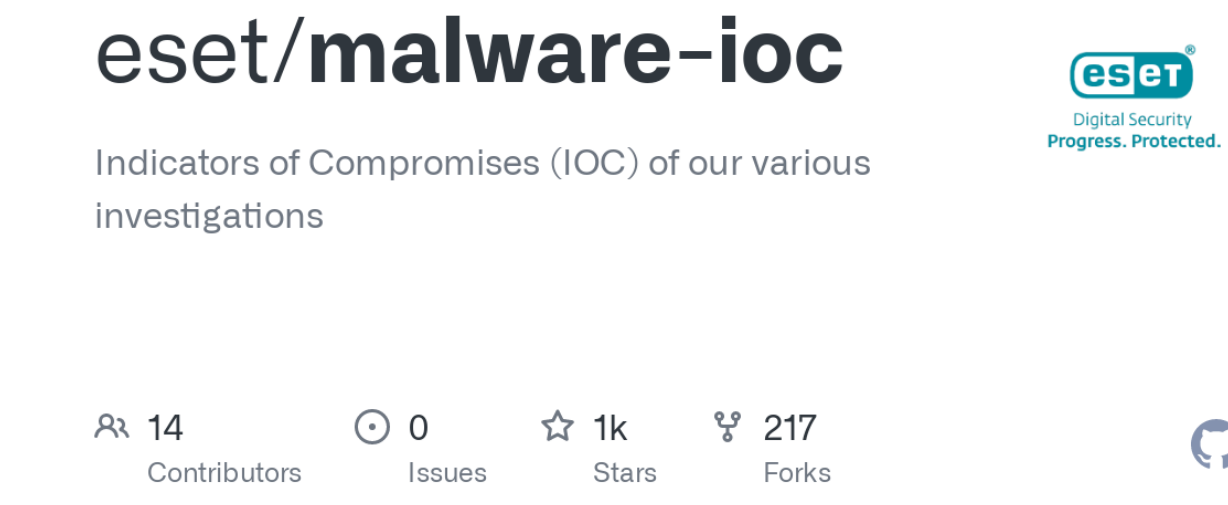
XDSpy Indicators of Compromise

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

eset



The blog post about XDSpy is available on WeLiveSecurity at https://www.welivesecurity.com/2020/10/02/xdspy-stealing-government-secrets-since-2011.

The MISP event is available in `misp-xdspy-event.json`.

Sample hashes

SHA-1 hash	ESET Detection Name	Description
`C125A05CC87EA45BB5D5D07D62946DAEE1160F73`	JS/TrojanDropper.Agent.OAZ	Spearphishing email (2015)
`99729AC323FC8A812FA2C8BE9AE82DF0F9B502CA`	LNK/TrojanDownloader.Agent.YJ	Malicious LNK downloader
`63B988D0869C6A099C7A57AAFEA612A90E30C10F`	Win64/Agent.VB	XDDown
`BB7A10F816D6FFFECB297D0BAE3BC2C0F2F2FFC6`	Win32/Agent.ABQB	XDDown (oldest known sample)
`844A3854F67F4F524992BCD90F8752404DF1DA11`	Win64/Spy.Agent.CC	XDRecon

SHA-1 hash	ESET Detection Name	Description
`B333043B47ABE49156195CC66C97B9F488E83442`	Win64/Spy.Agent.CC	XDUpload
`83EF84052AD9E7954ECE216A1479ABA9D403C36D`	Win64/Spy.Agent.CC	XDUpload
`88410D6EB663FBA2FD2826083A3999C3D3BD07C9`	Win32/Agent.ABYL	XDLoc
`CFD43C7A993EC2F203B17A9E6B8B392E9A296243`	Win32/PSW.Agent.OJS	XDPass
`3B8445AA70D01DEA553A7B198A767798F52BB68A`	DOC/Abnormal.V	Malicious RTF file that downloads the CVE-2020-0968 exploit
`AE34BEDBD39DA813E094E974A9E181A686D66069`	Win64/Agent.ACG	XDDown
`5FE5EE492DE157AA745F3DE7AE8AA095E0AFB994`	VBS/TrojanDropper.Agent.OLJ	Malicious script (Sep 2020)
`B807756E9CD7D131BD42C2F681878C7855063FE2`	Win64/Agent.AEJ	XDDown (most recent as of writing)

Filenames / Paths

- `%APPDATA%\Temp.NET\archset.dat`
- `%APPDATA%\Temp.NET\hdir.dat`
- `%APPDATA%\Temp.NET\list.dat`
- `%TEMP%\tmp%YEAR%%MONTH%%DAY%_%TICK_COUNT%.s`
- `%TEMP%\fl637136486220077590.data`
- `wgl.dat`
- `Windows Broker Manager.dat`
- `%TEMP%\Usermode COM Manager.dat`
- `%TEMP%\Usermode COM Manager.exe`

- `%APPDATA%\WINinit\WINlogon.exe`
- `%APPDATA%\msprotectexp\mswinexp.exe`
- `%APPDATA%\msvdemo\msbrowsmc.exe`
- `%APPDATA%\Explorer\msdmcm6.exe`
- `%APPDATA%\Explorer\browsms.exe`

C&C servers

Used in 2019 and 2020

- `downloadsprimary[.]com`
- `filedownload[.]email`
- `file-download[.]org`
- `minisnowhair[.]com`
- `download-365[.]com`
- `365downloading.com`
- `officeupdtcentr[.]com`
- `dropsklad[.]com`
- `getthatupdate[.]com`
- `boborux[.]com`
- `easytosay[.]org`
- `daftsync[.]com`
- `documentsklad[.]com`
- `wildboarcontest[.]com`
- `nomatterwhat[.]info`
- `maiwegwurst[.]com`
- `migration-info[.]com`
- `jerseygameengine[.]com`
- `seatwowave[.]com`
- `cracratutu[.]com`

- `chtcc[.]net`
- `ferrariframework[.]com`

Old network infrastructure

- `62.213.213[.]170`
- `93.63.198[.]40`
- `95.215.60[.]53`
- `forgeron[.]tk`
- `jahre999[.]tk`
- `omgtech.000space[.]com`
- `podzim[.]tk`
- `porfavor876[.]tk`
- `replacerc.000space[.]com`
- `settimana987[.]tk`