Peeling The Layers Of Vawtrak

October 20-21, 2015
Raul Alvarez
About Me
About Me

- Senior Security Researcher @ Fortinet
- 21 published articles in Virus Bulletin
- Regular contributor in our company blog
Agenda
Agenda

- Vawtrak and Tor
  - DGA
  - Tor
  - Tor2Web

- Vawtrak and its Layers
  - Different features
  - Different layers
  - Multiple armoring strategies within the layers

- Vawtrak and Volatility
  - Using Volatility
  - Malware as a platform
Banking Malware
Banking Malware and C&C

- Binary updates/enhancements
- Operational commands
- Storage of stolen banking credentials
- Latest configuration
Banking Malware Protection Strategy

- Binary armoring to avoid detection
- Continuous monitoring of AV detection
- Using DGA to minimize takedowns
- Hiding its C&C via Tor
Vawtrak
What is Vawtrak?

- Also known as Neverquest
- A banking trojan
- Uses layering techniques similar to a Matryoshka doll
- Uses multiple armoring strategies
- Uses DGA
- Uses Tor2web
Vawtrak and Tor
DGA – Hiding is not enough
- DGA – Domain name Generation Algorithm
- Also called PrDGA (Pseudo-random DGA)
- Generates a binary seed
  - Can be a constant value
  - Can be generated from the current time and date
- Generates a string of random alpha-numeric characters
- Adds a variation of TLDs, such as com, org, info
How DGA works

- Client-side and Server-side uses the same algorithm
- The server-side registers one or more generated domain names
- The client-side tries all possible combination of generated domain names
- The client-side establishes connection to the server-side
- The server-side un-registers the registered domain to avoid detection
C&C
Not a fixed string
Derived from a DWORD value
Controlled by 40-byte XOR key
Different variants, different domains
Vawtrak’s DGA

- seed
- byte generator
- alphanumeric generator

```
MOV ESI DWORD PTR SS:[EBP-0C]
MOV EAX DWORD PTR DS:[EDI+EBX+212]
XOR EDI,EDI
MOV DWORD PTR SS:[EBP-10],EAX
LEA EAX,[EBP-10]
PUSH EAX
CALL byte gen_
PUSH ECX
MOV ECX,DWORD PTR DS:[16E2144]
ADD ECX,EAX
XOR AL,BYTE PTR DS:[EDI+ECX+216]
INC EDI
CMP EDI,40
JB SHORT 016BD7FC
```

```
PUSH EBP
MOV EBP,ESP
CMP DWORD PTR SS:[EBP+8],0
JE SHORT 016C0D1D
PUSH 4
POP EAX
IMUL EAX,EAX,0
MOV ECX,DWORD PTR SS:[EBP+8]
IMUL EAX,DWORD PTR DS:[EAX+ECX],343FD
ADD EAX,269EC3
PUSH 4
POP EAX
IMUL ECX,EAX,0
MOV EDX,DWORD PTR SS:[EBP+8]
MOV DWORD PTR DS:[ECX+EDX],EAX
PUSH 4
POP EAX
IMUL EAX,EAX,0
MOV EDX,DWORD PTR SS:[EBP+8]
MOV EAX,DWORD PTR DS:[EAX+ECX]
SHR EAX,10
AND EAX,00007FFF
JMP SHORT 016C0D51
```
Different variants, different domains

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>41982</td>
<td>6</td>
<td></td>
<td>30</td>
<td>4.2</td>
<td>DNS</td>
</tr>
<tr>
<td>42009</td>
<td>8</td>
<td></td>
<td>30</td>
<td>4.2</td>
<td>DNS</td>
</tr>
<tr>
<td>42013</td>
<td>8</td>
<td></td>
<td>30</td>
<td>4.2</td>
<td>DNS</td>
</tr>
<tr>
<td>43156</td>
<td>8</td>
<td></td>
<td>30</td>
<td>4.2</td>
<td>DNS</td>
</tr>
<tr>
<td>43184</td>
<td>1</td>
<td></td>
<td>30</td>
<td>4.2</td>
<td>DNS</td>
</tr>
<tr>
<td>43303</td>
<td>1</td>
<td></td>
<td>30</td>
<td>4.2</td>
<td>DNS</td>
</tr>
<tr>
<td>43380</td>
<td>1</td>
<td></td>
<td>30</td>
<td>4.2</td>
<td>DNS</td>
</tr>
<tr>
<td>43421</td>
<td>1</td>
<td></td>
<td>30</td>
<td>4.2</td>
<td>DNS</td>
</tr>
<tr>
<td>43428</td>
<td>1</td>
<td></td>
<td>30</td>
<td>4.2</td>
<td>DNS</td>
</tr>
<tr>
<td>43435</td>
<td>2</td>
<td></td>
<td>30</td>
<td>4.2</td>
<td>DNS</td>
</tr>
</tbody>
</table>

sample #1
Different variants, different domains

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>465</td>
<td>7</td>
<td>40</td>
<td>94.2</td>
<td>DNS</td>
<td>Standard query A <a href="http://www.laref.ru">www.laref.ru</a></td>
</tr>
<tr>
<td>483</td>
<td>7</td>
<td>40</td>
<td>94.2</td>
<td>DNS</td>
<td>Standard query A fy nds ed.ru</td>
</tr>
<tr>
<td>493</td>
<td>7</td>
<td>40</td>
<td>94.2</td>
<td>DNS</td>
<td>Standard query A zdn vuy fm.com</td>
</tr>
<tr>
<td>497</td>
<td>8</td>
<td>40</td>
<td>94.2</td>
<td>DNS</td>
<td>Standard query A nav y.com</td>
</tr>
<tr>
<td>504</td>
<td>8</td>
<td>40</td>
<td>94.2</td>
<td>DNS</td>
<td>Standard query A der y.com</td>
</tr>
<tr>
<td>562</td>
<td>9</td>
<td>40</td>
<td>94.2</td>
<td>DNS</td>
<td>Standard query A un rrh eg.ru</td>
</tr>
<tr>
<td>577</td>
<td>1</td>
<td>40</td>
<td>94.2</td>
<td>DNS</td>
<td>Standard query A r w asmuch.ru</td>
</tr>
<tr>
<td>581</td>
<td>1</td>
<td>40</td>
<td>94.2</td>
<td>DNS</td>
<td>Standard query A ge ntant in.ru</td>
</tr>
<tr>
<td>585</td>
<td>1</td>
<td>40</td>
<td>94.2</td>
<td>DNS</td>
<td>Standard query A w a hep.ru</td>
</tr>
<tr>
<td>586</td>
<td>1</td>
<td>40</td>
<td>94.2</td>
<td>DNS</td>
<td>Standard query A w a hep.ru</td>
</tr>
<tr>
<td>587</td>
<td>1</td>
<td>40</td>
<td>94.2</td>
<td>DNS</td>
<td>Standard query A w a hep.ru</td>
</tr>
<tr>
<td>588</td>
<td>1</td>
<td>40</td>
<td>94.2</td>
<td>DNS</td>
<td>Standard query A w a hep.ru</td>
</tr>
<tr>
<td>590</td>
<td>1</td>
<td>40</td>
<td>94.2</td>
<td>DNS</td>
<td>Standard query A w a hep.ru</td>
</tr>
</tbody>
</table>

sample #2
Different variants, different domains

<table>
<thead>
<tr>
<th>No.</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>66</td>
<td>50</td>
<td></td>
<td>4.2</td>
<td>DNS Standard query A</td>
</tr>
<tr>
<td>104</td>
<td>50</td>
<td></td>
<td>4.2</td>
<td>DNS Standard query A</td>
</tr>
<tr>
<td>148</td>
<td>50</td>
<td></td>
<td>4.2</td>
<td>DNS Standard query A</td>
</tr>
<tr>
<td>152</td>
<td>50</td>
<td></td>
<td>4.2</td>
<td>DNS Standard query A</td>
</tr>
<tr>
<td>166</td>
<td>50</td>
<td></td>
<td>4.2</td>
<td>DNS Standard query A</td>
</tr>
<tr>
<td>171</td>
<td>50</td>
<td></td>
<td>4.2</td>
<td>DNS Standard query A</td>
</tr>
<tr>
<td>175</td>
<td>50</td>
<td></td>
<td>4.2</td>
<td>DNS Standard query A</td>
</tr>
<tr>
<td>180</td>
<td>50</td>
<td></td>
<td>4.2</td>
<td>DNS Standard query A</td>
</tr>
<tr>
<td>218</td>
<td>50</td>
<td></td>
<td>4.2</td>
<td>DNS Standard query A</td>
</tr>
<tr>
<td>232</td>
<td>50</td>
<td></td>
<td>4.2</td>
<td>DNS Standard query A</td>
</tr>
<tr>
<td>246</td>
<td>50</td>
<td></td>
<td>4.2</td>
<td>DNS Standard query A</td>
</tr>
<tr>
<td>275</td>
<td>50</td>
<td></td>
<td>4.2</td>
<td>DNS Standard query A</td>
</tr>
<tr>
<td>288</td>
<td>50</td>
<td></td>
<td>4.2</td>
<td>DNS Standard query A</td>
</tr>
<tr>
<td>300</td>
<td>50</td>
<td></td>
<td>4.2</td>
<td>DNS Standard query A</td>
</tr>
<tr>
<td>305</td>
<td>50</td>
<td></td>
<td>4.2</td>
<td>DNS Standard query A</td>
</tr>
</tbody>
</table>

sample #3
Different variants, different domains

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>42914</td>
<td>3:00</td>
<td>1 1</td>
<td>1.2</td>
<td>DNS</td>
<td>Standard query A <a href="http://www.crow.com">www.crow.com</a></td>
</tr>
<tr>
<td>42929</td>
<td>5:15</td>
<td>1 1</td>
<td>1.2</td>
<td>DNS</td>
<td>Standard query A q tenantel.com</td>
</tr>
<tr>
<td>42936</td>
<td>5:15</td>
<td>1 1</td>
<td>1.2</td>
<td>DNS</td>
<td>Standard query A m erstargon.ru</td>
</tr>
<tr>
<td>42937</td>
<td>5:15</td>
<td>1 1</td>
<td>1.2</td>
<td>DNS</td>
<td>Standard query A m erstargon.ru</td>
</tr>
<tr>
<td>42938</td>
<td>5:15</td>
<td>1 1</td>
<td>1.2</td>
<td>DNS</td>
<td>Standard query A m erstargon.ru</td>
</tr>
<tr>
<td>42939</td>
<td>5:15</td>
<td>1 1</td>
<td>1.2</td>
<td>DNS</td>
<td>Standard query A m erstargon.ru</td>
</tr>
<tr>
<td>42949</td>
<td>5:15</td>
<td>1 1</td>
<td>1.2</td>
<td>DNS</td>
<td>Standard query A l rowler.ru</td>
</tr>
<tr>
<td>42950</td>
<td>5:15</td>
<td>1 1</td>
<td>1.2</td>
<td>DNS</td>
<td>Standard query A l rowler.ru</td>
</tr>
<tr>
<td>42951</td>
<td>5:15</td>
<td>1 1</td>
<td>1.2</td>
<td>DNS</td>
<td>Standard query A l rowler.ru</td>
</tr>
<tr>
<td>43133</td>
<td>6:15</td>
<td>1 1</td>
<td>1.2</td>
<td>DNS</td>
<td>Standard query A o rda.ru</td>
</tr>
<tr>
<td>43197</td>
<td>6:15</td>
<td>1 1</td>
<td>1.2</td>
<td>DNS</td>
<td>Standard query A y yalam.ru</td>
</tr>
<tr>
<td>43210</td>
<td>6:15</td>
<td>1 1</td>
<td>1.2</td>
<td>DNS</td>
<td>Standard query A a to.ru</td>
</tr>
<tr>
<td>43217</td>
<td>6:15</td>
<td>1 1</td>
<td>1.2</td>
<td>DNS</td>
<td>Standard query A b time.ru</td>
</tr>
<tr>
<td>43227</td>
<td>6:15</td>
<td>1 1</td>
<td>1.2</td>
<td>DNS</td>
<td>Standard query A l han.com</td>
</tr>
<tr>
<td>43261</td>
<td>6:15</td>
<td>1 1</td>
<td>1.2</td>
<td>DNS</td>
<td>Standard query A k sh1.com</td>
</tr>
<tr>
<td>43276</td>
<td>6:15</td>
<td>1 1</td>
<td>1.2</td>
<td>DNS</td>
<td>Standard query A u tus.com</td>
</tr>
<tr>
<td>43298</td>
<td>6:15</td>
<td>1 1</td>
<td>1.2</td>
<td>DNS</td>
<td>Standard query A c dhlisjohn.com</td>
</tr>
<tr>
<td>43302</td>
<td>6:15</td>
<td>1 1</td>
<td>1.2</td>
<td>DNS</td>
<td>Standard query A l entehed.com</td>
</tr>
<tr>
<td>43312</td>
<td>6:15</td>
<td>1 1</td>
<td>1.2</td>
<td>DNS</td>
<td>Standard query A r eugrigh.com</td>
</tr>
<tr>
<td>43319</td>
<td>6:15</td>
<td>1 1</td>
<td>1.2</td>
<td>DNS</td>
<td>Standard query A o rsforrep.com</td>
</tr>
<tr>
<td>43325</td>
<td>6:15</td>
<td>1 1</td>
<td>1.2</td>
<td>DNS</td>
<td>Standard query A s mines.com</td>
</tr>
<tr>
<td>43327</td>
<td>6:15</td>
<td>1 1</td>
<td>1.2</td>
<td>DNS</td>
<td>Standard query A s mines.com</td>
</tr>
<tr>
<td>43328</td>
<td>6:15</td>
<td>1 1</td>
<td>1.2</td>
<td>DNS</td>
<td>Standard query A s mines.com</td>
</tr>
<tr>
<td>43341</td>
<td>6:15</td>
<td>1 1</td>
<td>1.2</td>
<td>DNS</td>
<td>Standard query A p ndmaheg.ru</td>
</tr>
<tr>
<td>43348</td>
<td>6:15</td>
<td>1 1</td>
<td>1.2</td>
<td>DNS</td>
<td>Standard query A p thec.ru</td>
</tr>
<tr>
<td>43358</td>
<td>6:15</td>
<td>1 1</td>
<td>1.2</td>
<td>DNS</td>
<td>Standard query A d onrab.ru</td>
</tr>
<tr>
<td>43365</td>
<td>6:15</td>
<td>1 1</td>
<td>1.2</td>
<td>DNS</td>
<td>Standard query A m bet.ru</td>
</tr>
<tr>
<td>43366</td>
<td>6:15</td>
<td>1 1</td>
<td>1.2</td>
<td>DNS</td>
<td>Standard query A m bet.ru</td>
</tr>
</tbody>
</table>

Sample #4
Tor2Web C&C
Vawtrak’s DGA

- **Seed**
- **Byte generator**
- **Alphanumeric generator**

```plaintext
CALL domain.name_generator
CMP EAX, 0
JE SHORT 016B3082
PUSH 16D9E30
LEA EAX, [EBP-4C]
PUSH EAX
LEA EAX, [EBP-14C]
PUSH 16D9E3C
PUSH EAX
CALL DWORD PTR DS:[wprintfa]
```

```plaintext
ASCII "tor2web.org"
```

```plaintext
ASCII "https://%s.%s/favicon.ico"
```
<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>121</td>
<td>40</td>
<td>4.2</td>
<td>DNS</td>
<td>Standard query A ot</td>
<td>gxbcwvrqs.tcr2web.org</td>
</tr>
<tr>
<td>141</td>
<td>40</td>
<td>4.2</td>
<td>DNS</td>
<td>Standard query A 4b</td>
<td>24e7n6gnb.tcr2web.org</td>
</tr>
<tr>
<td>161</td>
<td>40</td>
<td>4.2</td>
<td>DNS</td>
<td>Standard query A bc</td>
<td>f4m3lnw4o.tcr2web.org</td>
</tr>
<tr>
<td>245</td>
<td>40</td>
<td>4.2</td>
<td>DNS</td>
<td>Standard query A ot</td>
<td>gxbcwvrqs.tcr2web.org</td>
</tr>
<tr>
<td>265</td>
<td>40</td>
<td>4.2</td>
<td>DNS</td>
<td>Standard query A 4b</td>
<td>24e7n6gnb.tcr2web.org</td>
</tr>
<tr>
<td>285</td>
<td>40</td>
<td>4.2</td>
<td>DNS</td>
<td>Standard query A bc</td>
<td>f4m3lnw4o.tcr2web.org</td>
</tr>
<tr>
<td>370</td>
<td>40</td>
<td>4.2</td>
<td>DNS</td>
<td>Standard query A 4b</td>
<td>24e7n6gnb.tcr2web.org</td>
</tr>
<tr>
<td>390</td>
<td>40</td>
<td>4.2</td>
<td>DNS</td>
<td>Standard query A bc</td>
<td>f4m3lnw4o.tcr2web.org</td>
</tr>
<tr>
<td>410</td>
<td>40</td>
<td>4.2</td>
<td>DNS</td>
<td>Standard query A ot</td>
<td>gxbcwvrqs.tcr2web.org</td>
</tr>
<tr>
<td>599</td>
<td>40</td>
<td>4.2</td>
<td>DNS</td>
<td>Standard query A 4b</td>
<td>24e7n6gnb.tcr2web.org</td>
</tr>
<tr>
<td>619</td>
<td>40</td>
<td>4.2</td>
<td>DNS</td>
<td>Standard query A bc</td>
<td>f4m3lnw4o.tcr2web.org</td>
</tr>
<tr>
<td>639</td>
<td>40</td>
<td>4.2</td>
<td>DNS</td>
<td>Standard query A ot</td>
<td>gxbcwvrqs.tcr2web.org</td>
</tr>
</tbody>
</table>

sample #2
### Tor2Web C&C

#### sample #4

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>46171</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>DNS</td>
<td>Standard query A ots gxbcwvrqs.tor2web.org</td>
</tr>
<tr>
<td>46273</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>DNS</td>
<td>Standard query A 4bpi 24a7n6gbn.tor2web.org</td>
</tr>
<tr>
<td>46336</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>DNS</td>
<td>Standard query A bc3 F4m31nw4o.tor2web.org</td>
</tr>
</tbody>
</table>
How Tor Works
How Tor Works

Step 1: Alice’s Tor client obtains a list of Tor nodes from a directory server.

Image taken from torproject.org
How Tor Works

Step 2: Alice’s Tor client picks a random path to destination server. **Green links are encrypted, red links are in the clear.**

Image taken from torproject.org
How Tor Works

Step 3: If at a later time, the user visits another site, Alice’s tor client selects a second random path. Again, **green links** are encrypted, **red links** are in the clear.

Image taken from torproject.org
Tor and Hidden Services
Hidden Service: **Deep Web Radio**
Hidden Service: Electronic Store

BEST DEEPWEB ELECTRONICS STORE
BRAND NEW ELECTRONICS FOR GOOD PRICES

APPLE

<table>
<thead>
<tr>
<th>Product</th>
<th>Price</th>
<th>Order</th>
</tr>
</thead>
<tbody>
<tr>
<td>iPhone 6 Plus 16GB</td>
<td>B1.35</td>
<td></td>
</tr>
<tr>
<td>iPhone 6 16GB</td>
<td>B1.15</td>
<td></td>
</tr>
<tr>
<td>iPhone 5S 16GB</td>
<td>B0.99</td>
<td></td>
</tr>
<tr>
<td>iPad Air 2 64GB</td>
<td>B1.38</td>
<td></td>
</tr>
<tr>
<td>iPad Mini 3 64GB</td>
<td>B1.23</td>
<td></td>
</tr>
<tr>
<td>MacBook Air 13&quot; 128GB</td>
<td>B1.65</td>
<td></td>
</tr>
</tbody>
</table>

SAMSUNG

<table>
<thead>
<tr>
<th>Product</th>
<th>Price</th>
<th>Order</th>
</tr>
</thead>
<tbody>
<tr>
<td>Galaxy Note Edge 32GB</td>
<td>B1.21</td>
<td></td>
</tr>
<tr>
<td>Galaxy Note 4 N910 32GB</td>
<td>B0.95</td>
<td></td>
</tr>
<tr>
<td>Galaxy S5 32GB</td>
<td>B0.9</td>
<td></td>
</tr>
<tr>
<td>Galaxy Note 3 N9005 4G</td>
<td>B0.78</td>
<td></td>
</tr>
<tr>
<td>Galaxy S5 G900FD Dual SIM</td>
<td>B0.86</td>
<td></td>
</tr>
<tr>
<td>Nexus 10 32GB</td>
<td>B0.67</td>
<td></td>
</tr>
</tbody>
</table>
Hidden Service: Online News
Hidden Service: Free Email

Welcome to

What is Free Email is a darknet email service that allows you to send and receive email without revealing your location or identity. We provide this service to help journalists and activists combat the dragnet surveillance that exists on the Internet today. Even if you aren’t in conflict with the state or anyone in particular you as a human being deserve privacy.

Why should you trust us? You don’t have to trust us, in fact we recommend you don’t! When you send email using our webportal we recommend you encrypt your messages using PGP.

Are there any rules to using this thing? Generally we are pretty chill, all we ask is that you don’t use our FREE service to:

- Spam people
- Threaten people
- Harm people

Everything else is cool with us.

SIGN UP

**** Over 64,000 served and even faster storage! ****
Hidden Service: File Storage

Welcome to TorSafe!

TorSafe is able to host your files online in a secure way:
1. File Sharing you can organize your files in library and share them between users and group of users.
2. Anonymous we use the tor network, we are compatible with TorBrowser and are compliant with the best practices of Tor.
3. Secure strong encryption (AES256) is used to encrypt your files, only the owner of the key (password) can read the files, even not the TorSafe.
4. Collaboration exchange messages, files, discussions, conversations in a collaborative way with the other members.
5. wiki create your own wiki page in a WYSIWYG editor. You can keep personal notes or share pages.
6. Versioning of your files you can keep multiple versions of your files and come back to a previous versions in case of disaster.

Pricing Plan

<table>
<thead>
<tr>
<th>Plan</th>
<th>Copper</th>
<th>Bronze</th>
<th>Silver</th>
<th>Gold</th>
<th>Platinum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pro Hosting in datacenter</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Storage</td>
<td>10MB</td>
<td>1GB</td>
<td>5GB</td>
<td>1250GB</td>
<td></td>
</tr>
<tr>
<td>Number of users</td>
<td>1</td>
<td>1</td>
<td>5</td>
<td>50</td>
<td></td>
</tr>
<tr>
<td>Number of groups</td>
<td>Unlimited</td>
<td>Unlimited</td>
<td>Unlimited</td>
<td>Unlimited</td>
<td></td>
</tr>
<tr>
<td>Monthly bandwidth</td>
<td>1GB/month</td>
<td>10GB/month</td>
<td>Unlimited</td>
<td>Unlimited</td>
<td></td>
</tr>
<tr>
<td>Internal Backup (of encrypted data)</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Activation fee</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Price</td>
<td>Free</td>
<td>Free for early adopters!</td>
<td>256/month</td>
<td>333/month</td>
<td>1000/month</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>equivalent in bc</td>
<td>equivalent in bc</td>
<td>equivalent in bc</td>
</tr>
<tr>
<td>Comment</td>
<td>Limited account, intended for test purpose</td>
<td>For independent!</td>
<td>For a small team</td>
<td>For a medium team</td>
<td></td>
</tr>
</tbody>
</table>

We accept bitcoins [ 1PPJWAKT8i6954ZFLQZVTZBqt77JUdQl51j ] Contact torsafe@bitmessage.ch for an order or any questions

Our key points

ANONYMOUS

We are compliant with the Tor guidelines. Source: https://www.torproject.org/download/download.html

Use the Tor Browser™ You can use the Tor Browser to surf on TorSafe. Tor Browser is a customized version to protect your privacy and your identity.

Can't enable or install browser plugins™ You don't need any plugins that can break your anonymity such as Flash, RealPlayer, Quicktime
Hidden Service: Tor Supermarket

TorSupermarket Is Singing Its Swan Song.

June is the last month we are accepting new customers. It's time to say goodbye.
We are switching to a reseller-only business model and will only serve resellers from July 1st onwards.
You can hop the departing train and become a reseller Yourself by buying 3 or more items now.

For this occasion, a large scale goodbye clearance sale has started. Do not miss out.

We would like to Thank You all for Your cooperation over the last three and a half years. We started as a small start-up called PremiumTor way back in 2011 - we grew, but in many ways remained the same. It has indeed been a journey full of obstacles and fears, false feedbacks and clone sites hindering our mission and attacking our legitimacy, hackers and unfair payment solution providers trying to steal our funds, You name it. But we perserved. We are retiring from serving customers now and will only respond to a select list of partners with whom we grew and spread. This is Your last chance to join them. Farewell, and Farefree.

Thank You.
Hidden Service: Chat Rooms

Terms

The terms of service are pretty much just following the rules. Don’t be stupid, be respectful, and enjoy your time.

1. No child pornography. That doesn’t mean a censorship on discussing pedophilia, but it sure as hell isn’t allowed, and it is dodgy, ask before posting.

2. No public commercial trade. We don’t want Galaxy2 to become a market targeted by different governments not be allowed, because what may be legal in one place might not be legal another. It’s easier to just say and isn’t allowed. What happens in private conversation between members is private. But don’t advertise it.

3. Images and Avatars: Images of children are not allowed as avatars, sexualized or not. Images of trade or not allowed at all on Galaxy2. Pornography (S and p) is gone, and other forms might pass the test, but if so the are either Private or Friends viewable. It’s not allowed in Public or Logged in users, or as an Avatar. We won’t explicitly want to see it, and not to be accidentally viewable by anyone. Please make sure to use the correct.

4. Be respectful. Galaxy2 is meant to be a respectful community where ideas, philosophies, views, etc., can be discussed, learned, taught, communicated,whatever. It should be done in a respectful manner. Trolling, flaming and simply being an ass towards others doesn’t belong here. Go anywhere ideal for that.

5. The Galaxy2 Admin Team: The Galaxy2 Admin Team is here for the benefit of the community. We’re not trying to censor you, suppress you, or just plain annoy you. We want the community to grow and prosper, but for it to do just that, we need to be able to handle issues before they become too damaging to the overall community. And as such, we maintain the right to do our job. If we believe something is harmful for Galaxy2, or something violates the simple rules set forth, we will take action.

Once that’s said, we don’t consider our self unapologistic. We are willing to discuss and explain anything you may feel is wrong or right. We are more human and do make mistakes, as if you feel like we did something wrong, tell us and let’s have a mature dialog about it.

Comment/discuss the rules here.
Hidden Service: The Hidden Wiki

Welcome to The Hidden Wiki New hidden wiki url 2015 http://zql8It...er.onion & Add it to bookmarks and spread it!!!

Editor’s picks
Bored? Pick a random page from the article index and replace one of these slots with it.
- The Matrix - Very nice to read.
- How to Exit the Matrix - Learn how to Protect yourself and your rights, online and off.
- Verifying PGP signatures - A short and simple how-to guide.
- In Praise Of Hawala - Anonymous informal value transfer system.

Volunteer
Here are five different things that you can help us out with.
- Plunder other hidden service lists for links and place them here!
- File the SnapBBSIndex links wherever they go.
- Set external links to HTTPS where available, good certificate, and same content.
- Care to start recording onionland’s history? Check out Onionland’s Museum.
- Perform Dead Services Duties.

Introduction Points
- Appear search engine for Tor Hidden Services (allows you to add new sites to its database).
- The Hidden Wiki - Service that searches the clearnet.
- The Hidden Wiki - System. Claims to index around 1.1 Million pages.
- The Hidden Wiki - Marketers of sites, moderated.
- The Hidden Wiki - Markets and more.
- The Hidden Wiki more orderly and updated!
- The Hidden Wiki - 2 days old users can edit the main page.
- The Hidden Wiki - Spider robot finding known Onion sites. It does not list onions which are down.
- The Hidden Wiki - Community editable wiki that welcomes all users. Allows a variety of uses. Now recruiting Admins. [Down 2015/6]
And so much more …

- Email/Messaging
- Books
- Financial
- Audio/Music
- Domain/Hosting
- Security
- Blogs
- Social networks
- Forums
- And so much more …
Browsing hidden services via a normal web browser

Tor2web: Browse the Tor Onion Services

What's Tor2web
Tor is a software project that lets you anonymously browse the Internet. Tor2web is a project to let Internet users access Tor Onion Services without using Tor Browser.

Getting started
Whenever you see a URL like http://duskj1dksiugc6.onion/, that's a Tor Onion service. Just replace onion with .onion.to or .onion.city or .onionдоб or .onion.direct or any other domain made available by volunteers Tor2web operators Example:

https://duskj1dksiugc6.onion.to/

This connects you with Tor2web, which then talks to the onion service via Tor and relays the response back to you.

WARNING: Tor2web only protects publishers, not readers. As a reader installing Tor Browser will give you much greater anonymity, confidentiality, and authentication than using Tor2web. Using Tor2web trades off security for convenience and usability.

Tor2web & Tor Onion Sites Resources
Below a set of useful resources, Tor Onion Services indexes, search engines and applications available on the internet through Tor2web Proxies:

Firefox automatically sends some data to Mozilla so that we can improve your experience.
Header page

onion.to does not host this content; we are simply a conduit connecting Internet users to content hosted inside the Tor network.
onion.to does not provide any anonymity. You are strongly advised to download the Tor Browser Bundle and access this content over Tor.

For more information see our website for more details and send us your feedback.
Can Vawtrak really use DGA to create a randomized Tor C&Cs?
Pre-set .onion domains

Pseudorandom DGA will not work

Tor2Web C&C is not so random
<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>121</td>
<td>40</td>
<td>4.2</td>
<td>DNS</td>
<td>Standard query A ot</td>
<td>gxbcwrqs.tor2web.org</td>
</tr>
<tr>
<td>141</td>
<td>40</td>
<td>4.2</td>
<td>DNS</td>
<td>Standard query A 4b</td>
<td>24e7n6gbbc.tor2web.org</td>
</tr>
<tr>
<td>161</td>
<td>40</td>
<td>4.2</td>
<td>DNS</td>
<td>Standard query A bc</td>
<td>f4m31nw4o.tor2web.org</td>
</tr>
<tr>
<td>245</td>
<td>40</td>
<td>4.2</td>
<td>DNS</td>
<td>Standard query A ot</td>
<td>gxbcwrqs.tor2web.org</td>
</tr>
<tr>
<td>265</td>
<td>40</td>
<td>4.2</td>
<td>DNS</td>
<td>Standard query A 4b</td>
<td>24e7n6gbbc.tor2web.org</td>
</tr>
<tr>
<td>285</td>
<td>40</td>
<td>4.2</td>
<td>DNS</td>
<td>Standard query A bc</td>
<td>f4m31nw4o.tor2web.org</td>
</tr>
<tr>
<td>370</td>
<td>40</td>
<td>4.2</td>
<td>DNS</td>
<td>Standard query A 4b</td>
<td>24e7n6gbbc.tor2web.org</td>
</tr>
<tr>
<td>390</td>
<td>40</td>
<td>4.2</td>
<td>DNS</td>
<td>Standard query A bc</td>
<td>f4m31nw4o.tor2web.org</td>
</tr>
<tr>
<td>410</td>
<td>40</td>
<td>4.2</td>
<td>DNS</td>
<td>Standard query A ot</td>
<td>gxbcwrqs.tor2web.org</td>
</tr>
<tr>
<td>599</td>
<td>40</td>
<td>4.2</td>
<td>DNS</td>
<td>Standard query A 4b</td>
<td>24e7n6gbbc.tor2web.org</td>
</tr>
<tr>
<td>619</td>
<td>40</td>
<td>4.2</td>
<td>DNS</td>
<td>Standard query A bc</td>
<td>f4m31nw4o.tor2web.org</td>
</tr>
<tr>
<td>639</td>
<td>40</td>
<td>4.2</td>
<td>DNS</td>
<td>Standard query A ot</td>
<td>gxbcwrqs.tor2web.org</td>
</tr>
</tbody>
</table>

sample #2
Sample #4
Vawtrak and its Layers
### Armoring Strategies Within The Layers

<table>
<thead>
<tr>
<th>Anti-Emulator</th>
<th>Anti-Debugger</th>
<th>Anti-Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption/Decryption</td>
<td>Hashing</td>
<td>Compression/Decompression</td>
</tr>
<tr>
<td>Garbage Collection</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Code injection</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Layers of Vawtrak

Layer 1:
- Anti-Emulator
- Anti-Debugger
- Anti-Analysis

Layer 2:
- Decryption
- Garbage collection
- Decompression RtlDecompressBuffer

Layer 3:
- Decrypted + Compressed
- Self-code Injection
- Resource section
- Hashing for validity
- Decryption

Layer 4:
- Decoy (encrypted)
- Overlay

Layer 2
Layer 1: Anti-Emulator

Layer 1:
- Anti-Emulator
- Anti-Debugger
- Anti-Analysis

Layer 2:
- Decryption
- Garbage collection
- Decompression
- RtlDecompressBuffer

Layer 3:
- Self-code Injection
- Anti-Antimalware
- Resource section
- Hashing for validity
- Decryption

Layer 2:
- Decoy (encrypted)
- Overlay

Layer 3:
- Decrypted + compressed

Layer 4:
- Layer 2
Layer 1: Anti-Emulator

Hundreds of assembly language instruction 0x00

ADD BYTE PTR DS:[eax],al
Layer 1: Anti-Debugger

Layer 1:
- Anti-Emulator
- Anti-Debugger
- Anti-Analysis

Layer 2:
- Decryption
- Garbage collection
- Decompression

Layer 2:
- RtlDecompressBuffer

Layer 3:
- Decrypted + compressed
- Decrypted

Layer 3:
- Resource section
- Hashing for validity
- Decryption

Layer 4

Overlay

Decoy (encrypted)
Layer 1: Anti-Debugger

PEB (Process Environment Block)

- BeingDebugged
- ImageBase
- SpareBool
- Mutant

Stage 1

Stage 2

Confidential
Layer 1: Anti-Analysis

Layer 1
- Anti-Emulator
- Anti-Debugger
- Anti-Analysis

Layer 2
- Decryption
- Garbage collection
- Decryption
- RtlDecompressBuffer

Layer 3
- Decrypted + compressed
- Decompressed

Layer 4
- Self-code Injection
- Anti-Antimalware
- Resource section
- Hashing for validity
- Decryption
Layer 1: Anti-Analysis

CreateFileA API

using RETN
Layer 1: Decryption

Layer 1:
- Anti-Emulator
- Anti-Debugger
- Anti-Analysis

Layer 2:
- Decryption
- Garbage collection
- Decompression
  - Decryption
  - RtlDecompressBuffer

Layer 3:
- Layer 3 decrypted + compressed
- Decrypted + compressed
- Decompressed

Layer 4:
- Decryption
- Hashing for validity
- Resource section

Layer 2:
- Overlay
- Decoy (encrypted)

Self-code Injection

Anti-Antimalware

Resource section

Layer 2

Layer 3

Layer 4
Layer 2: Decryption + Garbage Collection

Layer 1
- Anti-Emulator
- Anti-Debugger
- Anti-Analysis

Layer 2
- Decryption
- Garbage Collection
  - Decryption
  - Garbage Collection
  - Decompression
    - RtlDecompressBuffer

Layer 3
- Decrypted + Compressed

Decoy (encrypted)

Layer 4
- Decryption
- Hashing for Validity
- Decryption

Self-code Injection
- Anti-Antimalware
- Resource Section
- Layer 2
- Layer 3
- Layer 4

Confidential
Layer 2: Decryption + Garbage Collection

- Decryption algorithm
- Garbage code
- Relevant code
- Decrypted/compressed executable
Layer 2: Decompression

Layer 1
- Anti-Emulator
- Anti-Debugger
- Anti-Analysis

Layer 2
- Decryption
- Garbage collection
- Decompression
- RtlDecompressBuffer

Layer 3
- Decrypted + compressed
- Decompressed

Layer 4
- Layer 2 (encrypted)
- Decoy
- Overlay

Self-code Injection
- Anti-Antimalware
- Resource section
- Decryption
- Hashing for validity
Layer 2: Decompression

RtlDecompressBuffer

Syntax:

NTSTATUS RtlDecompressBuffer(
    _In_  USHORT CompressionFormat,
    _Out_ PUCHAR UncompressedBuffer,
    _In_  ULONG UncompressedBufferSize,
    _In_  PUCHAR CompressedBuffer,
    _In_  ULONG CompressedBufferSize,
    _Out_ PULONG FinalUncompressedSize
);

RtlDecompressBuffer( 0x102, 0x1744e8, 0x30e00, 0x1436d0, 0x2F9AE, 0x12fcc4)
Layer 2: Self-code Injection

Layer 1:
- Anti-Emulator
- Anti-Debugger
- Anti-Analysis

Layer 2:
- Decryption
- Garbage collection
- Decompression
  - RtlDecompressBuffer
- Self-code Injection

Layer 3:
- Anti-Antimalware
- Resource section
- Hashing for validity
- Decryption

Layer 4:
- Layer 2 (encrypted)
- Overlay
- Layer 3 decrypted + compressed
- Layer 3 decompressed

Decoy
Layer 2: Self-code Injection

Steps:
1. Allocates new memory (0x8a0000)
2. Copies the decompressed Layer 3 to 0x8a0000
3. Zeroes out the original location (0x400000) of Layer 2
4. Copies Layer 3 from 0x8a0000 to 0x400000
5. Fixes IAT of Layer 3 in 0x400000
6. Executes Layer 3
Layer 3: Anti-antimalware

Layer 1
- Anti-Emulator
- Anti-Debugger
- Anti-Analysis

Layer 2
- Decryption
- Garbage collection
- Decompression
  - RtlDecompressBuffer
- Self-code Injection

Layer 3
- Anti-Antimalware
  - Resource section
  - Hashing for validity
  - Decryption

Layer 2 (encrypted)
- Decoy

Layer 3 (decrypted + compressed)
- Overlay

Layer 3 (decompressed)

Layer 4
1. Traverses the following folders:
   • Program Files
   • Program Files (x86)
   • %AppData%
2. Creates hash value for the antimalware pathname
3. Creates registry key
   • HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Paths\[hash value]
   • SaferFlags = 0
   • ItemData = pathname
Layer 3: Anti-antimalware
Layer 3: Generating Layer 4

Layer 1:
- Anti-Emulator
- Anti-Debugger
- Anti-Analysis

Layer 2:
- Decryption
- Garbage collection
- Decompression
  - RtlDecompressBuffer

Layer 3:
- Self-code Injection
  - Anti-Antimalware
    - resource section
    - hashing for validity
    - decryption

Layer 2:
- Layer 3 encrypted
- Layer 3 decrypted + compressed
- Layer 3 decompressed

Layer 4:
- Decrypted + compressed
- Decompressed
- Hashing for validity
- Decryption
Layer 3: Generating Layer 4

1. Copies RT_RCDATA from .rscr section to the heap memory
2. Calculates the hash (0x24D2EDEA) of the raw data
3. Decrypts the raw data
4. Calculates the hash(0x52194545) of the decrypted data(DLL)
5. Creates random filename + “.dat”
6. Copies the decrypted data from heap memory to newly created file (Layer 4)
7. Creates new startup registry key for Layer 4(DLL)
Demo
Decoy File
Vawtrak and Volatility
http://www.volatilityfoundation.org/#!24/c12wa
c:\v24 --profile=WinXPSP2x86 -f vawtrak.vmem \texttt{psxview}

<table>
<thead>
<tr>
<th>Offset(P)</th>
<th>Name</th>
<th>PID</th>
<th>pslst</th>
<th>psscan</th>
<th>thrdproc</th>
<th>pspcid</th>
<th>csrss</th>
<th>session</th>
<th>deskth</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x01b8db28</td>
<td>mainOUT-crypted</td>
<td>224</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td>0x019d4c90</td>
<td>cmd.exe</td>
<td>1420</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td>0x01aa01d8</td>
<td>lsass.exe</td>
<td>680</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td>0x01704218</td>
<td>wsctfy.exe</td>
<td>1672</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td>0x0193c8d8</td>
<td>jusched.exe</td>
<td>1832</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td>0x018ebda0</td>
<td>winlogon.exe</td>
<td>624</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td>0x01aa4a28</td>
<td>svchost.exe</td>
<td>1208</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td>0x01aaada0</td>
<td>svchost.exe</td>
<td>1044</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td>0x018deac0</td>
<td>explorer.exe</td>
<td>1692</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
<td>True</td>
</tr>
</tbody>
</table>
c:\v24 --profile=WinXPSP2x86 -f vawtrak.vmem malfind -p 224

Volatility Foundation Volatility Framework 2.4
Process: mainOUT-crypted Pid: 224 Address: 0x890000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x00890000  55 53 57 56 81 ec 98 01 00 00 8b 84 24 ac 01 00 USWV........$...
0x00890010  00 c7 84 24 d4 00 00 00 00 00 00 c7 84 24 fc ...$............$.
0x00890020  00 00 00 00 00 00 00 66 c7 84 24 9e 00 00 00 0f ......f..$......
0x00890030  6e c7 84 24 38 01 00 00 01 00 00 00 8b 8c 24 38 n..$8.............$8

0x890000 55  
PUSH EBP
0x890001 53  
PUSH EBX
0x890002 57  
PUSH EDI
0x890003 56  
PUSH ESI
0x890004 81ec98010000  
SUB ESP, 0x198
0x89000a 8b8424ac010000  
MOV EAX, [ESP+0x1ac]
0x890011 c78424d40000000000000000  
MOV DWORD [ESP+0xd4], 0x0
0x89001c c78424fc0000000000000000  
MOV DWORD [ESP+0xfc], 0x0
0x890027 66c784249e00000000f6e  
MOV WORD [ESP+0x9e], 0x6e0f
0x890031 c78424380100000000000000  
MOV DWORD [ESP+0x138], 0x1
0x89003c 8b  
DB 0x8b
0x89003d 8c2438  
MOV [EAX+EDI], FS
Rule: r1
Owner: Process mainOUT-crypted Pid 224
0x77dd0000 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ..............
0x77dd0010 b8 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 00 00 00 00 00 00 00
0x77dd0040 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 ........@........
0x77dd0050 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6f is.program.canno
0x77dd0060 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 mode....$.;
0x77dd0070 a8 6a e2 68 ec 0b 8c 3b ec 0b 8c 3b ec 0b 8c 3b .j.h;...;...;...;
0x77dd0090 2f 04 d1 3b eb 0b 8c 3b 2f 04 83 3b e1 0b 8c 3b 0x77dd00a0 3d 07 d3 3b ee 0b 8c 3b ec 0b 8d 3b 54 0a 8c 3b /
0x77dd00b0 2f 04 d0 3b ed 0b 8c 3b 2f 04 d2 3b ed 0b 8c 3b =;................;
0x77dd00c0 2f 04 ec 3b f1 0b 8c 3b 2f 04 d3 3b 7e 0b 8c 3b /
0x77dd00d0 2f 04 d6 3b ed 0b 8c 3b 52 69 63 68 ec 0b 8c 3b /
0x77dd00e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 PE..L...q..I....
0x77dd00f0 50 45 00 00 4c 01 04 00 71 03 90 49 00 00 00 00 MZu..H<.Q@;.r.3.
0x77de8218 4d 5a 75 1d 8b 48 3c 8d 51 40 3b da 72 13 33 d2 .<.PE.......[]..
0x77de8228 81 3c 01 50 45 00 00 0f 94 c2 8b c2 5b 5d c2 04 .3......MZ......
0x77de8238 00 33 c0 eb f7 90 90 90 4d 5a 00 90 90 90 90 90 <<next slide>>
Rule: r1
Owner: Process mainOUT-crypted Pid 224

0x00400000  4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00
0x00400010  b8 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00
0x00400020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x00400030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x00400040  0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68
0x00400050  69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e
0x00400060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x00400070  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x00400080  52 6f d7 9a 16 0e b9 c9 16 0e b9 c9 16 0e b9 c9
0x00400090  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x004000a0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x004000b0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x004000c0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x004000d0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x004000e0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x004000f0  06 22 2c 52 00 00 00 00 00 00 00 00 00 00 00 00

MZ................
.................@
.................
.................
.................!
..L!Th
is.program.canno
........
t.be.run.in.DOS.
mode....$
........
Ro...........
.v,...........
.v*...........J...
yx.....yx#
....
yx$.....Rich....
........
........ PE..L...
n",R............
Rule: r1
Owner: Process mainOUT-crypted Pid 224

0x001436d3  4d 5a 90 00 03 00 00 00 82 04 00 30 ff ff 00 00
0x001436e3  b8 00 38 2d 01 00 40 04 38 19 00 e8 00 0c 0e 1f
0x001436f3  00 ba 0e 00 b4 09 cd 21 b8 00 01 4c cd 21 54 68
0x00143703  69 73 00 20 70 6f 67 72 61 6d 00 20 63 61 6e
0x00143713  00 6d 6f 80 64 65 0d 0d 0a 24 04 86
0x00143723  00 4d 6f 80 64 65 2e 0d
0x00143733  02 07 52 69 63 06 68 01 33 15
0x00143743  00 22 2c 52 05 13 00 e0 00 03 01 0b
0x00143753  01 0a 00 42 00 01 46 e6 02 00 00 00 01 96 7e 10
0x00143773  00 05 81 02 00 02 81 05 80 0b 05 cc 00 01
0x00143793  82 19 85 03 00 60 80 9a 00 9a f4 5f c7 02 0f 81
0x001437b3  02 14 81 15 86 03 06 03 41 02 00 68 5c 00 00 8c
0x001437c3  01 04 80 30 00 00 1c d0 80 18 45 00 50 00 04 00
Rule: r1
Owner: Process mainOUT-crypted Pid 224

0x001744e8  4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00  MZ.............
0x001744f8  b8 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .........@
0x00174508  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........
0x00174518  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e8 00 00 00
0x00174528  0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68  ........!..L!Th
0x00174538  69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6f  is.program.canno
0x00174548  74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20  t.be.run.in.DOS.
0x00174558  6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00  mode....$
0x00174568  52 6f d7 9a 16 0e b9 c9 16 0e b9 c9 16 0e b9 c9  Ro.........
0x00174578  6f d7 9a 16 0e b9 c9 16 0e b9 c9 16 0e b9 c9 .v,.........
0x00174588  1f 76 2c c9 16 0e b9 c9 16 0e b9 c9 16 0e b9 c9 .v*.........J...
0x00174598  1f 76 2a c9 16 0e b9 c9 16 0e b9 c9 16 0e b9 c9 yx.....yx#
0x001745a8  79 78 24 c9 16 0e b9 c9 52 69 63 68 16 0e b9 c9 yx$.....Rich..
0x001745b8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........
0x001745c8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........PE,.L...
0x001745d8  6e 22 2c 52 00 00 00 00 00 00 00 00 00 00 e0 00 03 01 n",R.........
Rule: r1
Owner: Process mainOUT-crypted Pid 224
0x008a0000 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ .............
0x008a0010 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 ........@........
0x008a0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..........
0x008a0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..........
0x008a0040 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 ........ is.program.canno
0x008a0050 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 Th is.be.run.in.DOS.
0x008a0060 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 mode....$........
0x008a0070 52 6f d7 9a 16 0e b9 c9 16 0e b9 c9 16 0e b9 c9 Ro.............
0x008a0080 1f 76 2c c9 17 0e b9 c9 16 0e b9 c9 15 0e b9 c9 .v,.............
0x008a0090 1f 76 2a c9 1b 0e b9 c9 16 0e b8 c9 4a 0e b9 c9 .v*........J....
0x008a00a0 79 78 24 2c 99 17 0e b9 c9 52 69 63 68 16 0e b9 c9 yx....yx#......
0x008a00b0 79 78 17 c9 1b 0e b9 c9 79 78 23 c9 17 0e b9 c9 yx$.....Rich....
0x008a00c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..........
0x008a00d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..........
0x008a00e0 6e 22 2c 52 00 00 00 00 00 00 00 00 00 e0 00 03 01 n",R.............
Rule: r1
Owner: Process mainOUT-crypted Pid 224

0x00aaa668  4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00  
MZ.............

0x00aaa678  b8 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00  
........@

0x00aaa688  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  

0x00aaa698  00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00  

0x00aaa6a8  0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68  
This.program.cannot.be.run.in.DOS.

0x00aaa6b8  69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6f  

t

0x00aaa6c8  74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20  
t.be.run.in.DOS.

0x00aaa6d8  6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00  
mode....$

0x00aaa6e8  8b 95 09 e6 cf f4 67 b5 cf f4 67 b5 cf f4 67 b5  
.......g...g...g.

0x00aaa6f8  3e 32 a8 b5 d6 f4 67 b5 3e 32 aa b5 c4 f4 67 b5  
>2....g.>2....g.

0x00aaa708  3e 32 a9 b5 95 f4 67 b5 c6 8c f4 b5 ca f4 67 b5  
>2....g....g.

0x00aaa718  cf f4 66 b5 9c f4 67 b5 54 1f a8 b5 cd f4 67 b5  
..f...g.T......g.

0x00aaa728  54 1f ae b5 ce f4 67 b5 54 1f ab b5 ce f4 67 b5  
T......g.T......g.

0x00aaa738  52 69 63 68 cf f4 67 b5 50 45 00 00 4c 01 05 00  
Rich...g.PE.L...

0x00aaa748  42 e1 2d 52 00 00 00 00 00 00 00 00 00 e0 00 02 21  
B.-R.............!

0x00aaa758  0b 01 08 00 00 30 02 00 00 00 02 00 00 00 00 00  
.....0...........
Libraries (DLL) loaded in the memory also have the MZ header.
Malware As A Platform
Malware As A Platform

vawtrak

encrypted overlay

vawtrak

decrypted overlay

Diana-23.jpg

mainOUT-crypted-5.exe

compressed exe

decompressed executable

decompressed executable

mainOUT-crypted-5.exe

resource section

decompressed executable

decompressed executable

payload executable