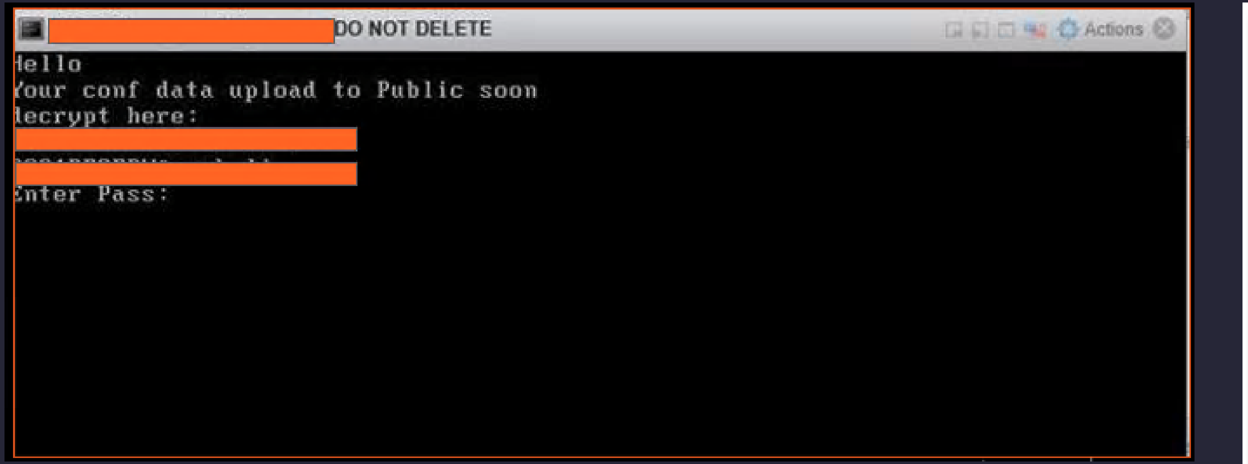
rightmove

True Stories of Ransomware

Myths, lies, and misconception's uncovered.

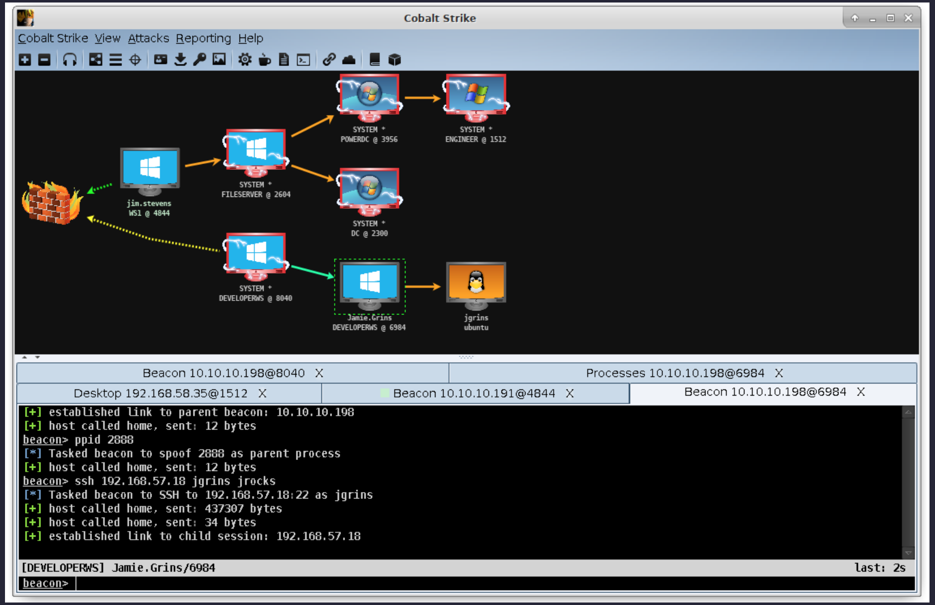
“A highly sophisticated attack…”

rightmove

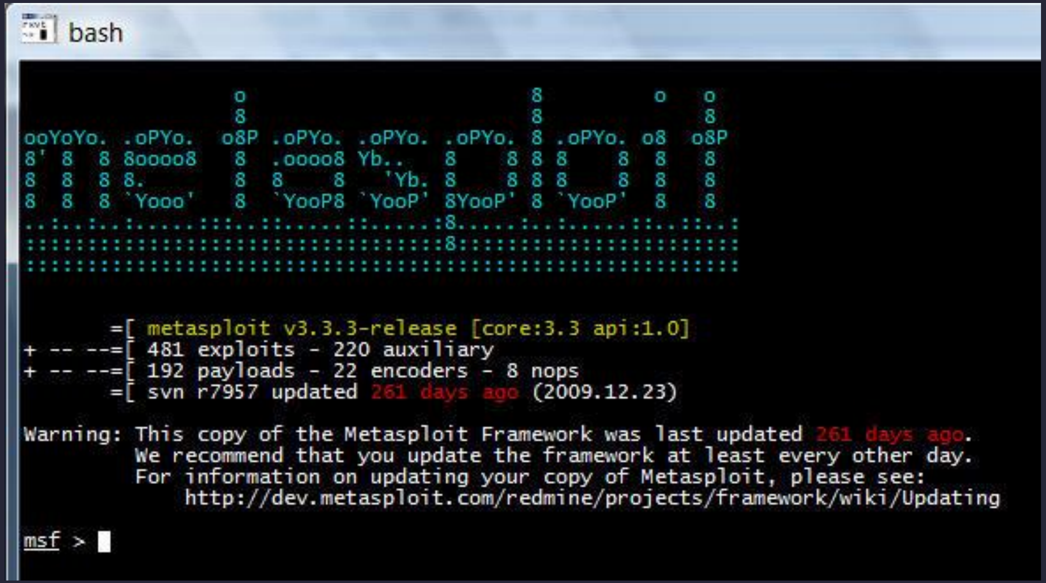


[redacted] DO NOT DELETE

```
Hello
Your conf data upload to Public soon
decrypt here:
[redacted]
Enter Pass:
```



```
[+] established link to parent beacon: 10.10.10.198
[+] host called home, sent: 12 bytes
beacon> ppid 2888
[*] Tasked beacon to spoof 2888 as parent process
[+] host called home, sent: 12 bytes
beacon> ssh 192.168.57.18 jgrins jrocks
[*] Tasked beacon to SSH to 192.168.57.18:22 as jgrins
[+] host called home, sent: 437307 bytes
[+] host called home, sent: 34 bytes
[+] established link to child session: 192.168.57.18

[DEVELOPERWS] Jamie.Grins/6984                                  last: 2s
beacon>
```

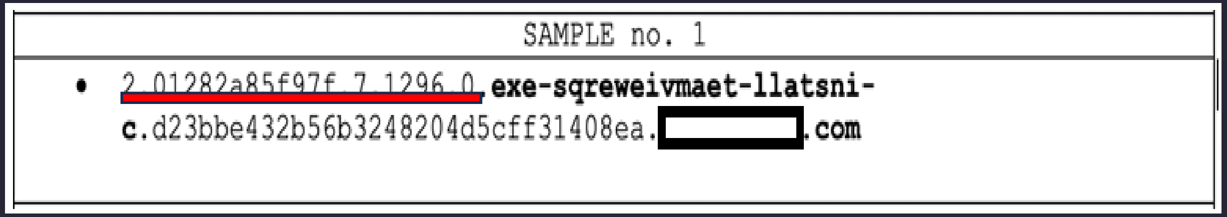


```
                o                       8         o   o
                8                       8             8
ooYoYo. .oPYo. o8P .oPYo. .oPYo. .oPYo. 8 .oPYo. o8  o8P
8' 8  8 8oooo8  8  .oooo8 Yb..   8    8 8 8    8  8   8
8  8  8 8.      8  8    8   'Yb. 8    8 8 8    8  8   8
8  8  8 `Yooo'  8  `YooP8 `YooP' 8YooP' 8 `YooP'  8   8
..:..:..:.....::..:.....::.....:8.....:..:.....::..::..:
::::::::::::::::::::::::::::::::8:::::::::::::::::::::::
::::::::::::::::::::::::::::::::::::::::::::::::::::::::


       =[ metasploit v3.3.3-release [core:3.3 api:1.0]
+ -- --=[ 481 exploits - 220 auxiliary
+ -- --=[ 192 payloads - 22 encoders - 8 nops
       =[ svn r7957 updated 261 days ago (2009.12.23)

Warning: This copy of the Metasploit Framework was last updated 261 days ago.
         We recommend that you update the framework at least every other day.
         For information on updating your copy of Metasploit, please see:
             http://dev.metasploit.com/redmine/projects/framework/wiki/Updating

msf >
```

SHODAN

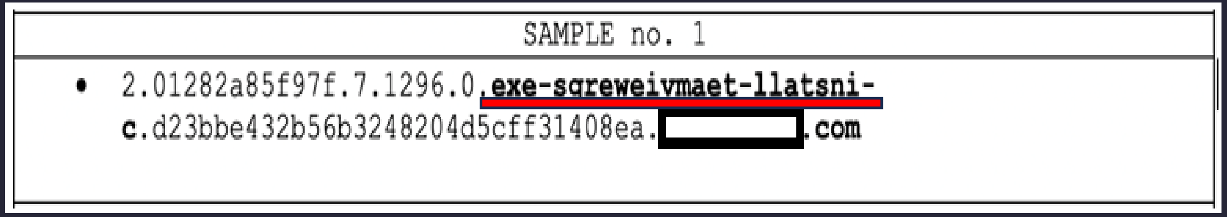
“Threat ‘intelligence’ & Attribution ”

Over 100,000 “DNS requests leaving the network and heading to an IP address in China. The domain had been recently “re-registered” to an individual in China..



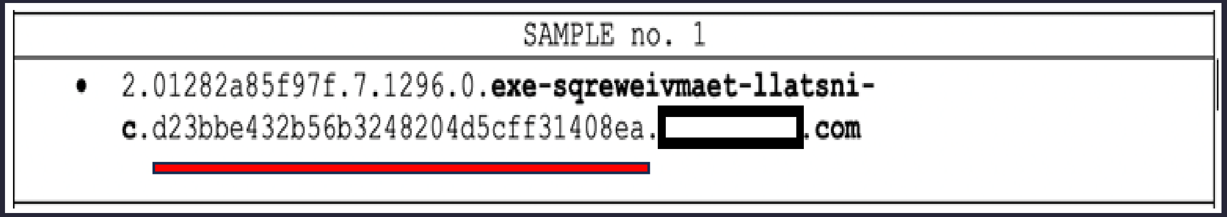
SAMPLE no. 1

```
• 2.01282a85f97f.7.1296.0.exe-sqreweivmaet-llatsni-
  c.d23bbe432b56b3248204d5cff31408ea.[redacted].com
```



SAMPLE no. 1

```
• 2.01282a85f97f.7.1296.0.exe-sqreweivmaet-llatsni-
  c.d23bbe432b56b3248204d5cff31408ea.[redacted].com
```



SAMPLE no. 1

```
• 2.01282a85f97f.7.1296.0.exe-sqreweivmaet-llatsni-
  c.d23bbe432b56b3248204d5cff31408ea.[redacted].com
```

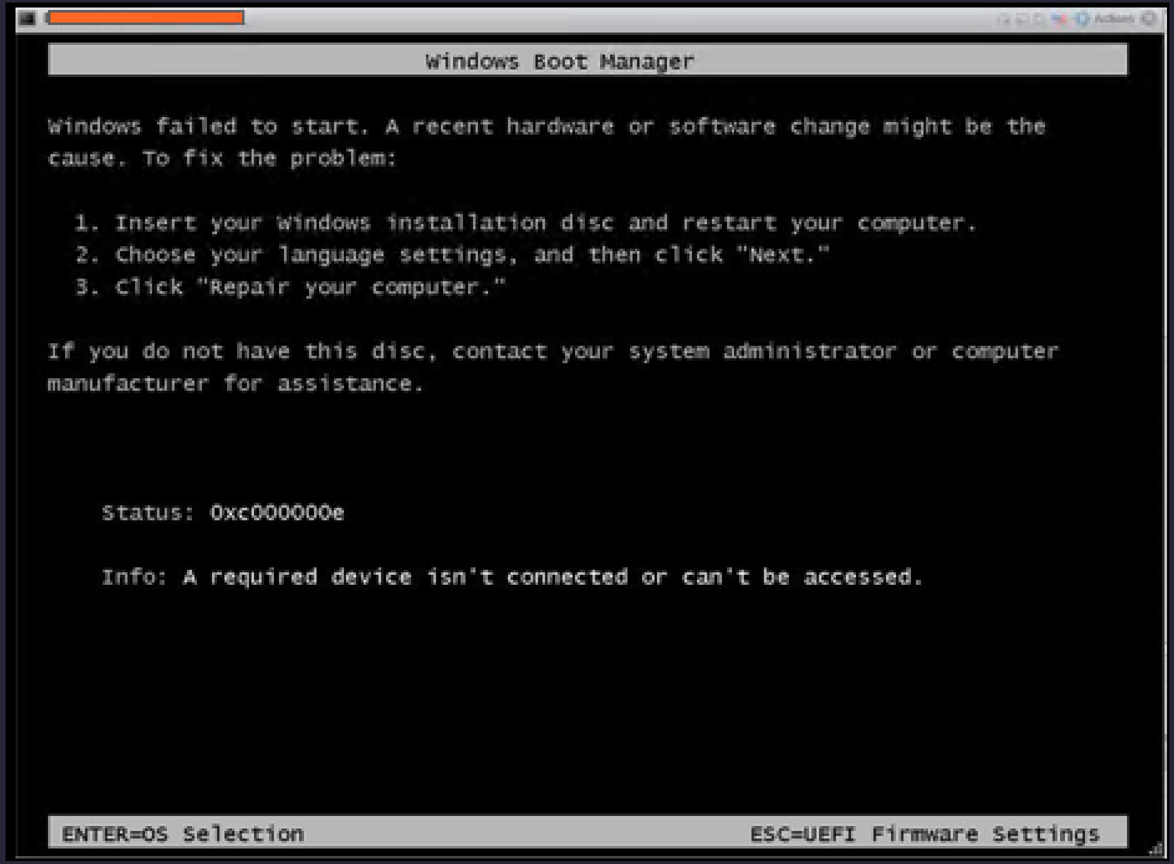
- Each DNS request had a unique number string at the start

- Followed by a file name, written backwards.

- Then a hash value, and finally the domain the data was being sent to.

“Backing up your false sense of security”

rightmove



```
                          Windows Boot Manager

Windows failed to start. A recent hardware or software change might be the
cause. To fix the problem:

  1. Insert your Windows installation disc and restart your computer.
  2. Choose your language settings, and then click "Next."
  3. Click "Repair your computer."

If you do not have this disc, contact your system administrator or computer
manufacturer for assistance.


    Status: 0xc000000e

    Info: A required device isn't connected or can't be accessed.



ENTER=OS Selection                                  ESC=UEFI Firmware Settings
```

- Your backups are a target for attackers, even the dimmest of the dumb.
- Most tape backups will recover at a maximum of 400mps, older tap systems can be as slow at 40mps.
- An 80TB (rough average size for a small network) would take 20 days just to get data of the tape drive.
- Now work out where you are going to put that 80TBs of data, especially if you are starting recovery while a CSIRT is still investigating.
- Getting to your backups should be the goal of your yearly red-team.

“Cyber insurance payday”

rightmove

- Ransom demand from the attacker - £1,000,000.
- Legal fees to a law firm in the UK to run due-diligence on the attackers and establish legal cover for making the payment - £50,000
- Fees to a “ransomware negotiation” company – they got a discount from the attackers as part of the service - £40,000 .
- “fluctuation” fee for the ransomware payment to be converted into bitcoin - £20,000.
- Fees to an external accountancy firm to liquidate the £1,000,000 – estimated at £30,000.
- Fees to a US Law firm for FBI notification – estimated at £40,000.
- Fees to an external “communications company” for share holders and media comments - £60,000 + undisclosed retainer fee for long term support.
- 240 hours of none retainer emergency response – £84,000.
- Over time for 3 weeks work to at least 20 staff – Estimated at £200,000
- 3 weeks loss of earnings, reported to be £300,000 per day – roughly £4,500,000 based on a 5 day working week over three weeks.

Total* £6,024,000

***This is a rough cost**

- New hyperconverged VMWare stack x3 - £360,000
- Active Directory audit and re-build - £80,000
- Network re-design, adding segmentation and SD-WAN integration - £40,000
- New hardware to support the new network, FWs, Switches (40GB upgrade) and multiple new ISP lines (estimated) - £1.6m (ongoing payments in the region of £100k per annum)
- Data recovery from end user laptops (consultancy) - £30,000
- Rushed migration to SharePoint online - £40,000
- Money put aside to deal with long term revenue loss: customers got offered huge discounts to keep them onside – Well over £250,000
- Loss of three IT staff: New hire fees, short term consultants fees, project manger fees – (estimated) £50,000+
- Cost to reputation – Priceless

Total* £2,450,000

***This is a rough cost**

rightmove

Thank you, any questions?