8E4B7BD05BE6674F6C_warfsgfdydcikf.mkv.swf_557f8d4c6f8b386c32001def807dc71
APT28APT28_2015-07_Telus_Trojan-Downloader.Win32.Sofacy.B APT28_2015-07_Telus_Trojan-
Downloader.Win32.Sofacy.BB8B3F53CA2CD64BD101CB59C6553F6289A72D9BB.dll_dcf6906a9a0c970bcd93f451b9b7932a9a527274f99865a7d704
APT28APT28_2015-09_Root9_APT28_Technical_Followup APT28_2015-

09_Root9_APT28_Technical_Followup0450AAF8ED309CA6BAF303837701B5B23AAC6F05_servicehost.dll_800af1c9d341b846a856a1e686be6a3e56
APT28_2015-
09_Root9_APT28_Technical_FollowupCDEEA936331FCDD8158C876E9D23539F8976C305_exe_5e70a5c47c6b59dae7faf0f2d62b28b3730a0e3daf0b5
APT28_2015-
09_Root9_APT28_Technical_FollowupF46F84E53263A33E266AAE520CB2C1BD0A73354E_winexesvc.exe_77e7fb6b56c3ece4ef4e93b6dc608be0513
APT28APT28_2015-09_SFecure_Sofacy-recycles-carberp-and-metasploit-code APT28_2015-09_SFecure_Sofacy-
recycles-carberp-and-metasploit-codeDlls
Dlls21835AAFE6D46840BB697E8B0D4AAC06DEC44F5B211b7100fd799e9eaabeb13cfa4462313d13f2e5b241168005425b15410556bcf26d04078da6b
Dlls3B52046DD7E1D5684EABBD9038B651726714AB69d535c3fc5f0f98e021bea0d6277d2559d4525abc9dd2b7ab7f0c22e58a0117980039afdf15bed04
Dlls5C3E709517F41FEBF03109FA9D597F2CCC495956ac75fd7d79e64384b9c4053b37e5623f0ac7b666814fd016b3d21d7812f4a272104511f90ca666fa
Dlls7319A2751BD13B2364031F1E69035ACFC4FD4D18c0d1762561f8c2f812d868a3939d23f08325cd6e26fb39cf7a08787e771a6cf708e0b45350d1ea2
Dlls9FC43E32C887B7697BF6D6933E9859D29581EAD0a3c757af9e7a9a60e235d08d54740fbcbf28267386a010197a50b65f24e815aa527f2adbc53c609c
DllsAC61A299F81D1CFF4EA857AFD1B323724AAC3F04acf8cda38b0d1b6a0d3664a0e33deb96638e7ca68643d4b01432f0ecaaa0495b805cc3cccc17a7
DllsB8B3F53CA2CD64BD101CB59C6553F6289A72D9BBdcf6906a9a0c970bcd93f451b9b7932a9a527274f99865a7d70487fe22e62f692f8b239d6cb808
DllsD3AA282B390A5CB29D15A97E0A046305038DBEFE18efc091b431c39d3e59be445429a7bceae782130b06d95f3373ff7d5c0977a8019960bdf80614
DllsD85E44D386315B0258847495BE1711450AC02D9Fc4ffab85d84b494e1c450819a0e9c7db500fa112a204b6abb365101013a17749ce83403c30cd37f7
DllsED9F3E5E889D281437B945993C6C2A80C60FDEDC2dfc90375a09459033d430d046216d22261b0a5912965ea95b8ae02aae1e761a61f9ad3a9fb85e
DllsF7608EF62A45822E9300D390064E667028B75DEA75f71713a429589e87cf2656107d2bfcb6fff95a74f9847f1a4282b38f148d80e4684d9c35d9ae79fa
APT28_2015-09_SFecure_Sofacy-recycles-carberp-and-metasploit-codeDroppers
Droppers015425010BD4CF9D511F7FCD0FC17FC17C23EEC1c2a0344a2bbb29d9b56d378386afcbed63d0b28114f6277b901132bc1cc1f541a594ee72f2
Droppers4FAE67D3988DA117608A7548D9029CADDBFB3EBFc6a80316ea97218df11e11125337233ab0b3f0d6e6c593e2a2046833080574f98566c48a1
Droppers51B0E3CD6360D50424BF776B3CD673DD45FD0F97973e0c922eb07aad530d8a1de19c77557c4101caf833aa9025fec4f04a637c049c929459ad
Droppers63D1D33E7418DAF200DC4660FC9A59492DDD50D92d4eaa0331abbc6d867f5f979b2c890db4f755c91c2790f4ab9bac4ee60725132323e13a2(
DroppersB4A515EF9DE037F18D96B9B0E48271180F5725B7afe09fb5a2b97f9e119f70292092604ed93f22d46090bfc19ef51963a781eeb864390c66d934
DroppersB7788AF2EF073D7B3FB84086496896E7404E625Eeda061c497ba73441994a30e36f55b1db1800cb1d4b755e05b0fca251b8c6da96bb85f8042f2
DroppersB8AABE12502F7D55AE332905ACEE80A10E3BC39991381cd82cdd5f52bbc7b30d34cb8d831a09ce8a9210d2530d6ce1d59bfae2ac617ac8955
DroppersF3D50C1F7D5F322C1A1F9A72FF122CAC990881EE77089c094c0f2c15898ff0f021945148eb6620442c3ab327f3ccff1cc6d63d6ffe7729186f7e
APT28APT28_2015-10_New Adobe Flash Zero-Day Used in Pawn Storm APT28_2015-10_New Adobe Flash Zero-Day
Used in Pawn
Storm2DF498F32D8BAD89D0D6D30275C19127763D5568763D5568.swf_6ca857721be6fff26b10867c99bd8c80b4064721d911e9606edf366173325945
APT28_2015-10_New Adobe Flash Zero-Day Used in Pawn
StormA5FCA59A2FAE0A12512336CA1B78F857AFC06445AFC06445_
mgswizap.dll_f1d3447a2bff56646478b0adb7d0451c5a414a39851c4e22d4f9383211dfc080e16e2caffd90fa06dcbe51d11fdb0d6c
APT28APT28_2015-10_Root9_APT28_targets Financial Markets APT28_2015-10_Root9_APT28_targets Financial
Markets0450AAF8ED309CA6BAF303837701B5B23AAC6F05_servicehost.dll_800af1c9d341b846a856a1e686be6a3e566ab945f61be016bfd9e83cc1b64
APT28_2015-10_Root9_APT28_targets Financial
MarketsF325970FD24BB088F1BEFDAE5788152329E26BF3_SupUpNvidia.exe_0369620eb139c3875a62e36bb7abdae8b1f2d461856bb6f2760785ee1af
APT28APT28_2015-12_Bitdefender_In-depth_analysis_of_APT28â€"The_Political_Cyber-Espionage APT28_2015-
12_Bitdefender_In-depth_analysis_of_APT28â€"The_Political_Cyber-EspionageBitdefender_In-
depth_analysis_of_APT28â€"The_Political_Cyber-
Espionage.pdf1a5d89f6fd3f1ed5f4e76084b0fa7806a76b1ec9d196b5c071992486d096ad475226e92b6db06c351e3a4ad4e4949248
APT28_2015-12_Bitdefender_In-depth_analysis_of_APT28â€"The_Political_Cyber-
EspionageCB796F2986700DF9CE7D8F8D7A3F47F2EB4DF682_xp.exe_APT2878450806e56b1f224d00455efcd04ce3b29a16ec907997e523f97e77b885
APT28_2015-12_Bitdefender_In-depth_analysis_of_APT28â€"The_Political_Cyber-
EspionageF080E509C988A9578862665B4FCF1E4BF8D77C3E_Linux.Fysbis.A_ksysdefd_elf_APT28075b6695ab63f36af65f7ffd45cccd3902c7cf55fd5
APT28_2015-12_Bitdefender_In-depth_analysis_of_APT28â€"The_Political_Cyber-EspionageSIMILAR
SIMILAR356d03f6975f443d6db6c5069d778af9_exe_356d03f6975f443d6db6c5069d778af93f14fc9c29763da76dcbc8a2aaa61658781d1b215ee322a0ebf
SIMILAR78450806e56b1f224d00455efcd04ce3_xp.exe_APT2878450806e56b1f224d00455efcd04ce3b29a16ec907997e523f97e77b885d4a8c19cb81b1a
SIMILARe49bce75070a7a3c63a7cebb699342b3_CVE-2014-
4076_tan.exe_e49bce75070a7a3c63a7cebb699342b316d49a40333f584b19606733b4deef1b9ecace2c32950010ad1450b44ce3716e
APT28APT28_2015-12_Kaspersky_Sofacy APT hits high profile targets APT28_2015-12_Kaspersky_Sofacy APT hits high
profile
targets1A4F39C0262822B0623213B8ED3F56DEE0117CD59_tf394kv.dll_8c4d896957c36ec4abeb07b2802268b96cd30c85dd8a64ca529c6eab98a757fb3
APT28_2015-12_Kaspersky_Sofacy APT hits high profile
targets1A4F39C0262822B0623213B8ED3F56DEE0117CD5_tf394kv.dll_8c4d896957c36ec4abeb07b2802268b96cd30c85dd8a64ca529c6eab98a757fb32
APT28_2015-12_Kaspersky_Sofacy APT hits high profile
targets314EF7909CA0ED3A744D2F59AB5AC8B8AE259319.dll_(4.3)AZZYimplants-
USBStealerf6f88caf49a3e32174387cacfa144a89e917166adf6e1135444f327d8fff6ec6c6a8606d65dda4e24c2f416d23b69d45
APT28_2015-12_Kaspersky_Sofacy APT hits high profile
targets3E2E245B635B04F006A0044388BD968DF9C3238C_IGFSRVC.dll_USBStealerce151285e8f0e7b2b90162ba171a4b904e4606313c423b681e1111
APT28_2015-12_Kaspersky_Sofacy APT hits high profile
targets776C04A10BDEEC9C10F51632A589E2C52AABDF48_USBGuard.exe_8cb08140ddb00ac373d29d37657a03cc690b483751b890d487bb63712e5
APT28_2015-12_Kaspersky_Sofacy APT hits high profile
targetsAF86743852CC9DF557B62485715AF4C6D73644D3_AZZY4.3installerc3ae4a37094ecfe95c2badecf40bf5bb67ecc3b8c6057090c7982883e8d9d0

APT28_2015-12_Kaspersky_Sofacy APT hits high profile
targetsC78FCAE030A66F388BF8CEA569422F5A79B7B96C_tmpdt.tmp_(4.3)AZZYimplantce8b99df8642c065b6af43fde1f786a31bab1a3e0e501d3c14
APT28_2015-12_Kaspersky_Sofacy APT hits high profile
targetsC78FCAE030A66F388BF8CEA569422F5A79B7B96C_tmpdt.tmp__ce8b99df8642c065b6af43fde1f786a31bab1a3e0e501d3c14652ecf60870e483
APT28_2015-12_Kaspersky_Sofacy APT hits high profile
targetsE251B3EB1449F7016DF78D113571BEA57F92FC36c_servicehost.dll_USBStealer8b238931a7f64fddcad3057a96855f6c92dcb0d8394d0df1064e6
APT28_2015-12_Kaspersky_Sofacy APT hits high profile
targetsE3B7704D4C887B40A9802E0695BAE379358F3BA0_Stand-
aloneAZZYbackdoora96f4b8ac7aa9dbf4624424b7602d4f7a9dc96d45702538c2086a749ba2fb467ba8d8b603e513bdef62a024dfeb124cb
APT28_2015-12_Kaspersky_Sofacy APT hits high profile
targetsF325970FD24BB088F1BEFDAE5788152329E26BF3_SupUpNvidia.exe_USBStealer0369620eb139c3875a62e36bb7abdae8b1f2d461856bb6f276
APT28APT28_2015_06_Microsoft_Security_Intelligence_Report_V19
APT28_2015_06_Microsoft_Security_Intelligence_Report_V190450AAF8ED309CA6BAF303837701B5B23AAC6F05_servicehost.dll_800af1c9d341b
APT28_2015_06_Microsoft_Security_Intelligence_Report_V191535D85BEE8A9ADB52E8179AF20983FB0558CCB3.exe_4ac8d16ff796e825625ad18
APT28APT28_2016-02_PaloAlto_Fysbis Sofacy Linux Backdoor APT28_2016-02_PaloAlto_Fysbis Sofacy Linux
Backdoor9444D2B29C6401BC7C2D14F071B11EC9014AE040_Fysbis_elf_364ff454dcf00420cff13a57bcb784678bca0031f3b691421cb15f9c6e71ce193
APT28_2016-02_PaloAlto_Fysbis Sofacy Linux BackdoorA Look Into Fysbis_ Sofacyâ€™s Linux Backdoor - Palo Alto
Networks
Blog.pdf9a6b771c934415f74a203e0dfab9edbe1b6c3e6ef673f14536ff8d7c2bf18f9358a9a7f8962a24e2255f54ac451af86c
APT28_2016-02_PaloAlto_Fysbis Sofacy Linux
BackdoorECDDA7ACA5C805E5BE6E0AB2017592439DE7E32C_ksysdefd_elfe107c5c84ded6cd9391aede7f04d64c8fd8b2ea9a2e8a67e4cb3904b49c7
APT28_2016-02_PaloAlto_Fysbis Sofacy Linux
BackdoorF080E509C988A9578862665B4FCF1E4BF8D77C3E075b6695ab63f36af65f7ffd45cccd3902c7cf55fd5c5809ce2dce56085ba43795f2480423a4
APT29 APT29_2016-06_Crowdstrike_Bears in the Midst Intrusion into the Democratic National Committee APT29_2016-
06_Crowdstrike_Bears in the Midst Intrusion into the Democratic National
Committee0B3852AE641DF8ADA629E245747062F889B26659.exe_cc9e6578a47182a941a478b276320e06fd39d2837b30e7233bc54598ff51bdc2f8c41
APT29_2016-06_Crowdstrike_Bears in the Midst Intrusion into the Democratic National
Committee74C190CD0C42304720C686D50F8184AC3FADDBE9.exe_19172b9210295518ca52e93a29cfe8f440ae43b7d6c413becc92b07076fa128b875c
APT29_2016-06_Crowdstrike_Bears in the Midst Intrusion into the Democratic National CommitteeBears in the Midst_
Intrusion into the Democratic National Committee
Â».pdfdd5e31f9d323e6c3e09e367e6bd0e7b12d815b11f3b916bdc27b049402f5f1c024cffe2318a4f27ebfa3b8a9fffe2880
APT29_2016-06_Crowdstrike_Bears in the Midst Intrusion into the Democratic National
CommitteeCB872EDD1F532C10D0167C99530A65C4D4532A1E.exe_ce227ae503e166b77bf46b6c8f5ee4dab101cd29e18a515753409ae86ce68a4cedbe
APT29_2016-06_Crowdstrike_Bears in the Midst Intrusion into the Democratic National
CommitteeE2B98C594961AAE731B0CCEE5F9607080EC57197_pagemgr.exe_004b55a66b3a86a1ce0a0b9b69b959766c1bce76f4d2358656132b6b1d4
APT29_2016-06_Crowdstrike_Bears in the Midst Intrusion into the Democratic National
CommitteeF09780BA9EB7F7426F93126BC198292F5106424B_VmUpgradeHelper.exe_9e7053a4b6c9081220a694ec93211b4e4845761c9bed0563d0aa8
APT28APT28_2016-07_Invincea_Tunnel of Gov DNC Hack and the Russian XTunnel APT28_2016-07_Invincea_Tunnel
of Gov DNC Hack and the Russian
XTunnelE2101519714F8A4056A9DE18443BC6E8A1F1B977_PortMapClient.exe_ad44a7c5e18e9958dda66ccfc406cd44b81b10bdf4f29347979ea8a171
APT28_2016-07_Invincea_Tunnel of Gov DNC Hack and the Russian
XTunnelF09780BA9EB7F7426F93126BC198292F5106424B_VmUpgradeHelper.exe_9e7053a4b6c9081220a694ec93211b4e4845761c9bed0563d0aa83
APT28_2016-07_Invincea_Tunnel of Gov DNC Hack and the Russian XTunnelTunnel of Gov_ DNC Hack and the Russian
XTunnel _
Invincea.pdfb1b88f78c2f4393d437da4ce743ac5e8fb0cb4527efc48c90a2cd3e9e46ce59eaa280c85c50d7b680c98bb159c27881d
APT28APT28_2016-10_ESET_Observing the Comings and Goings APT28_2016-10_ESET_Observing the Comings and
Goingseset-sednit-part-
2.pdfc3c278991ad051fbace1e2f3a4c20998f9ed13d5aa43c74287a936bf52772080fc26b5c62a805e19abceb20ef08ea5ff
APT28_2016-10_ESET_Observing the Comings and GoingsSedreco-dropper Sedreco-
dropper4F895DB287062A4EE1A2C5415900B56E2CF158425363e5cc28687b7dd71f1e257eab2d5dd403ded7c4acfffe8dc2a3ad8fb848f08388b4c345210
Sedreco-
dropper87F45E82EDD63EF05C41D18AEDDEAC00C49F1AEE9617f3948b1886ebc95689c02d2cf264378ef276eeaa4a29dab46d114710fc14ba0a9f964f
Sedreco-
dropper8EE6CEC34070F20FD8AD4BB202A5B08AEA22ABFA30cda69cf82637dfa2ffdc803bf2aead20ac1420eade0bdb464cd9f6d26a84094271b252c0
Sedreco-
dropper9E779C8B68780AC860920FCB4A8E700D97F084EFf686304cff9b35ea0d7647820ab525ba2c81023a146d2b5003d2b0c617ebf2eb1501dc6e55fc
Sedreco-
dropperC23F18DE9779C4F14A3655823F235F8E221D0F6A9f82abbaebc1093a187f1887df2cf926ec2f14916e0b52fb727111962dff9846839137968e322
Sedreco-
dropperE034E0D9AD069BAB5A6E68C1517C15665ABE67C96a24be8f61bcd789622dc55ebb7db90bfb3a3339e2ba82cb3dcdc43d0e49e7b8a26ced3a58
Sedreco-
dropperE17615331BDCE4AFA45E4912BDCC989EACF284BC5e93cf87040cf225ab5b5b9f9f0a0d036bbec6b2927325891cc008d3378d30941fe9d21e5c
APT28_2016-10_ESET_Observing the Comings and GoingsSedreco_payload
Sedreco_payload04301B59C6EB71DB2F701086B617A98C6E026872cf30b7550f04a9372c3257c9b5cff3e937bf2c81184297231495643444 9fd294e793b

Sedreco_payload11AF174294EE970AC7FD177746D23CDC8FFB92D79422ca55f7fca4449259d8878ede5e47ba1c02aa6c12794a33c4742e62cbda3c17d
Sedreco_payloadE3B7704D4C887B40A9802E0695BAE379358F3BA0a96f4b8ac7aa9dbf4624424b7602d4f7a9dc96d45702538c2086a749ba2fb467ba8d
APT28_2016-10_ESET_Observing the Comings and GoingsXAgent-LIN XAgent-
LIN7E33A52E53E85DDB1DC8DC300E6558735ACF10CEfd8d1b48f91864dc5acb429a49932ca3dd8facad6c0626b6c94e1cc891698d4982782a5564aae
XAgent-
LIN9444D2B29C6401BC7C2D14F071B11EC9014AE040364ff454dcf00420cff13a57bcb784678bca0031f3b691421cb15f9c6e71ce193355d2d8cf2b1904
XAgent-
LINECDDA7ACA5C805E5BE6E0AB2017592439DE7E32Ce107c5c84ded6cd9391aede7f04d64c8fd8b2ea9a2e8a67e4cb3904b49c789d57ed9b1ce5bebf
XAgent-
LINF080E509C988A9578862665B4FCF1E4BF8D77C3E075b6695ab63f36af65f7ffd45cccd3902c7cf55fd5c5809ce2dce56085ba43795f2480423a42565
APT28_2016-10_ESET_Observing the Comings and GoingsXAgent-WIN XAgent-
WIN072933FA35B585511003F36E3885563E1B55D55A99b93cfcff258eb49e7af603d779a146c19d266af9e33dae096e45e7624ab3a3f642c8de580e902fe
XAgent-
WIN082141F1C24FB49981CC70A9ED50CDA582EE04DD7a055cbe6672f77b2271c1cb8e2670b899d3f03fc6f048c74e58da6fb7ea1e831ba31d58194ad
XAgent-
WIN08C4D755F14FD6DF76EC86DA6EAB1B5574DFBAFD26ac59dab32f6246e1ce3da7506d48fa5f6b2a0d1d966fc4f1ed292b46240767f4acb06c1351
XAgent-
WIN0F04DAD5194F97BB4F1808DF19196B04B4AEE1B88b6d824619e993f74973eedfaf18be78972e907a901a7716f3b8f9651eadd65a0ce09bbc78a1ce
XAgent-
WIN3403519FA3EDE4D07FB4C05D422A9F8C026CEDBF113cc4a88fd28ea4398e312093a6a4d5ddab96e4a8e909065e05c4b6a73ba351ea45ad480625
XAgent-
WIN499FF777C88AEACBBAA47EDDE183C944AC7E91D2ea726d3e8f6516807366584f3c5b5e2a82c4e9bc100533482a15a1d756d55e1a604d330eff8f
XAgent-
WIN4B74C90C9D9CE7668AA9EB09978C1D8D4DFDA24A409848dabfd110f4d373dd0a97ff708e24e11c80f1d4c1e9db654d54cc784db6b5f4a126f9fe5
XAgent-
WIN4BC32A3894F64B4BE931FF20390712B4EC60548857cc08213ab8b6d4a538e4568d00a123b23193bff95c4e65af0c9848036eb80ef006503a78be842
XAgent-
WIN5F05A8CB6FEF24A91B3BD6C137B23AB3166F39AE9ca6ead1384953d787487d399c23cb4107393ac2e890772f70adf9e8d3aa07ab2f98e2726e3be
XAgent-
WIN71636E025FA308FC5B8065136F3DD692870CB8A496ed0a7976e57ae0bb79dcbd67e39743ea957d663dbc0b28844f6aa7dfdc5ac0110a4004ac46c87
XAgent-
WIN780AA72F0397CB6C2A78536201BD9DB4818FA02Aeffd7b2411975447fd36603445b380c7d0e019229493a1cfb3ffc918a2d8ffcbaee31f9132293c9
XAgent-
WINA70ED3AE0BC3521E743191259753BE945972118B9a66142acfc7739f78c23ab1252db45b715f69916db9ff8fedf6630307f4ebb84aae6653fd0e5930
XAgent-
WINBAA4C177A53CFA5CC103296B07B62565E1C7799F9d1a09bb98bf1ee31f390b60b0cf724ddea4e560017b4da05e8fd0a03ba74239723349934ee8f
XAgent-
WINC18EDCBA2C31533B7CDB6649A970DCE397F4B13C4265f6e8cc545b925912867ec8af2f11fc2dbfda41860b2385314c87e81f1ebb4f9ae1106b697
XAgent-
WINC2E8C584D5401952AF4F1DB08CF4B6016874DDAC078755389b98d17788eb5148e23109a654c4ce98970a44f92be748ebda9fcfb7b30e08d98491
XAgent-
WIND00AC5498D0735D5AE0DEA42A1F477CF8B8B082612a9fff59de1663dec1b45ea2ede22f568065abd6482405614d245537600ea60857c6ec9febac
XAgent-
WIND0DB619A7A160949528D46D20FC0151BF9775C32ee64d3273f9b4d80020c24edcbbf961ee031299fa1381b40c660b8cd831bb861654f900a1e2952
XAgent-
WINE816EC78462B5925A1F3EF3CDB3CAC6267222E72404eb3f7554392e85e56aed414db845594c220653ea7421c60e3eafd753a9ae9d69b475d61230
XAgent-
WINF1EE563D44E2B1020B7A556E080159F64F3FD69958ca9243d35e529499dd17d27642b419bebe0be0cf8349706b2feb789572e035955209d5bf5d5f
APT28_2016-10_ESET_Observing the Comings and GoingsXtunnel
Xtunnel0450AAF8ED309CA6BAF303837701B5B23AAC6F05800af1c9d341b846a856a1e686be6a3e566ab945f61be016bfd9e83cc1b64f783b9b8deb89
Xtunnel067913B28840E926BF3B4BFAC95291C9114D378702522ce47a8db9544f8877dace7e0833d2a60644297545716 82f475b6b67f36526f1573d8461
Xtunnel1535D85BEE8A9ADB52E8179AF20983FB0558CCB34ac8d16ff796e825625ad1861546e2e88c488b029188e3280ed3614346575a4a390e0dda00
Xtunnel42DEE38929A93DFD45C39045708C57DA15D7586Cae4ded48da0766d237ce2262202c3c96a2c9041ee1918523e67dbaf1c514f98609d4dbe451b
Xtunnel8F4F0EDD5FB3737914180FF28ED0E9CCA25BF4CCe766e048bd222cfd2b9cc1bf24125dac1289ee3d29967f491542c0bdeff6974aad6b37932e9
Xtunnel982D9241147AAACF795174A9DAB0E645CF56B9220ebfac6dba63ff8b35cbd374ef33323ac9ef265fc0a174f3033ff21b8f0274224eb7154dca97f
Xtunnel99B454262DC26B081600E844371982A49D334E5Eac3e087e43be67bdc674747c665b46c2a979c5094f75548043a22b174aa10e1f2025371bd9e1
XtunnelC637E01F50F5FBD2160B191F6371C5DE2AC56DE4b2dc7c29cbf8d71d1dd57b474f1e04b9c6a9db52a3855d980a7f383dbe2fb70300a12b7a3a4
XtunnelC91B192F4CD47BA0C8E49BE438D035790FF85E70672b8d14d1d3e97c24baf69d50937afc1c8869abf756e77e1b6d7d0ad5ca8f1cdce1a111315c
XtunnelCDEEA936331FCDD8158C876E9D23539F8976C3055e70a5c47c6b59dae7faf0f2d62b28b3730a0e3daf0b54f065bdd2ca427fbe10e8d4e28646a5
XtunnelDB731119FCA496064F8045061033A5976301770D34651f2df01b956f1989da4b3ea4033860ee6fdca66444bdc2e4b00dc67a1b0fdee5a3cd997981
XtunnelDE3946B83411489797232560DB838A802370EA711d1287d4a3ba5d02cca91f51863db7384dd8ab2471337a56b431433b7e8db2a659dc5d9dc548
XtunnelE945DE27EBFD1BAF8E8D2A81F4FB0D4523D85D6Acd1c521b6ae08fc97e3d69f242f00f9ed2e947a39714478983764b270985d2529ff682ffec9
APT28APT28_2016-10_ESET_Sednit A Mysterious Downloader APT28_2016-10_ESET_Sednit A Mysterious
Downloader1CC2B6B208B7687763659AEB5DCB76C5C2FBBF26.scr_006b418307c534754f055436a91848aa6507caba5835cad645ae80a081b9828403

APT28_2016-10_ESET_Sednit A Mysterious
Downloader49ACBA812894444C634B034962D46F986E0257CF.exe_23ae20329174d44ebc8dbfa9891c62603e23201e6c52470e73a92af2ded12e6a5d1a
APT28_2016-10_ESET_Sednit A Mysterious
Downloader4C9C7C4FD83EDAF7EC80687A7A957826DE038DD7.exe_0eefeaf2fb78ebc49e7beba505da273d6ccc375923a00571dffca613a036f77a9fc1
APT28_2016-10_ESET_Sednit A Mysterious
Downloader4F92D364CE871C1AEBBF3C5D2445C296EF535632.exe_9227678b90869c5a67a05defcaf21dfb79a508ba42247ddf92accbf5987b1ffc7ba2(
APT28_2016-10_ESET_Sednit A Mysterious
Downloader516EC3584073A1C05C0D909B8B6C15ECB10933F1.exe_607a7401962eaf78b93676c9f5ca6a26ecd2c8e79554f226b69bed7357f61c75f1f1a
APT28_2016-10_ESET_Sednit A Mysterious
Downloader593D0EB95227E41D299659842395E76B55AA048D.exe_6cd2c953102792b738664d69ce41e080a13aa88c32eb020071c2c92f5364fd98f6de
APT28_2016-10_ESET_Sednit A Mysterious
Downloader593D0EB95227E41D299659842395E76B55AA048D_dll_6cd2c953102792b738664d69ce41e080a13aa88c32eb020071c2c92f5364fd98f6de
APT28_2016-10_ESET_Sednit A Mysterious
Downloader5C132AE63E3B41F7B2385740B9109B473856A6A5.dll_94ebc9ef5565f98b1aa1e97c6d35c2e0cfc60d5db3bfb4ec462d5e4bd5222f04d7383c
APT28_2016-10_ESET_Sednit A Mysterious
Downloader5FC4D555CA7E0536D18043977602D421A6FD65F9.exe_81d9649612b05829476854bde71b8c3f1faf645c2b43cd78cc70df6bcbcd95e38f19
APT28_2016-10_ESET_Sednit A Mysterious
Downloader669A02E330F5AFC55A3775C4C6959B3F9E9965CF.exe_a0f212fd0f103ca8beaf8362f74903a2a50cb9ce1f01ea335c95870484903734ba9cd
APT28_2016-10_ESET_Sednit A Mysterious
Downloader6CAA48CD9532DA4CABD6994F62B8211AB9672D9E_bk.exe_9df2ddb2631ff5439c34f80ace40cd29f18fe2853ef0d4898085cc5581ae35b8
APT28_2016-10_ESET_Sednit A Mysterious
Downloader7394EA20C3D510C938EF83A2D0195B767CD99ED7_x32.dll_d70f4e9d55698f69c5f63b1a2e1507eb471fbdc52b501dfe6275a32f89a8a6b0
APT28_2016-10_ESET_Sednit A Mysterious
Downloader9F3AB8779F2B81CAE83F62245AFB124266765939.exe_3430bf72d2694e428a73c84d5ac4a4b9b1900cb7d1216d1dbc19b4c6c8567d48215
APT28_2016-10_ESET_Sednit A Mysterious
DownloaderE8ACA4B0CFE509783A34FF908287F98CAB968D9E.exe_991ffdbf860756a4589164de26dd7ccf44e8d3ffa0989176e62b8462b3d14ad38ed
APT28_2016-10_ESET_Sednit A Mysterious
DownloaderEE788901CD804965F1CD00A0AFC713C8623430C4.exe_93c589e9eaf3272bc0349d605b85c566f9c0303d07800ed7cba1394cd326bbe8f49
APT28_2016-10_ESET_Sednit A Mysterious
DownloaderEE788901CD804965F1CD00A0AFC713C8623430C46.exe_93c589e9eaf3272bc0349d605b85c566f9c0303d07800ed7cba1394cd326bbe8f4
APT28_2016-10_ESET_Sednit A Mysterious Downloadereset-sednit-
part3.pdfa7b4e01335aac544a12c6f88aab80cd92c7a60963b94b6fc924abdcb19da4d32f35c86cdfe2277b0081cd02c72435b48
APT28APT28_2016-10_ESET_Sednit Approaching the Target APT28_2016-10_ESET_Sednit Approaching the
Target015425010BD4CF9D511F7FCD0FC17FC17C23EEC1c2a0344a2bbb29d9b56d378386afcbed63d0b28114f6277b901132bc1cc1f541a594ee72f27d
APT28_2016-10_ESET_Sednit Approaching the
Target0F7893E2647A7204DBF4B72E50678545573C3A1035283c2e60a3cba6734f4f98c443d11fda43d39c749c121e99bba00ce809ca63794df3f704e7ad4
APT28_2016-10_ESET_Sednit Approaching the
Target10686CC4E46CF3FFBDEB71DD565329A80787C439d7c471729bc124babf32945eb5706eb6bc8fec92eee715e77c762693f1ae2bbcd6a3f3127f122
APT28_2016-10_ESET_Sednit Approaching the
Target17661A04B4B150A6F70AFDABE3FD9839CC56BEE8a579d53a1d29684de6d2c0cbabd525c56562e2ac60afa314cd463f771fcfb8be70f947f6e2b3
APT28_2016-10_ESET_Sednit Approaching the
Target21835AAFE6D46840BB697E8B0D4AAC06DEC44F5B211b7100fd799e9eaabeb13cfa4462313d13f2e5b241168005425b15410556bcf26d04078da
APT28_2016-10_ESET_Sednit Approaching the
Target2663EB655918C598BE1B2231D7C018D8350A0EF9540e4a7a28ca1514e53c2564993d8d8731dd3e3c05fabbfeafbcb7f5616dba30bbb2b1fc77dba6
APT28_2016-10_ESET_Sednit Approaching the
Target2C86A6D6E9915A7F38D119888EDE60B38AB1D69D56e011137b9678f1fcc54f9372198bae69d5123a277dc1f618be5edcc95938a0df148c856d2e
APT28_2016-10_ESET_Sednit Approaching the
Target351C3762BE9948D01034C69ACED97628099A90B083cf67a5d2e68f9c00fbbe6d7d9203bf853dbbba09e2463c45c0ad913d15d67d15792d888f81b
APT28_2016-10_ESET_Sednit Approaching the
Target3956CFE34566BA8805F9B1FE0D2639606A404CD4dffb22a1a6a757443ab403d61e760f0c0356f5fa9907ea060a7d6964e65f019896deb1c7e303b7
APT28_2016-10_ESET_Sednit Approaching the
Target4D5E923351F52A9D5C94EE90E6A00E6FCED733EF6159c094a663a171efd531b23a46716de00eaf295a28f5497dbb5cb8f647537b6e55dd666135
APT28_2016-10_ESET_Sednit Approaching the
Target4FAE67D3988DA117608A7548D9029CADDBFB3EBFc6a80316ea97218df11e11125337233ab0b3f0d6e6c593e2a2046833080574f98566c48a1ed
APT28_2016-10_ESET_Sednit Approaching the
Target51B0E3CD6360D50424BF776B3CD673DD45FD0F97973e0c922eb07aad530d8a1de19c77557c4101caf833aa9025fec4f04a637c049c929459ad3e4
APT28_2016-10_ESET_Sednit Approaching the
Target51E42368639D593D0AE2968BD2849DC20735C071dfc836e035cb6c43ce26ed870f61d7e813468ebe5d47d57d62777043c80784cbf475fb2de1df45
APT28_2016-10_ESET_Sednit Approaching the
Target5C3E709517F41FEBF03109FA9D597F2CCC495956ac75fd7d79e64384b9c4053b37e5623f0ac7b666814fd016b3d21d7812f4a272104511f90ca666
APT28_2016-10_ESET_Sednit Approaching the
Target63D1D33E7418DAF200DC4660FC9A59492DDD50D92d4eaa0331abbc6d867f5f979b2c890db4f755c91c2790f4ab9bac4ee60725132323e13a2688
APT28_2016-10_ESET_Sednit Approaching the
Target69D8CA2A02241A1F88A525617CF18971C99FB63Bed601bbd4dd0e267afb0be840cb27c904c52957270e63efa4b81a1c6551c706b82951f019b682

APT28_2016-10_ESET_Sednit Approaching the
Target6FB3FD8C2580C84314B14510944700144A9E31DFf7ee38ca49cd4ae35824ce5738b6e58763911ebce691c4b7c9582f37f63f6f439d2ce56e992bfbd
APT28_2016-10_ESET_Sednit Approaching the
Target80DCA565807FA69A75A7DD278CEF1DAAEE34236E9863f1efc5274b3d449b5b7467819d280abda721c4f1ca626f5d8bd2ce186aa98b197ca68d5
APT28_2016-10_ESET_Sednit Approaching the
Target842B0759B5796979877A2BAC82A33500163DED67291af793767f5c5f2dc9c6d44f1bfb59f50791f9909c542e4abb5e3f760c896995758a832b0699
APT28_2016-10_ESET_Sednit Approaching the
Target8F99774926B2E0BF85E5147AACA8BBBBCC5F1D48c2988e3e4f70d5901b234ff1c1363dcc69940a20ab9abb31a03fcefe6de92a16ed474bbdff328
APT28_2016-10_ESET_Sednit Approaching the
Target90C3B756B1BB849CBA80994D445E96A9872D0CF521d63e99ed7dcd8baec74e6ce65c9ef3dfa8a85e26c07a348a854130c652dcc6d29b203ee230c
APT28_2016-10_ESET_Sednit Approaching the
Target99F927F97838EB47C1D59500EE9155ADB55B806A07c8a0a792a5447daf08ac32d1e283e88f0674cb85f28b2619a6e0ddc74ce71e92ce4c3162056
APT28_2016-10_ESET_Sednit Approaching the
Target9FC43E32C887B7697BF6D6933E9859D29581EAD0a3c757af9e7a9a60e235d08d54740fbcbf28267386a010197a50b65f24e815aa527f2adbc53c60
APT28_2016-10_ESET_Sednit Approaching the
TargetA43EF43F3C3DB76A4A9CA8F40F7B2C89888F03997c2b1de614a9664103b6ff7f3d73f83dc2551c4e6521ac72982cb952503a2e6f016356e02ee31
APT28_2016-10_ESET_Sednit Approaching the
TargetA5FCA59A2FAE0A12512336CA1B78F857AFC06445f1d3447a2bff56646478b0adb7d0451c5a414a39851c4e22d4f9383211dfc080e16e2caffd90fa
APT28_2016-10_ESET_Sednit Approaching the
TargetA857BCCF4CC5C15B60667ECD865112999E1E56BA0c334645a4c12513020aaabc3b78ef9fe1b1143c0003c6905227df37d40aacbaecc2be8b9d865
APT28_2016-10_ESET_Sednit Approaching the
TargetB4A515EF9DE037F18D96B9B0E48271180F5725B7afe09fb5a2b97f9e119f70292092604ed93f22d46090bfc19ef51963a781eeb864390c66d9347e8
APT28_2016-10_ESET_Sednit Approaching the
TargetB7788AF2EF073D7B3FB84086496896E7404E625Eeda061c497ba73441994a30e36f55b1db1800cb1d4b755e05b0fca251b8c6da96bb85f8042f2d7
APT28_2016-10_ESET_Sednit Approaching the
TargetB8AABE12502F7D55AE332905ACEE80A10E3BC39991381cd82cdd5f52bbc7b30d34cb8d831a09ce8a9210d2530d6ce1d59bfae2ac617ac89558c
APT28_2016-10_ESET_Sednit Approaching the
TargetC1EAE93785C9CB917CFB260D3ABF6432C6FDAF4D732fbf0a4ceb10e9a2254af59ae4f8806236a1bdd76ed90659a36f58b3e073623c34c6436d2
APT28_2016-10_ESET_Sednit Approaching the
TargetC2E8C584D5401952AF4F1DB08CF4B6016874DDAC078755389b98d17788eb5148e23109a654c4ce98970a44f92be748ebda9fcfb7b30e08d9849
APT28_2016-10_ESET_Sednit Approaching the
TargetC345A85C01360F2833752A253A5094FF421FC83912193185 22fa28252368f58f36820ac2fbd5c2cf1c1f17402cc313fe3266b097a46e08f48b97157
APT28_2016-10_ESET_Sednit Approaching the
TargetD3AA282B390A5CB29D15A97E0A046305038DBEFE18efc091b431c39d3e59be445429a7bceae782130b06d95f3373ff7d5c0977a8019960bdf806
APT28_2016-10_ESET_Sednit Approaching the
TargetD85E44D386315B0258847495BE1711450AC02D9Fc4ffab85d84b494e1c450819a0e9c7db500fa112a204b6abb365101013a17749ce83403c30cd37
APT28_2016-10_ESET_Sednit Approaching the
TargetD9989A46D590EBC792F14AA6FEC30560DFE931B18b031fce1d0c38d6b4c68d52b2764c7e4bcd11142d5b9f96730715905152a645a1bf487921dc
APT28_2016-10_ESET_Sednit Approaching the
TargetE5FB715A1C70402774EE2C518FB0E4E9CD3FDCFF072c692783c67ea56da9de0a53a60d11c431ae04c79ade56e1902094acf51e5bf6b54d65363d
APT28_2016-10_ESET_Sednit Approaching the
TargetE742B917D3EF41992E67389CD2FE2AAB0F9ACE5B7764499bb1c4720d0f1d302f15be792c63047199037892f66dc083420e2fc60655a77075684
APT28_2016-10_ESET_Sednit Approaching the
TargetED9F3E5E889D281437B945993C6C2A80C60FDEDC2dfc90375a09459033d430d046216d22261b0a5912965ea95b8ae02aae1e761a61f9ad3a9fb8
APT28_2016-10_ESET_Sednit Approaching the
TargetF024DBAB65198467C2B832DE9724CB70E24AF0DD7b1bfd7c1866040e8f618fe67b93bea5df47a939809f925475bc19804319652635848b8f346f
APT28_2016-10_ESET_Sednit Approaching the
TargetF3D50C1F7D5F322C1A1F9A72FF122CAC990881EE77089c094c0f2c15898ff0f021945148eb6620442c3ab327f3ccff1cc6d63d6ffe7729186f7e8ac
APT28_2016-10_ESET_Sednit Approaching the
TargetF7608EF62A45822E9300D390064E667028B75DEA75f71713a429589e87cf2656107d2bfcb6fff95a74f9847f1a4282b38f148d80e4684d9c35d9ae7
APT28_2016-10_ESET_Sednit Approaching the Targeteset-sednit-
part1.pdfbae0221feefb37e6b81f5ca893864743b31b27aa0808aea5b0e8823ecb07402c0c2bbf6818a22457e146c97f685162b4
APT28APT28_2016-10_Sekoia_Rootkit analysisUse case on HideDRV APT28_2016-10_Sekoia_Rootkit analysisUse case
on
HideDRV83E54CB97644DE7084126E702937F8C3A2486A2F_fsflt.sys_f8c8f6456c5a52ef24aa426e6b1216854bfe2216ee63657312af1b2507c8f2bf362f
APT28_2016-10_Sekoia_Rootkit analysisUse case on
HideDRV9F3AB8779F2B81CAE83F62245AFB124266765939_fsflt.13430bf72d2694e428a73c84d5ac4a4b9b1900cb7d1216d1dbc19b4c6c8567d482151
APT28APT28_2017-02_Bitdefender_OSX_XAgent APT28_2017-
02_Bitdefender_OSX_XAgent70A1C4ED3A09A44A41D54C4FD4B409A5FC3159F6_XAgent_OSX4fe4b9560e99e33dabca553e2eeee5102a854997a4
