# Malspam pushes Matanbuchus malware, leads to Cobalt Strike

By SANS Internet Storm Center

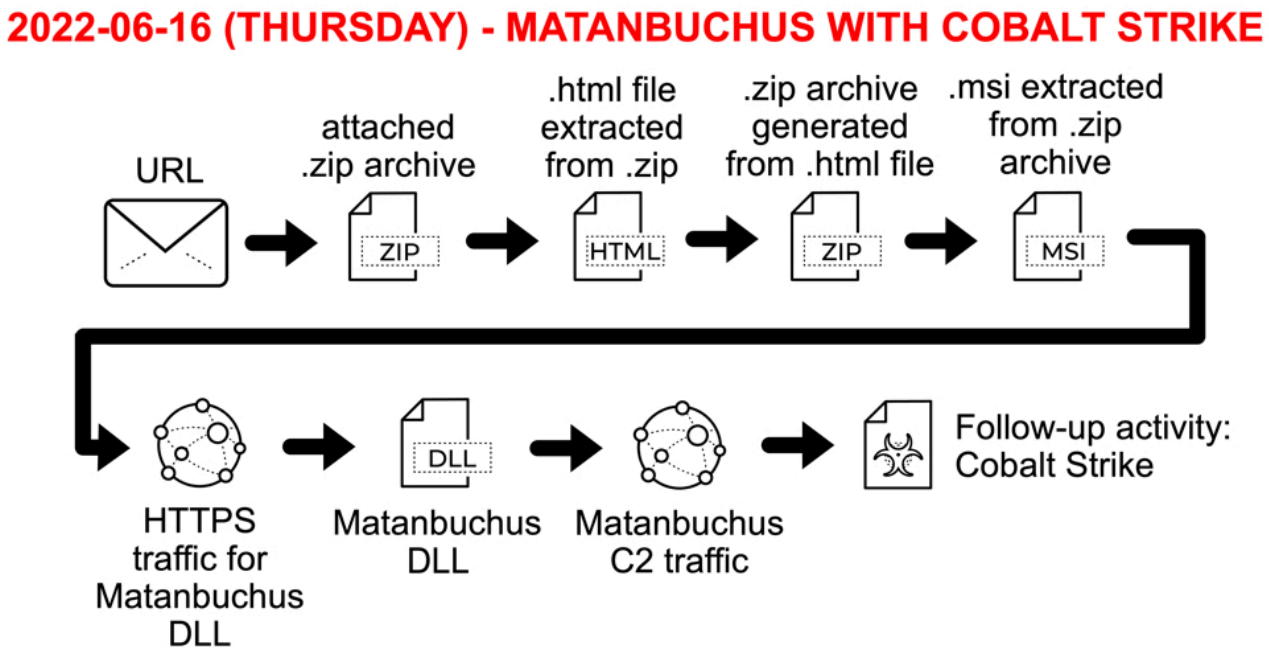
Archived: 2026-04-05 12:59:20 UTC

***Introduction***

On Thursday 2022-06-16, threat researchers discovered a wave of malicious spam (malspam) pushing Matanbuchus malware:

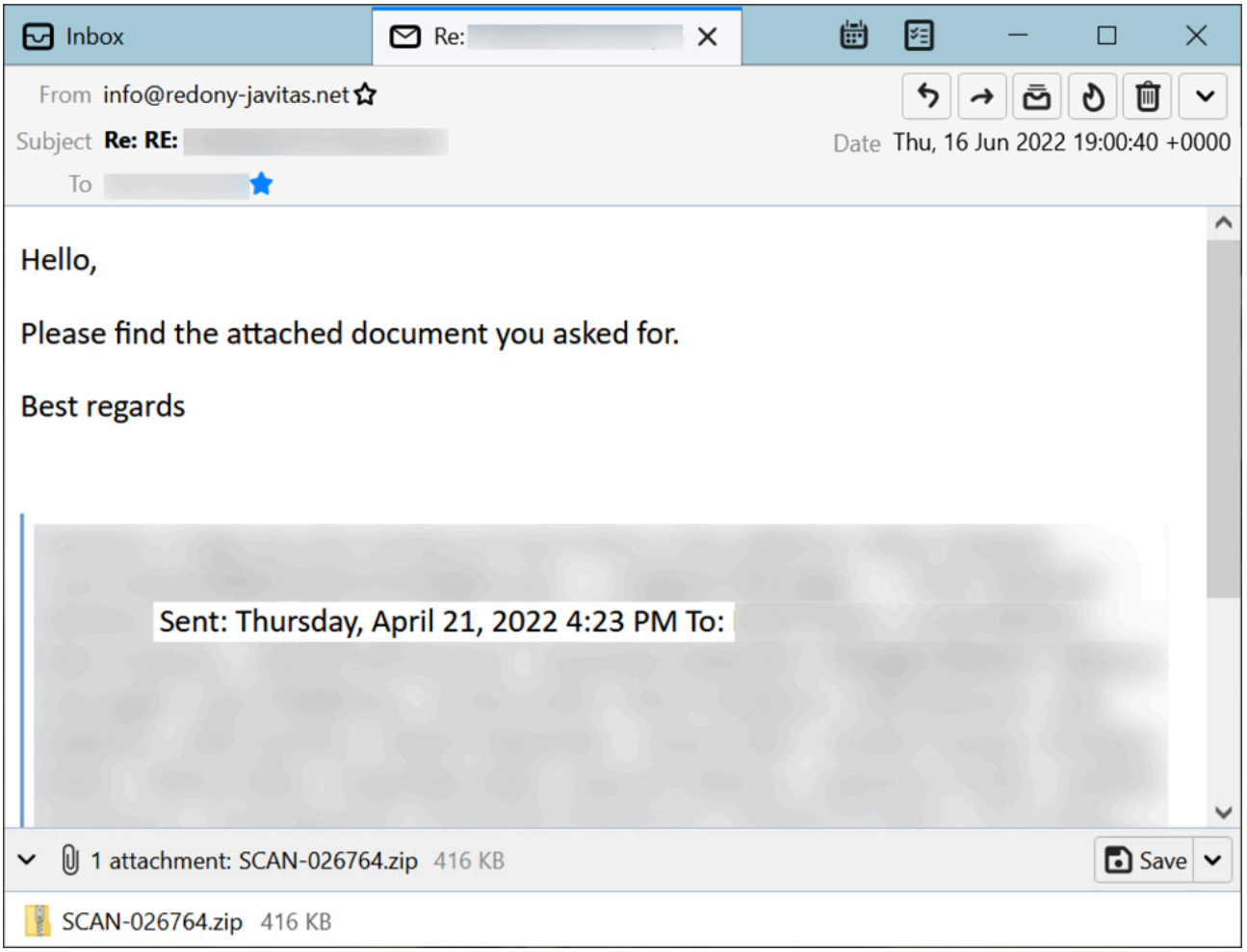
- https://twitter.com/pr0xylife/status/1537511268591992840
- https://twitter.com/executemalware/status/1537569201577156611

Today's diary reviews the activity, which led to Cobalt Strike in my lab environment.

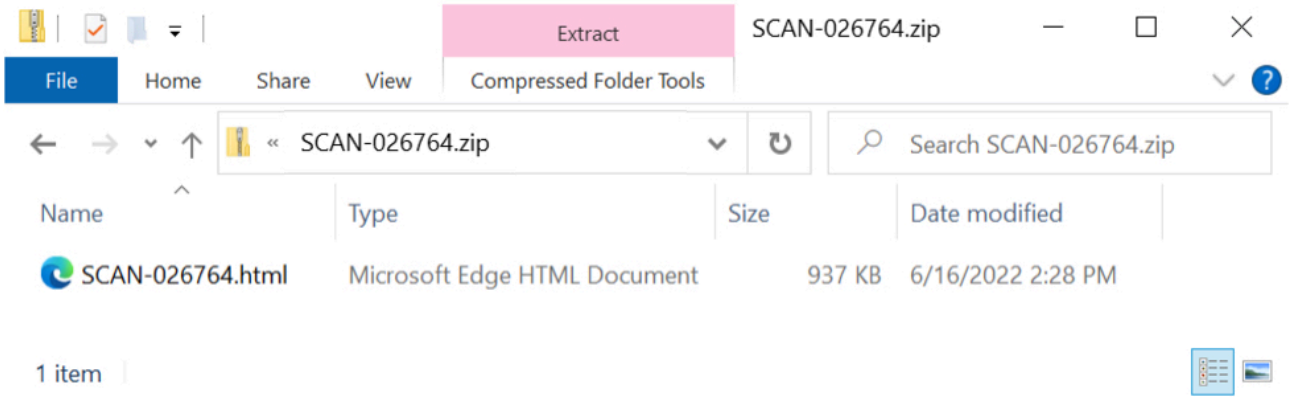



*Shown above: Flow chart for Matanbuchus activity on Thursday 2022-06-16.*

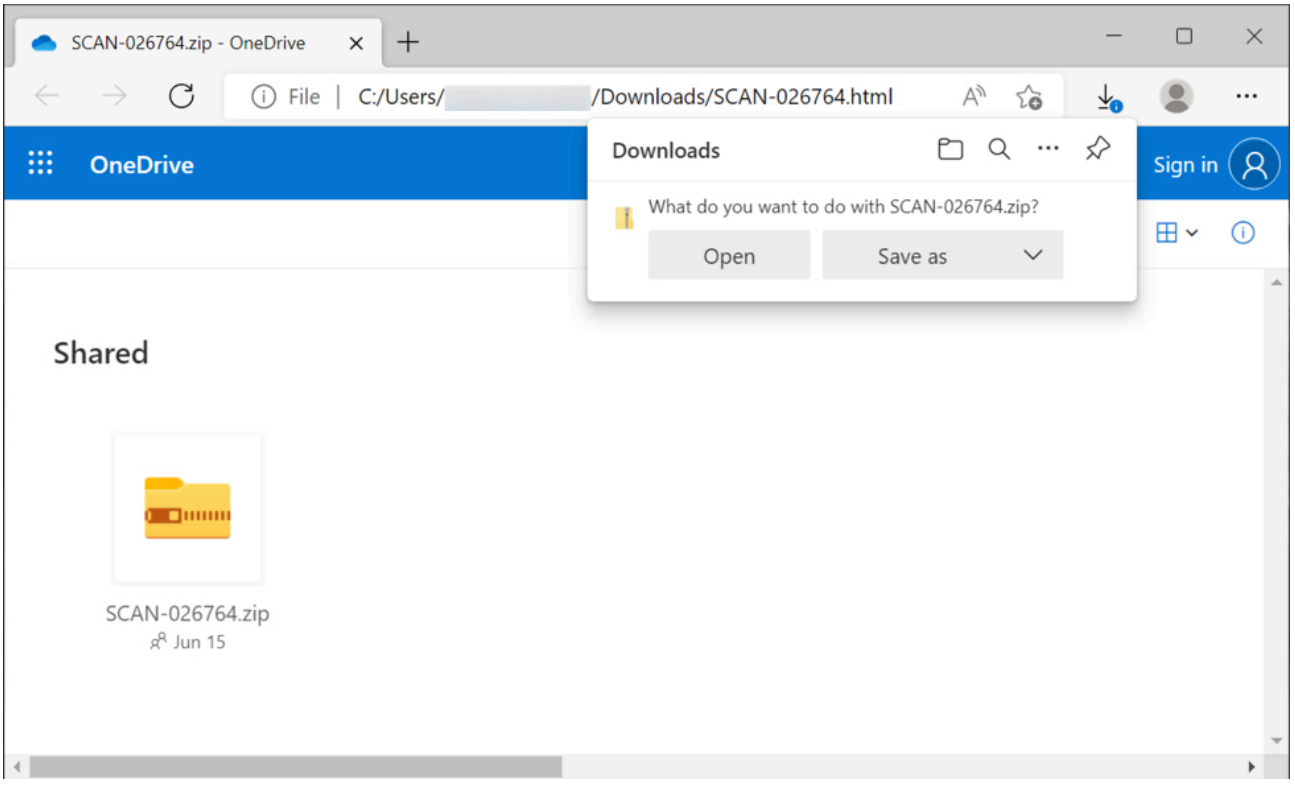
***Email and Attachment***



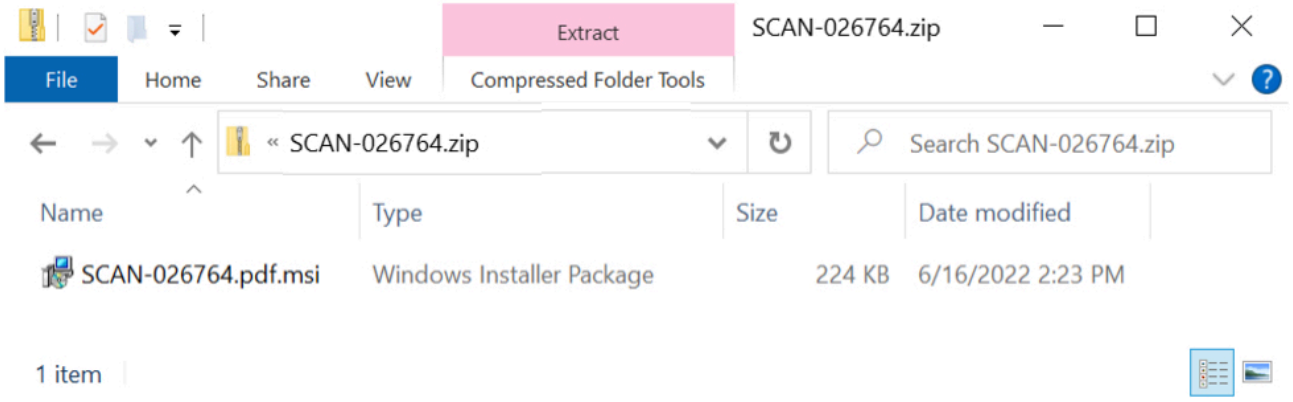

*Shown above: Screenshot from one of the emails pushing Matanbuchus on 2022-06-16.*



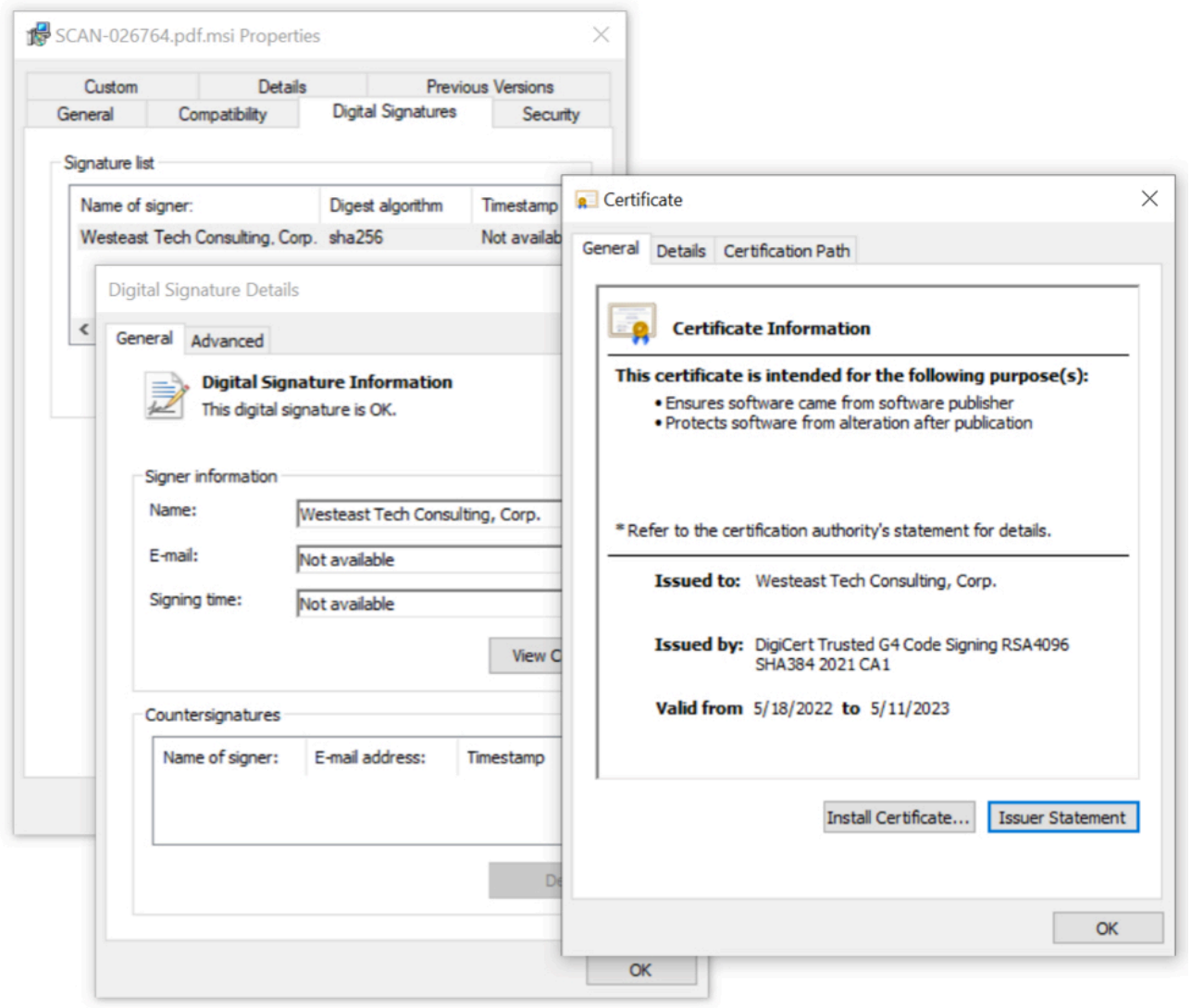

*Shown above: The email attachment is a zip archive that contains an HTML file.*




*Shown above: The HTML file pretends to be a OneDrive page, however, the HTML file actually contains base64 text that is converted to a file for download.*

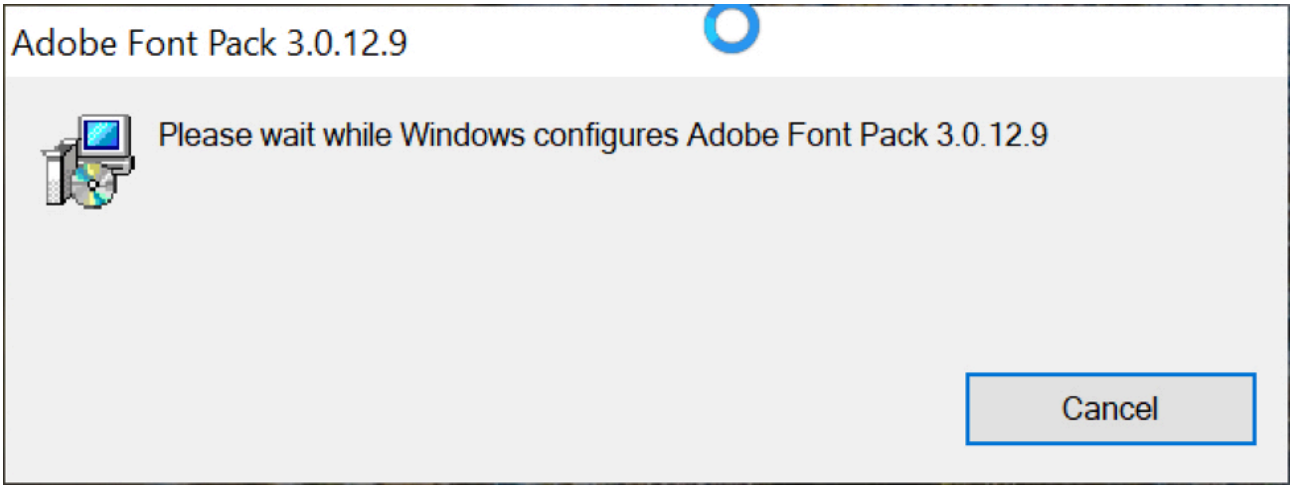



*Shown above: Zip archive downloaded from the HTML file contains an MSI package.*

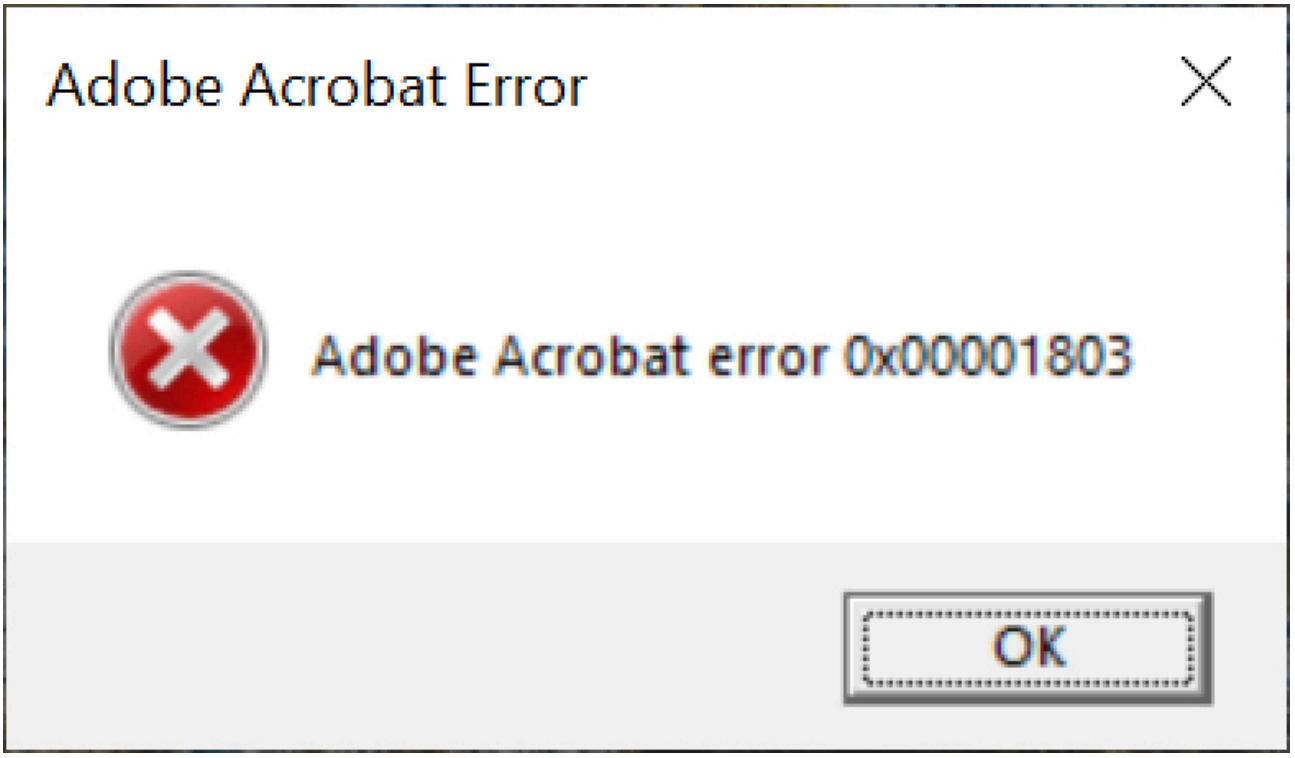



*Shown above: MSI extracted from the second zip archive is signed using a certificate, apparently from Digicert.*

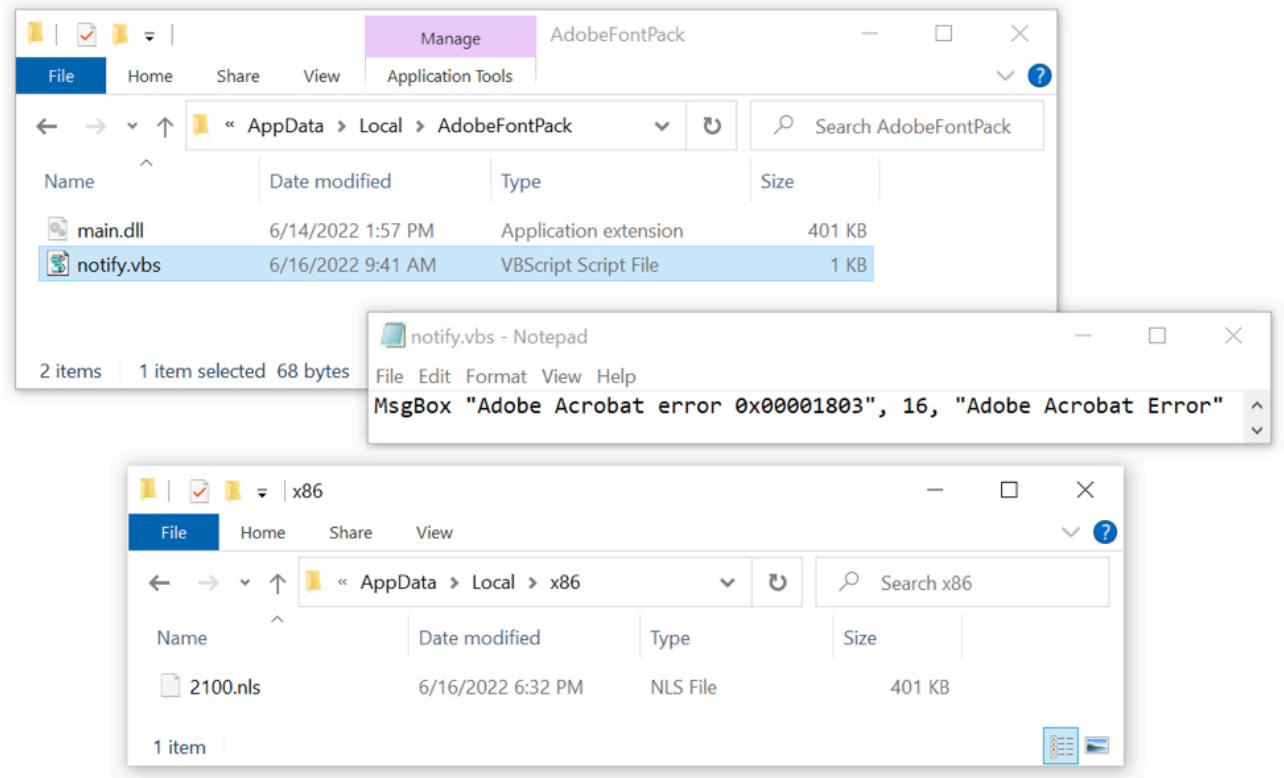
***Running the MSI Package***




*Shown above: MSI package pretends to install an Adobe font pack.*

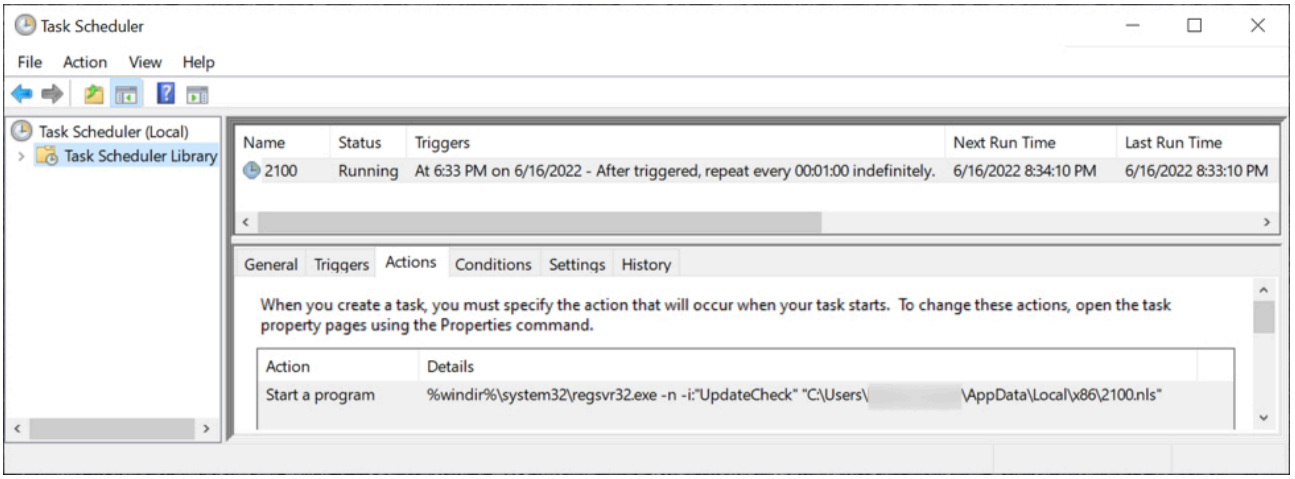



*Shown above: Installation process presents a fake error message.*



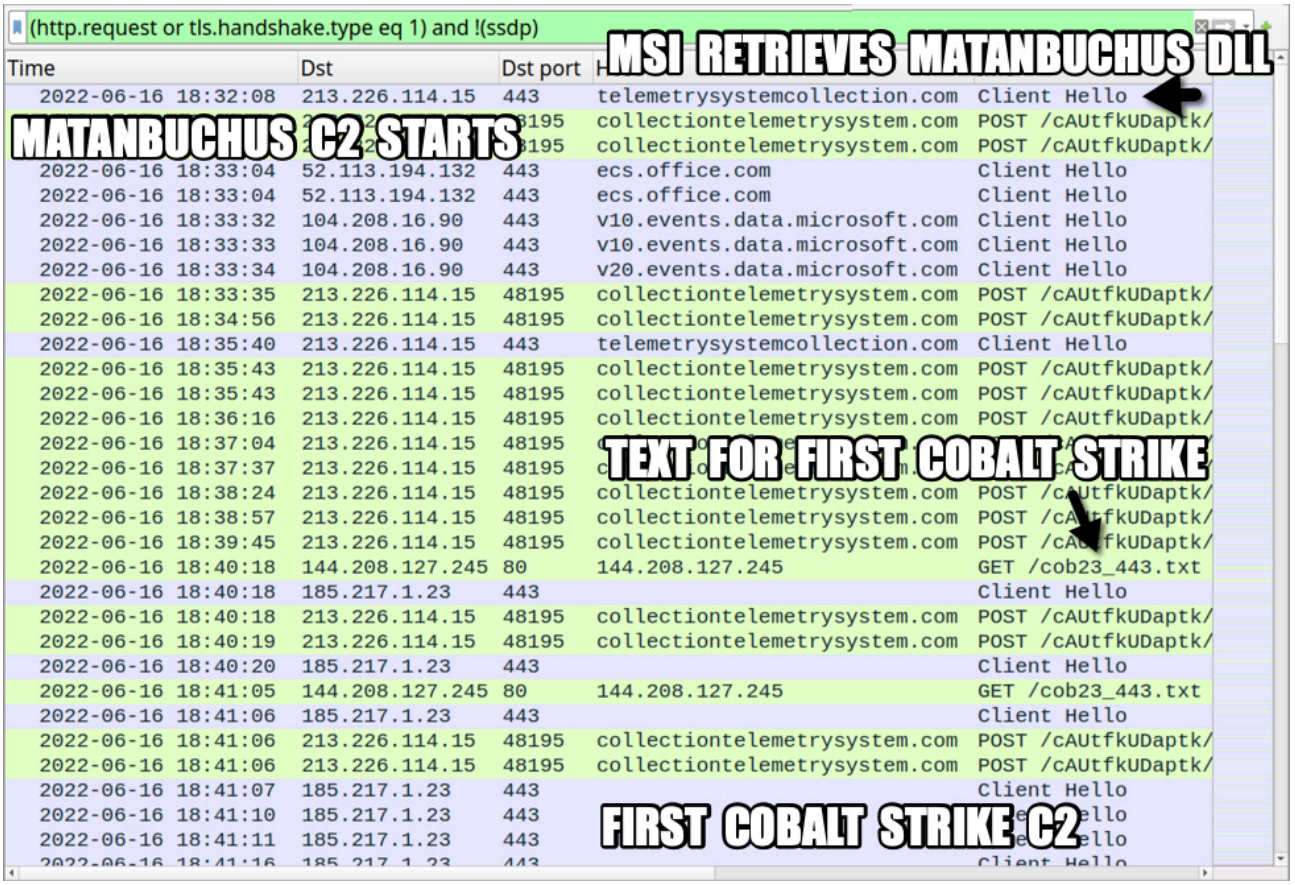

*Shown above: VBS file that generated the fake error message, and the Matanbuchus DLL saved to the infected host in two different locations.*

NOTE: In the above image, the Matanbuchus file ***main.dll*** was dropped by the .msi package, while ***2100.nls*** was retrieved through HTTPS traffic after ***main.dll*** was run. Both have the same SHA256 hash.

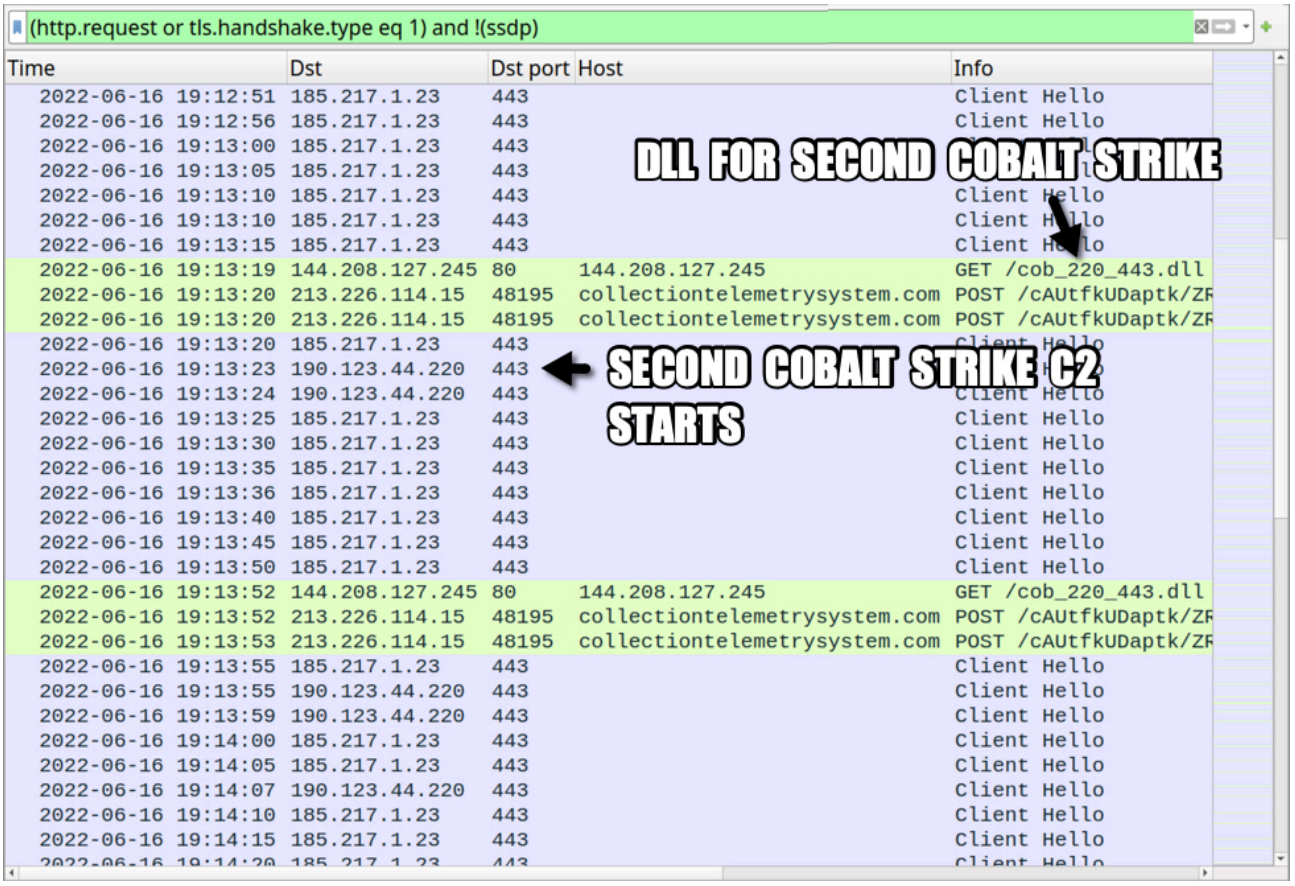



*Shown above: Scheduled task to keep the Matanbuchus malware persistent.*

***Traffic From an Infected Windows Host***




*Shown above: Traffic from an infected Windows host filtered in Wireshark (part 1 of 2).*




| Time | Dst | Dst port | Host | Info |
|---|---|---|---|---|
| 2022-06-16 19:12:51 | 185.217.1.23 | 443 | | Client Hello |
| 2022-06-16 19:12:56 | 185.217.1.23 | 443 | | Client Hello |
| 2022-06-16 19:13:00 | 185.217.1.23 | 443 | | Client Hello |
| 2022-06-16 19:13:05 | 185.217.1.23 | 443 | | Client Hello |
| 2022-06-16 19:13:10 | 185.217.1.23 | 443 | | Client Hello |
| 2022-06-16 19:13:10 | 185.217.1.23 | 443 | | Client Hello |
| 2022-06-16 19:13:15 | 185.217.1.23 | 443 | | Client Hello |
| 2022-06-16 19:13:19 | 144.208.127.245 | 80 | 144.208.127.245 | GET /cob_220_443.dll |
| 2022-06-16 19:13:20 | 213.226.114.15 | 48195 | collectiontelemetrysystem.com | POST /cAUtfkUDaptk/ZF |
| 2022-06-16 19:13:20 | 213.226.114.15 | 48195 | collectiontelemetrysystem.com | POST /cAUtfkUDaptk/ZF |
| 2022-06-16 19:13:20 | 185.217.1.23 | 443 | | Client Hello |
| 2022-06-16 19:13:23 | 190.123.44.220 | 443 | | Client Hello |
| 2022-06-16 19:13:24 | 190.123.44.220 | 443 | | Client Hello |
| 2022-06-16 19:13:25 | 185.217.1.23 | 443 | | Client Hello |
| 2022-06-16 19:13:30 | 185.217.1.23 | 443 | | Client Hello |
| 2022-06-16 19:13:35 | 185.217.1.23 | 443 | | Client Hello |
| 2022-06-16 19:13:36 | 185.217.1.23 | 443 | | Client Hello |
| 2022-06-16 19:13:40 | 185.217.1.23 | 443 | | Client Hello |
| 2022-06-16 19:13:45 | 185.217.1.23 | 443 | | Client Hello |
| 2022-06-16 19:13:50 | 185.217.1.23 | 443 | | Client Hello |
| 2022-06-16 19:13:52 | 144.208.127.245 | 80 | 144.208.127.245 | GET /cob_220_443.dll |
| 2022-06-16 19:13:52 | 213.226.114.15 | 48195 | collectiontelemetrysystem.com | POST /cAUtfkUDaptk/ZF |
| 2022-06-16 19:13:53 | 213.226.114.15 | 48195 | collectiontelemetrysystem.com | POST /cAUtfkUDaptk/ZF |
| 2022-06-16 19:13:55 | 185.217.1.23 | 443 | | Client Hello |
| 2022-06-16 19:13:55 | 190.123.44.220 | 443 | | Client Hello |
| 2022-06-16 19:13:59 | 190.123.44.220 | 443 | | Client Hello |
| 2022-06-16 19:14:00 | 185.217.1.23 | 443 | | Client Hello |
| 2022-06-16 19:14:05 | 185.217.1.23 | 443 | | Client Hello |
| 2022-06-16 19:14:07 | 190.123.44.220 | 443 | | Client Hello |
| 2022-06-16 19:14:10 | 185.217.1.23 | 443 | | Client Hello |
| 2022-06-16 19:14:15 | 185.217.1.23 | 443 | | Client Hello |

*Shown above: Traffic from an infected Windows host filtered in Wireshark (part 2 of 2).*

***Indicators of Compromise (IOCs)***

SHA256 hashes for 7 unique attachments from 14 email examples on 2022-06-16:

- 72426e6b8ea42012675c07bf9a2895bcd7eae15c82343b4b71aece29d96a7b22 SCAN-016063.zip
- 6b2428fcf9e3a555a3a29fc5582baa1eda15e555c1c85d7bef7ac981d76b6068 SCAN-026764.zip
- af534b21a0a0b0c09047e1f3d4f0cdd73fb37f03b745dbb42ffd2340a379dc42 SCAN-068589.zip
- b9720e833fa96fec76f492295d7a46b6f524b958278d322c4ccecdc313811f11 SCAN-231112.zip
- 23fe3af756e900b5878ec685b2c80acd6f821453c03d10d23871069b23a02926 SCAN-287004.zip
- 53af0319d68b0dcbf7cb37559ddfd70cce8c526614c218b5765babdc54500a49 SCAN-446993.zip
- 4242064d3f62b0ded528d89032517747998d2fe9888d5feaa2a3684de2370912 SCAN-511007.zip

SHA256 hashes for HTML files extracted from the above 7 zip archives:

- d0e2e92ec9d3921dc73b962354c7708f06a1a34cce67e8b67af4581adfc7aaad SCAN-016063.html
- 56ec91b8e594824a678508b694a7107d55cf9cd77a1e01a6a44993836b40ec7a SCAN-026764.html
- cc08642ddbbb8f735a3263180164cda6cf3b73a490fc742d5c3e31130504e97c SCAN-068589.html
- e3b98dac9c4c57a046c50ce530c79855c9fe4025a9902d0f45b0fb0394409730 SCAN-231112.html
- c117b17bf187a3d52278eb229a1f2ac8a73967d162ad0cfc55089d304b1cc8a7 SCAN-287004.html
- 82add858e5a64789b26c77e5ec4608e1f162aacbc9163920a0d4aa53eb3e9713 SCAN-446993.html
- 5708dced57f30ff79e789401360300fe3d5bdcf8f988ede6539b9608dfeb58fd SCAN-511007.html

SHA256 hashes for zip archives generated by the above 7 HTML files:

- 63242d49d842cdf699b0ec04ad7bba8867080f8337d3e0ec7e768d10573142b3  SCAN-016063.zip
- 6c5eb5d9a66200f0ab69ee49ba6411abf29840bce00ed0681ec8b48e24fd83da  SCAN-026764.zip
- ef4ea3976bad1cd68a2da2d926677c0cb04f4fc6e0b629b9a29a1c61ae984c46  SCAN-068589.zip
- 19bbebd1e8ec335262e846149a893f4ce803f201e4dee7f3770d95287f9245f3  SCAN-231112.zip
- de26167160e7df91bbd992a3523ea6a82049932b947452bb58e9eed3011c769a  SCAN-287004.zip
- 7f0bf9496f21050fbc1a3ce5ad35dc300f595c71ad9e73ff5fc5c06b2e35a435  SCAN-446993.zip
- 1bc74dfb2142e4929244c6c7e10415664d4e71a5301eaf8e03cb426fab0876f8  SCAN-511007.zip

SHA256 hashes for .msi packages extracted from the above 7 zip archives:

- face46e6593206867da39e47001f134a00385898a36b8142a21ad54954682666  SCAN-016063.pdf.msi
- e22ec74cd833a85882d5a8e76fa3b35daff0b7390bfbcd6b1ab270fd3741ceea  SCAN-026764.pdf.msi
- 2d8740ea16e9457a358ebea73ad377ff75f7aa9bdf748f0d801f5a261977eda4  SCAN-068589.pdf.msi
- 5dcbffef867b44bbb828cfb4a21c9fb1fa3404b4d8b6f4e8118c62addbf859da  SCAN-231112.pdf.msi
- c6e9477fd41ac9822269486c77d0f5d560ee2f558148ca95cf1de39dea034186  SCAN-287004.pdf.msi
- 4fd90cf681ad260f13d3eb9e38b0f05365d3984e38cfba28f160b0f810ffd4d3  SCAN-446993.pdf.msi
- 7e37d028789ab2b47bcab159da6458da2e8198617b0e7760174e4a0eea07d9c9  SCAN-511007.pdf.msi

32-bit DLL for Matanbuchus:

SHA256 hash: f8cc2cf36e193774f13c9c5f23ab777496dcd7ca588f4f73b45a7a5ffa96145e

- File size: 410,624 bytes
- File location: hxxps://telemetrysystemcollection[.]com/m8YYdu/mCQ2U9/auth.aspx
- File location: C:\Users*[username]*\AppData\Local\AdobeFontPack\main.dll
- File location: C:\Users*[username]*\AppData\Local\x86\[4 ASCII characters for hex].nls
- File type: PE32 executable (DLL) (console) Intel 80386, for MS Windows
- Run method: regsvr32.exe *[filename]*

Note: The above DLL was dropped by the .msi package, then it was also retrieved over HTTPS from telemetrysystemcollection[.]com. The HTTPS traffic is probably a way to update the DLL, but in this case, the new file had the same file hash as the original.

Second file sent over HTTPS traffic from telemetrysystemcollection[.]com:

SHA256 hash: 39ec827d24fe68d341cff2a85ef0a7375e9c313064903b92d4c32c7413d84661

- File size: 832,128 bytes
- File location: hxxps://telemetrysystemcollection[.]com/m8YYdu/mCQ2U9/home.aspx
- File type: base64 text

SHA256 hash: a5b06297d86aee3c261df7415a4fa873f38bd5573523178000d89a8d5fd64b9a

- File size: 605,184 bytes
- File description: XOR-ed binary converted from the above base64 text
- File type: data

- Note: This binary XOR-ed with the ASCII string: FuHZu4rQgn3eqLZ6FB48Deybj49xEUCtDTAmF

SHA256 hash: bd68ecd681b844232f050c21c1ea914590351ef64e889d8ef37ea63bd9e2a2ec

- File size: 605,184 bytes
- File type: PE32 executable (DLL) (console) Intel 80386, for MS Windows
- File description: DLL file converted from the above XOR-ed binary
- Note: Unknown entry point for this DLL file

First Cobalt Strike file (ASCII text):

SHA256 hash: 4ee7350176014c7fcb8d33a79dcb1076794a2f86e9b2348f2715ca81f011e799

- File size: 1,668 bytes
- File location: hxxp://144.208.127[.]245/cob23_443.txt
- File type: ASCII text, with very long lines, with no line terminators

SHA256 hash: 7643468adbc1fca4342b7458f0e1dc4ae11c0dde7c06e52fea02c1e057314def

- File size: 834 bytes
- File type: data
- File description: above ASCII text entered into hex editor converted to data binary

Second Cobalt Strike file (32-bit DLL):

SHA256 hash: 6d3259011b9f2abd3b0c3dc5b609ac503392a7d8dea018b78ecd39ec097b3968

- File size: 16,384 bytes
- File location: hxxp://144.208.127[.]245/cob_220_443.dll
- File type: PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
- Run method: regsvr32.exe *[filename]*

Infection traffic:

Traffic for Matanbuchus DLL:

- 213.226.114[.]15 port 443 (HTTPS) - telemetrysystemcollection[.]com - GET /m8YYdu/mCQ2U9/auth.aspx

Additional traffic returning base64 text for XOR-encoded binary:

- 213.226.114[.]15 port 443 (HTTPS) - telemetrysystemcollection[.]com - GET /m8YYdu/mCQ2U9/home.aspx

Matanbuchus C2 traffic:

- 213.226.114[.]15 port 48195 (HTTP) - collectiontelemetrysystem[.]com - POST /cAUtfkUDaptk/ZRSeiy/requets/index.php

Traffic caused by Matanbuchus for Cobalt Strike:

- 144.208.127[.]245 port 80 - 144.208[.]127.245 - GET /cob23_443.txt
- 144.208.127[.]245 port 80 - 144.208[.]127.245 - GET /cob_220_443.dll

First Cobalt Strike C2 traffic:

- 185.217.1[.]23 port 443 - hxxps://extic[.]icu/empower/type.tiff
- 185.217.1[.]23 port 443 - hxxps://extic[.]icu/*[unknown]*

Second Cobalt Strike C2 traffic:

- 190.123.44[.]220 port 443 - hxxps://reykh[.]icu/load/hunt.jpgv
- 190.123.44[.]220 port 443 - hxxps://reykh[.]icu/thaw.txt

Note: The above Cobalt Strike activity did not generate any DNS traffic for the associated .icu domains.

***Final Words***

14 email examples, a packet capture (pcap) of traffic from an infected Windows host, and the associated malware/artifacts can be found here.

---

Brad Duncan
brad [at] malware-traffic-analysis.net

---