IOC Resource for Russia-Ukraine Conflict-Related Cyberattacks

Indicators of Compromise

Indicators of Compromise (IoCs)

This document is an IOC guide meant for Trend Micro customers. The IoCs listed below are all detected and blocked across Trend Micro products. This document will constantly be updated with new indicators as the stories continue to develop.

Files related to Conti

Sourced from Trend Micro

Related Hashes	Trend Micro Detection
911c16d41f49198482aa4d75054cb0e10b07d68c	Ransom.Win32.CONTI.SMYXBLD
3a81355ccfd6d3846fa435b5893ea5cd18e6c9fa	
a803a4b305415b66f22ed29d08017c286b8cb9ef	
b9505c86dd3ae120c0be1201e51af44de4266b36	
655269c264f7b044d8f406cd980fc00c3b8e21ca	
38cd341de09c7d393adf93596b691e7237d0a2e7	
6c7b35e36830c1cc613fb08280ee25e5fbba9937	
5bf5551cee1635709598c90836733550727245ba	
5f27447dcc66c1c4152e23decb47f82c32883080	

File related to Ukraine-related spam email

Sourced from Trend Micro

Related Hashes	Trend Micro Detection (VSAPI/TRENDX)
f6294b2acf0f15453697f16597de734da8a9d92f	TrojanSpy.Win32.AVEMARIA.AYAD| TROJ.Win32.TRX.XXPE50FFF053

KILLDISK (Hermetic Wiper)

Sourced externally

- https://twitter.com/esetresearch/status/1496581903205511181?s=21
- https://therecord.media/second-data-wiper-attack-hits-ukraine-computer-networks/

Related Hashes	Trend Micro Detection (VSAPI/TRENDX)
61b25d11392172e587d8da3045812a66c3385451	Trojan.Win32.KILLDISK.SMYECBW | TROJ.Win32.TRX.XXPE50FFF053E0002
912342f1c840a42f6b74132f8a7c4ffe7d40fb77	Trojan.Win32.KILLDISK.SMYECBW | TROJ.Win32.TRX.XXPE50FFF053E0003
9518e4ae0862ae871cf9fb634b50b07c66a2c379	Trojan.Win32.KILLDISK.SMYECBW | TROJ.Win32.TRX.XXPE50FFF053E0002
d9a3596af0463797df4ff25b7999184946e3bfa2	Trojan.Win32.KILLDISK.SMYECBW | TROJ.Win32.TRX.XXPE50FFF053E0003
0d8cc992f279ec45e8b8dfd05a700ff1f0437f29	Trojan.Win32.KILLDISK.SMYECBW | TROJ.Win32.TRX.XXPE50FFF053E0004

Gamaredon

Sourced externally

- https://unit42.paloaltonetworks.com/gamaredon-primitive-bear-ukraine-update-2021/
  https://cyware.com/news/gamaredon-responsible-for-attacks-on-ukraine-since-2021-0350fe82
- https://github.com/pan-unit42/iocs/blob/master/Gamaredon/2022_02_Gamaredon_UPDATE.txt
- https://github.com/pan-unit42/iocs/blob/master/Gamaredon/Gamaredon_IoCs_JAN2022.txt

Related Hashes	Trend Micro Detection (VSAPI/TRENDX)
cbc7f2afe334bc160b741dde2e857ff26e01925744b9f0668a826aa4a1437ab8	TROJ_FRS.VSNTB322
a82cb2076b7274179d5f7246f8db274eda47a89392875b3c700f2fa15d70ab2e	TROJ_FRS.VSNTB322
839170c51d75bd1dc77f17b957846ace0caa19a83de837277d7294a47e5023b3	Trojan.W97M.TEMPLINJECTOR.ZGJB
bdb4f98bf2bed83b09278bcf7b85771688fb1292612d6c82ad0eb8d7e3256fa1	Trojan.W97M.DULLDOWN.ZGJB
cbc7f2afe334bc160b741dde2e857ff26e01925744b9f0668a826aa4a1437ab8	TROJ_FRS.VSNTB322
edecec2c413770fa929937c04ecf889e5c58d562c6e08ef0bfcd65ce482d397c	Trojan.X97M.CVE20170199.YXCBP
6f21dde5cf5394eebf779451d45494dfeb22c2eebbb4af1aa3f779724dadf8af	Trojan.W97M.TEMPLINJECTOR.ZGJB
aa07ab7dba1aeb41c57bcdcbca54cefb85afb6f8927d33bf88aef5c19878ba92	Trojan.W97M.TEMPLINJECTOR.ZGJB
8831eb86996d4778be526a6fd281c98d624b155940aae463b45dda1c5f979f1c	Trojan.X97M.CVE20170199.YXCBP
3590dd881d094b020fe4b93bb6894e768b878ebcda7f03589da6671db2c652e5	Trojan.W97M.TEMPLINJECTOR.ZGJB
420960a10e3f3730ab124bfefceedc032ef06c7b38fa014b2b59462365a5f08d	Trojan.W97M.TEMPLINJECTOR.ZGJB

081b548f9e06488d367497b02de972394b0da10b473a245bdf0c026e6406b86b	Trojan.W97M.TEMPLINJECTOR.ZGJB

Whispergate

Sourced externally

- https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/

Related Hashes	**Trend Micro Detection (VSAPI/TRENDX)**
189166d382c73c242ba45889d57980548d4ba37e	Trojan.Win32.WHISPERGATE.YXCAQ | TROJ.Win32.TRX.XXPE50FFF053
16525cb2fd86dce842107eb1ba6174b23f188537	Trojan.MSIL.WHISPERGATE.YXCAQ| TSPY.Win32.TRX.XXPE50FFF053
b2d863fc444b99c479859ad7f012b840f896172e	Trojan.MSIL.WHISPERGATE.YXCAQ
4c5006cee3e3f7147df37cd03775bfd48e572ca5	Trojan.Win32.FRS.VSNW11A22
82d29b52e35e7938e7ee610c04ea9daaf5e08e90	Trojan.MSIL.WHISPERGATE.YXCAQ
a67205dc84ec29eb71bb259b19c1a1783865c0fc	Trojan.Win32.WHISPERGATE.YXCAX
97aa0b096abc89d403a2176079fb77be990a4011	Trojan.MSIL.WHISPERGATE.YXCBU | TROJ.Win32.TRX.XXPE50FFF053

SaintBot

Related Hashes	**Trend Micro Detection**
e8207e8c31a8613112223d126d4f12e7a5f8caf4acaaf40834302ce49f37cc9c	Backdoor.Win32.SAINTBOT.A
75f728fa692347e096386acd19a5da9b02dca372b66918be7171c522d9c6b42d	Trojan.MSIL.SAINTALL.A

OutSteel

Related Hashes	**Trend Micro Detection**
7ee8cfde9e4c718af6783ddd8341d63c4919851ba6418b599b2f3c2ac8d70a32	TrojanSpy.MSIL.OUTSTEEL.YMCBB
320d091b3f8de8688ce3b45cdda64a451ea6c22da1fcea60fe31101eb6f0f6c2	Trojan.Win32.FRS.VSNW14B22

Decoy Ransomware (GoLang-based)

Sourced externally

- https://twitter.com/AvastThreatLabs/status/1496663206634344449

- https://twitter.com/chen_erlich/status/1496844075332509701
- https://www.bleepingcomputer.com/news/security/ransomware-used-as-decoy-in-data-wiping-attacks-on-ukraine/

Related Hashes	Trend Micro Detection
f32d791ec9e6385a91b45942c230f52aff1626df	Ransom.Win64.GOFILECODER.THBBDBB

Clipbanker Malware

Sourced externally

- https://twitter.com/malwrhunterteam/status/1497235270416097287

Related Hashes	Trend Micro Detection
0fbd7abc2755ccc4d853d06ca7ad8562c5c12b40	TrojanSpy.Win32.CLIPBANKER.THCOABB
728da6dea7be8c4249c40bb45ead9a4885257d72d130db3caa0e19c108041760	TROJ_FRS.0NA104BP22
738c3dbc72b2edcb0e90eda5e235d4398a42326099954a20a9691e02bf1f8ab0	TROJ_FRS.0NA104BP22

IsaacWiper

Sourced externally

- https://www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine/

Related Hashes	Trend Micro Detection
13037b749aa4b1eda538fda26d6ac41c8f7b1d02d83f47b0d187dd645154e033	Trojan.Win32.KILLMBR.YECCA

URLs related to Gamaredon and Actinium APT targeting Ukraine

- deep-pondering[.]gortomalo[.]ru
- hxxp://185.46[.]10.45/wordpress.html
- hxxp://185.46[.]10.45/counter.html
- deep-six[.]gortomalo[.]ru
- hxxp://185.46[.]10.45/set.lgo/deerfood3
- hxxp://185.46[.]10.45/currently/credit/m4v
- hxxp://185.46[.]10.45/set.lgo/deerfood223
- hxxp://5.252.178.184
- 5.252.178[.]184:33163
- deprive.lotorgas[.]ru
- hxxp://5.252.178.188
- 2.59.36[.]204
- 5.252.178[.]183

- archlinuxo[.]ru
- centosi[.]ru
- cupsman[.]ru
- linuxo[.]ru
- ubunto[.]ru
- freebsdo[.]ru
- aaa[.]archlinuxo[.]ru
- aaa[.]centosi[.]ru
- aaa[.]cupsman[.]ru
- aaa[.]koparas[.]ru
- aaa[.]pitroksa[.]ru
- aaa[.]ubunto[.]ru
- end22[.]kassanfo[.]ru
- falcon1[.]freebsdo[.]ru
- falcon21[.]freebsdo[.]ru
- globe55[.]koparas[.]ru
- intercept37[.]freebsdo[.]ru
- pretend23[.]cupsman[.]ru
- shoes34[.]linuxo[.]ru
- stopped100[.]kilotora[.]ru
- ambulance[.]globe24[.]koparas[.]ru
- ambulance[.]globe90[.]koparas[.]ru
- configolders4_config4[.]vivaldar[.]ru
- counteract[.]end22[.]kassanfo[.]ru
- countless[.]intercept37[.]freebsdo[.]ru
- enforce[.]shoes34[.]linuxo[.]ru
- naturally[.]stopped100[.]kilotora[.]ru
- necessity[.]amateur100[.]pitroksa[.]ru
- koparas[.]ru
- loralis[.]ru pitroksa[.]ru
- aaa.loralis[.]ru aaa.koparas[.]ru
- aaa.pitroksa[.]ru
- gloomily67.golitus[.]ru
- interference20.holotras[.]ru
- 2.59.36.194

URLs related to Clipbanker Malware

- hxxp://179.43.175[.]171/qelh/CL.exe
- hxxp://179.43.175[.]171/qelh/png.hta

Files related to FoxBlade / HermeticWiper Malware

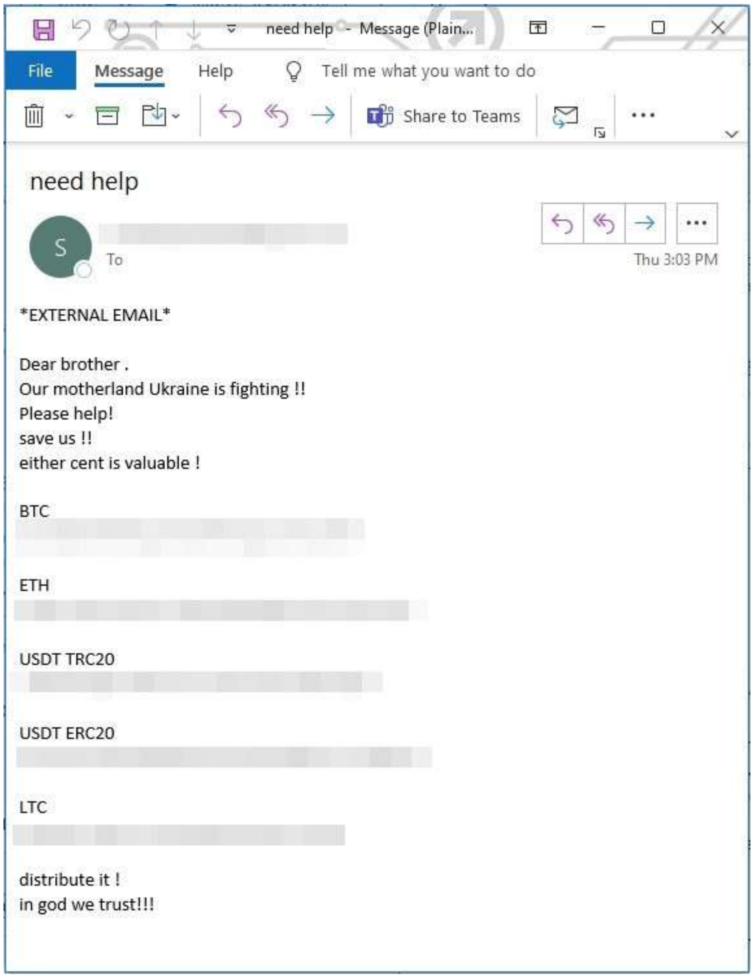
Related Hashes	Trend Micro Detection
4aa186b5fdcc8248a9672bf21241f77dd395872ec4876c90af5d27ae565e4cb7	TrojanSpy.Win32.KILLDISK.SMYECBW
06086c1da4590dcc7f1e10a6be3431e1166286a9e7761f2de9de79d7fda9c397	TrojanSpy.Win32.KILLDISK.SMYECBW

0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da	TrojanSpy.Win32.KILLDISK.YACBX
1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591	TrojanSpy.Win32.KILLDISK.YECBW
2c10b2ec0b995b88c27d141d6f7b14d6b8177c52818687e4ff8e6ecf53adf5bf	TrojanSpy.Win32.KILLDISK.YECBX
3c557727953a8f6b4788984464fb77741b821991acbf5e746aebdd02615b1767	TrojanSpy.Win32.KILLDISK.YECBX

Files related to Stormous Ransomware

Related Hashes	Trend Micro Detection
96ba3ba94db07e895090cdaca701a922523649cf6d6801b358c5ff62416be9fa	Ransom.PHP.STORMOUS.YXCCBT
b7863120606168b3731395d9850bbf25661d05c6e094c032fc486e15daeb5666	HTML.STORMOUS.YXCCBT.note

Screenshots of Ukraine-related cryptocurrency donation requests sourced by Trend Micro



need help

[redacted]

EXTERNAL EMAIL

Dear brother .
Our motherland Ukraine is fighting !!
Please help!
save us !!
either cent is valuable !

BTC
[redacted]

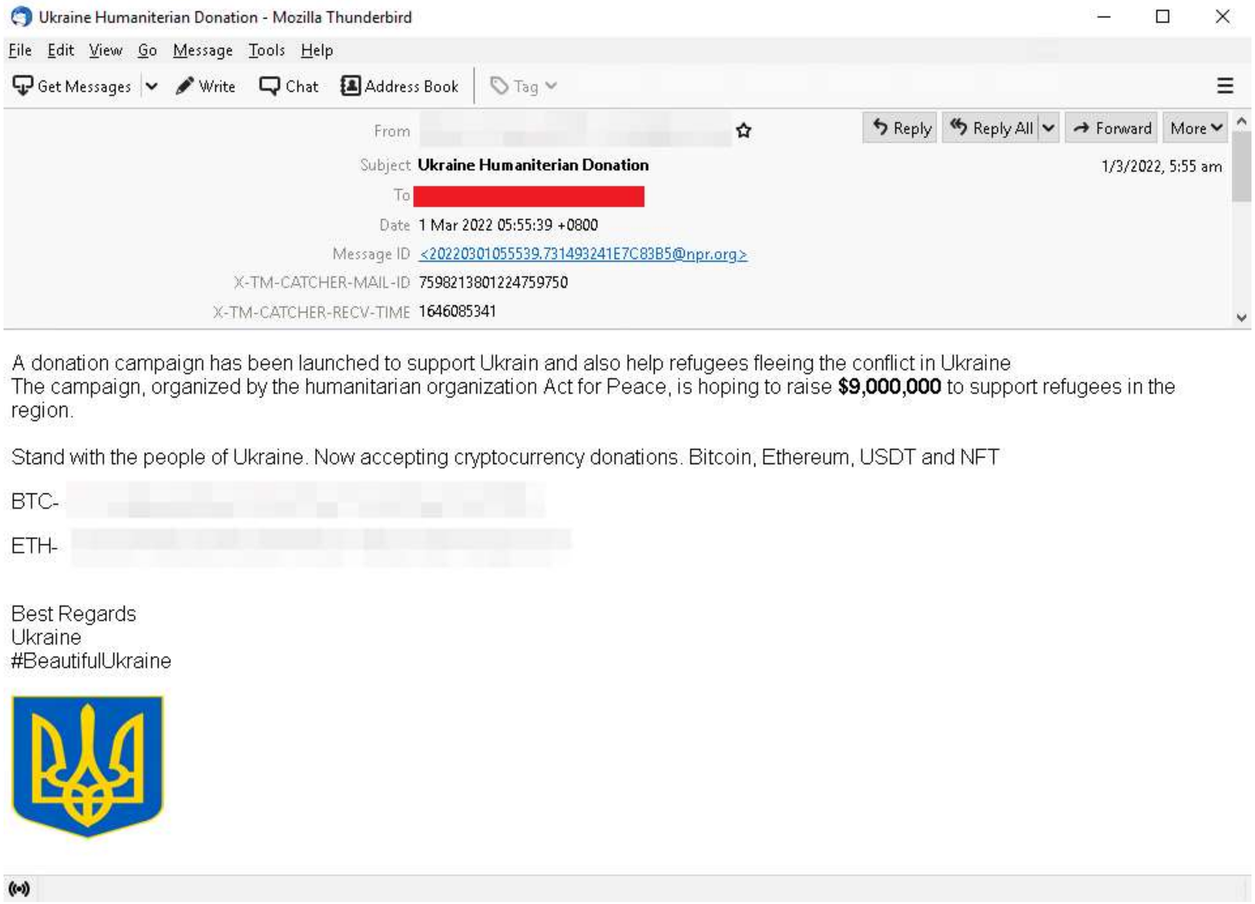
ETH
[redacted]

USDT TRC20
[redacted]

USDT ERC20
[redacted]

LTC
[redacted]

distribute it !
in god we trust!!!


Ukraine Humaniterian Donation - Mozilla Thunderbird
File Edit View Go Message Tools Help
Get Messages
Write
Chat
Address Book
Tag
Reply
Reply All
Forward
More

From [redacted]

Subject **Ukraine Humaniterian Donation**

1/3/2022, 5:55 am

To [redacted]

Date 1 Mar 2022 05:55:39 +0800

Message ID <20220301055539.731493241E7C83B5@npr.org>

X-TM-CATCHER-MAIL-ID 7598213801224759750

X-TM-CATCHER-RECV-TIME 1646085341

A donation campaign has been launched to support Ukrain and also help refugees fleeing the conflict in Ukraine
The campaign, organized by the humanitarian organization Act for Peace, is hoping to raise **$9,000,000** to support refugees in the region.

Stand with the people of Ukraine. Now accepting cryptocurrency donations. Bitcoin, Ethereum, USDT and NFT

BTC- [redacted]

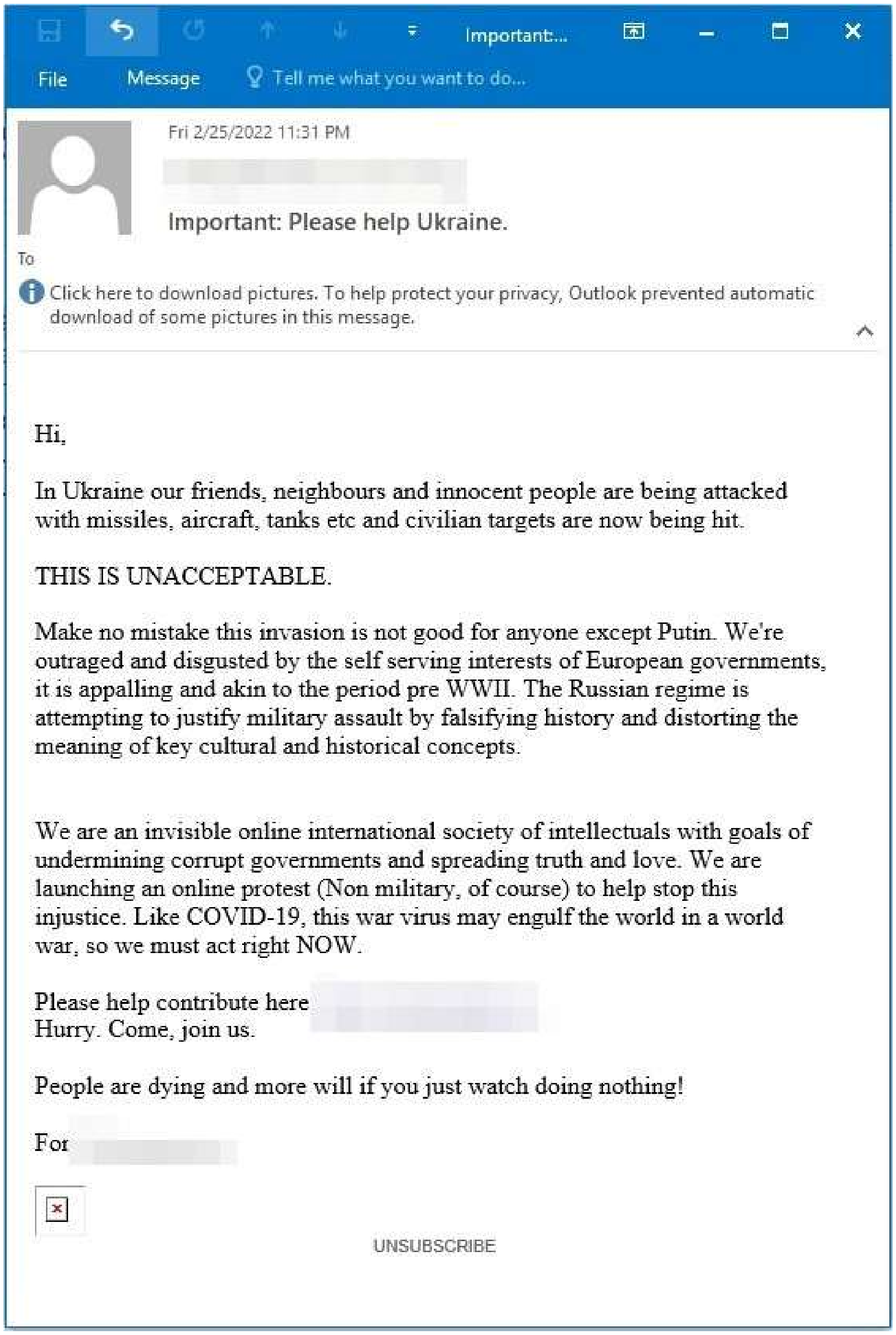
ETH- [redacted]

Best Regards
Ukraine
#BeautifulUkraine

URLs connected to spam emails and other Ukraine-related scams sourced by Trend Micro

- hxxps://netizenati[.]org
- savethekidsukraine[.]com

Screenshots of spam emails and other Ukraine-related scams sourced by Trend Micro



Fri 2/25/2022 11:31 PM

[redacted]

Important: Please help Ukraine.

To

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Hi,

In Ukraine our friends, neighbours and innocent people are being attacked with missiles, aircraft, tanks etc and civilian targets are now being hit.

THIS IS UNACCEPTABLE.

Make no mistake this invasion is not good for anyone except Putin. We're outraged and disgusted by the self serving interests of European governments, it is appalling and akin to the period pre WWII. The Russian regime is attempting to justify military assault by falsifying history and distorting the meaning of key cultural and historical concepts.

We are an invisible online international society of intellectuals with goals of undermining corrupt governments and spreading truth and love. We are launching an online protest (Non military, of course) to help stop this injustice. Like COVID-19, this war virus may engulf the world in a world war, so we must act right NOW.

Please help contribute here [redacted]
Hurry. Come, join us.

People are dying and more will if you just watch doing nothing!

For [redacted]

UNSUBSCRIBE