

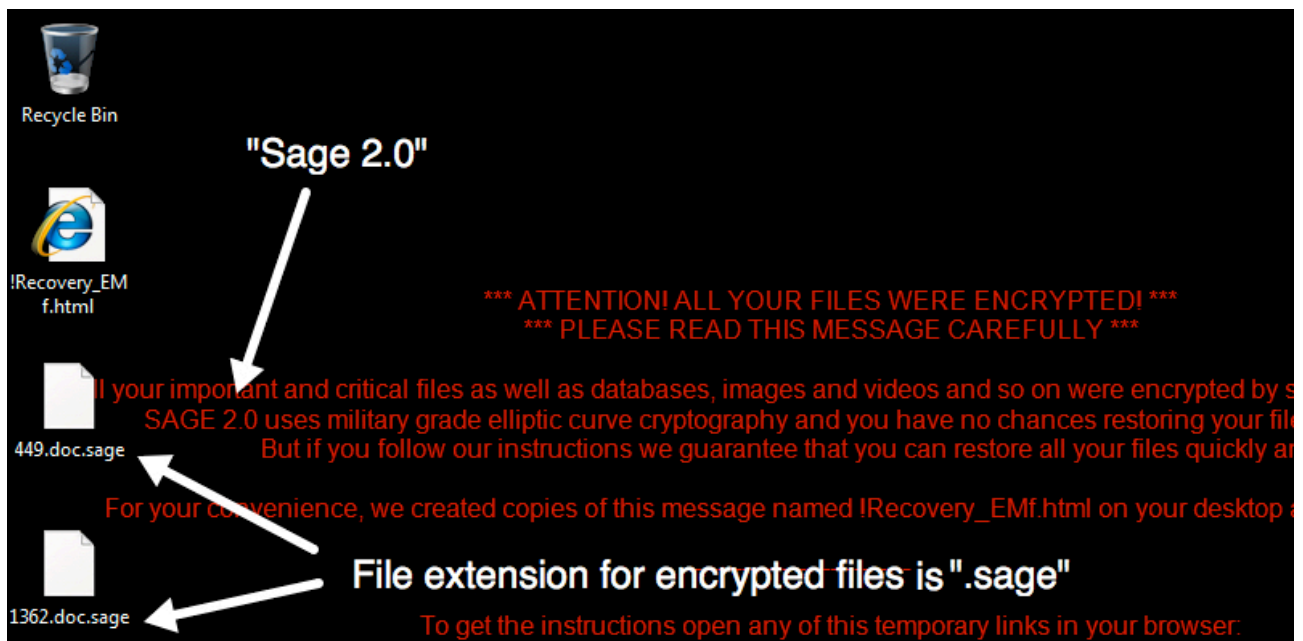
Sage 2.0 Ransomware - SANS Internet Storm Center

By SANS Internet Storm Center

Archived: 2026-04-05 19:04:08 UTC

Introduction

On Friday 2017-01-20, I checked a malicious spam (malspam) campaign that normally distributes Cerber ransomware. That Friday it delivered ransomware I'd never seen before called "Sage." More specifically, it was "Sage 2.0."



Shown above: It's always fun to find ransomware that's not Cerber or Locky.

Sage is yet another family of ransomware in an already crowded field. It was noted on BleepingComputer forums back in December 2016 [[1](#), [2](#)], and Sage is a variant of [CryLocker](#) [[3](#)]. Unfortunately, I can't find an in-depth write-up on Sage that I like. With that in mind, this diary examines Sage 2.0.

The malspam

Emails from this particular campaign generally have no subject lines, and they always have no message text. The only content is a zip attachment containing a Word document with a malicious macro that downloads and installs ransomware. Sometimes, I'll see a .js file instead of a Word document, but it does the same thing.

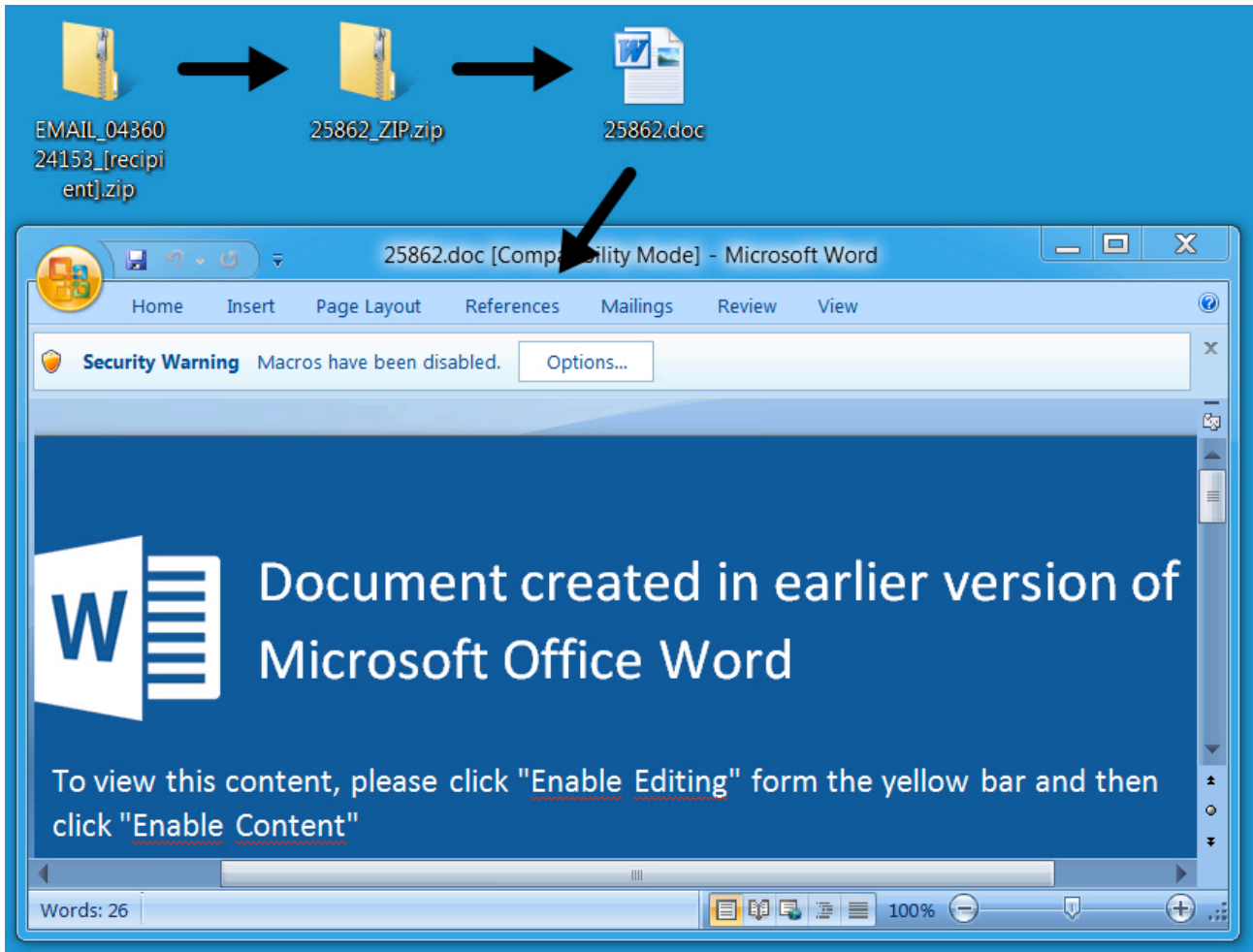
Date/Time	Sending mail server	Sending address (spoofed)	Subject	Attachment
2017-01-19 07:19 UTC	116.107.81.133	<dan_calkin@maysoft.com>	(none)	EMAIL_807388025533838_[recipient].zip
2017-01-19 07:51 UTC	colomna.net	<danny.h@post.cz>	(none)	EMAIL_42654088199_[recipient].zip
2017-01-19 08:13 UTC	vnpt.vn	<anna@monadance.org>	(none)	EMAIL_7281945_[recipient].zip
2017-01-19 14:35 UTC	hinet.net	<panakova@technicalmuseum.cz>	(none)	EMAIL_608170693_[recipient].zip
2017-01-19 15:53 UTC	dyn.bashtel.ru	<g_yorum35@windowslive.com>	(none)	EMAIL_6161214_[recipient].zip
2017-01-19 16:52 UTC	69.80.21.25	<jiggymovementbusiness@gmail.com>	(none)	EMAIL_327120_[recipient].zip
2017-01-19 16:57 UTC	ucom.am	<sherryloveless@gmail.com>	(none)	505635089.zip
2017-01-20 00:26 UTC	city-telekom.ru	<kasia_094@wp.pl>	(none)	EMAIL_77900715_[recipient].zip
2017-01-20 14:19 UTC	maxwifi.com.br	<highlandersboxingclub@live.com>	(none)	96676808070.zip
2017-01-20 16:36 UTC	c2h.no	<mmutchek@cox.net>	(none)	EMAIL_0436024153_[recipient].zip

Shown above: Data from a spreadsheet tracking the malspam (1 of 3).

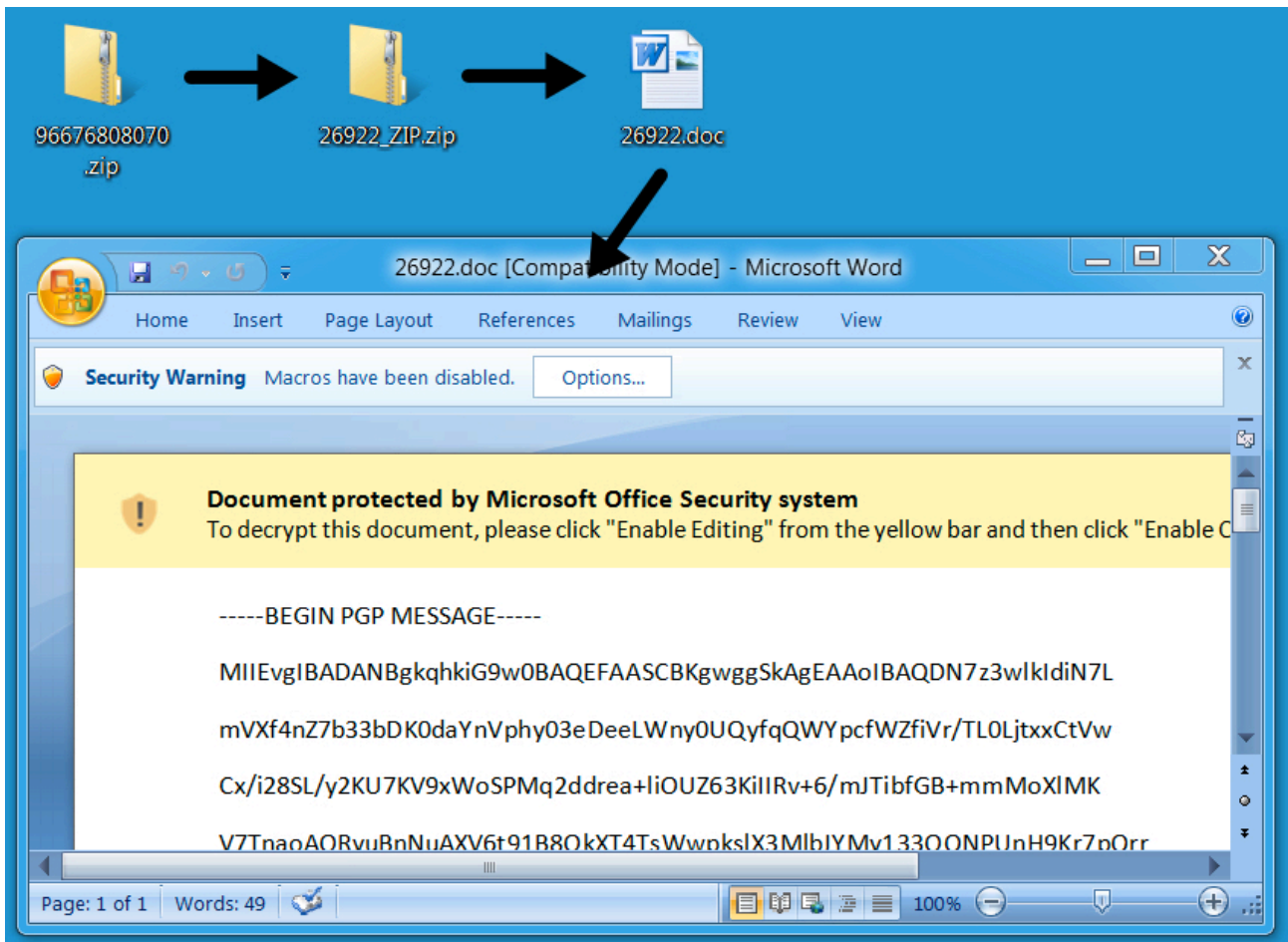
Often, the recipient's name is part of the attachment's file name. I replace those names with [recipient] before I share any info. A more interesting fact is the attachments are often double-zipped. They contain another zip archive before you get to the Word document or .js file.

Attachment	ZIP inside the ZIP	Extracted file
EMAIL_807388025533838_[recipient].zip	22044_ZIP.zip	22044.js
EMAIL_42654088199_[recipient].zip	380_ZIP.zip	380.js
EMAIL_7281945_[recipient].zip	12824_ZIP.zip	12824.js
EMAIL_608170693_[recipient].zip	13622_ZIP.zip	13622.doc
EMAIL_6161214_[recipient].zip	32449_ZIP.zip	32449.doc
EMAIL_327120_[recipient].zip	22230_ZIP.zip	22230.doc
505635089.zip	8970_ZIP.zip	8970.doc
EMAIL_77900715_[recipient].zip	20703_ZIP.zip	20703.doc
96676808070.zip	26922_ZIP.zip	26922.doc
EMAIL_0436024153_[recipient].zip	25862_ZIP.zip	25862.doc

Shown above: Data from a spreadsheet tracking the malspam (2 of 3).



Shown above: Example of a Word document with a malicious macro.



Shown above: Another example of the Word document with a malicious macro.

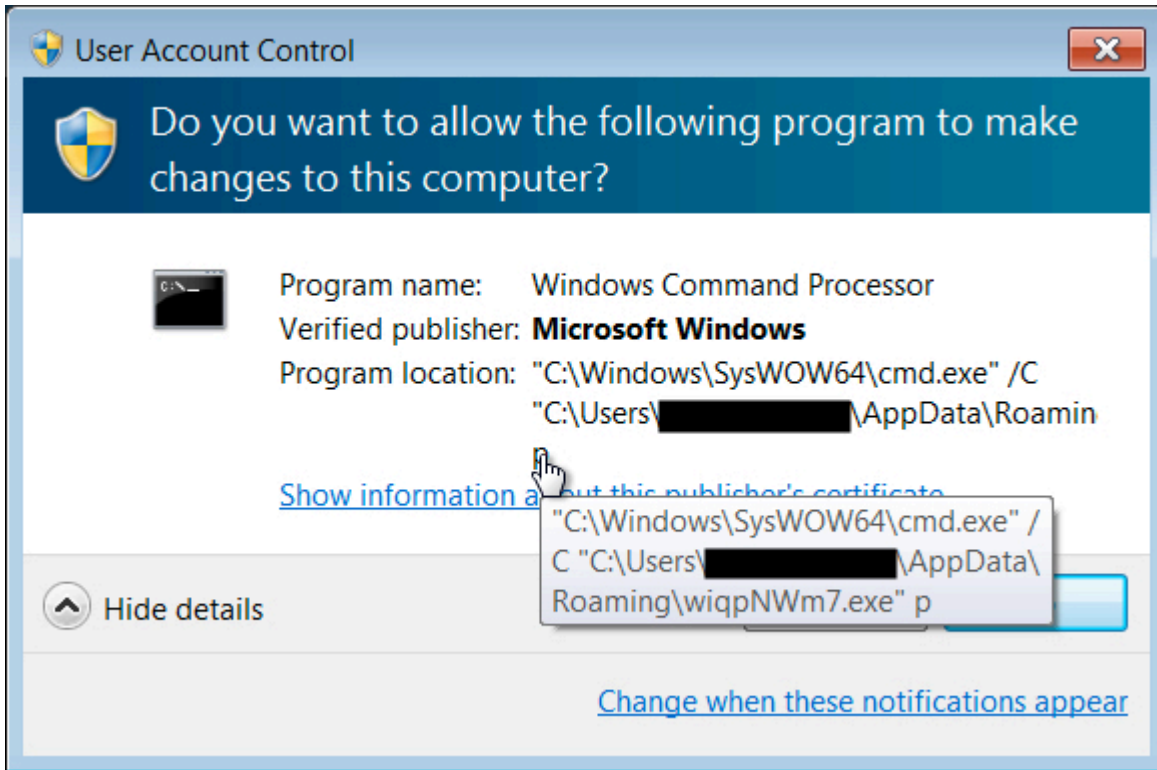
The Word document macros or .js files are designed to download and install ransomware. In most cases on Friday, the ransomware was Sage 2.0.

Extracted file	URL generated by extracted file	Ransomware on the local host	Ransomware
22044.js	fortycooola.top - GET /user.php?f=0.dat	C:\Users\[username]\AppData\Local\Temp\equcuh.exe	Sage 2.0
380.js	fortycooola.top - GET /user.php?f=0.dat	C:\Users\[username]\AppData\Local\Temp\mulwyqr.exe	Sage 2.0
12824.js	fortycooola.top - GET /user.php?f=0.dat	C:\Users\[username]\AppData\Local\Temp\jmaxgo.exe	Sage 2.0
13622.doc	smoeroota.top - GET /read.php?f=0.dat	C:\Users\[username]\AppData\Local\Temp\Roaming.Exe	Sage 2.0
32449.doc	smoeroota.top - GET /read.php?f=0.dat	C:\Users\[username]\AppData\Local\Temp\Roaming.exe	Sage 2.0
22230.doc	smoeroota.top - GET /read.php?f=0.dat	C:\Users\[username]\AppData\Local\Temp\Roaming.exe	Sage 2.0
8970.doc	cocalolo.top - GET /search.php	C:\Users\[username]\AppData\Local\Temp\Roaming.exe	Cerber
20703.doc	smoeroota.top - GET /read.php?f=0.dat	C:\Users\[username]\AppData\Local\Temp\Roaming.EXE	Sage 2.0
26922.doc	truepokemonant.top - GET /search.php	C:\Users\[username]\AppData\Local\Temp\Roaming.eXe	Cerber
25862.doc	newfoodas.top - GET /read.php?f=0.dat	C:\Users\[username]\AppData\Local\Temp\Roaming.exe	Sage 2.0

Shown above: Data from a spreadsheet tracking the malspam (3 of 3), mostly Sage 2.0.

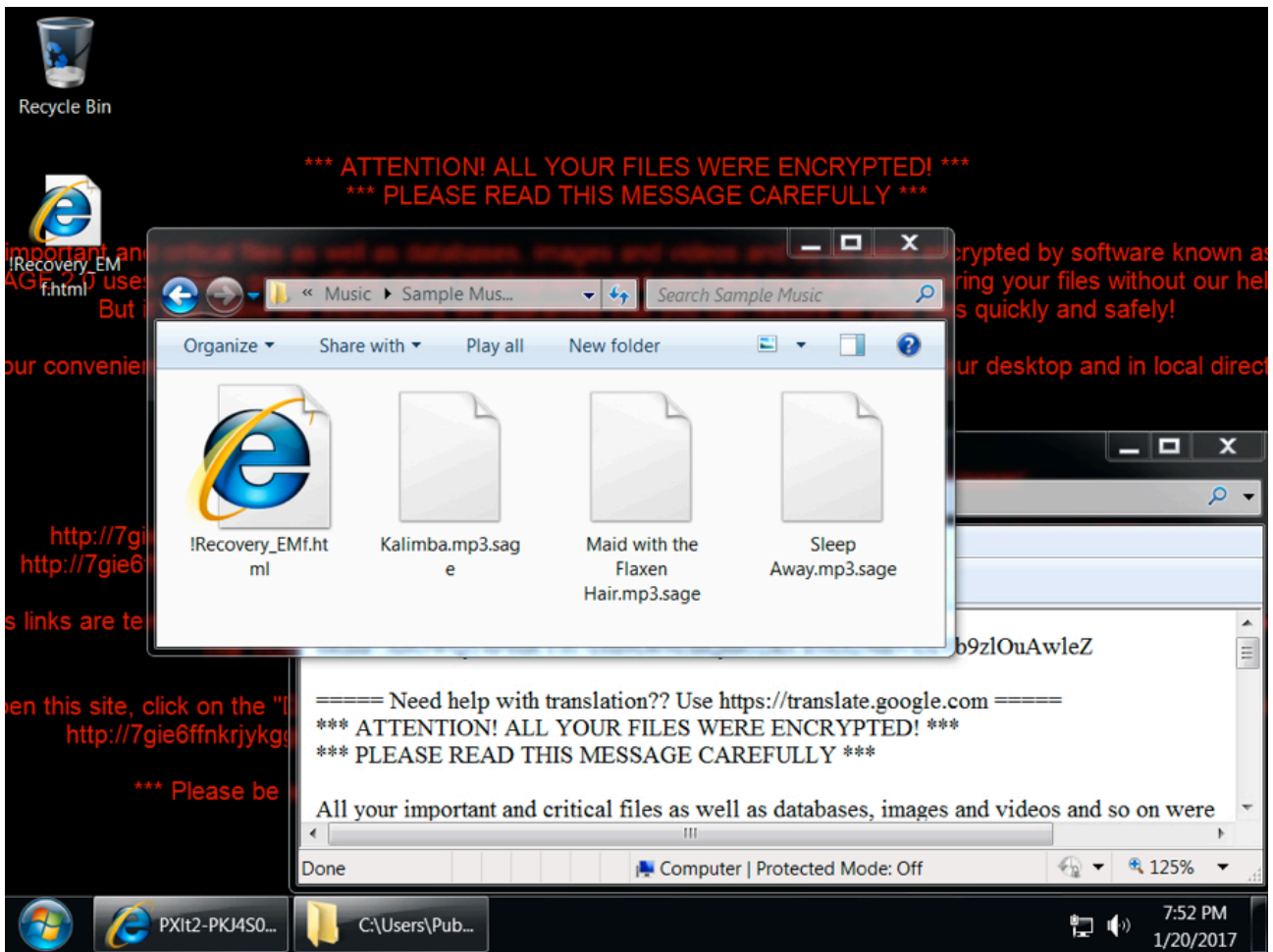
The infected host

Under default settings, an infected Windows 7 host will present a UAC window before Sage continues any further. It keeps appearing until you click yes.



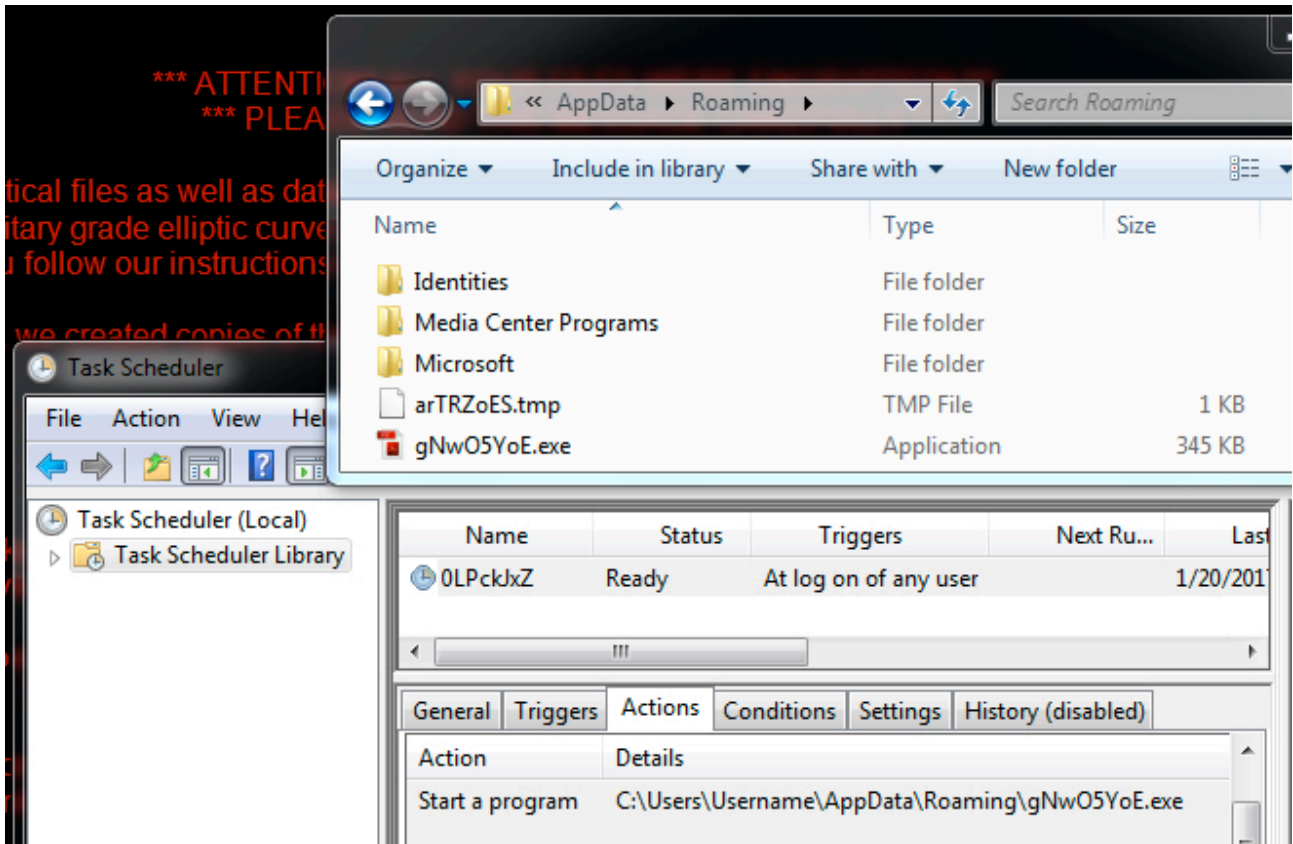
Shown above: UAC pop-up caused by Sage.

The infected Windows host has an image of the decryption instructions as the desktop background. There's also an HTML file with the same instructions dropped to the desktop. The same HTML file is also dropped to any directory with encrypted files. ".sage" is the suffix for all encrypted files.



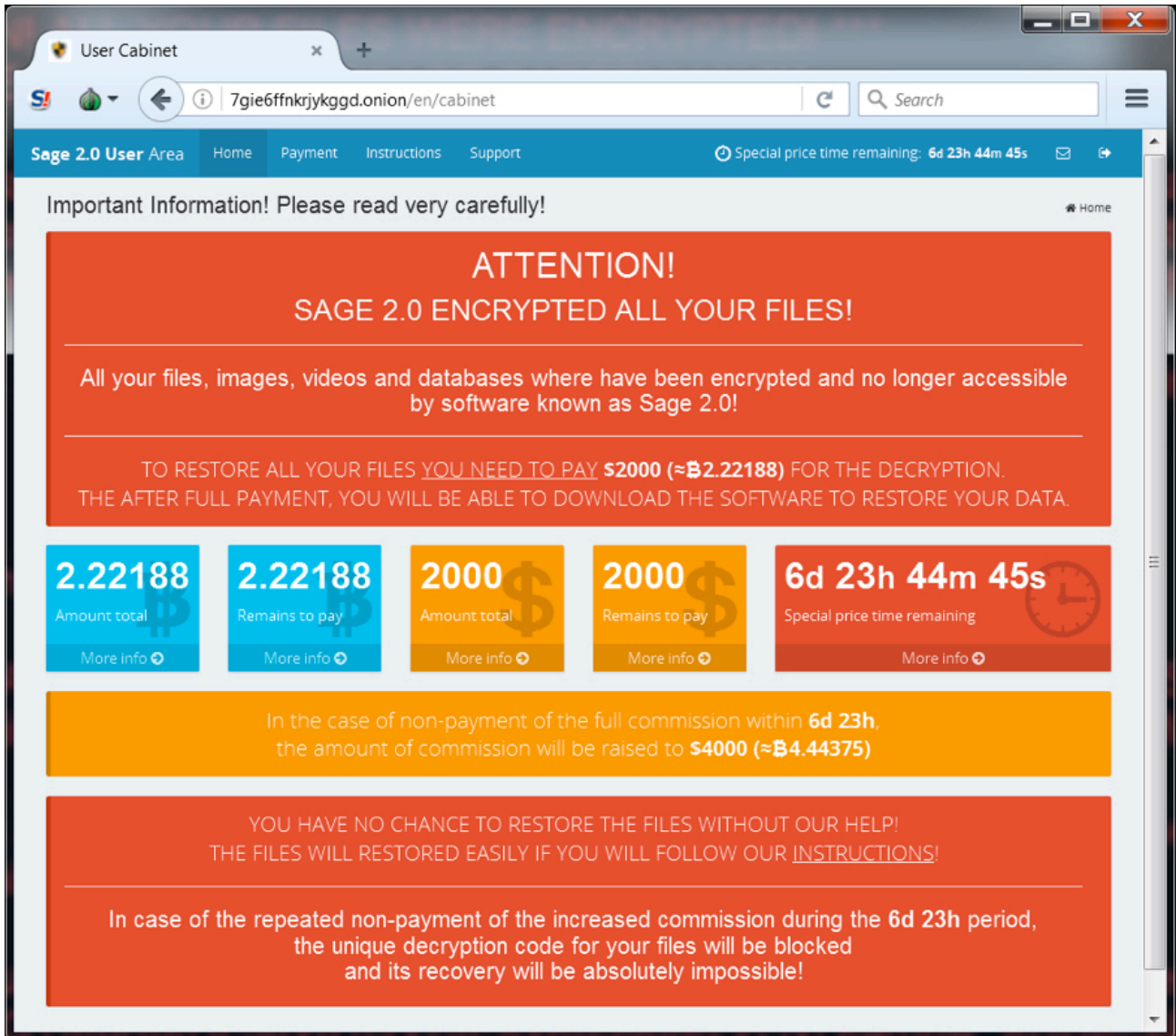
Shown above: Desktop of an infected Windows host.

Sage ransomware is kept persistent by a scheduled task, and it's stored as an executable in the user's **AppData\Roaming** directory.



Shown above: Sage ransomware and it's scheduled task for persistence.

Following the decryption instructions should take you to a Tor-based domain with a decryptor screen. On Friday, the cost to decrypt the files was \$2,000 US dollars (or 2.22188 bitcoin).



Shown above: The Sage 2.0 decryptor.

Sage 2.0 traffic

Sage ransomware generates post-infection traffic. In the image below, an initial HTTP GET request to **smoeroota.top** was caused by a .js file retrieving the ransomware. The remaining HTTP POST requests are callback traffic generated by Sage 2.0 from the infected Windows host.

Date/Time	Dst	port	Host	Info
2017-01-20 21:10:29	54.165.109.229	80	smoeroota.top	GET /read.php?f=0.dat HTTP/1.1
2017-01-20 21:10:38	66.23.246.239	80	mbfce24rgn65bx3g.er29sl.in	POST / HTTP/1.1
2017-01-20 21:10:45	54.146.39.22	80	mbfce24rgn65bx3g.er29sl.in	POST / HTTP/1.1
2017-01-20 21:11:03	66.23.246.239	80	mbfce24rgn65bx3g.er29sl.in	POST / HTTP/1.1
2017-01-20 21:11:05	66.23.246.239	80	mbfce24rgn65bx3g.er29sl.in	POST / HTTP/1.1
2017-01-20 21:11:17	54.146.39.22	80	mbfce24rgn65bx3g.er29sl.in	POST / HTTP/1.1
2017-01-20 21:12:18	66.23.246.239	80	mbfce24rgn65bx3g.er29sl.in	POST / HTTP/1.1

Shown above: Screenshot of the infection traffic, filtered in Wireshark.

```

POST / HTTP/1.1
Host: mbfce24rgn65bx3g.er29sl.in
Content-Length: 162
Connection: close

...j
....Zu.....A z_\j.j....G.nlr._0.....
...,j.c..B..eR.E.3.....]...
..4.7..x.j.'o3*.\...H...
.J...ECZ5o..... .b.....c.;.B....]8.yqJ.B&....Z..R.4.m[a.LK.P_E
.HTTP/1.1 200 OK
Server: nginx
Date: Fri, 20 Jan 2017 21:10:57 GMT
Content-Length: 1
Connection: close

k|
    
```

Shown above: TCP stream of an HTTP request for the post-infection traffic.

When the callback domains for Sage didn't resolve in DNS, the infected host sent UDP packets sent to over 7,000 IP addresses. I think this could be UDP-based peer-to-peer (P2P) traffic, and it appears to be somehow encoded or encrypted. BleepingComputer's September 2016 write-up on CryLocker shows the same type of UDP post-infection traffic, but CryLocker's traffic was not encrypted [4].

Date/Time	Dst	port	Host	Info
2017-01-20 18:13:09	84.200.34.99	80	fortycooola.top	GET /user.php?f=0.dat HTTP/1.1
2017-01-20 18:13:12	10.1.20.1	53		Standard query 0xcd6 A mbfce24rgn65bx3g.er29sl.in
2017-01-20 18:13:13	10.1.20.1	53		Standard query 0xcd6 A mbfce24rgn65bx3g.er29sl.in
2017-01-20 18:13:14	10.1.20.1	53		Standard query 0xcd6 A mbfce24rgn65bx3g.er29sl.in
2017-01-20 18:13:17	10.1.20.1	53		Standard query 0xcd6 A mbfce24rgn65bx3g.er29sl.in
2017-01-20 18:13:21	10.1.20.1	53		Standard query 0xcd6 A mbfce24rgn65bx3g.er29sl.in
2017-01-20 18:13:25	10.1.20.1	53		Standard query 0x12a5 A mbfce24rgn65bx3g.er29sl.in
2017-01-20 18:13:26	10.1.20.1	53		Standard query 0x12a5 A mbfce24rgn65bx3g.er29sl.in
2017-01-20 18:13:27	10.1.20.1	53		Standard query 0x12a5 A mbfce24rgn65bx3g.er29sl.in
2017-01-20 18:13:29	10.1.20.1	53		Standard query 0x12a5 A mbfce24rgn65bx3g.er29sl.in
2017-01-20 18:13:33	10.1.20.1	53		Standard query 0x12a5 A mbfce24rgn65bx3g.er29sl.in
2017-01-20 18:13:36	10.1.20.101	54171		Standard query response 0x12a5 No such name
2017-01-20 18:13:36	10.1.20.101	65523		Standard query response 0xcd6 No such name
2017-01-20 18:13:36	10.1.20.101	65523		Standard query response 0xcd6 No such name
2017-01-20 18:13:36	10.1.20.101	65523		Standard query response 0xcd6 No such name
2017-01-20 18:13:36	10.1.20.1	53		Standard query 0xf48d A mbfce24rgn65bx3g.rzunt3u2.com
2017-01-20 18:13:36	10.1.20.101	54171		Standard query response 0x12a5 No such name
2017-01-20 18:13:36	10.1.20.101	65523		Standard query response 0xcd6 No such name

Shown above: An HTTP request for the Sage 2.0 binary, followed by callback domains not resolving in DNS.

Filter: **udp and !(dns)** Expression... Clear Apply Save Filter

Date/Time	Dst	port	Info
2017-01-20 18:14:11	211.114.4.45	13655	Source port: 51646 Destination port: 13655
2017-01-20 18:14:11	138.197.53.223	13655	Source port: 51646 Destination port: 13655
2017-01-20 18:14:11	211.114.186.119	13655	Source port: 51646 Destination port: 13655
2017-01-20 18:14:11	211.114.35.219	13655	Source port: 51646 Destination port: 13655
2017-01-20 18:14:11	211.114.128.4	13655	Source port: 51646 Destination port: 13655
2017-01-20 18:14:11	5.45.86.15	13655	Source port: 51646 Destination port: 13655
2017-01-20 18:14:11	5.45.111.91	13655	Source port: 51646 Destination port: 13655
2017-01-20 18:14:11	138.197.92.93	13655	Source port: 51646 Destination port: 13655
2017-01-20 18:14:11	5.45.173.171	13655	Source port: 51646 Destination port: 13655
2017-01-20 18:14:11	138.197.50.41	13655	Source port: 51646 Destination port: 13655
2017-01-20 18:14:11	5.45.27.108	13655	Source port: 51646 Destination port: 13655
2017-01-20 18:14:11	211.114.88.146	13655	Source port: 51646 Destination port: 13655

Shown above: UDP traffic caused by Sage 2.0 when callback domains were unavailable.

2017-01-20 18:14:11	211.114.4.45	13655	Source port: 51646 Destination port: 13655
2017-01-20 18:14:11	138.197.53.223	13655	Source port: 51646 Destination port: 13655
2017-01-20 18:14:11	211.114.186.119	13655	Source port: 51646 Destination port: 13655
2017-01-20 18:14:11	211.114.35.219	13655	Source port: 51646 Destination port: 13655

```

+ Frame 391: 204 bytes on wire (1632 bits), 204 bytes captured (1632 bits)
+ Ethernet II, Src: Hewlett-_1c:47:ae (00:08:02:1c:47:ae), Dst: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1)
+ Internet Protocol Version 4, Src: 10.1.20.101 (10.1.20.101), Dst: 211.114.4.45 (211.114.4.45)
+ User Datagram Protocol, Src Port: 51646 (51646), Dst Port: 13655 (13655)
- Data (162 bytes)
  Data: 04c88dfa51a881cbd01926c2892671da8c21403cc8204d8b...
  [Length: 162]
  .....
```

```

0000 20 e5 2a b6 93 f1 00 08 02 1c 47 ae 08 00 45 00  .*..... ..G...E.
0010 00 be 00 c0 00 00 80 11 43 6a 0a 01 14 65 d3 72  ....Cj...e.r
0020 04 2d c9 be 35 57 00 aa b4 3c 04 c8 8d fa 51 a8  ...5W.. .<...Q.
0030 81 cb d0 19 26 c2 89 26 71 da 8c 21 40 3c c8 20  ...&..& q..!@<.
0040 4d 8b c1 6b d1 84 9e 0d 47 31 e8 d6 c5 88 09 3e  M.k.... G1.....>
0050 88 b7 28 81 1e a4 f4 81 c4 54 76 ab 4b 79 10 32  ..(..... .Tv.Ky.2
0060 b4 22 1b f8 f3 f1 5f f4 47 0f 36 de df cd 23 af  ."..... G.6...#.
0070 5c d4 aa 07 cd f2 2c 29 9e 47 c5 1a 68 30 58 6e  \.....) .G..h0Xn
0080 33 3a 8f 72 6d 50 a2 fd 70 36 69 65 7c cc 3f d4  3:.rMP.. p6ie|?.
0090 22 a8 dc 97 fa 42 93 bf b0 15 24 9f 33 c9 35 f2  "...B.. ..$.3.5.
00a0 d1 0a ec 37 49 6c 64 ed e6 7c b8 e0 a3 97 84 bb  ...7Ild. .|.....
00b0 87 a7 71 e9 16 10 54 15 22 21 ee f2 4b 2b 76 7b  ..q...T. "!...K+v{
00c0 90 be 81 ab f8 f6 2c 64 9c 9f 52 db  ....,d ..R.
```

Shown above: Examining one of the UDP packets.

Indicators of Compromise (IOCs)

Below are IOCs for Sage 2.0 from Friday 2017-01-20:

Ransomware downloads caused by Word document macros or .js files:

- 54.165.109.229 port 80 - **smoeroota.top** - GET /read.php?f=0.dat
- 54.165.109.229 port 80 - **newfoodas.top** - GET /read.php?f=0.dat

- 84.200.34.99 port 80 - **fortycooola.top** - GET /user.php?f=0.dat

Post-infection traffic:

- 54.146.39.22 port 80 - **mbfce24rgn65bx3g.er29sl.in** - POST /
- 66.23.246.239 port 80 - **mbfce24rgn65bx3g.er29sl.in** - POST /
- **mbfce24rgn65bx3g.rzunt3u2.com** (DNS queries did not resolve)
- Various IP addresses, UDP port 13655 - possible P2P traffic

Tor-based domains to view the decryption instructions:

- **7gie6ffnrjykggd.rzunt3u2.com**
- **7gie6ffnrjykggd.er29sl.in**
- **7gie6ffnrjykggd.onion**

SHA256 hashes for the Sage 2.0 ransomware samples:

- 0ecf3617c1d3313fdb41729c95215c4d2575b4b11666c1e9341f149d02405c05 (352,328 bytes)
- 362baeb80b854c201c4e7a1cfd3332fd58201e845f6aeb7def05ff0e00bf339 (352,328 bytes)
- 3b4e0460d4a5d876e7e64bb706f7fdbbc6934e2dea7fa06e34ce01de8b78934c (352,328 bytes)
- 8a0a191d055b4b4dd15c66bfb9df223b384abb75d4bb438594231788fb556bc2 (352,328 bytes)
- ccd6a495dfb2c5e26cd65e34c9569615428801e01fd89ead8d5ce1e70c680850 (352,328 bytes)

Examples of locations on the infected Windows host where Sage 2.0 was made persistent:

- C:\Users\[username]\AppData\Roaming\gNwO5YoE.exe
- C:\Users\[username]\AppData\Roaming\wiqpNWm7.exe
- NOTE: File names appear to consists 8 random alphabetic characters with an .exe suffix.

Final words

An important note: URLs for the ransomware download will send Cerber one day, but the same URLs can send something like Sage ransomware the next.

I'm not sure how widely-distributed Sage ransomware is. I've only seen it from this one malspam campaign, and I've only seen it one day so far. I'm also not sure how effective this particular campaign is. It seems these emails can easily be blocked, so few end users may have actually seen Sage 2.0.

Still, Sage is another name in the wide variety of existing ransomware families. This illustrates how profitable ransomware remains for cyber criminals.

Pcaps, emails, malware, and artifacts for this diary are available [here](#).

Brad Duncan

brad [at] malware-traffic-analysis.net

References:

- [1] <https://www.bleepingcomputer.com/forums/t/634978/sage-file-sample-extension-sage/>
- [2] <https://www.bleepingcomputer.com/forums/t/634747/sage-ransomware-sage-support-help-topic/>
- [3] <https://www.pcrisk.com/removal-guides/10732-sage-ransomware>
- [4] <https://www.bleepingcomputer.com/news/security/the-crylocker-ransomware-communicates-using-udp-and-stores-data-on-imgur-com/>

Source: <https://isc.sans.edu/forums/diary/Sage+20+Ransomware/21959/>