

FortiGuard



Threat Research and Response

Up to Date on the Threat Landscape

- FortiGuard Introduction
- Threat Landscape Update
 - Cyber Criminal Organizations
 - Services
 - Modern Malware

Derek Manky
Sr. Security Strategist

FORTINET



World Wide Coverage - FortiGuard Distribution Network (FDN)

Antivirus

Web Filtering

Fortinet Analysis & Management Service (FAMS)

Intrusion Prevention

Antispam

Application Control

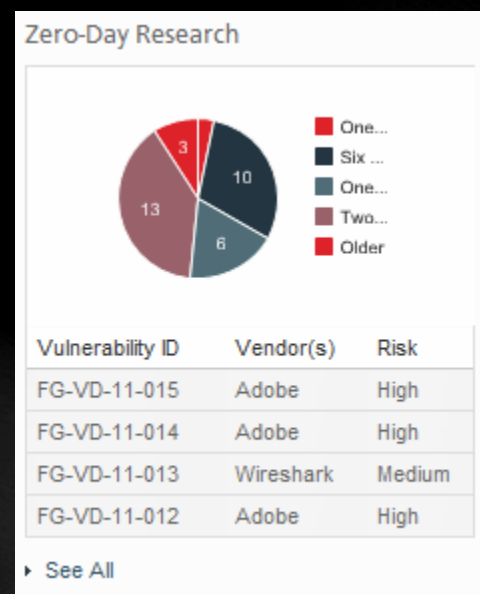
Database Security

Web Security

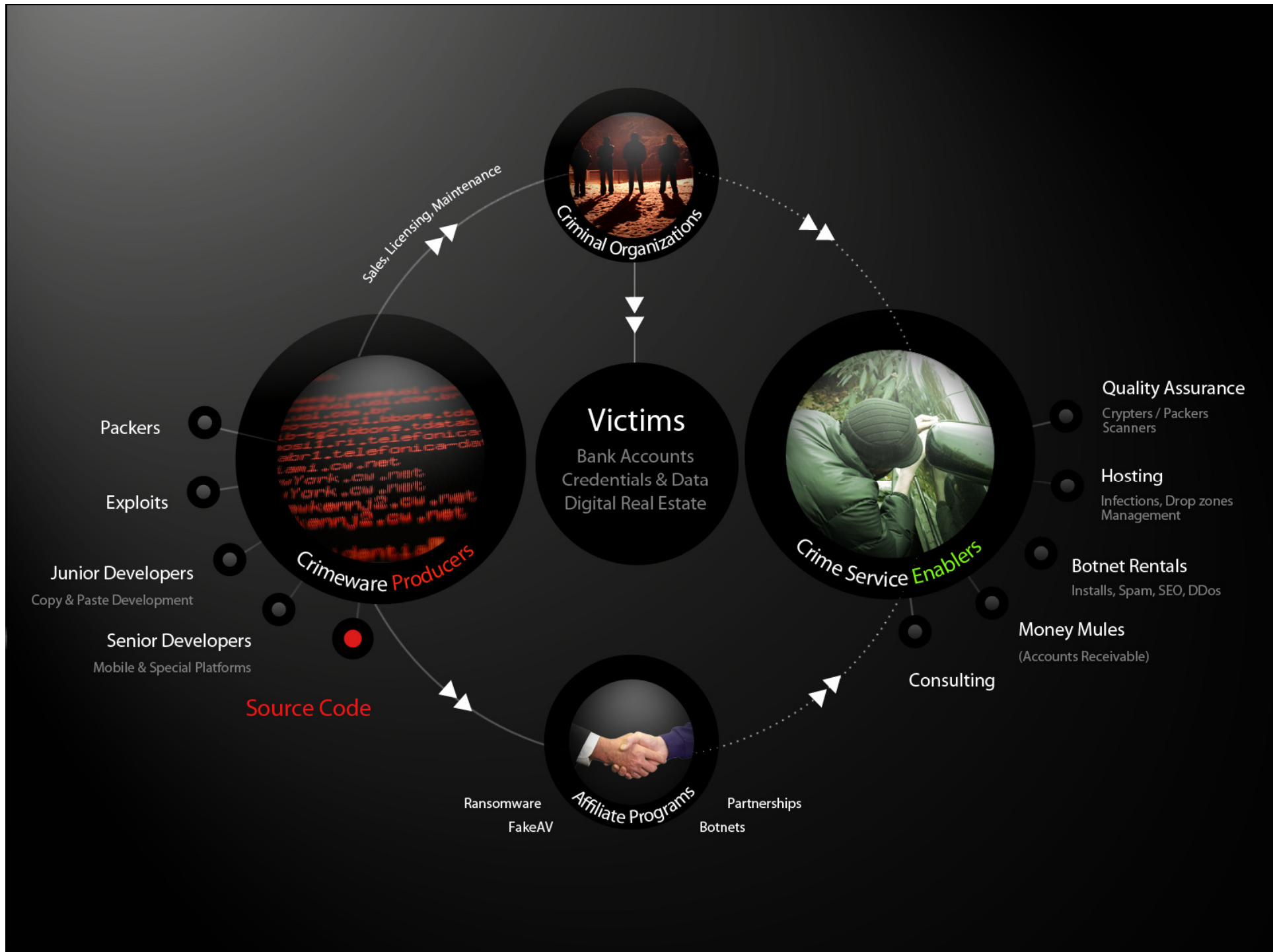
Vulnerability Control and Management (VCM)

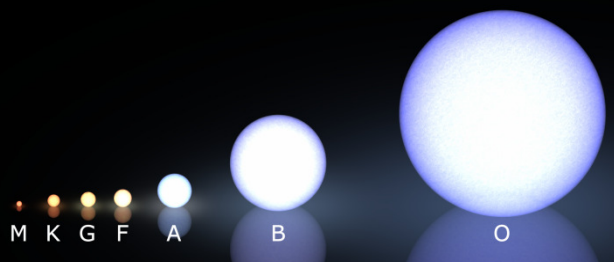
Zero-Day Threat Research

- World Wide Research Team (**130+**)
- 130+ Zero-Days Discovered Since 2008
 - Mostly Critical
 - *September 2011: 33 in Zero-Day State*
 - **6 > 1 Year ... 19 > 2 Years**




Forum of Incident Response and Security Teams






Programs, Partnerships



BETTER RATES! NO HOLD!
ONLY REAL ONLINE STATISTIC!

REGISTER TODAY




→ MAIN
→ ABOUT US
→ CONDITIONS
→ RATES
→ FAQ
→ CONTACTS

The partnership program **«Earning4u»** is the easiest way to earn money. All you need to do to start working with us is [register](#).

You will earn **from 6\$(Asia) to 140\$(USA)** per 1000 installs. You can view all prices in the [«Rates»](#) section.

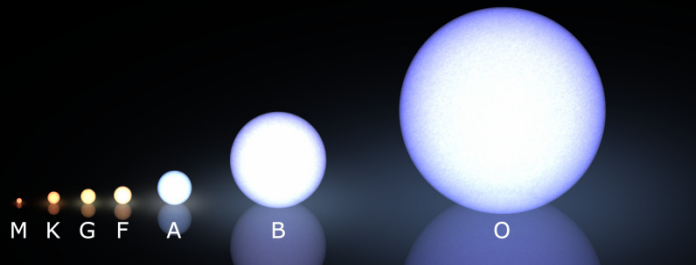
Our Rates

Country:	Rate in \$ for 1000 installs:
United States	140
United Kingdom	110
Netherlands	30
France	30
Poland	20
Italy	65
Germany	30
Spain	30
Australia	55
Greece	30
Other	20
Asia	6



* We also reserve the right to delete any account

* And remember - **all SPAM is prohibited!**

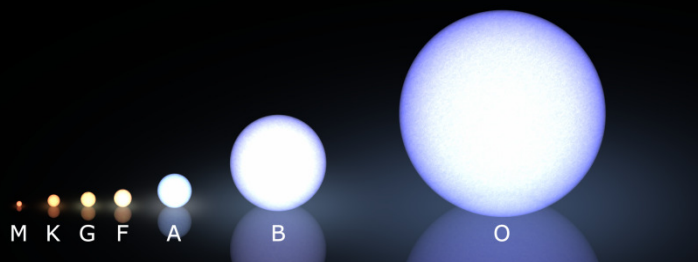


Modern Threats

- **Mobile**
 - Banking Components
 - Full Botnets (Droid Kungfu)

- **“Advanced Persistent Threats”**
 - Stuxnet, Duqu (S7 Code)
 - Multiple Components, Criminal Elements
 - Gh0st Net, Shady Rat, Aurora – Vulns

- **Ransomware**



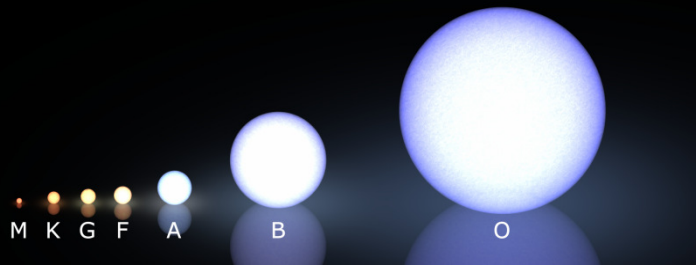
Gh0st RAT

The screenshot displays the Gh0st RAT web interface. On the left, there is a list of connected clients with columns for ID, WAN IP, and other details. The main area shows several camera feeds from different locations, including what appears to be a person's face and an interior room. A taskbar at the bottom shows system information like CPU usage (35%), network speed (S: 0.08 kb/s, R: 1.19.01 kb/s), and the time (20:49). A watermark 'www.tixseft.com' is visible in the top right of the interface.

Where Are We Going?

- **Blackmail and Targeted Ransom**
Mobile
- **SCADA Vulnerability Focus**
Web, Cloud Interfaces
- **Sponsored Attacks, Advanced Evasion**
Crime as a Service, Crimeware
- **Vigilante Justice**





Ransomware

You entered this site because your PC had been cracked and all the drives were encrypted with the algorithm AES - 128, that is also used by governmental and army services of many countries to protect the information.

You can restore the PC and all the information by means of Internet payment systems [Ukash](#) or [Paysafecard](#). The ways to acquire the Vouchers of these systems you can find [here](#).

Warning for ones aimed to save money:

- 1) The password includes 16+ symbols thus excluding the possibility to guess it.
- 2) Any attempt to restore (Live CD, Boot Disks, Windows CD And the like) will lead to loss of the public encryption key resulting to your PC decryption failure.
- 2) Do not spent money and time for computer specialists. They are unable to help you. Your only way out is to restore your data free of losses is to purchase the access code.

Once you pay the necessary sum, we guarantee to provide you with the password for your PC. Thereafter our program will automatically decode all your data and will retrieve your PC. Do think about your files and presentations, photos and videos, saved favorites and save games - all this worth that little sum we ask for.

What Should We Be Doing?

- Public-Private Relationships
- Education & Awareness
- Policy & Focus
- Enforcement & Focus (Cash Flow, etc)
- Security & Strategy



Useful Resources



FortiGuard Center

- <http://www.fortiguard.com>
 - Advisories, Reports, Tools, Encyclopedia

Fortinet YouTube Channel



- <http://www.youtube.com/securenetworks>
 - Security Minute Educational Videos



Fortinet & Network World – Security Podcast

- <http://www.networkworld.com/podcasts/secthreat/index.xml>



FortiGuard Labs & Fortinet Blog

- <http://blog.fortinet.com>



twitter.com/fortinet



facebook.com/fortinet