INDICATOR SHARING

Microsoft Teams Spearphishing - UserCentric.exe

TLP:WHITE

Feb 18, 2022

In a report from Avanan, researchers identified a file used by threat actors to spearphish users in Microsoft Teams. Further investigation into malicious activity surrounding this file revealed several parent files and other malicious files related to activity. The indicators are from several pivots while conducting research to find information around UserCentric.exe.

Health-ISAC is sharing these IOCs to increase sector awareness. Organizations are encouraged to ingest these IOCs manually if no automatic ingestion systems are implemented. For Health-ISAC members who have implemented the Health-ISAC Indicator Threat Sharing (HITS) program, the IOCs related to this alert have been automatically imported into your environment.

For guidance on how to disable this alert category or share IOCs via the Health-ISAC Threat Intelligence Portal (HTIP), please visit the respective “How To” Knowledge Base articles “HTIP - Alert Categories” and “HTIP - Share Threat Intel" using the link below:

https://health-isac.cyware.com/webapp/user/knowledge-base

Health-ISAC encourages members to share IOCs via the Health-ISAC Threat Intelligence Portal (HTIP) to take advantage of attributed or anonymous sharing across ISACs and other cybersecurity related entities.

Reference(s)	Avanan
Report Source(s)	Peer Organization

Threat Indicator(s)

SHA256:
61f387816c6ad78e2b466f015096cf561bd721481e2788303215e03b979333c1
021c93c646c6bad0b633b33e5029a8e4728c6aa506ec8481d534878ce51ef66
0
ca24e92e6f5cab62fd64dec406a3f66492e91e7a715a1a566f2b4557373d71bf
bc5daeaec6afd947cbe1392d0492682bb0e0140ec79b486d6407228591fc0307
fe1440c176b375ccb9d50c3715579e7d2eb4f1522fd494fb01aeb57581c12118
467b16427f3b1170e168775d918348621a12adf7a2131a65e24e3b23bcd0242
1
bc5326ae0a2f109c071f9fcda67a4959b757821cb7c76fc985ece26284b1aa99
8c7c8a5129a185a4e4c9f106edb3498a932f5f9bd3802a932a184ba0181394f3
ea73a0669eaa34684991c6e7c079315e665597911a59091ff03c0b678566782d
2e81664ec6ecf53aa3e3311bd8dc37bce3c60871ea1ce084fb0911e009c72aa3
a283e78dfb441291d605447edee72b26725d4ac283b56e66563b0453a110a75
4
240b7054baee4fec92e32062ad0c20633e2d6bbb337aeea03d1e1d915472299
4
77be573f570546b28d7e884e6895987dcb7fa0a6432ed67867f0ec8a48ef860d
4d9d6a6c556367974015318d59accdbfbcaad8d78d3f26b30e808829d06536cb
1a0fab18c0e6c7cea6ac0485fd05f13bc4a896738ccc3a933f652e9ff30c98bd
d0012e8f65ec3482b0b32f7276182a00815c9e35d3c3580271a78cad356ecf49
ff01c477f5d366688e5a41e9c868538c061031d36a89eda6dcbdd4d0bcf5646c
af3d39ee9fe15ddbb0eb1a30334c891d662c1e6f8b560fdc3b256dbdfcd1851b

632ad3572242a89b5caf80062bc386ac1840c497768e84c7ca609f9779069ab9
76a9c9bd6af14091801da1928d7bffc7f2d1638a80a72dbd909e86ff97135afb
36de485500ad6426c9471c1ec8d2286bf18f882801ccf5341afb714db840d54f
b08c304fb0b148076c787b29990f0143792881419653b173abdd9e6fb1635125
470d174e1f315e6f8506a82f1dd3014ef611be24e7e5cc545b21f6abbd7e4664
272b5fbd260b11267ab6c9af53f699bd7ae7e38b61cb1e5f19e3da0cf26e5ad4
9884e9d1b4f8a873ccbd81f8ad0ae257776d2348d027d811a56475e028360d87
de1cd22fcf995353c67dd562e3d6a8c7b0d819750f47996e73c3849757905cac
fb0ce594127cc647b9f24c4deb73e88e21706629fc63e234826b65075a4d85c2
5dcc1e0a197922907bca2c4369f778bd07ee4b1bbbdf633e987a028a314d548e
cbdcb9c068a56d9e24f3f69b66b7f2c2236b1f6ff0c5af09f1a49428e8c21537
48455dcfa842d9aaa5bdcc4319c6b6a7ac61b34db39a4221b73fcadfc3128ea3
39127e3cf39703bc2190e9f35fcb6fa05a516c38fe38931e241785ea962c2883
8f933507f126ac424876e92484237c0941d438d2df5d4eef013dd58f335593f6
5798758bbc833df09bceba3fb38dfa95dbe82d1a51b94ea300392654fc2b2665

SHA1:
cdb4c21c533cc1bc14da2d905ef5cefe1bc4d2e0
d9e096cfe3907fd1e3d6eca1888dad131c29f0c3
69e0207515e913243b94c2d3a116d232ff79af5f
07f60151b9246dc541170fdee2b5f2c9212ed654
3e89ff837147c16b4e41c30d6c796374e0b8e62c

URL(s):
http://51.49.0.0

IP(s):
51.49.0.0

MD5:
b8c4601cabea4aa9903eefe7ada17106
5d00afdfbace03fe04b71e11d9b965e5
1d6ab8efef233fa4ef9dd612dbad549b
4c96cc29e94e6d0df0dd2d956e56dfd2
3da7fed6a2dca26488b0779ddef965b9
c594b792b9c556ea62a30de541d2fb03
4cdbcab8c5b362c734d648dc51fda37d
65967042a67dfdf36f7674a7f841e51f
d2582190f9f5efda52bfcb2c6fe0162f
04e6650582aaf1277f1649c5c58b2134
19c548818a83a3f1f3fdac69d3f5d985
9dbfcdc17bee179882157739e886eb5d
9fef3414b8370f0273e975bc6a6e72ae
ad141985abfea5e2a38a08cf62466205
d6eb82c324cab2f36e345863fad95090

b845aa2e31712da62ffa71c55cbd80db
e6063db550935f68ba04cdc4dbe4df6c
92dc6ef532fbb4a5c3201469a5b5eb63
c23038dd7c22ca3c7c5ecb212aa856fd
1e6626595c22e311dee121bf106fc620

Notes
Initial Source: https://www.avanan.com/blog/hackers-attach-malicious-.exe-files-to-teams-conversations

Course of Action (COA)

- Implement protection that downloads all files in a sandbox and inspects them for malicious content
- Deploy robust, full-suite security that secures all lines of business communication, including Teams
- Encourage end-users to reach out to IT when seeing an unfamiliar file

Alert ID ff9bc520

View Alert

Tags spearphishing, Microsoft Teams

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Knowledge Base Check out our Knowledge Base for HITS integration documentation. https://health-isac.cyware.com/webapp/user/knowledge-base/f4b0c136/

For Questions or Comments Please email us at toc@h-isac.org

Download Health-ISAC’s Information Sharing App.

For more update and alerts, visit: **https://health-isac.cyware.com**