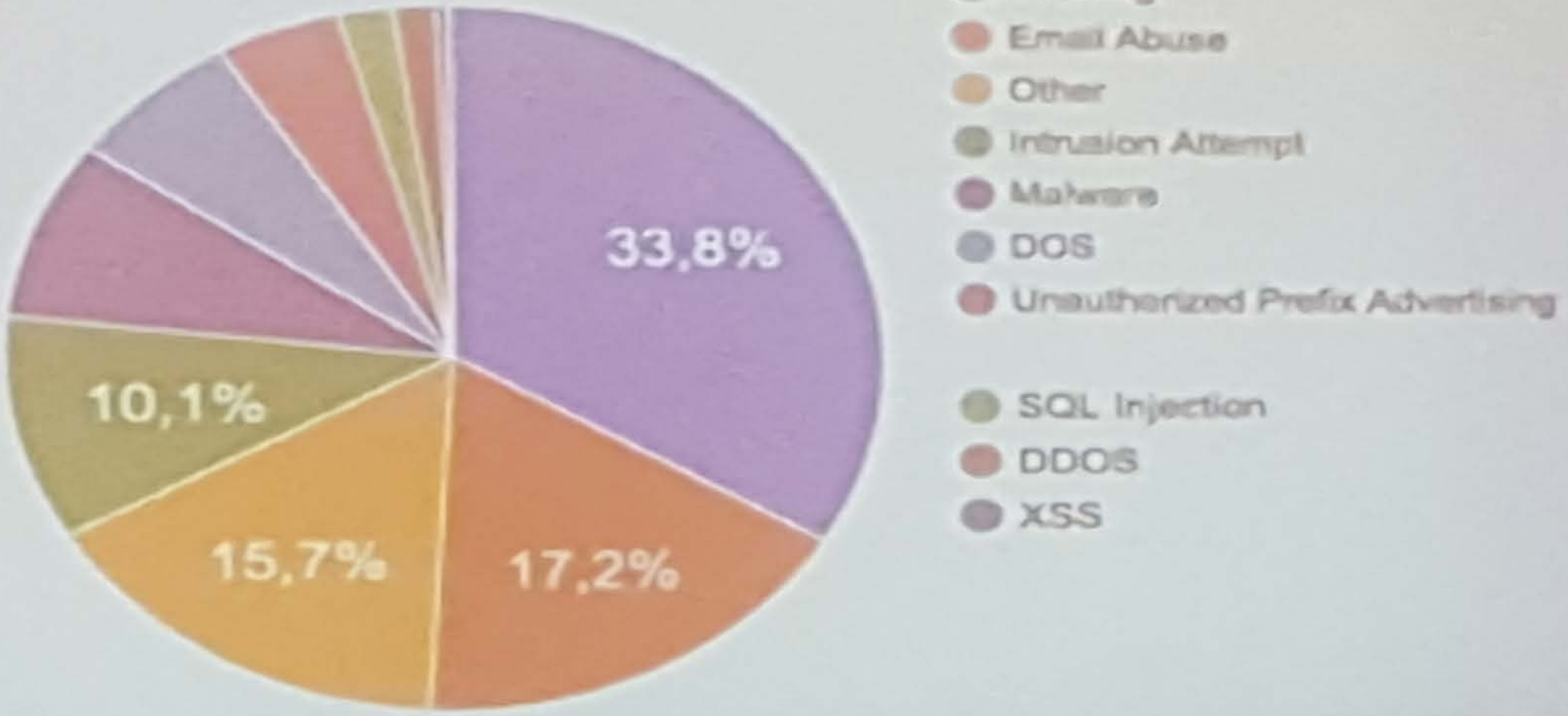
Incident Type

Security Incidents managed by WARP



Lessons ~~learned~~ to learn

- Share information when you have it for the sake of sharing
- Don't ignore threats without verifying the potential impact
- Make sure your trusted network understand the principles
- Consider using honeytokens/watermarks when sharing
- Collect unsampled flows
- Deploy SSL inspection for corporate network traffic
- Monitor traffic inside the network, not just at the perimeter

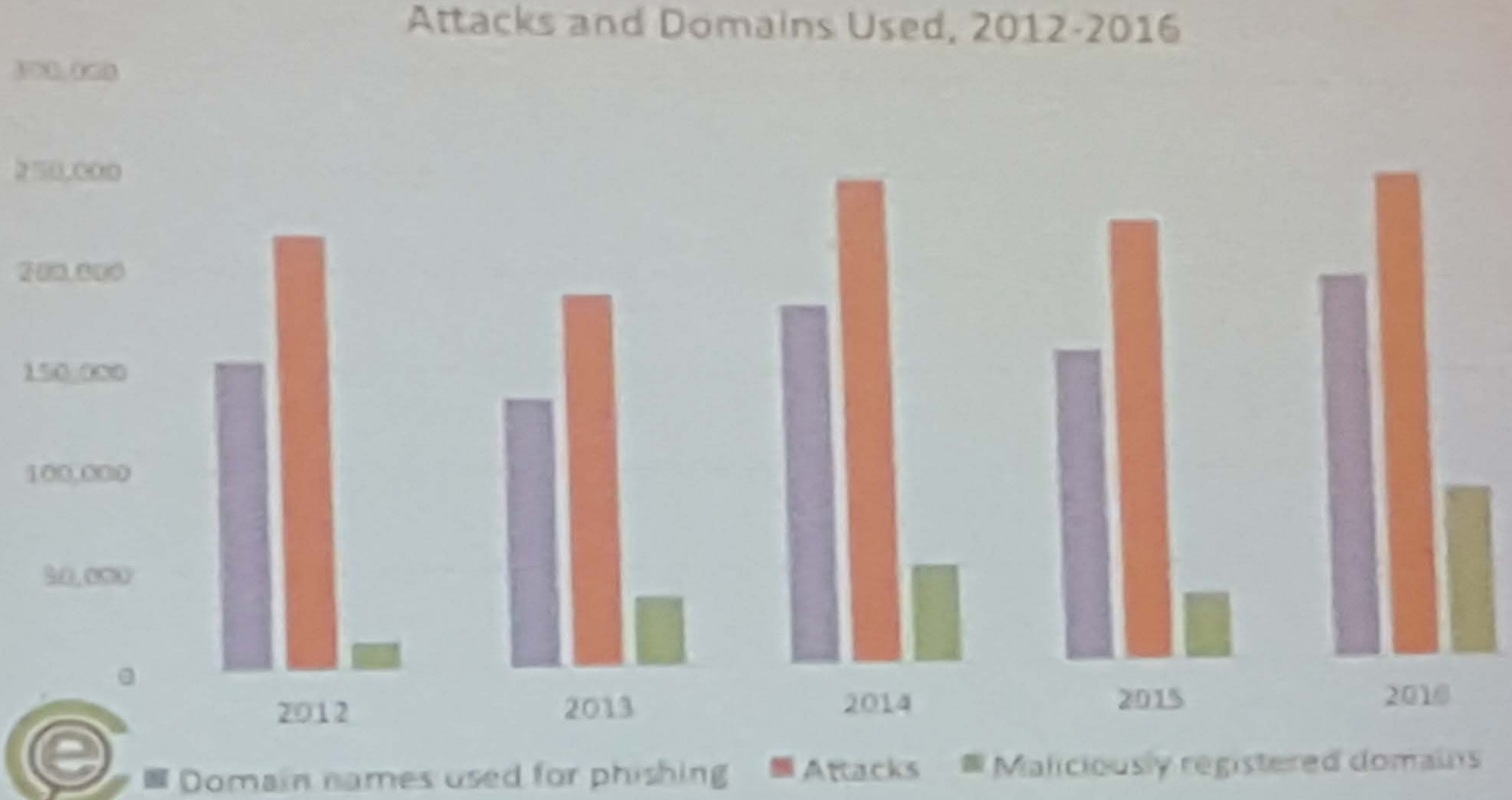
Data Driven Routines - Vetting

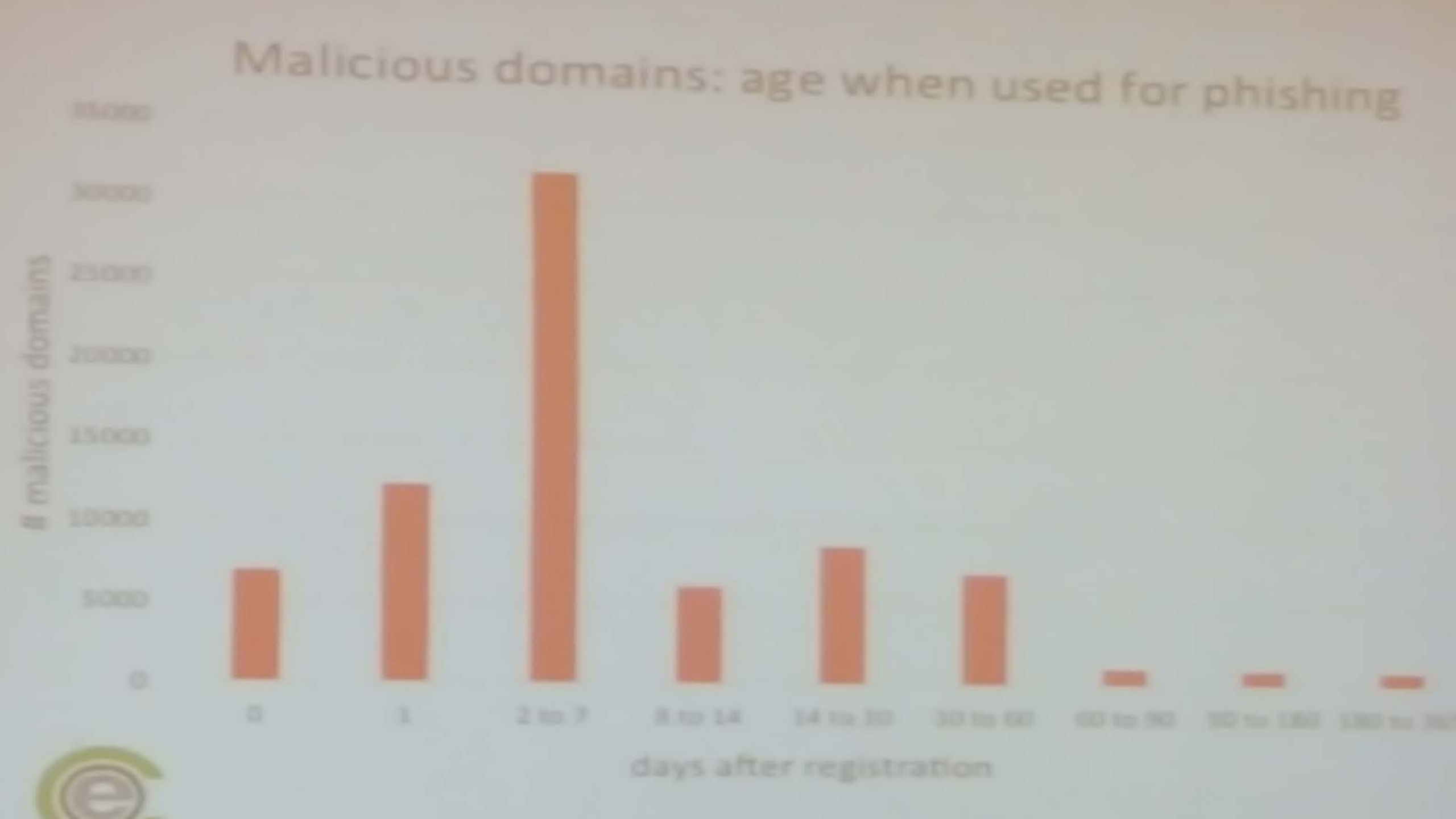
- Vetting
  - Limits on new users and accounts.
  - Reach out personally to suspicious accounts
  - Educate employees and sales teams on things to look for.
  - Preauthorization of new accounts
  - Track usage and establish a baseline of normal usage.

The Last Mile

- Takedowns are important, however, blacklisting is crucial
- Security is community driven
- Sharing is caring
- Centralization promotes collaboration and complete picture
- Everyone has their own prioritization and metrics

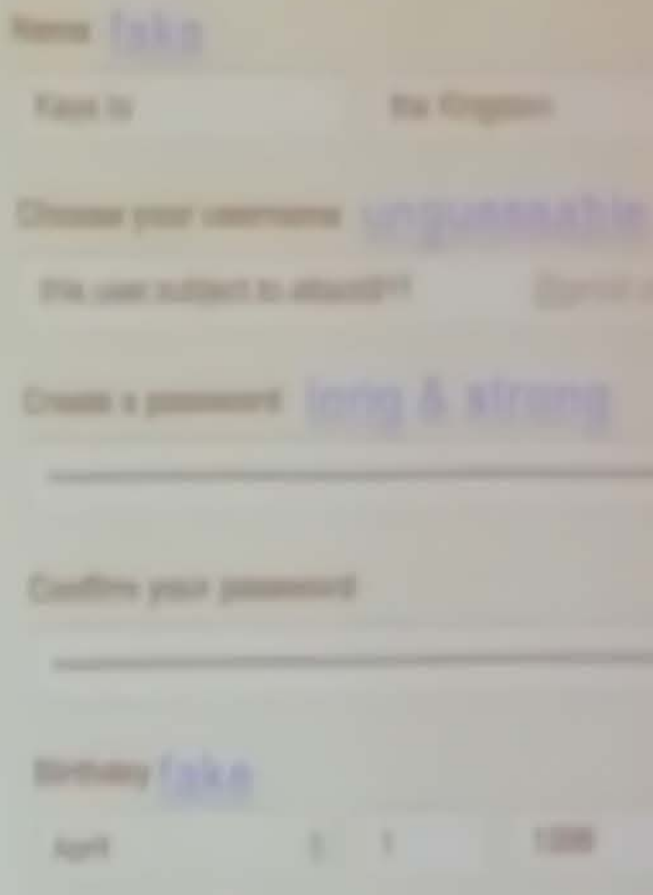
2016: 252,732 attacks, on 199,581 domains, with 88,216 malicious domain registrations




Malicious domains: age when used for phishing
malicious domains
35000
30000
25000
20000
15000
10000
5000
0
0
1
2 to 7
8 to 14
14 to 30
30 to 60
60 to 90
90 to 180
180 to 365
days after registration

Attacks on Bitcoin Exchanges

- Spear-phishing
- Targeted malware
- Elaborate phone scams
- Phone number porting



How You Can Use It

- RPZ Feeds
  - Subscribe to one or more internal/external feeds
  - Maybe build your own feed for internal use
  - Maybe offer your feed to external subscribers
- RPZ Rule Patterns
  - Qname, Wildcard, RespAddr, NSName, NSAddr, SrcAddr
- RPZ Rule Actions
  - NXDomain, Alias, NoError, Replace, or Bypass

Honeypot

I. Black market

II. Hosting/service provider in Tor

III. Underground forum

IV. Misconfigured server (FTP/SSH/IRC)

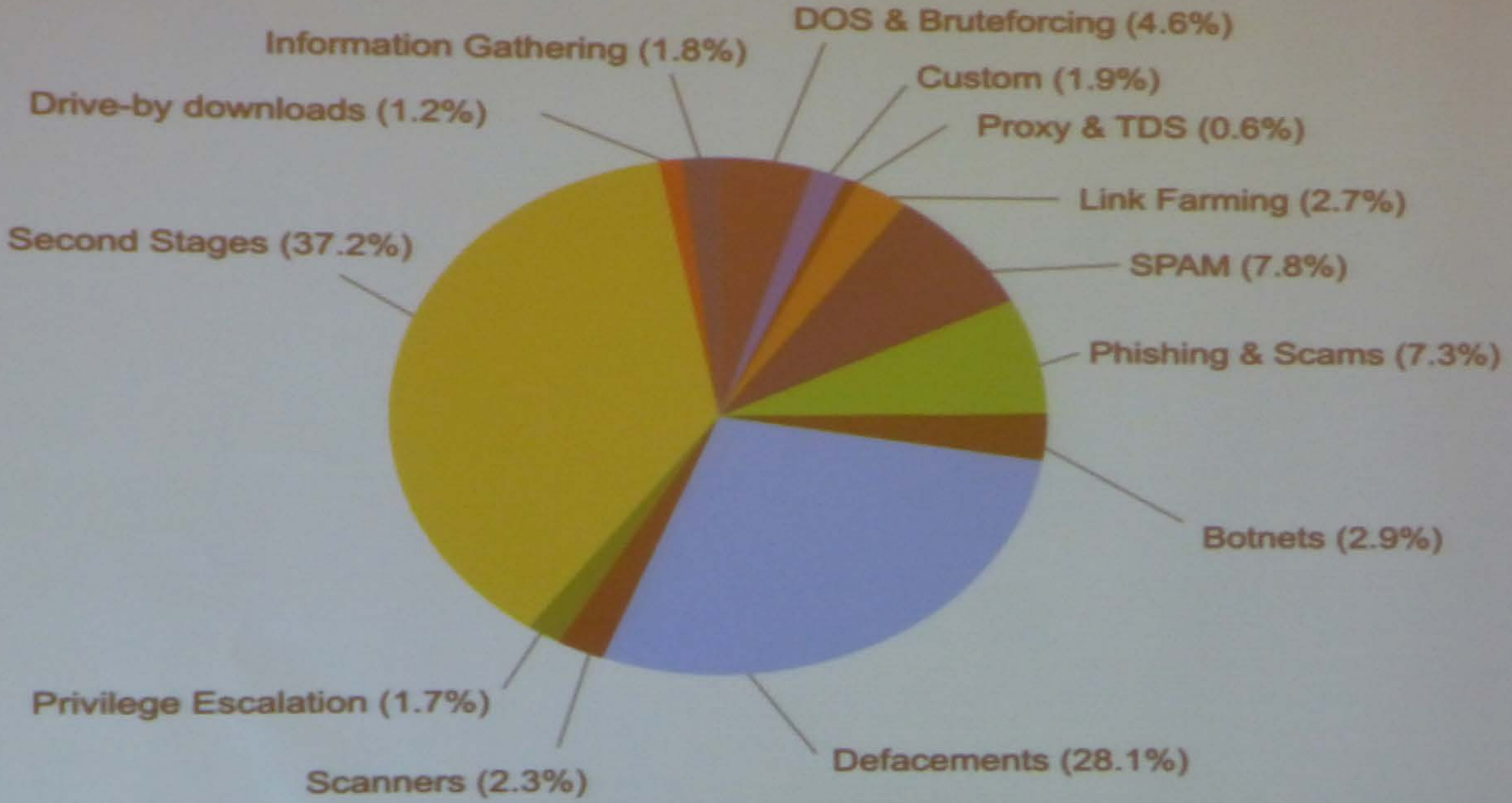
Technology

I. OsCommerce

II. WordPress + Shells

III. Custom

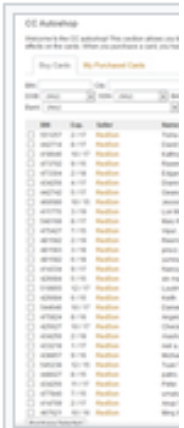
IV. Debian Linux



[Canali et al. NDSS 2013]

Resale [edit]

Stolen data may be bundled as a 'Base' or 'First-hand base' if the seller participated in the theft themselves. Resellers may buy 'packs' of dumps from multiple sources. Ultimately, the data may be sold on darknet markets and other carding sites and forum 'dump shops'[11] specialising in these types of illegal goods.[12][13]



An manage
AlphaBay d

On the more sophisticated of such sites, individual 'dumps' may be purchased by zip code and country so as to avoid alerting banks about their misuse.[14] Automatic checker services perform validation en masse in order to quickly check if a card has yet to be blocked. Sellers will advertise their dump's 'valid rate', based on estimates or checker data. Cards with a greater than 90% valid rate command higher prices. 'Cobs' or changes of billing are highly valued, where sufficient information is captured to allow redirection of the registered card's billing and shipping addresses to one under the carder's control.[15]

Full identity information may be sold as 'Fullz' inclusive of social security number, data of birth and address to perform more lucrative identity theft.[16][17]

Fraudulent vendors are referred to as 'rippers', vendors who take buyer's money then never deliver. This is increasingly mitigated via forum and store based feedback systems as well as through strict site invitation and referral policies.[18]

Whilst some carding forums will exist only on the dark web, today most exist on the internet, and many will use the Cloudflare network protection service.[

Estimated per card prices, in US$, for stolen payment card data 2015[22]

Payment Card Number With CVV2	United States	United Kingdom	Canada	Australia	European Union
Software-generated	$5–8	$20–$25	$20–$25	$21–$25	$25–$30
With Bank ID Number	$15	$25	$25	$25	$30
With Date of Birth	$15	$30	$30	$30	$35
With Fullzinfo	$30	$35	$40	$40	$45

Specialization and prices

	Specialized users			Unspecialized users		
	№	%	$	№	%	$
CVVs	166	39.1	9.28	299	54.7	10.46
Dumps	193	45.4	32.56	41	7.5	42.61
Fullz	45	10.6	35.86	95	17.4	30.20
Paypal	21	4.9	1.99	112	20.5	3.17
Total	425	100.0		547	100.0	