Hunting Them All

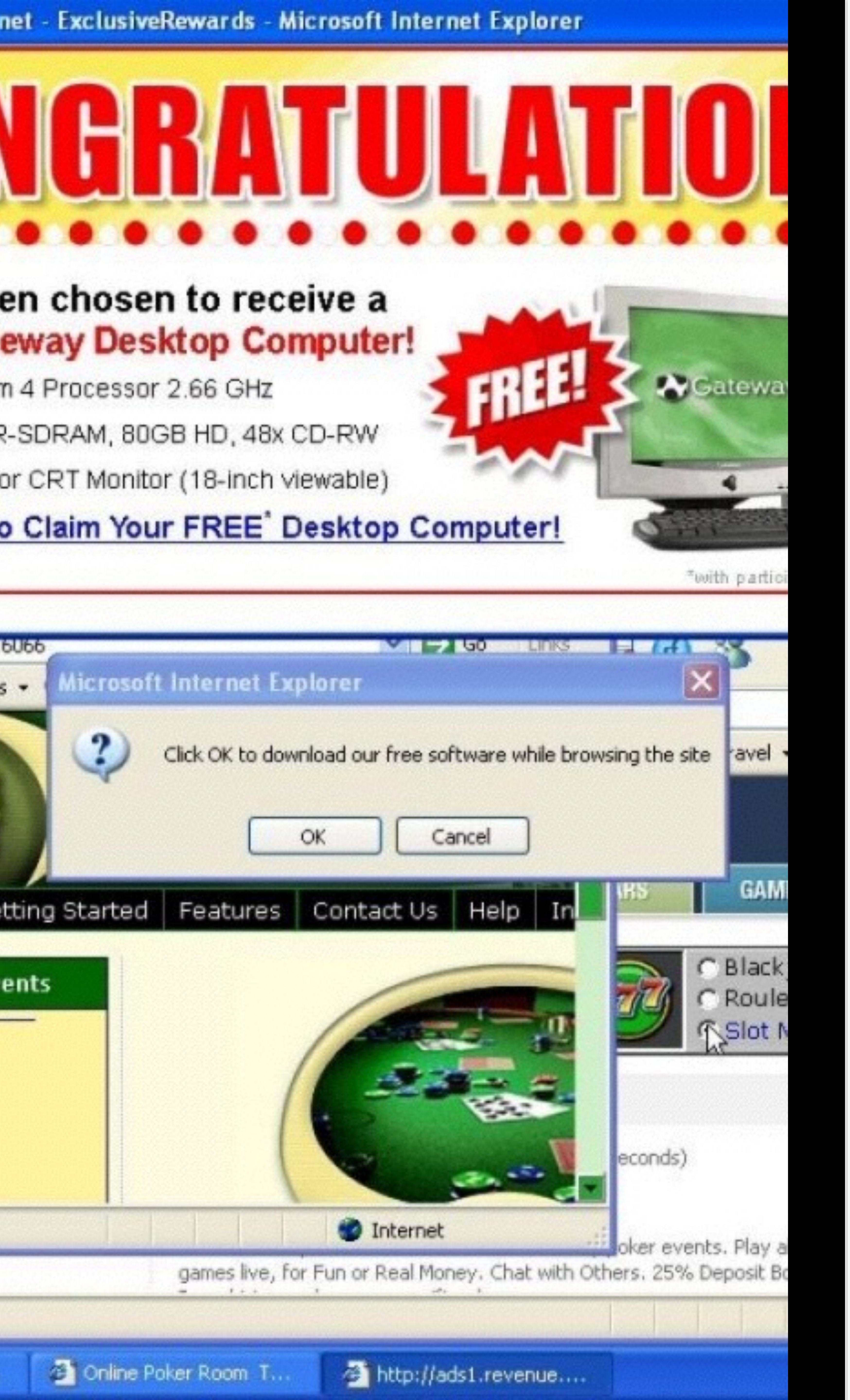
The Journey

Veronica Valeros | @verovaleros
Cognitive Threat Analytics
Cisco Systems

Who am I?

Twitter:	@verovaleros
LinkedIn:	/in/veronicavalerossaracho
Github:	/verovaleros
Cisco Blogs:	blogs.cisco.com/author/valeros
Research:	researchgate.net/profile/Valeros_Veronica

- Lead threat intelligence analyst and threat researcher at Cognitive Threat Analytics, Cisco Systems
- Co-Founder of MatesLab Hackerspace (Mar del Plata, Argentina)
- Core member of Security Without Borders (@swborders)



net - ExclusiveRewards - Microsoft Internet Explorer

NGRATULATIO

en chosen to receive a
eway Desktop Computer!
m 4 Processor 2.66 GHz
R-SDRAM, 80GB HD, 48x CD-RW
or CRT Monitor (18-inch viewable)

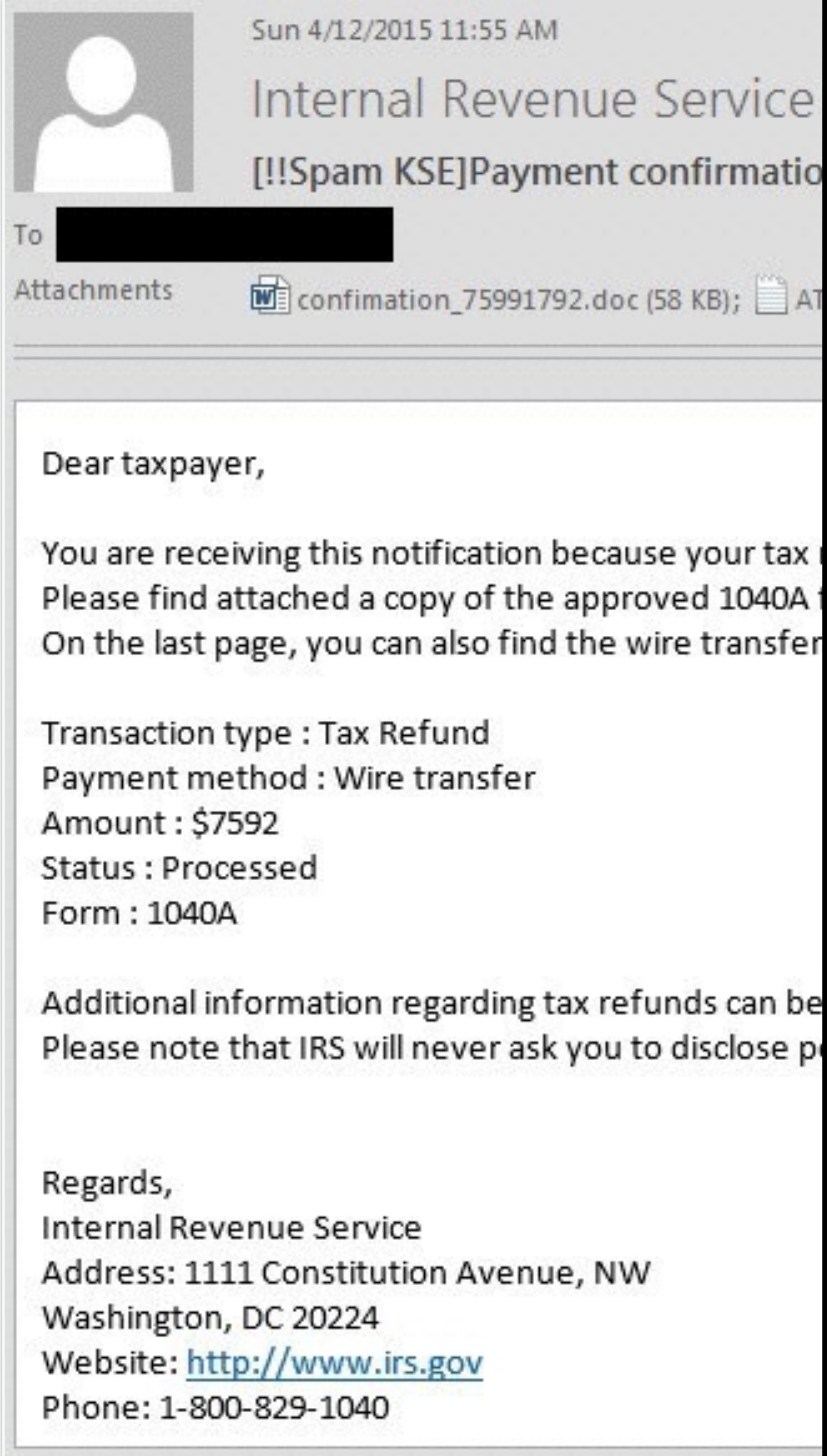
o Claim Your FREE* Desktop Computer!

*with partic

Microsoft Internet Explorer

Click OK to download our free software while browsing the site

oker events. Play a
games live, for Fun or Real Money. Chat with Others. 25% Deposit Bo



Sun 4/12/2015 11:55 AM

Internal Revenue Service

[!!Spam KSE]Payment confirmatio

To [redacted]

Attachments confimation_75991792.doc (58 KB); AT

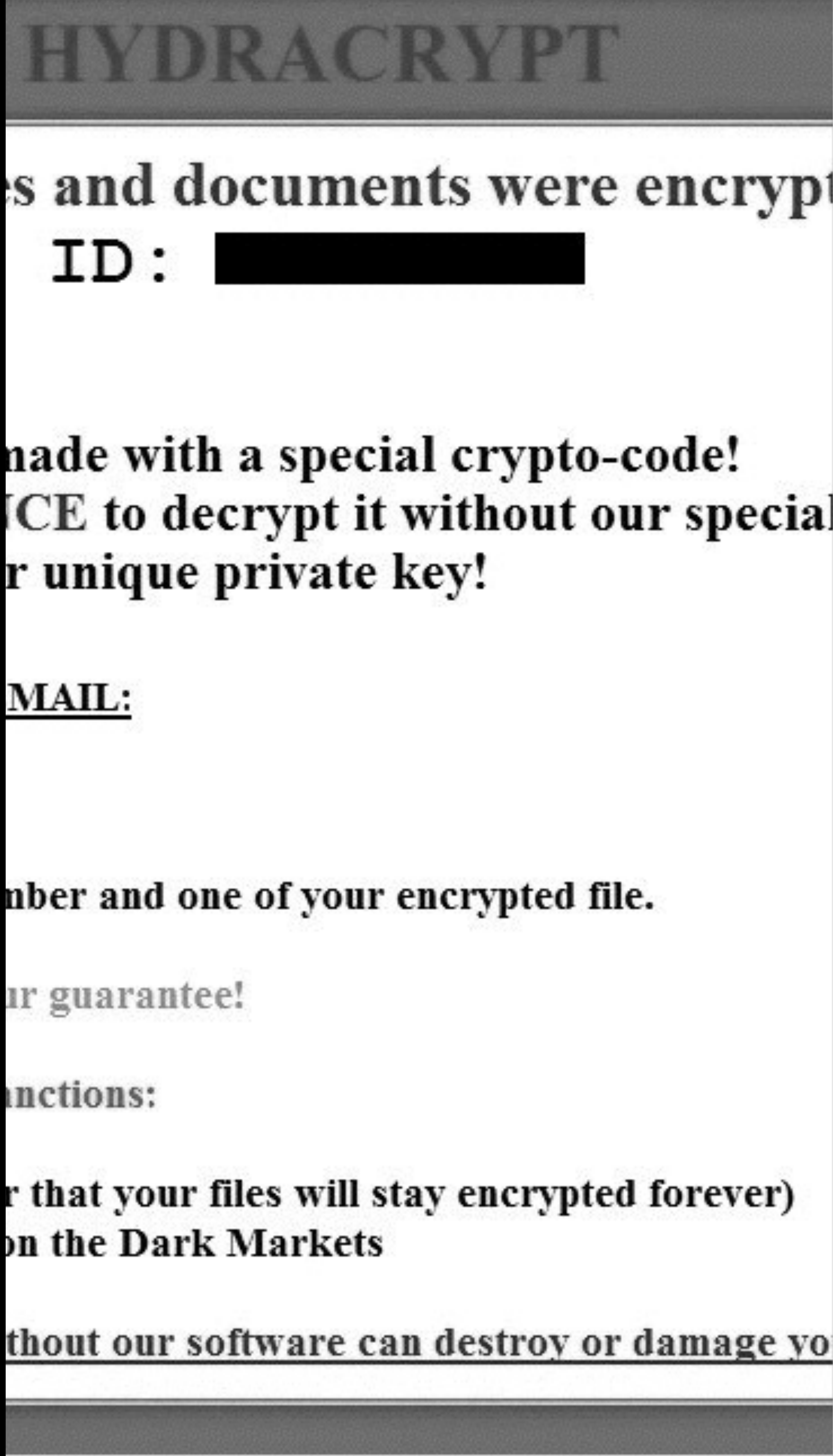
Dear taxpayer,

You are receiving this notification because your tax
Please find attached a copy of the approved 1040A
On the last page, you can also find the wire transfer

Transaction type : Tax Refund
Payment method : Wire transfer
Amount : $7592
Status : Processed
Form : 1040A

Additional information regarding tax refunds can be
Please note that IRS will never ask you to disclose p

Regards,
Internal Revenue Service
Address: 1111 Constitution Avenue, NW
Washington, DC 20224
Website: http://www.irs.gov
Phone: 1-800-829-1040



HYDRACRYPT

s and documents were encrypt
ID: [redacted]

nade with a special crypto-code!
ICE to decrypt it without our specia
r unique private key!

MAIL:

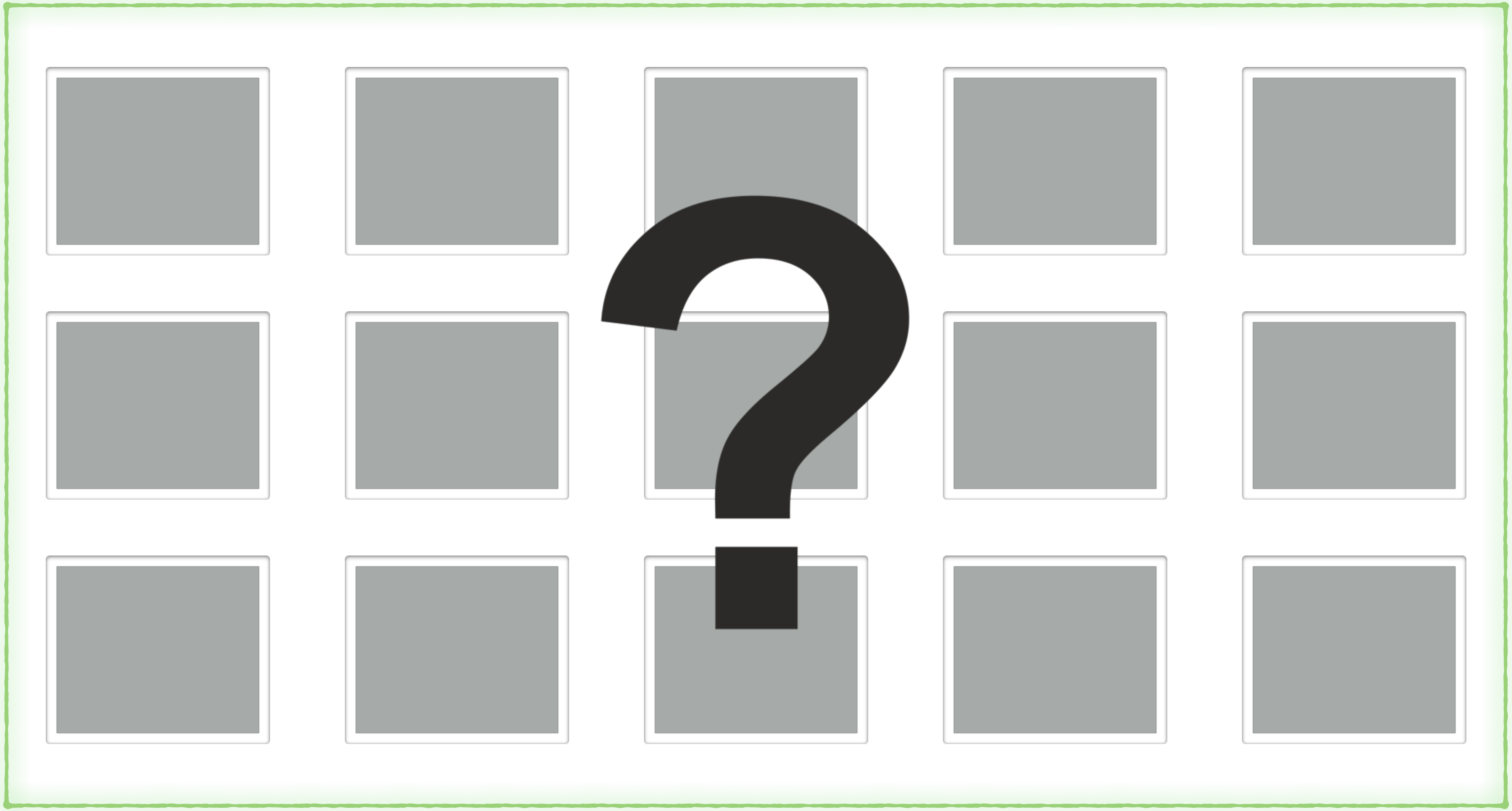
nber and one of your encrypted file.

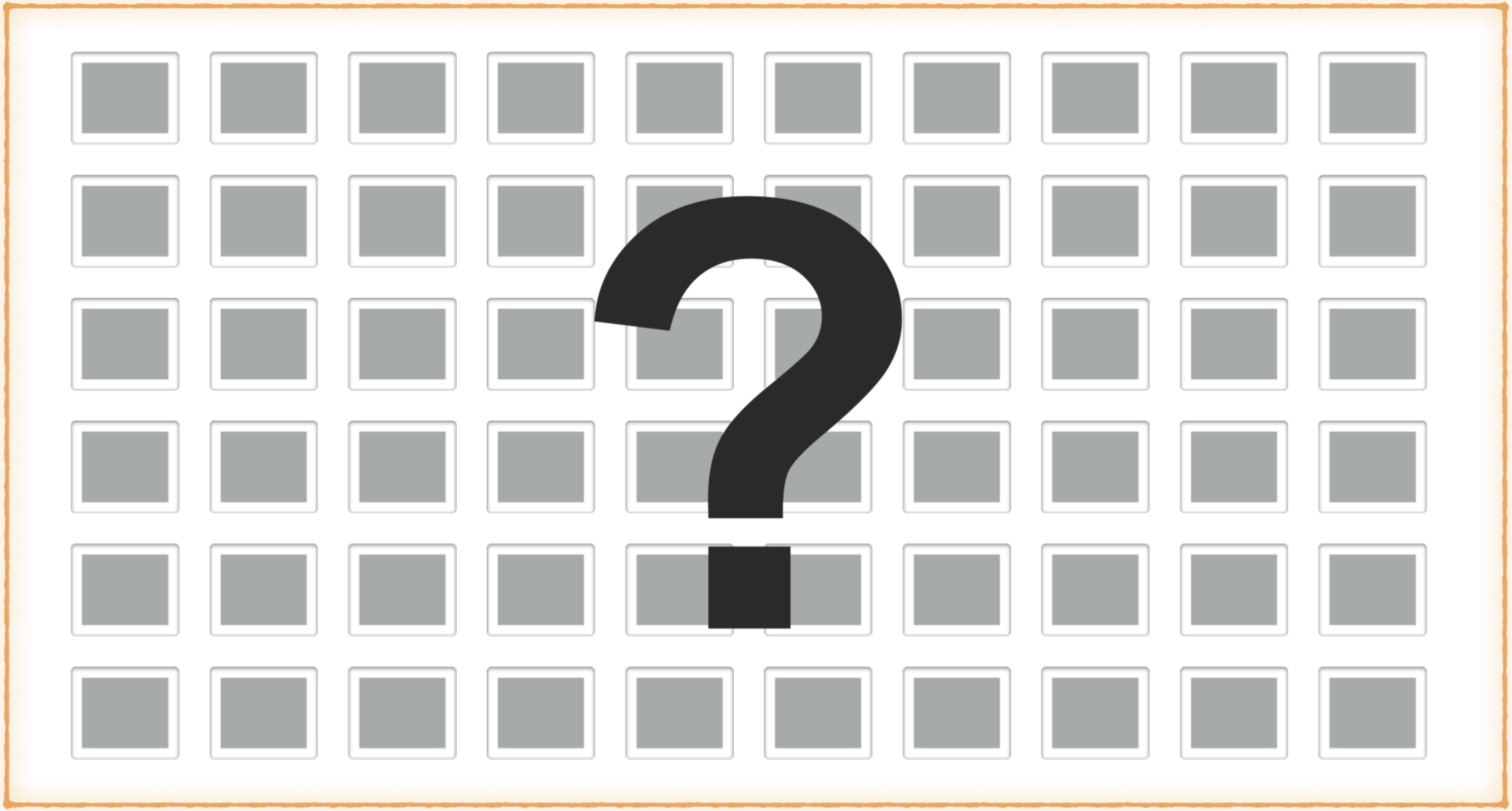
ır guarantee!

ınctions:

r that your files will stay encrypted forever)
on the Dark Markets

thout our software can destroy or damage yo





“(…) look for attacks that get past security systems and to catch intrusions in progress rather than after attackers have completed their objectives and done worse damage to the business.”

SANS Institute
The Who, What, Where, When,
Why and How of Effective Threat Hunting

Adversaries don’t need to be *l33t*,
they only need to be better than us.

They have time.

They abuse the weakest link.

They hide in plain sight.

They know our limitations.

Malware needs to be coded.

‘Less effort’ rule.

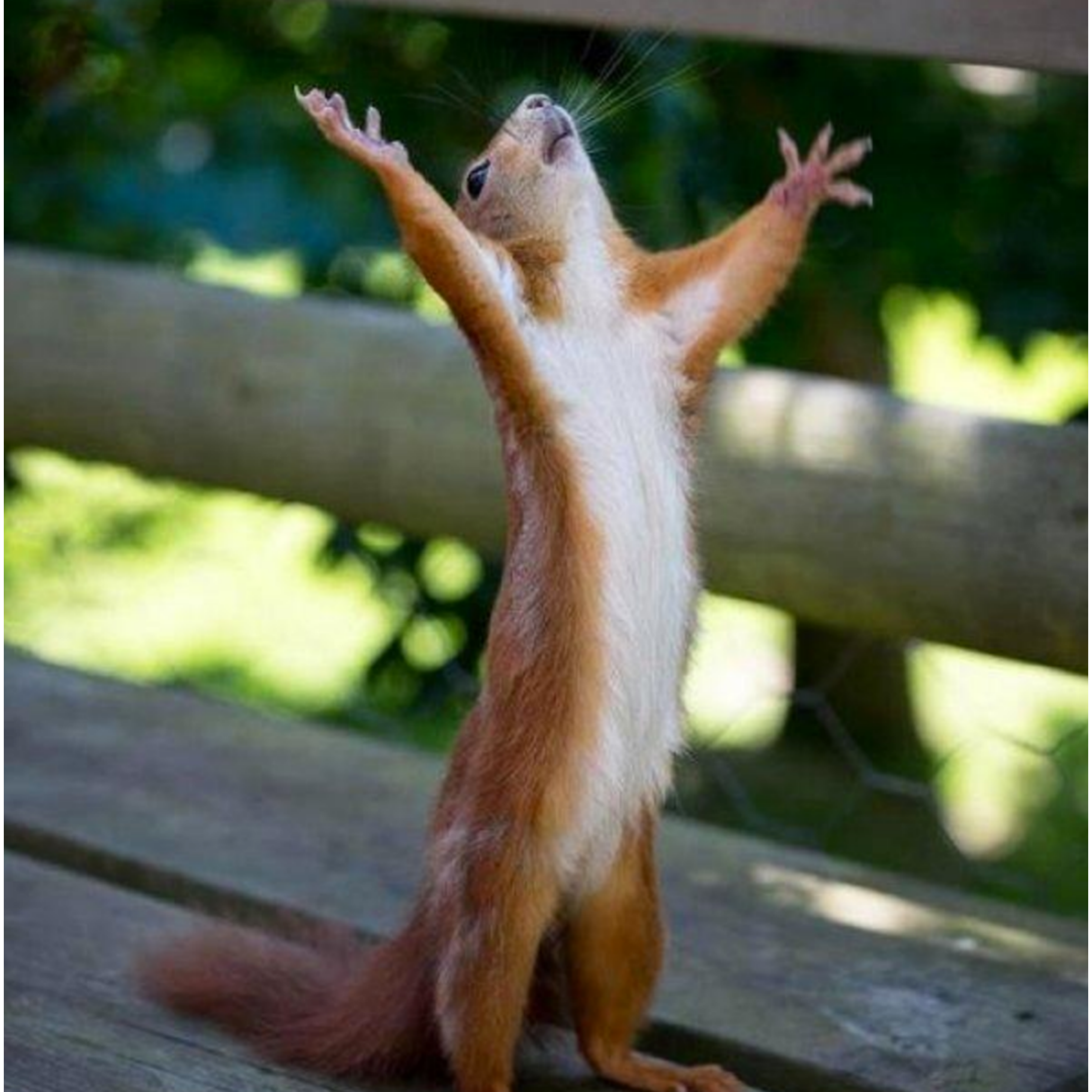
Similar mechanisms used.

They reuse code.

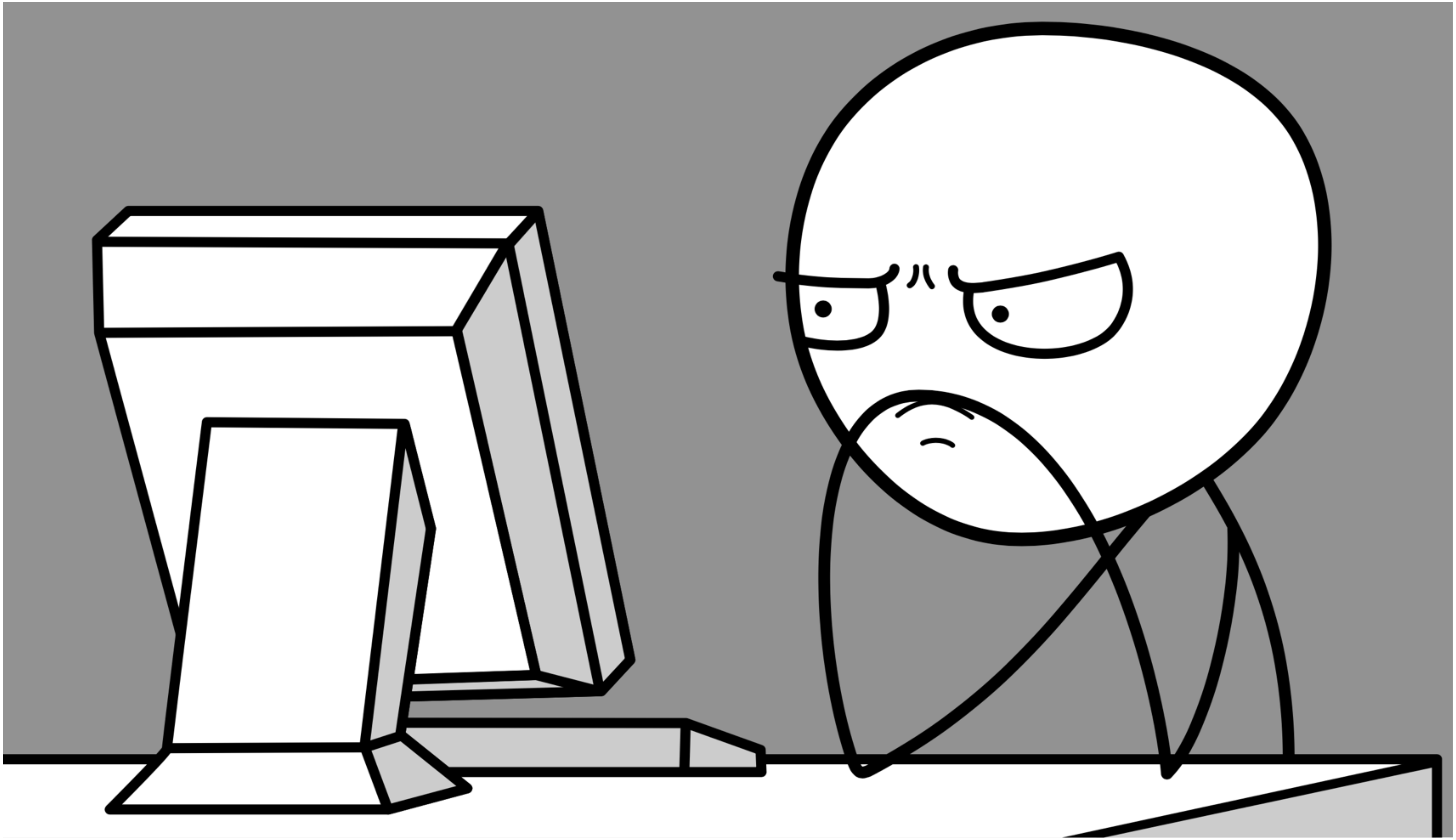
Not [usually] reinventing the wheel.

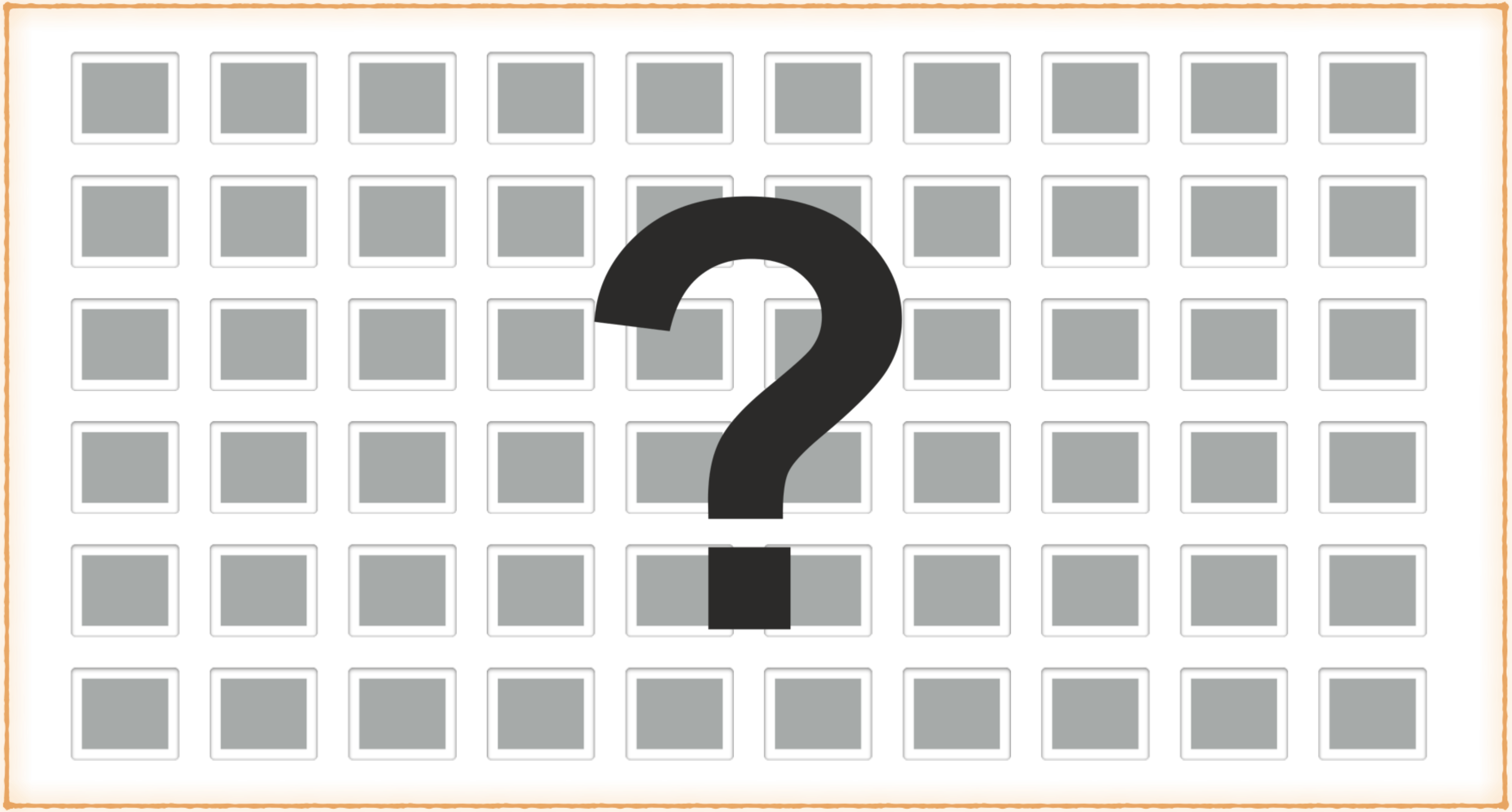
Modularity and flexibility in a malware implies [network] **communication**, often **periodic**.

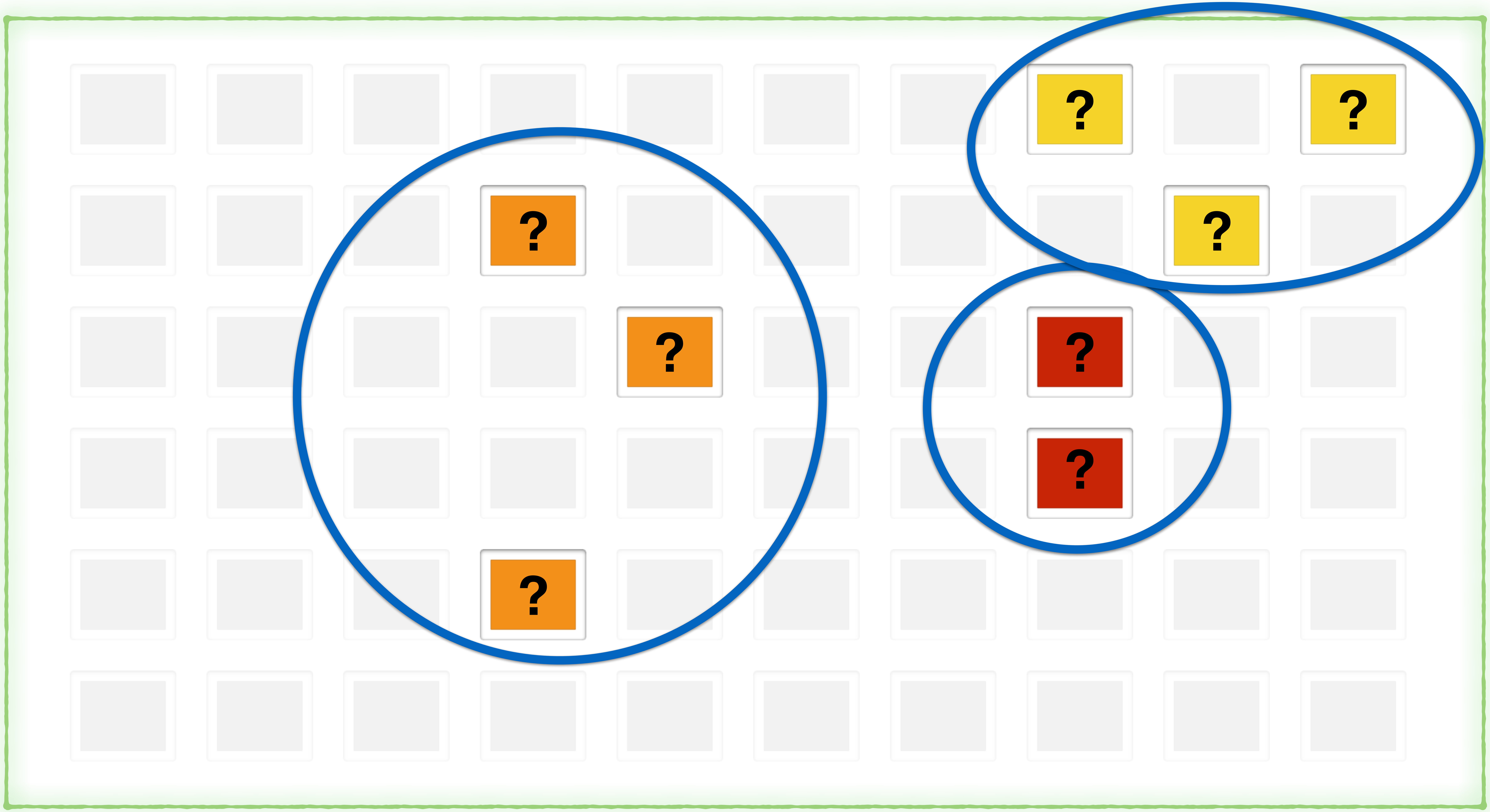
Hundreds of networks
Millions of users
Billions of web requests



So much data <3







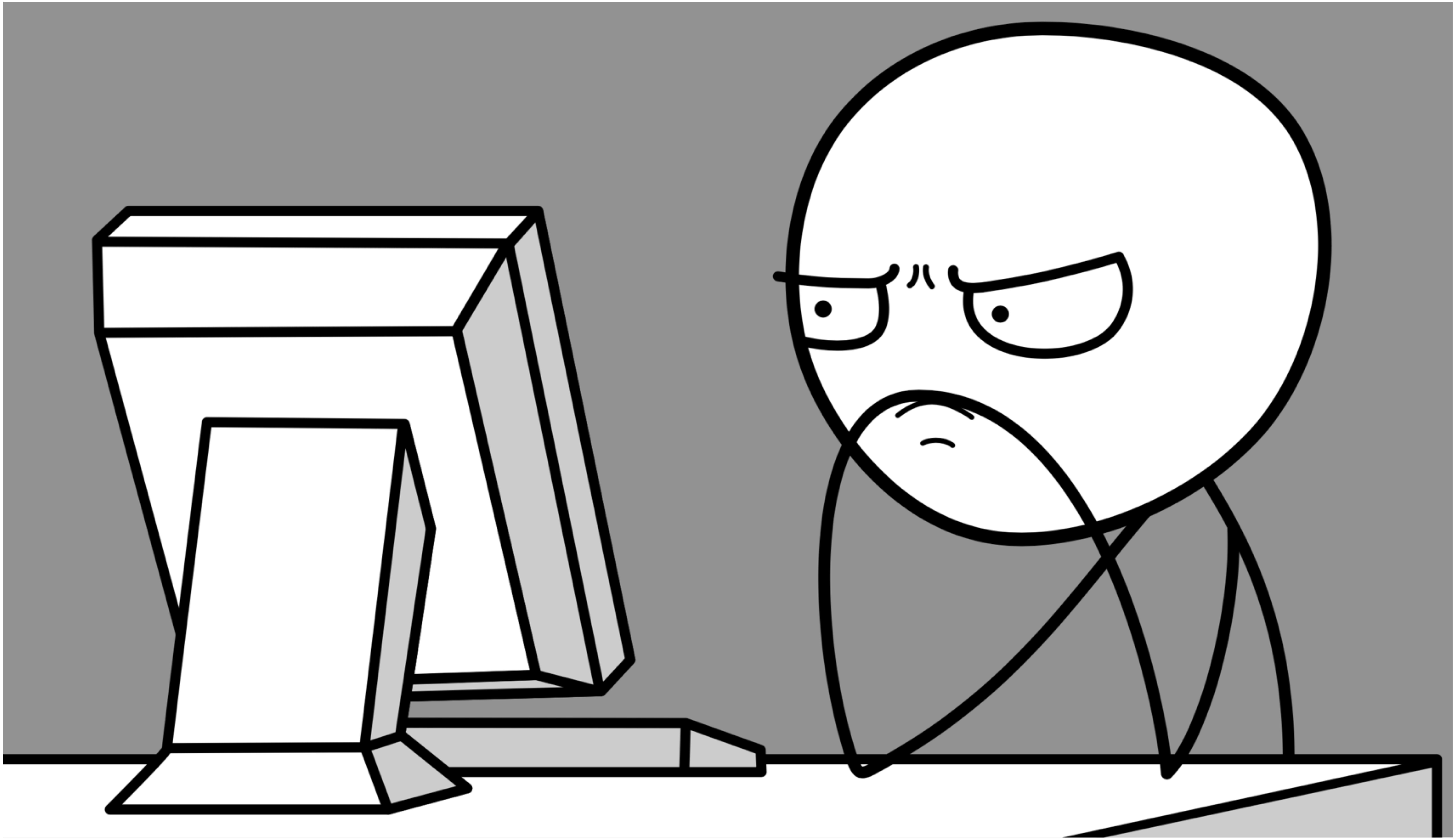
Machine Learning can make the difference.

```
2017-02-19 00:09:30 http://www.ceylanogullari.com/logof.gif?
8fcd2c7=1206294072 200   52.28.249.128    362   157        Mozilla/4.0
(compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322; .NET
CLR 2.0.50728)      text/plain

2017-02-19 00:09:31 http://www.bluecubecreatives.com/logos.gif?
8fcd5d3=603150156  200   69.172.201.153  314   1778      Mozilla/4.0
(compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322; .NET
CLR 2.0.50728)      text/html
```

Focusing our attention on what is important

After phase
CTA
Layer 1
Anomaly Detection
Trust Modeling
CTA
Layer 2
Event Classification
Entity & User Modeling
CTA
Layer 3
Relationship Modeling
10B
requests per day
20K
incidents per day
Anomalous
Web requests (flows)
Malicious
Events (flow sequences)
Threat
Incidents (aggregated events)



Strategy

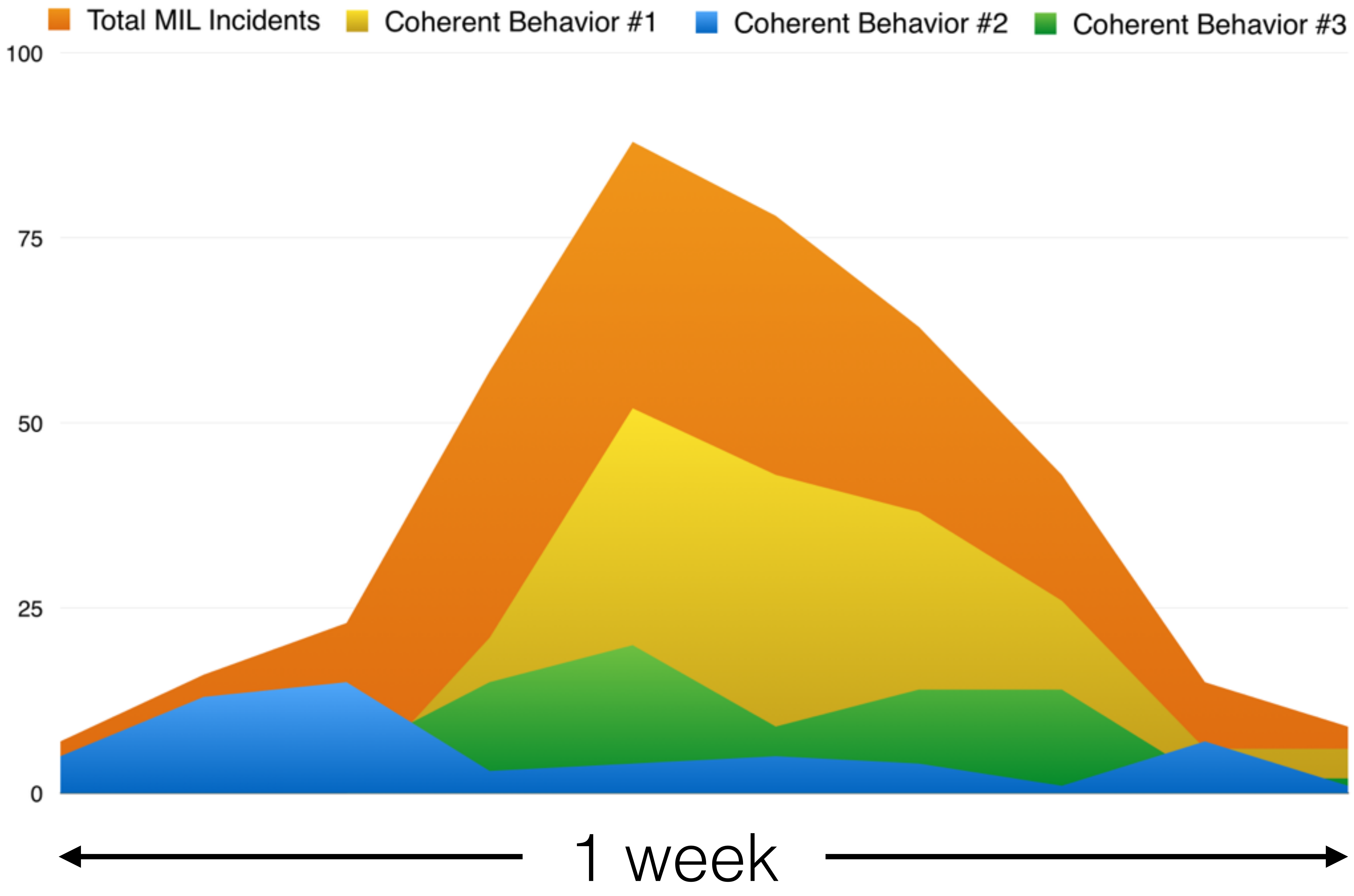
Force Strategy *Cunning*

✓

Force Strategy *Cunning*

Clean and Rinse

Multi-Instance Learning Classifier (MIL)



● Adware 1

● Adware 2

● DNS Changer v2015

Research by Karel Bartos, V. Franc, M. Softka.
http://blogs.cisco.com/security/talos/machine-learning-detectors

http://finhoome.info/u/?a=kLz-Yckq(..)&c=fPOnv(..)&r=987(..)

http://domenjob.com/u/?a=D-2n5k7(..)&c=vTB5(..)&r=589(..)

http://domenjob.net/u/?a=qk7BKV9(..)&c=m6V(..)&r=327(..)

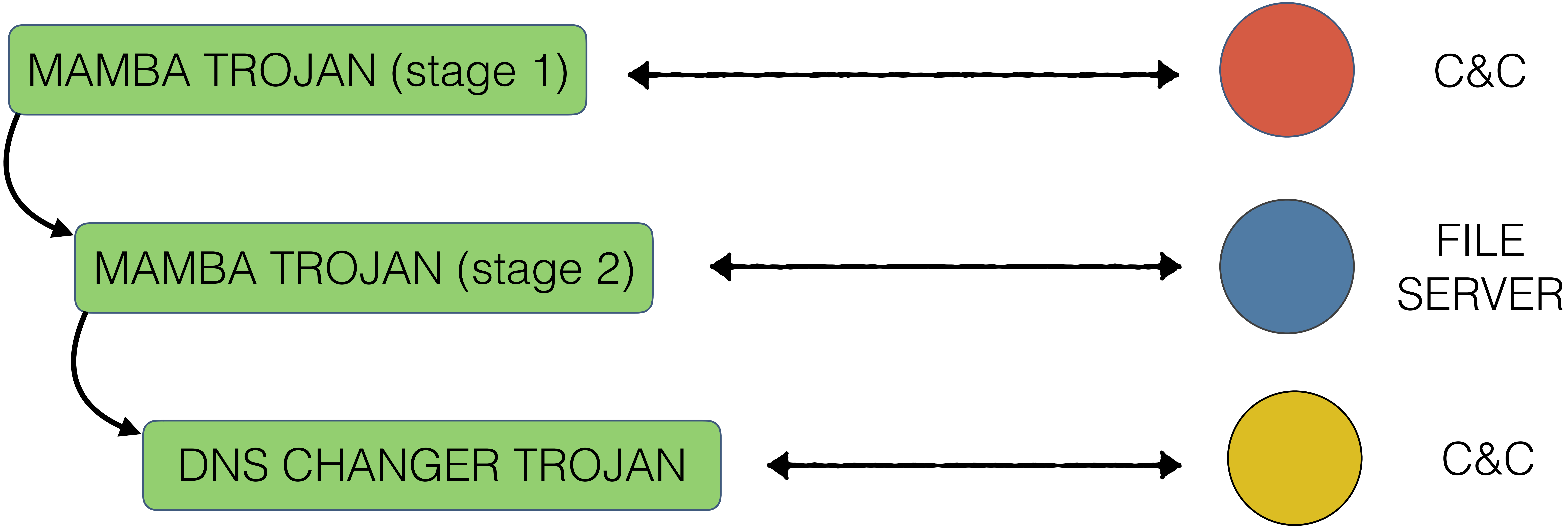
http://listcool.net/u/?q=jW6H5obe2(..)&c=be2G(..)&r=684(..)

http://listcool.info/u/?q=J5DM4nrA(..)&c=rASU(..)&r=911(..)

http://usafun.info/u/?q=S42YFQPC(..)&c=YFQP(..)&r=769(..)

http://realget.info/u/?a=fDrS_9vLG(..)&c=GM0-(..)&r=528(..)

http://alwaysweb.info/u/?a=G3ZGb(..)&c=wNR4(..)&r=781(..)

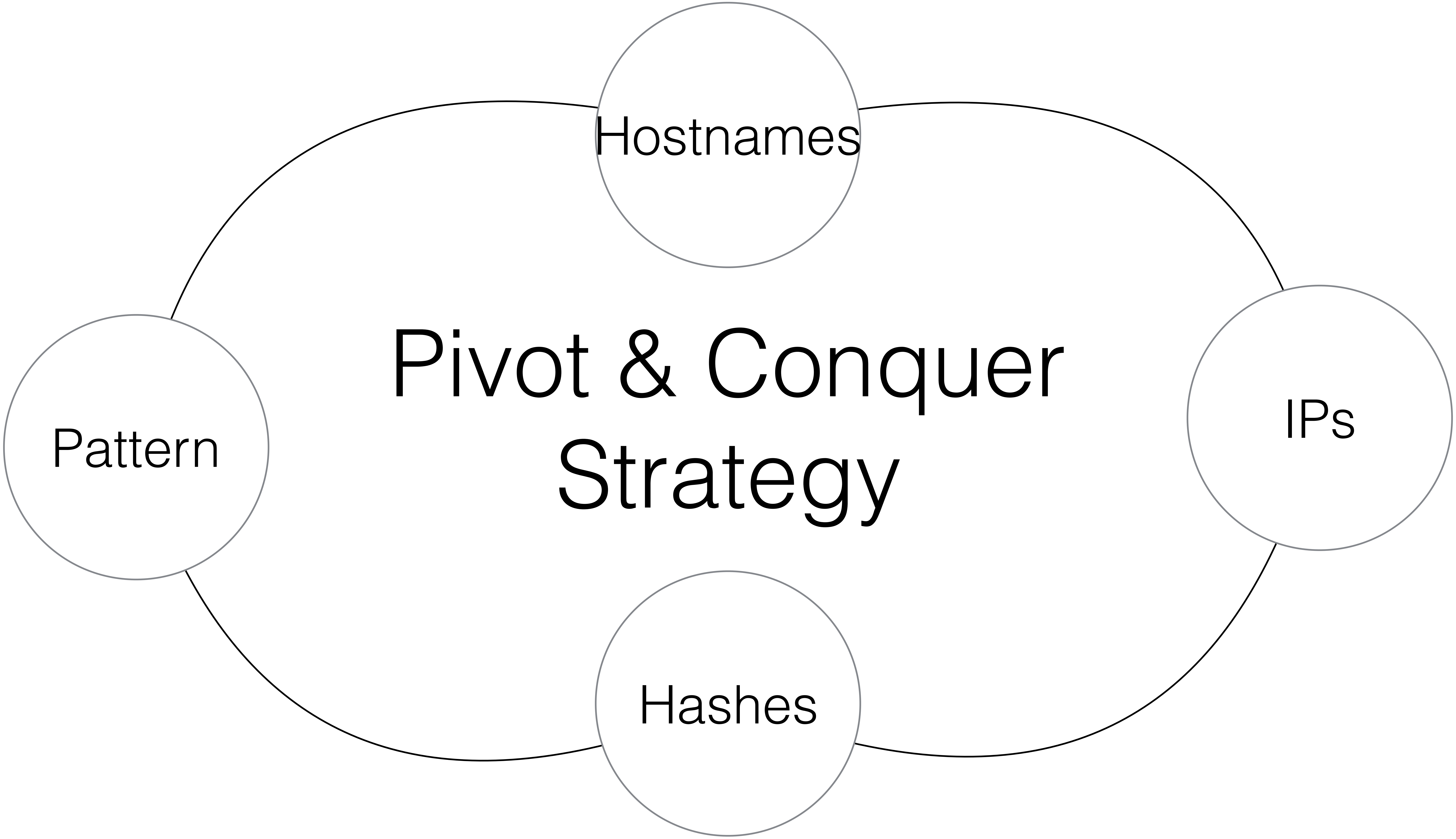


Thanks to Ross Gibb (Cisco AMP Threat Grid)!

Lets find well known malware

Lets find well known malware
(Thanks to our community we know about them!)

- Sality: ✓
- Zeus: ✓
- Asterope: ✓
- Cryptowall: ✓
- Vawtrak: ✓
- Andromeda: ✓
- Qbot: ✓
- Ramdo: ✓
- Geodo: ✓
- Necurs: ✓



Pivot & Conquer Strategy

Hostnames

IPs

Hashes

Pattern

The sality case

Modular botnet & file infector

UDP & HTTP Communication

Uses compromised sites

Active & stable since ~2003!

#infosec:
13 years later,
sality is still a problem.

IOCs will cause high number of FPs

http://www.ceylanogullari.com/logof.gif?8fcd2c7=1206294072

http://www.bluecubecreatives.com/logos.gif?8fcd5d3=603150156

Regexps are not flexible enough

How do I keep track of this?

Specialised classifier for Sality

http://www.bluecubecreatives.com/logos.gif?1c5de42b=475915307

http://www.ceylanogullari.com/logof.gif?1c5ddd77=1427740773

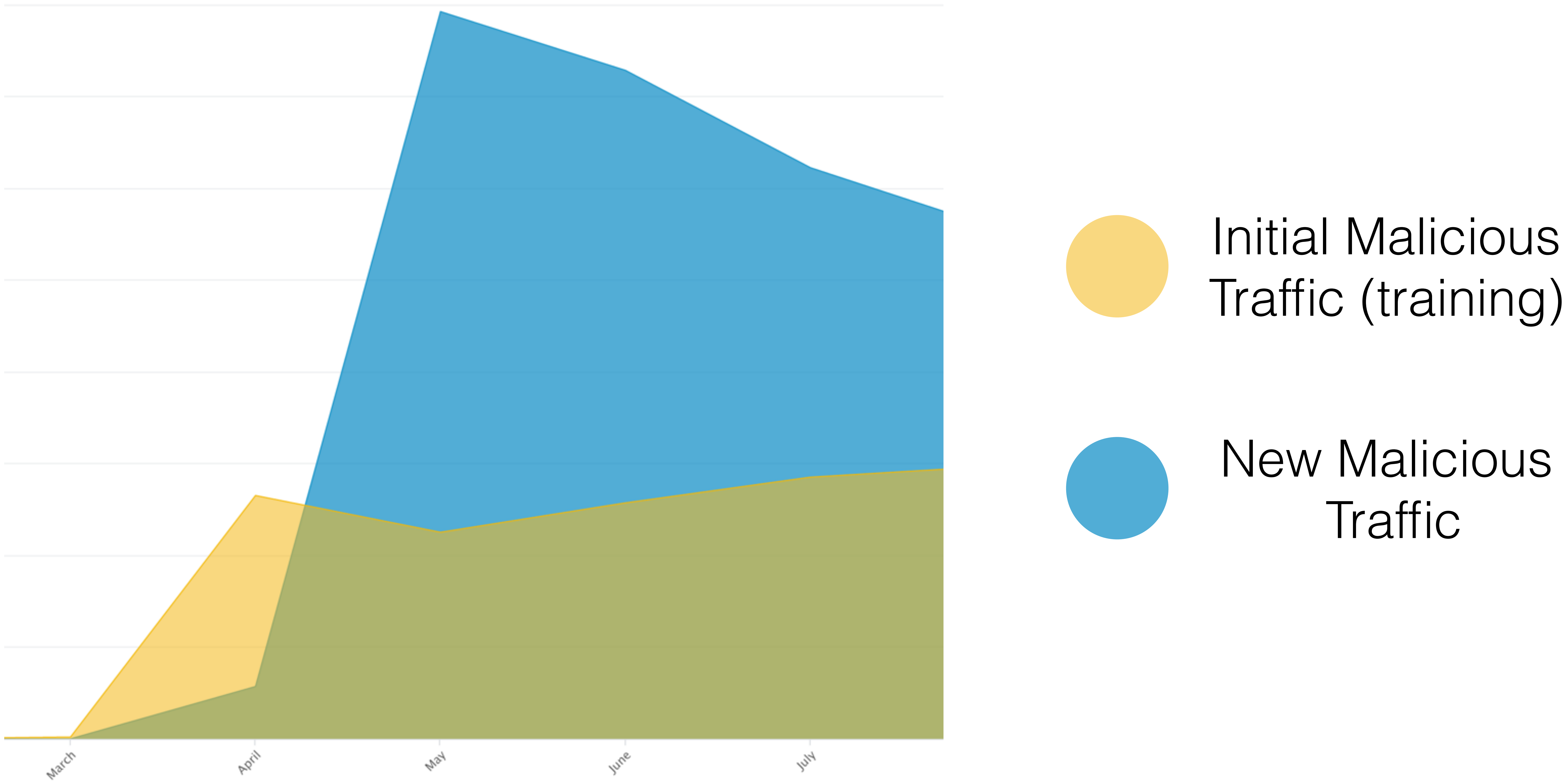
http://dewpoint-eg.com/images/logosa.gif?1c5dd29e=475910814

http://www.akkoncelik.com/images/logo.gif?1c67038=297820720

Analysts should spend their time **finding** new things

Can we create algorithms to automatically track malicious behaviours?

Modeling malware behavior



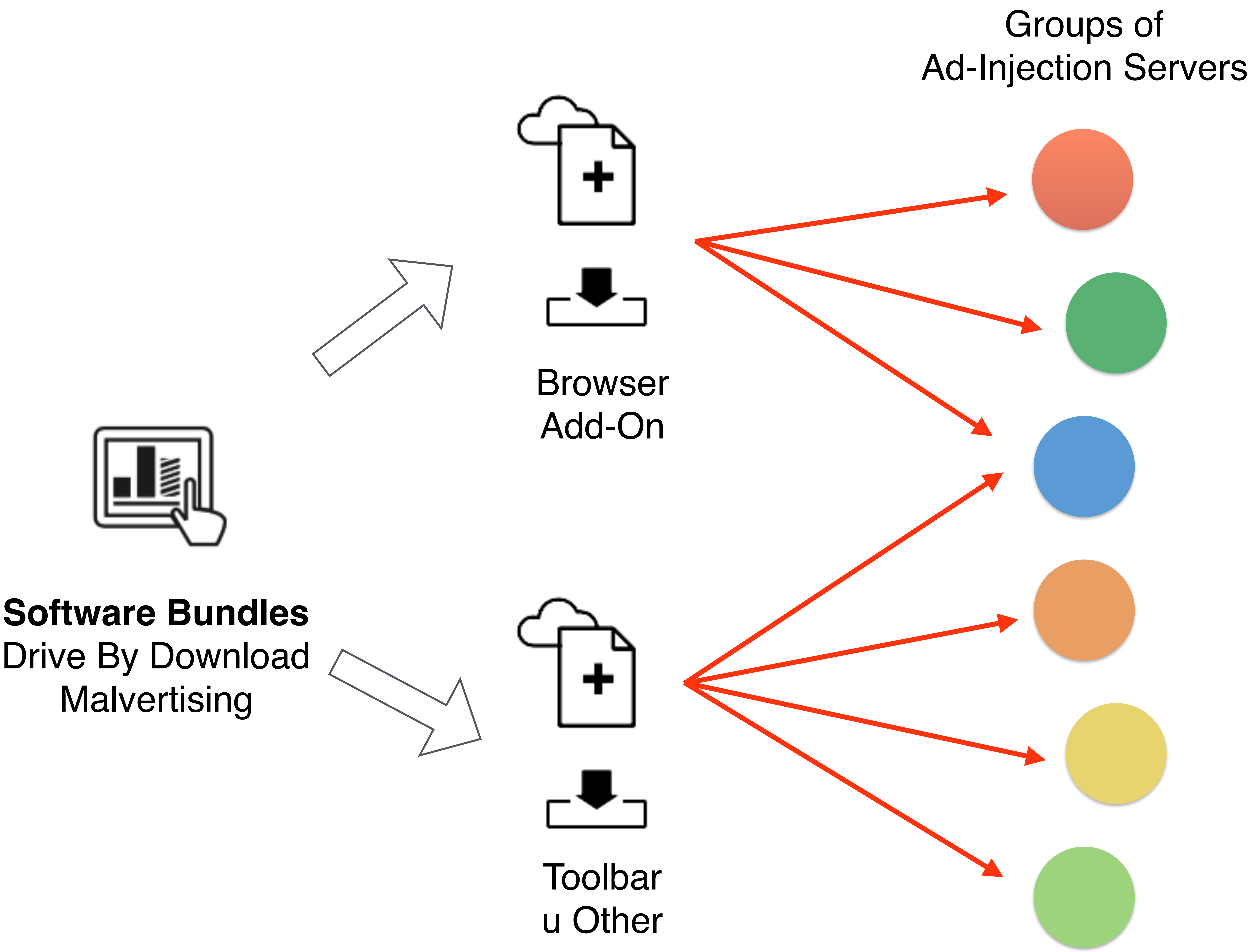
Tracking +200 malicious behaviors

60% is automated tracking

Let the machine do the machine work

While people worry about APTs,
Russia and China…

Adware exfiltrates our data
in plain sight…



Groups of
Ad-Injection Servers

Software Bundles
Drive By Download
Malvertising

Browser
Add-On

Toolbar
u Other

BROWSING
BEHAVIOR

REDUNDANCY

UNENCRYPTED

Exfiltration of Referer

Internal Sites

file:///C:/Users/[REDACTED]/AppData/Local/Microsoft/Windows/Temporary%20Internet%20Files/Content.Outlook/[REDACTED]/[REDACTED].pdf

Web Security Sites

http://alert.websec[REDACTED].com/alert/process?a=-3-A-kU0exaZkRLRYlyfI0GbX[REDACTED]

Exfiltration of Referer

Encrypted Sites

https://reservaciones.[REDACTED].com/travel

Personal Information

https://[REDACTED]airways.com/[REDACTED]/Booking/DeepLink?**trip_type**=one+way&[REDACTED]&fare_description=normal &persons.0=1 &depart=IXM&dest.1=MAA&date.0=07Mar&date_flexibility=flexible &origin=IN&userip=[REDACTED]&usercountry=[REDACTED]&referrerid=flexible&[REDACTED]&**from=**Madurai&**to=**Chennai&**departdate=**7/03/2016 &returndate=

Exfiltration of Referer

Personal Information

http://[REDACTED]bank.com/personal/[REDACTED]payments/pay-credi[REDACTED]

Information we consume

http://www.telegraph.co.uk/education/2016/04/22/this-maths-problem-has-thousands-of-people-baffled-can-you-work/

What can they know?

Our location

Our browsing history

Where do we work

Services we use

How are we protected

User credentials

Travel plans

Interests

Internal infrastructure of our organisation

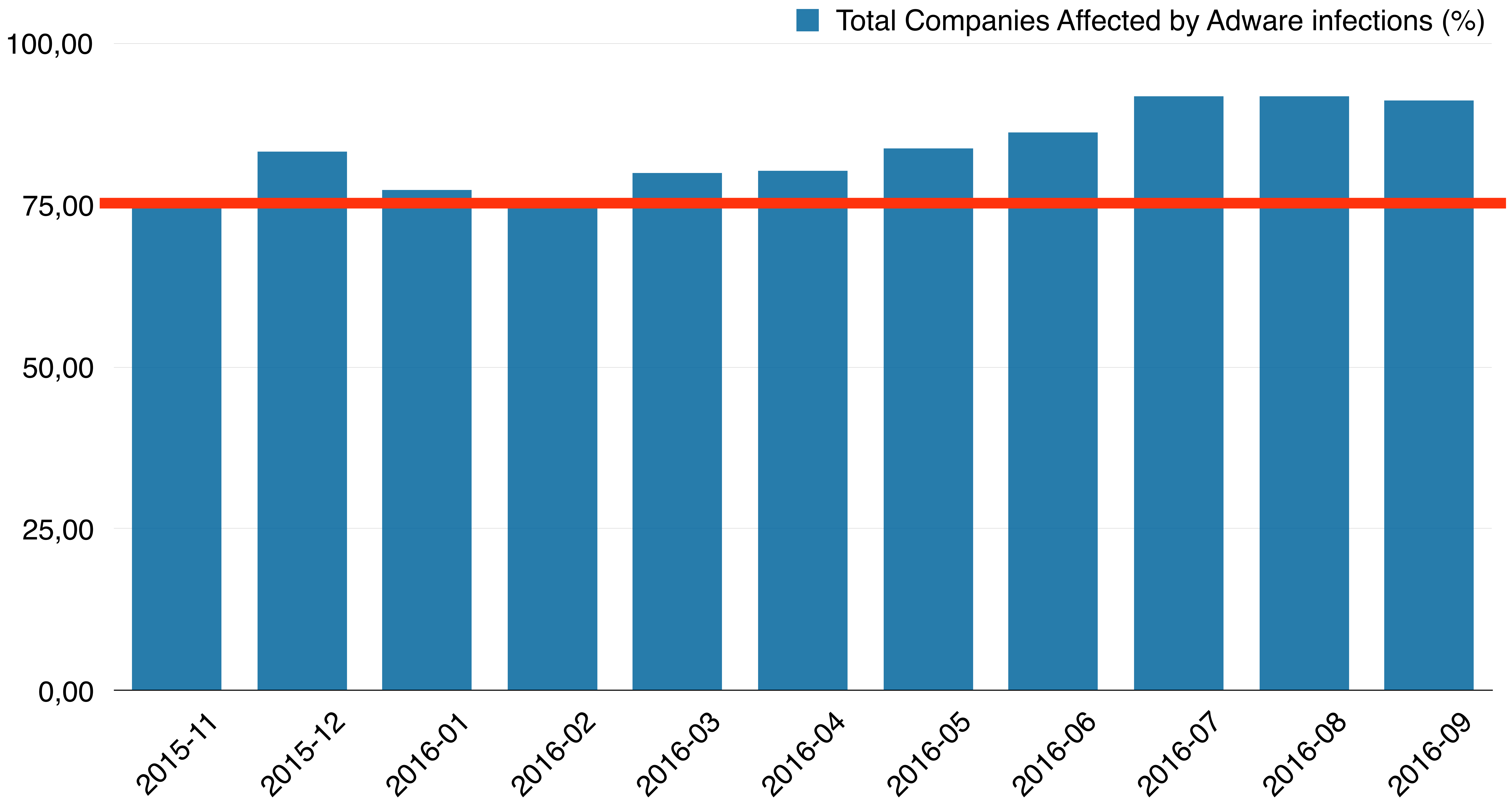
Time zone

Work hours

Relationships

Health issues

75% companies affected by adware

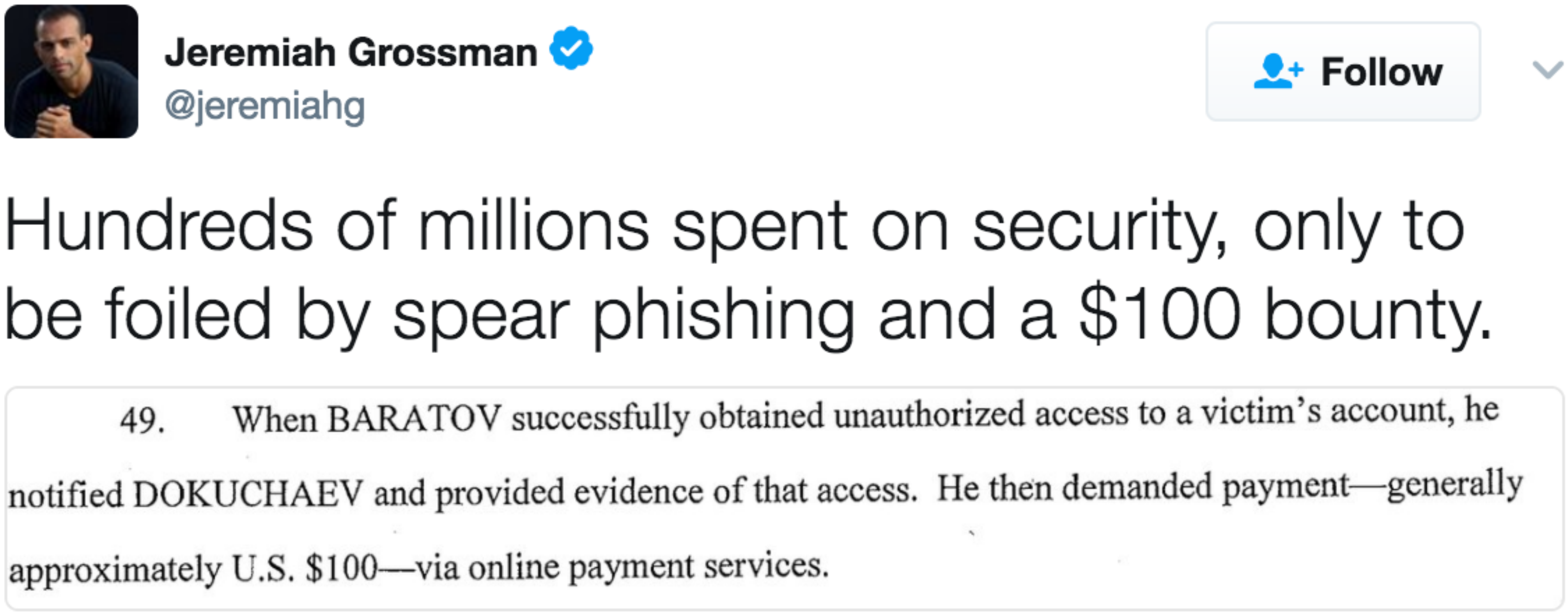


Threats are rarely unique

Know your network.

Use all tools at your disposal.

Don’t leave the users out.



Jeremiah Grossman

@jeremiahg

Hundreds of millions spent on security, only to be foiled by spear phishing and a $100 bounty.

49. When BARATOV successfully obtained unauthorized access to a victim's account, he notified DOKUCHAEV and provided evidence of that access. He then demanded payment—generally approximately U.S. $100—via online payment services.

Thank you

TROOPERS17
10 YEARS
MAKE THE WORLD A SAFER PLACE