



Such An Innocent Question: *How To Protect Against a Botnet?*

Elizabeth Martin

Director, Security Services

emartin@redlegg.com

312.854.1079

March 24, 2011



Topics

- Definition of a Botnet
- Botnets As a Business
- Botnet Attack Vectors
- Protection Solutions
- Emerging Solutions
- Fraud / Money Laundering
- Summary



What Is A Botnet?

- *Bot* refers to an compromised host that is remotely controlled by an operator, also known as a *zombie*
- *Net* refers to a collection of compromised hosts
- Botnets are remotely controlled by Botnet Operators, or *bot herders*, typically criminal organizations
- Botnets have been referred to as “Dark Cloud” computing in that a variety of services are offered



Botnet Services and Org Chart

- Spam - End-to-end spam botnet systems complete with fast-flux DNS features
- Phishing – Including spear phishing and whaling techniques
- DDoS – Distributed Denial of Service
- Data Harvesting – Searching, capturing, and sending Identity data, credentials, credit card numbers, bank account information, Social Networking profiles
- Botnet Ecosystem¹
 - **Affiliates** - Distribution, infection, etc.
 - **Resellers** - Laundering, traders, etc.
 - **Professional Service Providers** - Malware, exploit packs, translation, web design, etc.
 - **Managed Service Providers (MSS)** - DNS hosting, fluxing services, SEO, etc.
 - **Delivery Providers (SaaS)** – iFrame services, email/phishing campaigns, etc.
 - **Hosting Providers (PaaS)** - Bullet proof hosters, “friendly” ISP’s, malware hosting, etc.
 - **Infrastructure Providers (IaaS)** - Hacked servers, server redundancy, botnet victims, etc.

¹ - “Building Botnets for Fun & Profit”

Gunter Ollmann, VP Research, Damballa Inc., October, 2010



Financial Incentives & Botnet Pricing

- Compensation models include pay-per-click (PPC) and Pay-per-install (PPI)
- VeriSign's iDefence reports pricing starts as low as \$67 for 24 hours, and \$9 for hourly access
- M86 Security Labs reports PCs in the UK are worth \$60, in Australia \$100, and \$50 in the US
- Imperva reports a 24-hour DDoS attack ranges from \$50 to several thousand dollars. Spamming a million emails, given a list, ranges between \$150-\$200, while a monthly membership for phishing sites is roughly \$2,000.



Botnet Underground Market

- Commercial Market – Albeit Underground, for the most part, but botnets are not necessarily illegal everywhere
- Competitive Market – Feature Rich
 - Advanced stealth, obfuscation, and evasion features allow botnet operators to protect themselves against competing botnets, investigators, and law enforcement
 - Do-It-Yourself (DIY) kits allow for ease of bot creation and deployment
- Zeus 2.1, next generation of financial malware offers the following features:
 - Digital Signature Verification – Allows fraudsters to digitally sign their code to ensure no unauthorized code is added to their botnet
 - Data Encoding – Strings, data, and URLs are encoded and decoded only when needed, preventing the good guys from being able to access the data being captured
 - Strong Public Key – Incorporation of 1024-bit RSA public key to support the Digital Signature and Data Encoding
 - Mobile Version – A mobile version that is designed to help circumvent two-factor authentication
 - Advanced Business Model – The 2.1 version supports an advanced business model that allows Zeus to dominate the botnet market share by offering their fraudster clients advanced evasion techniques that prevent analysis and hostile takeover from law enforcement, researchers, or competing cybercriminal organizations
- Mergers & Acquisition Rumors
 - SpyEye and Zeus have been rumored to merge the codesets to create one “Super Trojan”



Common Botnet Attack Vectors

- Human Nature – Social Engineering techniques are used to convince a user to executed infected code
- Common Security Vulnerabilities – Typical vulnerabilities such as unpatched systems or poor configurations
- Vulnerable Web Sites – Allows for malicious code to be injected into the site, commonly via Ad networks
- Inbound DDoS – Launches flood of packets against target generated from distributed sources that can not be blocked
- Outbound Connectivity – Bots continuously update themselves with new malware via C&C channels



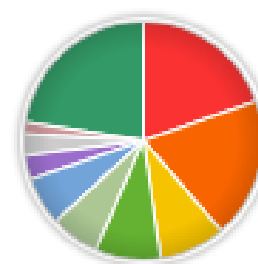
Vulnerability and Attack Statistics

Top 5 Vulnerabilities

	Patched
1. Internet Explorer MDAC	2006
2. Real Player IERPCtl	2007
3. Office Web Components	2002
4. Internet Explorer Deleted Object	2010
5. Microsoft Access Snapshot ActiveX	2008

[View more malware statistics](#)

Spam by Spambot Type



19.6% LETHIC
19% FESTI
9% GRUM
8.9% CUTWAIL 3
6.6% MAAZBEN
6.6% CUTWAIL 1
3.2% XARVESTER

[View more spam statistics](#)

Malicious Code Hosts by Country



1. United States - 25.9%
2. China - 18.8%
3. Ukraine - 14.2%

[View more malware statistics](#)

Spam Sources by Country



1. India - 9.4%
2. Brazil - 8.3%
3. Russia - 7.6%

[View more spam statistics](#)



Popular Botnets²

- **10. Waledac:** This prolific descendent of the infamous Storm botnet used social engineering scams such as e-cards and coupons to enlist an estimated 90K hosts before being whacked.
- **9. Mariposa:** Composed of up to 12 million hosts infected over P2P, MSN, and USB channels. Powered by the Butterfly bot, Mariposa spent about a year harvesting identities and credentials from hacked PCs and being rented by third parties for a variety of cybercrime campaigns. In December 2009, the Mariposa Working Group (lead by Defence Intelligence) commandeered Mariposa's C&C servers. But Mariposa's operators soon regained control, countering with a DoS attack against Defence Intelligence.
- **8. Zeus:** This on-line banking trojan was spread by phishing email and drive-by downloads over a period of three years, infesting millions of PCs, herded into hundreds of botnets. According to officials, banking credentials stolen from Zeus victims were used to initiate fraudulent transfers to "money mules" who were paid to route stolen funds back to organizers. In October 2010, the FBI announced that one large international crime network had used Zeus to steal \$70M from victim accounts, leading to 60 arrests in the US, 19 in the UK, and others in the Ukraine.
- **7. Bredolab:** Nearly half of all malware delivered by spam during 1H10 carried Bredo. This trojan often arrives with phishing messages that pose as money orders or failed delivery notices. Once executed, Bredo not only establishes C&C contact but attempts to recruit more bots. Last August, Dutch hosting provider LeaseWeb discovered that it was harboring 143 Bredo C&C servers. Over the next three months, the Dutch National High Tech Crime Team learned those servers were the well-hidden core of a multi-layer "botnet factory" that proxied C&C commands through drive-by download servers hosted elsewhere. A pain-staking investigation lead to successful take-down of nearly the entire Bredolab botnet, notification of 30 million Bredo-infected PC owners, and arrest of an Armenian accused of orchestrating this botnet.
- **6. Pushdo:** Botnets can be infuriatingly resilient. Consider Pushdo (a.k.a. Cutwail), responsible for up to 10 percent of all spam sent during the first half of 2010. Since 2007, Pushdo bots have issued a wide variety of spam blasts, from pharmaceutical ads to phishing messages and malware. In late August, researchers from LastLine identified 30 Pushdo C&C servers, hosted at 8 providers. Using provider notification, LastLine initiated a take down of 20, stopping nearly all Pushdo spam within 48 hours. Unfortunately, little cooperation could be obtained from other providers. Since then, Pushdo has recovered, operating under the control of those remaining C&C servers or perhaps new ones. Just last week, Pushdo variants were cited as the source of 22 percent of spam tracked by M86 Security Labs.

² - "The Top 10 Botnet Events of 2010"
Lisa Phifer, February 18, 2011



Popular Botnets (Cont'd)²

- **5. Grumbot:** Grumbot (aka Tedroo) is an extremely prolific botnet that tends to focus on sending Canadian pharmaceutical spam. After chugging along steadily throughout 2009, Grum message lengths suddenly decreased in early 2010, enabling per-bot message rates to spike roughly 50 percent. By March, Grumbots were reportedly cranking out over one quarter of all world-wide spam. One year later, Grum's share of the pie has fallen to 12 percent – but only because other botnets have surged.
- **4. Lethic:** Like Pushdo, Lethic has been slowed but not stopped by community efforts to dismantle this unusually fast botnet. Lethic C&C servers relay spam through an estimated 200-300K bots, which churn out copies at very high rates (12 to 60K per hour per bot). A Lethic C&C server take-down was organized by Neustar in January 2010, stopping roughly 10 percent of worldwide spam at that time. But by February, new C&C servers had appeared, ramping Lethic back up to a whopping 56 percent of all spam sent during 2Q10. Although the proportion of global spam represented by Lethic has since dropped, it continues to rank at or near the top of spambot lists (last week 22.5 percent).
- **3. Koobface:** Given the profits at stake, botnet operators are highly motivated to adapt. Take Koobface, the botnet born by exploiting users of social networks like Facebook, Friendster, MySpace, and Twitter. According to Information Warfare Monitor, Koobface operators also used pay-per-click (PPC) and per-per-install (PPI) affiliate programs to make \$2M over a one year period. Using URL redirection and fast flux DNS, Koobface earned its keep by presenting ads and selling fake AV programs. To keep investigators at bay, operators blocked their probes using IP blacklists, monitored malicious URL lists, abused short URLs in Twitter, and learned to bypass CAPTCHA. In short, Koobface demonstrated how creative criminals can turn defenses into evasion techniques.
- **2. Rustock:** Occasionally, even spambots need a vacation. Or so it seems for Rustock, which until mid-December consistently sent about 46 billion spams per day (up to 25K per hour per bot). Rustock is notoriously resistant to anti-malware, using rootkit techniques and TLS-encrypted HTTP to stubbornly evade detection. As a result, researchers were surprised to see Rustock spam halt on December 25th. But two weeks later, the botnet sprang back, doubling world-wide spam rates which had dropped to a two-year low during Rustock's hiatus. But why did Rustock take a holiday break? One factor may have been business disruption caused by the September closure of SpamIt.org and its affiliate payment program.
- **1. Stuxnet:** Perhaps the single-most sobering botnet event of 2010 was Stuxnet. According to a Symantec report, Stuxnet is highly-targeted weaponized malware that appears to have been injected into Iranian power plants over a 10 month period, from 5 identified vectors through infected USB drives. Detected in July 2010, Stuxnet exploited zero-day vulnerabilities in Windows and SCADA software to infect and spread among industrial control systems, organizing into a botnet of peripherals that were ready to spring into attack mode under command of a clearly-defined C&C. In short, Stuxnet is noteworthy not because of its size or speed, but because it raises the stakes. Clearly, botnets aren't just about pesky spam or spreading fake AV or even massive identity thefts. Botnets are a means to many ends – in this case, with potentially devastating fallout.

² - "The Top 10 Botnet Events of 2010"

Lisa Phifer, February 18, 2011



Takedowns

Once-prolific Pushdo botnet crippled

Torrent of spam choked

By [Dan Goodin](#) • [Get more from](#)

Posted in [Malware](#), 27th August 2010 1

Spam Affiliate Program Spamit.com to Close

March 17, 2011 7:00 PM PDT

Microsoft and feds bring down spam giant Rustock

by Jay Greene

[A](#) [A](#) Font size

[Print](#)

[E-mail](#)

[Share](#)

[41 comments](#)

[Tweet](#)

287

[Share](#)

206

[Reddit](#)

↑

↓

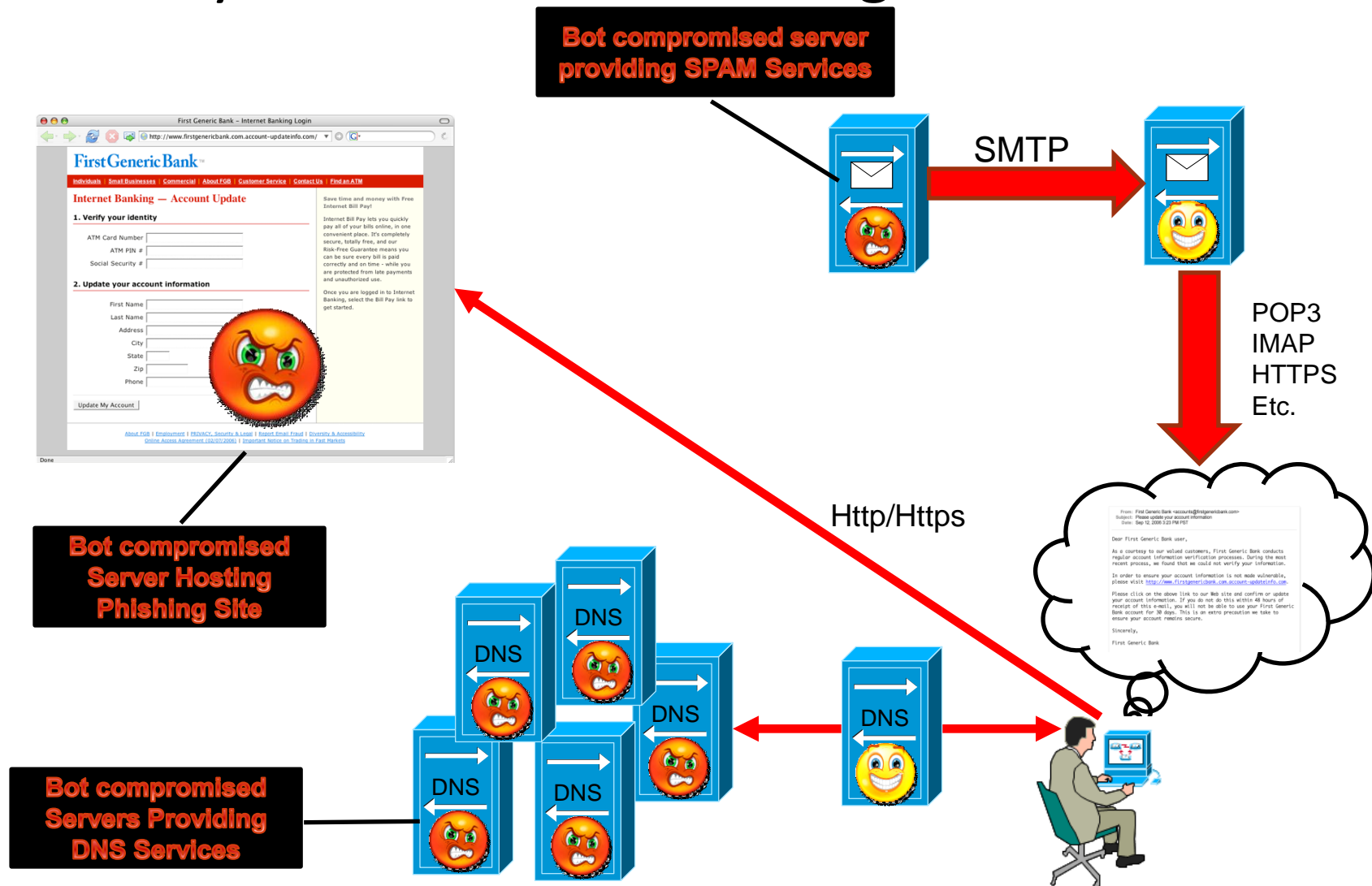
4 points

Good Guys Bring Down the Mega-D Botnet

Chalk up one for the defenders. Here's how a trio of security researchers used a three-step attack to defeat a 250,000-pronged botnet.

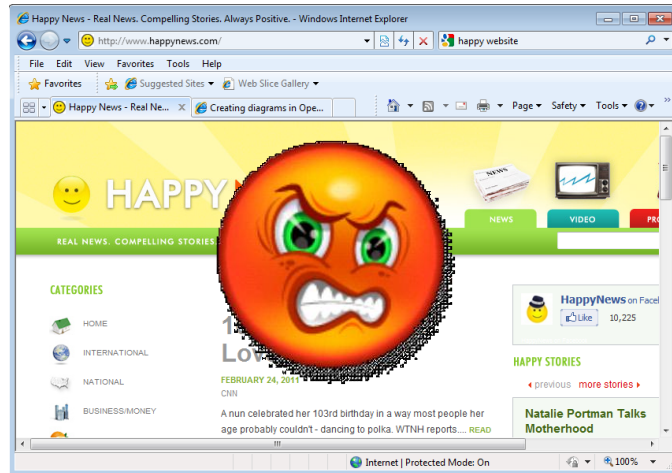


Anatomy of An Attack - Phishing



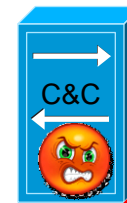


Anatomy of An Attack – Drive By Download



**Bot compromised web
server hosting malicious
code**

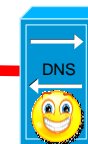
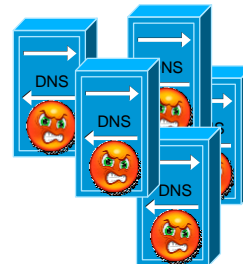
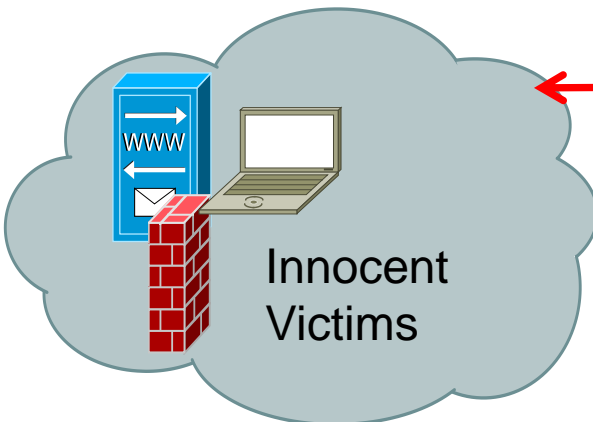
**Bot
compromised
end user
machine**



Encrypted
Command
& Control

Http/Https

**Malicious Activity:
DDoS; Data Harvesting; Etc.**



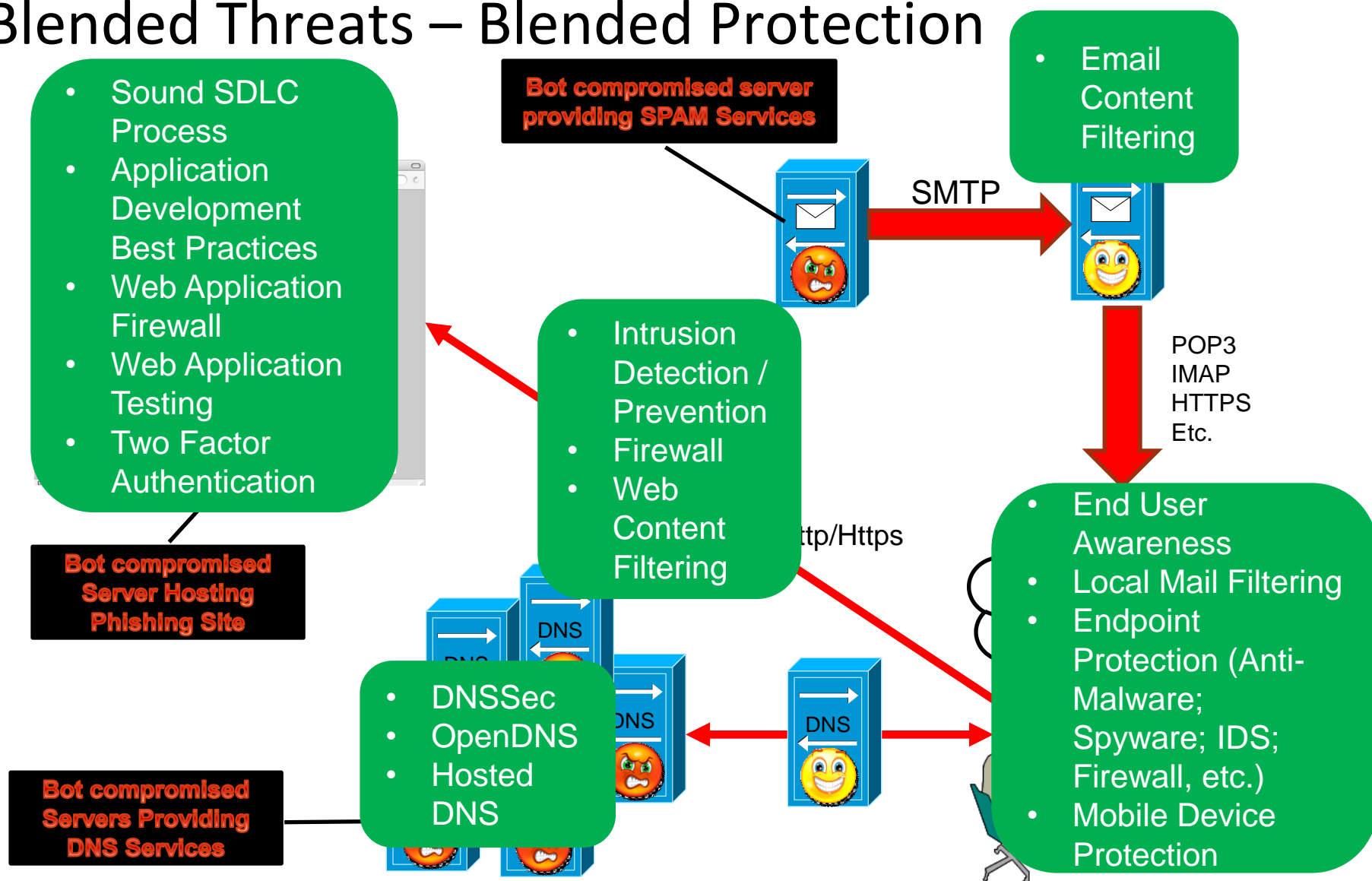


Blended Threats

- Combination of Attack Vectors and Techniques
- Single attack can be Web and Email Based
- Requires protection at multiple layers
- Requires constant diligence

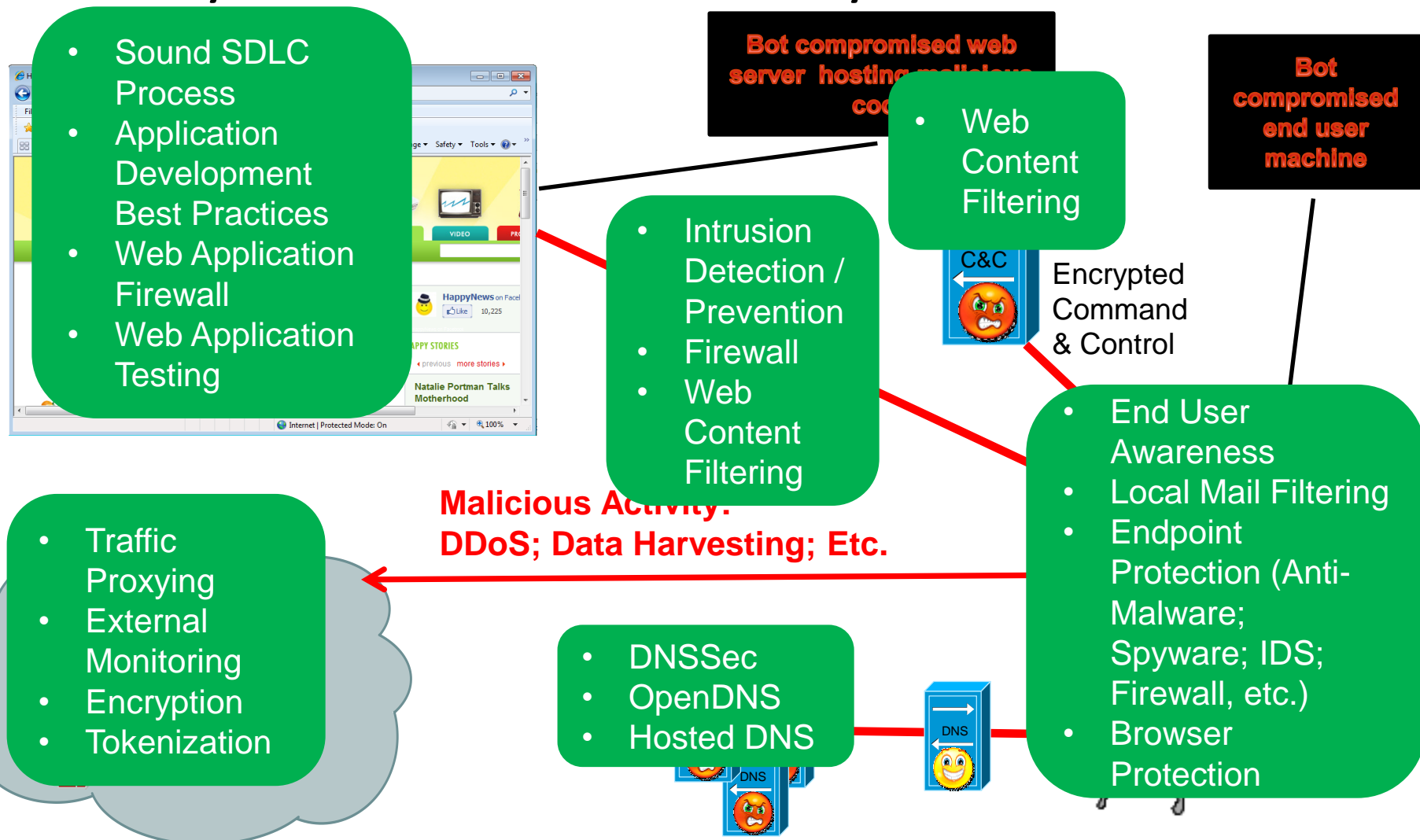


Blended Threats – Blended Protection






Anatomy of An Attack – Drive By Download





Fraud Protection & Money Laundering

- Bank Secrecy Act
- Patriot Act
- Anti-Money Laundering Practices
- Fraud Detection Services



About Us | Online Application | FAQ's | Affiliate | Ach Processing | Employment | Check Recovery | Links | Employment | Contact

★Specializing in High Risk Merchant Accounts since 1999

Some businesses MAY be classified as high risk for a number of reasons. Is your business classified as "High Risk"? High Risk Processor provides merchant services for high-risk merchant accounts, offshore merchant accounts and high-volume merchant accounts (examples of high risk merchants include mail order, telephone order, adult websites, direct marketing, infomercials, dating sites, online dating sites, escort services, outcall services, travel, telecom, timeshares, viagra / herbal supplements, subscription services, membership services, membership clubs, tickets, MLM, multi-level marketing, bail bonds, pawn shops, water filtration, high volume merchant accounts, international merchant accounts, companies facing high chargebacks, etc.). [Read our articles.](#)

★High Risk Processor can help.

High Risk Processor represents 25+ different processing sources (US based banks, Offshore banks, 3rd Party Processors, ACH Processors, Check Processors, etc.). Whether you are looking for one merchant account or multiple merchant accounts, we are certain that we can accommodate your processing needs. Regardless of business type or volume, we'll get your account approved quickly and keep it running smoothly without any volume caps. Let our staff of experienced industry veterans find the solution that's right for you.



Is There One Solution?

- No Silver Bullet!!
- Strategic Defense-In-Depth Approach Required
- Requires comprehensive protection at each point
- Good Old Fashioned Security Is Still Required!
 - Traditional Technologies such as Firewall, IDS/IPS, Content Filtering, Encryption, and Endpoint Security are still affective!
 - Basic best practices such as secure coding and host hardening will reduce exposure



Emerging Technologies

- Look for the security industry to provide innovative solutions
- Consider features such as Advanced Persistent Threat protection and Deep Content Inspection
- Some interesting vendors doing interesting things:
 - M86 – Proactive real-time detection across email & web, detects the intent of the page/code to determine the malicious intent, therefore able to detect very targeted attacks like Aurora - dynamic and emerging attacks.
 - Damballa - Advanced research, Inspection engines, correlated intelligence, and a global threat reputation system
 - IPTrust - Cloud based security intelligence monitoring
 - Trusteer – Financial Industry and End User Based Protection
 - Fidelis – Network based Deep Content Inspection
 - Arbor Networks or Prolexic Technologies for DDoS Protection



Summary

- Botnets are a global business with a supply chain every bit as organized and sophisticated as that of any legitimate business, and in fact perhaps more sophisticated than a lot of our own businesses
- Attacks are complex and require strategic approaches that consider the risks associated with the business
- The right solution(s) depend on your business
- Protection mechanisms will reduce your risk
- Get creative in solutions!
 - Ensure protection solutions start with policies and procedures
 - Open Source Solutions can be effective
 - Always consider Defense-In-Depth
 - Talk to your peers!



Q & A

Elizabeth Martin

Director, Security Services

emartin@redlegg.com

312.854.1079

March 24, 2011



References

- “The Dark Cloud: Understanding and Defending against Botnets and Stealthy Malware”
 - Eve Schooler, Intel, July 2010
 - <http://www.eetimes.com/EdTraining/DownloadFile?contentItemId=4201213&sponsor=intel&isSurveySuccess=True>
- VeriSign's iDefence Intelligence Operations Team
 - Study finds the average price for renting a botnet, May 26, 2010
 - <http://www.zdnet.com/blog/security/study-finds-the-average-price-for-renting-a-botnet/6528>
- “The Top 10 Botnet Events of 2010”
 - Lisa Phifer, February 18, 2011
 - <Http://www.esecurityplanet.com/features/article.php/3925436/The-Top-10-Botnet-Events-of-2010.htm>
- “The botnet market and what you get for your money”
 - Dan Raywood, October 26, 2010
 - <http://www.scmagazineuk.com/the-botnet-market-and-what-you-get-for-your-money/article/181756/>
- “RSA Conference: Researchers Go Inside the Botnet Threat”
 - Brian Prince , Feb 16th, 2011
 - <http://mobile.eweek.com/c/a/Security/RSA-Conference-Researchers-Go-Inside-the-Botnet-Threat-725521/>



References

- “Top 10 Botnet Threat Report – 2010”
 - Damballa Inc.
 - http://www.damballa.com/downloads/r_pubs/Damballa_2010_Top_10_Botnets_Report.pdf
- ¹ - “Building Botnets for Fun & Profit”
 - Gunter Ollmann, VP Research, Damballa Inc., October, 2010
 - http://www.damballa.com/downloads/r_pubs/HackerHalted2010.pdf