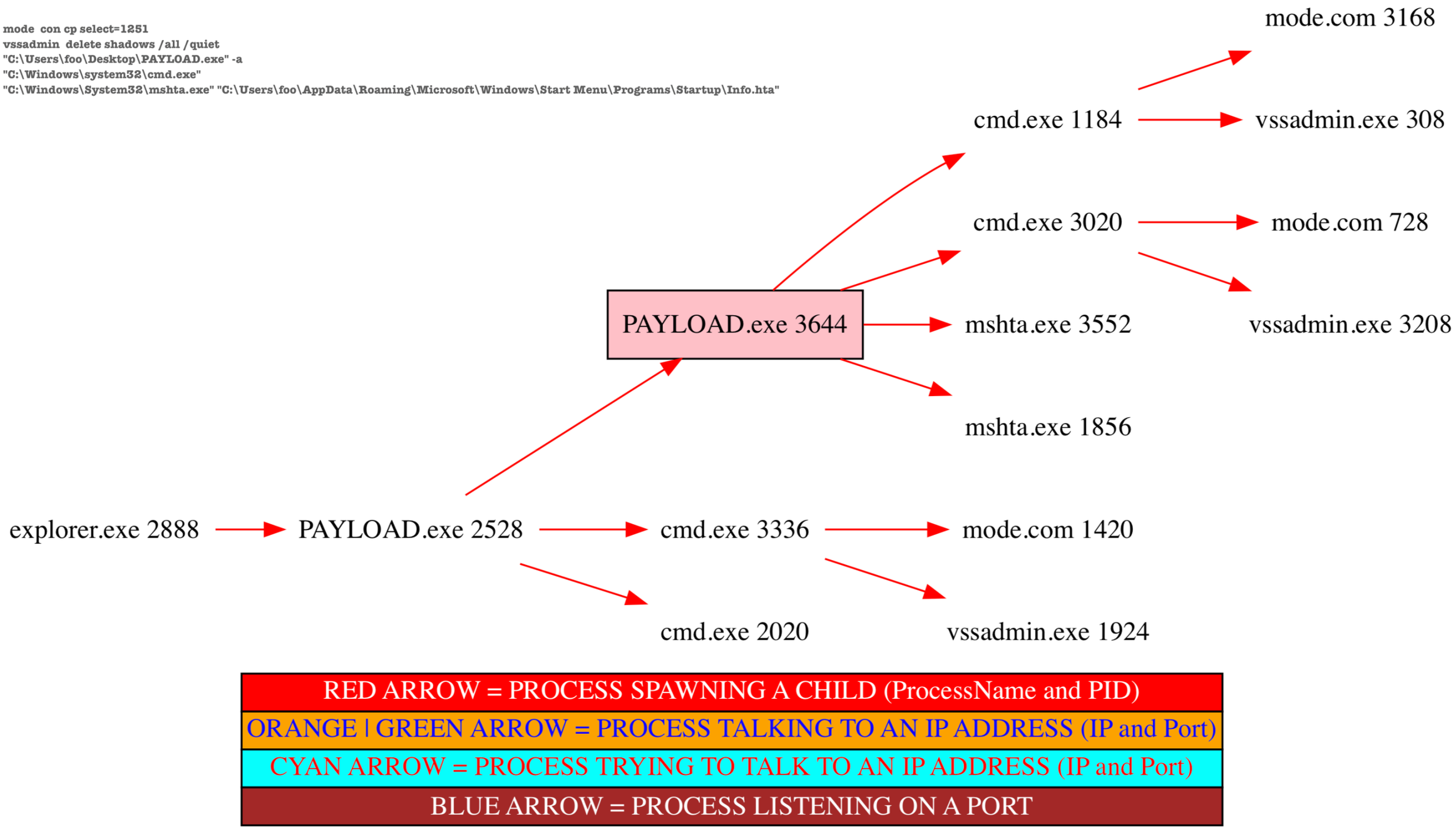
FILE_INFO

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
LINES: 250
WORDS: 1819
CHARS: 94211
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
MD5   : cb15ee1cece796a8f83015baa396fc2d
SHA256: f946b0318b6e5ce2dcdf6a4438cb4bfcfba8cdd72ff2785757edc3f1f147f172
SHA1  : aea6845399f9f89ee2aeecb44bc49cc9b99e3359
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Content Type: application/octet-stream
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
```

```
D&S: [false, false, PE, MZ]
BAS: 204
ARC: [x86]
```

DYNAMIC FLOW

```
mode  con cp select=1251
vssadmin  delete shadows /all /quiet
"C:\Users\foo\Desktop\PAYLOAD.exe" -a
"C:\Windows\system32\cmd.exe"
"C:\Windows\System32\mshta.exe" "C:\Users\foo\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Info.hta"
```



Dropped

```
[08-20-2018-09-54-54]-> F: \Users\foo\AppData\Local\VirtualStore\9XKSRibB8oDlvAU-qwMLjlfAAADvbM+CK52tC5sA4s4=.F2B655EA50AD93CEF0E7.da_vinci_code.id-E8643907.[heinonenfornoff@aol.com].combo ** 3490
[08-20-2018-09-54-54]-> F: \Users\foo\AppData\Local\VirtualStore\awpRfQ-rSorhAy2xxqKAwCSf5k4Gp6hjueLR+emyH1A=.F2B655EA50AD93CEF0E7.da_vinci_code.id-E8643907.[heinonenfornoff@aol.com].combo ** 3490
[08-20-2018-09-54-54]-> F: \Users\foo\AppData\Local\VirtualStore\BbGFoALw8B33muv3PD-mQOZVX018w0NPE4Ii6qZe35I=.F2B655EA50AD93CEF0E7.da_vinci_code.id-E8643907.[heinonenfornoff@aol.com].combo ** 3490
[08-20-2018-09-54-54]-> F: \Users\foo\AppData\Local\VirtualStore\iQXqaMAczikUUtZKR667trXI-kUGvIDRD520Q9nsDkY=.F2B655EA50AD93CEF0E7.da_vinci_code.id-E8643907.[heinonenfornoff@aol.com].combo ** 3490
[08-20-2018-09-54-54]-> F: \Users\foo\AppData\Local\VirtualStore\k-LjyRaPQz9kW3pnPjhRRPUdn9Xfg0hVZL2q1kgorbg=.F2B655EA50AD93CEF0E7.da_vinci_code.id-E8643907.[heinonenfornoff@aol.com].combo ** 3490
[08-20-2018-09-54-54]-> F: \Users\foo\AppData\Local\VirtualStore\nuIrZlvRR3jwn4oOvObr7v9ezpdlxuB5MxMSL2YOmAk=.F2B655EA50AD93CEF0E7.da_vinci_code.id-E8643907.[heinonenfornoff@aol.com].combo ** 3490
```

heinonenfornoff@aol.com

All your files have been encrypted!

All your files have been encrypted due to a security problem with your PC. If you want to restore them, write us to the e-mail heinonenfornoff@aol.com
Write this ID in the title of your message E8643907
In case of no answer in 24 hours write us to theese e-mails: peruginos@aol.com
You have to pay for decryption in Bitcoins. The price depends on how fast you write to us. After payment we will send you the decryption tool that will decrypt all your files.

Free decryption as guarantee

Before paying you can send us up to 1 file for free decryption. The total size of files must be less than 1Mb (non archived), and files should not contain valuable information. (databases,backups, large excel sheets, etc.)

How to obtain Bitcoins

The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click 'Buy bitcoins', and select the seller by payment method and price.
https://localbitcoins.com/buy_bitcoins
Also you can find other places to buy Bitcoins and beginners guide here:
http://www.coindesk.com/information/how-can-i-buy-bitcoins/

Attention!

- Do not rename encrypted files.
- Do not try to decrypt your data using third party software, it may cause permanent data loss.
- Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.

Strings{IMP}

```
RSDS%~m
C:\crysis\Release\PDB\payload.pdb
mshta.exe
CryptSIPDllIsMyFileType
CertDllVerifyRevocation
CertDllVerifyCTLUsage
CryptDllFormatObject
CertDllEnumSystemStore
CertDllOpenStoreProv
CryptCNGPKCS12GetMap
CryptCNGInitHMAC
CryptDllEncodeObject
CryptDllDecodeObject
CryptDllEncodeObjectEx
HMEN
Lmrv
Desktop
CryptDllExtractEncodedSignatureParameters
CryptDllExportPublicKeyInfoFromBCryptKeyHandle
Windows
CertDllUnregisterPhysicalStore
CertDllEnumPhysicalStore
CryptDllExportPrivateKeyInfoEx
CryptDllImportPrivateKeyInfoEx
CryptMsgDllCNGExportKeyTrans
CryptMsgDllCNGExportKeyAgree
CryptMsgDllCNGImportKeyTrans
CryptMsgDllCNGImportKeyAgree
CryptMsgDllGenEncryptKey
CryptMsgDllExportEncryptKey
CryptMsgDllImportEncryptKey
CryptMsgDllGenContentEncryptKey
CryptMsgDllExportKeyTrans
CryptMsgDllExportKeyAgree
CryptMsgDllExportMailList
CryptMsgDllImportKeyTrans
CryptMsgDllImportKeyAgree
CryptMsgDllImportMailList
Windows
System32
/C:\
Windows
System32
mshta.exe
CryptDllEncodePublicKeyAndParameters
<META HTTP-EQUIV="MSThemeCompatible" CONTENT="Yes">
<TITLE id=dialogTitle>
Analyze Document
</TITLE>
<SCRIPT>
var L_Dialog_ErrorMessage = "An error has occurred in this dialog.";
var L_ErrorNumber_Text = "Error: ";
var L_NoErrors_Text = "No errors found.";
var L_FramesetInBody_Text = "This document might not display properly because there is a FRAMESET within the BODY of the document. The page author can resolve this problem by<OL><li>Removing the BODY tag.</
li><li>Insuring that there is no additional HTML code between the HEAD of the document and the FRAMESET.</li></ol><br><hr>";
var L_ContentAfterFrameset_Text = "This document might not display properly because there is content after the FRAMESET.<br><hr>";
var L_ObjectNotInstalled_Text = "The following OBJECT did not install properly.<BR>";
var L_AppletNotInstalled_Text = "The following APPLET did not install properly.<BR>";
var L_EmbedNotInstalled_Text = "The following EMBED did not install properly.<BR>";
var L_ObjectNotInstalledReasons_Text = "<br><br>This might have been caused by one of the following conditions:<OL><LI>Your current security settings prevent this OBJECT from being used.</li><li>This OBJECT was
not properly installed on your computer.</li><li>The page or OBJECT was authored incorrectly.</li></ul><hr>";
var L_AppletNotInstalledReasons_Text = "<br><br>This might have been caused by one of the following conditions:<OL><LI>Your current security settings prevent this APPLET from being used.</li><li>This APPLET was
not properly installed on your computer.</li><li>The page or APPLET was authored incorrectly.</li></ul><hr>";
var L_EmbedNotInstalledReasons_Text = "<br><br>This might have been caused by one of the following conditions:<OL><LI>Your current security settings prevent this EMBED from being used.</li><li>This EMBED was
not properly installed on your computer.</li><li>The page or EMBED was authored incorrectly.</li></ul><hr>";
var L_ObjectNotApartmentModel_Text = "The following OBJECT may not work reliably in all circumstances because it doesn't use the Apartment threading model.<br>";
var L_StyleSheetNotInstalled_Text = "This document might not display properly because the following style sheet did not get installed: ";
</SCRIPT>
<SCRIPT LANGUAGE="JavaScript" src="analyze.js" defer></SCRIPT>
</HEAD>
<BODY ID=bdy onLoad="loadBdy()" style="font-family: 'MS Shell Dlg';
font-size: 8pt; background: threedface; color: windowtext;"
topmargin=0 scroll=no>
```

VT API

T: 54 in 65

****

Bkav:	W32.RansomeDNZ.Trojan
MicroWorld-eScan:	Trojan.Ransom.Crysis.E
CMC:	None
CAT-QuickHeal:	Trojan.Mauvaise.SL1
McAfee:	Ransom-WW!CB15EE1CECE7
Cylance:	Unsafe
AegisLab:	Troj.Ransom.W32.Crusis.tpcS
TheHacker:	Trojan/Filecoder.Crysis.l
K7GW:	Trojan (005331801)
K7AntiVirus:	Trojan (005331801)
Arcabit:	Trojan.Ransom.Crysis.E
TrendMicro:	Mal_Crysis
Baidu:	Win32.Trojan.WisdomEyes.16070401.9500.9991
F-Prot:	W32/Wadhrama.B
Symantec:	Ransom.Crysis
ESET-NOD32:	a variant of Win32/Filecoder.Crysis.P
TrendMicro-HouseCall:	Mal_Crysis
Paloalto:	generic.ml
ClamAV:	None
Kaspersky:	Trojan-Ransom.Win32.Crusis.to
BitDefender:	Trojan.Ransom.Crysis.E
Babable:	None
ViRobot:	Trojan.Win32.Ransom.94720.F
Tencent:	Trojan-Ransom.Win32.Crysis.a
Ad-Aware:	Trojan.Ransom.Crysis.E
Emsisoft:	Trojan.Ransom.Crysis.E (B)
Comodo:	None
F-Secure:	Trojan.Ransom.Crysis.E
DrWeb:	Trojan.Encoder.3953
VIPRE:	None
Invincea:	heuristic
McAfee-GW-Edition:	BehavesLike.Win32.Ransom.nc
Fortinet:	W32/Crysis.L!tr.ransom
Sophos:	Troj/Criakl-G
SentinelOne:	static engine - malicious
Cyren:	W32/Trojan.ILHO-9216
Jiangmin:	Trojan.Crypren.ic
Webroot:	W32.Ransom.Gen
Avira:	TR/Dropper.Gen
MAX:	malware (ai score=100)
Antiy-AVL:	Trojan/Win32.AGeneric
Kingsoft:	None