Malware-Traffic-Analysis.net - 2017-10-13 - Blank Slate campaign stops pushing Locky ransomware, starts pushing Sage 2.2 ransomware

NOTICE:

- The zip archives on this page have been updated, and they now use the new password scheme. For the new password, see the "about" page of this website.

ASSOCIATED FILES:

- 2017-10-13-Blank-Slate-campaign-pushes-Sage-2.2-ransomware.pcap.zip 1.6 MB (1,592,055 bytes)
- 2017-10-13-Blank-Slate-malspam-tracker.csv.zip 1.4 kB (1,390 bytes)
- 2017-10-13-email-and-malware-from-Blank-Slate-campaign-and-Sage-ransomware.zip 4.6 MB (4,600,704 bytes)

SOME BACKGROUND:

- 2017-03-02 - Palo Alto Networks Unit 42 Blog: "Blank Slate" Campaign Takes Advantage of Hosting Providers to Spread Ransomware.
- 2017-03-22 - Internet Storm Center (ISC): "Blank Slate" malspam still pushing Cerber ransomware.
- 2017-06-29 - ISC: Catching up with Blank Slate: a malspam campaign still going strong.
- 2017-07-31 - Bleeping Computer: Crypt GlobeImposter Ransomware Distributed via Blank Slate Malspam.
- 2017-08-02 - Malware-Traffic-Analysis.net: "Blank Slate" malspam pushing Gryphon ransomware (a BTCware variant).
- 2017-09-11 - Malware-Traffic-Analysis.net: Blank Slate malspam pushes "Lukitus" variant Locky ransomware.
- 2017-10-04 - Malware-Traffic-Analysis.net: Blank Slate malspam pushes "ykcol" variant Locky ransomware.

INTRODUCTION

Attachments from Blank Slate malspam have been pushing the ".asasin" variant of Locky ransomware, since that variant first appeared on Tuesday 2017-10-10. However, sometime on Friday 2017-10-13, Blank Slate malspam stopped pushing Locky. The most recent Locky I found from Blank Slate is SHA256 hash **51c73af1811c47fca69ea1de7d794d07090b4c892632529ea86ea9cee73779ce** originally submitted to VirusTotal on 2017-10-13 at 09:57 UTC.

Since then, Blank Slate has been pushing Sage 2.2 ransomware. The 2.2 version has been around for months now.

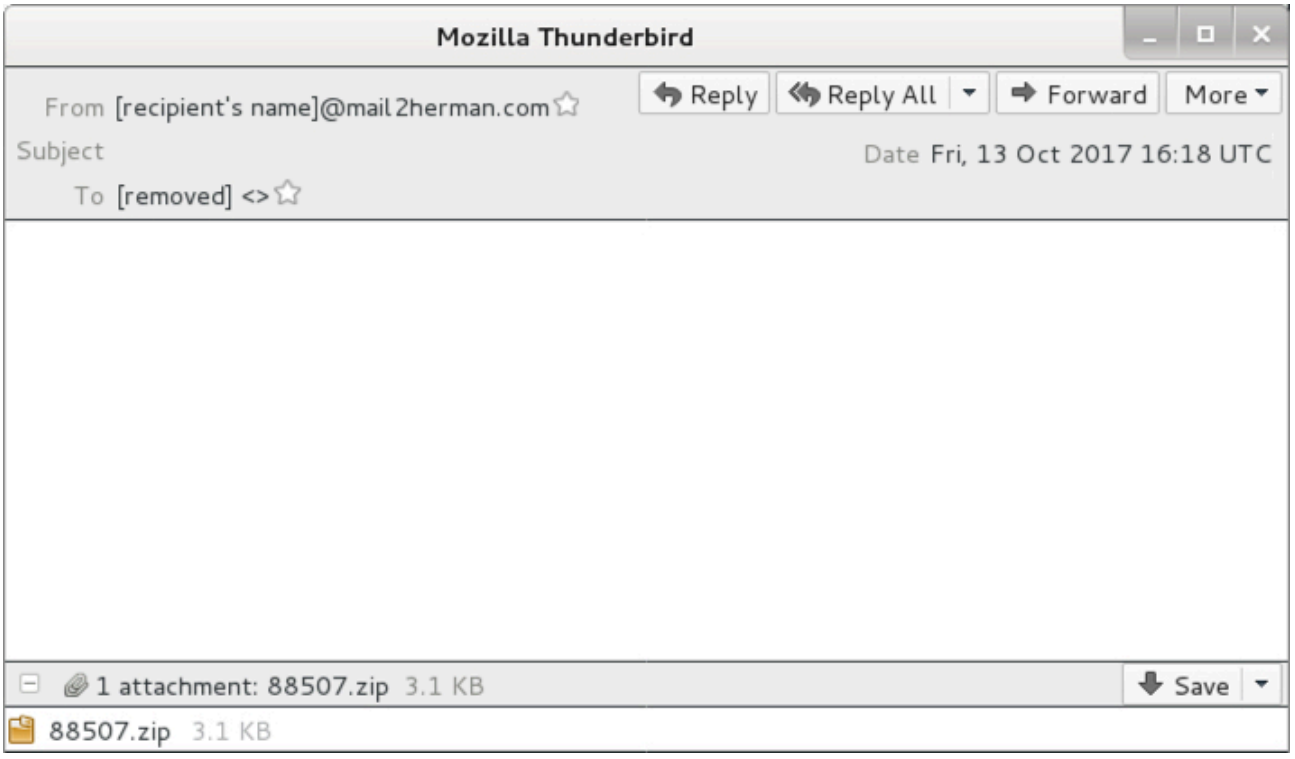
ADDITIONAL NOTES:

- Thanks to @unixronin who tipped me off to the changes today (link to Twitter thread).
- The HTA file with the decryption instructions states this is Sage 2.2, while the decryptor page states Sage 2.0. Despite the decryptor page, this appears to be Sage 2.2.

EMAILS

Date/Time	Sending host name and IP address	Sending email address (spoofed)	Subject	Attachment name
2017-10-13 00:01 UTC	hinet.net ([36.225.76.85])	chazy@baby200.wanadoo.co.uk	(none)	208221626.zip
2017-10-13 02:12 UTC	nsg-static-90.173.75.182-airtel.com ([182.75.173.90])	gangster911@bigmir.net	(none)	144294.zip
2017-10-13 02:34 UTC	[recpient's email domain] ([117.90.210.16])	atie121609@gmail.com	(none)	8686927439.zip
2017-10-13 03:43 UTC	hinet.net ([36.233.174.214])	daberle@abm.com	(none)	5637406077862.zip
2017-10-13 05:07 UTC	[recpient's email domain] ([220.80.5.237])	blackmailergp500@sheinlaw.com	(none)	84519555680060.zip
2017-10-13 06:10 UTC	[recpient's email domain] ([220.80.5.237])	[recipient's name]@mail2travis.com	(none)	198946214360482.zip
2017-10-13 06:20 UTC	hinet.net ([1.171.78.211])	ppp_productions@drillmec.com	(none)	35665301.zip
2017-10-13 06:46 UTC	hinet.net ([111.253.50.230])	x81@84.8m	(none)	119110093.zip
2017-10-13 06:58 UTC	fixed-187-189-99-40.totalplay.net ([187.189.99.40])	ffffjxs@rciap.com	(none)	3211643664315.zip
2017-10-13 06:59 UTC	[recpient's email domain] ([219.233.18.242])	[recipient's name]@hii.net	(none)	985635388572802.zip
2017-10-13 08:13 UTC	[recpient's email domain] ([197.248.210.10])	gracedsenoglu@gmail.com	(none)	13552145.doc
2017-10-13 08:28 UTC	vnpt.vn ([113.161.95.240])	sueli@sgmturismo.com.br	(none)	9422241891502.doc
2017-10-13 08:54 UTC	host-75-107-139-37.sevstar.net ([37.139.107.75])	mary.a.hopkins@nasa.gov	(none)	6053275.doc
2017-10-13 09:05 UTC	optimaxbd.net ([103.245.97.98])	roger.dhondt41@telenet.be	(none)	00256228970790.zip
2017-10-13 09:35 UTC	[recpient's email domain] ([116.96.85.128])	x9azfcyjd@163.com	(none)	6923637232.zip
2017-10-13 10:14 UTC	[recpient's email domain] ([27.96.87.219])	lofotseminaret@europharma.no	(none)	30652568754119.zip
2017-10-13 11:42 UTC	[recpient's email domain] ([103.87.168.152])	mathias.heinrich@web.de	(none)	915034748342236.zip
2017-10-13 11:56 UTC	hinet.net ([114.43.80.74])	fotoportret@poczta.fm	(none)	8535688411.zip
2017-10-13 12:33 UTC	[recpient's email domain] ([171.229.238.210])	ole.jorgen.etholm@arendal.kommune.no	(none)	10915849.zip
2017-10-13 15:16 UTC	cableworld.es ([89.29.171.152])	jtrois57@orange.fr	(none)	591790149701.zip
2017-10-13 15:20 UTC	[recpient's email domain] ([160.226.32.246])	br.camus@free.fr	(none)	003154376010488.zip
2017-10-13 16:18 UTC	speedy.com.ar ([181.21.50.222])	[recipient's name]@mail2herman.com	(none)	88507.zip
2017-10-13 17:30 UTC	singnet.com.sg ([219.74.128.74])	studentassistance@oregonstate.edu	(none)	402663106880419.zip

Shown above: Screenshot from the spreadsheet tacker. Some have .zip attachments, while other have .doc attachments.



Shown above: Screen shot from one of the emails.

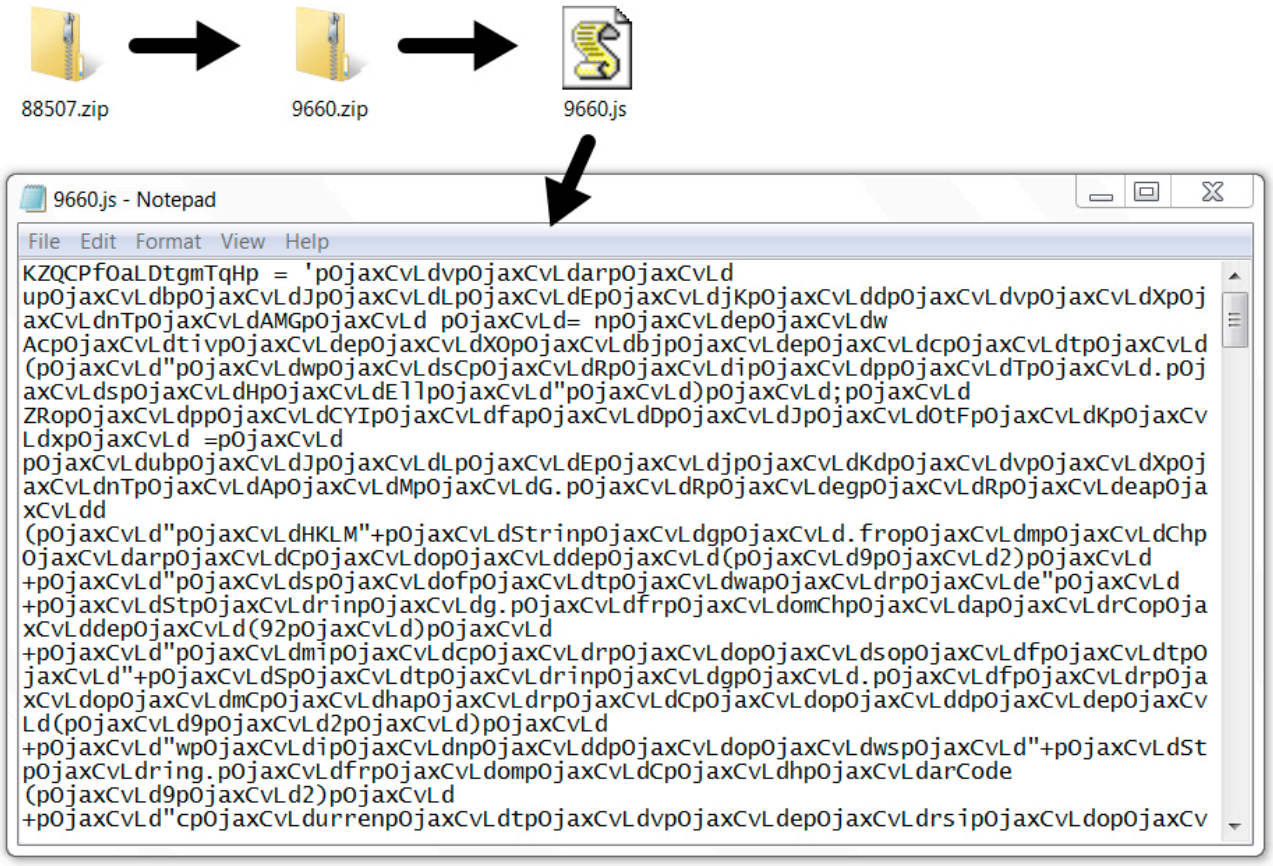
EMAILS NOTED:

- 2017-10-13 00:01 UTC -- From (spoofed): chazy@baby200.wanadoo[.]co[.]uk -- Attachment name: 208221626.zip
- 2017-10-13 02:12 UTC -- From (spoofed): gangster911@bigmir[.]net -- Attachment name: 144294.zip
- 2017-10-13 02:34 UTC -- From (spoofed): atie121609@gmail[.]com -- Attachment name: 8686927439.zip
- 2017-10-13 03:43 UTC -- From (spoofed): daberle@abm[.]com -- Attachment name: 5637406077862.zip
- 2017-10-13 05:07 UTC -- From (spoofed): blackmailergp500@sheinlaw[.]com -- Attachment name: 84519555680060.zip
- 2017-10-13 06:10 UTC -- From (spoofed): [recipient's name]@mail2travis[.]com -- Attachment name: 198946214360482.zip
- 2017-10-13 06:20 UTC -- From (spoofed): ppp_productions@drillmec[.]com -- Attachment name: 35665301.zip
- 2017-10-13 06:46 UTC -- From (spoofed): x81@84[.]8m -- Attachment name: 119110093.zip
- 2017-10-13 06:58 UTC -- From (spoofed): ffffjxs@rciap[.]com -- Attachment name: 3211643664315.zip
- 2017-10-13 06:59 UTC -- From (spoofed): [recipient's name]@hii[.]net -- Attachment name: 985635388572802.zip
- 2017-10-13 08:13 UTC -- From (spoofed): gracedsenoglu@gmail[.]com -- Attachment name: ***13552145.doc***
- 2017-10-13 08:28 UTC -- From (spoofed): sueli@sgmturismo[.]com[.]br -- Attachment name: ***9422241891502.doc***
- 2017-10-13 08:54 UTC -- From (spoofed): mary.a.hopkins@nasa[.]gov -- Attachment name: ***6053275.doc***
- 2017-10-13 09:05 UTC -- From (spoofed): roger.dhondt41@telenet[.]be -- Attachment name: 00256228970790.zip
- 2017-10-13 09:35 UTC -- From (spoofed): x9azfcyjd@163[.]com -- Attachment name: 6923637232.zip
- 2017-10-13 10:14 UTC -- From (spoofed): lofotseminaret@europharma[.]no -- Attachment name: 30652568754119.zip
- 2017-10-13 11:42 UTC -- From (spoofed): mathias.heinrich@web[.]de -- Attachment name: 915034748342236.zip
- 2017-10-13 11:56 UTC -- From (spoofed): fotoportret@poczta[.]fm -- Attachment name: 8535688411.zip
- 2017-10-13 12:33 UTC -- From (spoofed): ole.jorgen.etholm@arendal.kommune[.]no -- Attachment name: 10915849.zip
- 2017-10-13 15:16 UTC -- From (spoofed): jtrois57@orange[.]fr -- Attachment name: 591790149701.zip
- 2017-10-13 15:20 UTC -- From (spoofed): br.camus@free[.]fr -- Attachment name: 003154376010488.zip

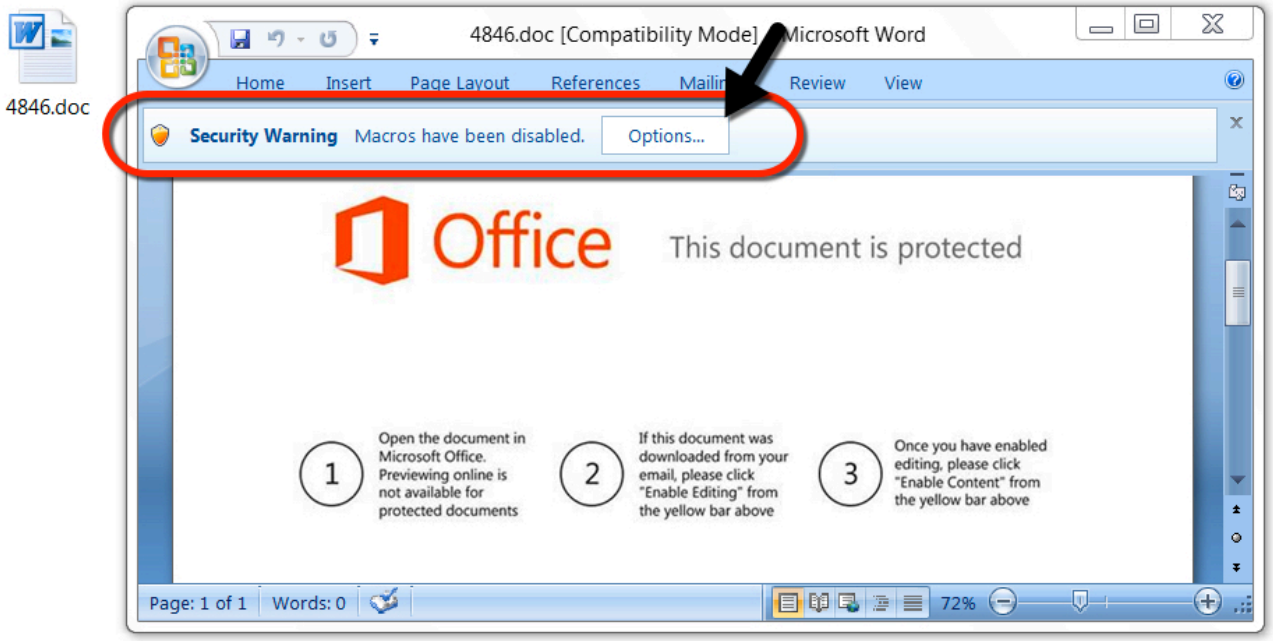
- 2017-10-13 16:18 UTC -- From (spoofed): [recipient's name]@mail2herman[.]com -- Attachment name: 88507.zip
- 2017-10-13 17:30 UTC -- From (spoofed): studentassistance@oregonstate[.]edu -- Attachment name: 402663106880419.zip

ZIP ATTACHMENT INFO:

- 88507.zip --> 9660.zip --> 9660.js
- 67214604.zip --> 29219.zip --> 29219.js
- 92181052.zip --> 29459.zip --> 29459.js
- 31084472583.zip --> 940.zip --> 940.js
- 525463435470.zip --> 28588.zip --> 28588.js
- 599450048391.zip --> 22032.zip --> 22032.js
- 58843249449955.zip --> 3832.zip --> 3832.js
- 004765275711512.zip --> 3902.zip --> 3902.js

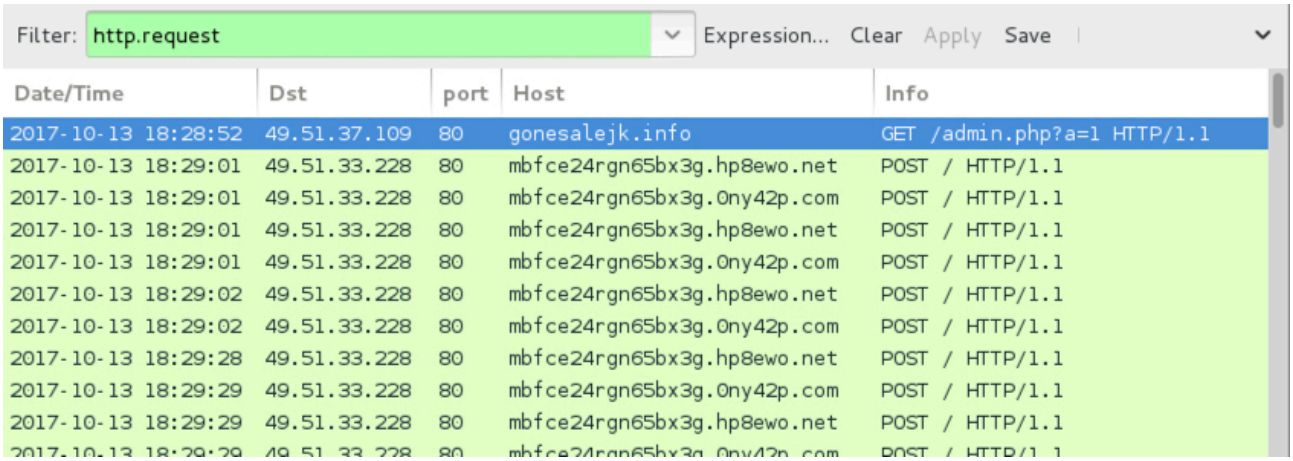


Shown above: If the attachment is a zip archive, it contains another zip archive with a malicious JavaScript (.js) file inside.



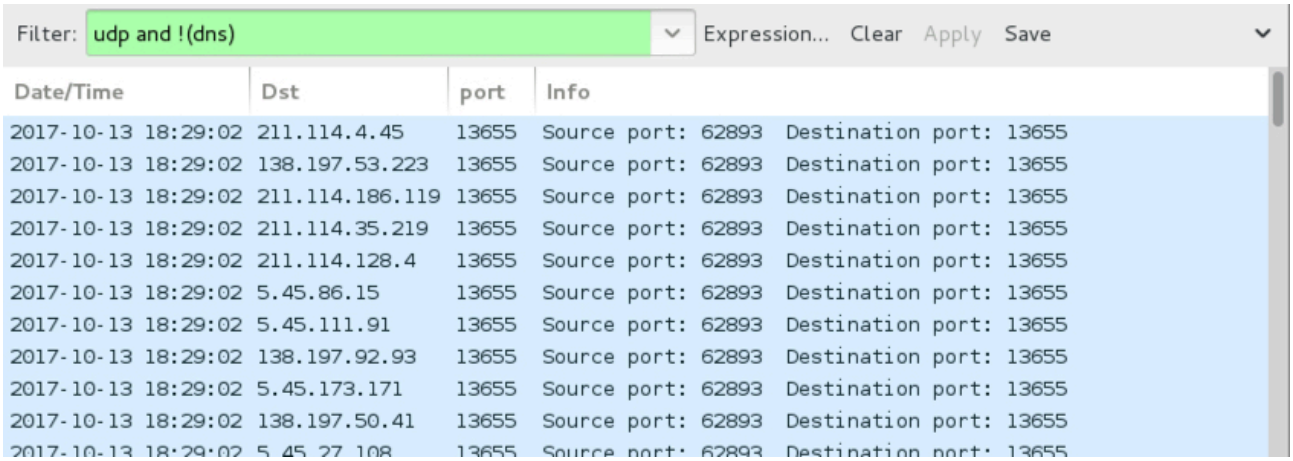
Shown above: If the attachment is a Word document, it has malcious macros.

TRAFFIC



Date/Time	Dst	port	Host	Info
2017-10-13 18:28:52	49.51.37.109	80	gonesalejk.info	GET /admin.php?a=1 HTTP/1.1
2017-10-13 18:29:01	49.51.33.228	80	mbfce24rgn65bx3g.hp8ewo.net	POST / HTTP/1.1
2017-10-13 18:29:01	49.51.33.228	80	mbfce24rgn65bx3g.0ny42p.com	POST / HTTP/1.1
2017-10-13 18:29:01	49.51.33.228	80	mbfce24rgn65bx3g.hp8ewo.net	POST / HTTP/1.1
2017-10-13 18:29:01	49.51.33.228	80	mbfce24rgn65bx3g.0ny42p.com	POST / HTTP/1.1
2017-10-13 18:29:02	49.51.33.228	80	mbfce24rgn65bx3g.hp8ewo.net	POST / HTTP/1.1
2017-10-13 18:29:02	49.51.33.228	80	mbfce24rgn65bx3g.0ny42p.com	POST / HTTP/1.1
2017-10-13 18:29:28	49.51.33.228	80	mbfce24rgn65bx3g.hp8ewo.net	POST / HTTP/1.1
2017-10-13 18:29:29	49.51.33.228	80	mbfce24rgn65bx3g.0ny42p.com	POST / HTTP/1.1
2017-10-13 18:29:29	49.51.33.228	80	mbfce24rgn65bx3g.hp8ewo.net	POST / HTTP/1.1

Shown above: HTTP traffic from an infection filtered in Wireshark.



Date/Time	Dst	port	Info
2017-10-13 18:29:02	211.114.4.45	13655	Source port: 62893 Destination port: 13655
2017-10-13 18:29:02	138.197.53.223	13655	Source port: 62893 Destination port: 13655
2017-10-13 18:29:02	211.114.186.119	13655	Source port: 62893 Destination port: 13655
2017-10-13 18:29:02	211.114.35.219	13655	Source port: 62893 Destination port: 13655
2017-10-13 18:29:02	211.114.128.4	13655	Source port: 62893 Destination port: 13655
2017-10-13 18:29:02	5.45.86.15	13655	Source port: 62893 Destination port: 13655
2017-10-13 18:29:02	5.45.111.91	13655	Source port: 62893 Destination port: 13655
2017-10-13 18:29:02	138.197.92.93	13655	Source port: 62893 Destination port: 13655
2017-10-13 18:29:02	5.45.173.171	13655	Source port: 62893 Destination port: 13655
2017-10-13 18:29:02	138.197.50.41	13655	Source port: 62893 Destination port: 13655

Shown above: UDP traffic from an infection filtered in Wireshark.

TRAFFIC GENERATED BY .JS/.DOC FILES TO DOWNLOAD SAGE RANSOMWARE:

- **gonesalejk[.]info** - GET /admin.php?a=1
- **johnmoplan[.]top** - GET /1.txt
- **johnmoplan[.]top** - GET /admin.php?a=1
- **jovolewnac[.]info** - GET /admin.php?a=1
- **sutranjdf[.]info** - GET /admin.php?a=2

SAGE POST-INFECTION TRAFFIC:

- 49.51.33[.]228 port 80 - **mbfce24rgn65bx3g.hp8ewo[.]net** - POST /
- 49.51.33[.]228 port 80 - **mbfce24rgn65bx3g.0ny42p[.]com** - POST /
- UDP connections to over 7,000 random-looking IP addresses over port 13655

DOMAINS FROM THE DECRYPTION INSTRUCTIONS:

- **z5dq36kjy5swjtmr.hp8ewo[.]net**
- **z5dq36kjy5swjtmr.0ny42p[.]com**
- **z5dq36kjy5swjtmr[.]onion**

ASSOCIATED FILES

ATTACHMENTS:

- b0aed0e368425dfe126491b71546ad27061a1c4346b4de51202766b4113620a7 - 4846.doc
- 55d6e3ed606acddf3c4112ffe4b4447f4bfacda9d03d187cbc2374b6048f5712 - 28255.doc
- da8db4d594370f36b93d4121897d4056cf2f36e61b55b6e8a9569e3121fad1df - 88507.zip
- 13584b8ab9b4c5cb7c89e60ca2fd46e0ce3771d50c0e9a5402415580179a13e0 - 67214604.zip
- 26ad4cf58b40b2df9ff39ab302d7bf15bbd4a7e064f614015797a13631160ee8 - 92181052.zip
- b9216e8e5201a8fc2433ce60cd379077c60c11c888edffc5d130e328ed2c7ffb - 31084472583.zip
- 12f96c81580efc35193561fd45e51abd9b742df11777a198d0df9e6800ce1c15 - 525463435470.zip
- dd18a44aa3166de08c77083dde6b0d697fde882a38a95f749a451b52c4eac4bc - 599450048391.zip
- caf07e4e2670dc3c6b824a1fdb0a0de90a00b0759e95c97e88d07f65d646769b - 58843249449955.zip
- 3528de5cdcf6529e1dd7f0e24ead27c0ae360f311e877530f98fb2ac9367c5cc - 004765275711512.zip

EXTRACTED .JS FILES:

- b1ae04485794079bc11902bcd56f4b36408fdedb18c44a55d2d919c65fab577a - 940.js
- 35abf5d73f96856c535499f04771f27103fdb1275e0e74bd4c963b9c3225e94e - 3832.js
- bab55dc85f006ae26ed5ad447089eb1be80cac75519a199d94620a01651cad13 - 3902.js
- e89ffc61e3c79115bfc3d855227405a850eb7a8fa3ac5c4bdd77389ba6945e31 - 9660.js
- aba9d22dd3573f0902a7219790915de8dbb0b07b5e25ed28c6a87b4acfaa0c39 - 22032.js
- 6bcb0a226921fc1a9e6bebd92dffd5dd528937e6bde50bbcc08fd7593e9da27c - 28588.js
- 942f64e913a1f3781adecd88e47f8da75981f69d20ce9206e3374f5331a54e0f - 29219.js
- 24fc14ae2bfa634a54cafc6b22a596ad2b85dba621388255d3e0eb6294cd03ae - 29459.js

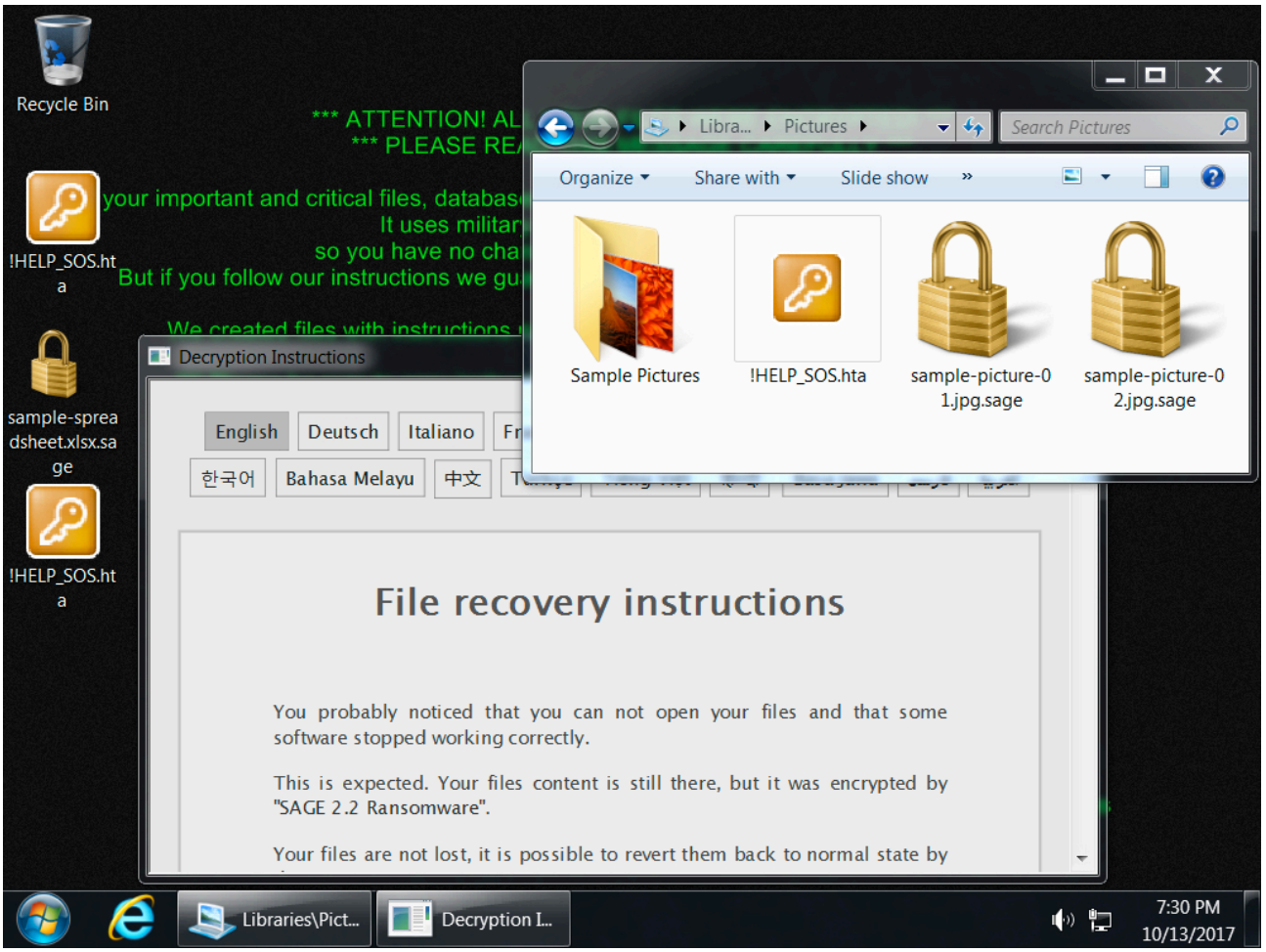
FOLLOW-UP MALWARE (SAGE 2.2 BINARIES):

- 6132c32a717ff1d5f5ff86ce0d4a27d59b332ec1f5e75f12c1346c0ab3fbda0c - 2017-10-13-Sage-ransomware-example-1-of-9.exe
- b16eea3a52ad7ffe0b18309395da9394982b6219f16e021e43ce57731d29a0ec - 2017-10-13-Sage-ransomware-example-2-of-9.exe
- 81609d5cdc5068ffd5975c1045710cecdbaa33a2eed682894322847e93c9cb21 - 2017-10-13-Sage-ransomware-example-3-of-9.exe
- cb219bf88ceeb2ecf95072576148e17e52e56e5f02876ac00a204a3bcb9352cc - 2017-10-13-Sage-ransomware-example-4-of-9.exe
- 008484650884010ac949d1041e48dd0abf4967c9ddf305a971ddfc32f9d4cfeb - 2017-10-13-Sage-ransomware-example-5-of-9.exe
- 5a99897d463f1685b83b2d017dc734ba657fe3f612a74fcba730b826fce5e44c - 2017-10-13-Sage-ransomware-example-6-of-9.exe
- 64978bc162765959aa0c3de15f4fce90041bf3bc01e668ba649eb7e686222a30 - 2017-10-13-Sage-ransomware-example-7-of-9.exe
- 046b9330d7da6619ff96ce3c94adc5f35fa2fb26cd1da7d2f57890bfde5e4f59 - 2017-10-13-Sage-ransomware-example-8-of-9.exe
- 8f1374b432fa7580397e57949b32044e89663215e71ad0252638875a61908323 - 2017-10-13-Sage-ransomware-example-9-of-9.exe

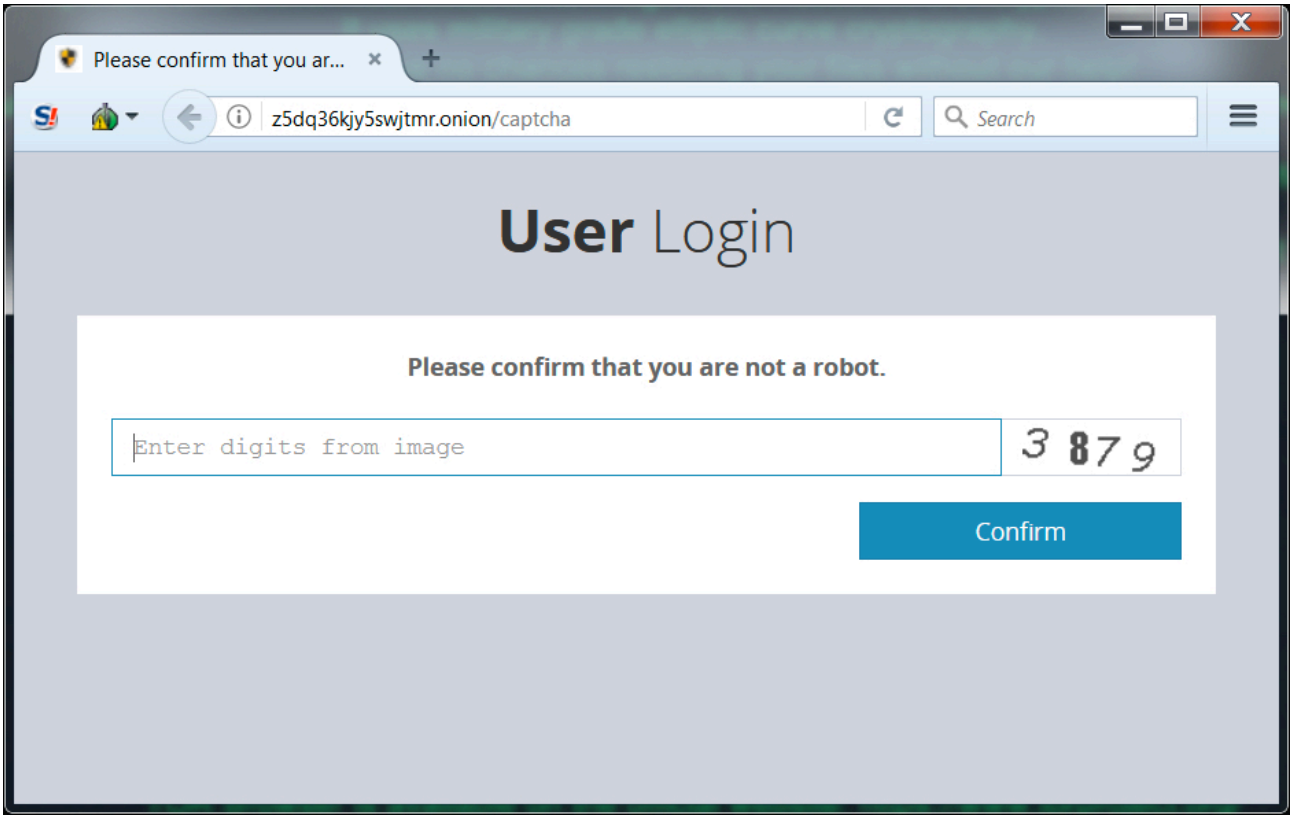
PATHS TO MALWARE:

- 4846.doc --> sutranjdf[.]info/admin.php?a=2 --> C:\Users\[username]\AppData\Local\Temp\32148.exe
- 28255.doc --> sutranjdf[.]info/admin.php?a=2 --> C:\Users\[username]\AppData\Local\Temp\4051.exe
- 940.js --> gonesalejk[.]info/admin.php?a=1 --> C:\Users\[username]\AppData\Roaming\Microsoft\Windows\Templates\417187.exe
- 3832.js --> gonesalejk[.]info/admin.php?a=1 --> C:\Users\[username]\AppData\Roaming\Microsoft\Windows\Templates\220986.exe
- 3902.js --> gonesalejk[.]info/admin.php?a=1 --> C:\Users\[username]\AppData\Roaming\Microsoft\Windows\Templates\27599.exe
- 9660.js --> gonesalejk[.]info/admin.php?a=1 --> C:\Users\[username]\AppData\Roaming\Microsoft\Windows\Templates\483882.exe
- 22032.js --> gonesalejk[.]info/admin.php?a=1 --> C:\Users\[username]\AppData\Roaming\Microsoft\Windows\Templates\636057.exe
- 28588.js --> jovolewnac[.]info/admin.php?a=1 --> C:\Users\[username]\AppData\Roaming\Microsoft\Windows\Templates\496938.exe
- 29219.js --> gonesalejk[.]info/admin.php?a=1 --> C:\Users\[username]\AppData\Roaming\Microsoft\Windows\Templates\803051.exe
- 29459.js --> johnmoplan[.]top/1.txt --> 404 not found (but johnmoplan[.]top/admin.php?a=1 works fine)

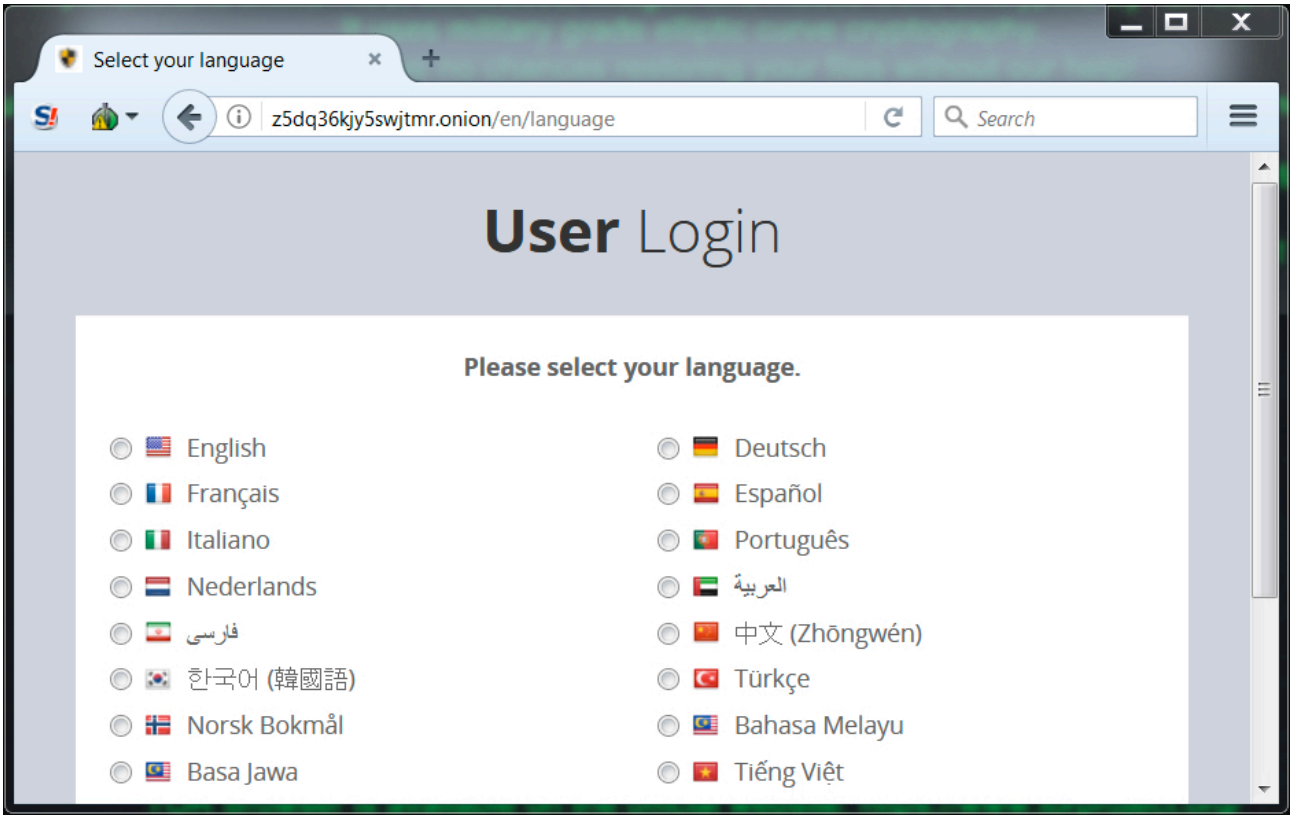
IMAGES



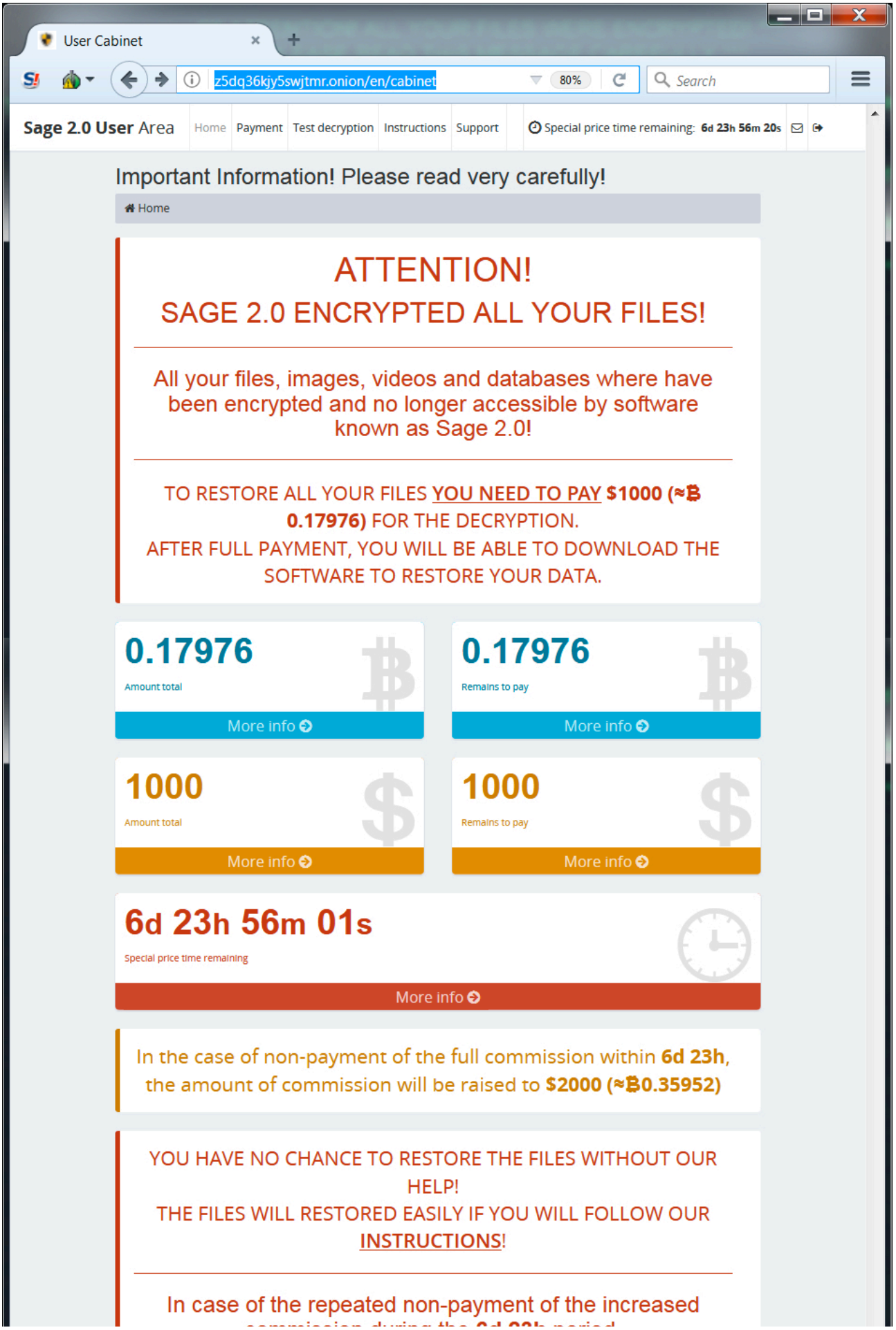
Shown above: Desktop of an infected Windows host.

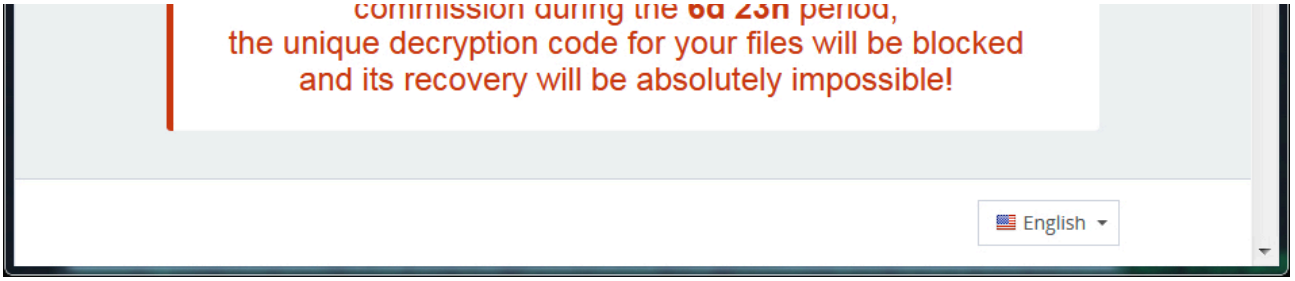


Shown above: When trying to view the decryptor, you first see a CAPTCHA screen to confirm you are not a robot.



Shown above: Selecting your language after the CAPTCHA screen.


User Cabinet
z5dq36kjy5swjtmr.onion/en/cabinet
80%
Search
Sage 2.0 User Area
Home
Payment
Test decryption
Instructions
Support
Special price time remaining: 6d 23h 56m 20s
Important Information! Please read very carefully!
Home
ATTENTION!
SAGE 2.0 ENCRYPTED ALL YOUR FILES!
All your files, images, videos and databases where have been encrypted and no longer accessible by software known as Sage 2.0!
TO RESTORE ALL YOUR FILES YOU NEED TO PAY $1000 (≈Ƀ 0.17976) FOR THE DECRYPTION.
AFTER FULL PAYMENT, YOU WILL BE ABLE TO DOWNLOAD THE SOFTWARE TO RESTORE YOUR DATA.
0.17976
Amount total
More info
0.17976
Remains to pay
More info
1000
Amount total
More info
1000
Remains to pay
More info
6d 23h 56m 01s
Special price time remaining
More info
In the case of non-payment of the full commission within 6d 23h, the amount of commission will be raised to $2000 (≈Ƀ0.35952)
YOU HAVE NO CHANCE TO RESTORE THE FILES WITHOUT OUR HELP!
THE FILES WILL RESTORED EASILY IF YOU WILL FOLLOW OUR INSTRUCTIONS!
In case of the repeated non-payment of the increased



Shown above: The Sage decryptor showing today's ransom cost.

Click here to return to the main page.
