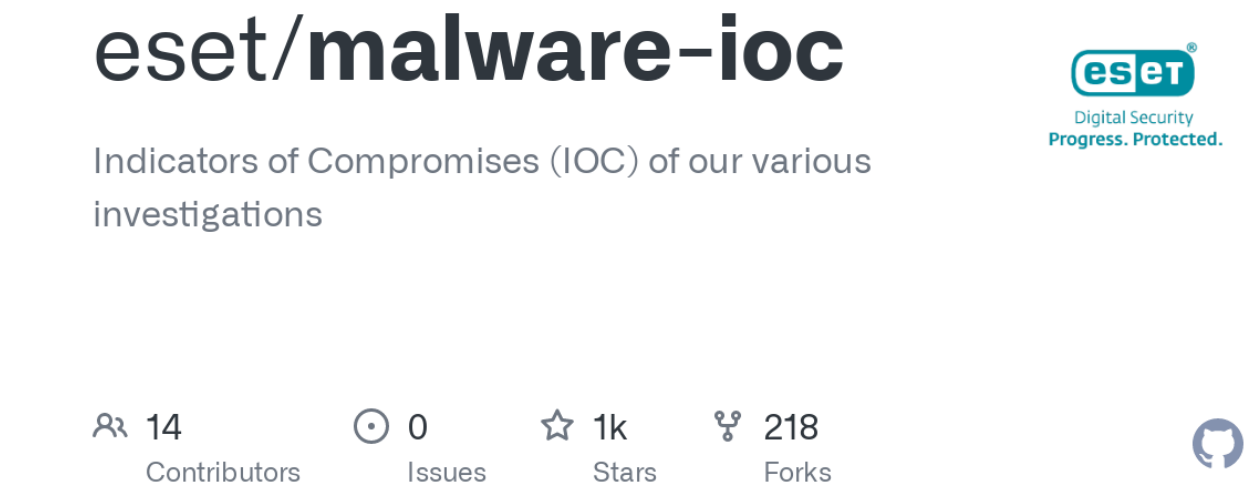
Donot Team — Indicators of Compromise

github.com/eset/malware-ioc/tree/master/donot

eset



An analysis of Donot Team campaigns in 2020 and 2021 is available as a blogpost on WeLiveSecurity.

Gedit - October 2021

Samples

SHA-1	Filename	ESET Detection Name
78E82F632856F293BDA86D77D02DF97EDBCDE918	cdc.dll	Win32/TrojanDownloader.Donot.C
D9F439E7D9EE9450CD504D5791FC73DA7C3F7E2E	wbiosr.exe	Win32/TrojanDownloader.Donot.D
CF7A56FD0613F63418B9DF3E2D7852FBB687BE3F	vdsc.exe	Win32/TrojanDownloader.Donot.E
B2263A6688E512D90629A3A621B2EE003B1B959E	wuaupdt.exe	Win32/ReverseShell.J
13B785493145C85B005E96D5029C20ACCFFE50F2	gedit.exe	Win32/Spy.Donot.A
E2A11F28F9511753698BA5CDBAA70E8141C9DFC3	wscs.exe	Win32/Spy.Donot.B
F67ABC483EE2114D96A90FA0A39496C42EF050B5	gedit.exe	Win32/Spy.Donot.B

Network

Download servers

- `request.soundedge[.]live/access/nasrzolofuju`
- `request.soundedge[.]live/access/birkalirajliruajirjiairuai`
- `share.printerjobs[.]xyz/id45sdjscj/<VICTIM_ID>`

Exfiltration server

`submin.seasonsbackup[.]xyz/backup/<VICTIM_ID>`

Reverse shell server

`80.255.3[.]67`

Gedit - July 2021

Samples

SHA-1	Filename	ESET Detection Name
`A71E70BA6F3CD083D20EDBC83C72AA823F31D7BF`	hxedit.exe	Win32/TrojanDownloader.Donot.N
`E101FB116F05B7B69BD2CAAFD744149E540EC6E9`	lmpss.exe	Win64/HackTool.Ligolo.A
`89D242E75172C79E2F6FC9B10B83377D940AE649`	gedit.exe	WinGo/Spy.Donot.A
`B42FEFE2AB961055EA10D445D9BB0906144647CE`	gedit.exe	WinGo/Spy.Donot.A
`B0704492382186D40069264C0488B65BA8222F1E`	disc.exe	Win32/Spy.Donot.L
`1A6FBD2735D3E27ECF7B5DD5FB6A21B153FACFDB`	disc.exe	Win32/Spy.Donot.A
`CEC2A3B121A669435847ADACD214BD0BE833E3AD`	disc.exe	Win32/Spy.Donot.M
`CBC4EC0D89FA7A2AD1B1708C5A36D1E304429203`	disc.exe	Win32/Spy.Donot.A
`9371F76527CA924163557C00329BF01F8AD9E8B7`	gedit.exe	Win32/Spy.Donot.J
`B427744B2781BC344B96907BF7D68719E65E9DCB`	wuaupdt.exe	Win32/TrojanDownloader.Donot.W

Network

Download server

- `request.submitonline[.]club/orderme/`

Exfiltration servers

- `oceansurvey[.]club/upload/<VICTIM_ID>`
- `request.soundedge[.]live/<COMPUTERNAME>/uload`

Reverse shell servers

- `80.255.3[.]67`
- `37.48.122[.]145`

Gedit – February/March 2021

Samples

SHA-1	Filename	ESET Detection Name
`A15D011BED98BCE65DB597FFD2D5FDE49D46CFA2`	BN_Webmail_List 2020.doc	Win32/Exploit.Agent.UN
`6AE606659F8E0E19B69F0CB61EB9A94E66693F35`	vbtr.dll	Win32/Spy.Donot.G
`0290ABF0530A2FD2DFB0DE29248BA3CABB58D2AD`	bcs01276.tmp (msdn022.dll)	Win32/TrojanDownloader.Donot.P
`66BA21B18B127DAA47CB16AB1F2E9FB7DE3F73E0`	Winhlp.exe	Win32/TrojanDownloader.Donot.J
`79A5B10C5214B1A3D7CA62A58574346C03D54C58`	nprint.exe	Win32/TrojanDownloader.Donot.K
`B427744B2781BC344B96907BF7D68719E65E9DCB`	wuaupdt.exe	Win32/TrojanDownloader.Donot.W
`E423A87B9F2A6DB29B3BA03AE7C4C21E5489E069`	lmpss.exe	WinGo/Spy.Donot.B
`F43845843D6E9FB4790BF70F1760843F08D43790`	innod.exe	Win32/Spy.Donot.G
`4FA31531108CC68FF1865E2EB5654F7B3DA8D820`	gedit.exe	Win32/Spy.Donot.G

Network

Download servers

- `firm.tplinkupdates[.]space/8ujdfuyer8d8f7d98jreerje`
- `firm.tplinkupdates[.]space/yu37hfgde64jskeruqbrgx`

- `space.lovingallupdates[.]life/orderme`

Exfiltration server

`oceansurvey[.]club/upload/<VICTIM_ID>`

Reverse shell server

`80.255.3[.]67`

Gedit – September 2020

Samples

SHA-1	Filename	ESET Detection Name
`49E58C6DE5245796AEF992D16A0962541F1DAE0C`	lmpss.exe	Win32/Spy.Donot.H
`6F38532CCFB33F921A45E67D84D2796461B5A7D4`	prodot.exe	Win32/TrojanDownloader.Donot.K
`FCFEE44DA272E6EB3FC2C071947DF1180F1A8AE1`	prodot.exe	Win32/TrojanDownloader.Donot.S
`7DDF48AB1CF99990CB61EEAEB3ED06ED8E70A81B`	gedit.exe	Win32/TrojanDownloader.Donot.AA
`DBC8FA70DFED7632EA21B9AACA07CC793712BFF3`	disc.exe	Win32/Spy.Donot.I
`CEF05A2DAB41287A495B9413D33F14D94A568C83`	wuaupdt.exe	Win32/Spy.Donot.A
`E7375B4F37ECEA77FDA2CEA1498CFB30A76BACC7`	prodot.exe	Win32/TrojanDownloader.Donot.AA
`771B4BEA921F509FC37016F5FA22890CA3338A65`	apic.dll	Win32/TrojanDownloader.Donot.A
`F74E6C2C0E26997FDB4DD89AA3D8BD5B270637CC`	njhy65tg.dll	Win32/TrojanDownloader.Donot.O

Network

Download servers

- `soundvista[.]club/sessionrequest`
- `soundvista[.]club/orderme/<VICTIM_ID>`
- `soundvista[.]club/winuser`

Exfiltration server

`request.resolverequest[.]live/upload/<COMPUTERNAME>-<Random_Number>`

Reverse shell server

`80.255.3[.]67`

DarkMusical – September 2021

Samples

SHA-1	Filename	ESET Detection Name
`1917316C854AF9DA9EBDBD4ED4CBADF4FDCFA4CE`	rihana.exe	Win32/TrojanDownloader.Donot.G
`6643ACD5B07444D1B2C049BDE61DD66BEB0BD247`	acrobat.dll	Win32/TrojanDownloader.Donot.F
`9185DEFC6F024285092B563EFA69EA410BD6F85B`	remember.exe	Win32/TrojanDownloader.Donot.H
`954CFEC261FEF2225ACEA6D47949D87EFF9BAB14`	forbidden.exe	Win32/TrojanDownloader.Donot.I
`7E9A4A13A76CCDEC880618BFF80C397790F3CFF3`	serviceup.exe	Win32/ReverseShell.J
`BF183A1EC4D88034D2AC825278FB084B4CB21EAD`	srcot.exe	Win32/Spy.Donot.F
`1FAA4A52AA84EDB6082DEA66F89C05E0F8374C4C`	upsvcsu.exe	WinGo/Spy.Donot.A
`2F2EA73B5EAF9F47DCFB7BF454A27A3FBF253A1E`	sdudate.exe	Win32/ReverseShell.J
`39F92CBEC05785BF9FF28B7F33906C702F142B90`	ndexid.exe	Win32/Spy.Donot.C
`1352A8394CCCE7491072AAAC9D19ED584E607757`	ndexid.exe	Win32/Spy.Donot.E
`623767BC142814AB28F8EC6590DC031E7965B9CD`	ndexid.exe	Win32/Spy.Donot.A

Network

Download servers

- `digitalresolve[.]live/<COMPUTERNAME>~<USERNAME>~<HW_PROFILE_GUID>/ekcvilsrkjiasfjkikiakik`
- `digitalresolve[.]live/<COMPUTERNAME>~<USERNAME>~<HW_PROFILE_GUID>/ziuriucjiekuiemoaeukjudjkgfkkj`
- `digitalresolve[.]live/<COMPUTERNAME>~<USERNAME>~<HW_PROFILE_GUID>/Sqieilcioelikalik`
- `printersolutions[.]live/<COMPUTERNAME>~<USERNAME>~<HW_PROFILE_GUID>/orderme`

Exfiltration server

`packetbite[.]live/<COMPUTERNAME>~<USERNAME>~<HW_PROFILE_GUID>/uload`

Reverse shell servers

- `37.120.198[.]208`
- `51.38.85[.]227`

DarkMusical – June 2021

Samples

SHA-1	Filename	ESET Detection Name
`BB0C857908AFC878CAEEC3A0DA2CBB0A4FD4EF04`	ertficial.dll	Win32/TrojanDownloader.Donot.X
`6194E0ECA5D494980DF5B9AB5CEA8379665ED46A`	ertficial.dll	Win32/TrojanDownloader.Donot.Y
`ACB4DF8708D21A6E269D5E7EE5AFB5168D7E4C70`	msofficedll.dll	Win32/TrojanDownloader.Donot.L
`B38F3515E9B5C8F4FB78AD17C42012E379B9E99A`	sccmo.exe	Win32/TrojanDownloader.Donot.M
`60B2ADE3B339DE4ECA9EC3AC1A04BDEFC127B358`	pscmo.exe	Win32/TrojanDownloader.Donot.I

Network

Download servers

- `biteupdates[.]live/<COMPUTERNAME>~<USERNAME>~<VICTIM_ID>/orderme`
- `biteupdates[.]live/<COMPUTERNAME>~<USERNAME>~<VICTIM_ID>/KdkdUe7KmmGFD`
- `biteupdates[.]live/<COMPUTERNAME>~<USERNAME>~<VICTIM_ID>/acdfsgbvdghd`
- `dataupdates[.]live/<COMPUTERNAME>~<USERNAME>~<VICTIM_ID>/DKixeXs44skdqqD`
- `dataupdates[.]live/<COMPUTERNAME>~<USERNAME>~<VICTIM_ID>/BcX21DKixeXs44skdqqD`

Henos – February/March 2021

Samples

SHA-1	Filename	ESET Detection Name

SHA-1	Filename	ESET Detection Name
`468A04B358B780C9CC3174E107A8D898DDE4B6DE`	Procurement Letter Feb 21.doc	Win32/Exploit.CVE-2017-11882.CP
`9DD042FC83119A02AAB881EDB62C5EA3947BE63E`	ctlm.dll	Win32/Spy.Donot.N
`25825268868366A31FA73095B0C5D0B696CD45A2`	stpnaqs.pmt (jptvbh.exe)	Win32/TrojanDownloader.Donot.Z
`540E7338725CBAA2F33966D5C1AE2C34552D4988`	henos.dll	Win32/Spy.Donot.G
`526E5C25140F7A70BA9F643ADA55AE24939D10AE`	plaapas.exe	Win32/Spy.Donot.B
`89ED760D544CEFC6082A3649E8079EC87425FE66`	javatemp.exe	Win32/Spy.Donot.G
`9CA5512906D43EB9E5D6319E3C3617182BBF5907`	pytemp.exe	Win32/Spy.Donot.A

Network

Download servers

- `info.printerupdates[.]online/<USERNAME>/Xddv21SDsxDl`
- `info.printerupdates[.]online/<COMPUTERNAME>~<USERNAME>/XddvInXdl`
- `info.printerupdates[.]online/<COMPUTERNAME>~<USERNAME>/ZuDDey1eDXUl`
- `info.printerupdates[.]online/<COMPUTERNAME>~<USERNAME>/Vyuib45xzlqn`

Exfiltration server

`manage.biteupdates[.]site/<PC_NAME>/uload`