Detecting Abuse in TLDs

A NameSentry™ presentation by
Greg Aaron and Michael Young

ICANN Toronto: 15 October 2012

© 2012 Illumintel Inc. All rights reserved.

ARCHITELOS

Defining Abuse

- Every service provider has Terms of Service (contract with users) that defines abuse.
  - TOS is how behavior on the Internet is regulated.
- For today, let us consider *abuse = exploiting Internet users*. Purposes that are deceptive, criminal, or malicious.
  - Malware
  - Phishing
  - Scams/frauds
  - Botnet command and control
- Not for today: brand infringement, hacked/infected sites, cybersquatting, hate speech, etc.

© 2012 Illumintel Inc. All rights reserved.

ARCHITELOS

How Many Domains in the World?

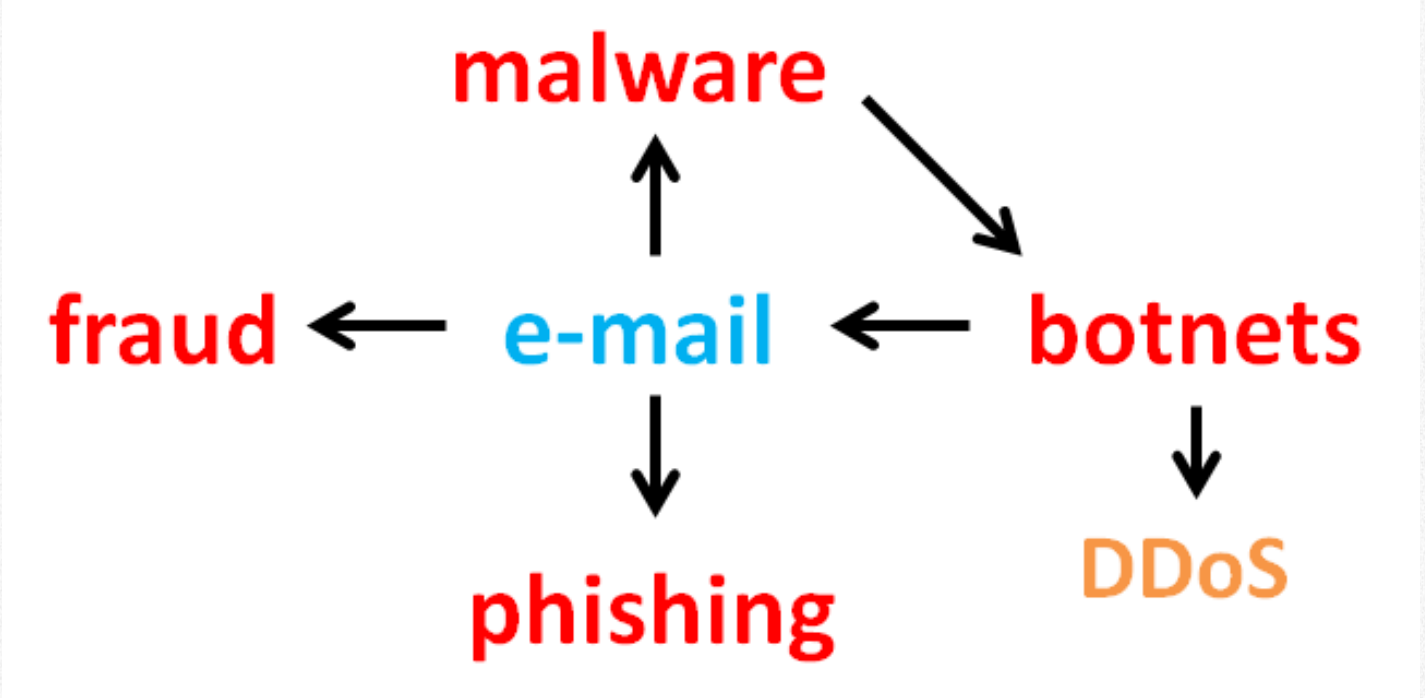
- May 2012: 240 million domains in all TLDs. *Sources: TLD registries, VeriSign/Zooknic, ICANN*
- Up from 219 million in May 2011 – growth of 21 million
- .COM/.NET renewal rate is 73%. .EU renewing at 84%.
- Assuming a 76% world renewal rate, 52.5 million + 21 million = **73 million new domains less than a year old**. That is 30% of all domains in existence.
- ~225,000 new domains registered/day.
- ~125,000 of those are in .COM, .NET, .ORG, .INFO, .BIZ, .US. *Source: DailyChanges.com – TLD zone files*

© 2012 Illumintel Inc. All rights reserved.

ARCHITELOS

Finding Problems

- Spider
- Reports from users via antivirus programs
- Traffic analysis
- Domains advertised in e-mail:



© 2012 Illumintel Inc. All rights reserved.

Abuse advertised via e-mail

ARCHITELOS

- Domains advertised in the body of e-mails: destinations users are lured to
- Consider **who** is sending, **what** they are sending, and **how**. ***Look at the behavior and intent…***
- **75% - 90% of all e-mail is abusive.**

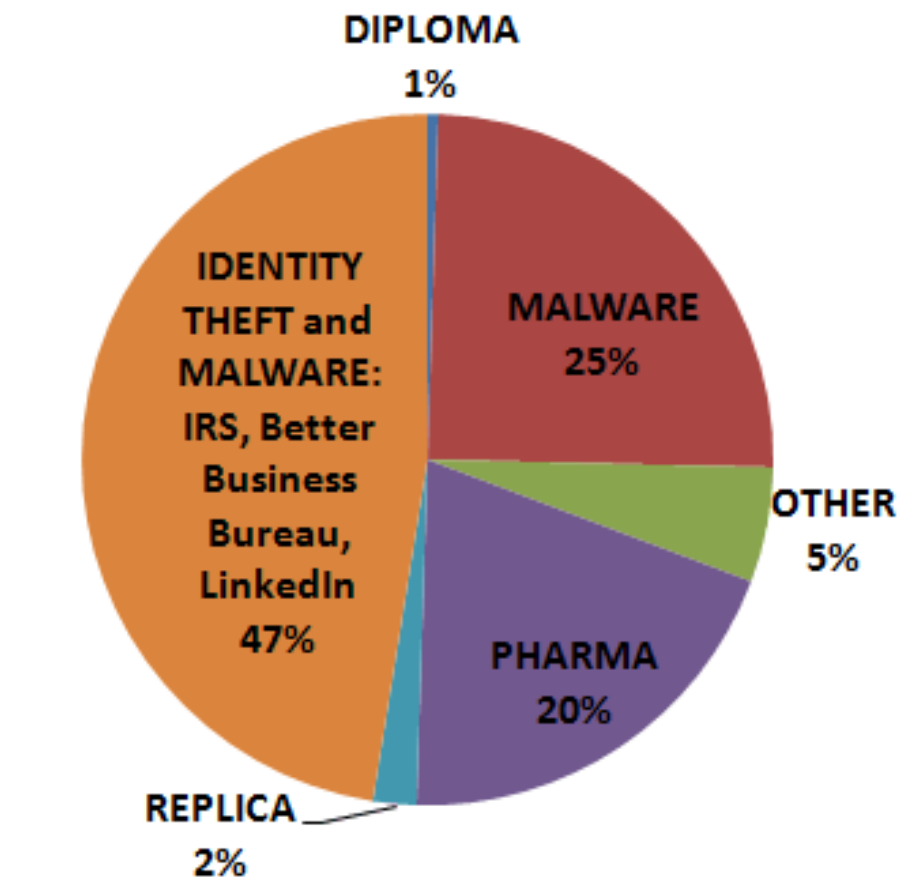
  Sources: Symantec; Trustwave; McAfee Labs; MAAWG.org: 400 million mailboxes, 250 billion bulk unsolicited messages.
- **How** is most of this mail sent? **From botnets.**

  Festi, Cutwail – billions of e-mails a day. Grum had 2.3 billion e-mail addresses.
  Source: KrebsOnSecurity.com.
- Also **"Snowshoe spam"**

  Spammers obtain IP blocks and distribute spam from it, "spreading out" their footprint. Goal is to hide origin and identity. IPs obtained by lying, and hijacking.
- Some links (domains) in e-mail lead through at least one redirect, through compromised Web sites and URL shorteners. Redirects increase the delay in getting blacklisted.

© 2012 Illumintel Inc. All rights reserved.

What are the e-mails advertising?



Internal Revenue Service
United States Department of the Treasury

After the last annual calculations of your financial activity we have concluded that you are eligible to get a tax refund of **$464**.
You may submit the tax refund application and give us 3-9 days in order to process it.

A refund can be hindered for many different reasons.
E.g., submitting invalid records or not meeting a deadline.

To get information about your tax refund please open this link.

Sincerely,
Tax Refund Department
Internal Revenue Service

© 2012 Illumintel Inc. All rights reserved.

ARCHITELOS

SURBL

- Block lists contain domains (Web sites) that appear in the bodies of unsolicited e-mail. Plus other domains registered for malware hosting sites, phishing sites.
- ~ 800,000 domains are on the list on a given day.
- ~ 6,500 new additions to the list each day (average). Domains stay on the list for varying amounts of time, ranging from a few days to a year.
- **2.4 million domain names appeared on SURBL in the last 12 months.**
- Most domains on the list are recently registered, then used/advertised shortly thereafter.
- 3-5% of listed domains are malware, and 1% are phishing.

Source: Jeff Chan/SURBL

© 2012 Illumintel Inc. All rights reserved.

ARCHITELOS

Spamhaus

- Maintains several real-time spam-blocking databases. Separate block lists for IP addresses, domain names.
- Domain Block List (DBL) contains domains advertised in body of unsolicited e-mail messages.
- ~ 331,000 domains are on the list on any given day.
- ~ 4,000 new additions to the list each day. Domains stay on the list an average of 4 months.
- **1,920,000 domains appeared on the DBL in the last 12 months.**
- 6,743,794 IPs currently listed; 8,990,271 IPs in last year.

Source: Spamhaus

© 2012 Illumintel Inc. All rights reserved.

ARCHITELOS

How Many Domains Registered for Abuse?

- SURBL and Spamhaus have an overlap of ~ 40%. Between them, **~3,456,000 unique domains listed per year**.
- Year: 3.5 million blacklisted, out of 73 million recent registrations = 5% of new registrations
- 5% is the floor. How many above that?
  - Add other sources of data
  - Blocklist providers don't find it all. In one large TLD, they did not list at least a third of domains owned by snowshoe spammers.
  - Language: Chinese phishing was under-counted by 60%. *APWG.ORG*
- 1 million+ domains being suspended each year. *(estimate)*
  - By registrars, registries, hosters. Number will remain unknown.

© 2012 Illumintel Inc. All rights reserved.

ARCHITELOS

Buying and Using the Domains

- Abusers can consume large numbers of domains. Use domains, those get blocked, and then buy new ones.
- How do they obtain all these domains?
  - Often using cash/gift cards
  - With false registrant data
  - From shady resellers
  - From willing registrars
- In most TLDs – abuse moves around.

© 2012 Illumintel Inc. All rights reserved.

NameSentry™ by Architelos Go 11 October

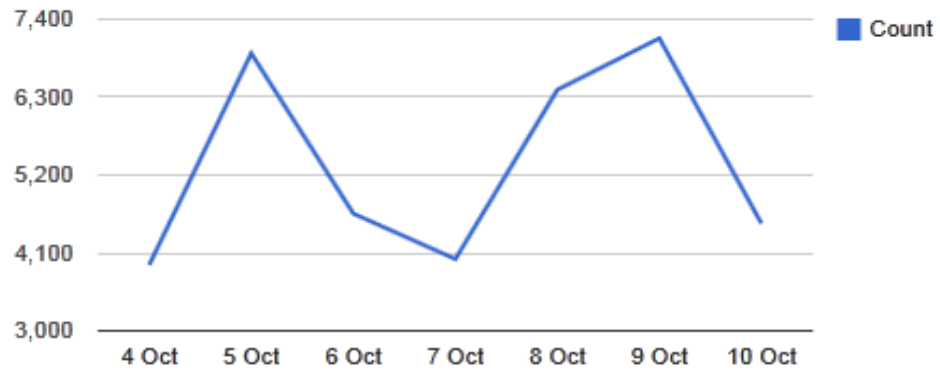
.COM Anti-Abuse Portal

- Home
- My Queues
- Abuse Types
  - Malware
  - Phishing
  - Spam
  - Infringement
- Manage Rules
- Reports
- Intelligence
- Admin
- My account
- Log out

410,278
abuse reports

5,518
new in last 24 hours

New abuse domains, last 7 days



View: 7 days | 30 days | 12 months

Latest

Last 10 domains reported:

- 54sndg837pxix9j.com NEW
- affordrabid.com NEW
- 3db5cngca5se5pd.com NEW
- 3za8m5xwx9gw92p.com NEW
- 22dizhi.com NEW
- 2p554abdzd7ah7s.com NEW
- activelife518.com NEW
- 6wgxyimhk6dms5a.com NEW
- 2komict.com NEW
- 4glm.com NEW

Abuse types

- malware: 5,499
- phishing: 590
- spam: 404,189

Sources

- Internet Identity: 590
- Malware Domain List: 1,233
- MalwareURL: 7,646
- Spyeye Tracker: 46
- Zeus RSS: 404
- Zeus: 573
- PalevoTracker: 25
- SURBL: 306,924
- Spamhaus: 161,368

ARCHITELOS

Predictions about nTLDs

- Will introduce new spaces where abuse will concentrate.
- Applicants are all proposing takedown programs, with many proposing proactive monitoring and mitigation measures.
- Active registry involvement in anti-abuse will be “the new normal”

© 2012 Illumintel Inc. All rights reserved.

ARCHITELOS

What Does It Mean For You?

1. The landscape is changing
   - Competitive landscape: new TLDs; pricing
   - Regulatory landscape
   - Crime landscape
2. Consider the needs of your organization and your users. Consider the risks they face.
3. Craft policies and procedures that are right for you, but are also effective.

© 2012 Illumintel Inc. All rights reserved.

ARCHITELOS

NameSentry™ new clients

© 2012 Illumintel Inc. All rights reserved.

Thank you.