A Glimpse Behind the Curtain: A Look into Crimeware-as-a-Service

Chester Wisniewski
Principal Research Scientist
Sophos
@chetwisniewski
A glimpse behind the curtain
• Explain how to get started
• Show crooks selling tutorials on VPNs, Tor, etc.
• Instruction manuals for cybercrime
• Will use Tor to live browse sites selling these guides
Safety First!

- How to stay safe using:
  - VPNs
  - Tor
  - Hidden mail services

<table>
<thead>
<tr>
<th>Product</th>
<th>Price</th>
<th>Buy Now</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hotspot Shield VPN Elite 5.20.2 + Patch</td>
<td>USD 2.06</td>
<td>[Buy Now]</td>
</tr>
<tr>
<td>Tails OS by Tor</td>
<td>USD 2.56</td>
<td>[Buy Now]</td>
</tr>
<tr>
<td>PUREVPN.COM - ★PREMIUM ACCOUNT★ [LIFETIME]</td>
<td>USD 12.57</td>
<td>[Buy Now]</td>
</tr>
<tr>
<td>AIRVPN.ORG - ★PREMIUM ACCOUNT★ [LIFETIME]</td>
<td>USD 3.55</td>
<td>[Buy Now]</td>
</tr>
</tbody>
</table>
Next slide is a demo – placeholder if network fails

- Crooks use stolen money to get started
- Show credit card marketplaces
- Show ads selling card thieving devices
- Leads to phishing slides showing how crooks acquire stolen card data. Apple phish slides will be shown after card info demo
Need seed money to start? Steal it.

[ Announcements ]

Tor Hidden Service Address Ready! :)

Our ONLY shop addresses are:

- redspic
- redspic
- thfcvte3vcf

**********************************************************************

[ 01:28:10 ]-[ 30-03-2017 ]---[ redspider ]---

Checker System Upgrade

Dear Members, from now on you will have 2 checker options - Try2check and CardOK. My personal recommendation is try2check for US & CA and card-ok for UK cards, but you should do as you know better. Also, if one checker is not responding or gives an error, you will be able to use the other one.

Fresh updates will come tonight.

[ 12:15:51 ]-[ 27-02-2017 ]---[ redspider ]---

Canada $60 premium bins are now $40

[ Prices Table ]

- [ Validity Rates for last 100 purchases ]-
  - UK Fulls :: 75% Valid
  - CA Fulls :: 82% Valid
  - US Fulls :: 71% Valid

---[ redspider ]---

- [ UK Full Info Cards ]--------
  - Fresh < 2 Weeks Old :: $30.00
  - Minimum Discounted Price :: $5.00

- [ CA Full Info Cards ]--------
  - Fresh < 2 Weeks Old :: $40.00
  - Minimum Discounted Price :: $7.00

- [ US Full Info Cards ]--------
  - Fresh < 2 Weeks Old :: $20.00
  - Minimum Discounted Price :: $5.00

---[ Discounts ]--------
  - More Than 2 Weeks Old :: 50%
  - More Than 4 Weeks Old :: 67%
  - DoB < 01.01.1995 :: 30%
  - Expires this or next month :: 50%

---[ Checker Service ]--------
  - Card Checker :: FREE
  - Refund Time :: 5/180 minutes

---[ redspider ]---
Need seed money to start? Steal it.
Need seed money to start? Steal it.

<table>
<thead>
<tr>
<th>Card Type</th>
<th>Card Number</th>
<th>Gender</th>
<th>Location</th>
<th>DOB</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>VISA</td>
<td>472409XXXXXXXXXXXX08/18 Female -/-</td>
<td>Edmonton</td>
<td>dob 10-1981</td>
<td>$40.00</td>
<td></td>
</tr>
<tr>
<td>VISA</td>
<td>450644XXXXXXXXXXXX12/19 Female -/-</td>
<td>st. john's</td>
<td>dob 08-1956</td>
<td>$40.00</td>
<td></td>
</tr>
<tr>
<td>VISA</td>
<td>450644XXXXXXXXXXXX07/19 Female -/-</td>
<td>Strathmore</td>
<td>dob 04-1995</td>
<td>$28.00</td>
<td></td>
</tr>
<tr>
<td>VISA</td>
<td>472409XXXXXXXXXXXX00/00 Male</td>
<td>New-Brunswick Campellton</td>
<td>150005108</td>
<td>$20.00</td>
<td></td>
</tr>
<tr>
<td>VISA</td>
<td>472409XXXXXXXXXXXX00/00 Female</td>
<td>Bc Surrey</td>
<td>6049899</td>
<td>$20.00</td>
<td></td>
</tr>
</tbody>
</table>
Afraid you will get ripped off? Do it yourself.
Where do card markets get their data?
Teach a man to phish...
ID theft plays a role
End with an expected outcome
Next slide is a demo – placeholder if network fails

- Return to demo here
- Show Tor search engines
- Show ads selling malware services
- Spamming as a service

- Next slides are backup
Search and you shall find

Search the DarkWeb Markets

Grams Search

I'm Feeling Lucky
Need help phishing?
Spamming is hard – Hire it out

Email Spam Service

<table>
<thead>
<tr>
<th>Author</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>SayWhat?</td>
<td>Features</td>
</tr>
<tr>
<td>Super Moderator</td>
<td>Random text in subject and letter</td>
</tr>
<tr>
<td></td>
<td>Attachment</td>
</tr>
<tr>
<td></td>
<td>Good inbox rate</td>
</tr>
<tr>
<td></td>
<td>Inbox Rate</td>
</tr>
<tr>
<td></td>
<td>My service is 100% Inbox depending on your</td>
</tr>
<tr>
<td></td>
<td>leads, letter, attachment and header you</td>
</tr>
<tr>
<td></td>
<td>need 80 to 90%</td>
</tr>
<tr>
<td></td>
<td>Price and Payment</td>
</tr>
<tr>
<td></td>
<td>Price is 2$/Lk leads with minimum order 100k</td>
</tr>
<tr>
<td></td>
<td>leads. Only BTC is accepted.</td>
</tr>
<tr>
<td></td>
<td>How can I track my campaign?</td>
</tr>
<tr>
<td></td>
<td>You can track through clicks on link you</td>
</tr>
<tr>
<td></td>
<td>provide</td>
</tr>
<tr>
<td></td>
<td>Rules</td>
</tr>
<tr>
<td></td>
<td>1) I only send mail, leads and letter you</td>
</tr>
<tr>
<td></td>
<td>provide.</td>
</tr>
<tr>
<td></td>
<td>2) Except child porn everything is accepted.</td>
</tr>
<tr>
<td></td>
<td>3) Escrow is more than welcome but im forum</td>
</tr>
<tr>
<td></td>
<td>staff.</td>
</tr>
<tr>
<td></td>
<td>4) Don’t offer me any percentage of your</td>
</tr>
<tr>
<td></td>
<td>affiliate i don’t need it.</td>
</tr>
<tr>
<td></td>
<td>5) If your attachment is a malware it should</td>
</tr>
<tr>
<td></td>
<td>be 100% FUD i won’t be responsible for inbox</td>
</tr>
<tr>
<td></td>
<td>rates.</td>
</tr>
<tr>
<td></td>
<td>Contact: PM ME for my jæber ID</td>
</tr>
</tbody>
</table>

Posts: 102
Joined: Sep 2014
Reputation: 9
Jabber:
Next slide is a demo – placeholder if network fails

- Demo document exploit building kits
- Next slide is backup
Exploiting with a GUI

**MACRO EXPLOIT BUILDER**

- Silent DOC Exploit - one file v1 2007
- Macro DOC Exploit - Unlimited
- FUD
- Advanced support
- Updates
- Pay Now

**SILENT EXPLOIT BUILDER**

- Silent DOC Exploit - Unlimited
- Macro DOC Exploit - Unlimited
- FUD or almost FUD
- Advanced support
- Updates
- Pay Now

**OFFENSIVE WARE Multi Exploit Builder**

- N1: Editable Macro DOC
- N2: PDF Open Action (Adobe 8.9+)
- N3: IE 9-11 Godmode HTML CVE-2016
- N4: Custom Ext Exploit (OMX)
- S1: VBS Exploit
- S2: JS Exploit
- S3: OHM Exploit
- S4: HTA Exploit
- S5: Semi-Silent Doc
- X1: Silent DOC (CVE-2015-2545 + SEMI)
- V1: Silent DOC (CVE-2010-3333)
- V2: Silent DOC (CVE-2012-0158)
- Auto-Refud Big Output (v2)

**Exploit available in this license plan**
Show me the money

We’ve learned what we need, proceed to cash in
Next slide is a demo – placeholder if network fails

- Demo botnet command and control
- Demo Satan RaaS website/service
- Next slides are backup
- Slides on other RaaS will be shown
What is Satan?

Apart from the mythological creature, Satan is a ransomware, a malicious software that once opened in a Windows system, encrypts all the files, and demands a ransom for the decryption tools.

How to make money with Satan?

First of all, you’ll need to sign up. Once you’ve sign up, you’ll have to log in to your account, create a new virus and download it. Once you’ve downloaded your newly created virus, you’re ready to start infecting people.

Now, the most important part: the bitcoin paid by the victim will be credited to your account. We will keep a 30% fee of the income, so, if you specified a 1 BTC ransom, you will get 0.7 BTC and we will get 0.3 BTC. The fee will become lower depending on the number of infections and payments you have.
Even crooks use 2FA

authenticate

-----BEGIN PGP MESSAGE-----
Version: GnuPG v1

hQMA01VcdFf90QAQ/9HlsT59zopXjQuEdy4Bev4tJnXAEiMoi812cOYkcTCc
rgkqwpye4u/1Sbw6hltIHi9ak3VJEd4MVLsQyV24UgrHvU/mmi5row5/rbK8
Cawg9YFeAE8vFgrwceYNEdGd92bgFX8tEu3hcvby3EWwxGULxHwWY75W/TeY
kikuNzZyF1wssP4kjqPMv1MsXytWfIYs0pX3kID+DxCBYmK0W0lgEWQf5e5r
Z+52AFgwP1bEKVUJ7FeUQeIOkOzwflCsd7fWEWafMqZ3IsyoJzrI9j4yGE5la
CE7161687/G+tv5ISCC2N/kcS8frSIW6DC6h0D5oDV3i2/WID+0Sn?Yw+G0en8S

Decrypted secret

Secret

Authenticate

Forgot your password?
Crowdsourced translations

Translation guidelines

1. All fields must be filled.
2. Anything between "%" should be only copied and not translated.
3. The field "English" should be filled with the name of the language you're translating (e.g. Deutsch, Español).
4. The characters used must be UTF-8 supported.
5. Only one translation is allowed per day.

The translations are manually checked and added once a day. Duplicates are ignored.

Languages already translated to:

English / Português

Your personal files have been encrypted. In order to decrypt them you'll have to pay %RANSOM% BTC

SOPHOS
The translations are manually checked and added once a day. Duplicates are ignored.

Languages already translated to:

English / Português / ภาษาไทย / Deutsch / Italiano / Español / Русский / Latviski

The translations are manually checked and added once a day. Duplicates are ignored.

Languages already translated to:

English / Português / ภาษาไทย / Deutsch / Italiano / Español / Русский / Latviski / Français / 中文

The translations are manually checked and added once a day. Duplicates are ignored.

Languages already translated to:

English / Português / ภาษาไทย / Deutsch / Italiano / Español / Русский / Latviski / Français / 中文 / Dutch / Romanian / Lithuanian

The translations are manually checked and added once a day. Duplicates are ignored.

Languages already translated to:

English / Português / ภาษาไทย / Deutsch / Italiano / Español / Русский / Latviski / Français / 中文 / Dutch / Romanian / Lithuanian / Eesti
You are running the trial version of our service. You may only load 20 users. Click here to purchase.

Download binary (*.EXE)

Global build
- 29/01/2017 12:29 PM

Your build
- 01/01/1970 01:00 AM

Campaign ID
- Generic (Demand: 0.4 BTC)

Information
Distribute the binary file over the internet and earn bitcoins from successful ransom payments.

Users will appear in the installs page when they successfully execute the binary file.
Open a support ticket

- About my account

What's your problem?

Create ticket
Dot Ransomware

We are selling our source code for 500$.
If you want to buy it then write new ticket to us.

What is this? This is Ransomware-as-a-Service.
We are ready to cooperate.

- Easy setup.
  Setup takes 5 minutes and very easy with our builder.

- High rates.
  You will get 50% of decryption price to your bitcoin wallet.

- Low requirements.
  Works fine on all systems beginning with Windows XP.
Cashing out

Time to do the laundering
Making a Bitcoin smoothie
- Show a few Bitcoin tumblers
- Explain how stolen goods play a role by showing Tor Warehouse site
- Need to escape? Buy a passport/Uber/airline ticket – Live demo using Tor search
- Explain the jail sentences – Not for the faint of heart
- Next slides are backup -
Finding the right blender
Grab some goodies

Welcome to The Greatest Carded Merchandise Store on Tor.

Spring is here. So is $7.

If you have any questions, contact us on TorWarehouse@Lalantos.org anytime.

Trust us. 100% Satisfaction Guaranteed. Click here to read the FAQ or select an item below.

- from $399
- $199
- from $299
- $199
- from $799

Frequently Asked Questions

Why are your products so cheap?

The reason behind our pricing structure becomes easy to understand once you are aware of the ways these products are obtained: by buying them from thieves in physical locations (in some cases) or carding on popular internet marketplaces (most of the time). Stealing is self-explanatory; carding, on the other hand, is an activity of using stolen Credit Card or PayPal details to order items from the aforementioned marketplaces. Effectively, we are able to obtain many popular items of merchandise at a fraction of their actual retail price.

Then why don’t you just sell these items for full price on eBay instead?

As you may already be aware, our website exists on the Tor network whereas eBay and other similar marketplaces belong on the clearnet, otherwise known simply as the World Wide Web. Dealing on the clearnet is equal to exposing oneself, which is obviously undesirable in this case – lots of unaccounted merchandise is a certain giveaway of illegal activities. The Tor network allows for a high level of anonymity and enables us to receive many more items and store them away from the eye of law enforcement. It also allows us to sell in much higher quantities, therefore selling them as quickly as possible is a logical choice - nobody will buy a stolen item for the full price and likewise we will profit more by selling cheaply and in bulk.

“...you guys are phenomenal. After getting scammed a few times on Amazon I was being very sceptic, but what the hell. News time for some more unboxing therapy!”

“...was getting worried you will not deliver. After ordering a Mac Mini for my son and not getting it on time, I swore the dark web off altogether. Good luck now, Mentor for life.”
Get away while looking good

- Bulgaria - Passport Scans
  - Price: $5.56
  - Views: 1286

- China - Passport Scans
  - Price: $5.56
  - Views: 1826

- Estonia - Passport Scan
  - Price: $5.56
  - Views: 983

- Indonesia - Passport Scans
  - Price: $5.56
  - Views: 629

- Ireland - Passport Scan
  - Price: $5.56
  - Views: 350

- Breitling Watch - Blue/Silver/Gold - Authentic Replica
  - Price: $135.47
  - Views: 236

- Polo caps
  - Price: $15.47
  - Views: 4241

- Mont Blanc Starwalker Doué Fineliner (Replica)
  - Price: $29.47
  - Views: 3790

- Armani Black Pyjamas Size XL
  - Price: $31.77
  - Views: 15881
  - Also available: Ralph Lauren lounge suit navy blue XXL: $31.77, Ralph Lauren lounge suit navy blue XL: $31.77

- Ralph Lauren Tracksuit hooded L
  - Price: $31.77
  - Views: 69240
  - Also available: Ralph Lauren lounge suit navy blue XXL: $31.77, Ralph Lauren lounge suit navy blue XL: $31.77
Get to the airport

🌟 The Ultimate UBER Package 🌟 Get UNLIMITED Free Rides ☞ Make $3,000+ a Month as Fake Uber Driver


Also available:

- Antidetect FF Browser – The MONEY MAKER! Worth over 400$!!! Get it Now!!! + Lifetime VPN + PayPal, USD 3.60
- Antidetect FF Browser – The MONEY MAKER! Worth over 400$!!! Get it Now!!! + Lifetime VPN + PayPal, USD 3.60
- ★ NSA HACKING - FORENSIC TOOLKIT ★ + FREE BONUS 11 FBI FORENSIC TOOLS ★ BEST FORENSIC PACK on the Ma, USD 3.60
- THE TERMINATOR PACK 37,000 ITEMS ▶ GUIDES ▶ TEMPLATES ▶ SOFTWARE ▶ E-whore/Pornleech, USD 7.60
- ►THE CARDER'S HOLY GRAIL -Antidetect 6.5 -Fraud Browser -Socks5/Proxy+VPN -List of Bins -Worth $550!, USD 7.60
- ►THE CARDER'S HOLY GRAIL -Antidetect 6.5 -Fraud Browser -Socks5/Proxy+VPN -List of Bins -Worth $550!, USD 7.60
Why buy a ticket? Take one.
Don’t do this at home

- Thugs who sent Brian Krebs heroin and a SWAT team sentenced
- Celebgate hacker who stole nude photos gets nine months in jail
- Man who hacked 130 celebrities jailed for five years
- Italian pair arrested over alleged hack of cardinals and masons
- Rogue admin jailed after taking down former employer’s network
Yahoo! yahoo arrested – Karim Baratov
LinkedIn, Dropbox & prison

Put your hands on the table!
What to do?

Next steps, risks and advice
Lessons learned

- No one is too small – commodification makes us all targets
- Effective defence must understand underground trends
User education

- Training not perfect, well worth doing
- Change the goals – Reduce clicks, but increase reports to security team
Low-hanging fruit

- Patch speed and thoroughness critical
- Know what you have – not just products, but requirements
Stay vigilant

- Keep an eye on the dark web!
- Recognize when your employees or customers are targeted and take protective actions
Thank you!

Questions?

Chester Wisniewski

chesterw@sophos.com

@chetwisniewski