cyber camp

CYBERSECURITY EVENT

2016

Exposing Koobface – The World's Largest Botnet

Dancho Danchev

GOBIERNO DE ESPAÑA

MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

incibe_

TRABAJANDO POR LA CONFIANZA DIGITAL

CyberCamp.es

[Who Am I?]

- Threat Intelligence Analyst – since 2007
  - http://ddanchev.blogspot.com
  - https://www.webroot.com/blog/author/ddanchev/
- Active Security Blogger – since 2007
  - http://www.zdnet.com/meet-the-team/us/dancho-danchev/
- Active Cybercrime Researcher – since 2007
- Past Experience
  - Managing Director, Astalavista.com
  - Security Blogger, Webroot, Inc.
  - Security Blogger, ZDNet, CBS Interactive

[Presentation Overview]

- What is Koobface?
  - World's largest botnet propagating over social media
- Who's Behind It?
- Koobface Botnet's Business Model
- Koobface Gang's Malicious Activity – Exposed
  - Social Media Propagation
  - Black Hat SEO (search engine optimization) Campaigns
  - Scareware-serving Campaigns
  - Client-side Exploits Serving Campaigns
- Interacting with the Koobface Botnet – Case Study
- Final words

[What is Koobface?]

- World's Largest Botnet Propagating Over Social Media
- Who's Behind It?
- Characteristics of the Botnet
  - Social-engineering driven propagation methodology
  - Templatiza-tion based propagation model
  - Scareware-affiliate-network based type of monetization model
  - Multi-tude of propagation attack vectors
    - Black Hat SEO (Search Engine Optimization)
    - Client-Side Exploits Serving Templati-zation Based Propagation Attack Vectors
    - Scareware-serving social media propagating attack vectors
- Scareware-Affiliate Network Based Type of Monetization Model

[Who's Behind It?]

- Profiling the Koobface Gang – A Russian-Based Cybercrime-facilitating Group
  - KrotReal – active team member of Ali Baba and 40 cybercrime-friendly group
  - Two years active investigation
    - Active community and ISP collaboration
    - Active botnet infrastructure monitoring
    - Multiple C&C server domains registered to typosquatted Dancho Danchev
    - Active C&C server domains take down

[Interacting with Koobface – a Case Study]

- Koobface Gang featured messages and greetings
    - C&C server communication featured messages and greetings - "*We express our high gratitude to Dancho Danchev (http://ddanchev.blogspot.com) for the help in bug fixing, researches and documentation for our software.*
- Multiple domains registered to typosquatted Dancho Danchev
    - pancho-2807.com is registered to Pancho Panchev
    - rdr20090924.info registered to Vancho Vanchev

[Who's Behind It?]

- Active C&C server infrastructure monitoring
  - Active ISP server cooperation
    - BlueConnex - Abuse Team – 85.234.141.92 - “*Three hours after notification, Blue Square Data Group Services Limited ensures that "the customer has been disconnected permanently". It's a fact. All of Koobface worm's campaigns currently redirect to nowhere.*”
    - AFILIAS - Abuse Team – 91.212.107.103 - “*Action is taken again the entire .info tld domain portfolio, the domains are suspended within a 48 hours period of time courtesy of AFILIAS.*”

[Who's Behind It?]

- Active C&C server infrastructure monitoring
  - Active ISP server cooperation
    - TelosSolutions - "*this customer has been removed from our network*"
    - Directi's Abuse Team - boomer-110809.com; upr200908013.com – taken offline courtesy of Directi's Abuse Team
    - Oc3 Networks & Web Solutions LLC - 67.215.238.178 – taken offline courtesy of Oc3 Networks & Web Solutions LLC
    - 91.212.107.103 - “*which was taken offline for a short period of time. ISP has been notified again*"

[Who's Behind It?]

- Active C&C server infrastructure monitoring and take down efforts
  - 24 hours period of time for active C&C server take down
  - Coordinated take down campaign across multiple ISPs including hosting providers
  - Koobface Gang to UKSERVERS-MNT - “we've been compromised”
  - Koobface 1.0 goes Koobface 2.0 – social engineering, and ISP cooperation goes rogue

[Who's Behind It?]

- Koobface Gang responded to my “10 Things You Didn't Know About the Koobface Gang” article, within, the, C&C server infrastructure
  - The gang is connected to, probably maintaining the click-fraud facilitating Bahama botnet
  - Koobface Gang: no connection
- Despite their steady revenue flow from sales of scareware, the gang once used trial software to take a screenshot of a YouTube video
  - Koobface gang: what's reason to buy software just for one screenshot?

[Who's Behind It?]

- The Koobface gang was behind the malvertising attack the hit the web site of the New York Times in September
    - Koobface Gang: no connection
- The gang conducted a several hours experiment in November, 2009 when for the first time ever client-side exploits were embedded on Koobface-serving compromised hosts
    - Koobface Gang: :)
- The Koobface gang was behind the massive (1+ million affected web sites) scareware serving campaign in November, 2009
    - Koobface Gang: :)

[Who's Behind It?]

- The Koobface Gang Monetizes Mac OS X Traffic through adult dating/Russian online movie marketplaces
  - Koobface Gang: :)
- Ali Baba and 40 LLC a.k.a the Koobface gang greeted the security community on Christmas
  - Koobface Gang: it was 'ali baba & 4' originally. you should be more careful
- The Koobface gang once redirected Facebook’s IP space to my personal blog
  - Koobface Gang: heh

[Who's Behind It?]

- The gang is experimenting with alternative propagation strategies, such as for instance Skype
  - Koobface Gang: strange error. there're no experiments on that
- The gang is monetizing traffic through the Crusade Affiliates scareware network
  - Koobface Gang: maybe. not 100% sure

[Who's Behind It?]

- Koobface Gang redirected Facebook's IP space to my personal blog
  - “Thanks for bringing this to our attention. I'm on the Security Incident Response team at Facebook and we just finished looking into this issue. We visit all links posted to Facebook as part of our link preview feature. We also take the opportunity to do some additional security screening to filter out bad content. Koobface in particular is fond of redirecting our requests to legitimate websites, and you seem to have done something to piss Koobface off. All visits to Koobface URLs from our IP space are currently being redirected to your blog."

[Koobface Botnet's Business Model]

- Koobface Botnet's business model – a case study in efficient scareware-serving affiliate based monetization model
  - Traffic acquisition
    - Facebook, Twitter, black hat SEO (search engine optimization), client-side exploits
  - Traffic monetization
  - Scareware-based affiliate network type of monetization scheme
  - Crusade-Affiliates

[Koobface Gang's Malicious Activity - Exposed]

- Social media propagation
  - Each and every infected host further spreads an infected message across the world's most popular social media platform – Facebook, Twitter – advertising fake Adobe Flash Player and YouTube video player
- Black Hat SEO (search engine optimization) campaigns
  - Diverse set of traffic acquisition tactics ultimately led to a diverse platform for spreading scareware affecting over 1M Web sites, in November, 2009

[Koobface Gang's Malicious Activity - Exposed]

- Scareware-serving Campaigns
  - Black hat SEO (search engine optimization) utilized for traffic acquisition
  - Social media propagation utilized for traffic acquisition
  - Bahama botnet connection
  - NYTimes malvertising campaign
  - Scareware-serving campaigns primarily served fake Adobe Flash Players and YouTube players

[Koobface Gang's Malicious Activity - Exposed]

- Client-side exploits embedded at Koobface infected hosts using iFrames
  - VBS/Psyme.BM; Exploit.Pidief.EX; Exploit.Win32.IMG-WMF
    - el3x.cn/test13/index.php
    - kiano-180809 .com/oko/help.html
    - ttt20091124.info/oko/help.html
- Double-layer monetization in action – client-side exploits and scareware served on Koobface-infected hosts

[Interacting with Koobface – a Case Study]

- Real-time monitoring and interaction with the botnet – a Case Study
  - Active 24/7/365 monitoring of Koobface Gang's infrastructure
    - Active real-time profiling of malicious campaigns served by the Koobface Gang
    - Real-time monitoring and profiling of Koobface Gang's infrastructure
    - Real-time monitoring and profiling of Koobface Gang's malicious software
    - Real-time monitoring and profiling of Koobface Gang's C&C infrastructure
- Final Words