HDDCryptor: Subtle Updates, Still a Credible Threat

Appendix

TrendLabs Security Intelligence Blog
Stephen Hilt and Fernando Mercês

November 2016

Indicators of Compromise (IoCs)

Each file has a unique function, although most of them are part of DiskCryptor open source software. Below are indicators of compromise we've observed over the past few months:

MD5s for "mount.exe"

	MD5	Compilation Timestamp		PDB string
1	c43a77d0fe42be421fa5f4b8adaa2e09	24 Apr 2016	03:00:35	e:\localsave\trunk\crp\crp\release\mount.pdb
2	e5470280d0229e45d87690b93659f646	10 Apr 2016	07:08:03	e:\localsave\trunk\crp\crp\release\mount.pdb
3	e540c93c2fae8f0d8ccee182704378ea	14 Oct 2016	03:21:21	c:\users\public.unkonw\desktop\crp_95\crp_95_02_05_v3\crp\release\mount.pdb
4	74f6bb93888a0b54fd0e0ed6d45da7cc	21 Nov 2016	17:32:39	c:\users\public.unkonw\desktop\crp_95_08_30_v3\crp\release\mount.pdb
5	2472e8c0532996acbaa21c46d1a84fda	23 Nov 2016	10:37:15	c:\users\public.unkonw\desktop\crp_95_08_30_v3\crp\release\mount.pdb

MD5s for RANSOM_HDDCRYPTOR

MD5	File Name	Ver	Compilation Timestamp		Ransomnote (modified dcapi.dll - from DiskCryptor open source software)	"mount.exe" MD5 (*1)
498bdcfb93d13fecaf92e96f77063abf	123.exe	Ver 1	24 Apr 2016	03:00:40	You are Hacked !!!! Your H.D.D Encrypted, Contact Us For Decryption Key (w889901665[at]yandex [.]com) YOURID: 123123	1
409d80bb94645fbc4a1fa61c07806883	139.exe	Ver 1	24 Apr 2016	03:00:40	You are Hacked !!!! Your H.D.D Encrypted , Contact Us For Decryption Key (w889901665[at]yandex [.]com) YOURID: 123139	1
e0358edb797489ffc585e8f517b30f1c	141.exe	Ver 1	24 Apr 2016	03:00:40	You are Hacked !!!! Your H.D.D Encrypted , Contact Us For Decryption Key (w889901665[at]yandex [.]com) YOURID: 123141	1
37c0d7f81f6cb81d50505d9c2d17133b	144.exe	Ver 1	24 Apr 2016	03:00:40	You are Hacked !!!! Your H.D.D Encrypted , Contact Us For Decryption Key (w889901665[at]yandex [.]com) YOURID: 123144	1

MD5	File Name	Ver	Compilation Timestamp		Ransomnote (modified dcapi.dll - from DiskCryptor open source software)	"mount.exe" MD5 (*1)
34fc48ef36d9159b2cd44e2beb8f8d86	152.exe	Ver 1	24 Apr 2016	03:00:40	You are Hacked !!!! Your H.D.D Encrypted , Contact Us For Decryption Key (w889901665[at]yandex[.]com) YOURID: 123152	2
acab552b552725cba7516070ca6fb673	output.exe	Ver 2	10 Apr 2016	07:26:06	You are Hacked! H.D.D Encrypted, Contact Us For Decryption Key(cryptom27[at]yandex [.]com) YOURID: 123180	3
97ea571579f417e8b1c7bf9cbac21994	dsd.exe	Ver 3	21 Nov 2016	17:32:45	*<no ransom note, just minimal changes on "dcapi.dl"l>* s/enter key: /enter_key/	4
682cfb092865e779e01331325130b123	output.exe	Ver 3	23 Nov 2016	10:37:28	You Hacked,ALL Data Encrypted,Contact For Key(cryptom27[at]yandex [.]com) ID:60019	5
38529ecca6f8857442331c40e1bd5f9d	output.exe	Ver 3	23 Nov 2016	10:37:28	You Hacked,ALL Data Encrypted,Contact For Key(cryptom27[at]yandex [.]com) ID:601	5

**1: The MD5 refers to MD5s in the first table (MD5s for "mount.exe").*

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses and governments provide layered content security to protect information on mobile devices, endpoints, gateways, servers and the cloud. All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™, and are supported by over 1,200 threat experts around the globe. For more information, visit www.trendmicro.com.

Securing Your Journey to the Cloud

10101 N. De Anza Blvd.
Cupertino, CA 95014

U.S. toll free: 1 +800.228.5651
Phone: 1 +408.257.1500
Fax: 1 +408.257.2003