Cyber SA 2018:

A Netnographic Study on the Dark Net Ecosystem for Ransomware

Yara Bayoumy, Per Håkon Meland, Guttorm Sindre
SINTEF / NTNU
The (visible) Web

The Deep Web

The Dark Net
"57% of .onion sites are used to conduct transactions of illegal goods and services"

Ransomware

"a type of malicious software (short: malware) that demands payment in exchange for a stolen functionality"
Ransomware-as-a-Service (RaaS)
Data Gathered

Dream Market

Browse by category
- Digital Goods 50253
- Drugs 63238
- Drugs Paraphernalia 333
- Services 4371
- Other 3343

Exchange
- BTC 1.0
- mBTC 1000.0
- BCH 6.1
- XMR 40.3
- USD 9765.6
- EUR 7369.6
- GGP 6514.7
- CAD 13370.0
- AUD 1117.6
- mBTC 6150.0
- SEK 7734.9
- NOK 71118.6
- DKK 54019.8
- TRY 37835.9
- CHF 56009.4
- HKD 69121.1
- RUB 55284.3
- INR 598049.8
- JPY 961342.2

Onion mirrors
- jst6yvwxehehvd4.onion
- dk88yj3uvn4tw2.onion
- 7ep7eckunru2cw31.onion
- v3paapqimqf4jg.onion
- lg1h1mjxg33y5c.onion
- 6a09g8zq2heav.onion
- x587wmj9jy2w.onion
- bkhq2qmkoww.onion
- syjyclend2by22.onion
- nh358c6o69jg.onion
- k3s249257bnpa.onion

330 search results (0.8 seconds)

Filter:
- Ships to
- Ships from
- Escrow
- Category
- Cryptocurrency
- Search text: ransomware
- Sort by
- Vandor

1 2 3 4 5 6 7 8 9 10 11

5 BITCOIN RANSOMWARE>> EXPERIENCED BUYERS>2018
- $0.000154
- BitcoinFraudr (5200) (4.82x)
- US -> WW

6 BITCOIN RANSOMWARE EASY MONEY WORKING 2018
- $0.000049
- TopShellSales (4600) (4.54x)
- WW -> WW

6 BITCOIN RANSOMWARE EASY MONEY SYSTEM
- $0.000593
- TheWealthMaker (5500) (4.87x)
- WW -> WW

6 BITCOIN RANSOMWARE EASY MONEY
- $0.000593
- TheWealthMaker (5800) (4.87x)
- WW -> WW

6 BITCOIN RANSOMWARE EASY MONEY WORKING 2018
- $0.000049
- TopShellSales (1450) (4.54x)
- WW -> WW

6 BITCOIN RANSOMWARE EASY MONEY
- $0.000593
- TheWealthMaker (5500) (4.87x)
- WW -> WW

6 BITCOIN RANSOMWARE EASY MONEY WORKING 2018
- $0.000049
- TopShellSales (1450) (4.54x)
- WW -> WW
Cost data

Carbon Black Price (BTC) vs Research Price (BTC)

- ALM4
- FUD Ransomware + C & C
- Custom Stealer

Welcome @ Stoned100

We are from Germany and start about one year to use the Darknet.
We are active and verified Vendor with 5 Star rating in different markets.
And now we have our own DrugStore. Why we do this?
AlphaBay → Dreammarket

TNO Report 2017. Alphabay exit, Hansa-down: Dream on?
Cost: Only $200
C# FUD Ransomware (AES 256 Encryption with a 64 chars long uncrackable key)
C# Decrypter-Stub Size: 250kb (unique exe for each buyer)
Features: Delayed Start, Mutex, Task Manager Disabler. Platform: Windows (both x86 and x64)
We custom wrote our own ransomware and now its for sale to the public.
We have made huge amounts of BTC using ransomware and now you can too.
We give your everything you need + help to spread your ransomware.
Everyone who has bought this product has made their BTC back in 3 days or less.
Everything can be custom - any special requests just ask.
Comes with very easy n00b friendly instructions. You set price and time for ransom.
We are asking $200 for the amazing ransomware. Don't miss out. I don't think we will be selling at this price for very long. It's too cheap.
I have read about a ransomware, that injects into companies' computers via excel file. Usually through job application. Goldeneye is the name if I am not mistaken.

So how can I get it (or something simular)- and even better- if anyone knows a project paying commission for the job done? Have quite few "clients" who deserve to get ripped off a little bit.

I checked with Satan, but registration is turned off for now.

Thanks

hacking  ransomware
Summary

• Authors???
• Vendors are resilient, drug-based reputation
• Distributors – beware of n00bs and insiders

Limitations

• A lot of the services and goods are hoaxes
• Many forums are expensive/invite only
• Linguistic bias

Continued work

• Scale-up
• Archive data
• Outside Dark Net