FPT UNIVERSITY

Develop the anomalies process detection system

Supervisor

Do Xuan Cho

Team member

Nguyen Anh Tuan	SE62864
Nguyen The Lam	SE63326
Nguyen Quang Dam	SE05820
Nguyen Quoc Anh	SE06070
Phan Manh Truong	SE02605

Table of content

1. Problem and Idea

2. Process of implementation

    - Hash service
    - IP-domain service
    - Domain ML service
    - Mitre service

3. Result

Problem and Idea

Problem

“There are two types of companies: those who have been hacked, and those who don’t yet know they have been hacked.” - Cisco CEO **John Chambers**.

Current solution

BKAV Antivirus

splunk

Kaspersky EDR

Our idea

- Realtime detect malicious behaviors.
- Collect Sysmon event log data analyst them.
- Central system detection.
- Easy to use and config rule.
- Forensic source of the attack.

Process of implementation

Technologies using

Flask

API

elasticsearch + logstash + kibana

redis

React

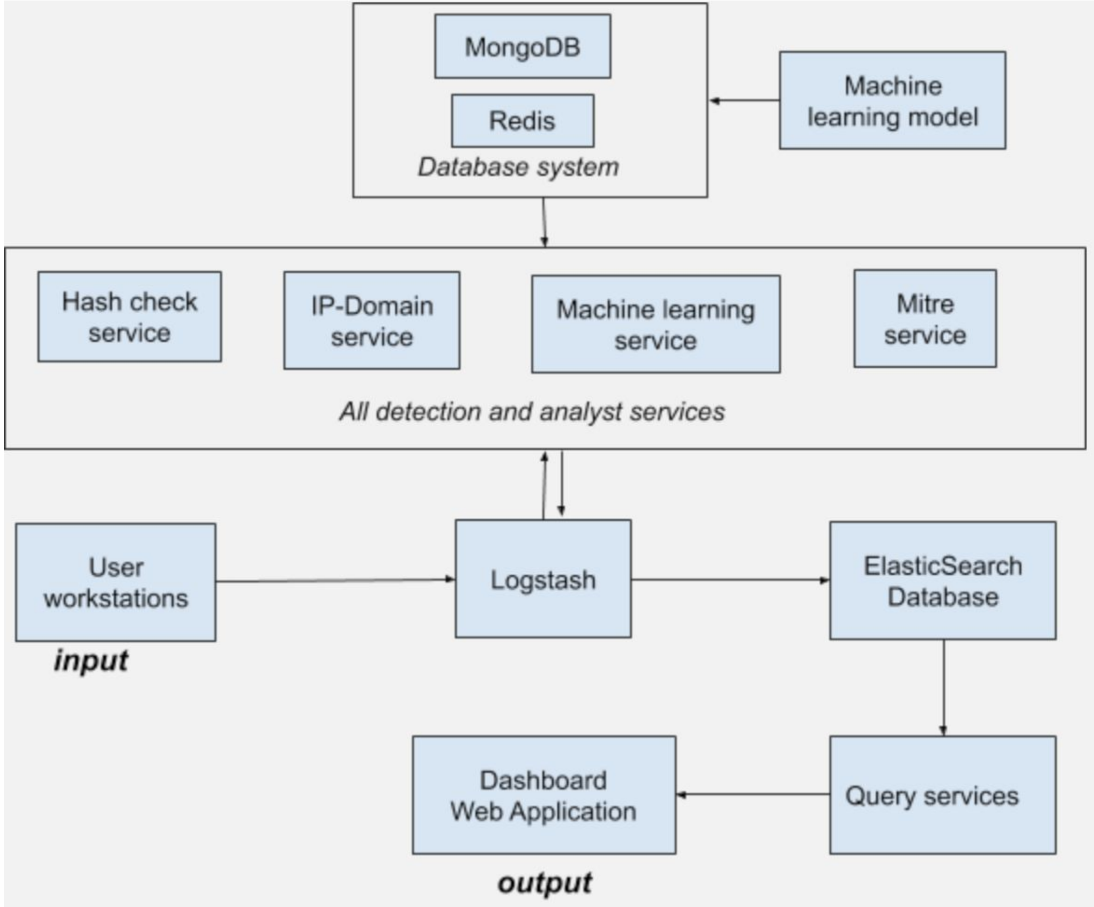
Google Cloud

mongoDB

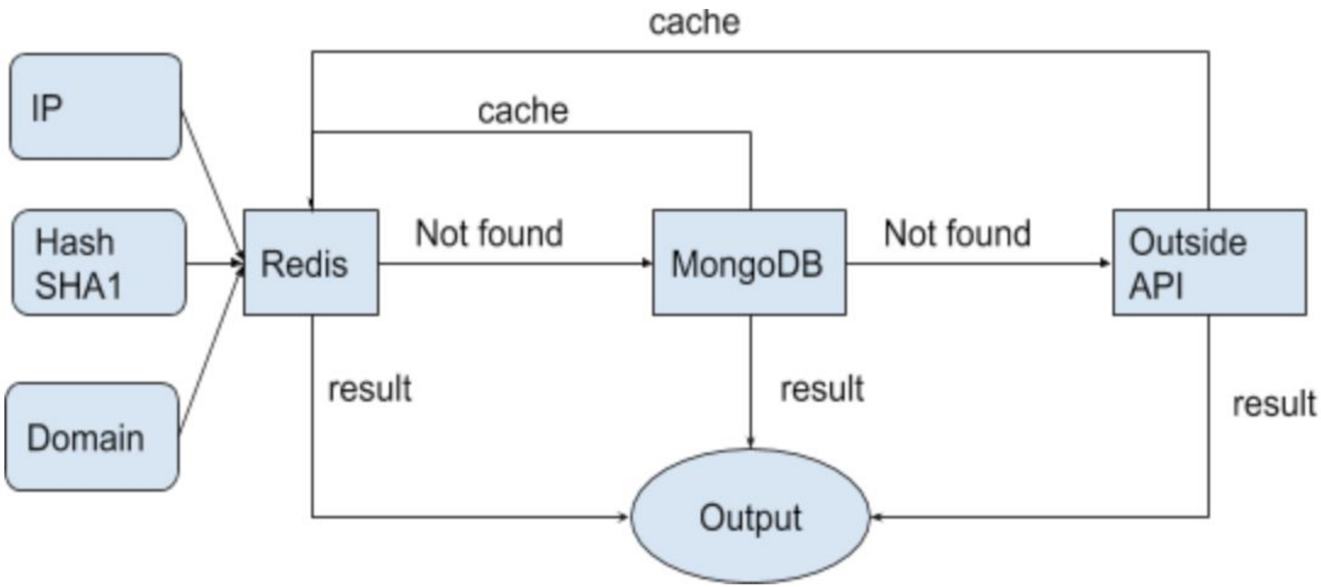
Microservice

Service	**Description**
Hash service	Detect blacklist SHA1
IP-domain service	Detect blacklist IP and domain
Domain ML service	Detect malicious domain based on machine learning model.
Mitre service	Detect malicious behavior based on rule.
Query service	Detect query service.
Dashboard web application	Show and visualize the result.

Overview system architecture

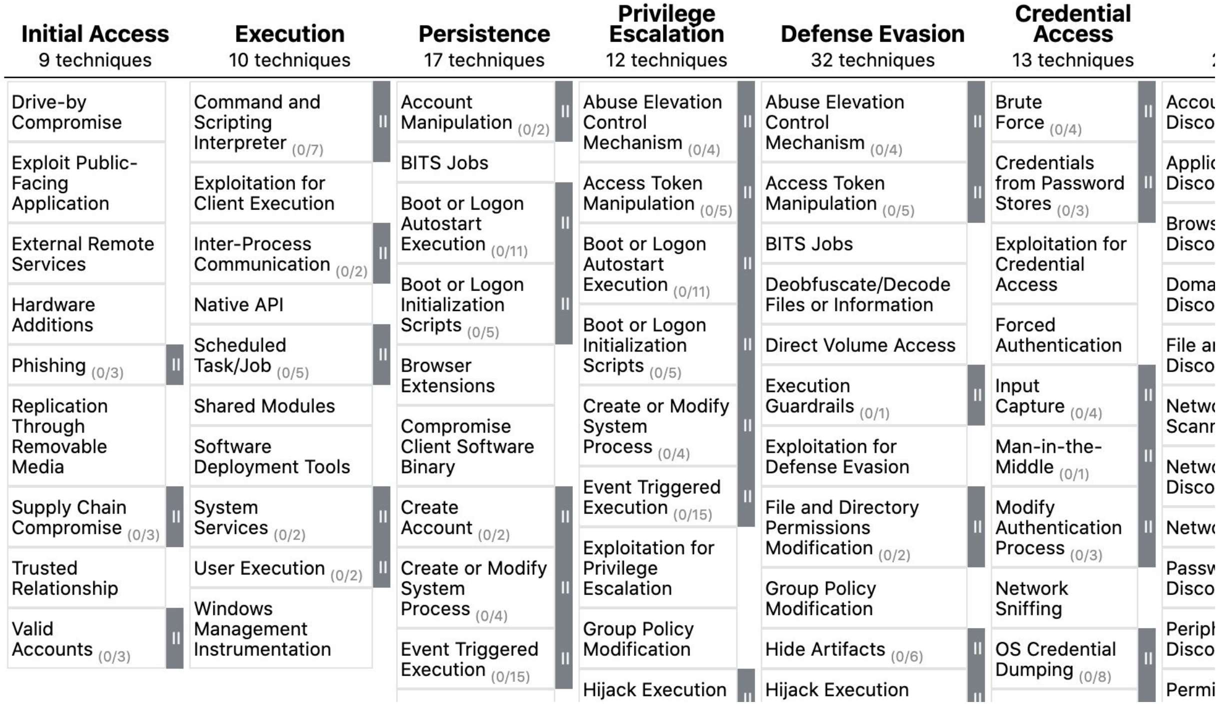


Hash service and IP-domain service



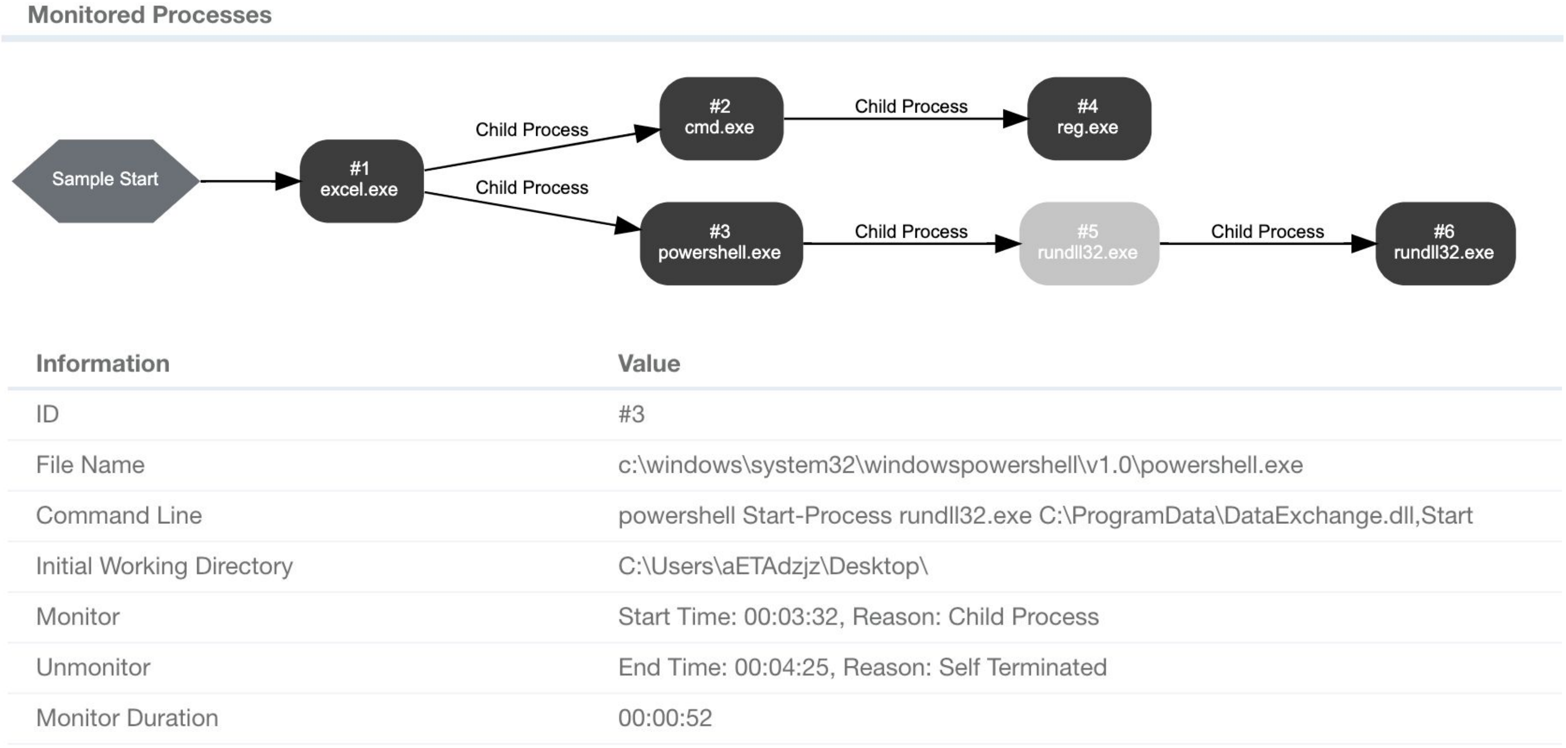
Mitre service

Mitre Att&ck matrix



Initial Access 9 techniques	Execution 10 techniques	Persistence 17 techniques	Privilege Escalation 12 techniques	Defense Evasion 32 techniques	Credential Access 13 techniques	
Drive-by Compromise	Command and Scripting Interpreter (0/7)	Account Manipulation (0/2)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Brute Force (0/4)	Accou Disco
Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Credentials from Password Stores (0/3)	Applic Disco
External Remote Services	Inter-Process Communication (0/2)	Boot or Logon Autostart Execution (0/11)	Boot or Logon Autostart Execution (0/11)	BITS Jobs	Exploitation for Credential Access	Brows Disco
Hardware Additions	Native API	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Deobfuscate/Decode Files or Information	Forced Authentication	Doma Disco
Phishing (0/3)	Scheduled Task/Job (0/5)	Browser Extensions	Create or Modify System Process (0/4)	Direct Volume Access	Input Capture (0/4)	File ar Disco
Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Event Triggered Execution (0/15)	Execution Guardrails (0/1)	Man-in-the-Middle (0/1)	Netwo Scann
Supply Chain Compromise (0/3)	Software Deployment Tools	Create Account (0/2)	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Modify Authentication Process (0/3)	Netwo Disco
Trusted Relationship	System Services (0/2)	Create or Modify System Process (0/4)	Group Policy Modification	File and Directory Permissions Modification (0/2)	Network Sniffing	Netwo
Valid Accounts (0/3)	User Execution (0/2)	Event Triggered Execution (0/15)	Hijack Execution	Group Policy Modification	OS Credential Dumping (0/8)	Passw Disco
	Windows Management Instrumentation			Hide Artifacts (0/6)		Periph Disco
				Hijack Execution		Permi

Mitre service



Monitored Processes

Information	Value
ID	#3
File Name	c:\windows\system32\windowspowershell\v1.0\powershell.exe
Command Line	powershell Start-Process rundll32.exe C:\ProgramData\DataExchange.dll,Start
Initial Working Directory	C:\Users\aETAdzjz\Desktop\
Monitor	Start Time: 00:03:32, Reason: Child Process
Unmonitor	End Time: 00:04:25, Reason: Self Terminated
Monitor Duration	00:00:52

source: vmray

Mitre service

Rule structure

```
title
status [optional]
description [optional]
references [optional]

detection
   {search-identifier} [optional]
      {string-list} [optional]
      {field: value} [optional]
   ...
   condition
fields [optional]
level [optional]
tags [optional]
...
[arbitrary custom fields]
```

Rule sample

```yaml
tags:
    - attack.command_and_control
    - attack.t1071
    - attack.t1071.004
```

```yaml
logsource:
    category: process_creation
    product: windows
detection:
    selection:
        Image|endswith:
            - '\powershell.exe'
        ParentImage|endswith:
            - '\excel.exe'
        CommandLine|contains:
            - 'DataExchange.dll'
    condition: selection
level: critical
```

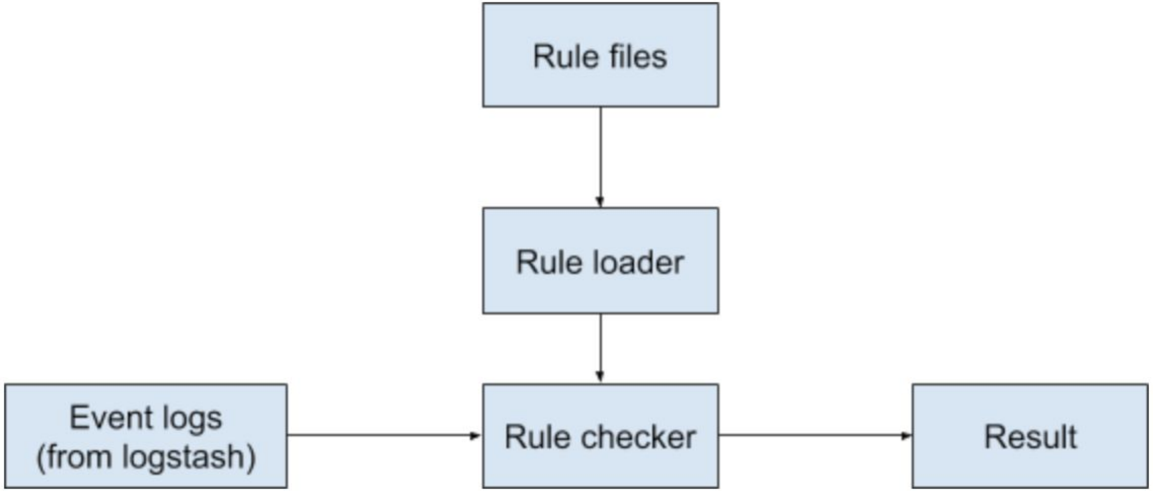
Rule sample

```
tags:
   - attack.lateral_movement
   - attack.g0010
   - attack.credential_access
   - attack.t1098
   - attack.exfiltration
   - attack.t1002
   - attack.t1560
```

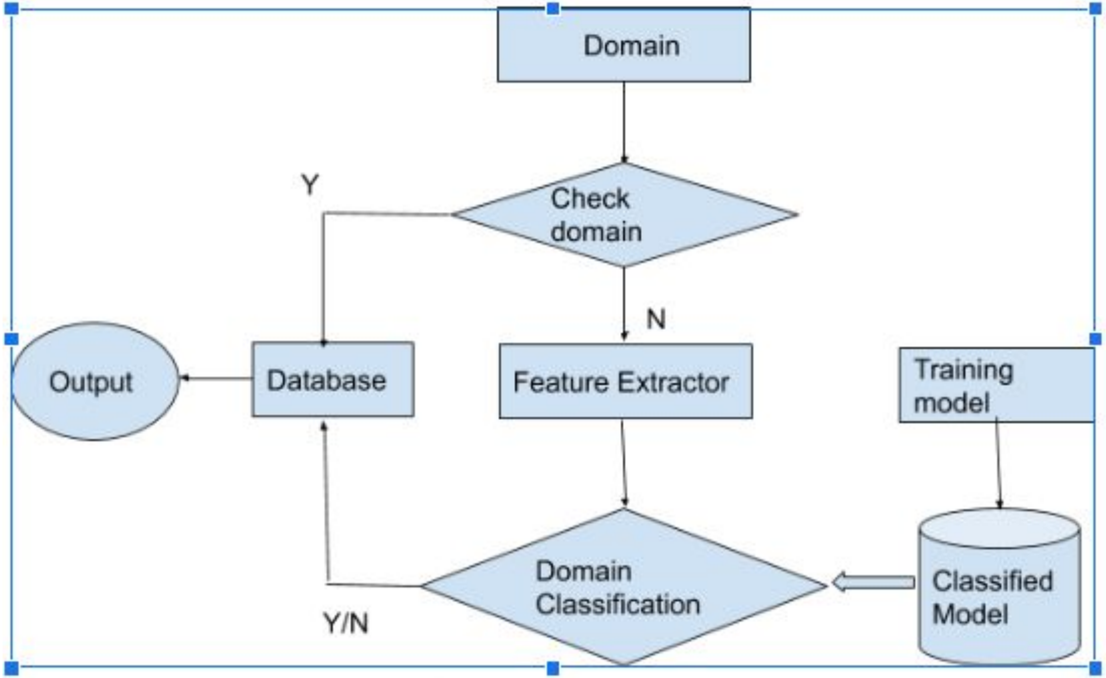
```
logsource:
   category: process_creation
   product: windows
detection:
   selection1:
       CommandLine:
           - '*\ldifde.exe -f -n *'
           - '*\7za.exe a 1.7z *'
           - '* eprod.ldf'
           - '*\aaaa\procdump64.exe*'
           - '*\aaaa\netsess.exe*'
           - '*\aaaa\7za.exe*'
           - '*copy .\1.7z \\*'
           - '*copy \\client\c$\aaaa\\*'
   selection2:
       Image: C:\Users\Public\7za.exe
      condition: selection1 or selection2
level: critical
```

Mitre service

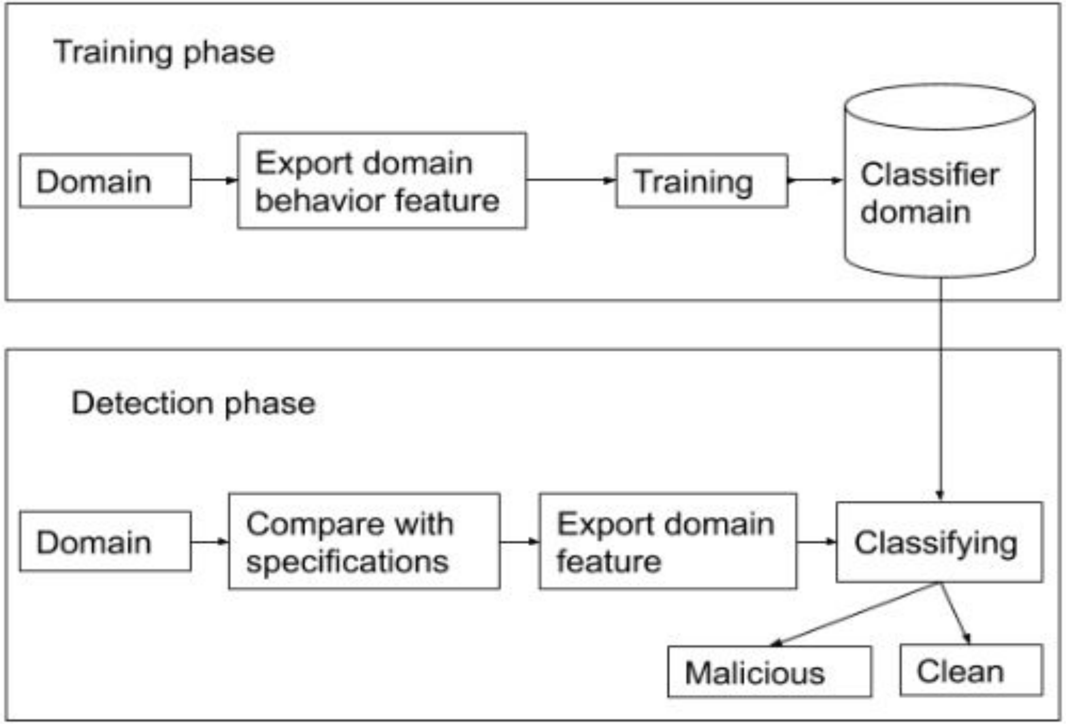
Overview of architecture



Machine learning service architecture



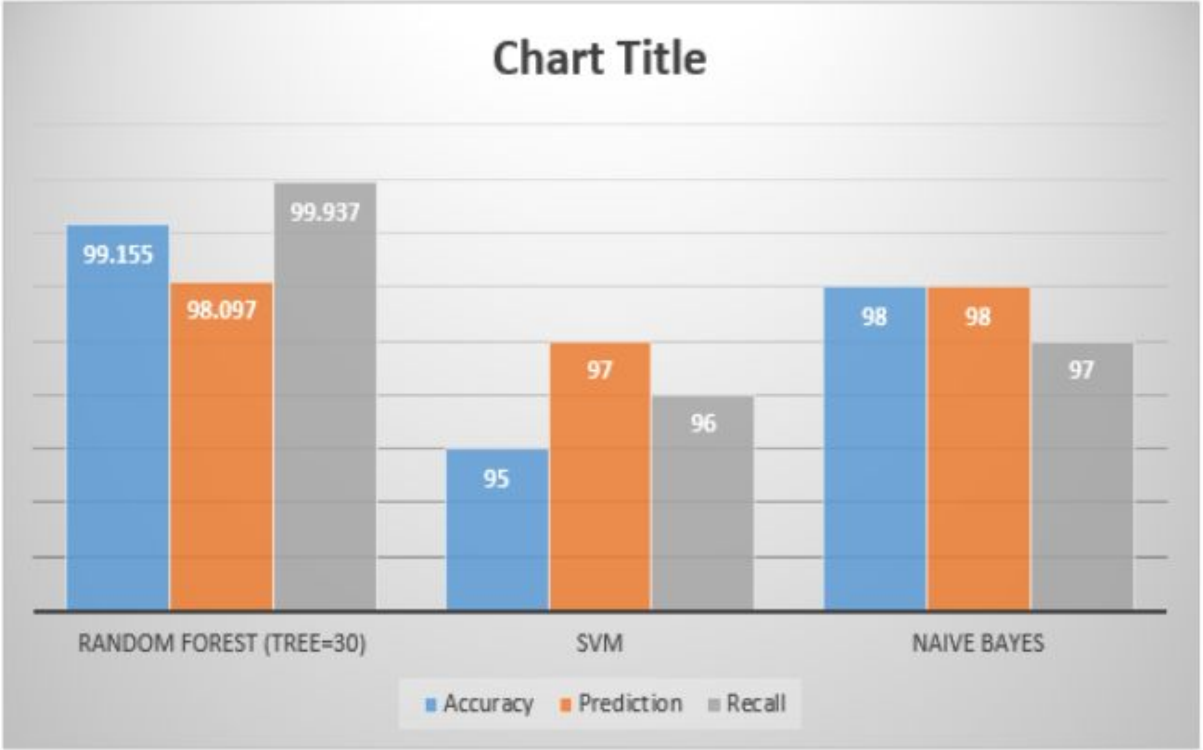
Machine learning architecture



Experimental detection of domain

Domain type	Number of records
malicious domain	99155
clean domain	63898
total	163053

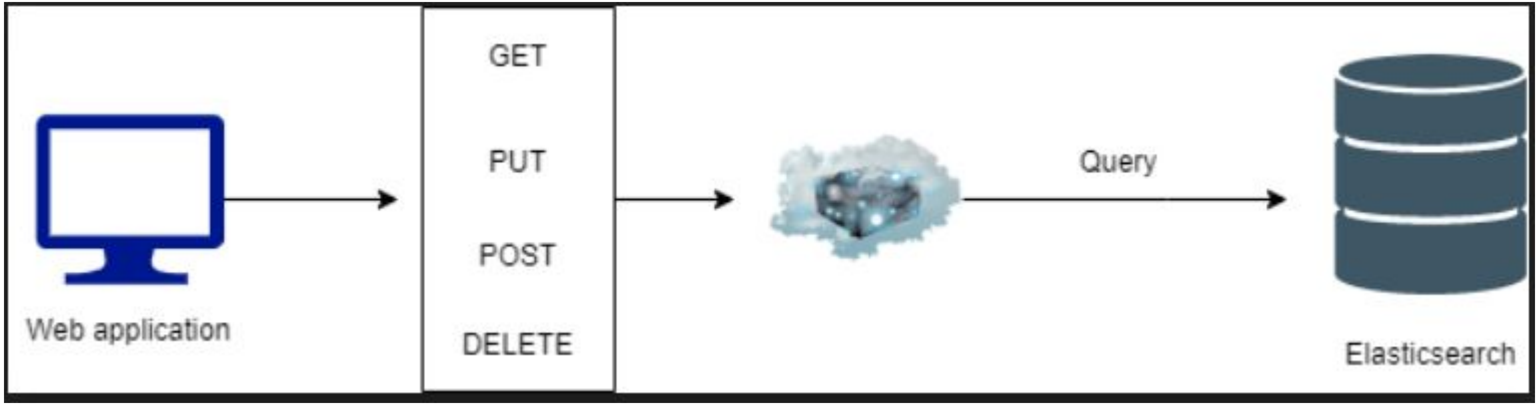
Experimental algorithm



Experimental results

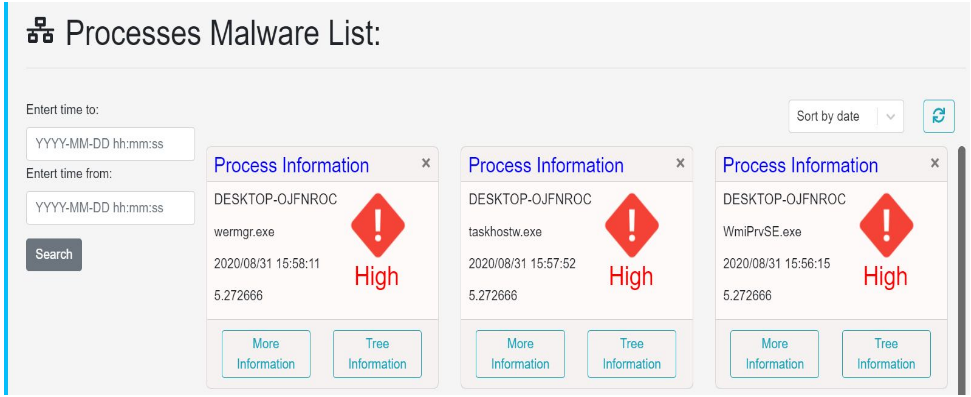
	positive	Negative
True	29116 (97.895％)	19237(99.870％)
False	626 (2.105％)	25 (0.130％)

Query service



Web portal

Search



Processes Malware List:

Entert time to:

YYYY-MM-DD hh:mm:ss

Entert time from:

YYYY-MM-DD hh:mm:ss

Process Information

DESKTOP-OJFNROC
wermgr.exe
2020/08/31 15:58:11
5.272666
High

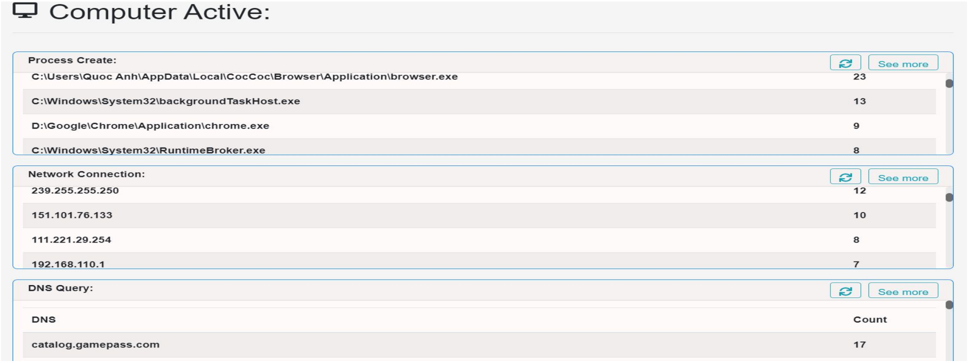
Process Information

DESKTOP-OJFNROC
taskhostw.exe
2020/08/31 15:57:52
5.272666
High

Process Information

DESKTOP-OJFNROC
WmiPrvSE.exe
2020/08/31 15:56:15
5.272666
High

Manage



Computer Active:

Process Create:

C:\Users\Quoc Anh\AppData\Local\CocCoc\Browser\Application\browser.exe	23
C:\Windows\System32\backgroundTaskHost.exe	13
D:\Google\Chrome\Application\chrome.exe	9
C:\Windows\System32\RuntimeBroker.exe	8

Network Connection:

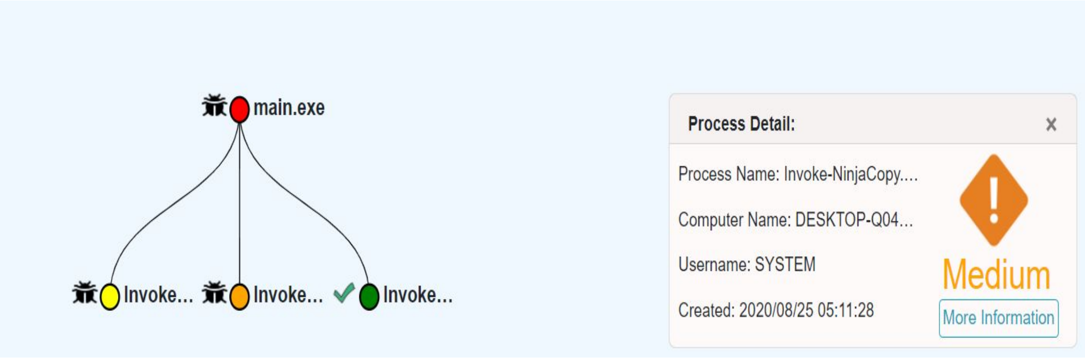
239.255.255.250	12
151.101.76.133	10
111.221.29.254	8
192.168.110.1	7

DNS Query:

DNS	Count
catalog.gamepass.com	17

Web portal

Tree Information



Process Detail: ×

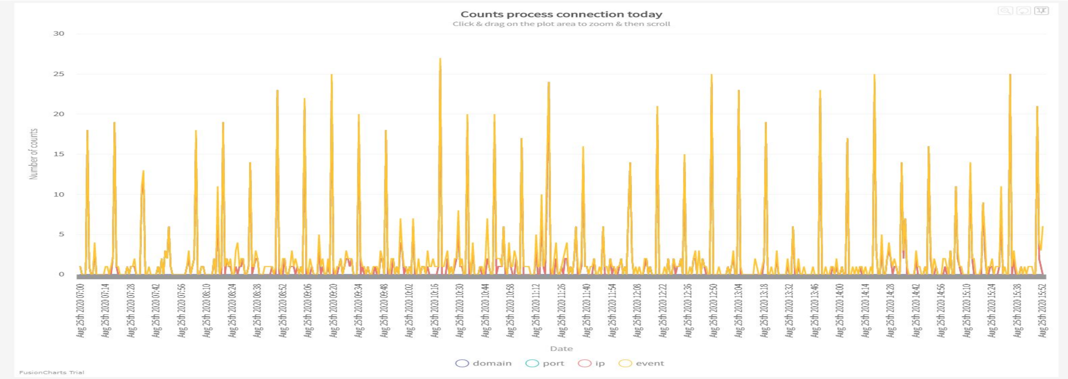
Process Name: Invoke-NinjaCopy....

Computer Name: DESKTOP-Q04...

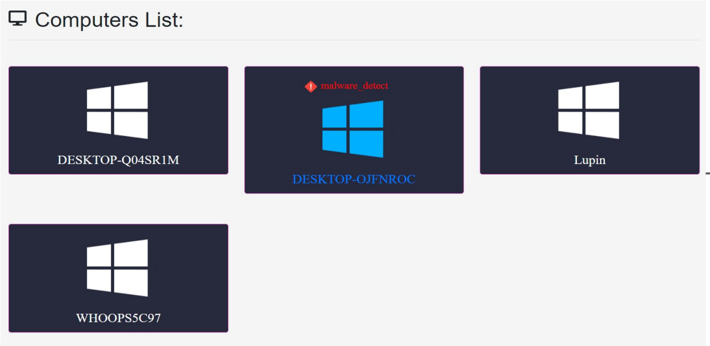
Username: SYSTEM

Created: 2020/08/25 05:11:28

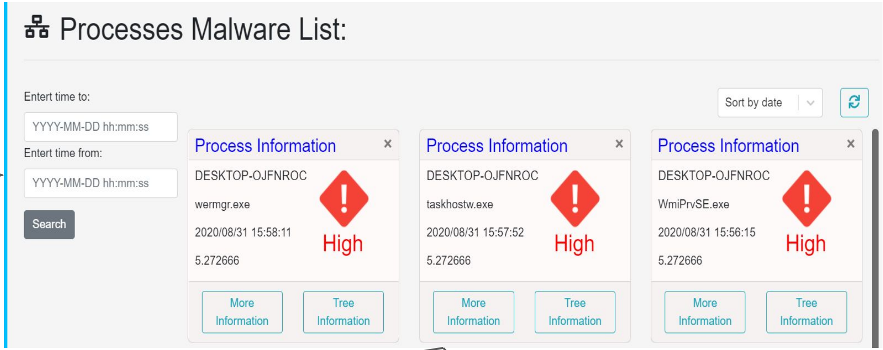
Line Charts



Web portal’s flow



Computers List:



Processes Malware List:

Entert time to: YYYY-MM-DD hh:mm:ss

Entert time from: YYYY-MM-DD hh:mm:ss

Process Information

DESKTOP-OJFNROC

wermgr.exe

2020/08/31 15:58:11

5.272666

High

Process Information

DESKTOP-OJFNROC

taskhostw.exe

2020/08/31 15:57:52

5.272666

High

Process Information

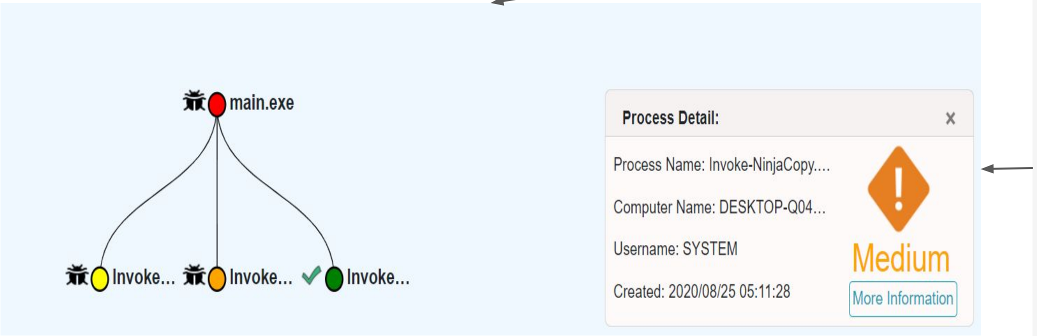
DESKTOP-OJFNROC

WmiPrvSE.exe

2020/08/31 15:56:15

5.272666

High



Process Detail:

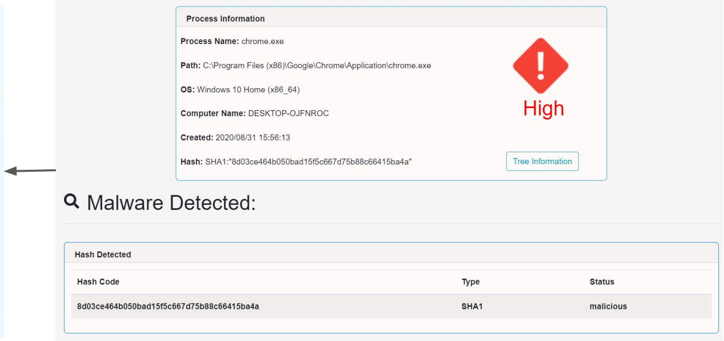
Process Name: Invoke-NinjaCopy....

Computer Name: DESKTOP-Q04...

Username: SYSTEM

Created: 2020/08/25 05:11:28

Medium



Process Information

Process Name: chrome.exe

Path: C:\Program Files (x86)\Google\Chrome\Application\chrome.exe

OS: Windows 10 Home (x86_64)

Computer Name: DESKTOP-OJFNROC

Created: 2020/08/31 15:56:13

Hash: SHA1:"8d03ce464b050bad15f5c667d75b88c66415ba4a"

High

Malware Detected:

Hash Detected

Hash Code	Type	Status
8d03ce464b050bad15f5c667d75b88c66415ba4a	SHA1	malicious

THANKS FOR LISTENING!

Demo and Q&A.