CYBOT™

Automated Investigation & Hunting Platform

Datasheet

CYBOT™ Threat Intelligence

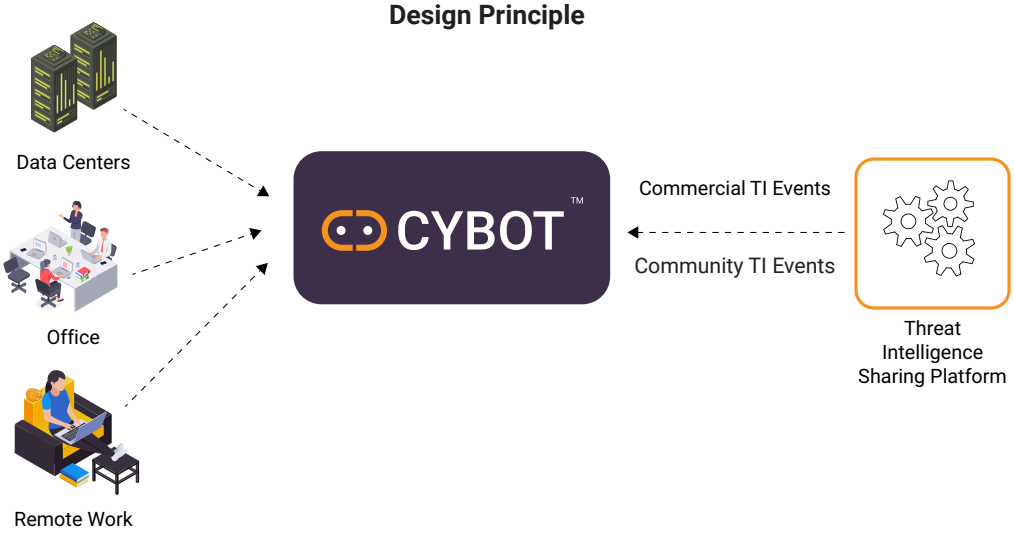
activebytes innovations

www.active-bytes.com

About the CYBOT™

- CYBOT™ collects raw logs from enterprise network, remote users, servers and stores to its Analytical engine in a contextualized & secured way. The logs then undergoes intelligent automatic analysis, thereby going the extra mile in threat hunting which, a human cannot.
- CYBOT™ is designed to be Adaptive to latest adversary techniques & tactics by keeping in track with the Threat Intelligence events that it is programmed to receive from our trusted community sources and Activebytes dedicated threat intelligence team.
- CYBOT™ intelligently & automatically hunts and investigate the threat leveraging Realtime Logs by performing correlation with TI IOCs received from even the dark sources, thereby detecting adversary attack patterns that a human can never pickup.
- Around the clock monitoring of logs & every unusual, suspected events is subjected to drill down level of investigation and is designed to provide automated options to respond along with suggestions and alerts to security team. This will help analysts to deal with the adversaries that already intruded the network

Design Principle



Why CYBOT™ is Your Automated Adaptive Threat Hunting Solution ?

CYBOT™ Threat Intelligence

CYBOT™ has a Threat Intelligence Platform which continuously gets updated with knowledge of latest cyber security threats in the industry worldwide. The inputted Information from both commercial and community threat intelligence events, news and vulnerabilities is accessible in CYBOT™ platform to both technical and non-technical teams in the form of user-friendly dashboards, printouts and emails . This provides analysts and incident responders with effective intelligence. CYBOT™ is designed to avoid repeated investigation on identical observables including IOCs and patterns , thereby reducing false-positives and noise to the analysts. We extend our security specialist's hands for threat intelligence services like domain take down.

CYBOT™ -Threat Intelligence

CYBOT™ transforms raw feeds from various commercial and community sources into useful intelligence. The value-added analyzed and contextualized intelligence feeds from Activebytes innovations is also inputted to the platform. This effective intelligence gives and extra edge to security team about the latest adversary techniques & tactic, sector targeted ,threat landscape etc. that takes place in world. The huge pool of relevant intelligence feeds helps CYBOT™ in early detection of hidden, un-known, and emerging threats and this helps the analysts to quickly defend & secure their environment.

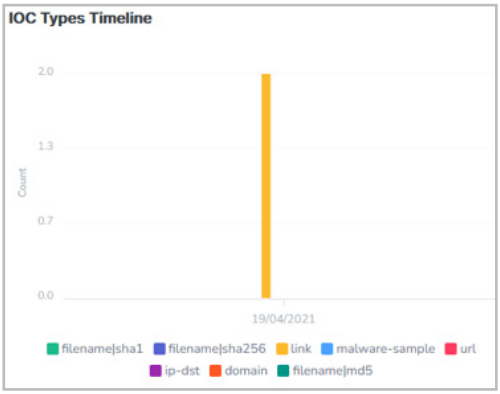
CYBOT™ protects your infrastructure from even the darkest corners

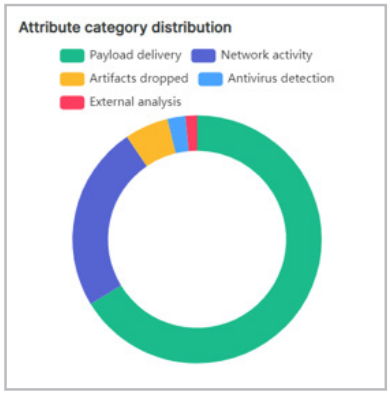
Threat intelligence feeds from various open source and dark web sources makes the CYBOT™ platform adaptive & efficient in detecting threat that escaped your defense system

No Malicious executions go undetected with TIP

With intelligence sharing, the latest technique adversary executions are fed to CYBOT™ and hence can perform faster malicious IP detection, Domain ,Hash detection etc

User friendly technical & non-technical management summary reports generated with option to download and set notifications



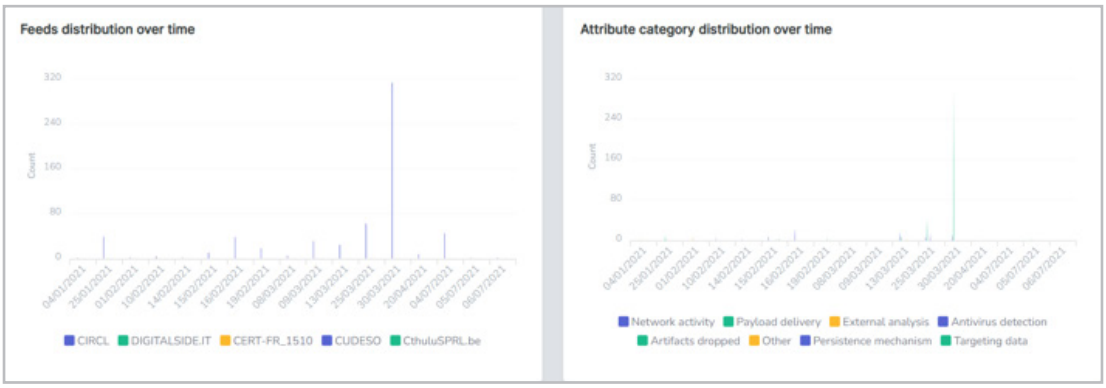


Some other features includes

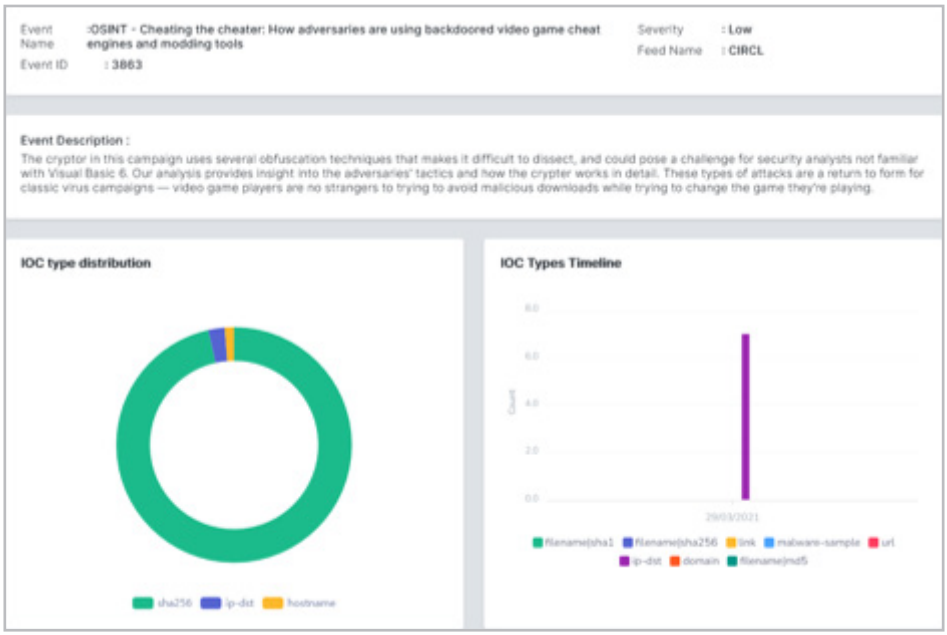
- Receiving and Sharing threat intelligence information in a controlled ,contextualized and structured manner benefiting the enterprise
- Receiving threat intelligence information from various open source, dark web sources and this makes the CYBOT™ intelligent and adaptive to latest attack trends.
- Receive latest emerging threat intelligence information from commercial sources as well
- CYBOT™ is Pre- configured to receive threat intelligence data from multiple sources & contextualize the data for effective correlation with observables in enterprise environment
- Role based access control and can be managed in settings option in platform
- Record all type of IOCs including IP, URLs, text, files, hashes, IDS signatures etc. and hence even manually undetectable threats don't escape the investigation
- Allows internal team to collaborate and discuss on security & vulnerability intelligence events and this benefits the whole team with knowledge of latest attacks and ways to defend from the same
- Allows organization to share threat intelligence information with peers effectively
- No restrictions with number of users and new users can be easily added by the admin
- 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 on Malware Information, Threat Intelligence News, Vulnerability and exploits information makes CYBOT™s resource pool rich with latest adversary factor

Sample Community Threat Intelligence Events

Capable to securely gather, share, store and correlate IoC's of targeted attacks, vulnerability information etc. This makes the automated hunt faster & efficient



Detailed information on each intelligence events, thereby providing the analysts and management insight on emerging threats. This will also help to decide the changes to be made in your present security defense framework. The print button can be used to get the details printed



Every IOC is listed in indicators table with in-depth information ,making the latest events resourceful for analysts

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

Sample Activebytes Threat Intelligence Events

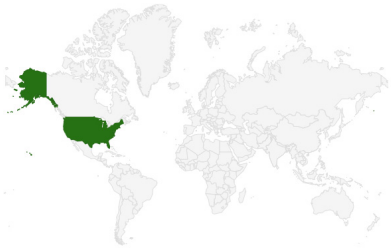
The time distribution gives insight into the adversary attack, vulnerability that trends during a particular time in the world, thereby providing idea for changes required in defense system

The Impact region helps you to understand the threat landscape and the degree of impact ,a particular attack has caused.

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

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

Impact Region



Expert analysis and comments on security intelligence & vulnerability intelligence is very important for any security team to update their own IT infrastructure security accordingly

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.

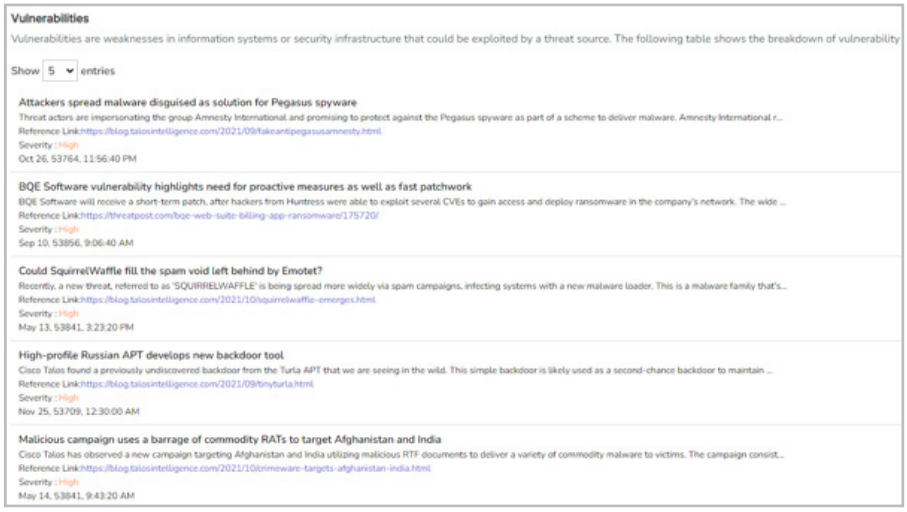
A key issue many private firms to cooperate with law enforcement is the lack of feedback or visibility of how their cases are progressing. While this lack of sharing back by law enforcement is understandable due to operational and investigative issues, it can be frustrating for private firms to see little 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.

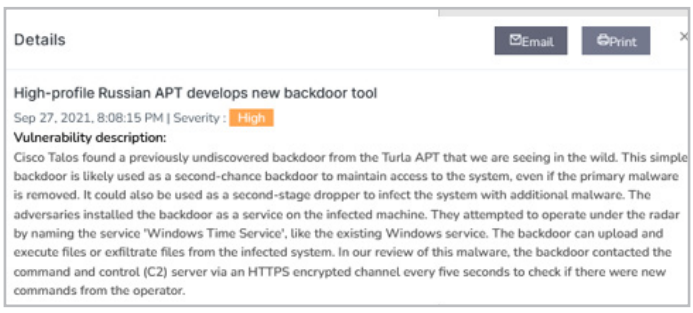
Business is anxious to remediate attacks while law enforcement wants to preserve evidence. These motives are often at odds.

Reference Link

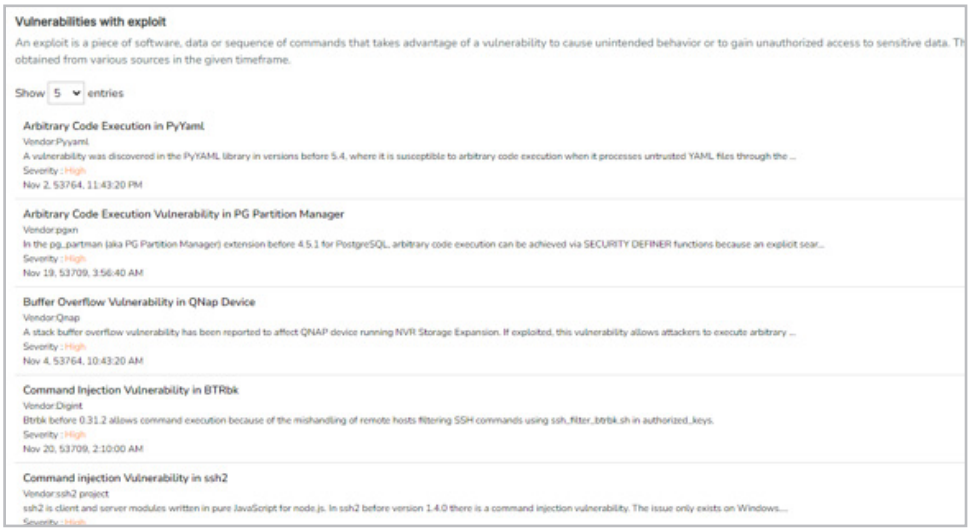
- https://www.scmagazine.com/analysis/cybercrime/doj-wants-to-know-what-are-the-impediments-to-working-with-law-enforcement
- https://www.nextgov.com/cybersecurity/2021/10/justice-official-dangles-liability-protections-encourage-private-sector-breach-reports/186253/

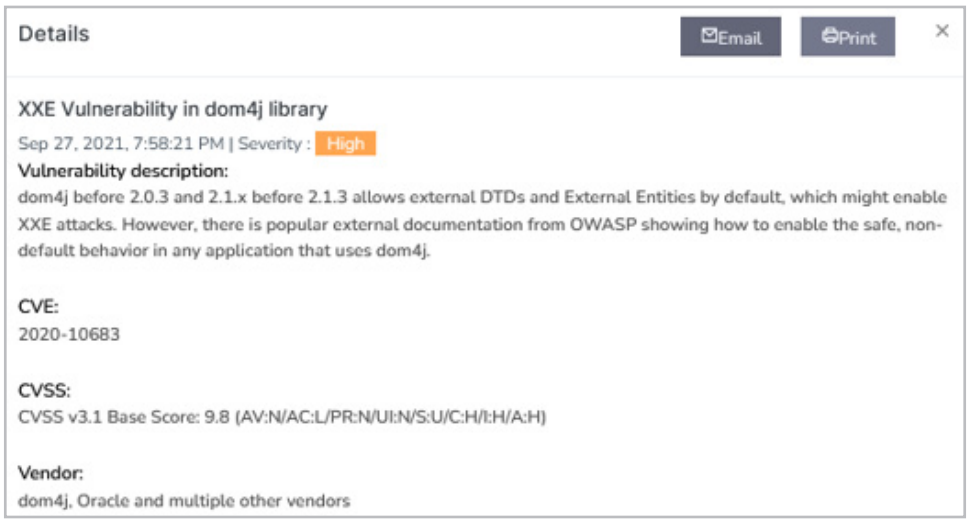
Any vulnerabilities in your environment can lead to a security breach and getting updates about the same for enterprise benefit is an added advantage

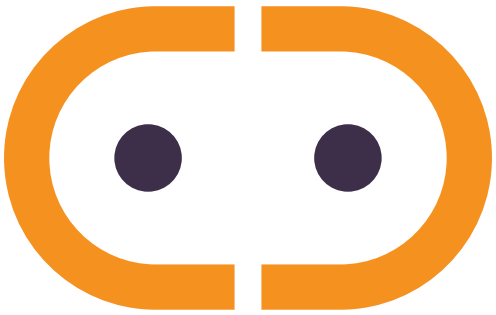




Vulnerabilities and exploits are crucial information's to security teams, since these need to be given extra focus during patch management







activebytes
innovations

www.active-bytes.com / contact@active-bytes.com
+971 50 513 3973