TrendLabs

Deciphering Confucius: A Look at the Group's Cyberespionage Operations

Appendix

TrendLabs Security Intelligence Blog
Daniel Lunghi and Jaromir Horejsi
Cyber Safety Solutions (CSS) Team
February 2018

Indicators of Compromise (IoCs)

Malicious/exploit-laden Rich Text Format (RTF) documents:

Hash (SHA-256)	Trend Micro Detection
4c6f74a274ea7255a178650a656c1d84c6d717043301917ffbf31285059bbd87	TROJ_MDROPPR.BDIR
f1a54dca2fdfe59ec3f537148460364fb5d046c9b4e7db5fc819a9732ae0e063	TROJ_CVE201711882.AG
65dec7020899647195bce984ec8dfb20503119fc2888f7c83b3d2493fd57aea9	TROJ_CVE201711882.SM

Backdoors and shells:

Hash (SHA-256)	Trend Micro Detection	Malware Name	
889cfc8b07dd2b1adacd08d5c2e25bcb43e1fffea1d8af0f7886ce4e6385cd13	TROJ_DELMOFU.DAM	sctrls	Internal name is in the Portable Executable (PE) structure
97c6dc02eaa6b8ce8d46460d5d94f57ceb4f355626d1cd3ddaf6dccea81d75e2	TROJ_DELMOFU.A		
a652f35cb877145e83ab813733083bb25c7fc717522abf10377de1f7a8fc4b43	TROJ_INJECTOR.POU	ByeBye Shell	Named by previous research
bb75c9ba7cc5163c39daa2ad35ce32001416654e76ed77896a793c4c0c34e619	TROJ_SNEEPY.B		
38489de0d8cdc5b208ead2ba87eb221e010e8b78099c8704281d2a7755815349	TROJ_SNEEPY.C		
b2c0878ae97dc48c413065626b05235c86d8dd7897bcdb741e68ca88c2a0ecc0			
8dd2c218c9ef809ffa27ce117007b2439c5df4d6f69f948381e5c75fe17aa1d1	BDKR_BYESHELL.A		
febd5232fe500962f382de753e2659d42e0e934229b1259bc28c6e857094b299			
1c67a8264da6b531239a5f310568f35254c04ace57409a644ff7b2754bbe1b35	BKDR_BUTERAT.YHQ	remote-access-c3	Internal name is shown in the program database (PDB) path
35d9012da0b1264657ef54518b638ff664713478d419d3f72e655c49a2b9209f			
3a69780947319168210a7656851ee5af73d7a417231c5d29da2c2281da2b0ece			
449d3145218e6146310f82bef55401a2d882cf41a1771dfcb8bff50bb815dda3			
caaee9e7039d9a775f78f563a76c33d3d643cc604f33247d92b36fb583768843	BKDR_SWRORT.SM	ReverseShellSimple	
3f4e884bd33032b6e0daab91d50a96c3e8f88938971accf7948e1da76a45704d	TROJ_REVSHELL.B		

Hash (SHA-256)	Trend Micro Detection	Malware Name	
da2ffe73cefd2ebbe0efa415da6eab91dacdc87dd46110d6aa0871f75a45bd2a	TROJ_REVSHELL.C	Tweety (reverse shell)	Internal name is shown in the reverse shell as string
341bb8dcbfe656bae3d11079be116dbc25cd4ef5554d0462d3eb62ed6d78c0d3	TROJ_KRYPIL.AUSREOM	sip_telephone	"phone_sip" and "sip_agents.exe" found in PE structure
782cc8a4347d607a1fab534181a318181e11724f7cef7f68cc63a39ba8ab1509			

Information/file stealers:

Hash (SHA-256)	Trend Micro Detection	Malware Name	
1b00b0c4aa3b442c1e0358a0067fcbcb2081370330388ebb88a0225d2a6be4de	BKDR_BUTERAT.YHQ	file-sweeper	Internal name is shown in the program database (PDB) path
2557b0e1d100dbf92e01dc07537a49353539f3e78df85753ed651142637c0872	TSPY_CONFSTEAL.A		
3803e67be2e686647bfda324dde1b00ecad0c01f8c192626565f32a03726e6ed			
aa9c7c350b62986883d43ee63bb4c3592eb7cd35e9d392cbbd2502e092eea86b	TROJ_PYLOADR.B	swissknife2	Name taken from file's manifest
5f96bf657af29be82cdafd71aeee4fdc68805ada749c085c4ab26c8f822337e7	TSPY_CONFSTEAL.A	svctrls	Internal name is in the Portable Executable (PE) structure
e2e4dfbed9aeaea61eff41981f4924b725fce01765581f94f9948448e874215f		Winframe	
266466827857f3bb680a601e96780fcc7d4b3323addc39af39349c88f7ee1955			
472ea4929c5e0fb4e29597311ed90a14c57bc67fbf26f81a3aac042aa3dccb55		usctrls	
793be04c163f7a9e026105dd78b88b378cb35188604cf99d8af1fc470d8db4c7		fileUpload	Internal name is shown in the program database (PDB) path
6322383a5cedc8e5de5f689c0fc4df7f96fc0e1ccf1d508e836a3e5842d05a73			

Malicious Android packages (APKs)/chat applications:

Hash (SHA-256)	Trend Micro Detection
fe59b0e9352931157563a19c33ef0f259dab19e1fec88bd94b7eab6e8c7b2b5f	ANDROIDOS_CHATSPY.A
6c009275d952cc6ec5d9d41fc9d7a47a31813483b768291c5c01e54a83787ca9	
f2d649046d1a8811426a257d70e9bdc371d27931d2b76b391b0a630c84172c4b	
cef50adae5e53a904246b688d8164535aff9062e3b446ac140cf42afd63ad0eb	

Tweety Chat (Windows):

Hash (SHA-256)	Trend Micro Detection
70200426178917e2c4737a0e53b30b706a481a47bfaed460b48e4b17611421c4	TROJ_CONFSTEAL.B
d4f74d05e1932b218d2da600f68a4c969e770e249240eea5a3020c0f8adf15e2	
c871410689004c712b6428a5f2b9bc7e49e6c84b740c7453e4eee835e13f1eba	TSPY_CONFSTEAL.B
e48d7b9e764032ca07c2335a16b19b6ba9243f993cc36af88a633c3ca428cedf	
f4d458a49c4b490f0033d48466716ded8221f261eae2f1c38ef78f550f42064d	
d439e32be9f8dbeda8d23e73d64bb92fcb795fbe9668aa9bcd028daddeccca2b	
f4d458a49c4b490f0033d48466716ded8221f261eae2f1c38ef78f550f42064d	

Confucius-related malware:

Hash (SHA-256)	Trend Micro Detection
4eec3329ff385d89e1c31dc7e58ec48abf87947ab122e68fbdc95df96fd298b7	TROJ_POWLOAD.GAA
4ae6313a056ef5762e96c0a8f2527bc686a39a317e07484da9229dd265e7d345	TSPY_PUTTINJ.A
2e539d0600466f5987994eef6ddaca883ee3ccb2d46ff756c37ea6c0bedefe6e	

Malicious domains and IP addresses related to Confucius:

Domain / IP Address
199[.]101[.]187[.]54
45[.]63[.]43[.]29
45[.]76[.]33[.]53
46[.]165[.]249[.]223[:]80
5[.]199[.]163[.]51[:]4343
91[.]210[.]107[.]106[:]80
91[.]210[.]107[.]109[:]80
91[.]210[.]107[.]110[:]80
hxxp://46[.]165[.]207[.]108/appstore/appservice[.]php
hxxp://5[.]135[.]73[.]109/abc[.]hta
hxxp://5[.]135[.]73[.]109/cpt[.]jpg
hxxp://91[.]210[.]107[.]104/search1[.]php
hxxp://94[.]242[.]219[.]205/bookmarks[.]php
hxxp://adhath[-]learning[.]com[:]4343
hxxp://adhath[-]learning[.]com[:]8080
hxxp://cloud[.]tweetychat[.]com/TweetyChat[.]exe
hxxp://cloud[.]tweetychat[.]com/TweetyChatx32[.]exe
hxxp://cloud[.]tweetychat[.]com/TweetyChatx64[.]exe
hxxp://freeintrnet[.]com
hxxp://mfone[.]net/strength[.]php
hxxp://mofu[.]tech/useregistration/newuser[.]php
hxxp://simplechatpoint[.]ddns[.]net/android_connect/insert_account[.]php
hxxp://simplechatpoint[.]ddns[.]net/android_connect/insert_contacts[.]php
hxxp://simplechatpoint[.]ddns[.]net/android_connect/insert_file_list[.]php
hxxp://simplechatpoint[.]ddns[.]net/android_connect/insert_sms[.]php
hxxp://simplechatpoint[.]ddns[.]net/android_connect/upload_file_content[.]php
hxxp://truth786[.]com
hxxp://tweetychat[.]com

Securing Your Journey to the Cloud

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.

Created by:

TrendLabs

Global Technical Support & R&D Center of TREND MICRO