TREND MICRO | research

‘Purple Fox’ Fileless Malware with Rookit Component Delivered by Rig Exploit Kit Now Abuses PowerShell

Appendix

Indicators of Compromise (IoCs)

File Name	SHA-256	Trend Micro Detection	TrendX Detection
1808164.jpg	07191e65af30541f71e876b6037079a070a34c435641897dc788c15e5f62f53c	Trojan.Win64.CVE20188120.C	Troj.Win32.TRX.XXPE50FFF031
1808132.jpg	b2cb65c9ac36f1e3fb31dfd5235c29b396be0968e6b225d625dc3c8fd72395f4	Trojan.Win32.CVE20188120.B	Troj.Win32.TRX.XXPE50FFF031
1505132.jpg	61113a0acd6469ce0d860db55c2afa3cdcbac2f5411fe8259cca43c10c042239	TROJ_CVE20151701.B	Troj.Win32.TRX.XXPE50FFF031
MsE7DEA78AApp.dll	db09af7752eab8227c9ee1edad061a13aba08a6a53289a9c9bba9da2e6cc1f5f	Trojan.Win32.FUPORPLEX.B	Troj.Win32.TRX.XXPE50FFF031
winupdate32.log	517a523039a21e1961088cac8236bf5f6ee197d6a47d08abf114ee3418af0c08	Trojan.Win32.FUPORPLEX.A	Troj.Win32.TRX.XXPE50FFF031
winupdate64.log	87ea8d5bcd1056e76af822896db63f07732dbfab3fc632e7cf13802ae68afc40	Trojan.Win64.FUPORPLEX.A	Troj.Win32.TRX.XXPE50FFF031
1603264.jpg	33a584a0d4907b063af867fd33cc39362b74e96e72d2ad97db7748131364eab1	TROJ64_EXPLOYT.THFAAAH	
1.htm-1	d9155d5e89692fac89a4defeb146ab6ad508d951bc4948067b44e5d0a6582b72	Trojan.VBS.CVE20188174.AMS	
driver.94775000.sys	3e2c3d27d06c3b8a0106282b5d24dc6a44af7fdad74bc4993a3f3bcb7a82858d	HackTool.Win32.Hider.AA	
2.htm-1	a5a6be8b51439c793d903fb92c952c729db8e8050010c499607ee512f42bceff	Trojan.VBS.CVE20146332.B	
4U22nOJHFdDmYcgCS.jpg	09a6fe2764de81c7c5d588dc0542230a0d36aac69305139349fa43f4ab5a09d4	Trojan.Win32.FUPORPLEX.A	
19_.htm-1	507fbe71ec4e059a6cffbf1f7c075073e51c20fa1bb0c9dbc830b5ad5179450a	Trojan.HTML.IFRAME.ASUQK	
pe.jpg	14ae024e8e580904113eea52ce2a000b37b2998c2f257d3bc2cd176e8d9de1a2	Trojan.PS1.POWERSPLOIT.B	
1505164.jpg	ca7bd2830405ed53fd7f56738d7644ff8ecfd5bc63d079d322c99601c6106843	Trojan.Win64.CVE20151701.A	
1603232.jpg	f0b0e0548b218fb81940a4daf85c3709b2159bb357cab2f55576af3d75d47094	HKTL_PRIVESC	
1.swf	498496827afc0aa5960d1cb1d60f7ae7699e0906e3a8c657b6864cff10772df0	Trojan.SWF.RIGEK.AC	
hta.hta-1	164e96f9c19277d40cf58102c1d6fd75dab47bce4f79065ef996a2588b3f737a	Trojan.PS1.POWERSPLOIT.B	
ps004.jpg	ac05a938bbfc4ff0daeb1e45b6ccfdd7cae5bd6aa6e54c49ec6c8feef2ae06c4	Trojan.PS1.POWERSPLOIT.B	

Related URLs, Domains, and IP Addresses:

- hxxp://141[.]98[.]216[.]130/1808164[.]jpg
- hxxp://141[.]98[.]216[.]130/1603264[.]jpg
- hxxp://141[.]98[.]216[.]130/1505164[.]jpg
- hxxp://141[.]98[.]216[.]130/1808132[.]jpg
- hxxp://141[.]98[.]216[.]130/1603232[.]jpg
- hxxp://141[.]98[.]216[.]130/1505132[.]jpg
- hxxp://141[.]98[.]216[.]130/pe[.]jpg
- hxxp://jeitacave[.]org/ps004[.]jpg
- hxxp://nw[.]brownsine[.]com/
- hxxp://zopso[.]org/

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