Monti Ransomware Unleashes a New Encryptor for Linux

b trendmicro.com/en_us/research/23/h/monti-ransomware-unleashes-a-new-encryptor-for-linux.html

August 14, 2023

Ransomware

The Monti ransomware collective has restarted their operations, focusing on institutions in the legal and governmental fields. Simultaneously, a new variant of Monti, based on the Linux platform, has surfaced, demonstrating notable differences from its previous Linux-based versions.

By: Nathaniel Morales, Joshua Paul Ignacio August 14, 2023 Read time: (words)

Introduction

The Monti <u>ransomware</u>, which has both Windows and <u>Linux-based</u> variants, gained attention from cybersecurity organizations and researchers when it was first <u>discovered in June 2022</u> because of its striking resemblance to the infamous <u>Conti ransomware</u> — not just in name but also the tactics that the threat actors used. The group, operating under the moniker "Monti," has also deliberately emulated the widely recognized tactics, techniques, and procedures (TTPs) of the Conti team, incorporating a substantial number of their tools and even using Conti's leaked source code. Since its discovery, the Monti group has been continuously targeting companies, exposing them on their leak site.

Industry	Count
Legal	3
Financial services	2
Healthcare	2
Others	6

Table 1. The industries of the companies that appeared on the Monti ransomware leak site. Data is from March to August 2023.

Following a two-month break from exposing victims on their leak site, the Monti ransomware group has resumed its malicious activities, this time targeting organizations within the legal and government sectors. Alongside this, a fresh Linux-based variant of Monti (Ransom.Linux.MONTI.THGOCBC) has emerged, displaying significant deviations from its other Linux-based predecessors. Unlike the earlier variant, which is primarily based on the

leaked Conti source code, this new version employs a different encryptor with additional distinct behaviors. As of writing, only three security vendors that had the sample tagged it as malicious on VirusTotal

Comparing the new variant to the old one using BinDiff, we found that it only showed a similarity rate of 29% as opposed to the 99% similarity rate of the older variants and Conti.

Overv	iew												
	Basic Blocks 100.0%			Jumps			Instructions -116.7%	Similarity 0.29					
				(No data to display)				Watched Function	0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0	30 20 20 20			
2169	/ 2169 Matched Fur	nctions											
							▼ 💥 🏶 🗹 Show s	tructural changes	Show only instructions	changed 💌 Sho	w identical		
	Similarity 🗸	Confidence -	Address	Primary Name	Туре	Address	Secondary Name	Туре	Basic Blocks	Jumps			
<u>a</u>	1.00	0.99	004298F0	sub_004298F0	Normal	00444A30	AES_decrypt	Normal	0 1 0		^		
<u>a</u>	1.00	0.99	004299B0	sub_00429980	Normal	00444AF0	private_AES_set_encrypt_key	Normal	0 1 0				
<u>æ</u>	1.00	0.99	0042C3B0	sub_0042C3B0	Normal	004C9CB0	vpaes_set_encrypt_key	Normal	0 1 0				
<u>~</u>	1.00	0.99	0042C3E0	sub_0042C3E0	Normal	004C9CE0	vpaes_set_decrypt_key	Normal	0 1 0		-		
杰	1.00	0.99	0043BD50	sub_0043BD50	Normal	004D3110	gcm_init_clmul	Normal	0 1 0				
杰	1.00	0.99	004E12A0	sub_004E12A0	Normal	004BAF30	def_is_number	Normal	0 1 0				
4	1.00	0.99	004F2E70	sub_004F2E70	Normal	004DAA80	cpy_bmp	Normal	0 1 0				
<u>~</u>	1.00	0.99	004F2E90	sub_004F2E90	Normal	004DAAA0	cpy_univ	Normal	0 1 0				
2	1.00	0.99	0041F580	sub_0041F580	Normal	00440480	CRYPTO_free	Normal	0 5 0	0 5	0		
4	1.00	0.99	004C19B0	sub_004C19B0	Normal	0049E480	RSA_eay_finish	Normal	0 7 0	0 9	0		
杰	1.00	0.99	004E01D0	sub_004E01D0	Normal	004B9F00	policy_node_free	Normal	0 6 0	0 6	0		
4	1.00	0.99	00460EA0	sub_00460EA0	Normal	0045FD60	X509_ALGOR_get0	Normal	0 8 0	0 10	0		
4	1.00	0.99	004CD130	sub_004CD130	Normal	0043F0F0	FIPS_rand_method	Normal	0 2 0	0 1	0		
4	1.00	0.99	00402DDC	sub_00402DDC	Normal	0042E9AC	call_gmon_start	Normal	0 3 0	0 3	0		
<u>a</u>	1.00	0.99	00407BC0	sub_00407BC0	Normal	004356C0	RAND_set_rand_method	Normal	0 3 0	0 3	0		
<u>a</u>	1.00	0.99	0043DC70	sub_0043DC70	Normal	00447AB0	BN_clear	Normal	0 3 0	0 3	0		
*	1.00	0.99	004C6EC0	sub_004C6EC0	Normal	004A3E00	pkey_rsa_cleanup	Normal	0 12 0	0 14	0		
杰	1.00	0.99	0048CAB0	sub_0048CAB0	Normal	0047EA80	X509_policy_level_node_count	Normal	0 4 0	0 5	0		
4	1.00	0.99	004FD530	sub_004FD530	Normal	004E4370	libc_csu_init	Normal	0 4 0	0 5	0		
4	1.00	0.99	0041F1E0	sub_0041F1E0	Normal	004402C0	CRYPTO_free_locked	Normal	0 5 0	0 5	0		
4	1.00	0.99	0047F2B0	sub_0047F2B0	Normal	00474330	X509_VERIFY_PARAM_add0_policy	Normal	0 5 0	0 6	0		
<u>a</u>	1.00	0.99	004299F0	sub_004299F0	Normal	00444B30	_x86_64_AES_set_encrypt_key	Normal	0 20 0	0 27	0		
<u>a</u>	1.00	0.99	0042D140	sub_0042D140	Normal	004CAA40	_bsaes_decrypt8	Normal	0 6 0	0 7	0		
杰	1.00	0.99	004620C0	sub_004620C0	Normal	00460AC0	bn_free	Normal	0 6 0	0 7	0		
4	1.00	0.99	0042C8C0	sub_0042C8C0	Normal	004CA1C0	_bsaes_encrypt8	Normal	0 7 0	0 8	0		
4	1.00	0.99	0045DF40	sub_0045DF40	Normal	0045CB80	EVP_PKEY_meth_free	Normal	0 9 0	0 10	0 🗸		
-		1			1	1							

Figure 1. Comparison of the old and new Monti variants using BinDiff

0						<u> </u>							
erview													
Basic Blocks 100.5%			Jumps 100.4%			Instructions - 150.8%	Similarity 0.99						
				4,000 									
49 / 4049 Matched F	unctions					- A Roma	and all all and an	C they ask in		and Distance			
Similarity (*	Confidence	Address	Primary Name	Tube -	Address	Secondary Name	Type	Basic Ba	rika	Jumps	Identical		
100	0.95	00440100	CRYPTO ant men debug functions	Normal	00440100	CRYPTO get men debug functions	Narmal	0 11	0.0	14			
100	0.95	88425188	sub 0042[100	Normal	0042[100	sub 0042E100	Normal	0 1	0		1		
1.00	0.96	00405240	CMS_SignerInfo_get0_alos	Normal	00485240	CMS_SignerInfo_get0_alos	Normal	0 9	0.0	12			
1.00	0.97	88447988	bn_cnp_words	Normal	00447900	bn_cmp_words	Normal	0 11	0.0	14	0		
1.00	0.97	08434148	BIO.clear_flags	Normal	00434140	810.clear.flags	Normal	0 1	0		_		
1.00	0.97	88434158	BIO_test_flags	Normal	00434150	BIO_test_flags	Normal	0 1	ö				
1.00	0.97	08434168	810.set_flags	Normal	00434160	810.set.flags	Normal	0 1	0				
108	0.97	88434178	BIO_get_callback	Normal	00434170	BIO_get_callback	Normal	0 1	0				
1.00	0.97	00434100	810.set.callback	Normal	00434189	810.set.callback	Normal	0 1	0				
1.08	0.97	88434198	BIO_set_callback_arg	Normal	00434190	BIO_set_callback_arg	Normal	0 1	0				
1.00	0.97	084341//0	810.get.callback.arg	Normal	004341A0	810.get.callback.arg	Normal	0 1	Ő				
1.08	0.97	88434188	BIO_method_name	Normal	00434180	810_method_name	Normal	0 1	0				
1.00	0.97	084341C8	BIO_method_type	Normal	00434100	810_method_type	Normal	0 1	0				
1.00	0.97	88434228	810_get_retry_reason	Normal	00434220	BI0_get_retry_reason	Normal	0 1	0				
1.00	0.97	08434E48	810_s_men	Normal	00434E40	810,s.men	Normal	0 1	0				
1.00	0.97	00435300	RAND_set_fips_drbg_type	Normal	004353E0	RAND_set_fips_drbg_type	Normal	0 1	0				
1.00	0.97	08435848	err_string_data_LHASH_COMP	Normal	00435840	err_string_data_LHASH_COMP	Normal	0 1	0				
1.00	0.97	88439228	PKCS7_SIGNER_INFO_get0_algs	Normal	00439220	PKCS7_SIGNER_INFO_get0_algs	Normal	0 7	0.0	9	0		
1.00	0.97	00430990	FIPS_x931_stick	Normal	0043C990	FIPS_x931_stick	Normal	0 1	0				
1.00	0.97	08430508	FIPS_x931_method	Normal	0043C900	FIPS_x931_method	Normal	0 1	0				
1.00	0.97	08430398	FIPS_drbg_get_app_data	Normal	00430390	FIPS_drbg.get_app_data	Normal	0 1	0				
1.00	0.97	084303A8	FIPS_drbg_set_app_data	Normal	004303A0	FIPS_drbg_set_app_data	Normal	0 1	0				
1.00	0.97	00430300	FIPS_drbg_get_blocklength	Normal	00430380	FIPS_drbg_get_blocklength	Normal	0 1	Ő				
1.00	0.97	004303C0	FIPS_drbg_get_strength	Normal	004303C0	FIPS_drbg_get_strength	Normal	0 1	0				
1.00	6.97	08430308	FIPS_drbg_set_check_interval	Normal	00430500	FIPS_drbg_set_check_interval	Normal	0 1	0				
1.00	0.97	08430308	FIPS_drbg_set_reseed_interval	Normal	004303E0	FIPS_drbg_set_reseed_interval	Normal	0 1	0				

Figure 2. Comparison of the old Monti variant and Conti ransomware using Bindiff

Analysis

The new Linux variant accepts the following command line arguments, omitting some arguments from its older variant and adding the *--whitelist* parameter. The following table shows the added parameters in bold text while the removed parameters from the old variant are shown in italicized text.

Argument	Description
help	Displays arguments usage
path <string></string>	Path to be encrypted
whitelist <string></string>	List of VMs to be skipped
vmkill	Option to Kill virtual machine (VM)
detach	Detach from terminal
size	removed
log	removed
vmlist	removed

Table 2. The command line arguments accepted by the new variant

Compared to its predecessor, the current version also employs the *-type=soft* parameter to terminate virtual machines on the system (as opposed to the *--type=hard* parameter). The shift to *--type=soft* suggests that the threat actors behind Monti may have chosen this approach to minimize the risk of immediate detection while carrying out their activities.

execlp("esxcli", "esxcli", "vm", "process", 5234374LL, "--type=soft", "--world-id", v11, 0LL);

Figure 3. Code snippet showing the -type=soft parameter used to terminate virtual machines Monti's developers also tampered with the */etc/motd* and *index.html* files, replacing their contents with a ransom note announcing that the server has been successfully infiltrated. Note that MOTD (or Message of the Day) is a text message displayed when a user logs in to a Linux operating system.

sub_4042B0("/etc/motd", off_7633E8); // RANSOM NOTE _Figure 4. sub_4042B0("/usr/lib/vmware/hostd/docroot/index.html", buf);

Function used to tamper files

	-		×			
File Actions Edit View Help						
All of your files are currently encrypted by MONTI strain. If you don't who we are - just "Google it."	kno	w				
As you already know, all of your data has been encrypted by our softwar It cannot be recovered by any means without contacting our team directl	e. y.					
DON'T TRY TO RECOVER your data by yourselves. Any attempt to recover your dat a (including the usage of the additional recovery software) can damage your f iles. However, if you want to try - we recommend choosing the data of the l <u>owest value</u> .						
DON'T TRY TO IGNORE us. We've downloaded a pack of your internal data a ready to publish it on our news website if you do not respond. So it will be better for both sides if you contact us as soon as possib	nd a le.	are				
DON'T TRY TO CONTACT feds or any recovery companies. We have our informants in these structures, so any of your complaints will be immediately directed to us. So if you will hire any recovery company for negotiations or send requests to the police/FBI/investigators, we will consider this as a hostile intent and initiate the publication of whole compromised data immediately.						
To prove that we REALLY CAN get your data back - we offer you to decryp random files completely free of charge.	t tv	vo				
You can contact our team directly for further instructions through our e:	webs	sit				

Figure 5. The new content of /etc/motd

Infection marker

One of the additions of this new variant is that it appends the bytes "MONTI" followed by an additional 256 bytes that is linked to the encryption key.

🔜 Hiew: 5.monti											
5.monti				↓FRO					0	051A578 Hiew 7.20	(c)SEN
0051A380:	09 B:	L D9	BD-4B	F6 48	33-66	F5 18	3 D1-28	8D F6	A 6F	o J⊓K÷H3fJt≓(j.o	
0051A390:	1F 18	3 73	78-8F	B8 7B	BD-41	FB 31	7 47-18	EA AI	F 24 -	ŢĮsxäą∢¤A√?GtΩ»\$	
0051A3A0:	6D 10	C 04	8F-3C	9D 31	3D-0E	CC 70) F4-3F	-29 A8	3 18		
0051A3B0:	36 C	0 <u>5</u> A	ØF-A3	A6 C7	3D-43	2B A	35-08	5F E1	L 6C	6 ^L Z₩ú≏ =ú+-5 <mark>●</mark> β1	
0051A3C0:	84 3:	L ØB	65-9A	6F 6F	2D-94	A1 21	D2-FC	4F 81	D ØC	ä1δeUoo-öí.π ⁿ Oì¥	
0051A3D0:	58 2	3 2B	2B-44	B3 8F	<u>C2-27</u>	<u>90 4</u>	1 80-19	74 39	2 30	X#++D[XT, EDC1430	
0051A3E0:	E7 21	E 64	47-8A	FC ØE	05-E5	85 El	3E-71	8C Ø	3 37	τ.dGè"#Ωσàθ>qî♥?	
0051A3F0:	18 5	2 <u>E3</u>	3D-FC	28 2C	68-5C	20 5) RA-58	81 0	85	TWIL="< ,h\ Jizü0å	
00518400:	H1 90	5 F3	D5-25	B4 66	CD-6A	47 91	08-BD	86 13	3 85	1ES FX1F=JGROPANN	
00518410:	FE 14	1 B6	65-5E	56 67	60-H6	53 B:	50-94	5H F2	2 DC		
0051H420:	87 3	8 83	PS-EA	ZE EF	86-8H	ED 40	41-EZ	58 EI	8 30	CTADE HAPPHIXED	
0051H430:	DE G	2 51	HD-CB	4F 46	78-83	OE 70	5 64-1H	DE 34	1 63		
00518440:	FB 4 DO D	7 70	D4-D2	36 03	23-04 04 ED	0D 40	5 03-FZ	01 01	9 (8		
00510450	CP A		74-60	30 HZ	41_00	00 07	A9_40	CD 01	1 33		
00510400-	06 10	. 45	74-07	96 90	41-00 C7_CB	E4 E6	944-40 944-172		5 50	9 CITRAILENSSCEAN	
00510490-	59 A	3 36	27-12	97 34	87-40	83 8	, 01-FJ	- EQ - 21	5 3G 7 87	PBR7USA-TSA-LIT	
00510490-	06 E	1 16	18-06	24 49	E9-1 E	00 F1	93-28	59 E	A 99		
00510400:	24 R	F3	R0-24	24 6F	10-78	B7 C	F5-19	87 15	7 8F	SIII SSotynt Leto	
0051A4B0:	4F 7	A AR	98-83	CØ F2	A0-6E	1F AL	F7-18	61 69	3F	N(Kija L) án kártah)	
0051A4C0:	Ø5 9	a CD	3B-FC	20 89	6B-AE	26 8	47-15	45 E	F 07	ΦE=:" EkczeGδE0+	
0051A4D0:	51 2	1 64	26-86	CE DF	55-7E	18 25	40-EC	28 C	2 4C	Ottñuè:!!I'~→"@oxIII.	
0051A4E0:	C4 Ø	2 80	C4-1D	F2 6F	FA-67	F6 31	ED-6E	2A 01	B B4	$-\Theta C \rightarrow 20 \cdot \alpha + = \Theta n \times 6^{-1}$	
0051A4F0:	2D A	7 E3	C1-50	70 A0	A8-AB	6D 43	4E-53	C9 E	0 25	IL-Ppác KmCNS r.#%	
0051A500:	72 B	3 3C	8A-49	BA 16	ØC-66	3F 61	18-D4	14 80	C AØ	ra<èll_fat 4911á	
0051A510:	C7 43	2 47	72-D8	7F 54	75-DD	CC 30	1 40-0D	89 31	8 10	BGr‡oTu 100 Fe;►	
0051A520:	38 23	2 50	9F-1F	98 BE	39-5B	1C D	7 A4-80	3D 71	E 38	8"Pf♥ij±9[={ ñC=*8	
0051A530:	FØ A:	2 3B	66-97	28 CD	8D-0C	42 Bl	3 99–1B	ØE 66	a 75 -	≡ó;fùζ=ì₽B≟Ö≁∏ju	
0051A540:	54 6	3 22	B3-35	E9 FA	44-06	C3 Ø	7 31-00	17 00	5 EØ	Th" 50 DΦ +1 ±Φα	
0051A550:	CE 80	3 4E	01-09	9A 5F	00-07	0B 01	00-01	23 03	3 01 -	#1N90Ü_ •89_9#♥9	
0051A560:	01 0	5 5D	00-00	01 00	0C-C0	B2 E0	0 0A-01	00 91	E AC	⊡otl © ♀└∭aco,© R-Xa	
0051A570:	9E Ø	00 6	4D-4F	4E 54	49- 5C	14 8	7 D3-57	B6 90	C B1	R MONTING WE	
0051A580:	9D 31	E DB	92-59	55 33	E4-C4	BE AI	E 4F-04	AD 09	9 EF	¥>_ÆYU3Σ—I≪O♦∔ on	
0051A590:	CB E	1 64	4F-05	DØ 71	E7-3F	F4 C	C7-91	21 E	5 B5	Tugan data the second s	
00518580:	DF D	L 6A	17-91	40 20	D3-29	96 52	AE-BA	BB CI	E 86	−∓j ža sj "⊃üR«[]jj¦jä	
00518580:	ZD E	EE	88-91	NA NR	U1-42	13 2	20-82	8F 6	4 D7	-ocjæogen:stodit	
0051H5C0:	D2 BI	10	88-B1	11 38	ZE-FH	C0 81	52-FY	긢뱄	44		
0051H5D0:	33 84	1 25	07-4Z	74 JU	82-6G	CO 37		51 8	5 76		
00514520:		별	06-05	DO DC		BD 71	71-35 20 E0	BC 51	L 00	18- 2-0042-005-1	
00514550:	C4 P	2 22	AC EE	73 FG	D0 14	TH E	3 37 E7	00 01	1 69		
00514000.	01 51		40 36	49 64		A0 0		27 61	6 82	SP Say Darry Land Ly Ry	
00510620-	R5 20		D5 C2	50 60	R5-1C	EE C	RG 54	17 4	2 28		
00510630-	52 0	62	15-02	6F AC	DF-47	OT CO	48-52	89 0	5 5 8	Raú Súo 2 CO HISEAN	
00510640	OR O	56	87-R5	90 70	08-49	A1 11	46-91	87 09	276	Solu Jin Hitter	
00516650:	FB 6	41	80-50	48 74	20-4D	AA FO	5C-2F	6F 4	2 EF	JmACNHt Ma ⁿ N ^c oB0	
00516660 :	66 4	2 C1	E7-09	6F F4	15-64	37 E	D4-1C	69 30	1 72	fI-ron (SdZ0 b-i0)	
0051A670:	61 E	62	AC-82	C2 C6	60-		_		التكاري ال	a ^w b [%] e ⁺ IIIII	00100/256
1Help 2Put	tBlk	BEdit	t 4Ma	ode 📕	Goto	6Dat	Ref 7S	earch	8Hea	der 9Files 10Quit	

🔜 Hiew: 3.monti															
3.monti					↓F	RO							Ø	0041205 Hiew 7.20	(c)SEN
00041010:	89	30	46	07-BC	84	6D	59-A3	04	EF	42-D2	-5C	72	8C	−0F+ ^y ñmYú♦∩Bπ∖rî	
00041020:	88	48	48	91-F7	F8	53	27-DE	4 C	87	48-E9	53	81	88	êJHæ≈°S'µL≏H0Süê	
00041030:	DØ	DB	<u>74</u>	41-00	ØF	EA	EB-B5	<u>5C</u>	7E	8A-94	<u>5C</u>	EC	34		
00041040:	86	07	FC	5F-ØE	AA	41	DA-B4	8D	21	15-4E	<u>F7</u>	F4	82	°•°_∏-A_fiæ§N≈fé	
00041050:	88	CE.	EA	59-A2	22	EF	88-7D	37	50	41-78	FD	<u>85</u>	52	Timtoone / // Hz / BR	
00041060:	DQ	52	E8	CØ-C7	3E	44	25-23	34	<u>#7</u>	58-33	30	58	H1	HYQ LIPDuo4ºZ3 <x1< td=""><td></td></x1<>	
	1J 3	Fb 2D	55	90-81 on 4 n	1F	62	E7-5F	CY DO	51	4F-DE	11	HZ	ED.		
00041080:	00	30	DC ED	DO-07	DD	38	57-08	DH	20	01-00	04	14 DC	20		
00041070-	RC	55	RC	67-RD	RO D	40 9n	25-20	EÉ.	00	59-13	RG	21	50	1, J, all , X501, 211-1 P	
000410R0:	FR	an	92	FE-40	11	62	30-CE	12	51	F2-C5	h4	F4	90	$\delta = f \parallel J = b = \frac{1}{2} t \alpha \Gamma + E \eta i$	
000410C0 :	52	ÅŘ	2F	DC-5D	69	97	7E-23	ÂÊ	Å2.	FB-2C	ČÊ	D8	έö-	RK/_liù~#ceJ.	
000410D0:	77	81	60	B3-CE	45	Ê3	87-46	37	28	E8-AC	ČĎ	D2	ĞВ.	wiill!ElleF7x0%=nk	
000410E0:	28	81	27	09-6B	3B	ÃØ	1E-1B	D8	ÂĔ	2E-1F	6B	A8	FE	(ii' 0k;á▲+≑«. ¥kč∎	
000410F0:	6A	02	81	F1-F0	08	3A	BC-00	82	24	5A-BA	67	ØA	AD	jeu±≡∎:4 é\$Z g⊡i	
00041100:	53	5D	98	B9-28	99	6C	AC-45	FD	7F	9B-69	D4	F4	F6 -	Šlÿ¦(Öl&E²o¢i ^l ſ÷	
00041110:	68	75	C4	15-23	EF	67	CA-F6	48	96	EF-88	87	5D	79	hu-S#Ng#+Hûnê≏İy	
00041120:	<u>8D</u>	75	D5	26-E8	78	<u>C7</u>	77-5B	DE	E3	B5-2D	27	<u>9</u> F	72	iu F&∑x] w[Щ=' fr	
00041130:	- 25	55	10	26-ØA	F9	4 E	F9-2D	DC	99	60-42	F4	80	C2	uU-&O'BfC+	
00041140:	H1	ED	FD	71-C2	<u>C5</u>	ZE.	E9-41	80	<u>C8</u>	FF-1F	82	10	84	102 gtt. UAU La Vern	
00041150:	BH	FZ	F8	79-00	DR.	FY.	7B-B6	BF	85	15-F9	HB	bB DC	bb -		
00041150:	05	13	13	E5-22	HJ	60	UP-56 90-03	65	28	25-H3 CC-00	20	BU	r ch		
00041120-	- 7 J	21	102	JH -7D 7R-R9	04	46	10-00	- D2	RE	CC-HO	67	00	12		
00041190:	Ø6	40	43	3E-C1	ØF.	nF.	18-37	ng.	0R	67-23	98	99	йČ –	◆LC>+ELC>+ELC>+CATE	
00041100:	F5	F9	ĈЙ	2D-ØF	67	őD.	C8-4B	32	1F	77-85	C2	9F	ĂČ	J → mom LK2 Vuà + f%	
000411B0:	63	30	83	46-23	14	EA	8E-59	78	DF	22-2B	80	CC .	4D	c<âF#¶ΩäYx [■] "+CIM	
000411C0:	F2	3E	16	EF-A9	62	C5	97-EF	1D	44	E8-60	8E	31	ØE	2>∎n-b+ùn+DQ`Ä1∏	
000411D0:	46	05	88	16-05	8A	45	15-D5	DC	07	6F-16	AØ	5D	AC	F 2 ê <u></u> _†èɧ F ∎•o_á]½	
000411E0:	6F	F7	20	99-BB	F8	61	01-37	68	81	5A-B7	04	51	79	o≈ öղ⁰a©7jüZղ♦Qy	
000411F0:	97	6D	07	F4-4E	<u>C4</u>	E2	4D-06	7B	CA	92-5C	70	AC	05	ùm●ſN-ſM全C出任\1%全	
00041200:	4D	4 F	4 E	54-49	<u>A8</u>	<u>9D</u>	69-33	38	FA	6F-76	05	36	DF	MONTI ¥i3: ov 26	
00041210:	ΕØ	46	DA	60-56	FЮ	ĘΖ	AF-4D	4C	94	E3-FE	FB	17	58	αF ⁻¹ U≡τ≫nL∳lt∎N <u>∓</u> Z	
00041220:	46	10	38	2D-1H	66	15	57-17	70	22	94-36 04 UD	2H	87	Fb C G	FP; # > f gY % phob U n÷	
00041230-	DO	00	22	C7_0C	71	34 D0	n2_00	E C	1E	71 7D	H0 E4	70	22	Cy=≤ aen _l zumaez=E	
00041250-	30	ER	RO	94-R0	81	12	22_2E	21	06	8n-73	80	FØ	20	=011811883>+93680>	
00041260:	D5	96	23	49-7D	81	8F	E1-38	87	20	C6-85	68	ÃÃ	42	nîs I di 868c ! EN 15B	
00041270:	98	FD	99	61-53	B2	BA	FB-AD	D5	6Ž	FC-75	96	31	31	ü²ÖaS∭l√i rg"uü11	
00041280:	8D	9F	3A	22-19	ØA	1B	85-FF	1 E	05	EC-A6	D8	35	7F	if:"↓0+à ▲✿መ≏‡5△	
00041290:	EB	A3	1 B	CØ-F4	ED	43	70-2B	88	29	04-5D	7F	BØ	93	δú←└ſøCp+ê>♦]△∭ô	
000412A0:	64	EB	64	42–8F	EØ	22	89-00	80	E7	C1-11	99	22	D6	dδdBÅα″ë Çτ∔4Ö‴π	
000412B0:	9E	60	5C	0C-BE	15	6F	6B-C1	20	2B	83-E3	1A	B8	82	^R `\\$±§ok⊥_+â∏→ ₇ é	
000412C0:	C4	BB	C2	2C-B5	5F	E1	5F-E6	92	F5	D7-AA	20	80	47	TTT+1_0_WEJ11p1G	
00041200:	AD.	U 5	C3	6F-70	CA	18	HF-66	СN	A1	50-32	50	61	H B	¥2fop=T»f LiP2\a%	
000412E0:	21	χŋ	11	91-D7	ED	31	8H-64	22	2F	GE-04	26	HN	75		
00041210	54	H8 01	07	5B-H4 CE-E4	14	20	DH AD	02	17	92 <u>6</u> 7	46	37	EA	04048 COOP	01007256
Thelp 2Put	FR11				nde		Goto	6	latI	lef 79	eave	h 9	Hea	der 9Files 100uit	00100/230
	OD TI		Sull(Jue		3000		Juci	101 10	ourt	0	nca	act a rice maguit	

Figure 6. Comparison of two files encrypted by Monti ransomware Before proceeding with its encryption routine, the ransomware will check specific conditions. First, it checks whether the file size is 261 bytes or below, which corresponds to the size of the infection marker it appends after encryption. If this condition is met — indicating that the file is not encrypted given that its size is smaller than the appended infection marker — the ransomware proceeds with the infection process.

If the initial condition is not met, Monti will then check the last 261 bytes of the file to verify the presence of the string "MONTI." If this string is detected, the file will be skipped, signifying that it has already been encrypted. However, if the string is not found, the malware will proceed with the encryption process for the file.

```
lseek(v4, -261LL, 2);
 v5 = old;
 v6 = "[%s] Error reading file meta before crypt.\n";
 if ( read(v4, &buf, 5uLL) == -1 )
 {
ERROR_LABEL:
   LOGGING 4058D0(v6, v5);
   LOWORD(\vee 32) = 2;
   fcntl(v4, 7, &v32);
   close(v4);
   return 0;
 }
 lseek(v4, 0LL, 0);
 if ( buf == 0x544E4F4D && BYTE4(buf) == 0x49 )// 0x544E4F4D => "TNOM" 0x49 => "I"
   v5 = old;
   v6 = "[%s] File already encrypted.\n";
   goto ERROR_LABEL;
 }
```

Figure 7. Code snippet to check for the presence of the "MONTI" string via the last 261 bytes of the file to be encrypted

Checking file sizes and Intermittent encryption

Based on our analysis, the new ransomware variant employed AES-256-CTR encryption using *evp_enc* from the OpenSSL library instead of Salsa20, which is implemented by the old variant

We also discovered that the sample we analyzed employs various encryption methods for files. Unlike the previous variant, which utilized a *--size* argument to determine the percentage of the file to be encrypted, this new variant solely relies on the file size for its encryption process. In this section, we break down the different ways that the Monti ransomware determines the size of the file to be encrypted.

```
v7 = sub_410C00();
sub_40CC10(v25, v7, 0LL, &v36, &v38);
initialization of Cipher value stored in v7
```

```
if ( v21 )
         {
           v22 = v21(a1, 0LL, 0LL, 0LL, v18);
           if (\sqrt{22} = -1)
           {
             sub_40A260(6u, 124, 133, "evp_enc.c", 632);
           }
           else if (v22)
           {
             v11 = *a1;
             goto LABEL_24;
           }
         }
                                                                  Figure 9.
         else
         {
           sub_40A260(6u, 124, 132, "evp_enc.c", 626);
         }
         LODWORD(v18) = 195;
ABEL 54:
         sub_40A260(6u, 123, 134, "evp_enc.c", v18);
         return 0LL;
       }
ABEL 40:
       v27 = sub_41F220(v19, "evp_enc.c", 178LL);
       a1[15] = v27;
       if ( 1v27 )
```

Function 40CC10 containing evp_enc.c from the OpenSSL library

.rodata:0000000004FFF20 word_4FFF2	.0 dw	38Ah	;	DATA XR	EF: s	sub_410C00+C^o	
.rodata:0000000004FFF22	dw	0					
.rodata:0000000004FFF24	dw	1					
.rodata:0000000004FFF26	dw	0					
.rodata:0000000004FFF28	dw	20h					
.rodata:0000000004FFF2A	dw	0					
.rodata:0000000004FFF2C	dw	10h					
.rodata:0000000004FFF2E	dw	0					
.rodata:0000000004FFF30	dw	4005h					
.rodata:0000000004FFF32	dw	0					
.rodata:0000000004FFF34	dw	0					
.rodata:0000000004FFF36	dw	0					
.rodata:0000000004FFF38	dw	0F3B0h					
.rodata:0000000004FFF3A	dw	40h					
.rodata:0000000004FFF3C	dw	0					
.rodata:0000000004FFF3E	dw	0					
.rodata:0000000004FFF40	dw	0F790h					
		1					

Figure 10. 0x38A, which corresponds to AES-256-CTR in OpenSSL nid

Figure 11. Checking file size and determining the size to be encrypted The sample will only encrypt the first 100,000 (0xFFFF) bytes of the file and append its infection marker at the end of the file if the file size is larger than 1.048MB but smaller than 4.19MB.

Hiew: B.Oxt.monD	L I X Hiew: B.txt			
B tyt monti IEPO	BBBEEFEE High 7 2B (c)SEN			
	00000080:	42 42 42 42 42 42 42 42 42 42 4	2 42 42 42 42 42 42 42 42 BBBBBBBBB	JEBBBBBBB 💽
000FFETF: 4F IF 18 00-98 00 61 73-H4 2F CT 10-01 0C H6 0	00000090:	42 42 42 42 42 42 42 42 42 42 42	2 42 42 42 42 42 42 42 BBBBBBBBB	BBBBBBB
8 000FFE8F: 16 16 92 E5-FC 51 B4 C7-1E 83 C7 06-7C 16 B1 1	2Eo"Q18 +1 _81	42 42 42 42 42 42 42 42 42 42 42	2 42 42 42 42 42 42 42 8888888888	REPRESE
800FFF9F 94 78 48 CD-2C 3C 71 C0-10 F4 84 4C-49 24 F4 8	$\tilde{n}(K = \langle \alpha^{L} \rangle f + L I S \Sigma C$			0000000
000FFF0F, D5 D2 5D 02-70 D7 F0 FD-20 10 02 44-DD 15 C2 C	m1201249120 .ht	42 42 42 42 42 42 42 42 42 4	2 42 42 42 42 42 42 42 42 88888888888	REBRERE
000FFERF: 03 02 30 33 10 01 F0 E0 33 10 03 44 00 FE 02 0	000000C0:	42 42 42 42 42 42 42 42 42 42 42	2 42 42 42 42 42 42 42 BBBBBBBB BB	388888888
000FFEBF: F3 BB DF 06-CE 46 9E 60-6B B8 E7 F3-91 0E 72 0		42 42 42 42 42 42 42 42 42 42 42	2 42 42 42 42 42 42 42 BBBBBBBBB	BBBBBBB
8 000FFECF: 0E 90 A4 4C-BF 1E 68 F4-E1 59 9B 91-B2 85 F8 7	5 JEñL₁ +h ſBY¢æ à°u popporo.	HO HO HO HO HO HO HO HO HO	2 H2 H2 H2 H2 H2 H2 H2 DDDDDDDDD	0000000
800FFEDE C5 84 CD F9-55 8F DR 23-F0 1C 95 51-13 58 FF 5				0000000
		42 42 42 42 42 42 42 42 42 42 4	2 42 42 42 42 42 42 42 42 8888888888	3BBBBBBBB
000FFEEF: 50 02 TC 32-TT 35 TO 42-F6 34 42 C4-DT FD DD H	00000100:	42 42 42 42 42 42 42 42 42 42	2 42 42 42 42 42 42 42 BBBBBBBBB	BBBBBBB
8 000FFEFF: F5 21 A9 B4-B6 B7 3E 1C-24 43 A4 13-AD 3F 40 A	D J!r1fm>-\$Cn‼;?8a	42 42 42 42 42 42 42 42 42 42 42	2 42 42 42 42 42 42 42 RRRRRRRR	RRRRRRR
000FFF0F: 8E 95 E7 78-39 00 F3 58-79 50 F0 28-F3 E7 C5 C	Aor(9JSXuPE+Stell	NO NO NO NO NO NO NO NO		00000000
000FFF1F, 26 FF 09 28-72 11 09 0F-12 PC 46 C0-29 CC 68 2	\$60(adout][[]]]	12 12 12 12 12 12 12 12 12 12	2 12 12 12 12 12 12 12 12 DDDDDDDD	0000000
	00000130:	42 42 42 42 42 42 42 42 42 42	2 42 42 42 42 42 42 42 8888888888	388888888
000FFF2F: 08 46 66 11-36 88 88 43-00 0F 41 DH-12 HB H3 6	00000140:	42 42 42 42 42 42 42 42 42 42 42	2 42 42 42 42 42 42 42 BBBBBBBBB	BBBBBBB
8 000FFF3F: 88 51 A5 D4-A8 62 BF E3-DC 98 59 07-38 31 BF 1	3] QN 5%b] II ¢Y+; 1] !! 00000150.	42 42 42 42 42 42 42 42 42 42	2 42 42 42 42 42 42 42 RERERERE	RRRRRRR
000FFF4F: F7 25 69 44-30 1A 80 EF-68 B2 8D C6-20 06 EE 7	S%iD8+C∩h@i ⊨ +Ex			00000000
000FFFFFF 75 0F 97 83-62 7F 71 F2-40 DB 07 50-0F F0 31 C	URNIN (200 904-1)	12 12 12 12 12 12 12 12 12 12	2 42 42 42 42 42 42 42 42 BBBBBBBBB	0000000
	00000170:	42 42 42 42 42 42 42 42 42 42 4	2 42 42 42 42 42 42 42 8BBBBBBB BB	3BBBBBBB
000FFF6F: 21 FC 73 15-72 72 80 C6-29 19 C4 DE-44 9D 89 B	00000180:	42 42 42 42 42 42 42 42 42 42	2 42 42 42 42 42 42 42 BBBBBBBBB	BBBBBBB
000FFF7F: 9D 84 3B 74-2A 8F C2 96-E0 4D 00 76-F3 24 97 B	S ¥ä;t×A⊤ûαM ⊍≤Şù	42 42 42 42 42 42 42 42 42 42 42	2 42 42 42 42 42 42 42 RRRRRRRR	RRRRRRR
8000FFF8F: EC F3 99 EF-7E 16 AB 8A-6D 21 D5 FA-0D CF A3 7	∞≤00~_%èmt F: J=úo	NO NO NO NO NO NO NO NO NO		00000000
800FFF9F 30 BB 20 F8-93 00 15 81-BF 0F 08 85-FB 05 04 6	a sa °ôásúd Liàd‡ki			ODDDDDD
	00000180:	42 42 42 42 42 42 42 42 42 42 4	2 42 42 42 42 42 42 42 88888888888	(BBBBBBB
000FFFHF: 30 66 HE FU-13 HB 39 D0-50 33 63 FF-66 36 96 2	000001C0:	42 42 42 42 42 42 42 42 42 42	2 42 42 42 42 42 42 42 BBBBBBBBB	BBBBBBB
000FFFBF: 95 F7 AF 86-28 C4 50 C7-F2 5A A2 60-E8 59 56 5	000001D0:	42 42 42 42 42 42 42 42 42 42 42	2 42 42 42 42 42 42 42 BBBBBBBBB	BBBBBBB
000FFFCF: C6 32 BD E1-09 EC E1 97-7F F6 FF 18-6A 7E 3D 8	5 =2 ¹⁰ BC∞Bùo+ †j~=8	42 42 42 42-42 42 42 42 42-43		00000000
000FFFDF: 36 0D 22 E2-00 21 58 CC-80 13 9E D2-43 1E 36 C				0000000
000FFFFFF 31 45 F7 DD-F2 1D 0D 8F-85 65 50 7F-51 50 20 8	15% F#19307~07xc			0000000
	00000200:	42 42 42 42 42 42 42 42 42 42	2 42 42 42 42 42 42 42 888888888 88	(BBBBBBB
000FFFFF: HH 42 42 42 42 42 42 42 42 42 42 42 42 42	00000210:	42 42 42 42 42 42 42 42 42 42	2 42 42 42 42 42 42 42 BBBBBBBBB	BBBBBBB
8010000F: 42 42 42 42 42 42 42 42 42 42 42 42 42	2 BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB	42 42 42 42 42 42 42 42 42 42 42	2 42 42 42 42 42 42 42 BBBBBBBBB	BBBBBBB
8 0010001F: 42 42 42 42 42 42 42 42 42 42 42 42 42	2 BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB	42 42 42 42-42 42 42 42 42-43		00000000
0010002F: 42 42 42 42 42 42 42 42 42 42 42 42 42	2 BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB			0000000
	00000240:	42 42 42 42 42 42 42 42 42 4	2 42 42 42 42 42 42 42 88888888888	REBRERE
	00000250:	42 42 42 42 42 42 42 42 42 42	2 42 42 42 42 42 42 42 42 BBBBBBBBB	(BBBBBBB
0010004F: 42 42 42 42 42 42 42 42 42 42 42 42 42	00000260:	42 42 42 42 42 42 42 42 42 42 42	2 42 42 42 42 42 42 42 BBBBBBBBB	BBBBBBB
0010005F: 42 42 42 42 42 42 42 42 42 42 42 42 42	2 BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB	42 42 42 42 42 42 42 42 42 42 42	2 42 42 42 42 42 42 42 BBBBBBBBB	BBBBBBB
8 0010006F: 42 42 42 42 42 42 42 42 42 42 42 42 42	2 BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB	42 42 42 42-42 42 42 42 42-43		00000000
8 0010007F: 42 42 42 42 42 42 42 42 42 42 42 42 42	2 BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB			00000000
00100005. 42 42 42 42 42 42 42 42 42 42 42 42 42	00000290:	42 42 42 42 42 42 42 42 42 4	2 42 42 42 42 42 42 42 8888888888 88	REBRERE
	000002A0:	42 42 42 42 42 42 42 42 42 42	2 42 42 42 42 42 42 42 BBBBBBBBB	38888888
0010003F: 42 42 42 42 42 42 42 42 42 42 42 42 42	00000280:	42 42 42 42 42 42 42 42 42 42	2 42 42 42 42 42 42 42 BBBBBBBBB	BBBBBBB
001000AF: 42 42 42 42 42 42 42 42 42 42 42 42 42	2 8888888888888888888888888888888888888	42 42 42 42 42 42 42 42 42 42 42	2 42 42 42 42 42 42 42 BBBBBBBBBB	8888888
001000BF: 42 42 42 42 42 42 42 42 42 42 42 42 42	2 BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB	42 42 42 42 42 42 42 42 42 42	2 42 42 42 42 42 42 42 42 500000000	REREER
8 001000CF: 42 42 42 42 42 42 42 42 42 42 42 42 42	BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB			0000000
001000F. 42 42 42 42 42 42 42 42 42 42 42 42 42	BRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR	42 42 42 42 42 42 42 42 42 42	2 42 42 42 42 42 42 42 42 8888888888	6666666
	000002F0:	42 42 42 42 42 42 42 42 42 42 43	2 <mark>42 42 42 42 42 42 42 42 8888888888888</mark>	0019FE60/1703520
001000EF: 42 42 42 42 42 42 42 42 42 42 42 42 42	Help 2P	utBlk_3Edit 4Hode 5Goto	6DatRef 7Search 8Header 9Files	• 100uit -

Figure 12. Encrypted file (left) vs original file (right)

If the file size exceeds 4.19MB, it employs a Shift Right operation to calculate the total size of the file to be encrypted (which depends on the actual file size). Meanwhile, files with a size smaller than 1.048MB will have all their content encrypted.



Figure 13. Encrypted file (left) vs original file (right). Using 0x635818(total size), Shift Right 2 is equivalent to 0x18D606 (bytes to be encrypted)

As with previous variants, the new version appends the *.monti* file extension to the encrypted files and drops its ransom note *readme.txt* to every directory.





Figure 14. Appending the .monti suffix to encrypted files (top) and the ransom note While analyzingthe samples, we discovered a decryption code that suggests the threat actor was testing its functionality. It seems that they forgot to remove this code when deploying the sample. However, the decryption code is currently ineffective since it requires a private key known only to the malware author and has no connection to the malware routine. Therefore, it will not be executed by the program.

Conclusion

It's likely that the threat actors behind Monti still employed parts of the Conti source code as the base for the new variant, as evidenced by some similar functions, but implemented significant changes to the code — especially to the encryption algorithm. Furthermore, by altering the code, Monti's operators are enhancing its ability to evade detection, making their malicious activities even more challenging to identify and mitigate.

It is advisable for organizations to adopt effective defense strategies that include protocols for safeguarding data and the establishment of procedures for backup and recovery to protect their systems from ransomware attacks. These measures ensure the security of data and its potential restoration even in the event of encryption or deletion.

We suggest the subsequent security measures to protect important data:

- Implement multifactor authentication (MFA) to impede attackers from progressing horizontally within a network and gaining access to sensitive data.
- Adhere to the 3-2-1 guideline when generating backups for crucial files. This guideline entails creating three backup copies in two distinct file formats, with one copy stored at a separate location. This approach ensures redundancy and minimizes the possibility of data loss.

Trend Micro Solutions

A multilayered approach to security can help organizations guard possible entry points into their system such as endpoints, emails, web, and networks. The following security technologies can detect malicious components and suspicious behavior to help protect organizations from ransomware:

<u>Trend Vision One</u>[™] provides multilayered protection and behavior detection, which helps block questionable behavior and tools early on before ransomware can do irreversible damage to the system.

<u>Trend Cloud OneTM – Workload Security</u> protects systems against both known and unknown threats that exploit vulnerabilities. This protection is made possible through techniques such as virtual patching and machine learning.

<u>Trend Micro™ Deep Discovery™ Email Inspector</u> employs custom sandboxing and advanced analysis techniques to effectively block malicious emails, including phishing emails that can serve as entry points for ransomware.

<u>Trend Micro Apex One</u>[™] offers next-level automated threat detection and response against advanced concerns such as fileless threats and ransomware, ensuring the protection of endpoints.

Additional Insights by Byron Gelera and Bren Matthew Ebriega

Indicators of Compromise Hashes

SHA1	Detection
f1c0054bc76e8753d4331a881cdf9156dd8b812a	Ransom.Linux.MONTI.THGOCBC
a0c9dd3f3e3d0e2cd5d1da06b3aac019cdbc74ef	Ransom.Linux.MONTI.THGADBC

URLs

• hxxp://monti5o7lvyrpyk26lqofnfvajtyqruwatlfaazgm3zskt3xiktudwid[.]onion

• hxxp://mblogci3rudehaagbryjznltdp33ojwzkq6hn2pckvjq33rycmzczpid[.]onion