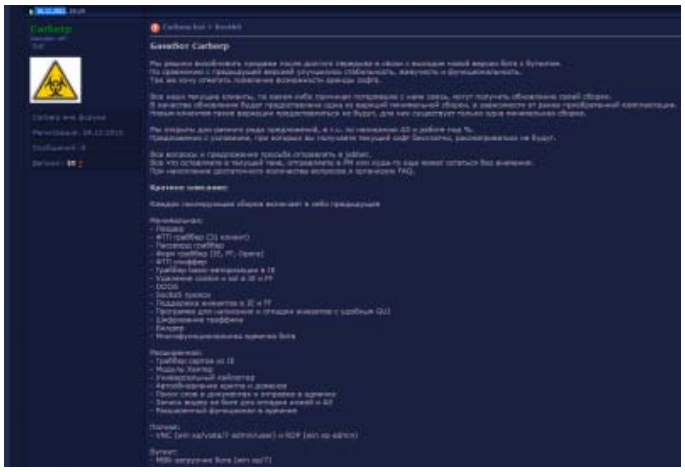
# Group-IB: Banking trojan «Carberp» sales were reborn with bootkit module

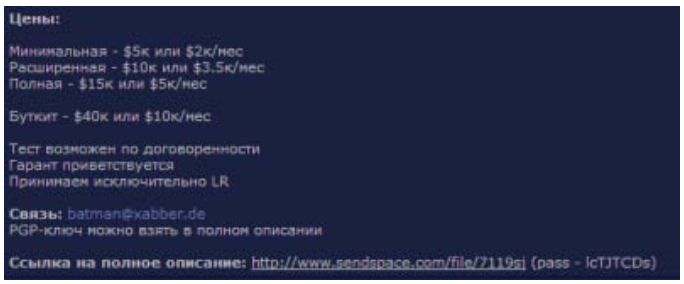
*(Translated from the original Italian)*

During the last week introduced you the excellent work done by the Group-IB, a security firm resident of the Moscow-based Skolkovo Foundation that has received a grant in the amount of 30m rubles (approximately $966,000) for the development of a global counter-cybercrime system named the CyberCop.

It was for me the opportunity to receive many interesting information of the evolution of cybercrime phenomena … today I desire to propose a exclusive… Banking trojan «Carberp is back again and Group-IB researchers have provided me the evidences.

Threat Intelligence Team discovered that after big pause Carberp sales were reborn in underground, which means that massive wave of online-banking thefts will begin close to New Year time.






Following the message posted in the forum:

> «We decided to reborn the sales after long pause because of the development of new Carberp version with bootkit module. If we compare with last version, we make stability, durability and functionality. Additionally we started to provide the opportunity of rent of our malware.
>
> All of our current clients, for whatever reason, have lost touch with us, can upgrade their assembly. As an update will be given one of varitsy minimal assembly, according to previously purchased a complete set.
>
> We won't provide such variants to new clients, for them we will provide 1 minimal pack. We are open to any kind of proposals, especially for writing of WEB-injects under %.
>
> We can't provide the malware for free on any conditions.
>
> All requests and questions please send to jabber.

# Group-IB: Banking trojan «Carberp» sales were reborn with bootkit module

All you send to this topic, send to PM or anywhere else, can stay without any attention.

If I have with a lots of questions, I will make a FAQ for all.

Brief description:

All new build will include all from the previous.

Minimal:

- Loader
- FTP password grabber (31 clients are supported)
- Password grabber
- Form grabber (IE, FF, Opera)
- FTP sniffer
- BASIC-authorization grabber for IE
- Cookie and sol deleted module for IE and FF
- DDOS
- Socks5
- Support of WEB-injects for IE and FF
- Special GUI tool for writing WEB-injectied
- Traffic encryption
- Builder
- Multifunctional multipanel

Extended:

- Certificated grabber from IE
- «Hunter» module
- Universal keylogger
- Crypt algo and logs updater
- Keywords search in files and upload them to the administrative panel
- Video recording on the bot and web-injected debugging
- Additional functions in web-panel

**Full**:

- VNC (win xp/vista/7 admin/user) and RDP (win xp admin)

Bootkit:

Prices:

Minimal - $5к or $2к/month

Extended - $10к or $3.5к/month

Full - $15к or $5к/month

Bootkit - $40к or $10к/month

We are ready to do test up to negotiations.

Garant is welcome.

We accept only LR

Full specification: http://www.sendspace.com/file/7119sj (pass - lcTJTCDs)

The most interesting is new bootkit module, the price of which is 40 000 USD or 10 000 USD on rent per month. It helps to infect MBR record which means that the hacker will have long term opportunity to control the victim without antivirus notifications.

The new thread from Carberp vendor on one of private underground forums called «verified.ms» was created for anonymization the seller uses GPG-key and Jabber contact.

The malware sellers started to use new scheme of Carberp sales by the opportunity of its rent, which was popular in selling of very qualified written and professional banking malware from very old famous underground networks called «RATNET» (valenok and htum were one the most famous vendors of professional private banking spyware for US and Canadian banks).

# Group-IB: Banking trojan «Carberp» sales were reborn with bootkit module

The sales model known as "malware as a service" is very dangerous because it open the doors to ordinary crime that without particular knowledge could move serious attacks against banking systems.

Sellers also started to provide special service of individual «web-injects» development for major US and CA banks such as WellsFargo, Citi, JP Morgan Chase, Bank of America, TD Bank and many others. Previously, Zeus and SpyEye, the Carberp Trojan program is primarily used to target online banking customers from Russia and other Russian-speaking countries like Ukraine, Belarus or Kazakhstan.

In June 2012, Group-IB provided assistance with forensic investigation and analysis to the Ministry of the Interior, and ESET researchers helped with the analysis of malicious software used by the Carberp gang, after which six more gang members held (http://blog.eset.com/2012/06/04/carberp-and-hodprot-six-more-gang-members-held).

It must be considered that banking system is a vital component of any countries, it represents a critical infrastructure that governments have to preserve with a proper cyber strategy.

Cyber criminals, but also hacktivists, state-sponsored hackers and cyber terrorists could be interested to attack banking for various purposes, for this reason it is crucial the monitoring of cyber underground and the detecting of initiative such as the one described in this article to not be caught unprepared by the cyber threat ... we cannot afford it.

Pierluigi Paganini

References

http://securityaffairs.co/wordpress/11084/hacking/korean-cyber-espionage-campaign-against-russia.html