

DiamondFox modular malware – a one-stop shop

 blog.checkpoint.com/2017/05/10/diamondfox-modular-malware-one-stop-shop/

May 10, 2017



Check Point researchers have conducted a thorough investigation of the DiamondFox malware-as-a-service in collaboration with Terbium Labs, a Dark Web Data Intelligence company. The report includes a review of the malware's sales procedure and customer reviews, as well as a full technical analysis of its multiple plugins. For the full DiamondFox report [click here](#).

Check Point Threat Intelligence teams constantly track the latest attack trends, campaigns and attack methods to maintain an up-to-date and accurate view of the cyber threat landscape.

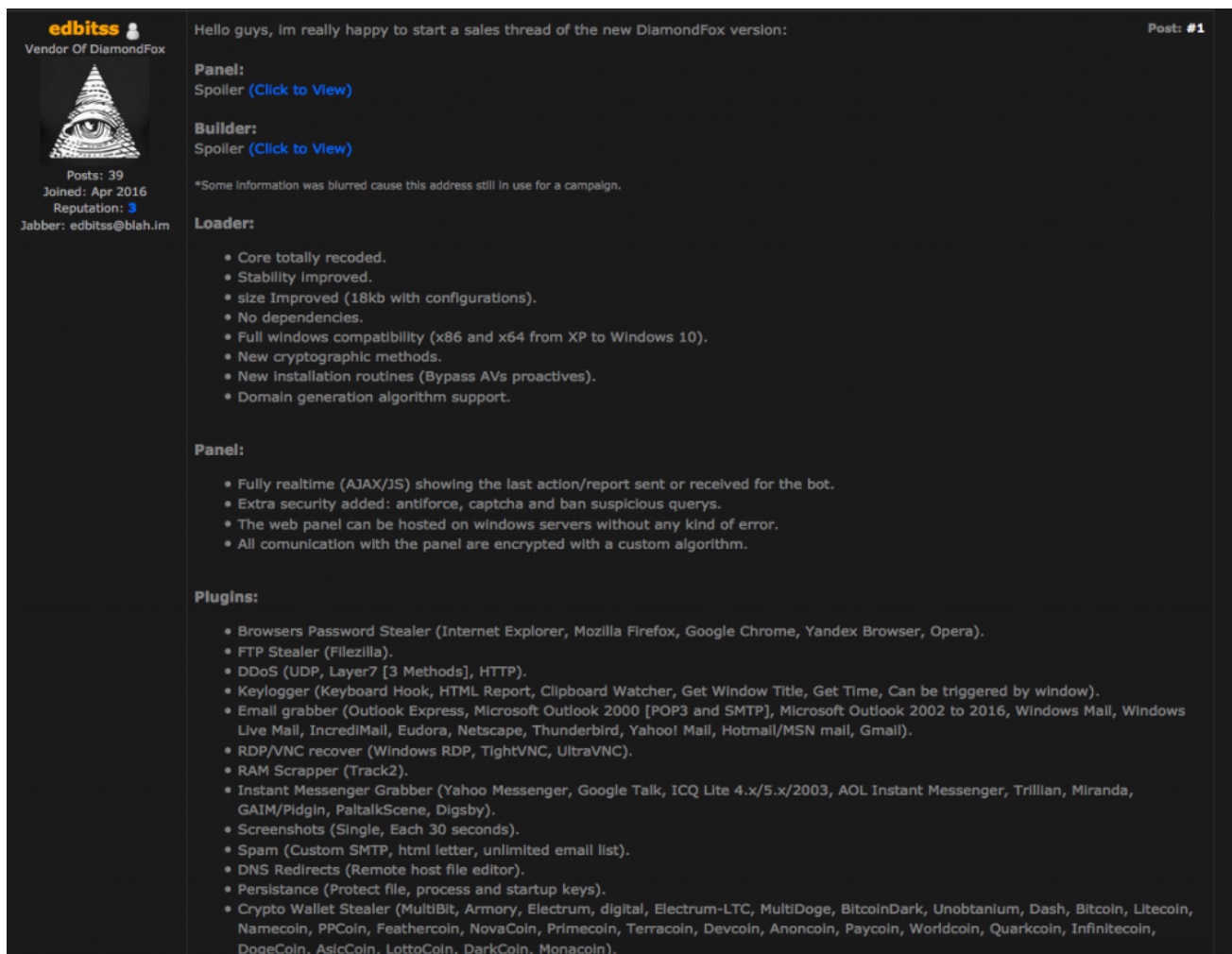
In recent years, an effective new business method has penetrated the thriving malware and attack tools market and led to the establishment of an entire industry – malware-as-a-service. This provides unskilled threat actors an easy entrance to the cyberattack world, and enables each user to start their own attack campaign without any technical knowledge. Drive-by attack methods, ransomware, banking Trojans and a variety of attack tools are now traded in underground forums and use a wide range of payment methods.

DiamondFox, a modular botnet offered for sale on various underground forums, is an outstanding demonstration of the many advantages of this business module. By purchasing a single product, the buyer is granted access to a variety of capabilities, in the form of plugins, and can plan and execute multiple campaigns: a tailored espionage campaign, a credentials theft campaign, which can be the basis of an extensive monetary theft operation, and even a simple, yet highly effective distributed denial of service (DDoS) attack.

Together with Terbium Labs, a Dark Web Data Intelligence company, we reviewed the DiamondFox malware's capabilities, sales procedure and user experience. This report also includes a full technical analysis of the malware's functionality, network communications and multiple plugins.

Malware ecosystem

Looking at the full list of capabilities of the latest version of DiamondFox, the Crystal version, this highly modular malware seems to cover everything from keylogging and browser password stealing, all the way to a variety of Distributed Denial of Service (DDoS) attack techniques through crypto currency wallet stealing. DiamondFox, one of the trendiest malware-as-a-service up for sale these days, is in fact a one-stop-shop: upon purchasing the malware for a certain period, a selection of plugins becomes accessible. All that's left for the buyer to do is to choose which one to activate for each victim and when.



edbitss
Vendor Of DiamondFox

Posts: 39
Joined: Apr 2016
Reputation: 3
Jabber: edbitss@blah.im

Hello guys, im really happy to start a sales thread of the new DiamondFox version: Post: #1

Panel:
Spoiler ([Click to View](#))

Builder:
Spoiler ([Click to View](#))

*Some Information was blurred cause this address still In use for a campaign.

Loader:

- Core totally recoded.
- Stability Improved.
- size Improved (18kb with configurations).
- No dependencies.
- Full windows compatiblility (x86 and x64 from XP to Windows 10).
- New cryptographic methods.
- New installation routines (Bypass AVs proactives).
- Domain generation algorithm support.

Panel:

- Fully realtime (AJAX/JS) showing the last action/report sent or received for the bot.
- Extra security added: antiforce, captcha and ban suspicious queries.
- The web panel can be hosted on windows servers without any kind of error.
- All communication with the panel are encrypted with a custom algorithm.

Plugins:

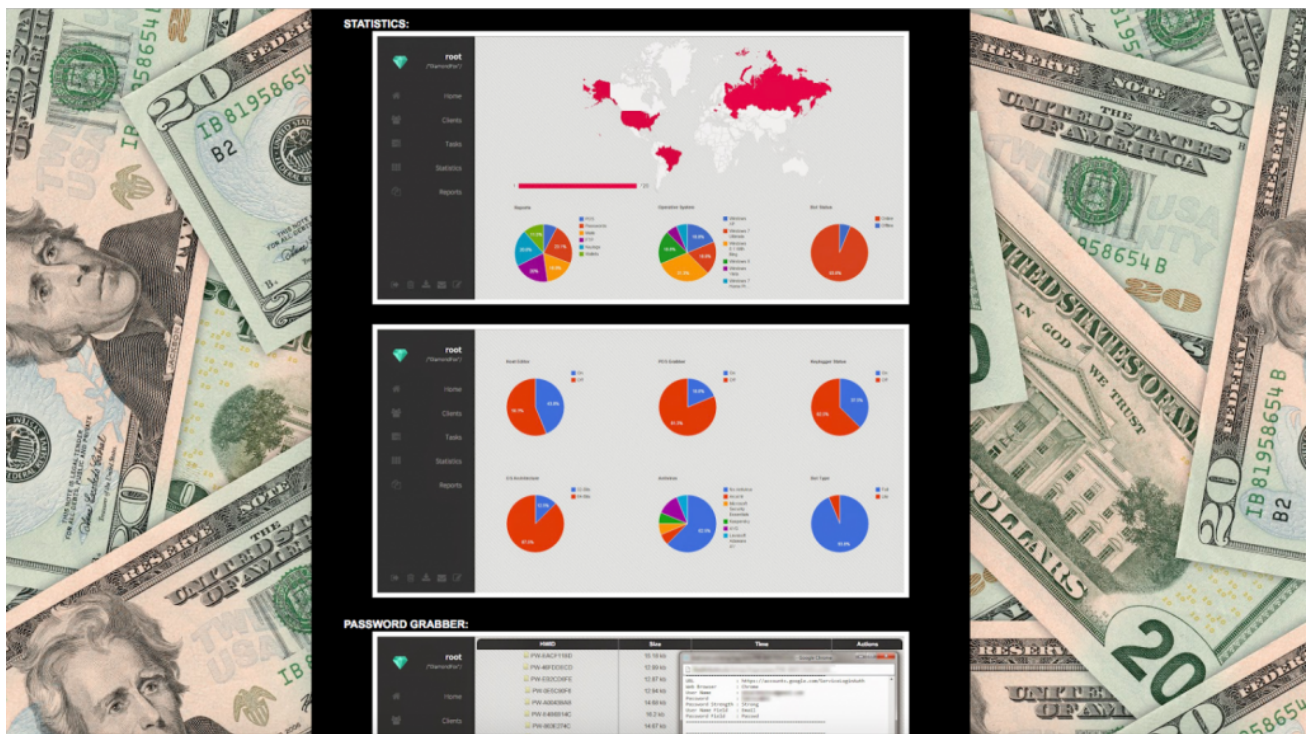
- Browsers Password Stealer (Internet Explorer, Mozilla Firefox, Google Chrome, Yandex Browser, Opera).
- FTP Stealer (Filezilla).
- DDoS (UDP, Layer7 [3 Methods], HTTP).
- Keylogger (Keyboard Hook, HTML Report, Clipboard Watcher, Get Window Title, Get Time, Can be triggered by window).
- Email grabber (Outlook Express, Microsoft Outlook 2000 [POP3 and SMTP], Microsoft Outlook 2002 to 2016, Windows Mail, Windows Live Mail, IncrediMail, Eudora, Netscape, Thunderbird, Yahoo! Mail, Hotmail/MSN mail, Gmail).
- RDP/VNC recover (Windows RDP, TightVNC, UltraVNC).
- RAM Scrapper (Track2).
- Instant Messenger Grabber (Yahoo Messenger, Google Talk, ICQ Lite 4.x/5.x/2003, AOL Instant Messenger, Trillian, Miranda, GAIM/Pidgin, PaltalkScene, Digsby).
- Screenshots (Single, Each 30 seconds).
- Spam (Custom SMTP, html letter, unlimited email list).
- DNS Redirects (Remote host file editor).
- Persistence (Protect file, process and startup keys).
- Crypto Wallet Stealer (MultiBit, Armory, Electrum, digital, Electrum-LTC, MultiDoge, BitcoinDark, Unobtanium, Dash, Bitcoin, Litecoin, Namecoin, PPCoin, Feathercoin, NovaCoin, Primecoin, Terracoin, Devcoin, Anoncoin, Paycoin, Worldcoin, Quarkcoin, Infinitecoin, Dogecoin, AsicCoin, LottoCoin, DarkCoin, Monacoin).

DiamondFox advertisement, dated April 2016

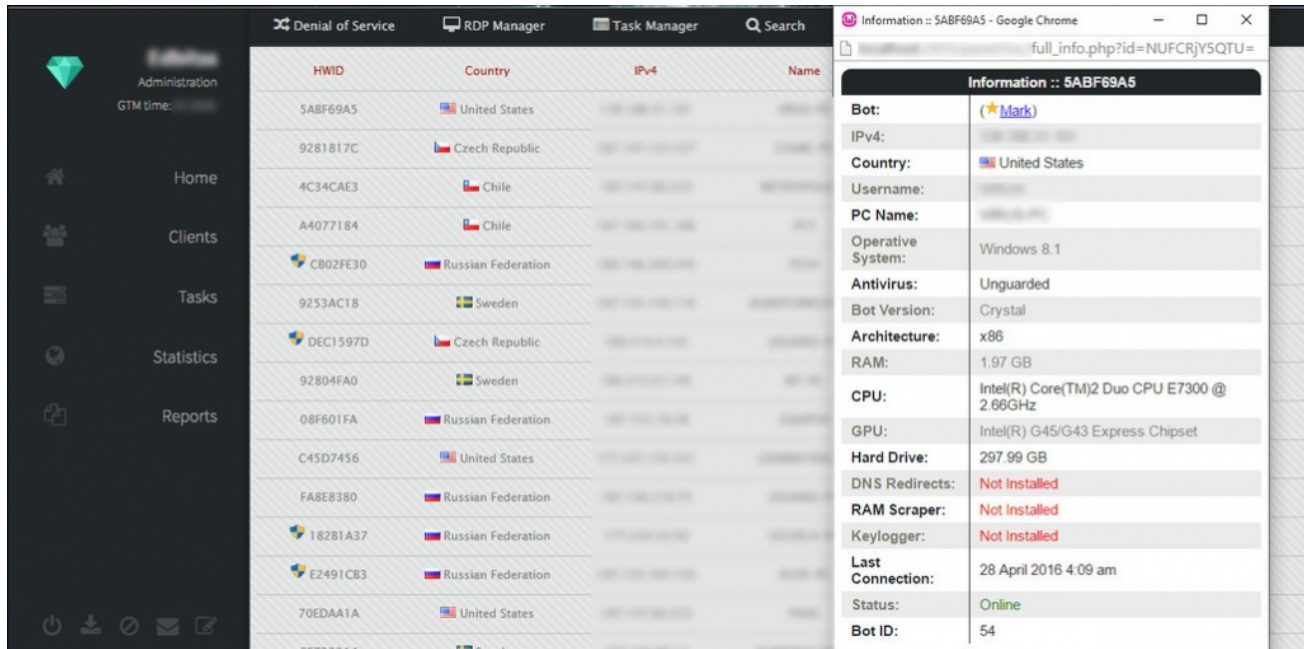
The ad displayed above, which presents the latest version of DiamondFox, includes a detailed explanation about the malware loader, the user panel and the actual core of DiamondFox – the plugins.

It also includes a carefully updated Changelog, which provides the potential buyers a detailed explanation about the improvements and features added to each of the versions.

At this point, after examining the highly successful Cerber Ransomware-as-a-service and the user-friendly Sundown Exploit Kit, there is no need to elaborate about the management panel granted to each user who purchases the malware. It goes without saying that the DiamondFox user panel is comprehensive and secured, and provides users real-time infection statistics as well as control over the activation of the plugins. Moreover, most of the DiamondFox advertisements guarantee free updates and support.

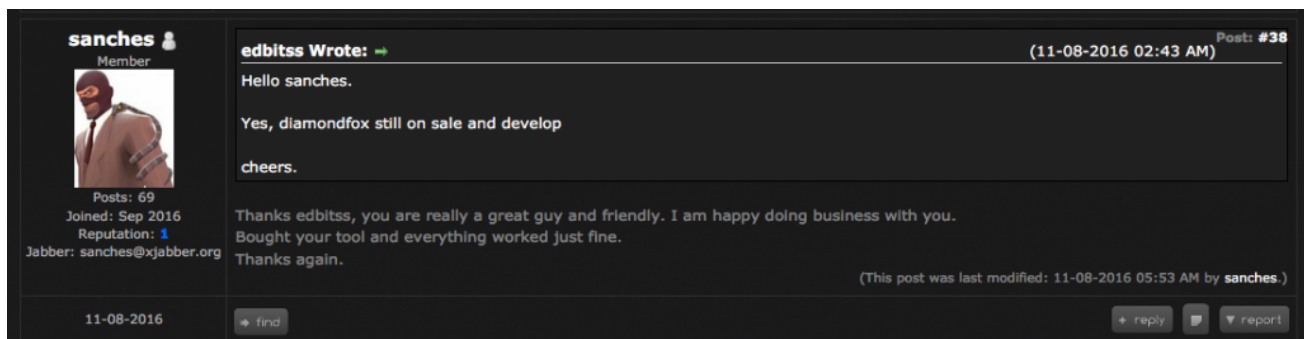


DiamondFox user panel screenshots



DiamondFox user panel screenshots, single victim view

So far, the DiamondFox botnet seems like the perfect solution for any actor seeking an easy way to initiate their own campaigns. DiamondFox offers a range of plugins, which provide the user several data theft possibilities, and the ability to self-spread via removable devices and social networks. DiamondFox can definitely be used as the basis of a monetary theft operation, or a tailored espionage campaign. Furthermore, it appears that the official malware vendor, an actor dubbed 'Edbitss', is truly invested in the improvement of the malware, as all updates, changes and fixes are carefully documented and shared with the potential buyers. Edbitss is clearly very responsive in all of the observed threads. Several customer reviews validate this impression and describe a quality, fully functioning product:



DiamondFox customer review

However, other reviews tell an entirely different story:

03-30-2016, 02:56 PM Post: #7

Conceal  

Prestige: 78
Posts: 346
Joined: Dec 2014
Reputation: **210**

Syria Wrote: (03-30-2016 02:51 PM)
It is not allowed here,
and the botnet is complete sh*t

Yeah, I'd agree. Sorry to trash it, but it's not very good.

The DDOS attack methods are far unstable, and the panel is rather ugly. The FG features aren't on-point either.

Private message me for my contact information.

PM Find TS **Quote Q+ Report**

DiamondFox customer review

We can't help but wonder which side is telling the truth.

As mentioned previously, *Edbitss* is the official DiamondFox vendor, based on evidence from the ads referred to in this report. The actor uses the same Jabber address in all of the observed ads, both on the clear web and on the Darknet: [\[email protected\]](#). However, different contact details were observed throughout the various ads, each using a top level domain linking the actor to another country. The actor claims to be located in Russia and appears to be fluent in Russian. However during the investigation, we came across a clear web landing page established by the actor in March 2016, on the domain 'blogspot.mx', the Mexican website of the highly popular blog-publishing service. From this, there is a high possibility the actor could live in Mexico.

Check Point customers are protected from DiamondFox by the following security technologies:

- The **Antivirus Software Blade** blocks every currently known variant of DiamondFox.
- The **Anti-Bot Software Blade** detects and blocks any attempt to communicate with DiamondFox's C&C addresses.
- Indicators of Compromise are provided in the [DiamondFox report](#) and the [detailed Appendices](#).