Top 10 Botnet Threat Report - 2010

Introduction

2010 was a big year for Internet crime with botnets and targeted attacks becoming headline news on an almost weekly basis. The public disclosure of international organizations such as Google, Adobe, Juniper Networks and many others succumbing to what would eventually be labeled as “Operation Aurora” kicked off the year and revealed that “sophisticated”, “advanced” and “persistent” malware were now every-day inclusions of the criminals toolkit.

Prior to 2010, many people thought in terms of Spam and DDoS whenever the term “botnet” was discussed. By the end of the year, botnets such as Mariposa, Aurora, Koobface and Stuxnet had become household names – revealing the breadth of crime commonly being facilitated with remotely controllable bot agents.

This brief report looks at the performance and prevalence of the top fifty botnets most commonly encountered by Damballa in the course of monitoring Internet-based threats – the threats most regularly encountered and damaging to home users and poorly secured businesses.

Top 10 Biggest Botnets

In 2010 we witnessed many new botnets come into existence. Of 2010's Top 10 largest botnets, six of these botnets did not exist in 2009 and only one (Monkif) was present in the 2009 Top 10 largest botnets.

First place was claimed by a new botnet that dramatically rose to international attention in the second half of the year. Claiming 14.8% of all unique infected victims in 2010 is a botnet associated with the TDL Gang – a criminal organization made famous for its advances in master-boot-record (MBR) rootkit technology and their commercially available do-it-yourself (DIY) botnet construction kit.

	2010 Botnet	Percentage of Victim Population	2009 Position
1	TDLBotnetA (RudeWarlockMob)	14.8%	--
2	RogueAVBotnet (FreakySpiderCartel)	5.7%	--
3	ZeusBotnetB (FourLakeRiders)	5.3%	--
4	Monkif	5.2%	5th
5	Koobface.A	4.0%	< top10
6	Conficker.C	2.8%	< top10
7	Hamweq (GraySunGirls)	2.5%	--
8	AdwareTrojanBotnet (WickedRockMonsters)	2.2%	--
9	Sality	2.1%	< top10
10	SpyEyeBotnetA (OneStreetTroop)	1.9%	--

The prevalence of improved DIY botnet construction kits and associated exploit packs is visible in the makeup of the 2010 Top 10. Botnet operators RudeWarlockMob, FreakySpiderCartel, FourLakeRiders, WickedRockMonsters and OneStreetTroop all built their botnets based on popular construction kits – often changing and augmenting the kits throughout the year as their infection campaigns and fraud objectives changed.

In 2010, the Top 10 largest botnets accounted for approximately 47% of all botnet compromised victims – down from 81% of the 2009 Top 10. This decrease was not unexpected as the number of new criminal botnet operators increased, as did the average number of botnets owned and managed by each botnet master.

Notes:

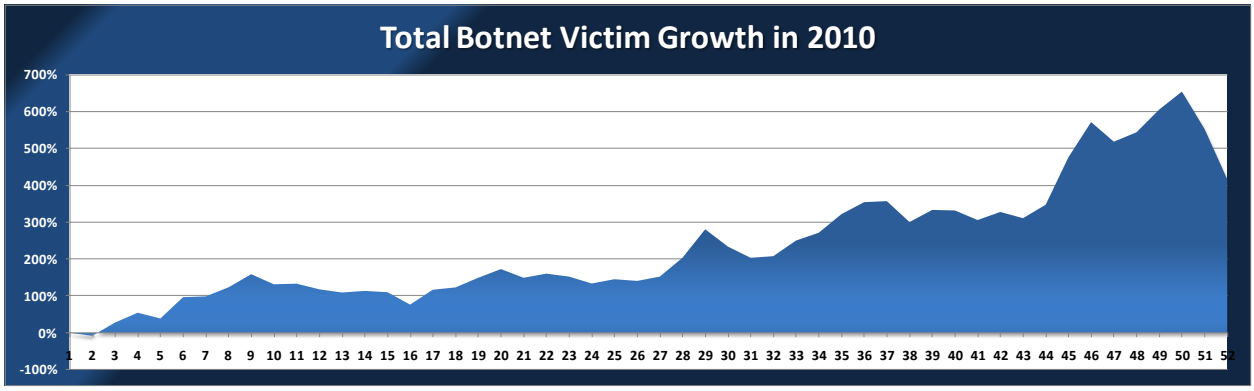
1. *Botnet operator names in parenthesis (i.e. RudeWarlockMob, FreakySpiderCartel, FourLakeRiders, WickedRockMonsters and OneStreetTroop) are names automatically assigned by Damballa systems for tracking unique criminal gangs and their campaigns for the purpose of attribution.*

2. *These observations and statistics are accumulated from Damballa sensors that monitor the Internet at large – and therefore represent what most home users and small businesses will be exposed to. It is important to note that enterprise networks that deploy multiple layers of protection technologies (and keep them updated) are much less likely to encounter these Top 10 largest botnets infecting systems and operating within their own networks. The Top 10 most regularly encountered enterprise botnets are considerably different – very few actually having botnet agents that are detectable with anti-virus products, let alone having been named.*

3. *The table above lists the Top 10 largest botnets of 2010 and their overall percentage of known botnet infected victims. There are a number of factors and network dynamics that make measuring "unique" botnet infections difficult. For the purpose of global monitoring and this report, Damballa measures the global victim populations based upon each unique victim IP address that reliably connects and interacts with a component of the criminals' botnet command-and-control (CnC) infrastructure once per week. Regardless of whether a particular IP address hosts multiple computers or is compromised with multiple bot agents and makes repeated connections throughout a week, it will be counted only once for that week. Each week a new and independent count of infected IP addresses is made.*

Botnet Growth

Analysis of global unique botnet victim populations on a per-week basis revealed substantial increases throughout 2010. At its peak, in the run up to Christmas (week 50), the total number of unique botnet victims were 654% greater than the victim population at the beginning of the year – with an average incremental growth of 8% per week throughout the year.



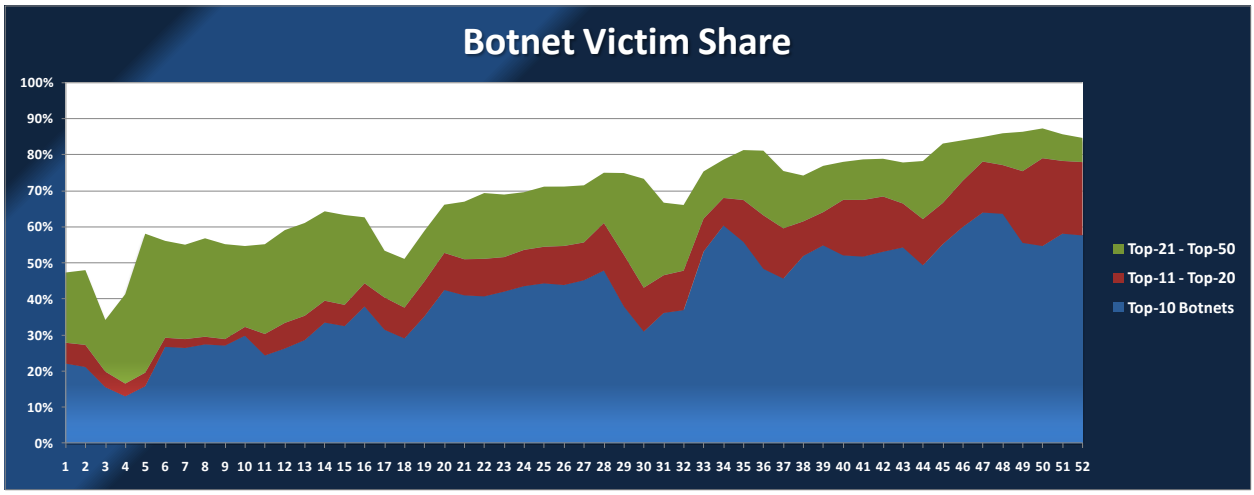
It is important to note that the substantial growth in botnet infections observed by Damballa is a reflection of the following:

1. The second half of 2010 saw the rapid evolution of many popular botnet DIY construction kits and the increased availability of feature-rich browser exploit packs.
2. Cyber criminals providing specialized malware distribution services became more proficient at installing bot agents on behalf of their customers (i.e. botnet operators).
3. The last quarter of 2010 was heavily influenced by the rapid growth of botnets utilizing the TDL MBR rootkit technology.
4. Damballa developed and deployed multiple new CnC detection technologies that increased their ability to detect additional categories of stealthy botnet deployments.

Botnet Victim Share

Throughout the year, the Top 10 largest botnets increased their total share of all bot infected victims. At the beginning of the year approximately 22% of observed botnet victims were infected with malware attributed to just ten botnet operators. By the end of the year, this proportion had grown to nearly 57% - more than doubling their share of global botnet victims.

In the meantime, the Top 20 and Top 50 botnets similarly increased their proportion of global bot infected victims from 28% to 78% and 47% to 85%, respectively, by the end of the year.



This dominance of the Top 10 largest botnets can likely be attributed to increased sophistication and breadth of their individual malware infection lifecycles. These botnet operators typically:

- Run multiple simultaneous infection campaigns
- Update the malware installed on their victims systems regularly
- Optimize their serial variant malware production systems to release “personalized” and one-of-a-kind malware with each new victim infection
- Invest in diverse infection delivery platforms
- Maintain robust botnet CnC topologies largely resistant to takedown or hijacking attempts

Multiple Infections

The processes Damballa uses to identify compromised systems also include the ability to uniquely identify the botnet(s) currently infecting the device. Of the tens-of-millions of infected systems identified throughout 2010, Damballa ascertained that 35.2% of infected IP addresses had two or more different botnets operating from them.

Botnets Under the Microscope

While thousands of botnets and botnet operators were tracked by Damballa in 2010, many have the same (if not identical) stories to tell – socially engineered exploitation of the victims device, installation of a multi-function botnet agent, theft of all salable information hosted on the victims device or within easy local-network reach, repeated botnet agent updates, and eventual transference to multiple criminal organizations with "specialist" requirements.

It is worth highlighting three interesting examples of botnets in 2010:

- **Zeus-based Botnets**
  Zeus is perhaps the most commonly encountered and easily accessible botnet DIY construction kit. It is used for an incredibly broad range of crimes – ranging from banking credential theft to back-dooring new equipment and long-term infiltration of industrial systems.

- **TDL Botnet**
  Advances in the botnet agents' functionality and its resilience to standard remediation practices make devices infected with the TDL rootkit an ideal platform for multi-tenant botnet installation – resulting in a profitable SaaS or PaaS business for their criminal controllers.

- **Hamweq**
  Hamweq is interesting because of its simplicity and its legacy communication characteristics – proving that being "advanced" is overrated.

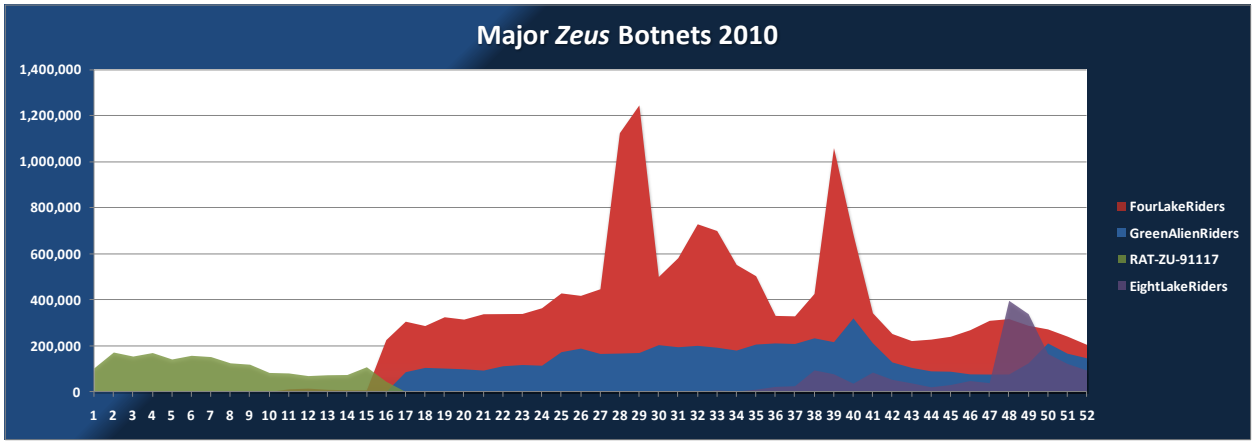
The data presented here is specific to compromise monitoring within ***North America***, from multiple sensor locations across multiple business sectors and industry verticals.

Zeus Botnets

In 2009, the Zeus-based botnet "RAT-ZU-91117" led the Top 10 – dominating 19% of botnet infections for the year. For the first quarter of 2010, the same Zeus-based botnet persisted, but was quickly superseded with the much larger and more successful "FourLakeRiders" Zeus-based botnet which attained third position in our 2010 Top 10 largest botnets.

Of the thousands of independent botnets Damballa tracked in 2010, only four Zeus-based botnets appeared in the Top 50 largest botnets and are depicted in the graph below.

Although these four botnets utilized the Zeus DIY construction kit, their supporting CnC infrastructures were different and were operated by distinct crime organizations. The Zeus CnC management console allows operators to integrate their preferred exploit packs and optimize their infection strategy. The infection sites managed by FourLakeRiders, GreenAlienRiders, RAT-ZU-91117 and EightLakeRiders each exhibited their own "unique" exploit pack characteristics – enabling a degree of attribution to each organization.

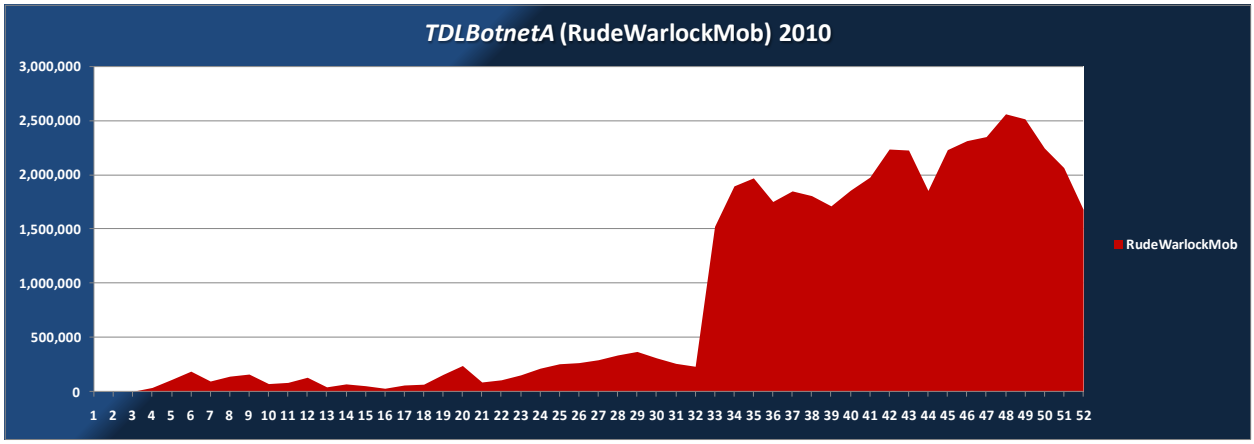


It is interesting to note the compromise profile similarity (and overlap) between the RAT-ZU-91117 and GreenAlienRiders. While the CnC infrastructure of the two botnets were independent, it is common for botnets to be sold, rented or hijacked among different criminal operators where the malware agent is updated or replaced by a bot agent owned by the new botnet operator. There is a high probability that something similar happened in this instance in mid-April 2010.

TDL Botnet

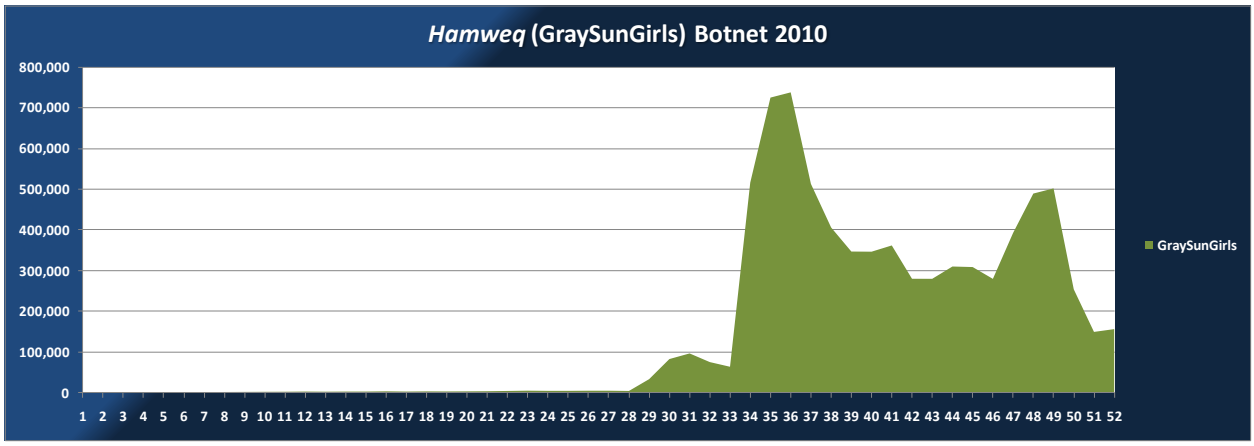
The largest botnet of 2010 was attributed to the authors of the TDL malware family (aka W32.Alueron, aka W32.Renos). Damballa tracks the botnet operators as "RudeWarlockMob" but they are also often publicly referred to as the TDL or TDSS Gang.

While the botnet was present throughout practically all of 2010, it wasn't until early August that the botnet grew at a phenomenal rate. The timing of this accelerated growth would appear to coincide with the release of the fourth major version of the TDL malware following the Defcon conference in Las Vegas. This version of the bot agent includes advanced rootkit functionality combined with a MBR hooking infector – making it resilient against standard remediation processes and highly persistent.



Hamweq Botnet

Known as GraySunGirls to Damballa, the Hamweq botnet received a lot of press attention last year and came in at the seventh position in our Top 10 largest botnets of 2010. Hamweq is interesting because of its simplicity and its legacy communication characteristics – proving that being "advanced" is overrated. Specifically, Hamweq exhibits old-style worm capabilities that utilize removable media (such as USB devices) to propagate and infect new victims and relies on IRC communications for its CnC.



While the Hamweq malware family has undergone many software revisions since its public identification back in the later half of 2008, it wasn't until the middle of 2010 that the botnet named from the malware grew at a substantial rate.

The characteristic saw-tooth movements visible in the graph above are representative of new Hamweq malware releases, followed by a spurt of worm-based infections and subsequent new anti-virus detection updates. The width of these individual saw-tooth growth phases are typically three to four weeks – which corresponds to the lag between large scale device compromise from a new malware variant and eventual "protection".

Conclusion

Whether using well known techniques, or the latest in armoring and deception, botnets continue to dominate the cyber threat landscape. With malware that can be repurposed, botnets that can be rented, and new and attractive targets in the proliferation of smart phones and mobile devices, 2011 will be a challenging year for enterprise security teams and service provider network abuse professionals. The criminals still possess the advantage in motivation, funding and patience.

While innovative solutions are now available to detect a breach and terminate the criminal communications, the bad guys will simply mount new campaigns. Staying ahead of the threat will require advanced knowledge of the building out of new botnet campaigns. A new wave of 'dynamic threat reputation systems' promise to deliver that competitive edge, and should enter the market in 2011. In the war on botnets, the arms race continues.

About Damballa Inc.

Damballa is a pioneer in the fight against cybercrime. Damballa provides the only network security solution that detects the remote control communication that criminals use to breach networks to steal personal and intellectual information, and conduct espionage or other fraudulent transactions. Patent-pending solutions from Damballa are platform and system-agnostic, protecting networks with any type of device including PCs, Macs, smart phones, as well as mobile and embedded systems. Damballa customers include Fortune 1000 companies, Internet and telecommunications service providers, government agencies and leading universities. Privately held, Damballa is headquartered in Atlanta.

http://www.damballa.com