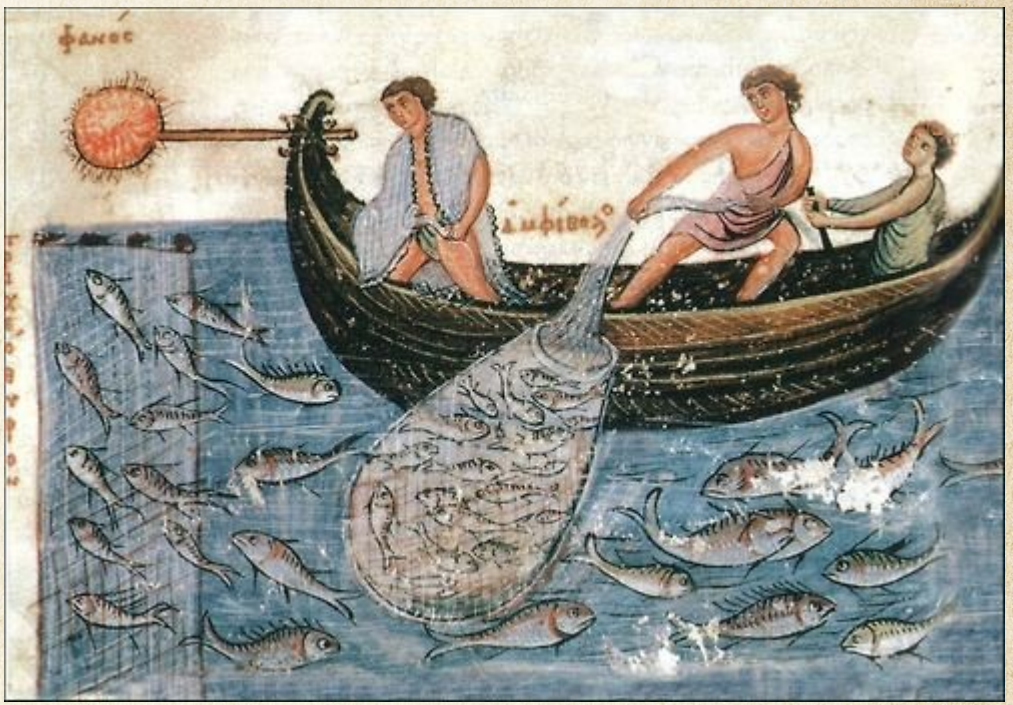
Domains of Greys
or
DNS Greylisting for Phun and Phishing Prevention

Eric Rand / @munin and Nik LaBelle

August, 2016

Phishers of Men – the Workflow Behind a Standard Phishing Attack

This is a generic attack scenario to use as an example to illustrate the concept.



* Send an Email to the Victim

* Victim clicks on the link and is sent to a plausible looking page

* Victim enters credentials; phisher collects those credentials

Phishing Works
Training Doesn't

Even with training, many users still click – about half for generic campaigns; up to 80% for spearphishing.

Training is largely ineffective, expensive, and requires frequent refreshes.

SMBs often do not have the time nor resources to engage in proper training.

Sources:
http://www.mcafee.com/us/about/news/2014/q3/20140904-01.aspx
https://www.engadget.com/2014/11/08/google-says-the-best-phishing-scams-have-a-45-percent-success-r/
https://www.computer.org/cms/Computer.org/ComputingNow/pdfs/IEEESecurityPrivacy-SpearPhishing-Jan-Feb2014.pdf

State of the Art:
Technical Countermeasures

Mail Header Rewrites to designate externally-sourced emails

(Low adoption; people expect external emails from customers)

Spam Filters

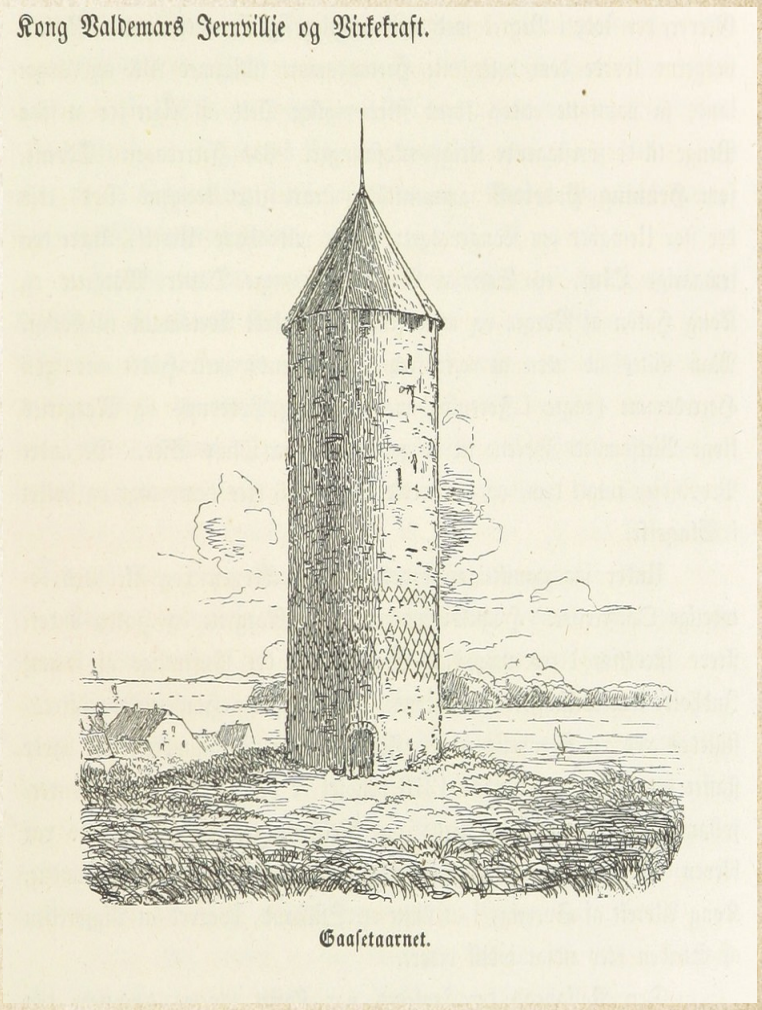
(Help a lot, but only partially mitigate the problem)

Blacklisting

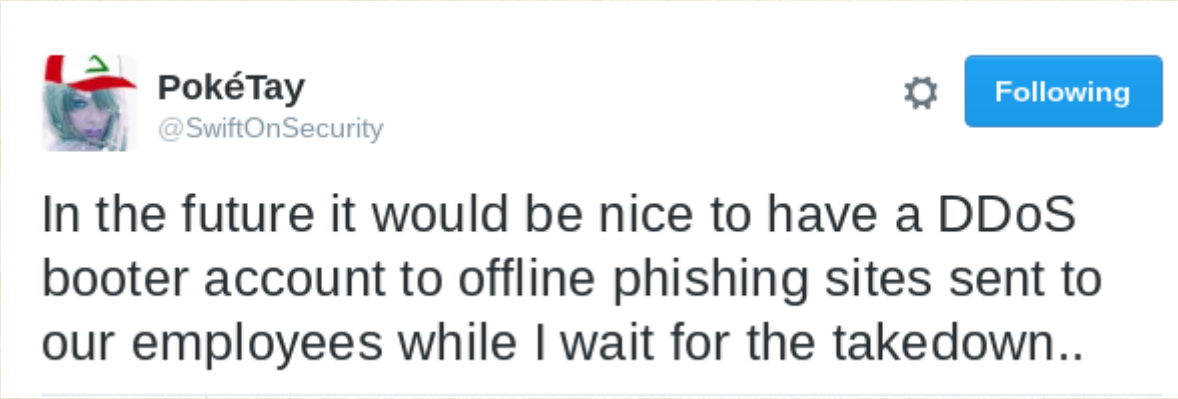
(Expensive, and reactive; often irrelevant to spearphishing campaigns)

Whitelisting

(Do you want new customers, ever?)



Frustration Ensues



Changing Tack

MERCHANT-MARINE, MAKING FOR PORT.

Analyze the workflow for a typical phisher

Phishing has logistical requirements – and these logistics have associated costs.

Phishing is a business! They want to increase revenues and minimize costs.

What things make phishing attacks fail already?

Points of Failure

Spam filters, like greylisting: unknown senders get delayed; email could be missed by target.

Password managers won't autofill on phishing domains.

….hey, wait a minute!

You Can't Phish a Machine

Phishing is inherently social, not technical.

People can be fooled by layouts, but password managers are 'dumb' – they only see the domain.

Unfortunately, password manager adoption only works if everyone cooperates to allow them.

(viz. https://www.wired.com/2015/07/websites-please-stop-blocking-password-managers-2015/) et al.

Borrowing the Machine's Vision

DNS sinkholing works pretty well in the real world for malware (and ad) blocking.

Phishing requires DNS to send the victim to the site.

Blacklists are reactive, though – can't block it 'til you know it's there – and by the time you know it's there, they've moved on.

Many phishing domains last a very short time – less than 24h as of 2012!

Sources:
https://www.usenix.org/legacy/event/leet08/tech/full_papers/mcgrath/mcgrath_html/index.html
https://docs.apwg.org/reports/APWG_GlobalPhishingSurvey_1H2012.pdf

Phishing is a Short Con

The attackers use the credentials they harvest quickly.

Phishers pivot to new campaigns quickly.

Lots of people are very invested in taking them down quickly – have to keep moving.

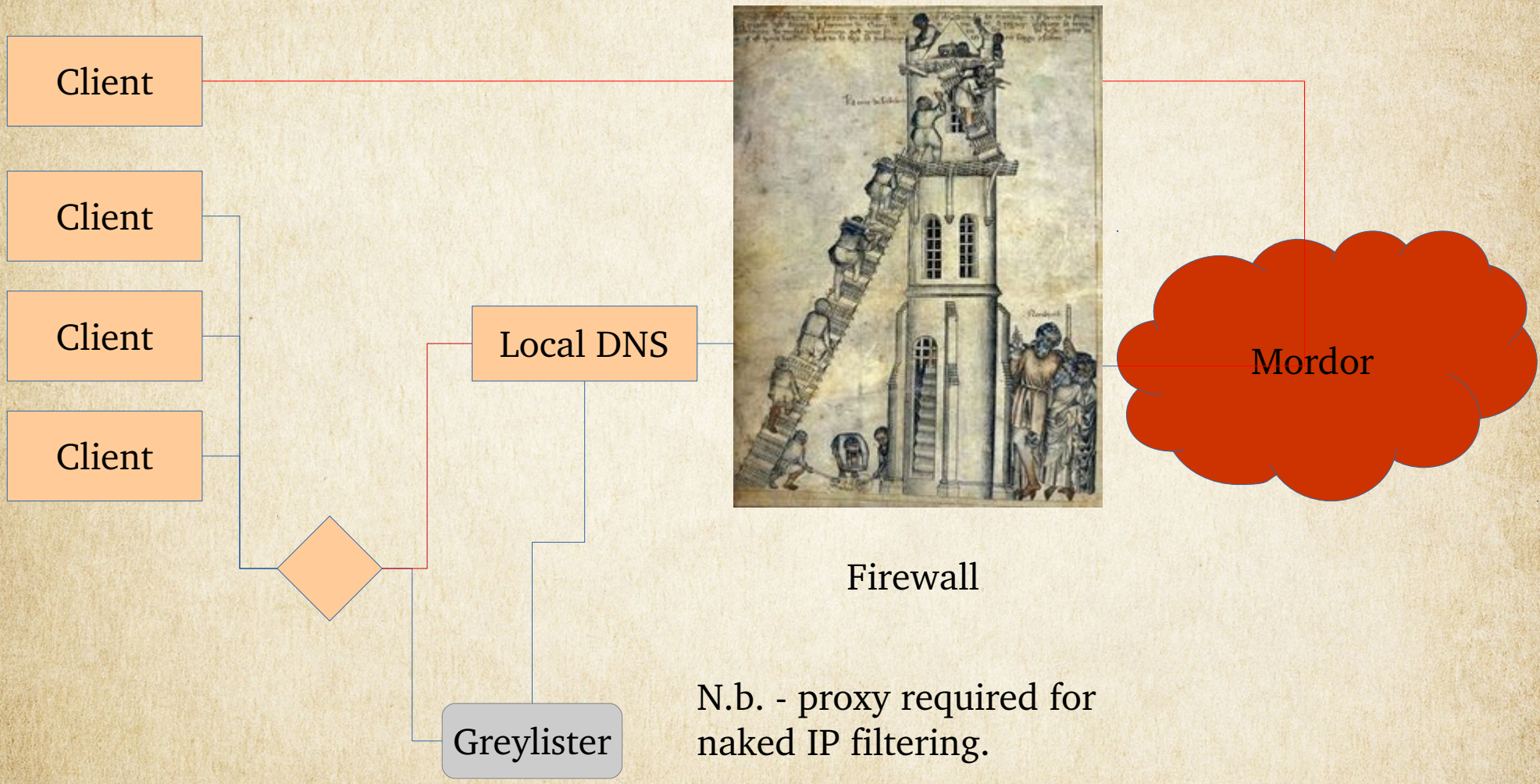
Blacklists may be reactive, but they catch up eventually.

They are forced to move quickly.

Paint it Grey

If you can delay phishing domains from resolving on your network, you can reduce the likelihood of your users being successfully phished.

Constructing your Countermeasures



Firewall

N.b. - proxy required for naked IP filtering.

POC

This is not production-ready software: use at your own risk!

Supports blacklisting, whitelisting

Whitelist local domain & known-good services

Blacklist known-bad & when you get suspicious greylist entries

Greylist writes logfiles – export to your SIEM!

24h greyout; 7 day blackout by default; configure per your needs

Drawbacks

Needs to have a very controlled network environment – the firewalling and proxies are mandatory for this to work.

May break some SSO type operations that rely on multiple redirects – Google Auth, for instance – at least temporarily until you whitelist.

Habitual Reddit surfers are going to have a bad time getting first posts.

But Wait! There's More!

Now that we're controlling how quickly newly seen domains resolve, what else can we break?

Botnet C&C!

Downloader Trojans!

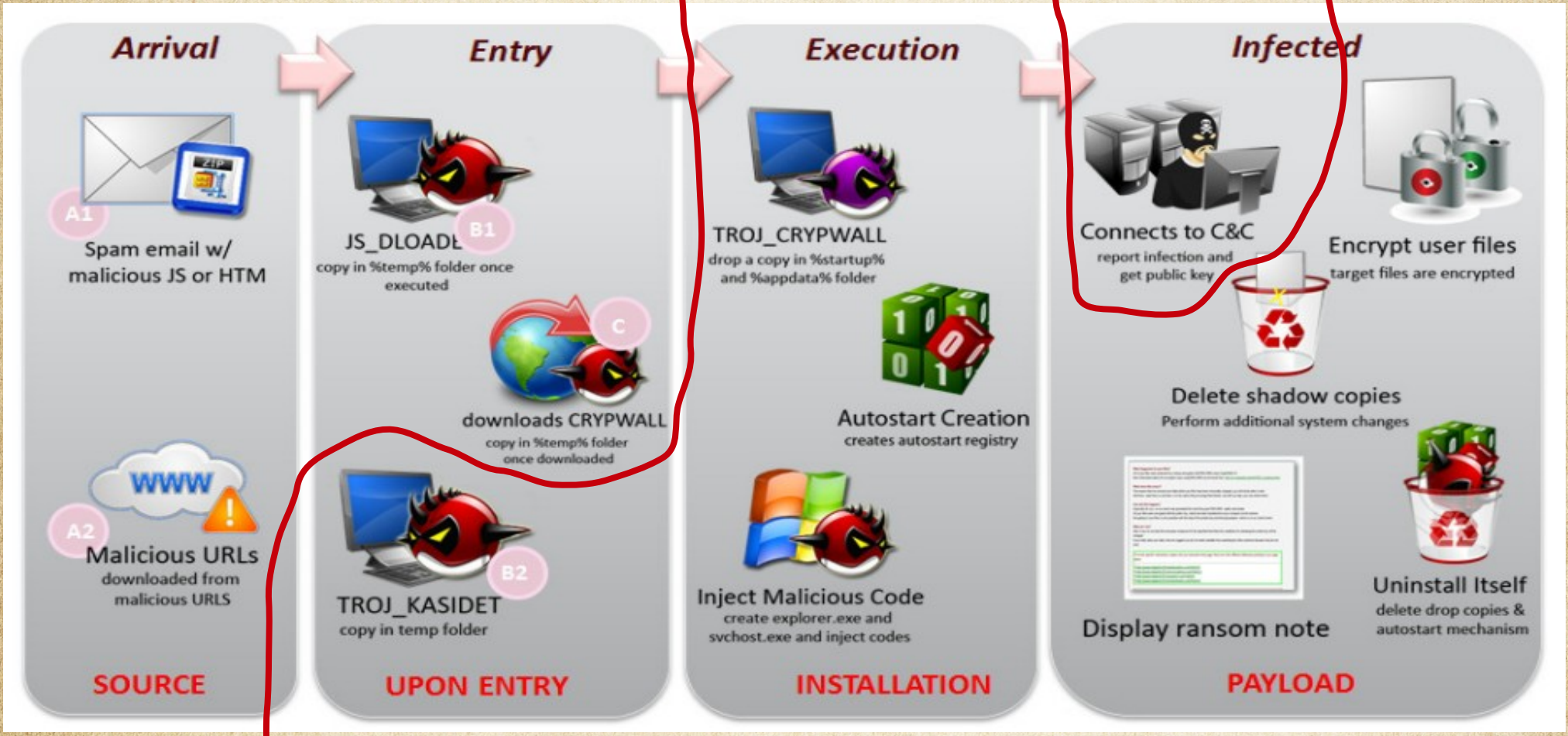
Typosquatting!

Bitsquatting!

Ransomware controls!

Foolish employees visiting pastebin for the first time!

Special Deliveries



Terra Incognita

Plenty of new avenues to develop - we've only scraped the surface of this particular technique.

Add functionality to foghorn – there's lots more DNS that could benefit here.

Other kinds of attack tools can be used for defensive roles.

Analyze other kinds of attacks to see how they can be slowed to the defender's advantage.

Final Remarks

Here's the code:

https://github.com/hasameli/foghorn

Use at your own risk!

Questions?

Many thanks to all those who assisted in refining the concept, pointed to research, and otherwise helped make this happen!