Dial One for Scam: A Large-Scale Analysis of **Technical Support Scams**

PragSec Lab

Stony Brook University

Najmeh Miramirkhani

Oleksii Starov

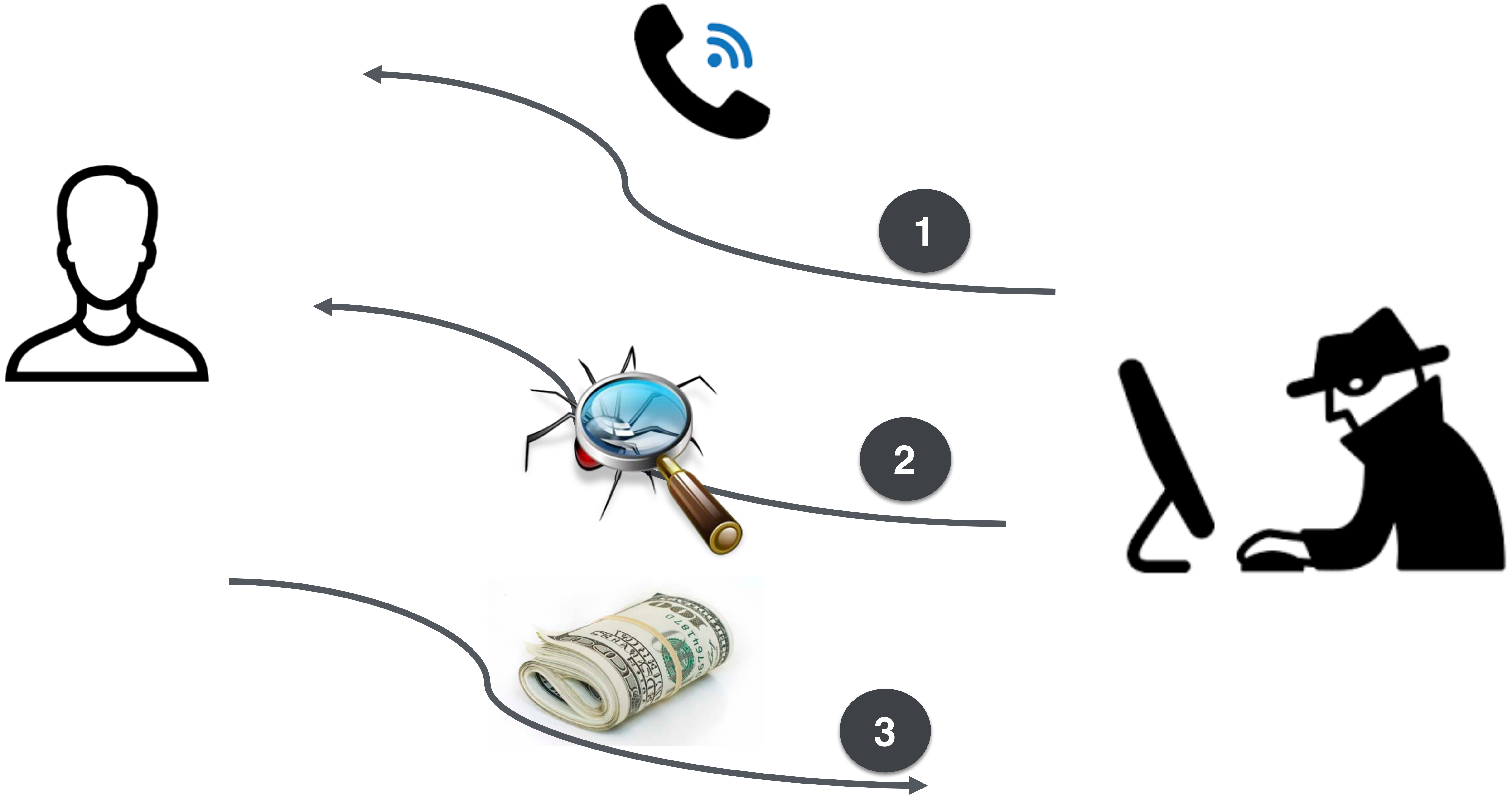
Nick Nikiforakis

What are Tech Support Scams?

Tech Support Scam Evolution

2008	Fake support cold calls
2013	A Twist: Scammers started to use malvertising
2014	IC3 issued a public service announcement
2014	Microsoft sued several campaigns
2015	FTC took down several big campaigns
2016	IC3 issued a public service announcement
2017	Got more aggressive and still an increasing threat

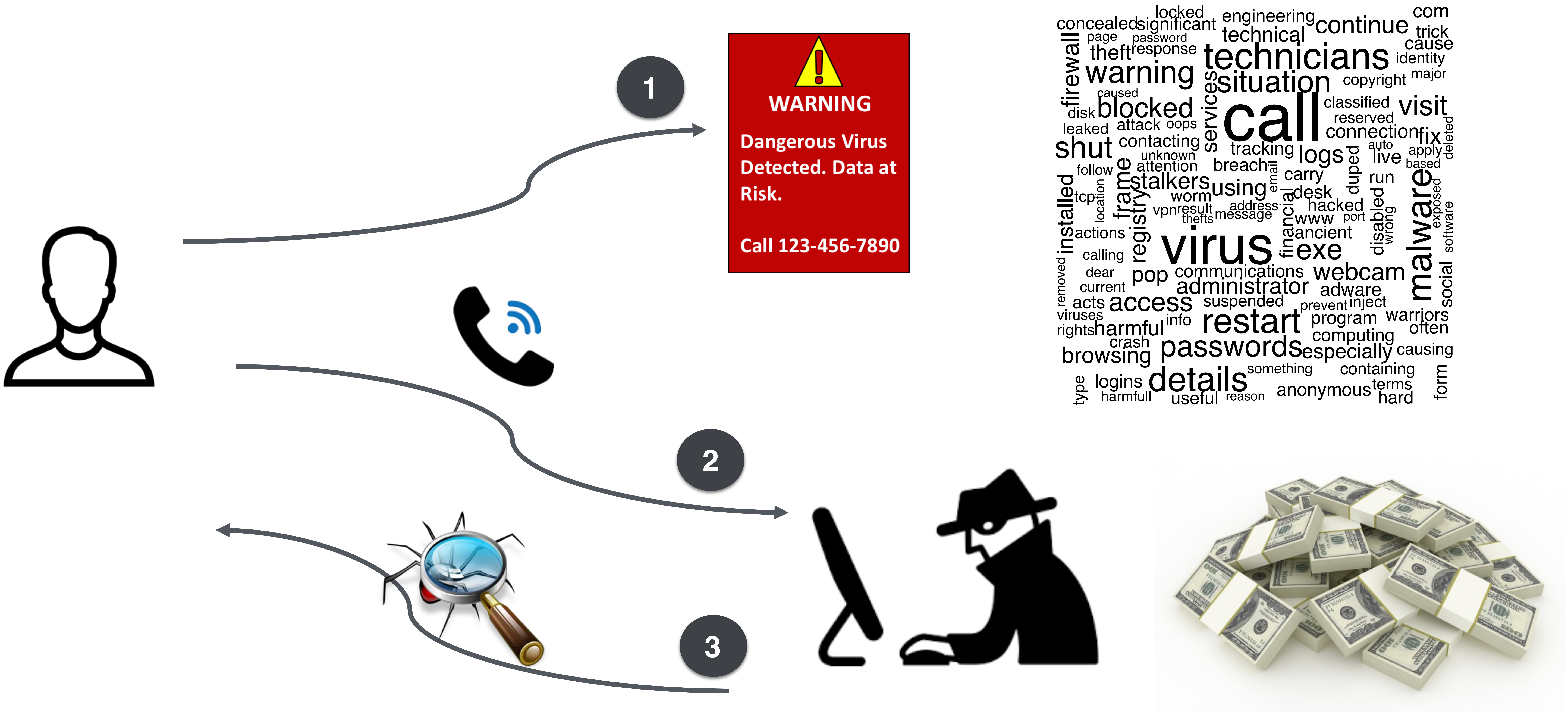
Tech Support Scam (Cold Calls)



Tech Support Scam Evolution

2008	Fake support cold calls
2013	A Twist: Scammers started to use malvertising
2014	IC3 issued a public service announcement
2014	Microsoft sued several campaigns
2015	FTC took down several big campaigns
2016	IC3 issued a public service announcement
2017	Got more aggressive and still an increasing threat

Tech Support Scam (malvertising)



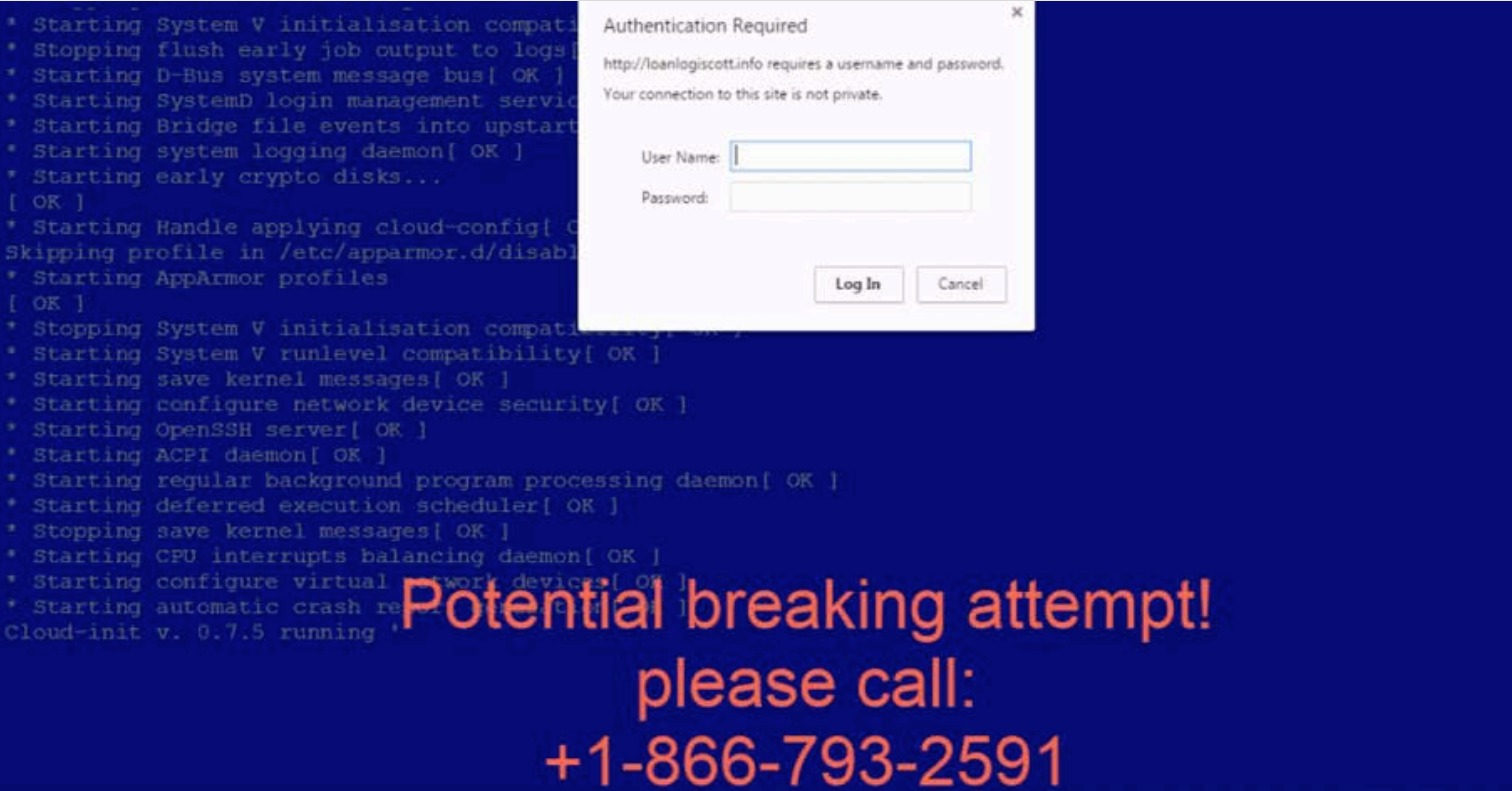
WARNING

Dangerous Virus Detected. Data at Risk.

Call 123-456-7890

1
2
3
locked
concealed significant engineering continue com
page password technical trick
firewall theft response technicians cause
identity
warning situation copyright major
services
caused
disk blocked call classified visit
reserved
leaked attack oops connection fix deleted
shut contacting tracking logs auto
unknown live apply
follow attention breach duped based
frame email carry run
installed stalkers using
tcp location registry worm financial desk malware exposed
vpn result address hacked disabled
thefts message www port wrong
actions ancient
virus exe software
calling
removed
dear pop communications webcam social
current administrator adware
acts access suspended prevent inject
viruses info restart program warriors
rights harmful often
crash computing
browsing passwords especially causing
something containing
type logins details anonymous terms form
harmfull useful reason hard

Tech Support Scam Page(1)



```
* Starting System V initialisation compati
* Stopping flush early job output to logs[
* Starting D-Bus system message bus[ OK ]
* Starting SystemD login management servic
* Starting Bridge file events into upstart
* Starting system logging daemon[ OK ]
* Starting early crypto disks...
[ OK ]
* Starting Handle applying cloud-config[ O
Skipping profile in /etc/apparmor.d/disabl
* Starting AppArmor profiles
[ OK ]
* Stopping System V initialisation compatibility[ OK ]
* Starting System V runlevel compatibility[ OK ]
* Starting save kernel messages[ OK ]
* Starting configure network device security[ OK ]
* Starting OpenSSH server[ OK ]
* Starting ACPI daemon[ OK ]
* Starting regular background program processing daemon[ OK ]
* Starting deferred execution scheduler[ OK ]
* Stopping save kernel messages[ OK ]
* Starting CPU interrupts balancing daemon[ OK ]
* Starting configure virtual network devices[ OK ]
* Starting automatic crash re
Cloud-init v. 0.7.5 running '
```

Authentication Required

http://loanlogiscott.info requires a username and password.

Your connection to this site is not private.

User Name:

Password:

Potential breaking attempt!
please call:
+1-866-793-2591

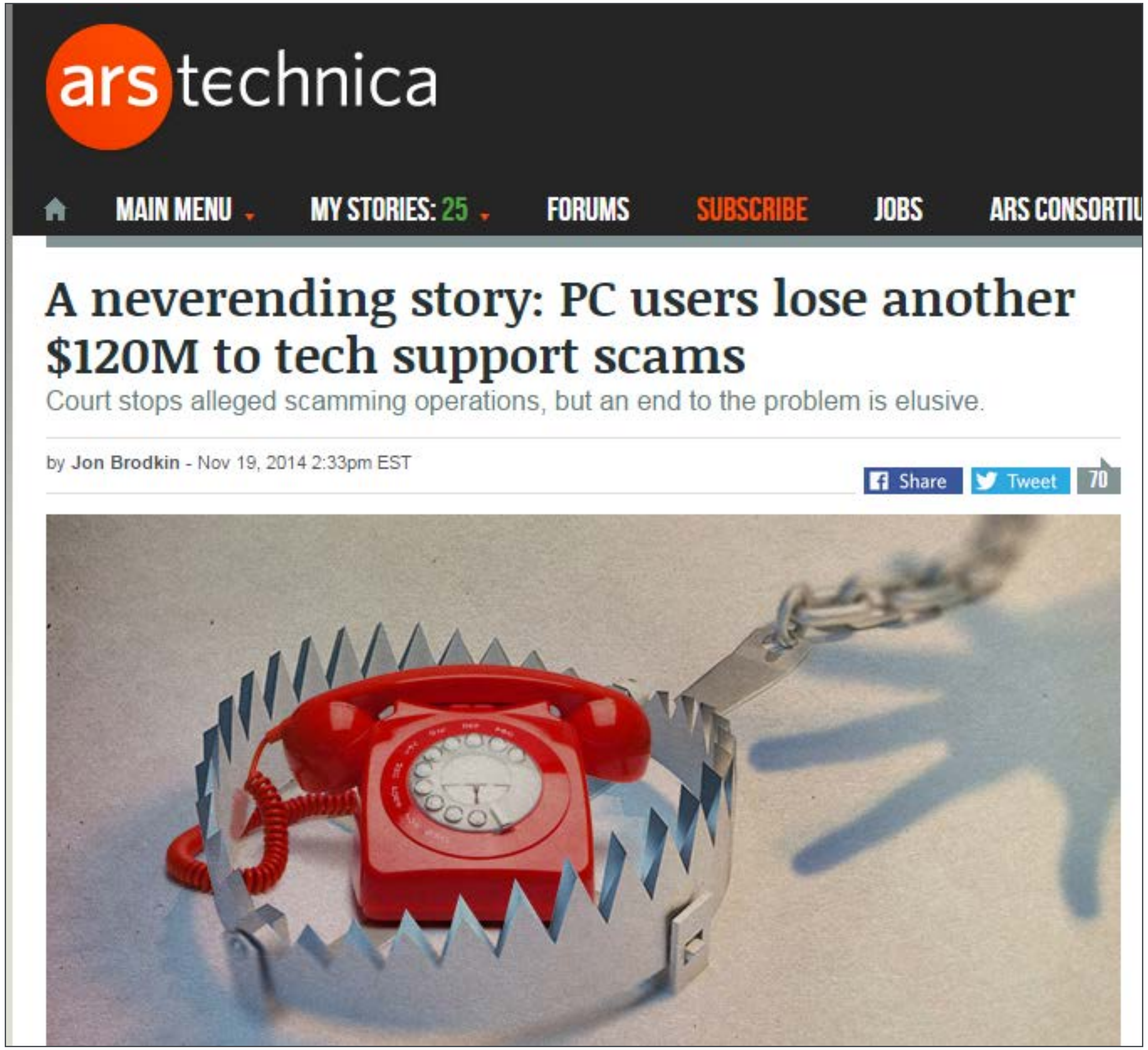
Tech Support Scam Evolution

2008	Fake support cold calls
2013	A Twist: Scammers started to use malvertising
2014	IC3 issued a public service announcement
2014	Microsoft sued several campaigns
2015	FTC took down several big campaigns
2016	IC3 issued a public service announcement
2017	Got more aggressive and still an increasing threat

Tech Support Scam Evolution

2008	Fake support cold calls
2013	A Twist: Scammers started to use malvertising
2014	IC3 issued a public service announcement
2014	Microsoft sued several campaigns
2015	FTC took down several big campaigns
2016	IC3 issued a public service announcement
2017	Got more aggressive and still an increasing threat

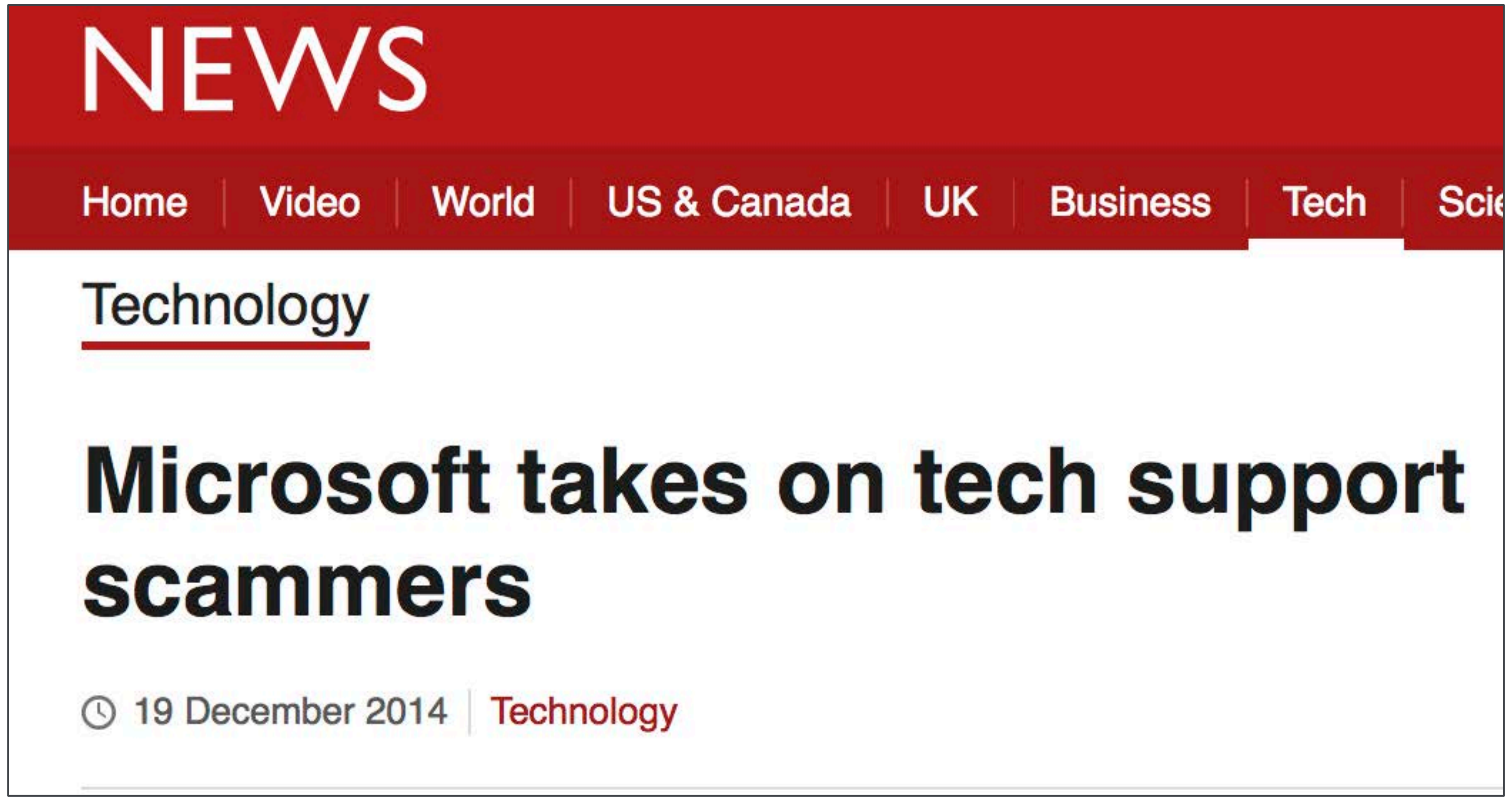
Growth of 200%



A neverending story: PC users lose another $120M to tech support scams

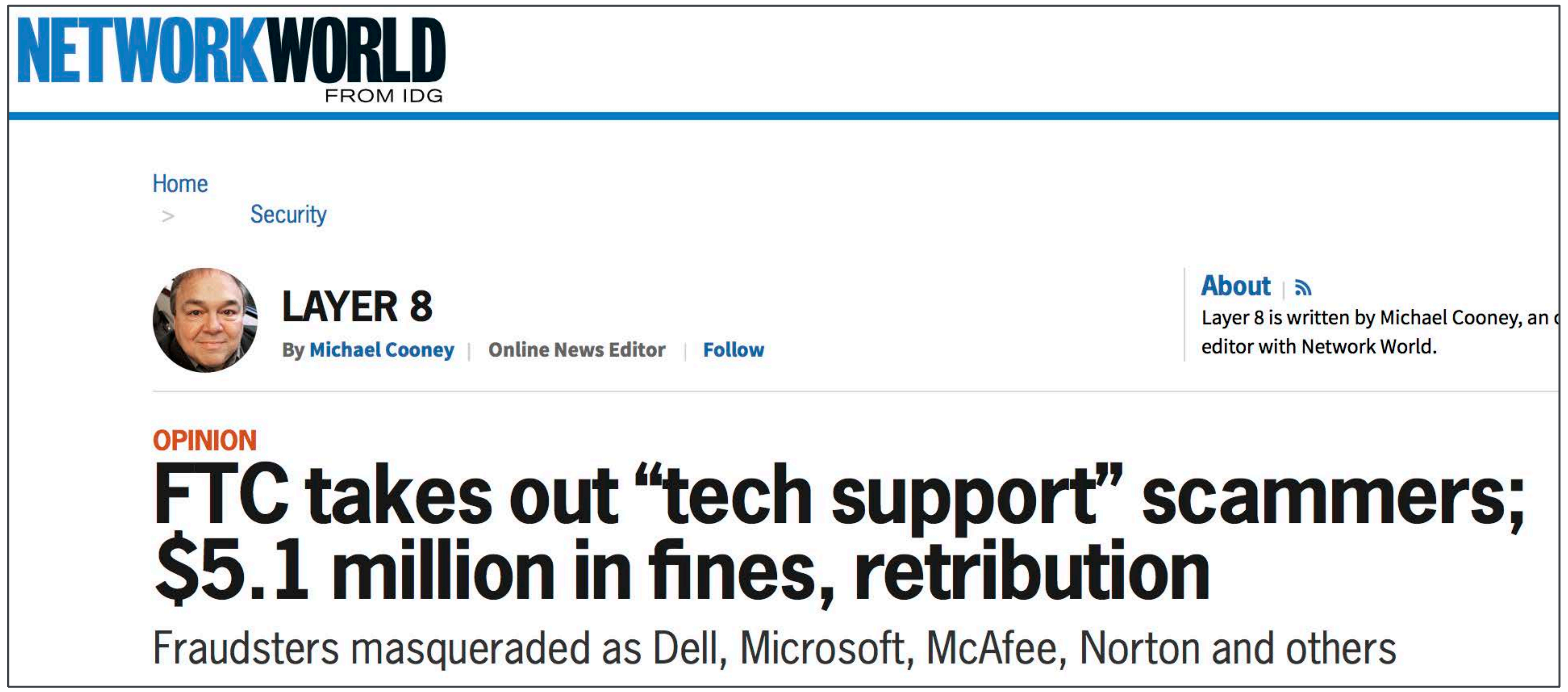
Court stops alleged scamming operations, but an end to the problem is elusive.

by Jon Brodkin - Nov 19, 2014 2:33pm EST



Microsoft takes on tech support scammers

19 December 2014 | Technology



LAYER 8

By Michael Cooney | Online News Editor | Follow

About

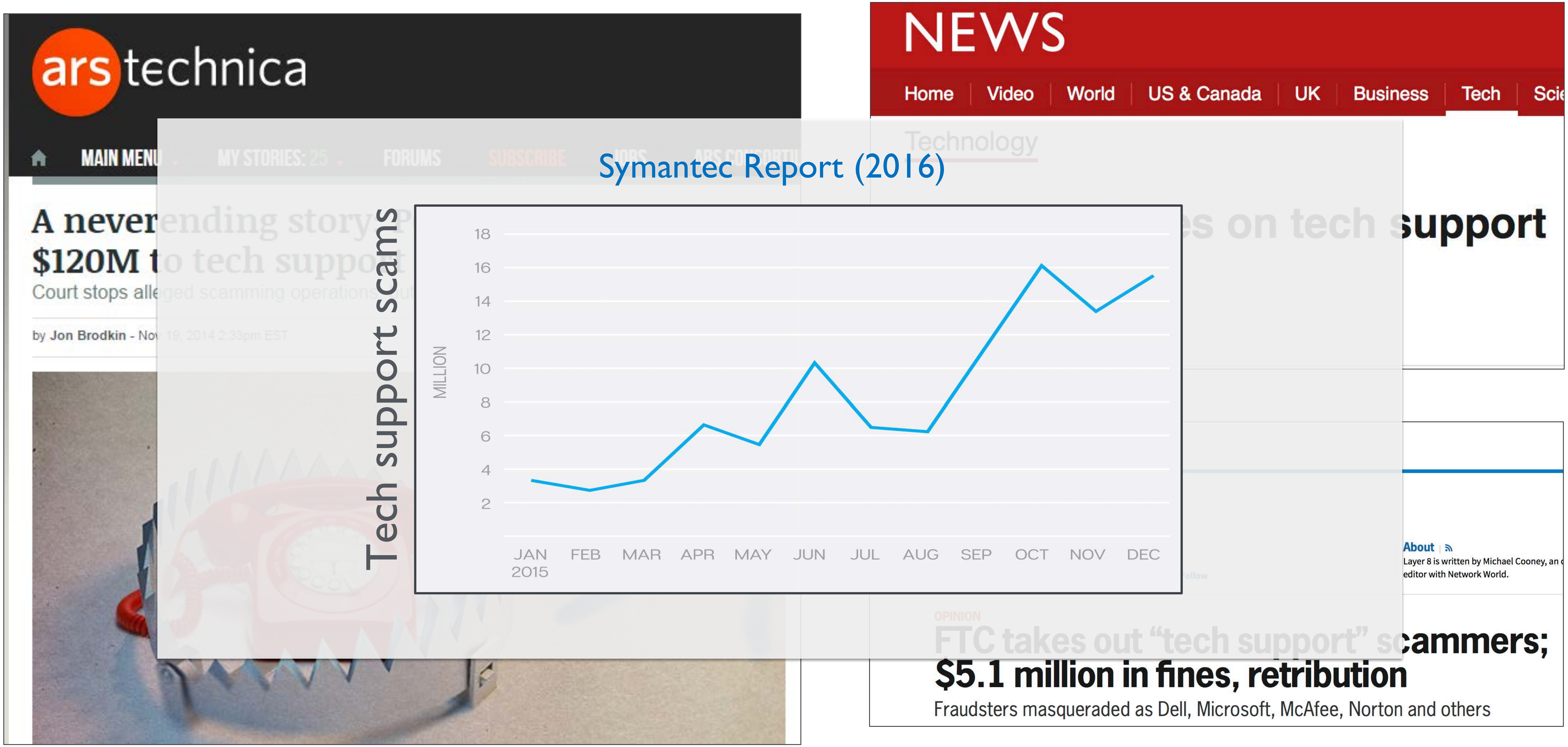
Layer 8 is written by Michael Cooney, an editor with Network World.

OPINION

FTC takes out “tech support” scammers; $5.1 million in fines, retribution

Fraudsters masqueraded as Dell, Microsoft, McAfee, Norton and others

Growth of 200%



A neverending story: P $120M to tech support

Court stops alleged scamming operations ou

by Jon Brodkin - Nov 19, 2014 2:33pm EST

es on tech support

Symantec Report (2016)

Layer 8 is written by Michael Cooney, an e editor with Network World.

OPINION

FTC takes out "tech support" scammers; $5.1 million in fines, retribution

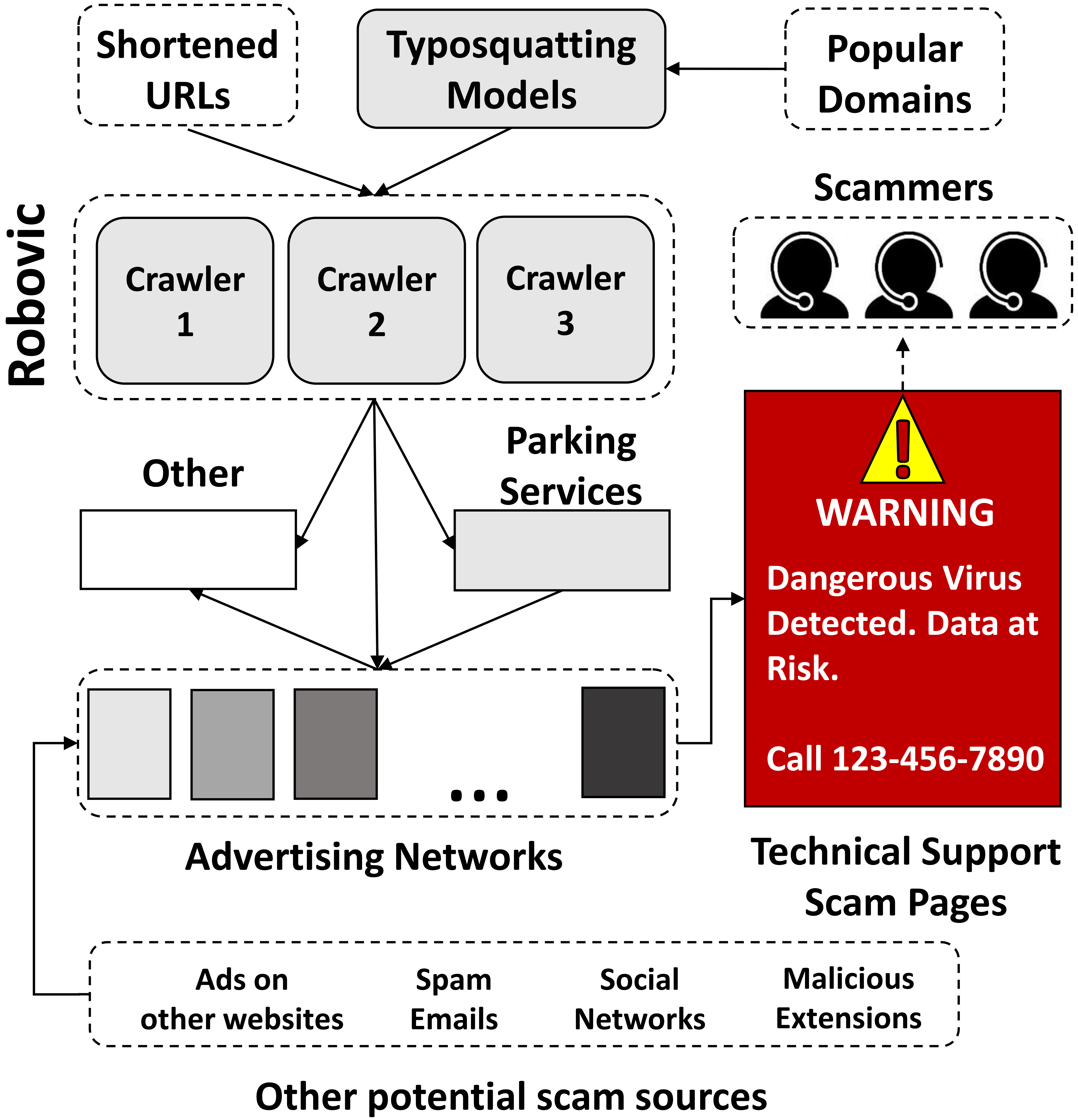
Fraudsters masqueraded as Dell, Microsoft, McAfee, Norton and others

Research Goals

- Systematic study of Tech Support Scam ecosystem
- To investigate the:
  - Prevalence
    - # Domains, # Phone Numbers, and #Scam Campaigns
  - Details about the underlying infrastructure
    - Hosting providers, ASes, and Telecommunication companies
  - Evasion and social engineering techniques
    - Tools used, call-center infrastructures, and prices

Tool Design (Robovic)

Data Collection Methodology



Collected Scam Domains

- Over 8 months
  - Crawled 8 Million domains
  - Resolved 5 Million domains
  - Detected 22,000 scam URLs
  - Extracted 8,600 unique scam domains
  - 1500 phone numbers

Short and readable domains

- computer-warning-message[.]com
- donotclose[.]website
- input-error[.]net

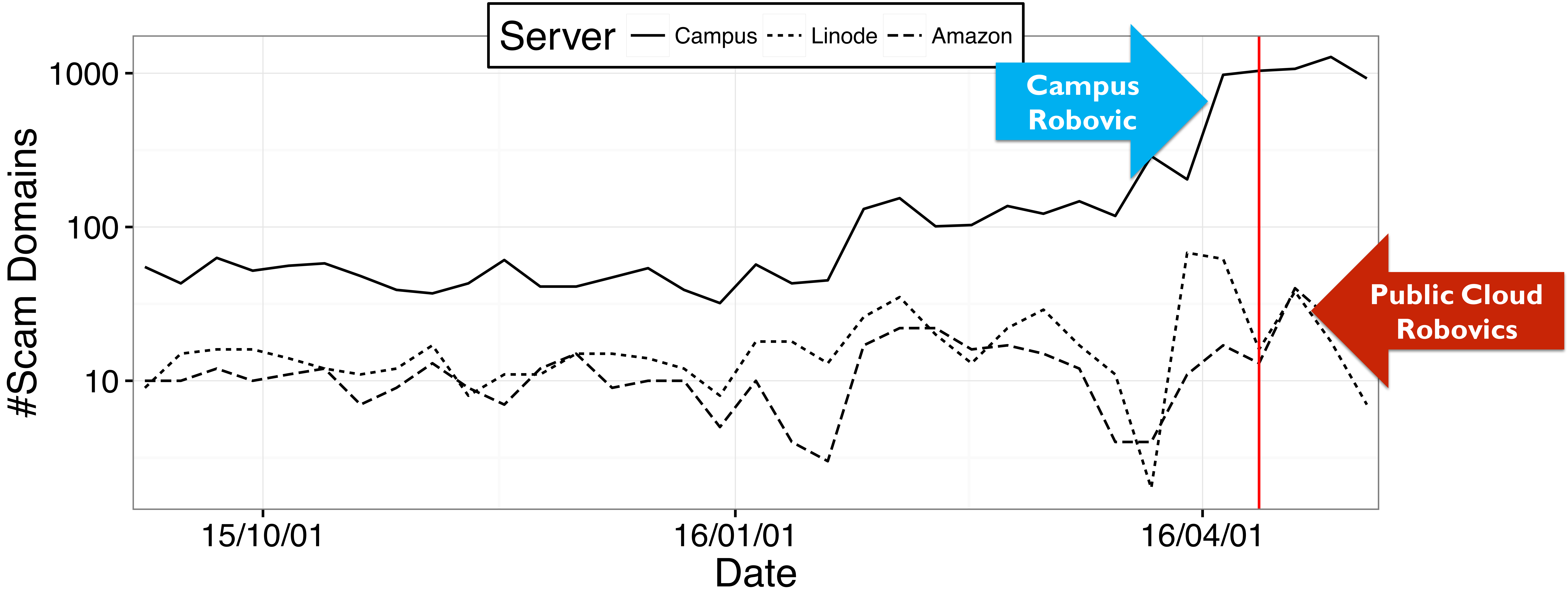
Long with readable parts

- 10.computerhaveaseriousproblempleasecallon18776431254tollfree.yourcomputerhaveaseriousproblempleasecallon18776431254tollfree.yourcomputerhaveaseriousproblempleasecallon18776431254tollfree.browsersecurity16[.]club

URLs from CDNs

- 1073964613.rsc.cdn77[.]org
- 924983738.r.cdnsun[.]net

Weekly Scam Domains



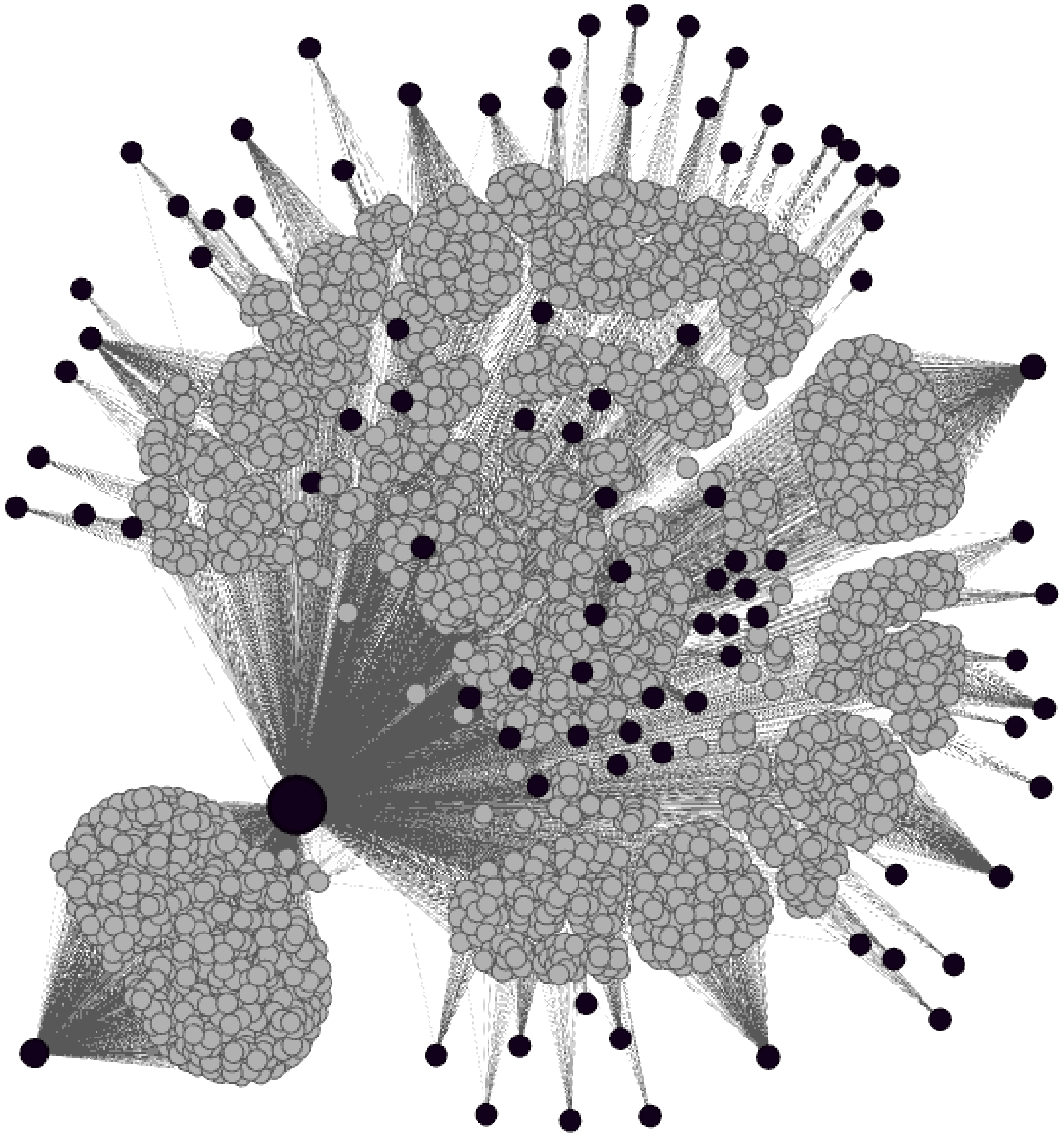
Campus Robovic

Public Cloud Robovics

Scam Domains & phone Numbers

- Hiding backend servers (16% used Cloudflare)
- Anonymized registration information (55%)
- Abuse a small number of Telco companies
    - 80% of numbers belong to Twilio, RingRevenue (Invoca), WilTel
    - Prefer those that provide APIs
        - Scalable solution for the scammers’ business
- Number of phone numbers is much less than the number of domains
    - Phone numbers can link together domains of the same campaign

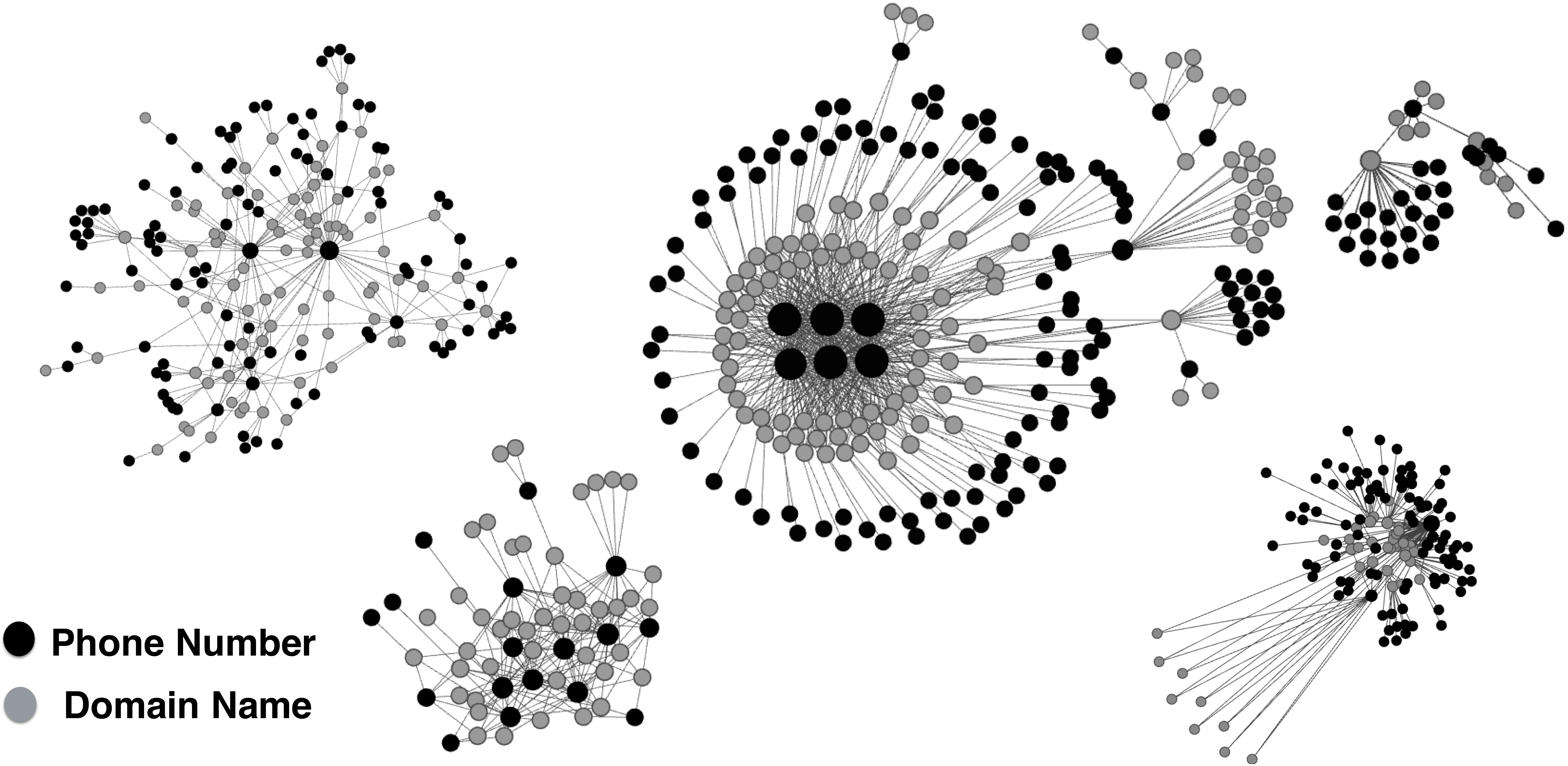
Scam Campaigns



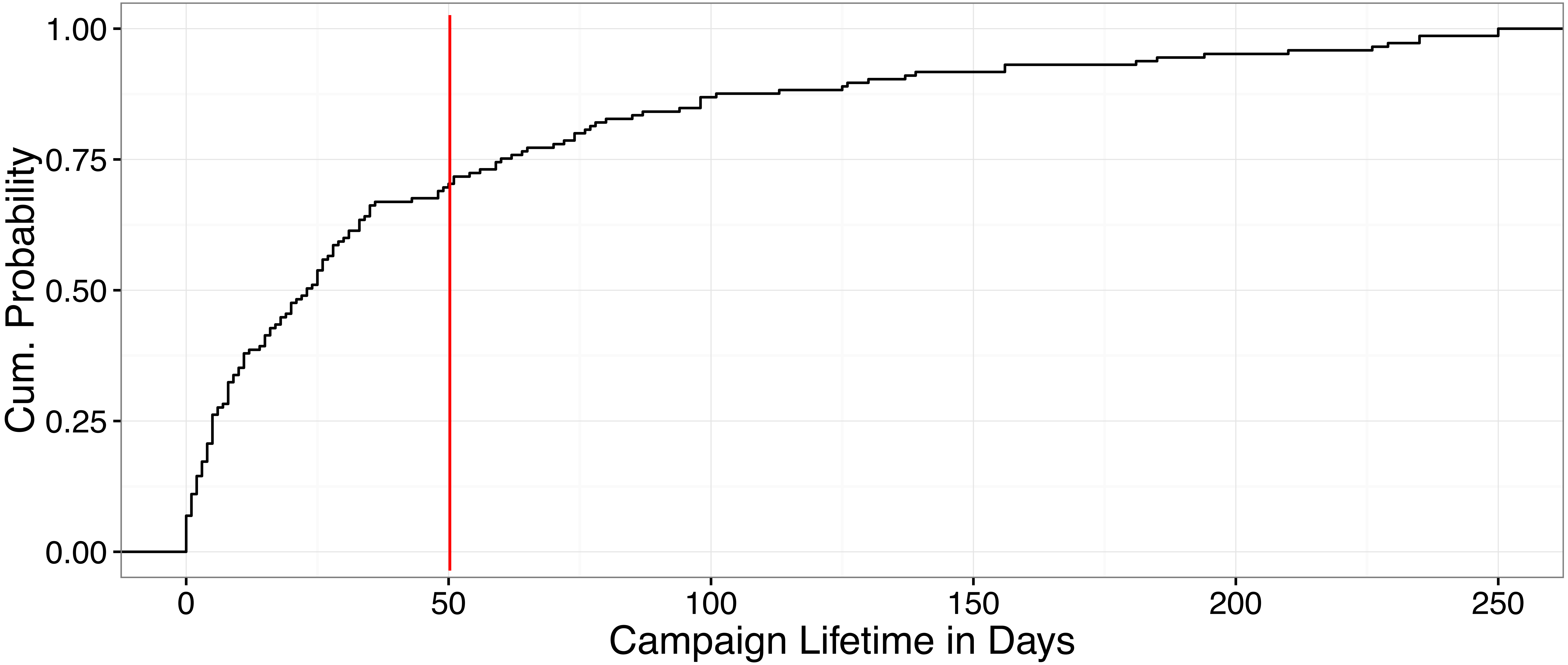
● Phone Number

● Domain Name

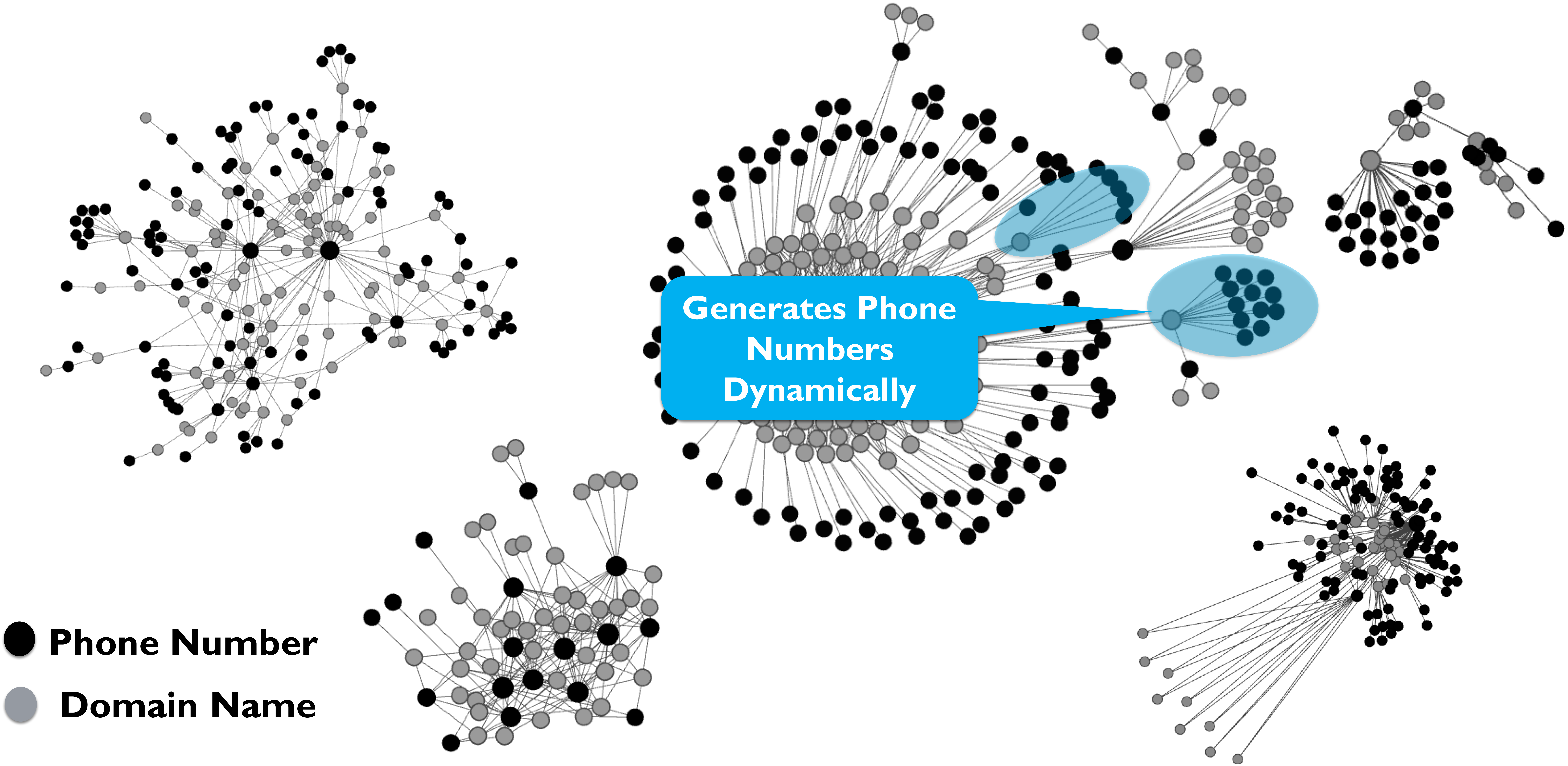
Scam Campaigns



Life time of Campaigns

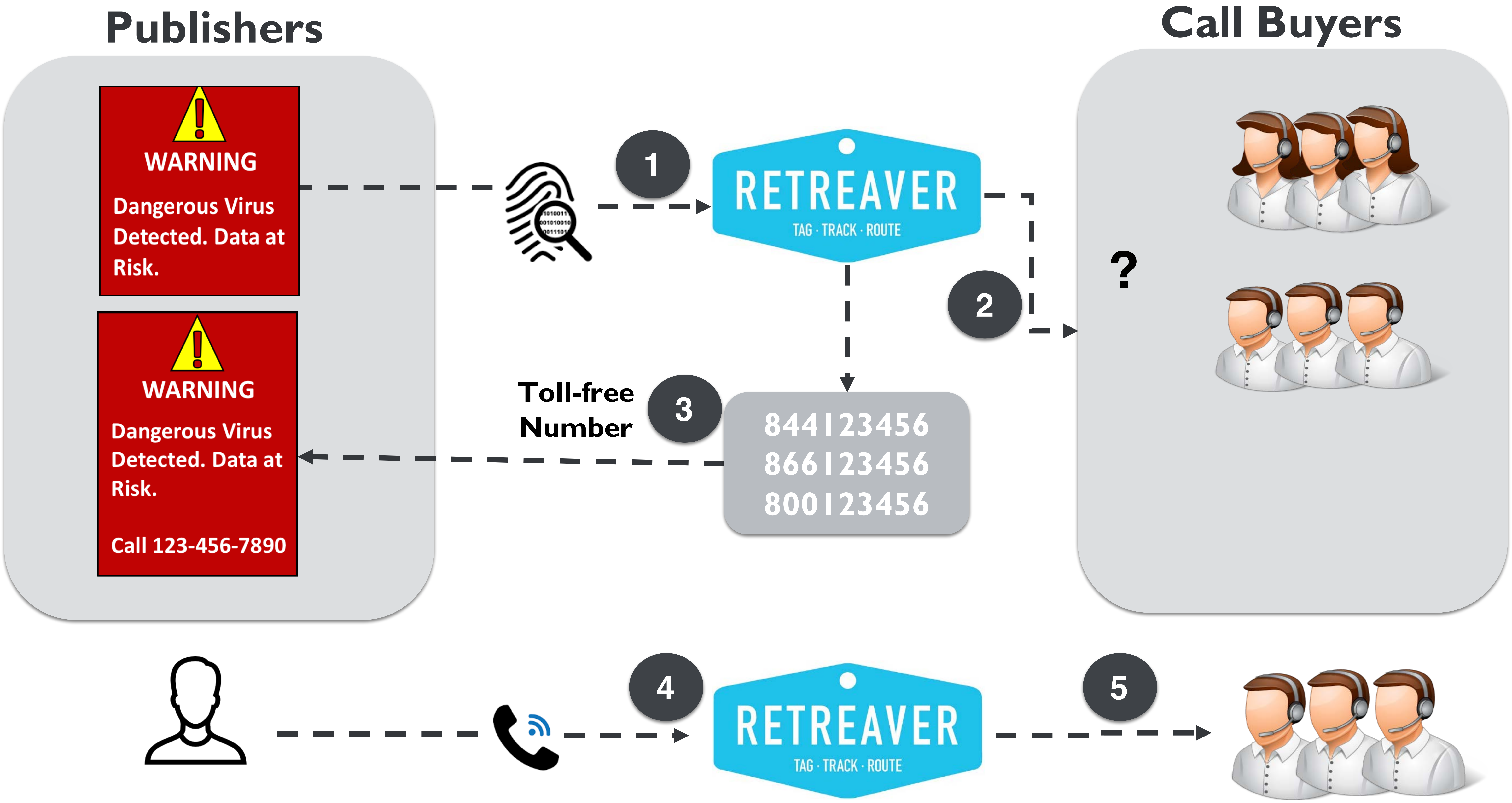


Phone-TLD+1 Relationship



Generates Phone Numbers Dynamically

Pay Per Call Marketing



Publishers

Call Buyers

WARNING

Dangerous Virus Detected. Data at Risk.

WARNING

Dangerous Virus Detected. Data at Risk.

Call 123-456-7890

1

2

?

Toll-free Number

3

844123456
866123456
800123456

4

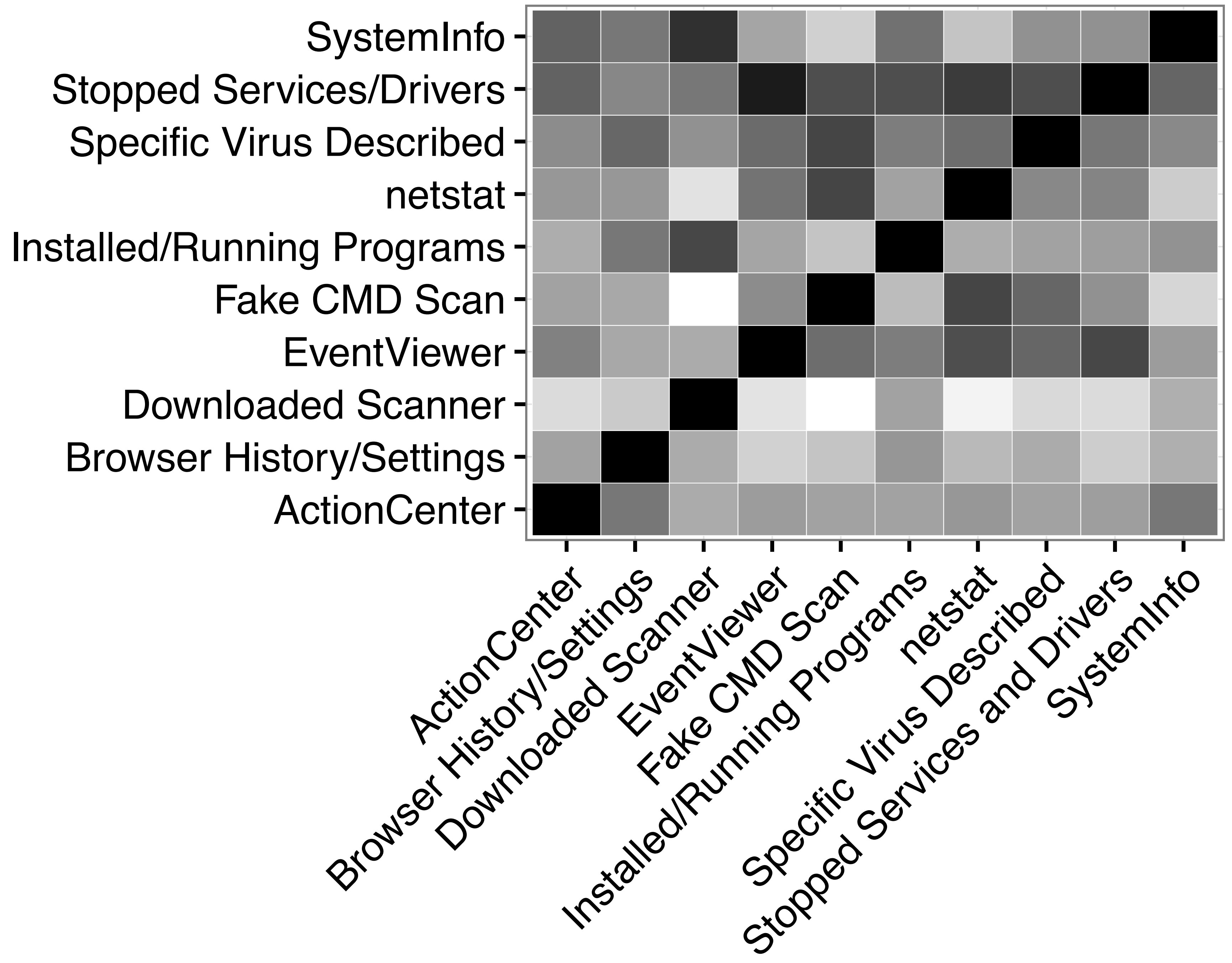
5

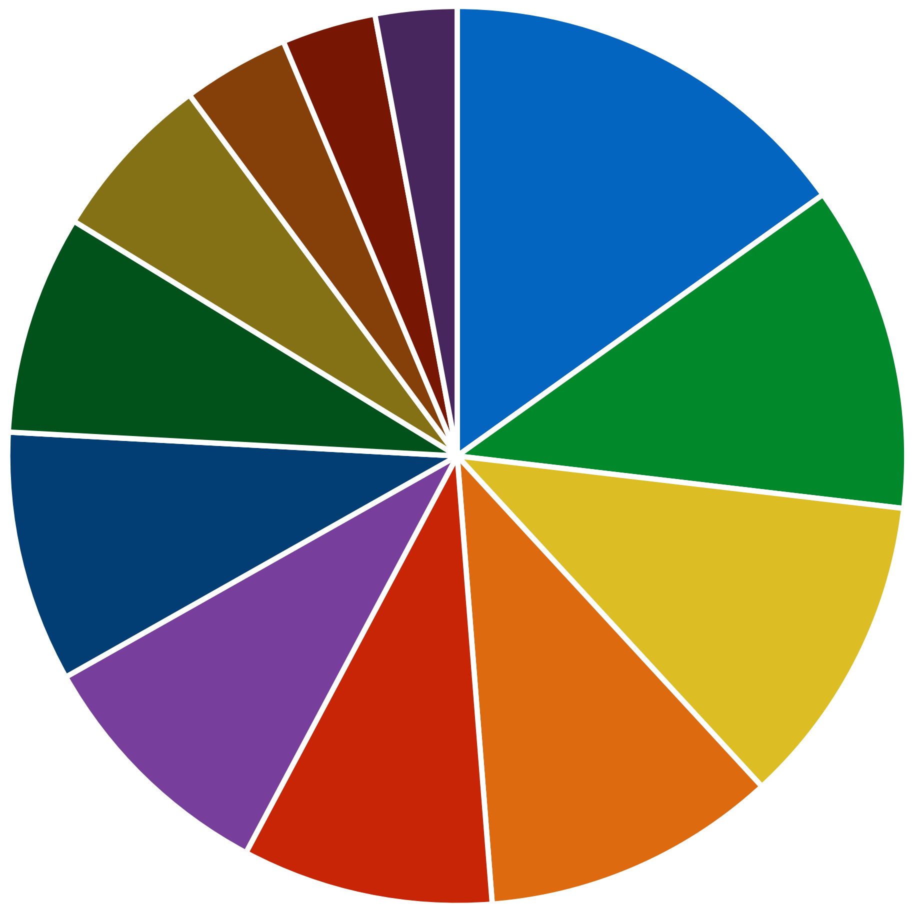
Meeting the Scammers

Environment set up

- Obtained permission from our IRB
- 60 interactions with the scammers
- Environment:
    - Artificially aged Windows 7 virtual machine
    - Tunneling the traffic through VPN
    - VoIP software with believable CallerID
    - Capturing network traffic, recording the screen and conversations

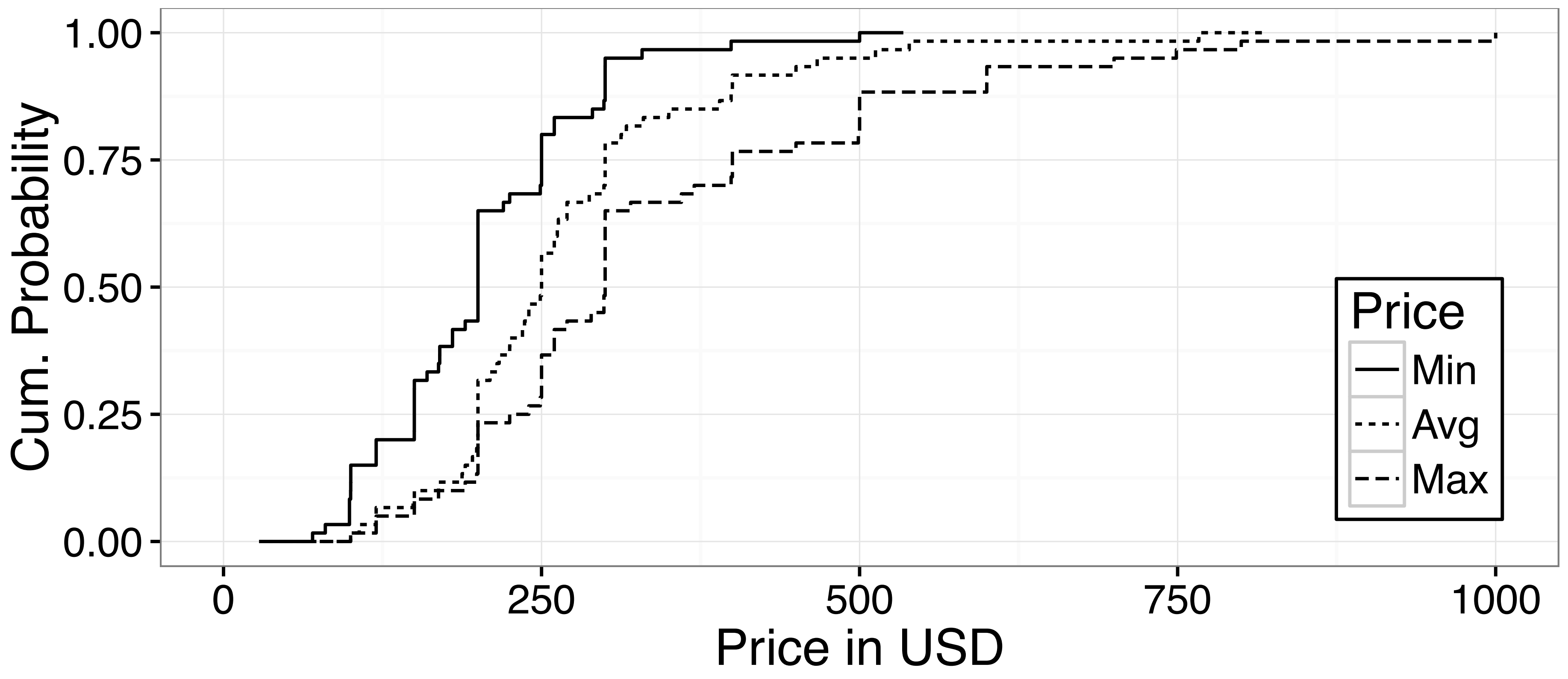
Scammers’ Tools & Techniques





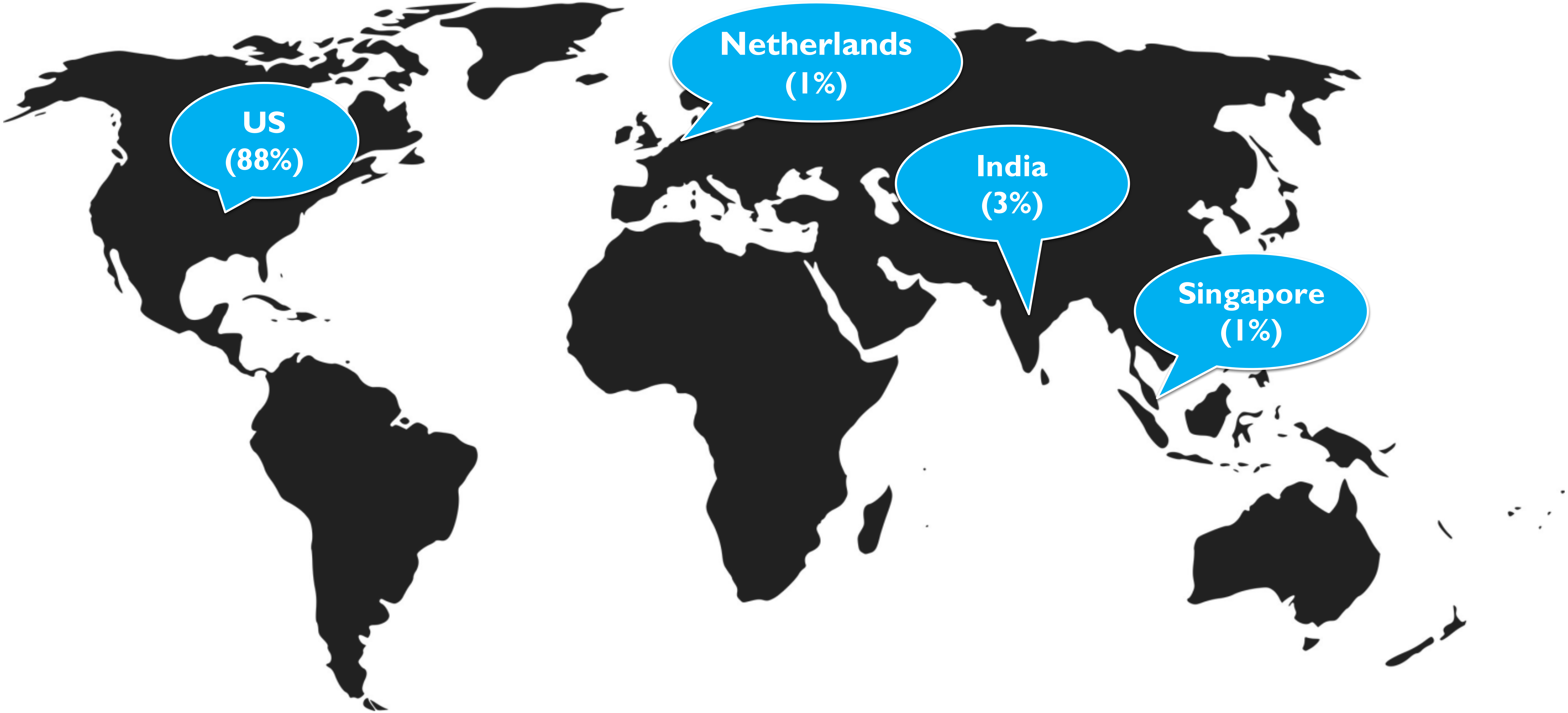
Social Engineering Techniques

- 🟦 Stopped Services/Drivers
- 🟩 Event Viewer
- 🟨 Specific Virus Explained
- 🟧 System Information
- 🟥 Action Center
- 🟪 Fake CMD Scan
- 🟦 Netstat Scan
- 🟩 Installed/Running Programs
- 🟫 Browsing History/Settings
- 🟫 Downloaded Scanner
- 🟥 Reliability/Performance
- 🟪 Other (Temp, Registry)

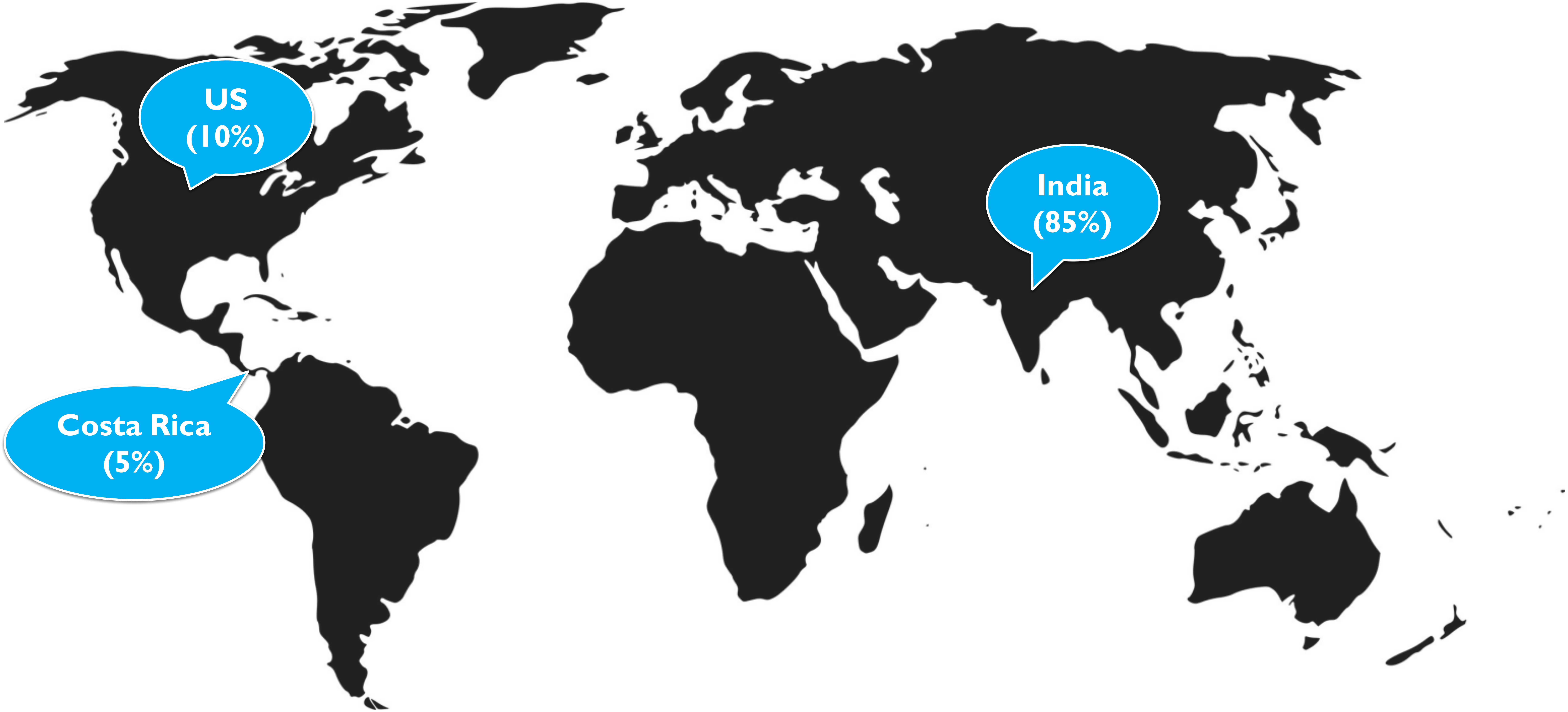


Scammer Physical Locations
&
Profit

Location of Scammers' Servers



Location of Call Centers



Number of Victims

- Monitoring Traffic of Scam Servers:
  - Misconfiguration of scam servers revealed their traffic
    - 142 scam domains were found which had misconfiguration
    - We monitored misconfigured servers every one minute over two months
  - Total visits : 1.7 million unique IPs
  - Max #visitors/domain : 138K unique IPs

Location of Victims

Canada (7%)
US(33%)
Singapore (1%)
Australia (26%)
New Zealand (5%)

Scammers' Profit

Average price of Tech Support Scam Package ($290)

*

Number of Victims (1.7 million unique IPs)

*

Conversion Rate (2% as a similar scareware)

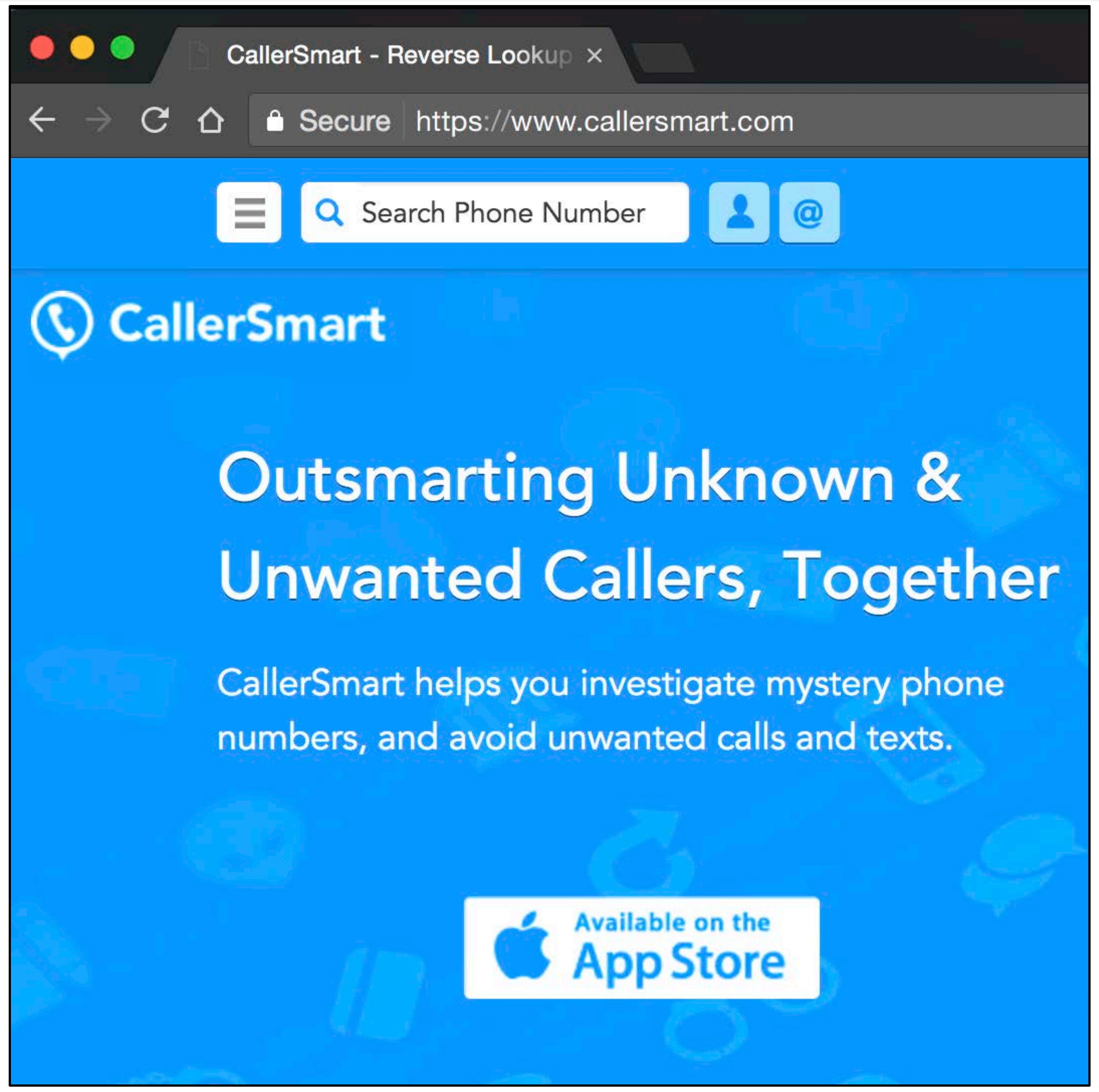
Scammers' profit = ~ $9.7 million in 2 months

(a lower bound)

Defense: Sufficiency of Current Blacklists

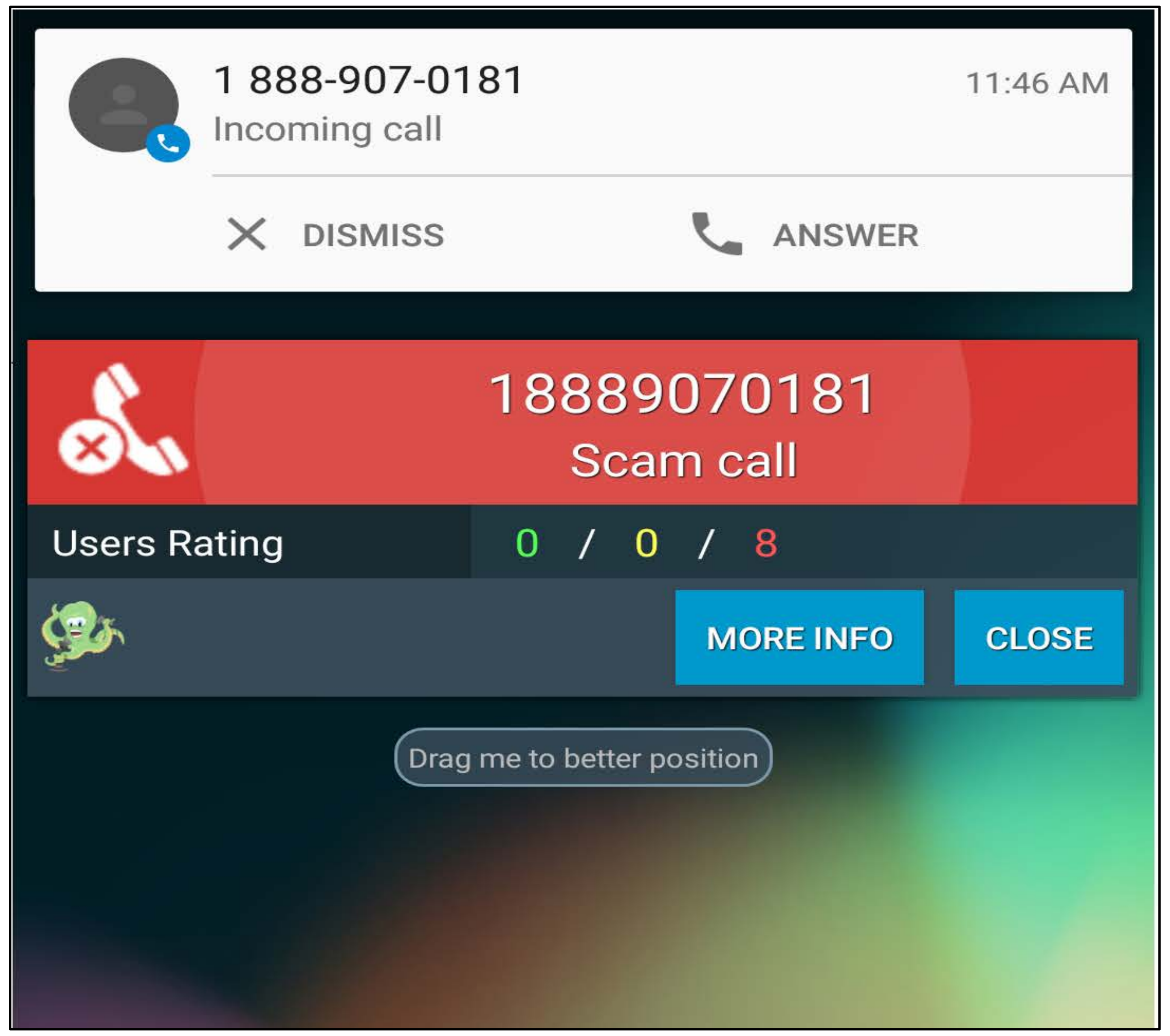
Blacklists: Phone Numbers

	Database	Coverage	Claimed Size
Website	mrnumber.com	19.9%	1.5 billion numbers
	800notes.com	18.5%	Unknown
	numberguru.com	1.0%	29 million lookups
	badnumbers.info	0.2%	968,639 complains
	callersmart.com	0.1%	5.9 million lookups
	scamnumbers.info	0.1%	31,162 numbers
Mobile App	Should I Answer?	0.5%	640 million lookups
	Truecaller	0.5%	2 billion numbers
	Hiya	0.3%	100 million numbers
	CallDetector	0.1%	100,000 complaints monthly
	Mr. Number	0.1%	1.5 billion numbers
	Together	**27.4%**	-


CallerSmart - Reverse Lookup
Secure https://www.callersmart.com
Search Phone Number
CallerSmart
Available on the App Store

Outsmarting Unknown & Unwanted Callers, Together

CallerSmart helps you investigate mystery phone numbers, and avoid unwanted calls and texts.

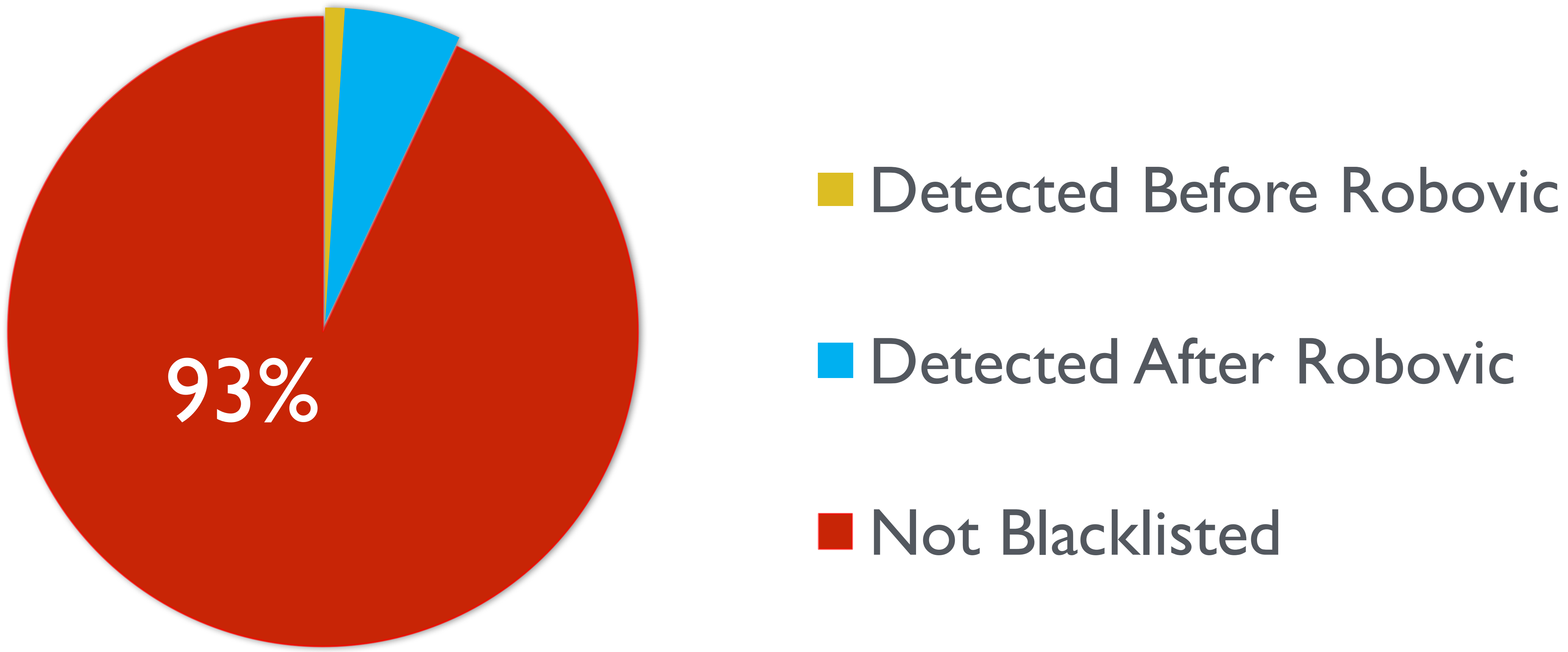


1 888-907-0181 11:46 AM
Incoming call

18889070181
Scam call

Users Rating 0 / 0 / 8

Blacklists: Domain Names



6 Blacklists (370K domains and IP addresses Together)

- hpHosts
- SANS suspicious domains
- malwaredomains
- malwaredomainlist
- Malc0de database
- abuse.ch

Why do blacklists not work?

- Tech Support Scams are highly dynamic
  - 30% of the domains are alive less than a day
  - Abusing CDNs to get fresh URLs
  - Majority of phone numbers registered recently
  - Phone numbers are generated dynamically

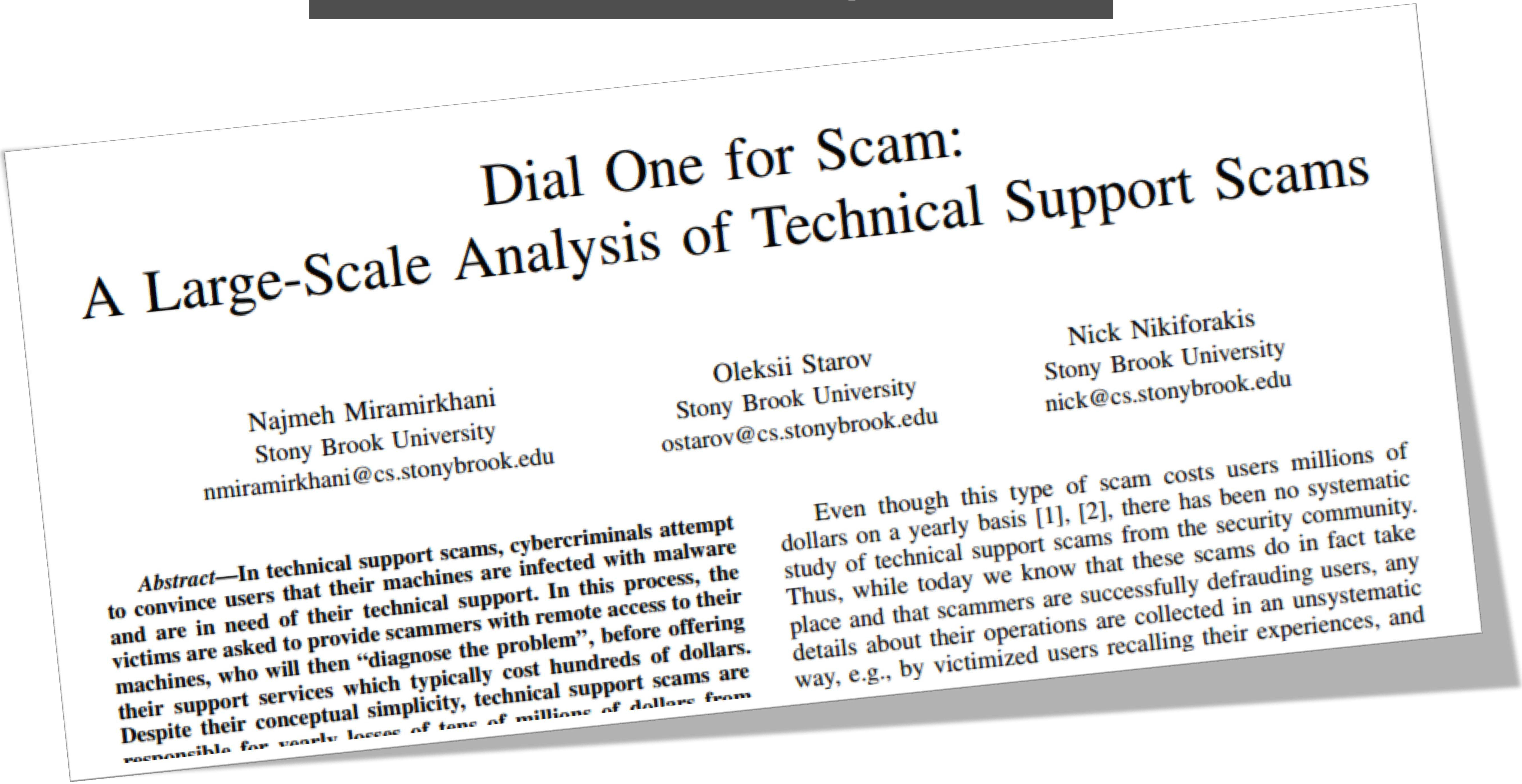
Defense against Tech Support Scam

- User Education
  - Explaining the concept of technical support scams is easier
  - Raising awareness through public services
- Browser Support
  - Average users do not know how to kill the browser process and clearing recent history
  - One universal shortcut to close unsafe pages

Summary

- Tech support scams pose a serious threat
- We conducted the first systematic study of tech support scams
- Reported prevalence of the scam and evasion techniques based on the collected corpus of thousands of domains and phone numbers
- Clustered campaigns and estimated their life time
- Interacted with 60 different scammers and identified the social engineering techniques
- Underline the need for user education and support from the browser vendors

nmiramirkhani@cs.stonybrook.edu



Dial One for Scam: A Large-Scale Analysis of Technical Support Scams

Najmeh Miramirkhani
Stony Brook University
nmiramirkhani@cs.stonybrook.edu

Oleksii Starov
Stony Brook University
ostarov@cs.stonybrook.edu

Nick Nikiforakis
Stony Brook University
nick@cs.stonybrook.edu

***Abstract*—In technical support scams, cybercriminals attempt to convince users that their machines are infected with malware and are in need of their technical support. In this process, the victims are asked to provide scammers with remote access to their machines, who will then "diagnose the problem", before offering their support services which typically cost hundreds of dollars. Despite their conceptual simplicity, technical support scams are responsible for yearly losses of tens of millions of dollars from**

Even though this type of scam costs users millions of dollars on a yearly basis [1], [2], there has been no systematic study of technical support scams from the security community. Thus, while today we know that these scams do in fact take place and that scammers are successfully defrauding users, any details about their operations are collected in an unsystematic way, e.g., by victimized users recalling their experiences, and