OFFSEC

www.offsec.ir

Modern SOC and cyber attacks on critical infrastructure

Hossein Lajevardi

Hossein@offsec.ir

[OFFSEC www.offsec.ir WhoAmI]

Hossein Lajevardi

- **Executive Director at Offsec**
- An InfoSec addict
- Threat Hunter and Red Teamer
- Research and Development of SIEM Solutions

hossein@OffSec.ir

@Ho_Lajevardi

lajevardi

"Hold the door!"

Hodor

Once a target, always a target...!

Over the past few years, cybersecurity has been moved from no effective education strategy to the mainstream area. Thus it is no time to rest. We must keep our eyes to the gate to protect our technological infrastructures.

Our purpose at the OFFSEC is to help Iran be a safer place to connect online.

OFFSEC

www.offsec.ir

-[Lessons from Attacks]-

Sophisticated State Actor

Australia on Monday (Feb 18) said
Cyber Security Centre officials "have also worked with **global anti-virus companies** to ensure Australia's friends and allies have the capacity to detect this malicious activity,"

- Many APT attackers know the network better than system admins
- Once inside the network, attackers generally don't need 0-days

-[Lessons from Attacks]-

Sophisticated State Actor

- The APT attacks condition and Iranian organizations as their targets
Example of Attack

An organization with 10,000 endpoints is estimated to see more than 660 attempted cyber attacks per day. according to report footprint (totaling approximately 15,000,000 global endpoints), this means there are, on average, 1 million attempted cyber attacks per day. (carbon black)
"Both Russia and China have used cyber operations in a bid to influence democratic votes."

-[EDR]-

Stop the Bad Actor

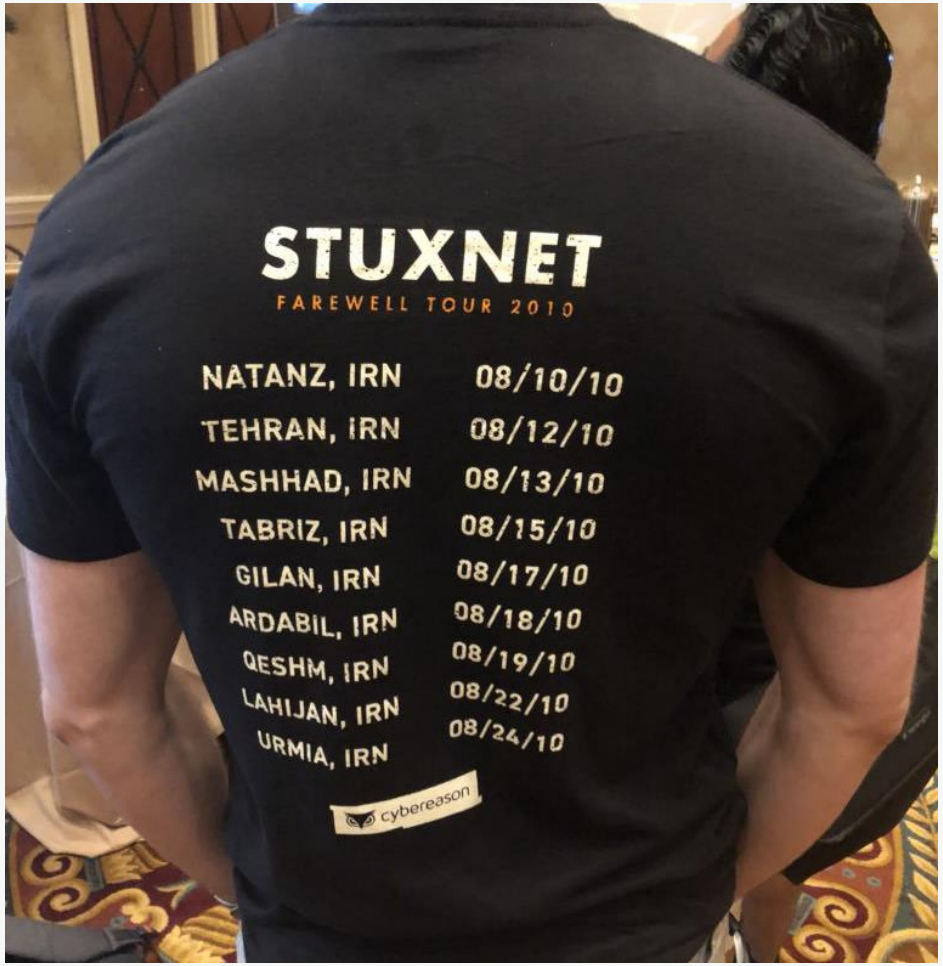
Don’ t Forget “ EDR tool isn’t going to replace your AV solution”

-[Farewell Tour 2019]-

Stop the Bad Guys

IRAN'S INFRASTRUCTURE UNDER ASSAULT

- Attackers rarely need 0-days
- Endpoint monitoring to detect lateral movement is more important than "stopping 0-days"



If you know the enemy and know yourself, you need not fear the result of a hundred battles.

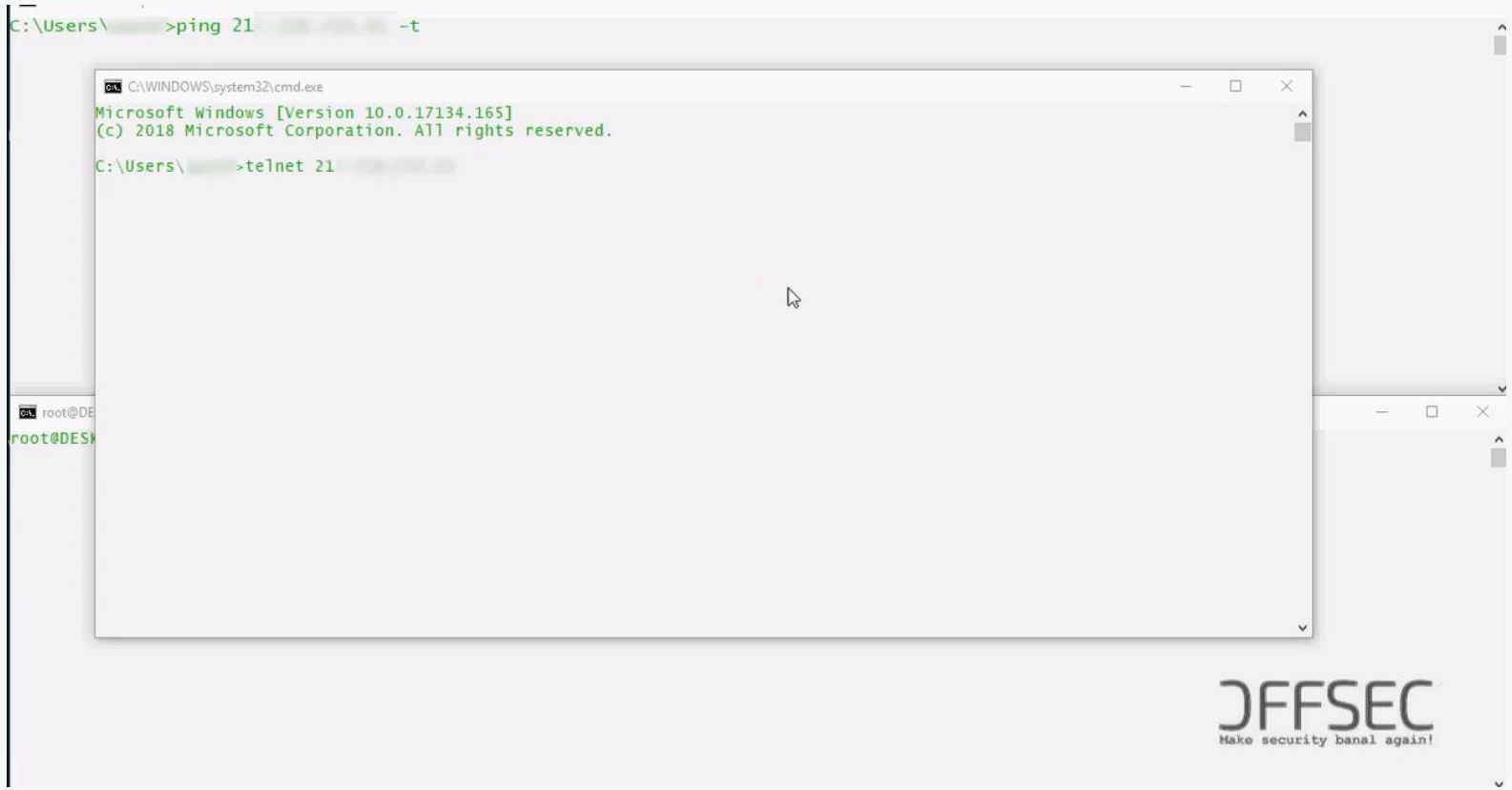
Cyber Security Needs more Security Vision

The Role of Human Error in Successful Cyber Attacks

"90 % of all cyber crime stems from some type of human error" (But in Iran? .... : |)

- demo about a successful infrastructure attack
- Benefits of Structure Asset Management framework
- Some Security Control on Internet-facing Assets

I've recently found a 0day vulnerability on Cisco devices (in this case, a video of a vulnerable governmental IP)



-[critical infrastructure]-

Cyber Security Needs more Security Vision

- Our infrastructure is more vulnerable than ever
- consider using automated solutions
- perform periodic (monthly) validation vulnerability scans.

why is it necessary to use the automated patch management?

The Art of Human Error in Cyber Attacks

- Less awareness into sub-points
- The ‘people’ factor is often ignored, yet it is a critical element in building a strong defense

let's see how an attacker can use
"lack of awareness " of the Network Administrator
and gain access from the Monitoring system and
find the Network Topology

No matter how good your security program is, you always need to make sure you have situational awareness.

Refrence : twitter.com/MalwareJake

Cyber Security Needs more Security Vision

let's see how an attacker can bypass ILO authentication

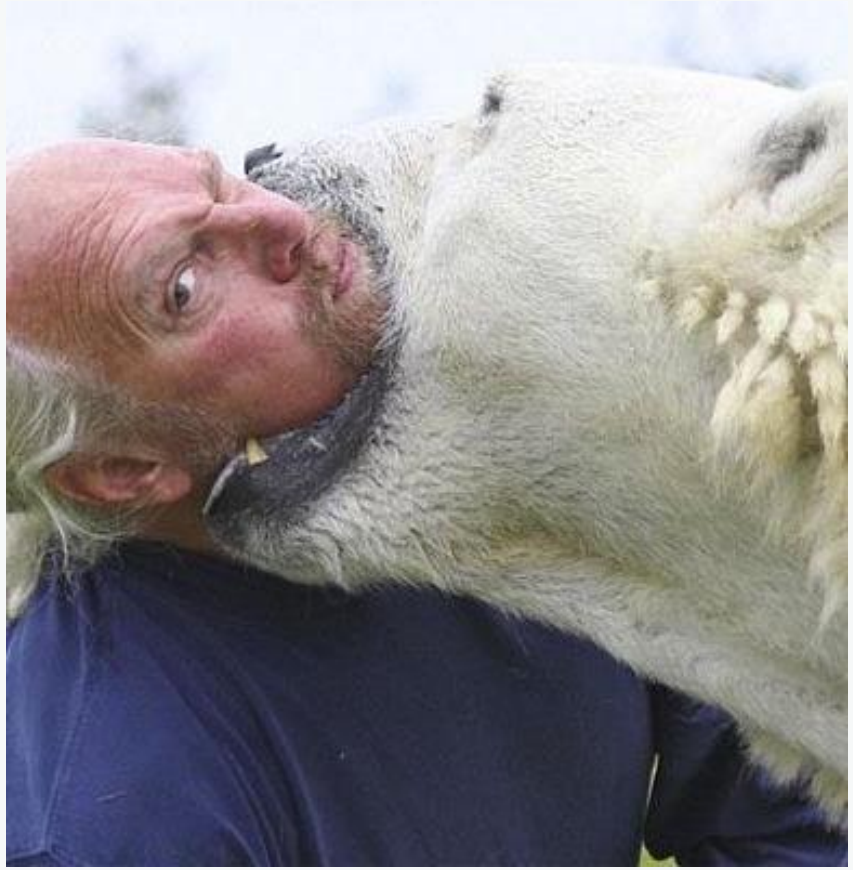
[+] Target is VULNERABLE!
[+] Account name: User Account Username: Administrator
[+] Account name: User Account Username: admins
[+] Account name: User Account Username: mohammadi
[+] Account name: User Account Username: OAtmp-Administrator-5C73B234
[+] Account name: User Account Username: Admin

- some important ILOs of Tehran universities are vulnerable
- Information Technology Company (ITC)
- and you can easily find the next target and its exploit

Strategies and Roadmaps (Successful Experience)

- Patched Infrastructure Could've Easily Reduced Losses
- Gaining Network Visibility
- Providing free tools and resources for governmental organizations (use development strategy)
- Develop a Vulnerability Assessment Plan
- Provide a comprehensive Security Training to all Staff

CIS® Center for Internet Security®



Log Management

Effective Log Management

Logging

- Collect information from different sources
- reliable factor
- Encryption
- Agent vs Agentless?

Management

- effective archiving system
- Log Retention Policy (outside of the log management)

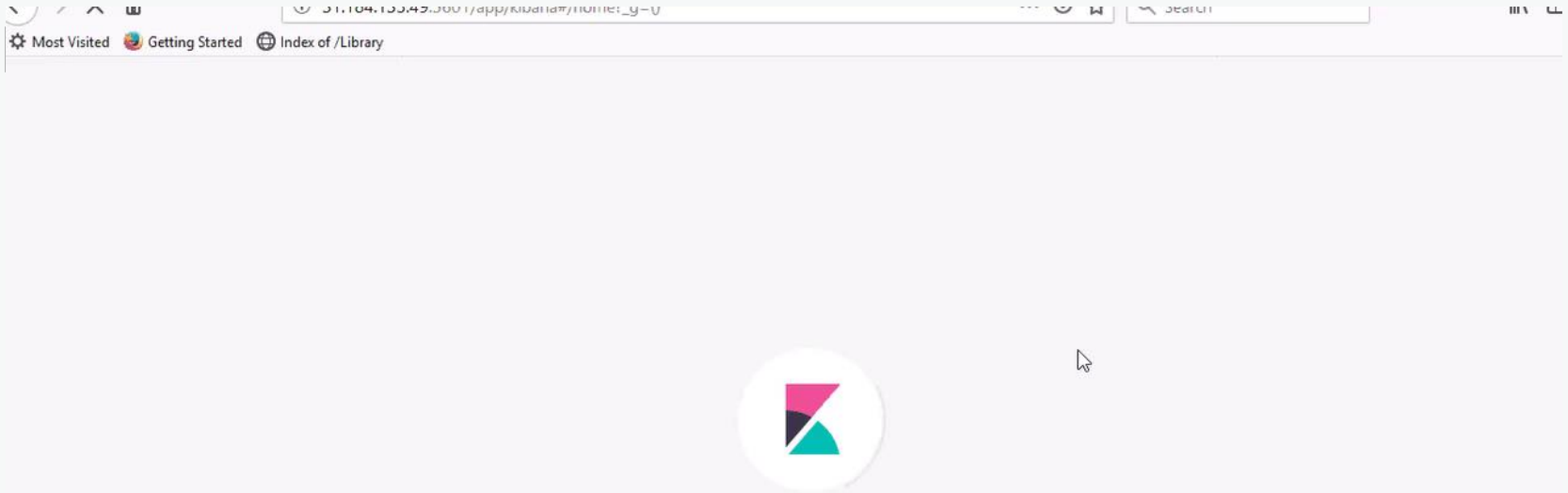
what are 3 ways of a successful implementation of Log management strategy?

elastic + logstash + kibana

graylog

solarwinds

Log Manageme



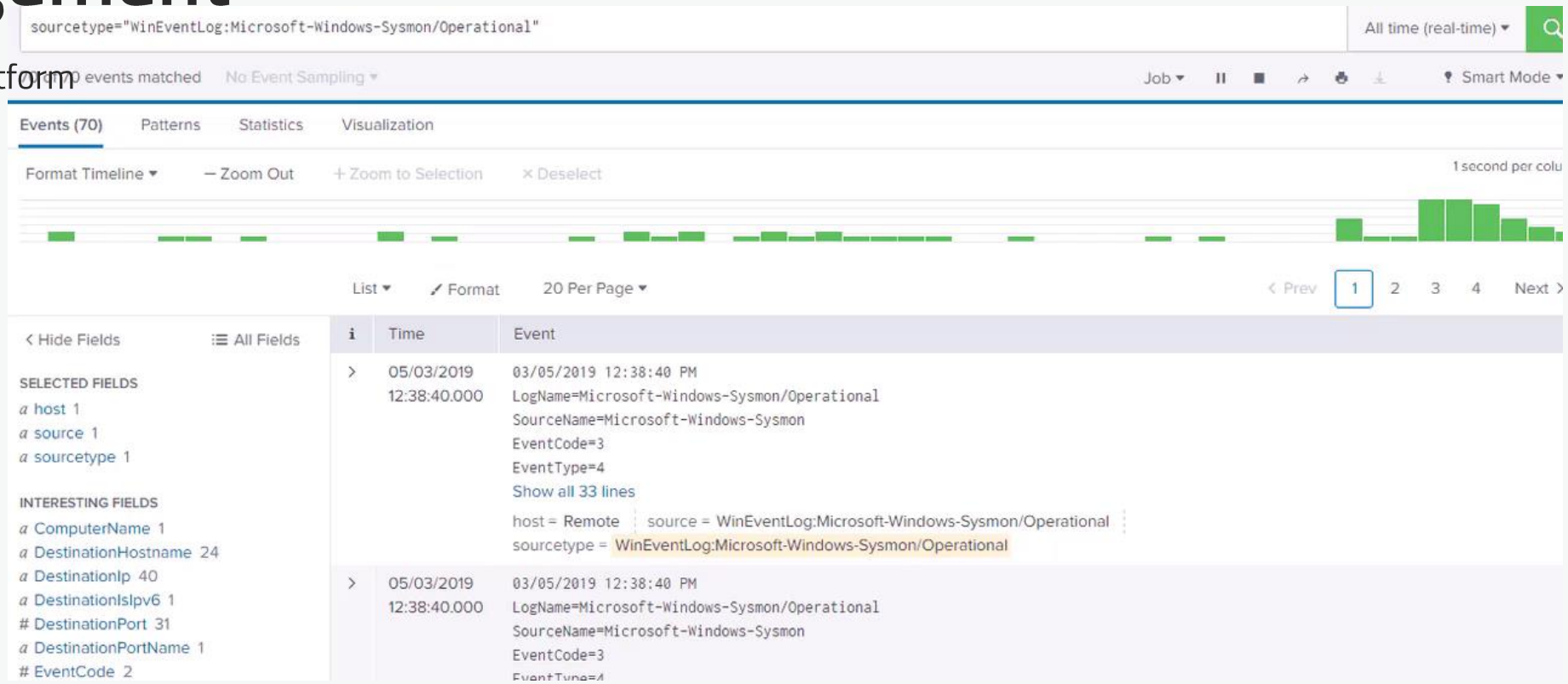
A common mistake in the implementation of log management

I'm using Splunk to show you "PowerShell is more than PowerShell.exe", But you don't have to use this product

Log Management

PowerShell as an Attack Platform

- PowerSploit
- EmpireProject
- RsRecon
- Powershell-C2



https://github.com/PowerShellMafia/PowerSploit

Not secure [redacted]9936/en-GB/app/search/search?q=search%20sourcetype%3D"WinEventLog%3AMicrosoft-Windows-Sysmon%2FOperati...

splunk>enterprise | App: Search & Reporting | Administrator | Messages | Settings | Activity | Help | Find

Search | Datasets | Reports | Alerts | Dashboards | Search & Reportin

New Search | Save As | Close

sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational" powershell

New Search

All time (real-time)

8 of 8 events matched | No Event Sampling | Job | Smart Mode

Events (8) | Patterns | Statistics | Visualization

Format Timeline | – Zoom Out | + Zoom to Selection | × Deselect | 1 second per colur

List | Format | 20 Per Page

< Hide Fields | All Fields

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a CommandLine 3

i	Time	Event
>	05/03/2019 12:53:13.000	... 18 lines omitted ... ProcessId: 9148 Image: C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe FileVersion: ? ... 3 lines omitted ... CommandLine: "C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2 CurrentDirectory: C:\WINDOWS\system32\

```
PS C:\>
PS C:\>
PS C:\>
PS C:\>
PS C:\> .\spoof.ps1
PS C:\> .\spoof.ps1
PS C:\> .\spoof.ps1
PS C:\>
```

Who needs customized malware?

splunk>enterprise App: Search ... Administrator Messages Settings Activity Help Find

Search Datasets Reports Alerts Dashboards Search & Reporting

New Search Save As Close

sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational" powershell All time (real-time)

2 of 2 events matched No Event Sampling Job Smart Mode

Events (2) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 10 milliseconds per column

List Format 20 Per Page

Hide Fields All Fields

SELECTED FIELDS

a host 1

a source 1

a sourcetype 1

INTERESTING FIELDS

i	Time	Event
>	05/03/2019 13:51:14.000	... 18 lines omitted ... ProcessId: 7460 Image: C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe FileVersion: ? ... 3 lines omitted ... CommandLine: "C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"

Select Windows PowerShell

```
PS C:\> .\Sample-Project.ps1
```

demo of real-time detection of a malicious PowerShell behavior

Recommendation....

JPCERTCC GitHub · SysmonSearch Wiki

https://github.com/JPCERTCC/SysmonSearch/wiki

The case study was conducted in the following environment:

Sysmon
ElasticSearch
Kibana
Winlogbeat

Windows Commands Abused by Attackers

In Windows OS, various commands (hereafter "Windows commands") are installed by default. However, what is actually used by general users is just a small part of it. On the other hand, JPCERT/CC has observed that attackers intruding into a network also use Windows commands in order to collect information and/or to spread malware infection within the network. What is worth noting here is the gap between those Window commands used by general users and by attackers. If there is a huge difference, it would be possible to detect or limit the attackers' behavior by monitoring/controlling the Windows command execution.
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html

JPCERT CC®
Japan Computer Emergency Response Team Coordination Center
JPCERT コーディネーションセンター

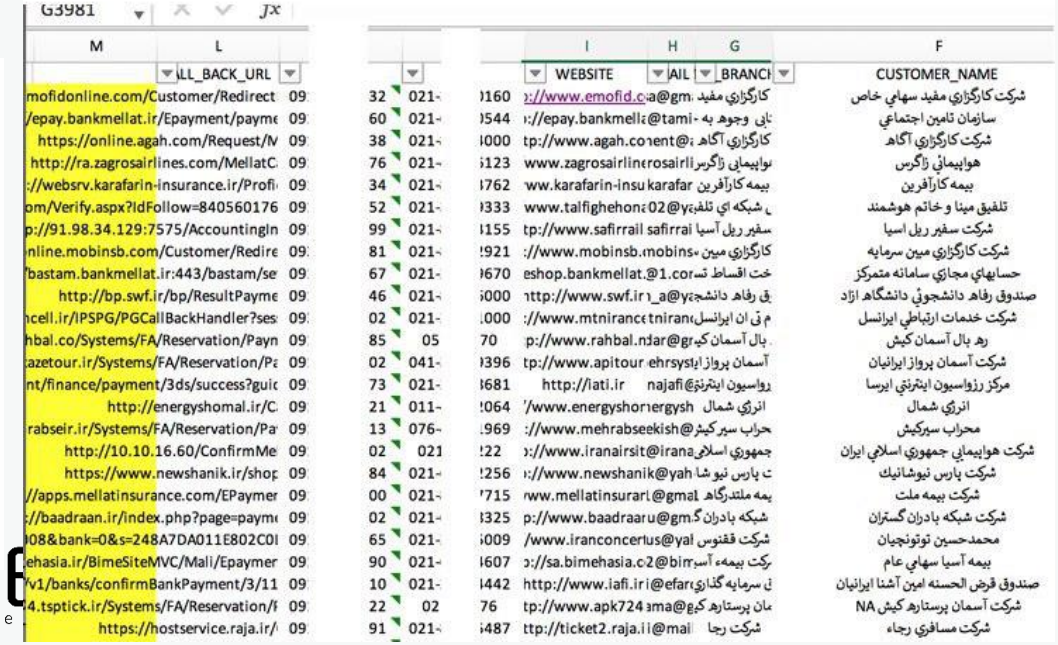
Ranking	Command	Times executed
1	tasklist	155
2	ver	95
3	ipconfig	76
4	systeminfo	40
5	net time	31
6	netstat	27
7	whoami	22
8	net start	16
9	qprocess	15
10	query	14

When the organization stands up a threat hunting program, but you don't have a SIEM, EDR, or even basic net flow. Then the boss says "why don't you just threat hunt with wireshark?"

Reference : twitter.com/MalwareJake

-[Data Breach]-

What We Can Do



What We Can Do

- solution or process that **identifies confidential data, tracks that data** as it moves through and out of the enterprise and **prevents unauthorized disclosure** of data by creating and enforcing disclosure policies

sample of a Governmental Data Leakage

What We Can Do

DLP primarily focuses on the following channels for preventing data loss:

- Endpoints
- Data in Motion
- Data at Rest

sample of a Governmental Data Leakage

Data Loss Prevention

DLP utilizes a combination of advanced technologies to accurately detect confidential data —whether it's at rest or in motion – and includes a variety of out-of-the-box policies (HIPAA, GDPR, PCI DSS, etc.) to help enable compliance with lower effort.

1. Vector Machine Learning (VML)
2. Sensitive Image Recognition (SIR)
3. Exact Data Matching (EDM)
4. Indexed Document Matching (IDM)
5. Described Content Matching (DCM)
6. Data Classification

let's see how a DLP solution can prevent data leakage (in 2 minutes)

Symantec Data Loss Prevention

https://192.168.1.181/ProtectManager/GetReport.do?reportID=2901&value(stat

Home | Incidents | Manage | System

Home > Exec. Summary - Endpoint

Administrator

Endpoint

Policy Summary

policy _Con ... (25 %) | policy _Con ... (41 %) | policy Con print_ Forbid den .. (4%)

Total	High	Med	Low	Info	Matches
119	119	0	0	0	331

Endpoint

Incidents - All

Jan 4, 2018 to Today

60 40 20 0 — 1/7/18 — 1/14/18

Total	High	Med	Low	Info	Matches
119	119	0	0	0	331

Incident		Matches
temp3.docx	1/20/18 9:53 AM	5
منع استفاده از برخی از سیستم عامل ها.docx	1/20/18 9:50 AM	5
New Microsoft Word Document.docx	1/8/18 9:41 AM	5
New Microsoft Word Document.docx	1/8/18 9:40 AM	5
http://clients1.google.com/ocsp	1/7/18 12:12 PM	1
[redacted].docx	1/7/18 11:43 AM	4
http://clients1.google.com/ocsp	1/7/18 11:41 AM	1
27.docx	1/7/18 11:18 AM	8
28.docx	1/7/18 11:13 AM	8
9A375E0F.xlsx	1/7/18 11:07 AM	22

Endpoint

Incident Status Summary

New (100%)

Total	High	Med	Low	Info	Matches
119	119	0	0	0	331

Endpoint

Highest Offenders

Total	High	Med	Low	Info	Matches
119	119	0	0	0	331

User Name	All	High	Matches
[redacted]	74	74	225
[redacted]	41	41	98
[redacted]	4	4	8

OFFSEC Make security banal again!

The rule's about SOAR

- **Security Orchestration, Automation and Response (SOAR)**
  - What exactly is SOAR?
  - Why you need ?

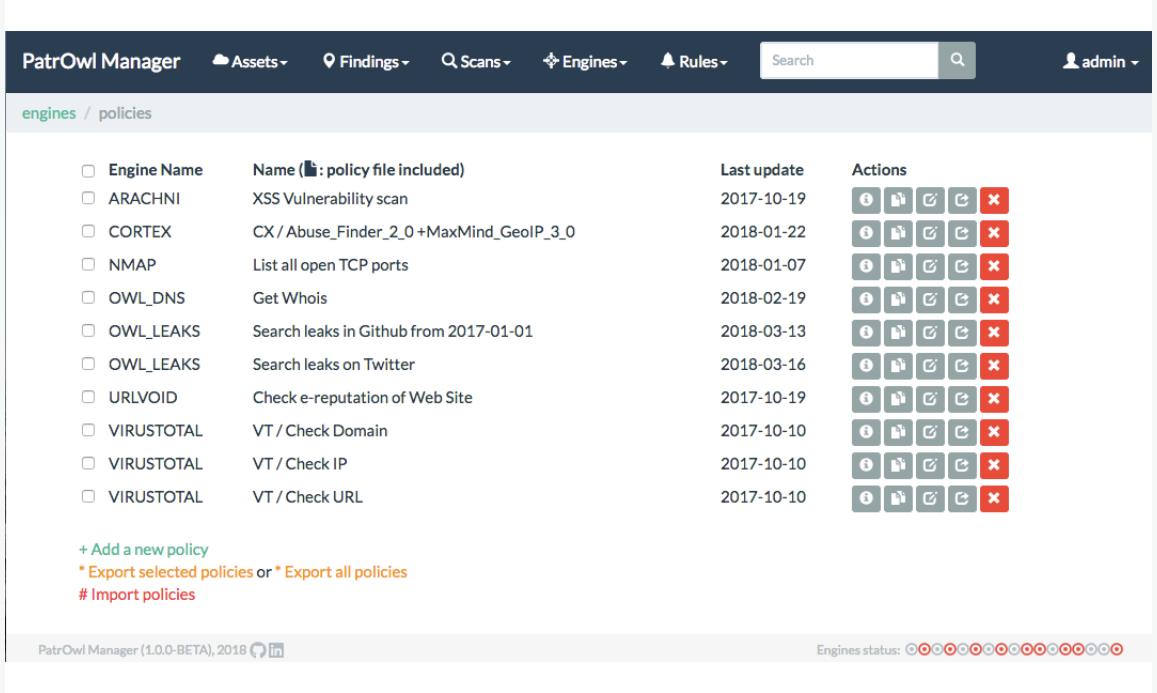
- Gartner has defined three logical groups for the different values of a SOAR solution (Ahlm, 2018):
  1. Create a better investigative platform
  2. Enhance SIEM management
  3. Optimize security team and program management

- common set of challenges
- increasing number of security tools
- Feeling Overwhelmed
- Competitive Analysis

-[SOAR in 2019]-

The rule's about SOAR

- Path to Automated Security Operation
  1. Purchasing a pre-configured offering
  2. Building out your own from "Scratch" , But how?



splunk> phantom

A useful roadmap for SOAR?

CIRCL MISP Threat Sharing

HiVE Sweet Social Impact

PatrOwl Continuous Threat Management

OFFSEC www.offsec.ir

Thanks to Ahmad Madadi

Hossein@offsec.ir

Resource :
https://www.symantec.com
https://www.gartner.com/en