New Fileless Botnet Novter Distributed by KovCoreG Malvertising Campaign

Appendix

Indicators of Compromise (IoCs)

Hashes related to Novter:

SHA-256	File Name and/or Attribution	Trend Micro Detection	TrendX Detection
1692f3b6619a6aca2e41a473d146f7a333f54e86ce507146e626e2d0f82b7c0d	05sall.js (all_socks_05/Nodster module)	Trojan.JS.Nodster.A	Downloader.JS.TRX.XXJSE9EFF011R5B53
022106b4da6d0049f6d3f790b0a8c46923f24a09f10071d49f47388da9d1c298	bav01.js (block_av_01 module)	Trojan.JS.WINDIVERT.B	Downloader.JS.TRX.XXJSE9EFF011, Downloader.JS.TRX.XXJSE9EFF011R5B53
b7c803fbdc13b22471339fcef6e9dfb4a818ed2857576e81d67887067a285442	em_02.js (call_02 module)	Trojan.JS.WINDIVERT.A	Downloader.JS.TRX.XXJSE9EFF011R5B53
a82dd93585094aeba4363c5aeedd1a85ef72c60a03738b25d452a5d895313875	module.avi.exe	Trojan.Win32.Novter.A	Troj.Win32.TRX.XXPE50FFF031
fc523f842e9b17b2706e489ffb537d183752e371d731fccda03deacad4f50c6b	Player1558973917.hta	Trojan.JS.KovCoreG.A	Downloader.JS.TRX.XXJSE9EFF011R5B53
4f600b1c0db498dcdb71e5c2750b8636f66fc7a0712e565ffb28fe4bd214b3b1	Nodster-related module	Trojan.JS.Nodster.A	
90f6e2a250175da3ddf03064e65c49eb033d52059be538f89565f4bb915e0e60	Nodster-related module	Trojan.JS.Nodster.A	
b7f76bfeb39f3ab30210ca78465927854f712b7d332091c476cd703095d27386	Nodster-related module	Trojan.JS.Nodster.A	
ba04eacaa80bb5da6b02e1e7fdf3775cf5a44a6179b2c142605e089d78a2f5b6	Payload/Novter-related	Trojan.Win32.Novter.A	
2f4a9ef2071ee896674e3da1a870d4efab4bb16e2e26ea3d7543d98b614ceab9	Payload/Novter-related	Trojan.Win32.Novter.A	
77498f0ef4087175aa85ce1388f9d02d14aaf280e52ce7c70f50d3b8405fea9f	Payload/Novter-related	Trojan.Win32.Novter.A	
b2d29bb9350a0df93d0918c0208af081f917129ee46544508f2e1cf30aa4f4ce	Payload/Novter-related	Trojan.Win32.Novter.A	
bf2cdd1dc2e20c42d2451c83b8280490879b3515aa6c15ab297419990e017142	Payload/Novter-related	Trojan.Win32.Novter.A	
a7656ccba0946d25a4efd96f4f4576494d5f1e23e6ad2acc16d2e684656a2d4f	Payload/Novter-related	Trojan.Win32.Novter.A	

Related URLs/Domains:

- hxxp://37[.]1[.]223[.]178/qmuw3fwdfw/tell2.dat (call_02 module URL)
- hxxp://37[.]1[.]223[.]178/qmuwwedfw/block_av_01.dat (block_av_01 module URL)
- hxxp://1065695240[.]rsc[.]cdn77[.]org/aefgwehh/05sall.dat (all_socks_05/Nodster’s module URL)
- hxxp://1118069275[.]rsc[.]cdn77[.]org/aefgwehh/05sall.dat (all_socks_05/Nodster’s module URL)
- bo0uiomeglecaptures[.]net (KovCoreG’s malvertising domain)
- uoibppop[.]tk (technical support scam’s domain)

IP Addresses related to Novter’s C&C servers:

- 5[.]61[.]42[.]103
- 37[.]1[.]221[.]156
- 37[.]252[.]8[.]85
- 37[.]252[.]10[.]66
- 91[.]247[.]36[.]14
- 92[.]187[.]110[.]52
- 185[.]243[.]114[.]53

IP Addresses related to Nodster’s C&C servers:

- 69[.]30[.]231[.]60
- 69[.]197[.]179[.]20
- 92[.]187[.]110[.]52
- 103[.]195[.]100[.]246
- 176[.]9[.]117[.]194
- 192[.]187[.]97[.]156

TREND MICRO™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information.

Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on new threats techniques. We continually work to anticipate new threats and deliver thought-provoking research.

www.trendmicro.com