APT17、マイクロソフトの「TechNet」をマルウェア拡散に悪用

malware-log.hatenablog.com/entry/2015/05/18/000000_1

2015-05-18

【概要】

■攻撃者

APT17, Hidden Lynx, Deputy Dog, Aurora Panda, Tailgater Team, Dogfish

■発生事象

2014年末に、Microsoft TechNetのフォーラムに、偽装されたマルウェア拡散用のC＆Cコードが埋め込まれているのを発見

【ニュース】

> ◆中国ハッカー集団、マイクロソフトの「TechNet」をマルウェア拡散に悪用 (ZDNet, 2015/05/18 11:25)
> http://japan.zdnet.com/article/35064621/

> ◆APT Group Embeds Command and Control Data on TechNet Pages (threat post, 2015/05/18 03:03)
> https://threatpost.com/apt-group-embeds-command-and-control-data-on-technet-pages/112881

【関連情報】

> ◆APT17: Hiding in Plain Sight - FireEye and Microsoft Expose Obfuscation Tactic (FireEye, 2015/05/18)
> https://www2.fireeye.com/WEB-2015RPTAPT17.html
> ⇒ https://malware-log.hatenablog.com/entry/2015/05/18/000000_3

【IOC情報】

> ◆7b9e87c5-b619-4a13-b862-0145614d359a.ioc (FireEye)
> https://github.com/fireeye/iocs/blob/master/APT17/7b9e87c5-b619-4a13-b862-0145614d359a.ioc

【関連まとめ記事】

◆全体まとめ
◆攻撃組織 / Actor (まとめ)
◆標的型攻撃組織 / APT (まとめ)

> ◆APT17 / Hiden Lynx (まとめ)
> https://malware-log.hatenablog.com/entry/APT17

【インディケータ情報】

■ハッシュ情報(MD5)

> - de56eb5046e518e266e67585afa34612
> - 195ade342a6a4ea0a58cfbfb43dc64cb
> - 4c21336dad66ebed2f7ee45d41e6cada
> - 0370002227619c205402c48bde4332f6
> - ac169b7d4708c6fa7fee9be5f7576414
> - 5f2fcba8bd42712d9975da208a1cc0ca
> - 5d16e5ee1cc571125ab1c44ecd47a04a
> - da88e711e4ffc7c617986fc585bce305
> - c016af303b5729e57d0e6563b3c51be4
> - 0b757d3dc43dab594262579226842531

■IPアドレス

> - 130.184.156.62
> - 69.80.72.165
> - 110.45.151.43
> - 121.101.73.231
> - 103.250.72.39
> - 148.251.71.75
> - 217.198.143.40
> - 178.62.20.110
> - 175.126.104.175
> - 103.250.72.254
> - 1.234.52.111
>
> 出典: https://github.com/fireeye/iocs/blob/master/APT17/7b9e87c5-b619-4a13-b862-0145614d359a.ioc

■7ad8944573fe10ad74b09c964d65c1dadad11b67b18dff8f5ea3bc6fe6c9afbf

MD5	4c21336dad66ebed2f7ee45d41e6cada
SHA1	52f1add5ad28dc30f68afda5d41b354533d8bce3
SHA256	7ad8944573fe10ad74b09c964d65c1dadad11b67b18dff8f5ea3bc6fe6c9afbf
SHA512	
SSDEEP	1536:kUCfyQleHyebwt7y8daEmjHicZPI6ZhbPxF30c8SlS3YG9VVZR3oOSj6:LCf1leHyeQ7y8daEmjHicZPI6ZhrlJ9P
authentihash	7373849314cbfc43d587ea430ed196249491f5b53e6a607e81b24039c4b8977f
imphash	403556d9f4bec7266681160adde7cc7c
File Size	86016 bytes
File Type	Win32 DLL
コンパイル日時	2013-08-26 08:22:30
Debug Path	

File Name	FXSST.DLL
File Path	
生成ファイル	
特徴	Zusy
	BlackCoffee
参考情報	https://www.virustotal.com/ja/file/7ad8944573fe10ad74b09c964d65c1dadad11b67b18dff8f5ea3bc6fe6c9afbf/analysis/
	https://www.reverse.it/sample/7ad8944573fe10ad74b09c964d65c1dadad11b67b18dff8f5ea3bc6fe6c9afbf?environmentId=1