

# Mapping criminal infrastructures from “patient zero” using Whois

David Piscitello  
Interisle Consulting Group

APWG

Massive data breaches  
– e.g., Target, Sony –  
were the result of a  
successful phishing  
attack

*Whois helps investigators  
learn what's below the  
surface of breaches or  
other cyber attacks*



# Patient zero



The first patient in an outbreak **who is** noticed by health authorities typically triggers a response or investigation





From patient zero investigators gather information to map the progression of a disease outbreak

- Who is patient zero?
- What are his symptoms?
- Where was he found?
- Where did he travel from and to?
- When did he travel?
- What threat does his condition pose?




# Index domains are the “patient zeros” of cyber investigations

- **Who is** the domain holder?
  - Notify the breach victim
  - Pursue the cyber attacker
- Where and when were the domains registered?
- *What other domains have similar registration data?*



**Attacks often involve a *conspiracy of domains...*  
use index domain to identify that conspiracy**



How do first  
responders  
use Whois?

Criminal Abuse of Domain Names:  
Bulk Registration and Contact Information Access

<http://www.interisle.net/sub/CriminalDomainAbuse.pdf>

# CASE STUDY CRIMINAL DOMAINS IN .TOKYO

- Abuse activity in .TOKYO from December 12, 2018 through December 25, 2018
- 8,715 .TOKYO criminal abuse domain names

Registrar	IANA ID	Criminal Abuse Domains Identified	Percent
GMO Internet, Inc. d/b/a Onamae.com	49	8,713	100.0
NameCheap, Inc.	1068	2	0.0

Nearly all of these were registered using a single registrar



1 ¥ = €0.0083

Anyone can win the domain first. Domain registration now!

Domain	Price
.com	999 yen
.net	1,160 yen
.jp	1,160 yen ~
.work	1 yen
.xyz	25 yen
.site	50 yen
.tokyo	149 yen

Current price expiration date: Thursday, August 22, 2019 until 17:00 (残り 19分 45秒 41秒 43)

Web site will create random names

Customers can upload a file of names

Search for a domain

1. Enter a string

2. Select domain type

Search results for .com, .xyz, .net, .biz, .jp, .site, .tokyo

Search results for .com, .xyz, .net, .biz, .jp, .site, .tokyo

Search results for .com, .xyz, .net, .biz, .jp, .site, .tokyo

## WHY THIS REGISTRAR?

- VERY CHEAP DOMAIN REGISTRATIONS
- CUSTOMERS CAN REGISTER IN VOLUME
- CUSTOMERS CAN GENERATE RANDOM LOOKING DOMAINS

# CHEAP DOMAIN NAMES CONTRIBUTE TO A CRIMINAL MARKETPLACE IN WHICH SMALL INVESTMENTS CAN YIELD EXTRAORDINARY RETURNS



1000s OF DOMAIN NAMES CAN BE ACQUIRED FOR PENNIES PER DOMAIN FROM REGISTRARS LIKE GMO INTERNET



MAILING LISTS CAN BE PURCHASED IN THE DARK WEB OR ONLINE



RANSOMWARE CAN BE PURCHASED AS A SERVICE FOR €35  
PHISHING KITS CAN BE DOWNLOADED FOR FREE FROM SOCIAL MEDIA SITES  
ONLINE TUTORIALS ARE AVAILABLE FROM YOUTUBE



ASSUMING A RANSOMWARE EXTORTION FEE OF \$200-500 USD, A RANSOMWARE ATTACK IS PROFITABLE WITH A HANDFUL OF VICTIMS



**EVEN A SINGLE RANSOMWARE OR PHISHING CAMPAIGN IS A LUCRATIVE ENTERPRISE**



# IDENTIFYING CRIMINAL ACTORS: SEARCH AND PIVOT

- .TOKYO sample spans a “post-GDPR” time period
- Use historical and recent Whois records
- Use {registrant name, registrant organization, registrant email} to
  - SEARCH historical Whois databases
  - PIVOT to other databases or social media
- to identify the criminal actors
- Only some Whois records contain contact data
- Assume that criminals submit inaccurate or fraudulently composed data



# WHAT DOES SEARCH-AND-PIVOT REVEALS?

- The harmful content or attack messages
- Where criminal actors host *infrastructure*, e.g.
  - Malware or ransomware executables
  - Phishing or financial fraud web pages
  - Political influence campaign material
  - Mail servers that send phishing lures
  - DNS servers that support DDoS attacks
- Other domain holders that may be part of a criminal enterprise
- Other Top-level domains in which the criminal actor has registered names





# WHAT SEARCH-AND-PIVOT FROM “PATIENT ZERO” REVEALED

- The suspect appears to have used GMO’s bulk registration tools to *generate thousands of random-looking domains names in matters of minutes.*
  - GMO offered .TOKYO domains registrations at very low cost.
- The suspect provided a registrant address in Japan.
  - The suspects targeted .TOKYO but not exclusively.  
.INFO, .CLUB, .ONLINE, .XYZ, .BIZ, .SPACE, and .WORK were also targeted.
- The suspect hosted Japanese phishing or malware at three hosting providers:
  - InterQ GMO Internet, Inc. , IDC Frontier, Inc., Sakura Internet, Inc.



The background features a close-up of a person's face, partially obscured by a dark, textured blue fabric. Overlaid on the image are several white, semi-transparent circular and arc-like graphics, some with tick marks, resembling a technical or digital interface. The overall color palette is dark, with shades of blue, black, and white.

## LET'S REVIEW:

JAPANESE SPAMMERS TARGETED  
JAPANESE USERS USING A  
JAPANESE REGISTRAR AND  
JAPANESE HOSTING OPERATORS





COMPLETE WHOIS RECORDS  
ARE ESSENTIAL  
IF FIRST RESPONDERS AND  
LAW ENFORCEMENT  
ARE TO IDENTIFY VICTIMS  
AND CRIMINAL ACTORS

BUT... DUE TO AN OVERLY  
BROAD INTERPRETATION OF  
THE EU GDPR

*PUBLIC WHOIS IS NOW  
DARK*

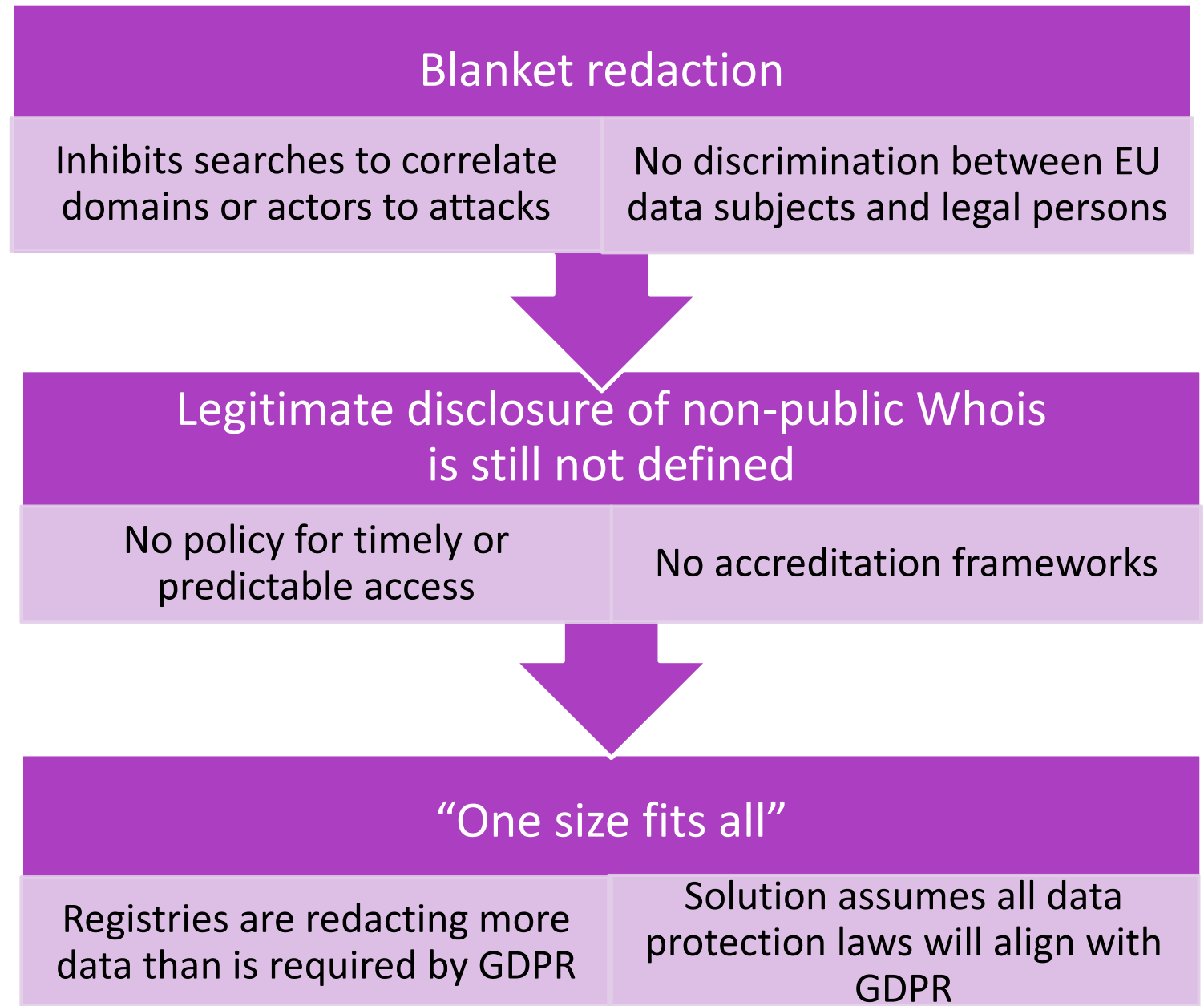


The background is a dark blue gradient with faint, concentric circular patterns. In the top-left corner, there is a circular inset containing a blurred image of CSS code. In the bottom-left corner, there is a circular inset showing a distorted, pixelated image of a person's face.

EU'S GDPR IS INTENDED TO  
PROTECT PERSONAL PRIVACY

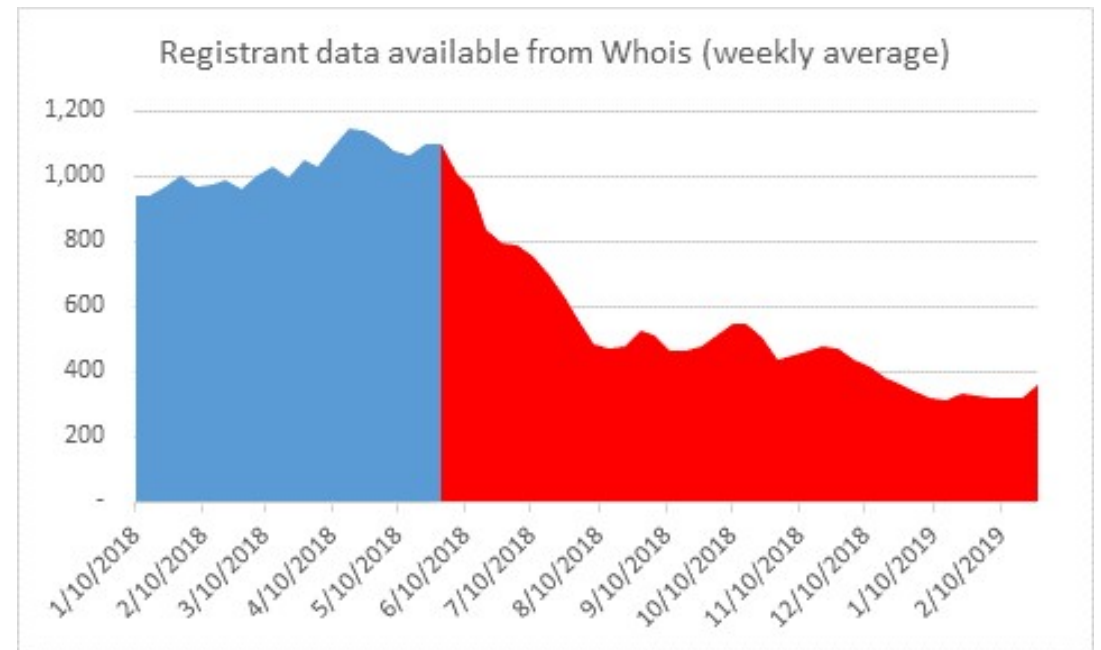
*Whois implementation  
protects Internet criminals  
or dark organizations*

# ADVERSE EFFECTS OF ICANN WHOIS POLICY





# EFFECT OF ICANN POLICY ON ACCESS TO HISTORICAL COMPLETE WHOIS RECORDS



Facts & Figures: Whois Policy Changes  
Impair Blocklisting Defenses  
<http://lnnk.in/@whoisimpedesblocklisting>





## **PRIVACY PROTECTION AND PUBLIC SAFETY: A DELICATE BALANCING ACT**

- WHEN PRIVACY REGULATION BLOCKS CRIMINAL INVESTIGATION CITIZENS ARE EXPOSED TO HARM AND LOSS
- DATA PROTECTION REGULATIONS MUST ACCOMMODATE FIRST RESPONDER AND LAW ENFORCEMENT ACCESS TO CRITICAL INFORMATION



# Creative Commons

- Slide 2, 3: Lassa Fever investigation, Mike Blyth  
<https://www.flickr.com/photos/blyth/>
- Slide 3: Enzootic Plague investigation, CDC Global,  
<https://www.flickr.com/photos/cdcglobal/>
- Slide 4: World Map, Share reproductions,  
<https://www.flickr.com/photos/shaireproductions/>
- Slide 10: Computer Hackers,  
<https://www.flickr.com/photos/121483302@N02/>
- All other images from Pixabay Images