Cyber Threat Intelligence (CTI): Tools and Applications

A session at the Nigeria Computer Society Cybersecurity Forum and Workshop 2.0

June, 2022

Hamzat Lateef – Security Engineering Lead, CyberPlural

Outline

- What is Cyber Threat Intelligence
- Why is Cyber Threat Intelligence important?
- Who Benefit from Cyber Threat Intelligence
- Cyber Threat Intelligence Life Cycle
- Cyber Threat Intelligence Use cases
- Type of Cyber Threat Intelligence
- Cyber Threat Intelligence Tools
- Application of Cyber Threat Intelligence
- Questions & Answers

What is Cyber Threat Intelligence?

Cyber Threat intelligence is data that is collected, processed, and analyzed to understand a threat actor's motives, targets, and attack behaviors.

Threat intelligence enables us to make faster, more informed, data-backed security decisions and change their behavior from reactive to proactive in the fight against threat actors

Threat intelligence is evidence-based knowledge (e.g., context, mechanisms, indicators, implications and action-oriented advice) about existing or emerging menaces or hazards to assets. – Gartner

Why is Cyber Threat Intelligence important?

In the world of cybersecurity, advanced persistent threats (APTs) and defenders are constantly trying to outmaneuver each other.

Data on a threat actor’s next move is crucial to proactively tailoring your defenses and preempt future attacks.

Organizations are increasingly recognizing the value of threat intelligence, with 72 percent planning to increase threat intelligence spending in upcoming quarters.

Most organizations today are focusing their efforts on only the most basic use cases.

- sheds light on the unknown, enabling security teams to make better decisions
- empowers cyber security stakeholders by revealing adversarial motives and their tactics, techniques, and procedures (TTPs)
- helps security professionals better understand the threat actor’s decision-making process
- empowers business stakeholders, such as executive boards, CISOs, CIOs and CTOs; to invest wisely, mitigate risk, become more efficient and make faster decisions

Who Benefit from Cyber Threat Intelligence?

Threat intelligence benefits organizations of all shapes and sizes by helping process threat data to better understand their attackers, respond faster to incidents, and proactively get ahead of a threat actor's next move

From top to bottom, threat intelligence offers unique advantages to every member of a security team

- Sec/IT Analyst
- SOC
- CSIRT / CERT
- Intel Analyst
- Executive Management

Sec/IT Analyst

Optimize prevention and detection capabilities and strengthen defenses

SOC

Prioritize incidents based on risk and impact to the organization

CSIRT /CERT

Accelerate incident investigations, management, and prioritization

Intel Analyst

Uncover and track threat actors targeting the organization

Executive Management

Understand the risks the organization faces and what the options are to address their impact

Cyber Threat Intelligence Life Cycle

The intelligence lifecycle is a process to transform raw data into finished intelligence for decision making and action. You will see many slightly different versions of the intelligence cycle in your research, but the goal is the same, to guide a cybersecurity team through the development and execution of an effective threat intelligence program.

This cycle consists of six steps resulting in a feedback loop to encourage continuous improvement

1 Requirements

2 Collection

3 Processing

4 Analysis

5 Dissemination

6 Feedback

Cyber Threat Intelligence Use cases

- Use TI to enrich alerts - Link alerts together into incidents - Tune newly deployed security controls	**SOC**
- Integrate TI feeds with other security products - Block bad IPs, URLS, domains, files etc.	**Sec/IT Analyst**
- Look wider and deeper for intrusion evidence - Review reports on threat actors to better detect them	**Intel Analyst**
- Look for information on the who/what/why/when/how of an incident - Analyze root cause to determine scope of the incident	**CSIRT /CERT**
- Assess overall threat level for the organization - Develop security roadmap	**Executive Management**

Cyber Threat Intelligence Types

Tactical

- Threat Feeds
- Real Time Alerts
- Automated Malware Analysis
- Threat Monitoring

Tactical intelligence is focused on the immediate future, is technical in nature, and identifies simple indicators of compromise (IOCs).

Operational

- Patch Prioritization
- Incident Response
- Operational Intelligence Reporting
- Actor Profiling

Strategic intelligence shows how global events, foreign policies, and other long-term local and international movements can potentially impact the cyber security of an organization.

Strategic

- Strategic Intelligence Reporting
- Campaign Tracking
- Insider Threat
- Threat Research
- Deception Operations.

These factors provide context, and context provides insight into how adversaries plan, conduct, and sustain campaigns and major operations

Cyber Threat Intelligence Tools & Application

2 Collection

OSINT +

DarkWeb +

Community Feeds+

Private Feeds +

Internal Networks

3 Processing

4 Analysis

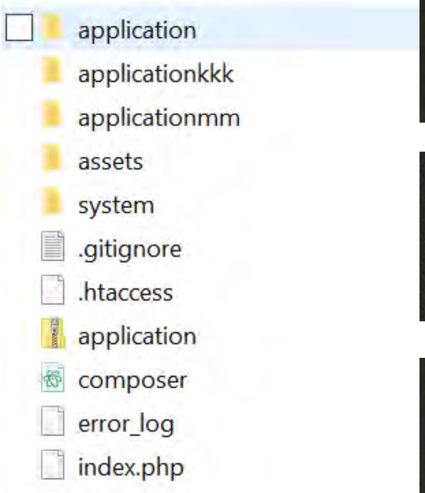
5 Dissemination

6 Feedback

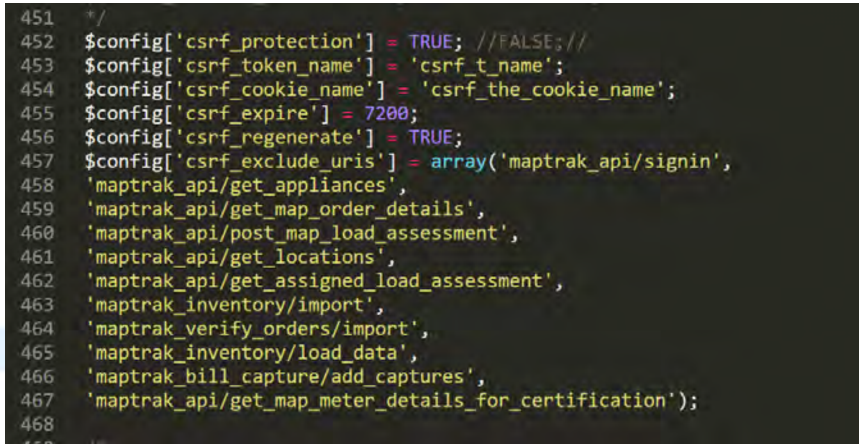
Use cases & Lab Session

Threat Intelligence Revealing Exposition of Sensitive Application Detail of a Utility Company

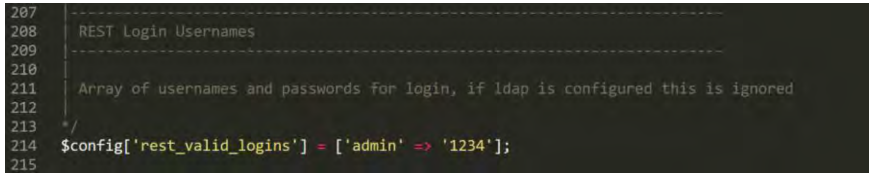
Confidentiality & Integrity



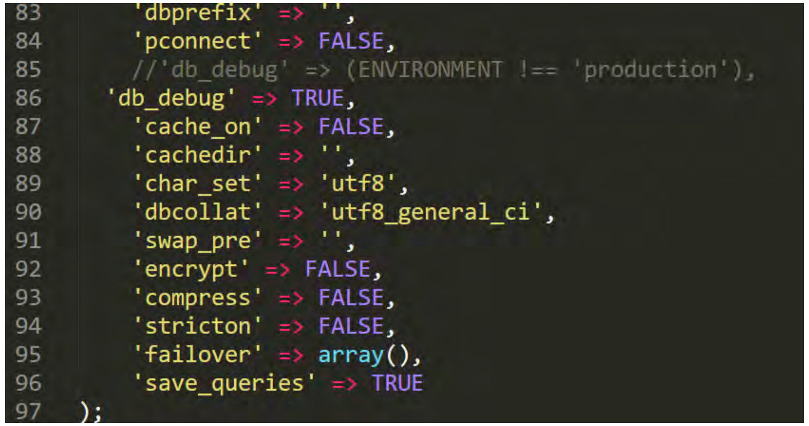
```
application
applicationkkk
applicationmm
assets
system
.gitignore
.htaccess
application
composer
error_log
index.php
```



```
*/
$config['csrf_protection'] = TRUE; //FALSE;//
$config['csrf_token_name'] = 'csrf_t_name';
$config['csrf_cookie_name'] = 'csrf_the_cookie_name';
$config['csrf_expire'] = 7200;
$config['csrf_regenerate'] = TRUE;
$config['csrf_exclude_uris'] = array('maptrak_api/signin',
'maptrak_api/get_appliances',
'maptrak_api/get_map_order_details',
'maptrak_api/post_map_load_assessment',
'maptrak_api/get_locations',
'maptrak_api/get_assigned_load_assessment',
'maptrak_inventory/import',
'maptrak_verify_orders/import',
'maptrak_inventory/load_data',
'maptrak_bill_capture/add_captures',
'maptrak_api/get_map_meter_details_for_certification');
```



```
|--------------------------------------------------------------------------
| REST Login Usernames
|--------------------------------------------------------------------------
|
| Array of usernames and passwords for login, if ldap is configured this is ignored
|
*/
$config['rest_valid_logins'] = ['admin' => '1234'];
```

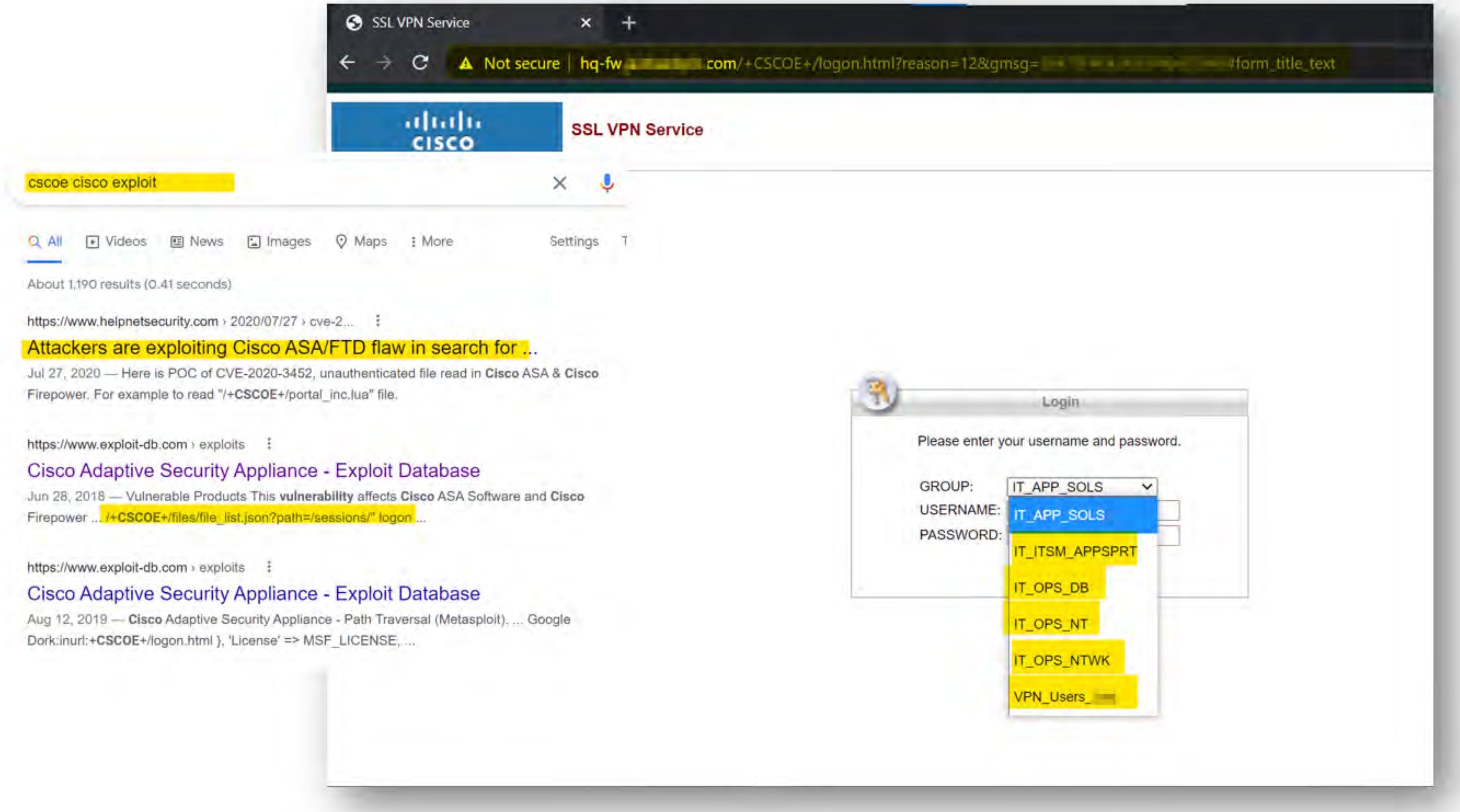


```
     'dbprefix' => '',
     'pconnect' => FALSE,
     //'db_debug' => (ENVIRONMENT !== 'production'),
    'db_debug' => TRUE,
     'cache_on' => FALSE,
     'cachedir' => '',
     'char_set' => 'utf8',
     'dbcollat' => 'utf8_general_ci',
     'swap_pre' => '',
     'encrypt' => FALSE,
     'compress' => FALSE,
     'stricton' => FALSE,
     'failover' => array(),
     'save_queries' => TRUE
);
```

Information Gathering on a financial focus organization –

Keeping Proactive with surface exposure.

Confidentiality & Integrity



⚠ Not secure | hq-fw[redacted]com/+CSCOE+/logon.html?reason=12&gmsg=[redacted]#form_title_text

SSL VPN Service

cscoe cisco exploit

About 1,190 results (0.41 seconds)

https://www.helpnetsecurity.com › 2020/07/27 › cve-2...

Attackers are exploiting Cisco ASA/FTD flaw in search for ...

Jul 27, 2020 — Here is POC of CVE-2020-3452, unauthenticated file read in **Cisco** ASA & **Cisco** Firepower. For example to read "/+**CSCOE**+/portal_inc.lua" file.

https://www.exploit-db.com › exploits

Cisco Adaptive Security Appliance - Exploit Database

Jun 28, 2018 — Vulnerable Products This **vulnerability** affects **Cisco** ASA Software and **Cisco** Firepower ... /+**CSCOE**+/files/file_list.json?path=/sessions/" logon ...

https://www.exploit-db.com › exploits

Cisco Adaptive Security Appliance - Exploit Database

Aug 12, 2019 — **Cisco** Adaptive Security Appliance - Path Traversal (Metasploit). ... Google Dork:inurl:+**CSCOE**+/logon.html }, 'License' => MSF_LICENSE, ...

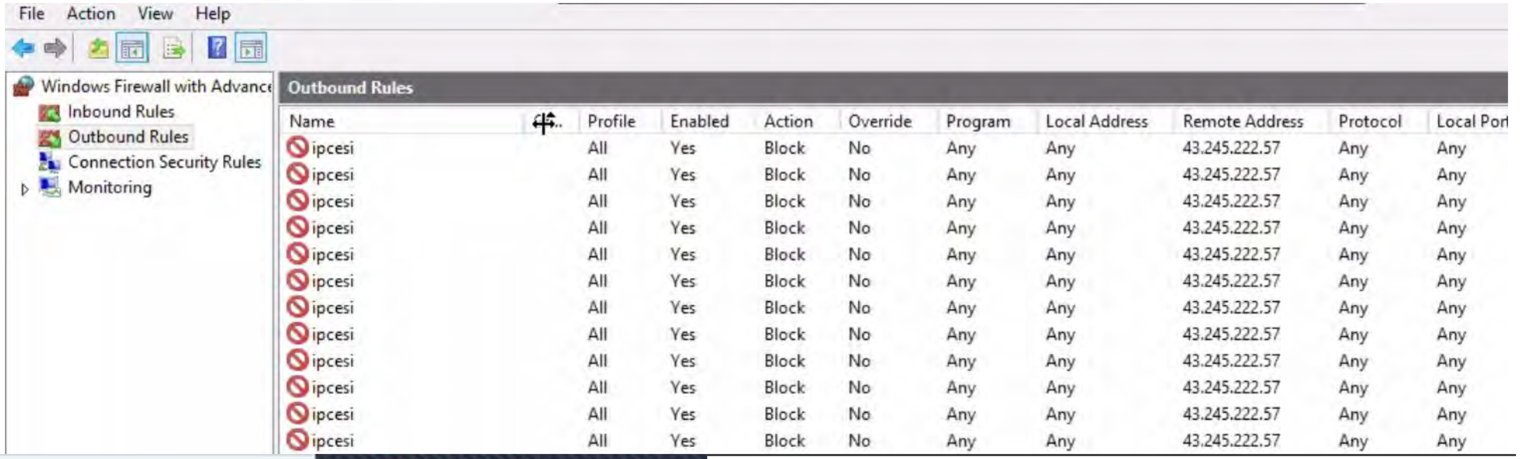
Please enter your username and password.

GROUP: IT_APP_SOLS
USERNAME:
PASSWORD:

IT_APP_SOLS
IT_ITSM_APPSPRT
IT_OPS_DB
IT_OPS_NT
IT_OPS_NTWK
VPN_Users_[redacted]

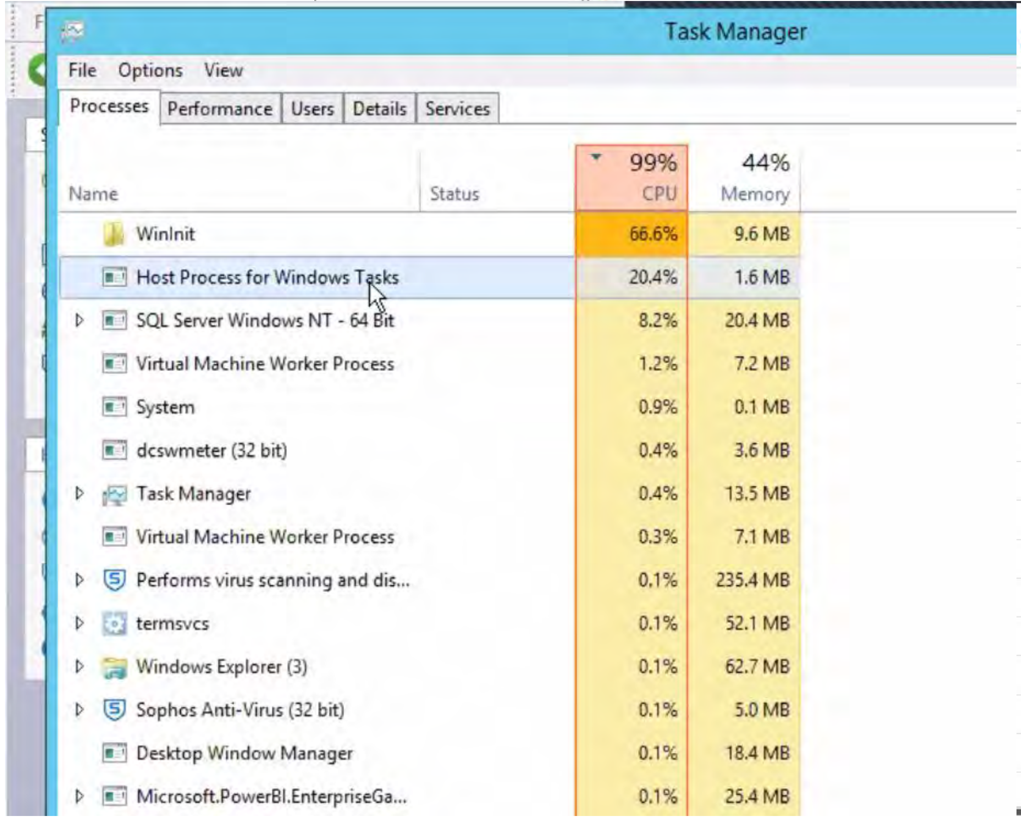
Cryptominer Infections / Credential Dumping Incident at a Utility Company.

Confidentiality, Integrity and Availability

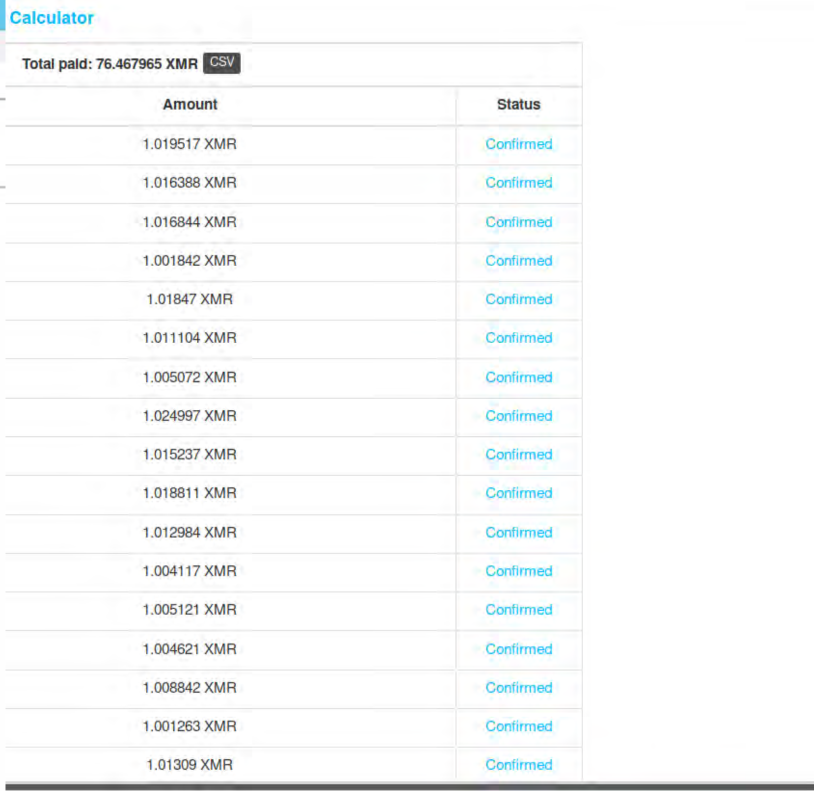


Outbound Rules

Name		Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol	Local Port
ipcesi		All	Yes	Block	No	Any	Any	43.245.222.57	Any	Any
ipcesi		All	Yes	Block	No	Any	Any	43.245.222.57	Any	Any
ipcesi		All	Yes	Block	No	Any	Any	43.245.222.57	Any	Any
ipcesi		All	Yes	Block	No	Any	Any	43.245.222.57	Any	Any
ipcesi		All	Yes	Block	No	Any	Any	43.245.222.57	Any	Any
ipcesi		All	Yes	Block	No	Any	Any	43.245.222.57	Any	Any
ipcesi		All	Yes	Block	No	Any	Any	43.245.222.57	Any	Any
ipcesi		All	Yes	Block	No	Any	Any	43.245.222.57	Any	Any
ipcesi		All	Yes	Block	No	Any	Any	43.245.222.57	Any	Any
ipcesi		All	Yes	Block	No	Any	Any	43.245.222.57	Any	Any
ipcesi		All	Yes	Block	No	Any	Any	43.245.222.57	Any	Any
ipcesi		All	Yes	Block	No	Any	Any	43.245.222.57	Any	Any



Name	Status	99% CPU	44% Memory
WinInit		66.6%	9.6 MB
Host Process for Windows Tasks		20.4%	1.6 MB
SQL Server Windows NT - 64 Bit		8.2%	20.4 MB
Virtual Machine Worker Process		1.2%	7.2 MB
System		0.9%	0.1 MB
dcswmeter (32 bit)		0.4%	3.6 MB
Task Manager		0.4%	13.5 MB
Virtual Machine Worker Process		0.3%	7.1 MB
Performs virus scanning and dis...		0.1%	235.4 MB
termsvcs		0.1%	52.1 MB
Windows Explorer (3)		0.1%	62.7 MB
Sophos Anti-Virus (32 bit)		0.1%	5.0 MB
Desktop Window Manager		0.1%	18.4 MB
Microsoft.PowerBI.EnterpriseGa...		0.1%	25.4 MB



Total paid: 76.467965 XMR

Amount	Status
1.019517 XMR	Confirmed
1.016388 XMR	Confirmed
1.016844 XMR	Confirmed
1.001842 XMR	Confirmed
1.01847 XMR	Confirmed
1.011104 XMR	Confirmed
1.005072 XMR	Confirmed
1.024997 XMR	Confirmed
1.015237 XMR	Confirmed
1.018811 XMR	Confirmed
1.012984 XMR	Confirmed
1.004117 XMR	Confirmed
1.005121 XMR	Confirmed
1.004621 XMR	Confirmed
1.008842 XMR	Confirmed
1.001263 XMR	Confirmed
1.01309 XMR	Confirmed

Questions & Answers

thank you

✌

follow on LinkedIn