Rocking your Windows Events with Elastic stack

Rodrigo Montoro
Pesquisador / Security Operations Center (SOC)
rodrigo@clavis.com.br

Partially supported by FAPERJ JCNE Proc. 203889
• Security Researcher (Octopus SIEM LABS)
• Author of 2 patents method to detect malware
• Logging and pcap addicted
• Dad
• Triathlete / Trail Runner
• Beer lover
Agenda

• Motivation
• Windows Events
• Elastic stack
• Demonstrations
• Conclusions
Motivation
Windows Events

- 9 categories
- 50+ subcategories
- Hundreds different Event IDs and fields
- Differences between Windows Versions
- Limit 300MB before erase old entries
Elastic Stack (former ELK)
How it works together?
• Open source
• Monitor Windows Events
  • Applications
  • Security
  • System
  • Hardware
• Encrypted communication
• Easy to install
Logstash filters

- grok
- geoip
- date
- cipher
- translate/dict
- cidr
- mutate
- xml
- json
- drop
Pro TIP!

- global.ip
- global.workstation
- global.username
- global.something
input {
  tcp {
    port => 1510
    tags => ["windows_ad"]
    codec => "json"
    type => "ad_eventlog"
  }
} # end input

output {
  elasticsearch {
    hosts => ["127.0.0.1"]
    codec => "plain"
    workers => 1
    index => "ad-%{+YYYY.MM.dd}"　
    manage_template => true
    template_name => "ad"
    template_overwrite => false
    flush_size => 100
    idle_flush_time => 1
  }
}

filter {
  if [type] == "ad_eventlog" {
    date {
      match => ["[EventTime]", "YYYY-MM-dd HH:mm:ss"]
    }
  }
  # Global IP / GEDIP
  if [DestAddress] {
    mutate { add_field => ["global.ip", "dst: %{DestAddress}" ] }
    geoip {
      source => "DestAddress"
      target => "global.geoip.dst"
    }
  }
  if [SourceAddress] {
    mutate { add_field => ["global.ip", "src: %{SourceAddress}" ] }
    geoip {
      source => "SourceAddress"
      target => "global.geoip.src"
    }
  }
  if [IpAddress] {
    mutate { add_field => ["global.ip", "src: %{IpAddress}" ] }
    geoip {
      source => "IpAddress"
      target => "global.geoip.src"
    }
  }
  #GlobalUser
  if [user] { mutate { add_field => ["global.user", "%{user}" ] } }
  if [TargetUserName] { mutate { add_field => ["global.user", "%{TargetUserName}" ] } }
  if [SubjectUserName] { mutate { add_field => ["global.user", "%{SubjectUserName}" ] } }
  if [UserName] { mutate { add_field => ["global.user", "%{UserName}" ] } }
  if [UserPrincipalName] { mutate { add_field => ["global.user", "%{UserPrincipalName}" ] } }
  if [OldTargetUserName] { mutate { add_field => ["global.user", "%{OldTargetUserName}" ] } }
  if [NewTargetUserName] { mutate { add_field => ["global.user", "%{NewTargetUserName}" ] } }
}
• Open source, distributed, full text search engine
• Based on Apache License
• Rapid access to information
• Stores data as structured JSON documents
• Supports single system OR multi-node clusters
• Easy to set up and scale – just add more nodes
• Provides a RESTful API
• Easy to create snapshots / backups
• INSECURE by default
• Discovery
  • Filters
  • Analysis
• Visualization
  • Improving analysis
  • Creating visual response
• Dashboards
• Plugins
Kibana Overview (demo)
import sys
import os
import commands
import datetime
from datetime import datetime
from elasticsearch import Elasticsearch, RequestsHttpConnection
es = Elasticsearch(connection_class=RequestsHttpConnection)
import json
import pprint
import time
from datetime import date
from datetime import datetime, tzinfo, timedelta
API Search sample

```
[root@OctopusLiveDemo SANS]# python remote_4624.py 'now-8h' 5 'ad-*' 2

===== SDC Research Labs =====
Horario comando - 2016-06-04 18:08:44.334709
Intervalo now-8h com total 4 Hits

Filtro executado - EventID:"4625" AND LogonType:"10"

==== Horario (GMT 0) : 2016-06-04T13:49:46.000Z
EventID: 4625
Target Username: sans
Process Name: C:\\Windows\\System32\\winlogon.exe
Country Source: Brazil
IP Source: 177.3.183.44

==== Horario (GMT 0) : 2016-06-04T13:49:53.000Z
EventID: 4625
Target Username: sans
Process Name: C:\\Windows\\System32\\winlogon.exe
Country Source: Brazil
IP Source: 177.3.183.44

==== Horario (GMT 0) : 2016-06-04T13:48:50.000Z
EventID: 4625
Target Username: sans
Process Name: C:\\Windows\\System32\\winlogon.exe
Country Source: Brazil
IP Source: 177.3.183.44

==== Horario (GMT 0) : 2016-06-04T11:02:15.000Z
EventID: 4625
Target Username: wqgw23
Process Name: C:\\Windows\\System32\\winlogon.exe
Country Source: Netherlands
IP Source: 185.56.82.34

[root@OctopusLiveDemo SANS]#
```
Demonstrations

- Kibana Overview
- Python API
  - Confidential file access
  - RDP access from not allowed user
  - Threat Intel correlation
  - TopX per field
Explore and understand all eventids and their fields
Be ready for forensics situation
Understand threat you are facing so you could "script"
Generate proactive alerts using Python API
Check new detections against old events
Make sure about Elastic stack hardening
Acknowledgements

The present work was partially supported by FAPERJ
Grant JCNE Proc. Number 203889
Coordinated by Raphael Machado
Thank you!!!

rodrigo@clavis.com.br

@spookerlabs / @ClavisSecurity

Rodrigo “Sp0oKeR” Montoro
Researcher / Security Operations Center (SOC)