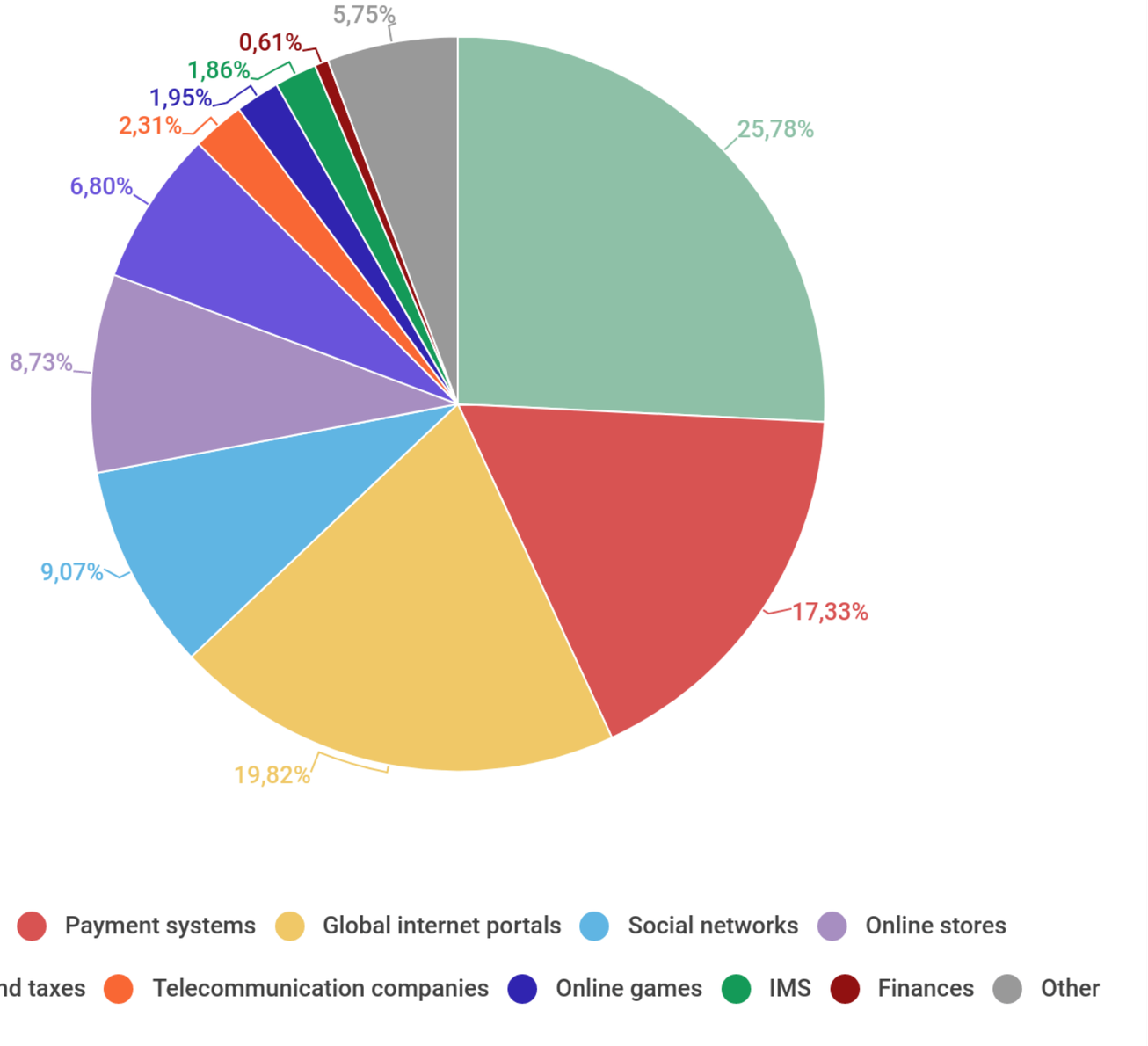
Jeopardize

a low(zero) cost threat intelligence&response tool against phishing domains

Utku Sen - DEF CON 28 Demo Labs

Who am I

- Security Analyst @HackerOne
- utkusen.com
- github.com/utkusen
- twitter.com/utkusen



KASPERSKY lab

Legitimate Admin 15:31

Activation of your account

Legitimate Admin <spoofed@gmail.com> SHOW MORE

Activation of your account

Wed, Apr 15 • 15:31

This message looks suspicious.

It is similar to other messages reported for phishing.

Mark as not phishing

Hi! This is totally legitimate email and you have nothing to worry about! Now, please click link below and type in your password!

Paypal Christmas Gifts
@PaypalChristm

paypall-christmasgifts.com

5:10 PM · Jan 1, 2019 · Twitter Web Client

Promoted by Paypal Christmas Gifts

1 Retweet **7** Likes

Show more replies

Attack Timeline

- 10:00 - Attacker promotes phishing tweet
- 10:15 - 300 people has seen the tweet
- 10:20 - 5 people entered their credentials
- 10:25 - accounts compromised
- 10:30 - Tweet is taken down due to the abuse reports

Solution?

- Abuse complaint to the domain&host provider ❌
- Abuse complaint to the Twitter ❌
- Abuse complaint to the Google ❌
- Be more proactive ✅

Being Proactive

- Detect possible phishing domains before the campaign ✅
- Do DDOS ❌ (If you have a huge budget) ✅
- Confuse the attacker ✅
- Observe the honey token flow ✅

What “jeopardize” does?

Early Detection

- Detects typosquatting, homograph etc. domains (fcaebook.com)
- **Analyzes**: *web server, name servers, HTML forms, Alexa ranking, page size, registration date etc.*
- Provides a “Risk Score”

FCAEBOOK.com

NS: Cloudflare
Web Server: ✅
Login Form: ✅
Registration: New

Risk Score: 90

FACEBOOKADS.com

NS: Godaddy
Web Server: ✅
Login Form: ❌
Registration: Old

Risk Score: 50

Confusing the Attacker & Buying Time

Attacker

Advertises

http://twitter.com

AcmeBank
TaxRefund

http://acmebnak.com

Username:
password:

User

Clicks

Sends Fake & Honey Creds

Jeopardize

Username	Password	
Utku	Kralbesiktas	LEGIT
David	Kingwestham	FAKE&HONEY
Serdar	Tissss	FAKE&HONEY
John	Lol123	FAKE&HONEY

From The Attacker’s Perspective

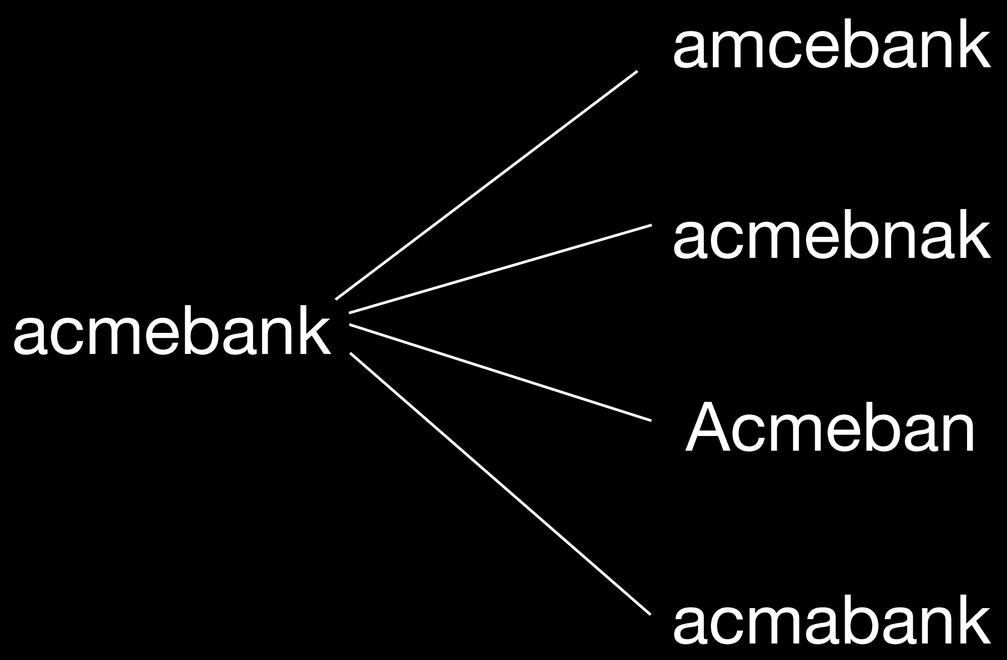
- Possibility 1) Most of the credentials are not working
- Possibility 2) All credentials are working but most of them are empty
- Losing time

From The Defender’s Perspective

- Observing the usage ratio of honey tokens.
- Tracking the attacker’s IP easily
- Detecting affected users
- More time to take precautions

How “jeopardize” works

Generating Domain Combinations



Detecting Registered Domains

- **Brute**: Combine the generated words (acmebnak, amcebank etc.) with all TLDs (com,net,xyz,live etc.)
    - **Pros**: Free
    - **Cons**: Slow
- **Daily**: Search the generated words (acmebnak, amcebank etc.) in daily registered domains
    - **Pros**: Fast
    - **Cons**: Requires zonefiles.io API key

Analyzing the Domains

- IP
- Web Server
- Name Servers
- Page Size
- If login form exists
- SSL Certificate
- Registration Date
- Alexa Ranking

Jeopardizing the Login Forms

- Feed the jeopardize with honey tokens
- Jeopardize sends them to the target domains

Saving the Results

```
<domain>
  <address>acmebnak.com</address>
  <name_servers>ns1.cloudflare.com ns2.cloudflare.com</name_servers>
  <mx_servers> </mx_servers>
  <date_flag>True</date_flag>
  <alexa_flag>False</alexa_flag>
  <webserver_flag>True</webserver_flag>
  <certificate_flag>False</certificate_flag>
  <form_flag>True</form_flag>
  <phishing_score>85</phishing_score>
</domain>
```

Usage

python3 jeopardize.py --domain facebook.com --type brute

python3 jeopardize.py --domain facebook.com --type incremental

python3 jeopardize.py --domain facebook.com --type daily -U user.txt -P pass.txt


jeopardize — -zsh — 135×42
utku@Utkus-MacBook-Pro jeopardize %

https://github.com/utkusen/jeopardize


helth