CYBOT HUNTER

Data Sheet

Host & Network Sensors

activebytes
innovations
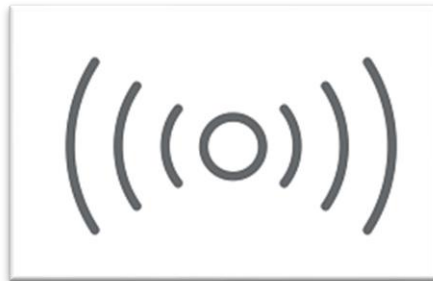
- ✓ Rich Data extraction from all major Operating systems
- ✓ Capable of extracting system behaviour, system communications form and to other systems, system communication to external ip addresses, common user behaviour
- ✓ Capable of extracting logs about execution operating system binaries
- ✓ Capable of extracting changes in registry of the Microsoft Windows operating system

HOST SENSOR

Settings

Type	Operating System
Event Collection	Windows

Events

- ☑ DLL and Driver Load
- ☑ DNS
- ☐ File
- ☑ Network
- ☑ Process
- ☑ Registry
- ☑ Security

Type	Operating System
Event Collection	Mac

Events

- ☐ File
- ☑ Process
- ☑ Network

Type	Operating System
Event Collection	Linux

Events

- ☐ File
- ☑ Process
- ☑ Network

✓ Capable of extracting all file creation, deletion modification activities inside the host

Files Created: Details of files created

	Created
	493,110

User Name	Host Name	File Name	File Path	Count
systemd-network	ip-172-31-4-115	.#2QF0oHb	/run/systemd/netif/links/.#2QF0oHb	1
systemd-network	ip-172-31-4-115	.#2XfMPZb	/run/systemd/netif/links/.#2XfMPZb	1
systemd-network	ip-172-31-4-115	.#2j4alAd	/run/systemd/netif/leases/.#2j4alAd	1
systemd-network	ip-172-31-4-115	.#2zdnagd	/run/systemd/netif/leases/.#2zdnagd	1
systemd-network	ip-172-31-4-115	.#state1LZwQd	/run/systemd/netif/.#state1LZwQd	1
systemd-network	ip-172-31-4-115	.#state6FEWjc	/run/systemd/netif/.#state6FEWjc	1
systemd-resolve	ip-172-31-4-115	.#resolv.confT5VHCl	/run/systemd/resolve/.#resolv.confT5VHCl	1

‹ 1 ... 204 205 206 207 **208** ›

Files Deleted : Details of files deleted

	Deleted
	372,256

User Names	Host Names	File Names	File Path	Count
Administrator	WIN-SRH715DO5HR	API-MS-Win-core-string...	C:\Users\ADMINI~1\AppData\Local\Temp\...	1
Administrator	WIN-SRH715DO5HR	API-MS-Win-core-string...	C:\Users\ADMINI~1\AppData\Local\Temp\...	1
Administrator	WIN-SRH715DO5HR	API-MS-Win-core-xstate...	C:\Users\ADMINI~1\AppData\Local\Temp\...	1
Administrator	WIN-SRH715DO5HR	API-MS-Win-core-xstate...	C:\Users\ADMINI~1\AppData\Local\Temp\...	1
Administrator	WIN-SRH715DO5HR	API-MS-Win-devices-co...	C:\Users\ADMINI~1\AppData\Local\Temp\...	1
Administrator	WIN-SRH715DO5HR	API-MS-Win-devices-co...	C:\Users\ADMINI~1\AppData\Local\Temp\...	1
Administrator	WIN-SRH715DO5HR	API-MS-Win-devices-co...	C:\Users\ADMINI~1\AppData\Local\Temp\...	1
Administrator	WIN-SRH715DO5HR	API-MS-Win-devices-co...	C:\Users\ADMINI~1\AppData\Local\Temp\...	1
Administrator	WIN-SRH715DO5HR	API-MS-Win-security-Isa...	C:\Users\ADMINI~1\AppData\Local\Temp\...	1
Administrator	WIN-SRH715DO5HR	API-MS-Win-security-Isa...	C:\Users\ADMINI~1\AppData\Local\Temp\...	1

‹ 1 ... 104 105 **106** 107 108 ... 112 ›

	Modified
	418,225

User Names	Host Names	File Names	File Path	Count
SYSTEM	WIN-SRH715DO5HR	MSOXMLED.EXE	C:\Program Files (x86)\Microsoft Office\r...	1
SYSTEM	WIN-SRH715DO5HR	integrator.exe	C:\ProgramData\Microsoft\ClickToRun\{9...	2
SYSTEM	WIN-SRH715DO5HR	mpengine.dll	C:\ProgramData\Microsoft\Windows Defe...	1
SYSTEM	WIN-SRH715DO5HR	mpengine.dll	C:\ProgramData\Microsoft\Windows Defe...	1
SYSTEM	WIN-SRH715DO5HR	ACCICONS.EXE	C:\Program Files (x86)\Microsoft Office\r...	1
SYSTEM	WIN-SRH715DO5HR	ACEDAO.DLL	C:\Program Files (x86)\Microsoft Office\r...	1
SYSTEM	WIN-SRH715DO5HR	DW20.EXE	C:\Program Files (x86)\Microsoft Office\r...	1
SYSTEM	WIN-SRH715DO5HR	DeploymentConfiguratio...	C:\ProgramData\Microsoft\ClickToRun\Ma...	1
SYSTEM	WIN-SRH715DO5HR	EXCEL.EXE	C:\Program Files (x86)\Microsoft Office\r...	1
SYSTEM	WIN-SRH715DO5HR	IntegratedOffice.exe	C:\Program Files\Microsoft Office 15\Clie...	1

‹ 1 ... 8 9 **10** 11 12 ... 15 ›

❏ Capabilities to collect other system/application logs from endpoints lays in local files as well as remote collection
❏ Remote collection mechanisms such as syslog, SNMP , HTTP API are supported
❏ Seamless integration with Data lake

activebytes
innovations

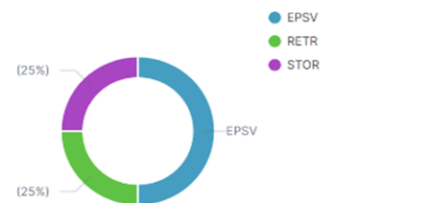(Simple diagrammatic representation of what happened inside the host)

NETWORK SENSOR

- ✓ Network sensor to extract rich logs from the network and feed it to the data-lake
- ✓ Capable of extracting domain lookups.
- ✓ Capable of extracting communication logs irrespective of TCP/IP Protocols.
- ✓ Capture high fidelity transaction logs in network
- ✓ Capture the network traffic across the network without installing agents across each network component

FTP Types : Distribution of type of FTP activities performed by users

- connection
- info
- protocol

protocol (33.33%) — connection (33.33%)

info (33.33%)
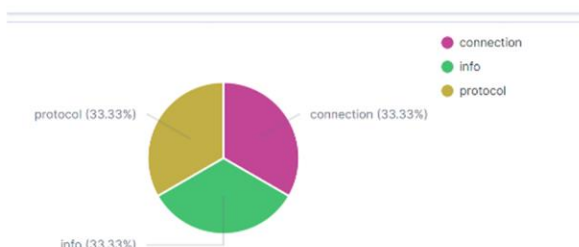
Top FTP Commands : Distribution of frequent FTP commands performed

- EPSV
- RETR
- STOR

(25%)

(25%)

EPSV

FTP Event Summary : Details of FTP activities performed

Host Name	Source IP	Destination IP	Session ID	FTP User	Reply Code	Reply Message	FTP Command	FTP Arg	Count
ip-172-31-4-115	192.168.1.182	192.168.1.231	CgMH9Q2kJPxD...	ftp	226	Transfer complete.	RETR	ftp://192.168.1.2...	1
ip-172-31-4-115	192.168.1.182	192.168.1.231	CgMH9Q2kJPxD...	ftp	226	Transfer complete.	STOR	ftp://192.168.1.2...	1
ip-172-31-4-115	192.168.1.182	192.168.1.231	CgMH9Q2kJPxD...	ftp	229	Entering Extende...	EPSV	-	1
ip-172-31-4-115	192.168.1.182	192.168.1.231	CgMH9Q2kJPxD...	ftp	229	Entering Extende...	EPSV	-	1

- ✓ Capable of capturing file-content metadata from network transactions
- ✓ Capture traffic to and 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

SAMPLE KERBEROS PROTOCOL NETWORK SENSOR DATA DASHBOARD

Description Details of Kerberos activities obtained via network sensor

Kerberos Count : Total kerberos activities peformed

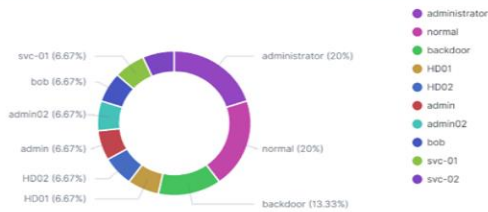**Top User Domains :** Distribution of most frequent domains in activites performed

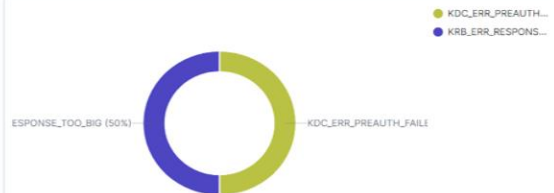**Kerberos Services :** Distribution of kerberos services

Request Types : Distribution of types of kerberos requests performed

134

● THREEBEESCO.COM (100%)

● krbtgt/THREEBEES... 0%

● AS AS (100%)

Top Users : Distribution of most frequent users (top 25) in activities performed

svc-01 (6.67%)
bob (6.67%)
admin02 (6.67%)
admin (6.67%)
HD02 (6.67%)
HD01 (6.67%)
administrator (20%)
normal (20%)
backdoor (13.33%)

● administrator
● normal
● backdoor
● HD01
● HD02
● admin
● admin02
● bob
● svc-01
● svc-02

Error Messages : Distribution of error messages that appeared during kerberos

ESPONSE_TOO_BIG (50%)
KDC_ERR_PREAUTH_FAILE

● KDC_ERR_PREAUTH...
● KRB_ERR_RESPONS...

Kerberos Details : Summary of kerberos activities performed

Clients	User Domains	Validity Until	Error Message	Request Types	Services	Success	Count
administrator/THREEB...	THREEBEESCO.COM	Jul 24, 2020 @ 00:46:3...	KDC_ERR_PREAUTH_F...	AS	krbtgt/THREEBEESCO....	false	1
normal/THREEBEESC...	THREEBEESCO.COM	Jul 24, 2020 @ 00:46:3...	KRB_ERR_RESPONSE_...	AS	krbtgt/THREEBEESCO....	false	1
backdoor/THREEBEES...	THREEBEESCO.COM	Jul 24, 2020 @ 00:46:3...	-	-	-	-	2
HD01/THREEBEESCO....	THREEBEESCO.COM	Jul 24, 2020 @ 00:46:3...	-	-	-	-	1
HD02/THREEBEESCO....	THREEBEESCO.COM	Jul 24, 2020 @ 00:46:3...	-	-	-	-	1
admin/THREEBEESCO....	THREEBEESCO.COM	Jul 24, 2020 @ 00:46:3...	-	-	-	-	1
admin02/THREEBEES...	THREEBEESCO.COM	Jul 24, 2020 @ 00:46:3...	-	-	-	-	1
bob/THREEBEESCO.C...	THREEBEESCO.COM	Jul 24, 2020 @ 00:46:3...	-	-	-	-	1
svc-01/THREEBEESC...	THREEBEESCO.COM	Jul 24, 2020 @ 00:46:3...	-	-	-	-	1
svc-02/THREEBEESC...	THREEBEESCO.COM	Jul 24, 2020 @ 00:46:3...	-	-	-	-	1

Recent Kerberos Events : Details of recent kerberos activities

1–50 of 134

Time	zeek.kerberos.client	zeek.kerberos.error.msg	zeek.kerberos.request_type	zeek.kerberos.success	zeek.kerberos.valid.until	zeek.kerberos.service
> Mar 17, 2021 @ 12:57:18.956	-	-	-	-	-	-
> Feb 22, 2021 @ 12:49:28.200	-	-	-	-	-	-
> Feb 22, 2021 @ 12:49:28.199	-	-	-	-	-	-
> Feb 22, 2021 @ 12:49:28.196	-	-	-	-	-	-
> Feb 22, 2021 @ 12:49:28.196	-	-	-	-	-	-
> Feb 22, 2021 @ 12:49:28.196	-	-	-	-	-	-
> Feb 22, 2021 @ 12:49:28.196	-	-	-	-	-	-
> Feb 22, 2021 @ 12:49:28.196	-	-	-	-	-	-
> Feb 22, 2021 @ 12:49:28.196	-	-	-	-	-	-

activebytes innovations

- ✓ Capable of integrating with proposed Data Lake
- ✓ Supports virtualized environment as well as dedicated appliance or hardware
- ✓ Allows analysts to look into past data for specific IOCs with its high-fidelity logs
- ✓ Capable to process and generate metadata of 50+ major application layer protocols

FULL LIST OF SUPPORTED PROTOCOLS

#	Protocol	#	Protocol
1	BITTORRENT	37	NCP
2	BITTORRENTTRACKER	38	CONTENTS_NETBIOSSSN
3	CONNSIZE	39	NETBIOSSSN
4	DCE_RPC	40	NTLM
5	DHCP	41	NTP
6	DNP3_TCP	42	PIA_TCP
7	DNP3_UDP	43	PIA_UDP
8	CONTENTS_DNS	44	POP3
9	DNS	45	RADIUS
10	FTP_DATA	46	RDP
11	IRC_DATA	47	RDPEUDP
12	FINGER	48	RFB
13	FTP	49	CONTENTS_NFS
14	FTP_ADAT	50	CONTENTS_RPC
15	GENEVE	51	MOUNT
16	GNUTELLA	52	NFS
17	GSSAPI	53	PORTMAPPER
18	GTPV1	54	SIP
19	HTTP	55	CONTENTS_SMB
20	ICMP	56	SMB
21	IDENT	57	SMTP
22	IMAP	58	SNMP
23	IRC	59	SOCKS
24	KRB	60	SSH
25	KRB_TCP	61	DTLS
26	CONTENTS_RLOGIN	62	SSL
27	CONTENTS_RSH	63	SYSLOG
28	LOGIN	64	CONTENTLINE
29	NVT	65	CONTENTS
30	RLOGIN	66	TCPSTATS
31	RSH	67	TCP
32	TELNET	68	TEREDO
33	MODBUS	69	UDP
34	MQTT	70	VXLAN
35	MYSQL	71	XMPP
36	CONTENTS_NCP		