SANS ISC: Excel spreadsheets push SystemBC malware - SANS Internet Storm Center SANS Site Network Current Site SANS Internet Storm Center Other SANS Sites Help Graduate Degree Programs Security Training Security Certification Security Awareness Training Penetration Testing Industrial Control Systems Cyber Defense Foundations DFIR Software Security Government OnSite Training SANS ISC InfoSec Forums

Excel spreadsheets push SystemBC malware

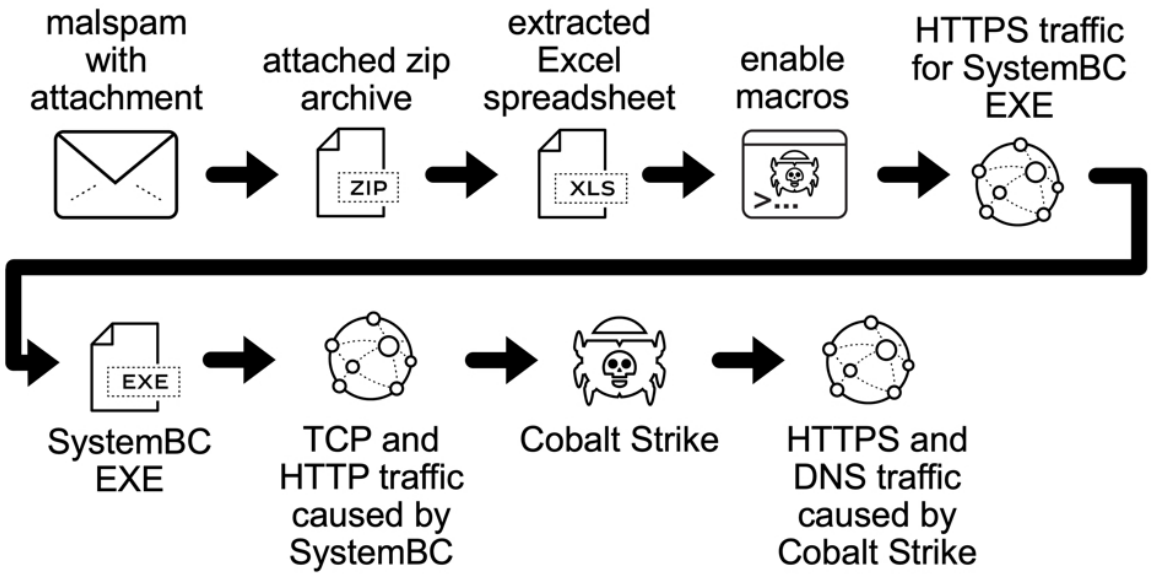
Brad
433 Posts
ISC Handler
Feb 3rd 2021

Introduction

On Monday 2021-02-01, a fellow researcher posted an Excel spreadsheet to the Hatching Triage sandbox. This Excel spreadsheet has a malicious macro, and it uses an updated GlobalSign template that I hadn't noticed before (link for the sample).

This Excel spreadsheet pushed what might be SystemBC malware when I tested it in my lab environment on Monday 2021-02-01. My lab host was part of an Active Directory (AD) environment, and I also saw Cobalt Strike as follow-up activity from this infection.

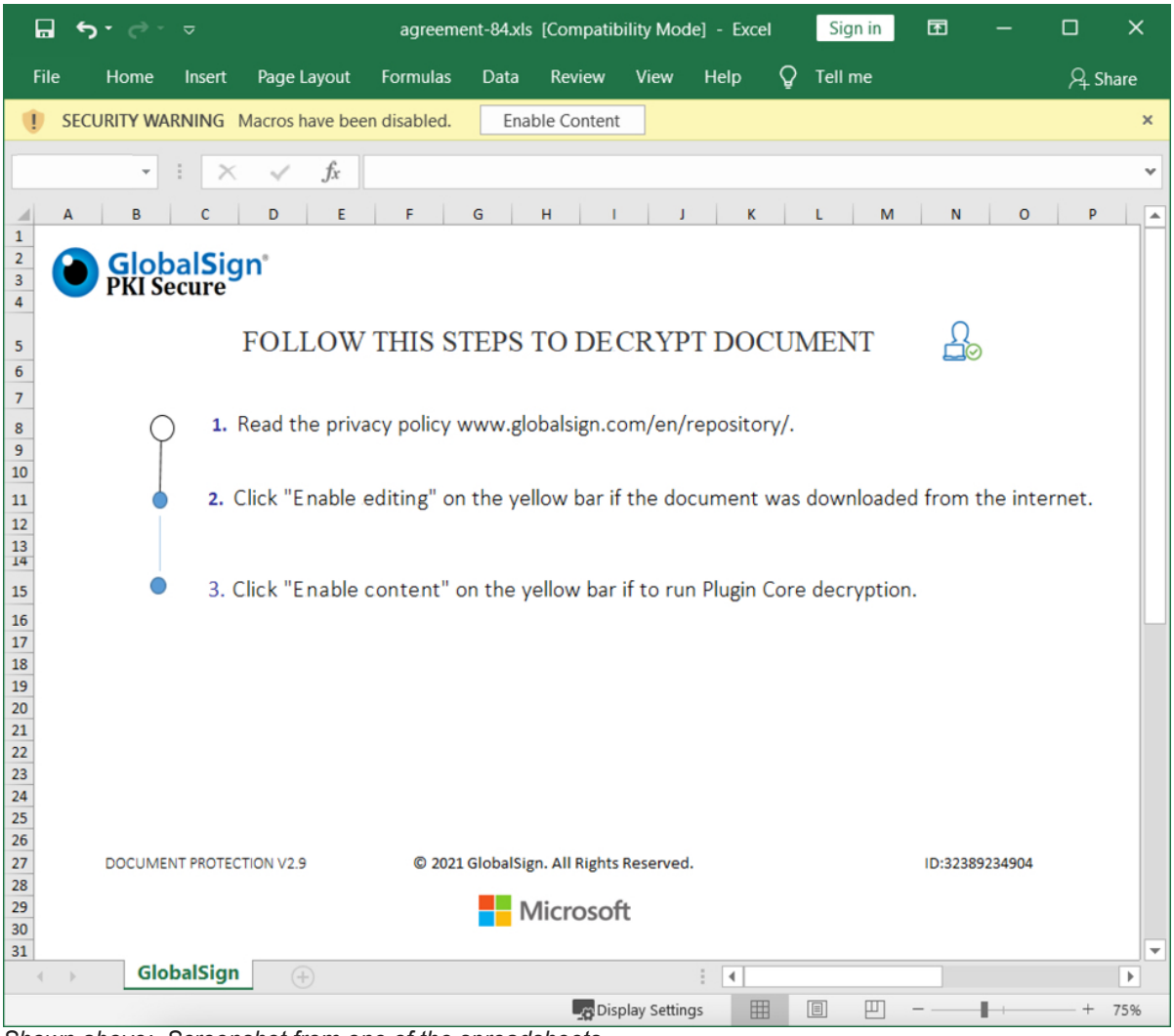
Today's diary reviews this specific instance of (what I think is) SystemBC and Cobalt Strike activity from Monday 2021-02-01.



Shown above: Flow chart from the SystemBC infection on Monday 2021-02-01.

Infection Path

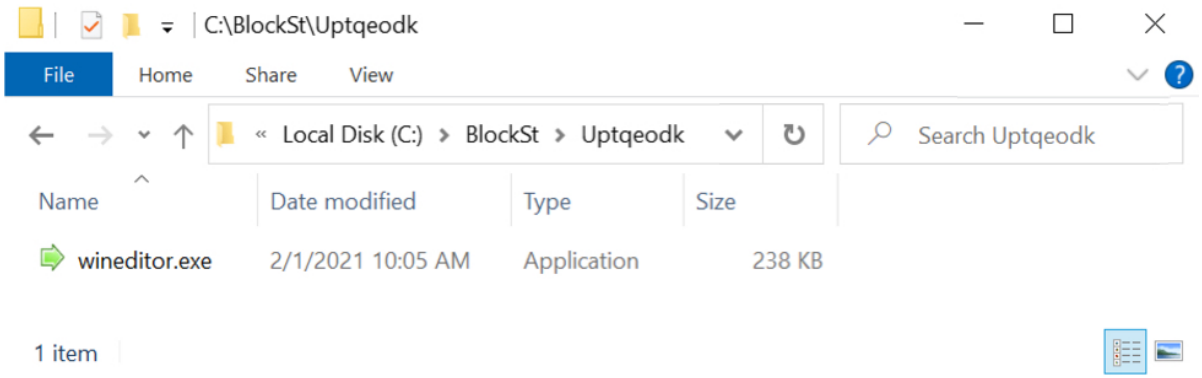
I didn't know where these spreadsheets were coming from when I investigated this activity on Monday 2021-02-01. By Tuesday 2021-02-02, several samples had come into VirusTotal showing at least 20 spreadsheets that were contained in zip archives. These appear to have been attachments using emails as a distribution method. Unfortunately, I couldn't find any emails submitted to VirusTotal yet that contained one of the zip archives.



Shown above: Screenshot from one of the spreadsheets.

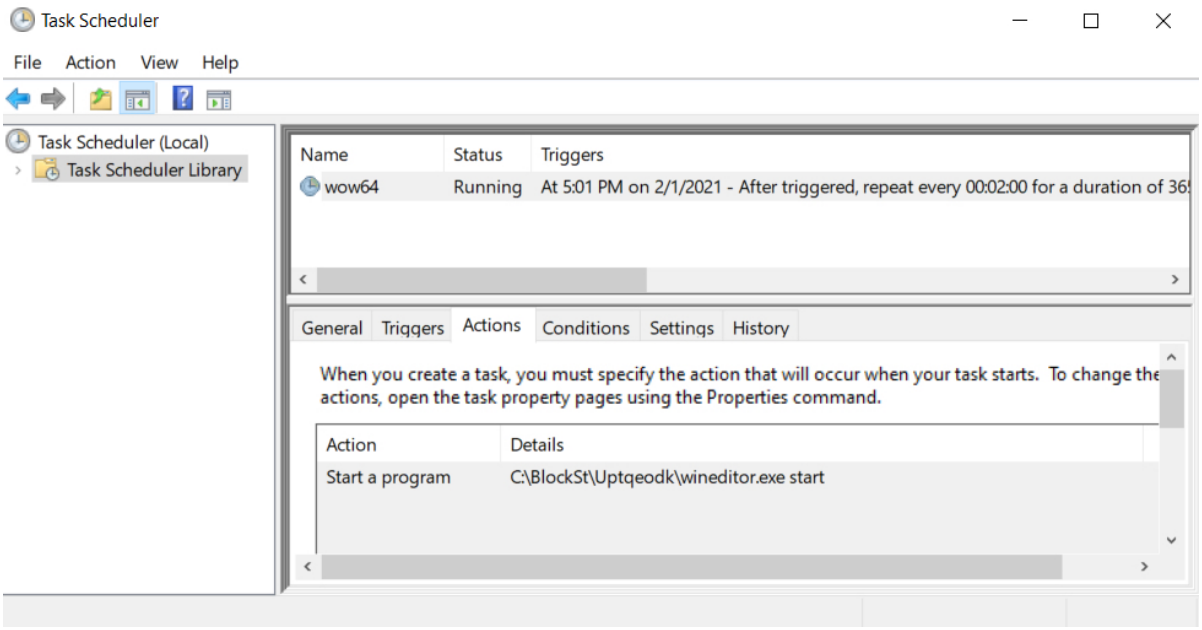
Spreadsheet macro grabs SystemBC malware

Enabling macros on a vulnerable Windows host caused HTTPS traffic to grab a Windows executable (EXE) file for SystemBC malware. This EXE was stored and run from new directory path created under the C:\ drive as shown below.



Shown above: SystemBC malware saved to the infected Windows host.

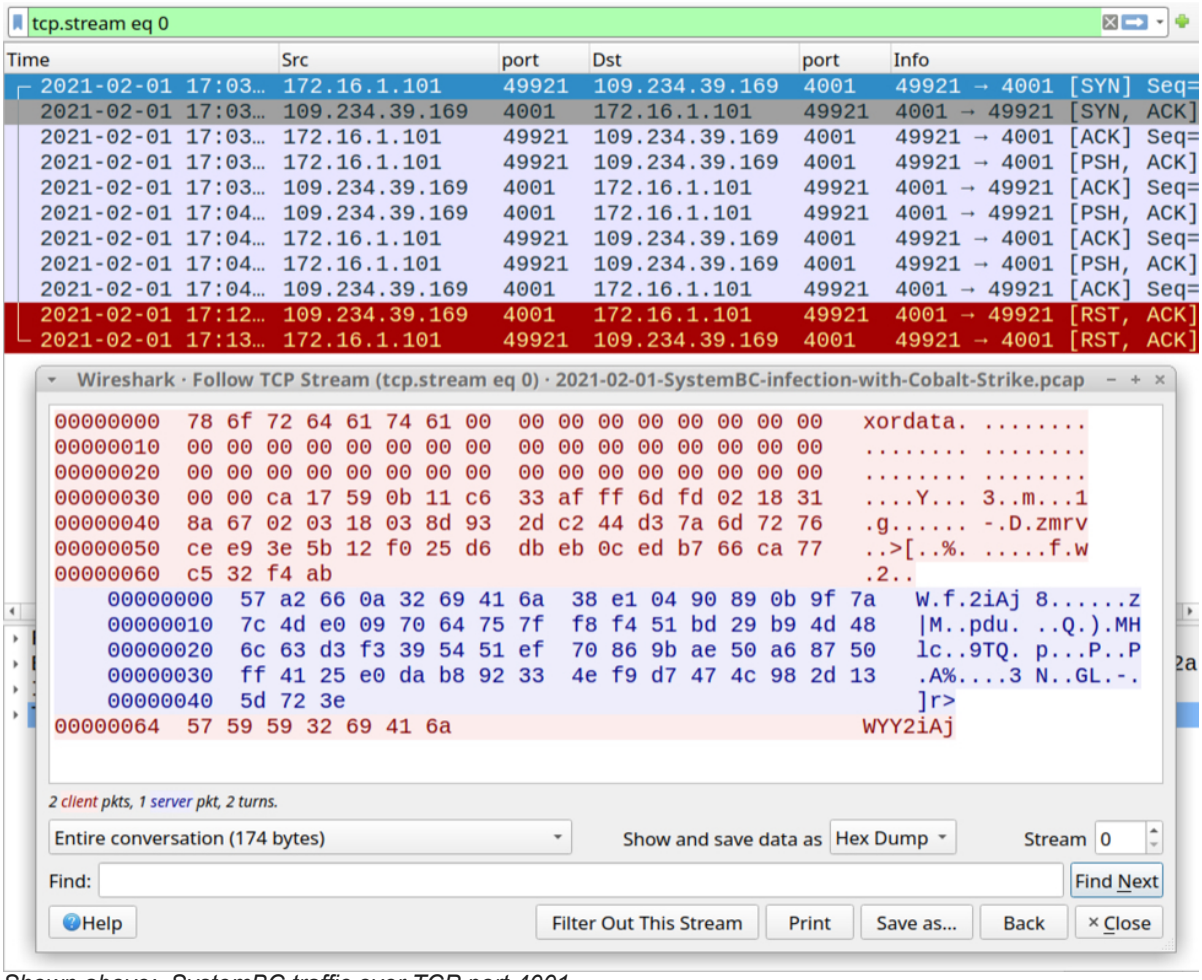
This EXE file was made persistent on the infected host through a scheduled task.



Shown above: Scheduled task to keep the malware persistent.

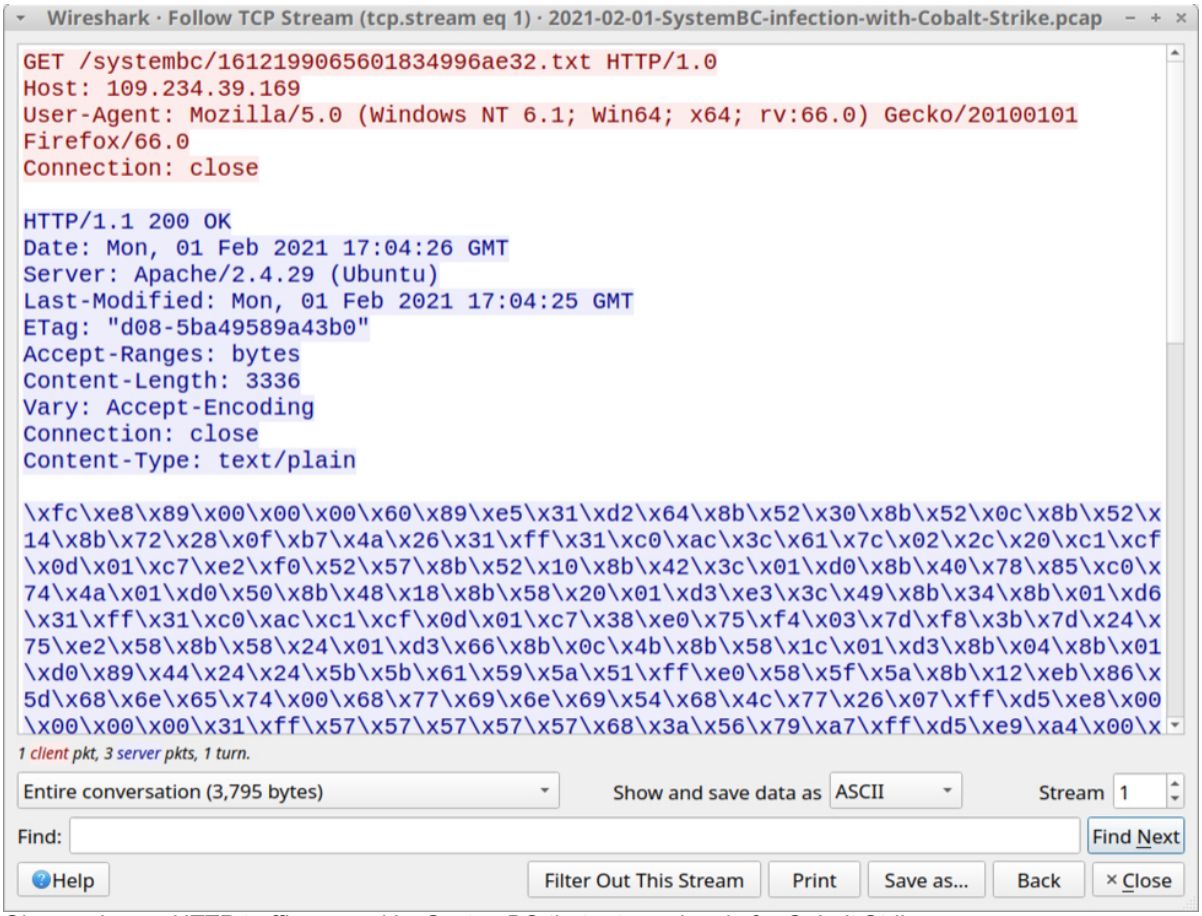
SystemBC post-infection traffic

The first post-infection traffic caused by SystemBC was TCP traffic to 109.234.39[.]169 over port 4001 as shown below.



Shown above: SystemBC traffic over TCP port 4001.

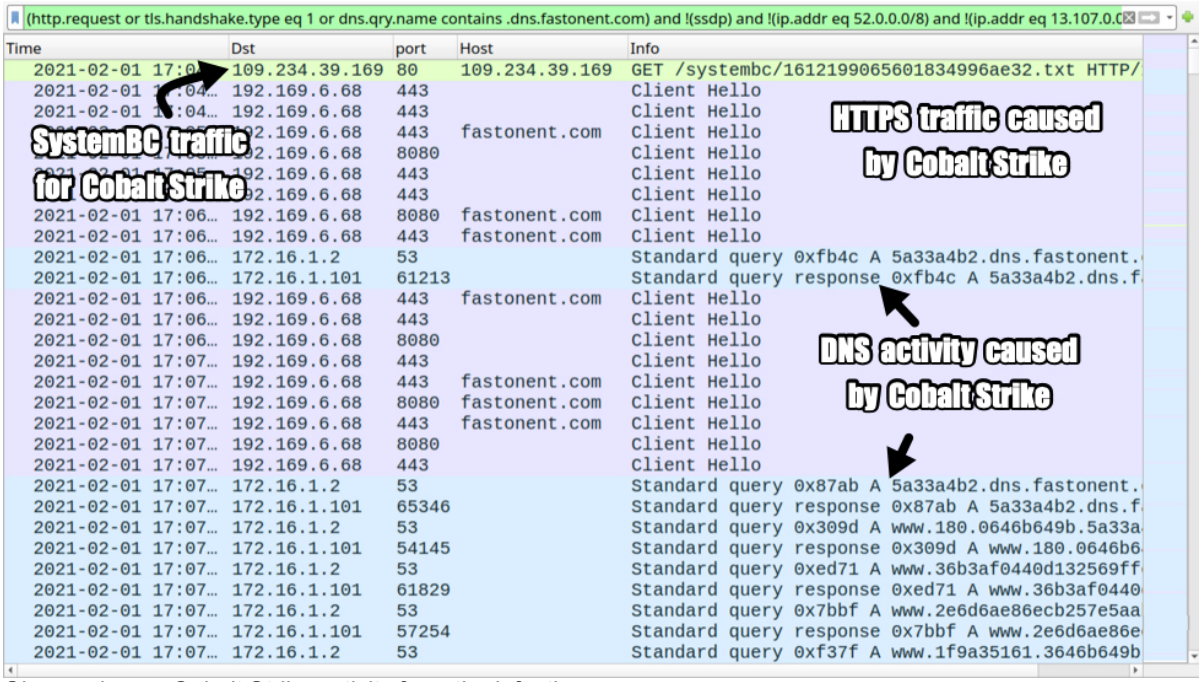
Next was HTTP traffic to the same IP address over TCP port 80 that returned obfuscated text containing code to start the Cobalt Strike activity.



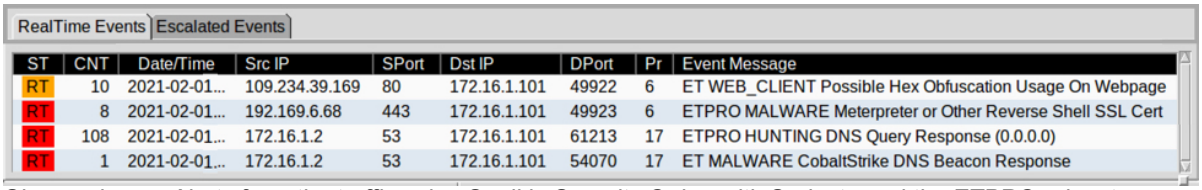
Shown above: HTTP traffic caused by SystemBC that returned code for Cobalt Strike.

Cobalt Strike traffic

Cobalt strike activity consisted of HTTPS traffic and DNS activity focused on the domain fastonent[.]com.



Shown above: Cobalt Strike activity from the infection.



RealTime Events | Escalated Events

ST	CNT	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	10	2021-02-01...	109.234.39.169	80	172.16.1.101	49922	6	ET WEB_CLIENT Possible Hex Obfuscation Usage On Webpage
RT	8	2021-02-01...	192.169.6.68	443	172.16.1.101	49923	6	ETPRO MALWARE Meterpreter or Other Reverse Shell SSL Cert
RT	108	2021-02-01...	172.16.1.2	53	172.16.1.101	61213	17	ETPRO HUNTING DNS Query Response (0.0.0.0)
RT	1	2021-02-01...	172.16.1.2	53	172.16.1.101	54070	17	ET MALWARE CobaltStrike DNS Beacon Response

Shown above: Alerts from the traffic using Squil in Security Onion with Suricata and the ETPRO ruleset.

Indicators of Compromise (IOCs)

SHA256 HASHES OF 20 ZIP ARCHIVES WITH THE 20 EXCEL FILES THEY CONTAIN:

- 31a04fe64502bfe6f73971f9de9736402dd9a21a66d41d3a4ecea5ee18852f1c documentation-82.zip
- a54b331832d61ae4e5a2ec32c46830df4aac4b26fe877956d2715bfb46b6cb97 Document21467.xls

- ce02ed48d9ab12dfe2202c16f1f272f75e5b1c0b64e48e385ca71608cb686fc8 documentation-17.zip
- 62f1ef07f7bab2ad9abf7aeb53e3a5632527a1839c3364fbaebadd78d6c18f4e Document13160.xls

- 4dfb0bb69a07f1cd7b46198b5edf8afebd0cdd02f27eb2c687447f692625fb9f contract-86.zip
- 59bbcecd3b1670afc5430e3b31377f24da24f4e755b7c563a842ce4e325aa61a Document24071.xls

- c3a38df6f4864d32c10e8ecf063e18cba56c3b1add3404634ea20ea109198620 agreement-92.zip
- 8ef917da85afcc5f7bfe9cc2afd29f44a7f0cda5ba0249b50ef448d547007461 Document1525.xls

- 3a181036cdc46e088f1cb98acd06062d32a8a11a8ef65fe7544bb22a2fd5c56e information-94.zip
- 387bdfedc306e087d8ceceb1f1f8f7a6b3c32110ca3d7273eb01e474349d1974 Document10668.xls

- 244625f6627cadadb7faf8a6b526e91aee4f5c1cadfa1c0d4fb996f4cc60a5ae documentation-18.zip
- 17ed4dc4369a90d2e24f1ab0fa1eeb6fca61f77b183499c47e5cfb9ce12130fb Document7833.xls

- cca4a3c8af9b549b445b7e2bcb2d45b95982890b6ed3b62fc882f0478f512b2f agreement-44.zip
- f682f0756ec96d262ae4c48083d720657685d9b56278bd07b2656f3b33be985e Document1047.xls

- dcff925d51e90586eb624f249e56b6abb7026b364fab84dcfcf44025e84ff7d9 DOCUMENT-30.zip
- 2e726c5a27e04633d407e13bd242ae71865eef13ac78bf9068e1200823e5ea81 Document15758.xls

- dc5a3675455d9486e7aa8aaf2463b69ad03c508375eb99b6fb3039d914677a9f information-94.zip
- 6c0ef43c1f8b4425d034a46812903b8a6345ae24e556e61e37c0f14eba8c8d2e Document15979.xls

- 7d1602138a26c0524b32570f3fb292fd5a7efbc5ed53ae260d7b7f3652a78969 documentation-83.zip
- b4107daacbbfac1b9bc9b3fa4e34a8d87037fa2c958db9d6d7df52380f15a1d1 Document16000.xls

- 0fb4d8ac3cdef038bf53c8f4269eef5845704a9e962b7609fd93a9f08cc2fab1 documentation-48.zip
- ff483bbb98d02d1e071d6f0e8f3a3c1706c246db71221455b29f4e54b0c4ef2f Document29060.xls

- 0cf4fff7f96cf695d3476e7dc66794d067acafbd2980f69526b874fc5b4c08be docs-62.zip
- 441f076519f0bdc04d110b4fa73dbafa3b667825ceab6d4099e36714bd1d7213 Document5804.xls

- 056911f208c9b475020627b83c8bf3a0151e30ec7f71113cf75abb950a431efc answer-46.zip
- 795a5d5c57dac1703c6b4bab9507d1c662180716b4afa89c261aa3bb6d164e2f Document10660.xls

- 31901336fdfae4fdeac46b937a059c618d5ba3e04d06bb8e95108a307e2c6d94 DOCUMENT-74.zip
- b2aa3ee1cc617f90e92664969a0856d98a97c727edd7c81ef83c038a34a432d5 Document4083.xls

- e06ee4e0bbe581edc39aecaab76e3fa12a53cb971ec0c106644703b376f5ed24 reaction-32.zip
- a3ce1043a7791b73fe14d7c29377467fd64df3b3b464c48a22a6d3bd2f7786aa Document18681.xls

41 OTHER EXCEL FILES WITH THE SAME DOCUMENT TEMPLATE:

- 044494acb6d781e6cc3b9a837b7ebca1e933080fe384a874f5eb9cca1ea76a55 DOCUMENT-99.xls
- 071809d68b777cae171284c2cc289b455a778b1f054cd0f244cf0fb6053dae2d documentation-47.xls
- 0e094197fca1947eb189006ddeb7d6ad9e5d1f58229e929bc0359887ed8a667d agreement-84.xls
- 134a5bfe06f87ace41e0e2fb6f503dca0d521cb188a0c06c1c4bc734ad01e894 Document5201.xls
- 13ef189260cd344e61a0ad5907c5e695372b00fe1f5d5b2b3e389ad2b99b85e4 documentation-32.xls
- 17fb4271ab9113a155c091c7d7bd590610da87e986ccf5962aa7fc4b82060574 SG_information-24.xls
- 19065d8aa76ba67d100d5cb429a8b147c61060cc49905529d982042a55caceef agreement-26.xls
- 1b63ff13d507f9d88d03e96c3ef86c7531da58348f336bc00bf2d2a2e378fd90 documentation-63.xls
- 1d8fd79934dc9e71562e50c042f9fa78a93fa2991d98c33e0b6ab20c0b522d5a required-47.xls
- 1e295b33d36dee63930728349be8d4c7b8e5b52f98e6a8d9ca50929c8a3c9fb1 contract-52.xls
- 2156a9f3d87d3df1cee3f815f609c2a3dc2757717ff60954683c34794e52b104 document-85.xls

- 21db2f562b9182a3fcdb0fce8c745b477be02b4a423a627cddf6a1c244b6c415 DOCUMENT-64.xls
- 2f66e8d84e87811feaf73e30b08be0ad6381271ddfb5071556bd26cd3db2c3f4 documents-74.xls
- 32452e930a813f41a24dc579a08e8dde1801603797d527ce1385ad414b00e676 Document9330.xls
- 32a904d301e8a30b7bd70804b905dd7b858b761979f3344bc2ec3bff0cb6d703 DOCUMENT-64.xls
- 3dcd7897ad927f4b2b860010963e02903bc68a2c0c86abb1a27b8cbaab2fa9b6 document-91.xls
- 418460bf69c01e47cbe261d7f7312475cda4305860fbbe3d3e6639b9adb78de5 Document8107.xls
- 49cb79f8547c9c94a7ab6642ba1c40fcd036625f71845f2c6203d76c5f7f46fb documents-44.xls
- 4af6e8805273ca9b3dea793bd712ed785ea5c5ed9e387cb8ab5059a4f364a303 docs-49.xls
- 584c2aab3fe9e1ec9f9dffecbd32e6af8b6b3fa3141c7ddf845763cbf14a82eb DOCUMENT-30.xls
- 5cecb7e104e73aa9916a7154a3004d1a71c59c8f473d693f3b285b2fd473e454 documentation-66.xls
- 669de92b909247d676daa6bab3b3ae5be4fbec2e77f66915267f032c1d7eb71a agreement-50.xls
- 6bf9612a2b8288d55b47648f9ad9ee80cca5058ced5fb77254e57f9ff2d701d3 contract-38.xls
- 6df34ffeffb9cc5def3c424cd8bb0f90ab921be24efd1f8fe52ea6c13e700334 data-65.xls
- 8072f20dd769519a621255307b03e85dca2fe227f48486b0aacc41903ab3bfdf Document12611.xls
- 8eb429c24872a501fafc783e8a0fcc53e0ebb5cc8ec4f2310fc10102b1d23a27 contract-90.xls
- 908cb8f6f39b9c310d8df54bddf667d23b0851bbf90b21ca89ea69d211f2c402 Document21461.xls
- 9519a0631804d18f95d4c3239df5e5ea56b8e5a890b73c889a58d6469958eb71 Document11622.xls
- 952ec18a6dc949ebd335f5eabed756d0f562aa3853fe9384dc0eded0de5f843b required-36.xls
- a274a08d84958666b6c94e1a6fc3b676aca387544a4218c8473e1a9a72124532 documentation-45.xls
- a7b362864724ccb5cba416ff45b4e137f22f8fed4492b5521e369026107031b2 Document9470.xls
- ab9b97d0d17b2434d2cfc66106ae07b903271ba603be1314b742338c23cce20c docs-72.xls
- c4d745576b47b6dd79a9d92cda7dbe60c2cda7d8960a07e33692e6e71f8e5eb3 document-78.xls
- c8fd542a9b500ada7afbff26b6c11dd2ab22aaefd30ef7a999410ee20d2fb043 answer-69.xls
- d0c96aacb07629b9d97641a0022b50827f73d86a34fa4929b126f398cf4cf486 Document21265.xls
- d3145f4f7b1c62f9a1937aa9e968da8b52ff4fde83c0dba3152567b2b65d809a documentation-49.xls
- d4e372014a40821f10780fcc12c6b5a1cdf4740738a0769e78f06dd10b6ec53f daret.xls
- d85eb8e5c39d7681155e39602ce30e0c3793b4513f1038e48334296db945e02d documentation-29.xls
- e26ab2d6cff95ba776ec6e7beb8c70f2e4d79467b71153ddb36177cb2b2a1273 Document4677.xls
- e64d605e857900a07c16e22e288c37355e4ebd6021898268ab5dded5c8c4efca documentation-99.xls
- f5e2351ff528c574dc23c7ef48ddac42546c86d77c28333b25112a9efbfb9d93 Document18108.xls

AT LEAST 7 URLS GENERATED BY EXCEL MACROS FOR A MALWARE PAYLOAD:

- hxxps://alnujaifi-portal[.]com/ds/3101.gif
- hxxps://clinica-cristal[.]com/ds/3101.gif
- hxxps://eyeqoptical[.]ca/ds/3101.gif
- hxxps://gbhtrade.com[.]br/ds/3101.gif
- hxxps://newstimeurdu[.]com/ds/3101.gif
- hxxps://remacon[.]net/ds/3101.gif
- hxxps://skconstruction[.]info/ds/3101.gif

MALWARE PAYLOAD EXAMPLE (SYSTEMBC EXE):

- SHA256 hash: 61499704920ee633ffb2baab36eb8eb70d5e0426bca584f9a4a872e4b930c417
- File size: 243,200 bytes
- File location: C:\BlockSt\Uptqeodk\wineditor.exe

SYSTEMBC TRAFFIC:

- 109.234.39.169 over TCP port 4001 - encoded/encrypted data
- 109.234.39.159 over TCP port 80 - GET /systembc/[24 ASCII characters representing hex string].txt

COBALT STRIKE ACTIVITY:

- 192.169.6.8 over TCP port 443 - no domain - HTTPS traffic
- 192.169.6.8 over TCP port 443 - fastonent[.]com - HTTPS traffic
- 192.169.6.8 over TCP port 8080 - fastonent[.]com - HTTPS traffic
- DNS queries/responses for various domains ending with .dns.fastonent[.]com

Final words

I'm not 100 percent sure this malware is SystemBC, but HTTP traffic caused by the EXE has /systembc/ in the URL, so I'm calling it SystemBC until someone identifies it as another malware family.

When I ran the spreadsheet on a stand-alone host, I only saw SystemBC traffic over TCP port 4001. I didn't see the Cobalt Strike traffic until I infected one of my lab hosts within an AD environment. This reflects a trend I've noticed with at least one another malware family (Hancitor), where Cobalt Strike doesn't appear unless the infected host is running in an AD environment.

A pcap of the infection traffic and and malware from the infected Windows host can be found here.

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

Thread locked Subscribe	Feb 3rd 2021 1 year ago
The same image was in Buerloader https://bazaar.abuse.ch/sample/030af453e0140f45b22c9e2fa1dc1441371e55455e4d207eaed78229800ff6b7/ and there were a similar Usedrange "A1:C63" in BazarLoader https://bazaar.abuse.ch/sample/75de7712c3817911df0973c769c348f24593b996b513c1550260626e69a8a99d/	Anonymous
Quote	Feb 3rd 2021 1 year ago
Refering to you diary from yesterday: New Example of XSL Script Processing aka "Mitre T1220" Labeled with "Dridex" https://bazaar.abuse.ch/sample/ddb6ba574987bb5c09e49ccf8446d63b192b04297a902081a32e57cd86cf5000/ uses the XSL-method as well: the code is in the text of the second form BTW: Thank you for the explanation about XSL	Anonymous
Quote	Feb 3rd 2021 1 year ago