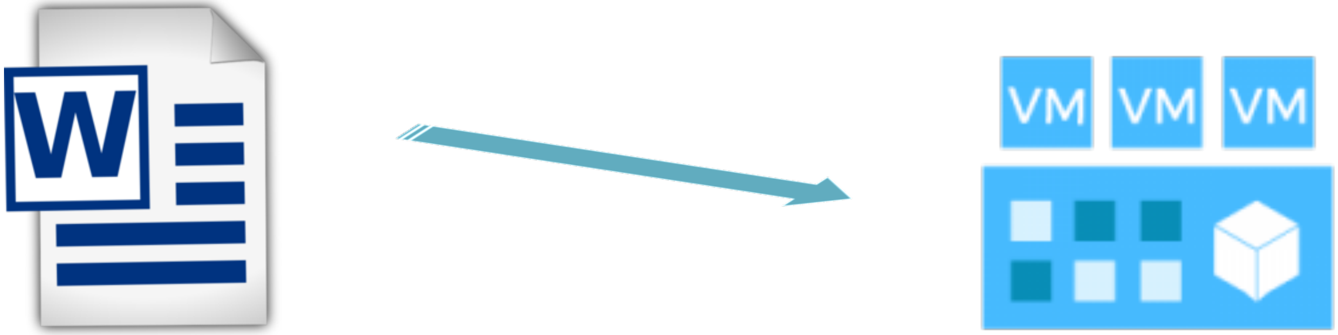
Bitdefender

BITDEFENDER SERENITY TECHNOLOGY

Sabin POTIRCA – Technical Project Manager
spotirca@bitdefender.com

BRIEF HISTORY

…two long years ago



- Send all documents from mail traffic to be opened in virtual machines
- Unclear purpose

BRIEF HISTORY (CON’D)

- A lot of research on technologies
- Was not a critical project
- Few resources, less progress, lots of issues
- Finally a “usable” framework

TURNING POINT

- Bring in the cavalry
- Start extracting information
- Much resources, such lack of results

WE NEED REAL WORLD DATA

- We like dogfooding
- Still not a critical project
- Easiest way to integrate was at network level
- Start the learning process

WE NEED REAL WORLD DATA (CONT'D)

- Why limit ourselves to SMTP?
- Added some more info extracted
- Entire HQ traffic filtered
- Re-start the learning process

MISTAKES WERE MADE

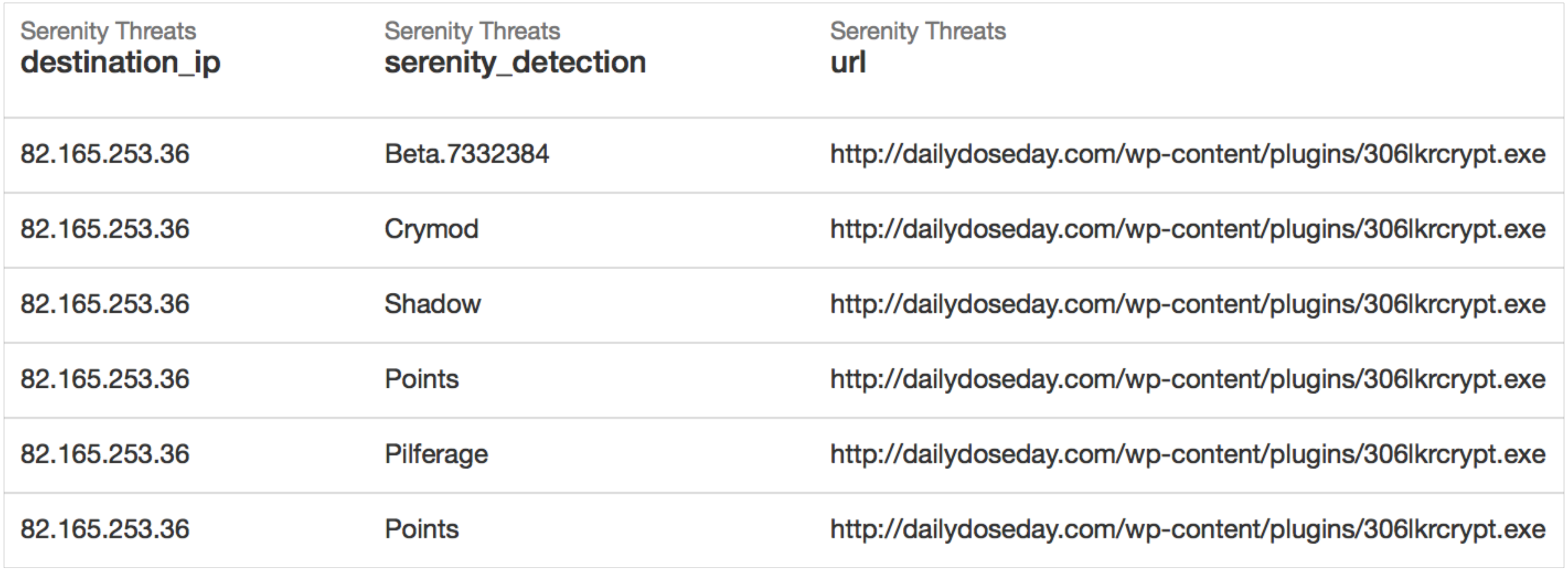
- In-house intercepting solutions vs open-source
- Focus on the wrong side of the optimizations war
- Aggressive vs too aggressive
- A lot of data, no means of visualizing

THERE WERE ALSO BENEFITS

- Discovered early on brand new malware
- We already had an idea of what and how it behaves
- Sped up the our reaction to emerging threats

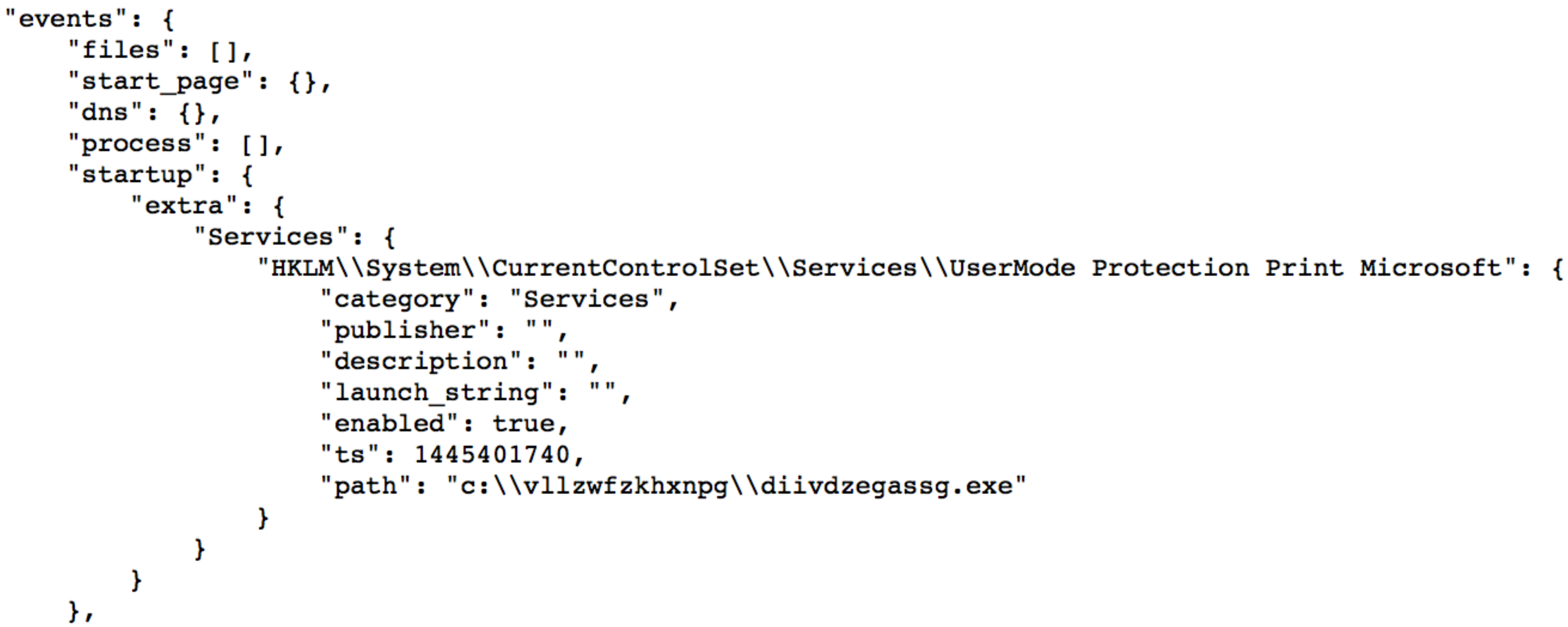
EXAMPLE

July, this year



Serenity Threats	Serenity Threats	Serenity Threats
destination_ip	**serenity_detection**	**url**
82.165.253.36	Beta.7332384	http://dailydoseday.com/wp-content/plugins/306lkrcrypt.exe
82.165.253.36	Crymod	http://dailydoseday.com/wp-content/plugins/306lkrcrypt.exe
82.165.253.36	Shadow	http://dailydoseday.com/wp-content/plugins/306lkrcrypt.exe
82.165.253.36	Points	http://dailydoseday.com/wp-content/plugins/306lkrcrypt.exe
82.165.253.36	Pilferage	http://dailydoseday.com/wp-content/plugins/306lkrcrypt.exe
82.165.253.36	Points	http://dailydoseday.com/wp-content/plugins/306lkrcrypt.exe

EXAMPLE OF ADDITIONAL INFO



```
"events": {
    "files": [],
    "start_page": {},
    "dns": {},
    "process": [],
    "startup": {
        "extra": {
            "Services": {
                "HKLM\\System\\CurrentControlSet\\Services\\UserMode Protection Print Microsoft": {
                    "category": "Services",
                    "publisher": "",
                    "description": "",
                    "launch_string": "",
                    "enabled": true,
                    "ts": 1445401740,
                    "path": "c:\\vllzwfzkhxnpg\\diivdzegassg.exe"
                }
            }
        }
    },
```

IN A PARALLEL UNIVERSE

- New project called KARMA
  - Focus on centralized management of events
  - Used mostly by the AM / AS / APH Labs for correlating various events / investigations
- Concept of Event Correlation was introduced

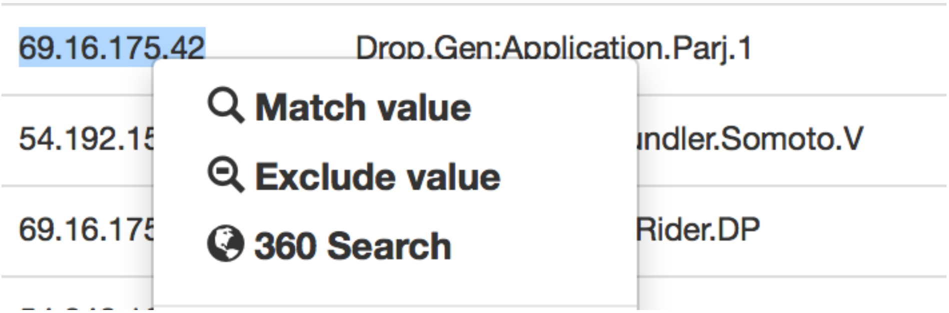
THE SYNERGY

- Serenity should and must send all malware events to KARMA
- Added some more events “sensors”
- And then added some more

ADDING MORE DATA

- Serenity already has access to a lot of other information
  - Added netflows

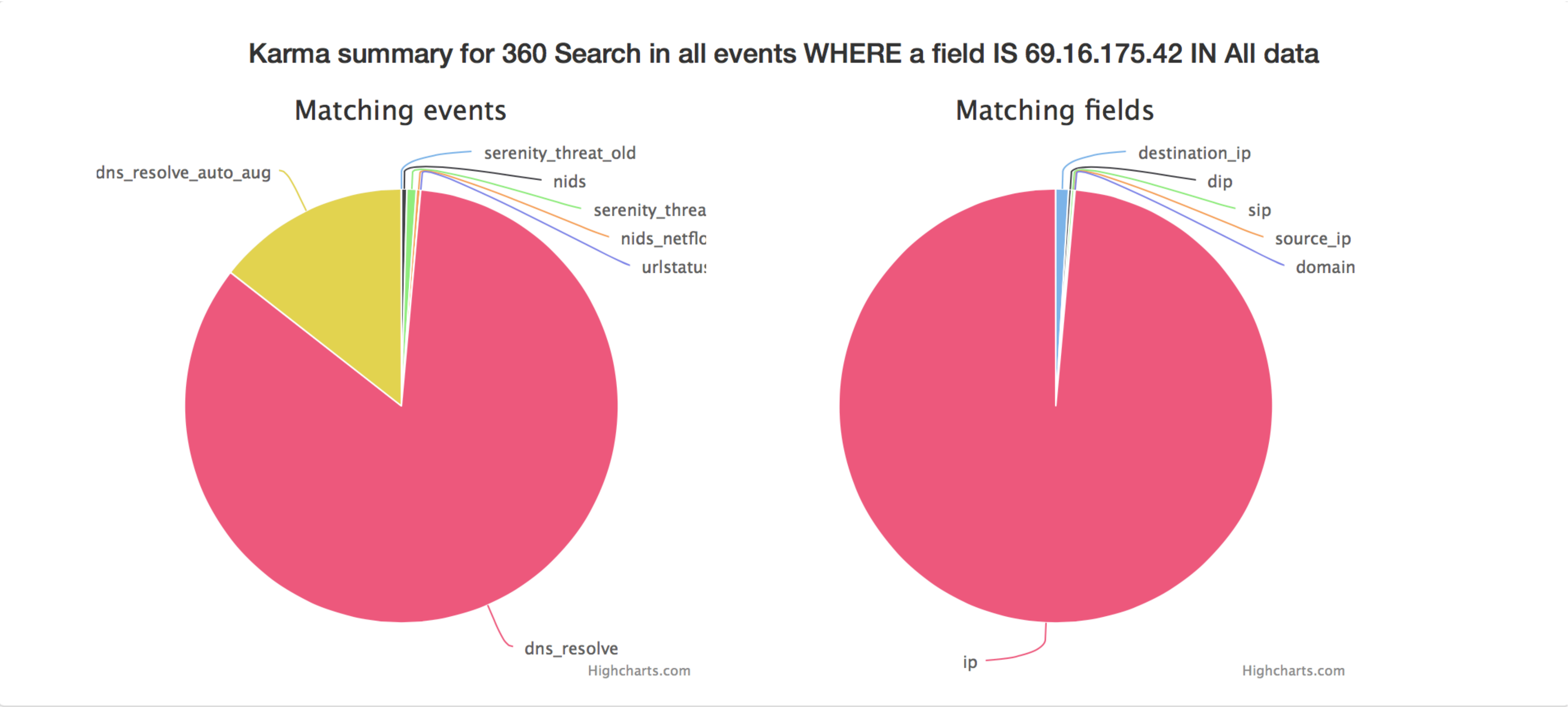
OUR FORENSICS



69.16.175.42	Drop.Gen:Application.Parj.1
54.192.15	ındler.Somoto.V
69.16.175	Rider.DP

- Search the entire Intelligence Database for various info
- Establish connections between different threat vectors

OUR FORENSICS (CONT'D)



- We also have pies and charts to back us …

SO MUCH DATA

- We have two teams of PhD’s and scientists
  - Machine Learning
  - Trends analysis

- On-going research for applications
- We already have (some) automated incident detection

BUT WE WANT MORE DATA

- Several external installations
- We would not refuse other beta-testers of the technology

ACHIEVEMENT UNLOCKED

- NOW It is considered a **CRITICAL** project

Thank you