

Deloitte Codex Enrichment for Anomali ThreatStream

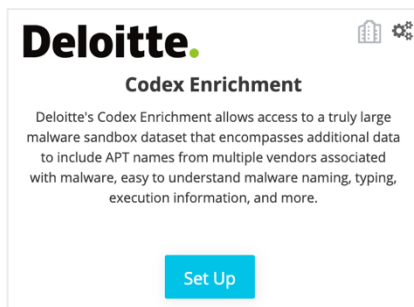
Deloitte's Codex Enrichment allows access to a truly large malware sandbox dataset that encompasses additional data to include APT names from multiple vendors associated with malware, easy to understand malware naming, typing, execution information, and more.

Enrichment Commands

The enrichment provides contextual information from Deloitte in the Enrichments section of observable details pages for domain, IP, email, hash and URL observables.

Activation

1. Log into the ThreatStream interface
2. In the top navigation bar, click the settings icon, then click “Integrations”
3. Click “Set Up” in the Codex enrichment box
4. Click “I have already registered.”
5. Enter:
 - a. Codex username



- b. Codex password
 - c. Query Limit – Limit the number of records returned when querying Deloitte Codex for domain, IP, email, hash and URL observables. A value of zero has no limits (default: 25)
6. Click “Activate”. You should receive a “Successfully Activated Package” message. If an error occurs, please contact Anomali Support for assistance.

Domain, IP, Email and URL View

Related hashes and malware metadata are presented when domain, IP, email, hash and URL observables are enriched, as seen below:

PASSIVE DNS (1,200)	THREATCROWD	VIRUSTOTAL ENRICHMENT	WHOIS HISTORY	RECORDED FUTURE	SAMPLEAPP ENRICHMENT	DELOITTE CODEX	RECORDED FUTURE	WHOIS	SUGGESTED ENRICHMENTS...
Malware									
25 ▾ 1 - 25 of 25 items									
File Type	Family	Family Category	First Seen (UTC)	Size	MD5	SHA1	SHA256		
office	cybergate	rat	2017-08-17 17:37	148992	9d556b6f44d8195f616823df1f3840c	4c67c7ee8f414a3cc29a97a13c41fa0f3d65bce	2c988eb46d5acce90d32257d26f8232611b61adb42c8cec2efa2a9943a020f46		
office	generic		2017-08-23 00:36	30484	f27a3cba1bdd294809a831860e57d154	2a35b07a322aac087b9187ecb8a35f9da2ef6f0	a383d25066ed6bb829aac0725dbb3f532715261dc40cb9a0e61c6e9c075582bb		
office	generic		2017-08-25 12:34	48653	fc8d62838970c7580e9f598e3056448	7f8e7722ff1d72293bca68b77a88a626619b915	2f6f1e3f7ed3b050929579b034b329a457b247e2eb3545072f179ec19d2b98		
office	obfusinjectbot		2017-03-28 15:58	60928	ec831de4e3e47c1843495fc8f288aa90	3c2c38cd26287aa4ebc2d59df6508031568edeaa	e61fc42a4f1d8b561c32ce1bf6683fb4b0e85757c561b0f972deca23766bc01		

Family

Clicking on the malware family name performs a multi-search within ThreatStream.

MD5, SHA1 and SHA256

Clicking any of the associated hashes opens a detailed observable view for the respective hash.

Hash View

Enriching hashes presents the following datasets:

- Files downloaded in sandbox (files downloaded during detonation)
- Files created in sandbox (files created during detonation)
- Files written in sandbox (files written during detonation)
- Files opened in sandbox (files opened during detonation)
- DLLs loaded in sandbox (DLLs loaded during detonation)
- Files executed in sandbox (files executed during detonation)
- Suricata IDS alerts
- Suricata malware signatures
- IPs (IPs observed during detonation)
- DNS (name resolution observed during detonation)
- URIs (URI requests observed during detonation)

Files downloaded in sandbox

25	1 - 5 of 5 items
Name	
http://covid-19.bufferkart.com/zaekil/785565.jpg	
http://mustgrow.com.br/cordobyqdg/785565.jpg	
http://www.seoberatung.de/hydyelg/785565.jpg	
http://agneszkawczolek.com/smw/785565.jpg	
http://amateen.slashinnovate.com/akmhthgpxw/785565.jpg	

Files created in sandbox

25	1 - 4 of 4 items
Name	
c:\users\arrow\appdata\roaming\microsoft\windows\cookies\arrow@agneszkawczolek[1].txt	
c:\users\arrow\appdata\roaming\microsoft\windows\cookies\arrow@covid-19.bufferkart[1].txt	
c:\users\arrow\appdata\local\temp\~d773bec12fa0d536f.tmp	
c:\users\arrow\appdata\local\microsoft\windows\temporary internet files\content.iad56mqgn785565[1].jpg	

Files opened in sandbox

25	1 - 25 of 35 items
Name	
c:\users\arrow\saved games\desktop.ini	
c:\users\arrow\biolaters bios3	
c:\	
c:\users\arrow\appdata	
c:\users\arrow\search\desktop.ini	
c:\users\arrow\video\desktop.ini	
c:\users\arrow\work\desktop.ini	
c:\users\arrow\appdata\roaming\microsoft\windows\cookies\arrow@agneszkawczolek[1].txt	
c:\users\	
c:\users\arrow\picture\desktop.ini	
c:\users\arrow\appdata\local\	
c:\users	
c:\users\arrow\appdata\roaming\microsoft\windows\cookies\index.dat	
c:\program files\microsoft office\office14\glsecui.dll	
c:\users\arrow\favorites\desktop.ini	
c:\program files\microsoft office\office14\msstyle.dll	
c:\users\arrow\music\desktop.ini	
c:\windows\system32\hiber.sys	
c:\users\arrow\appdata\local\temp\95ea033d75507efbfc7a30503dc7cca545a.xls	
c:\users\arrow\contact\desktop.ini	
c:\program files\common files\microsoft shared\office14\mgmts.dll	
c:\windows\system32\en-us\kernelbase.dll.mui	
c:\users\arrow\biolaters bios1	
c:\users\arrow	
c:\users\arrow\biolaters bios2	

DLL's loaded in sandbox

25	1 - 25 of 48 items
Name	
c:\windows\system32\mssock.dll	
urlmon.dll	
winsta.dll	
apphelp.dll	
dnssapi.dll	
uxtheme.dll	
c:\windows\system32\ole32.dll	
user32.dll	
c:\windows\system32\mgmp.dll	
c:\windows\system32\epudm.dll	
monstyle.dll	
urlmon.dll	
api-ms-win-service-management-l1-1-0.dll	
c:\windows\system32\msoct.dll	
..biolaters bios1	
..biolaters bios3	
..biolaters bios2	
oleau32.dll	
rasman.dll	
httpapi.dll	
ole32.dll	
cryptsp.dll	
c:\program files\microsoft office\office14\glsecui.dll	
c:\windows\system32\mssock.dll	
api-ms-win-security-adv-l1-1-0.dll	

Files executed in sandbox

25

1 - 5 of 5 items

Command
rundll32 _libolaters.fc3c2.dll;registerserver
rundll32 _libolaters.fc3c2.dll;registerserver
rundll32 _libolaters.fc3c2.dll;registerserver
rundll32 _libolaters.fc3c2.dll;registerserver
rundll32 _libolaters.fc3c1.dll;registerserver

Suricata IDS alerts

25

1 - 2 of 2 items

Protocol	Source IP	Source Port	Destination IP	Destination Port	Date	SID	Category	Signature
udp	192.168.59.88	60983	8.8.8.8	53	2021-02-09T12:49:40.927145+0000	2029709	potentially bad traffic	et hunting suspicious domain request for possible covid-19 domain m1
tcp	192.168.59.88	49212	119.18.58.55	80	2021-02-09T12:49:44.486179+0000	2029711	potentially bad traffic	et hunting suspicious get request with possible covid-19 domain m1

Suricata malware signatures

25

1 - 4 of 4 items

Severity	Description
2	performs some http requests
2	allocates read-write-execute memory (usually to unpack RAR)
3	network communications indicative of a potential document or script payload download was initiated by the process excel.exe
3	one or more martian processes was created

IPs

25

1 - 5 of 5 items

IP	Continent	Country	City	Latitude	Longitude	ASO	ASN
192.185.223.48	North America	United States		37.751	-87.822	UNIFIEDLAYER-AS-1	46606
94.136.10.73	Europe	Germany		51.2993	9.491	Hetzner Online GmbH	24940
119.18.58.55	Asia	India		20.0063	77.086	PUBLIC DOMAIN REGISTRY	394695
192.185.16.95	North America	United States		37.751	-87.822	UNIFIEDLAYER-AS-1	46606
5.252.230.98	Europe	Poland		52.2394	21.0362	UP.pl Sp. z o.o.	203417

DNS

25

1 - 5 of 5 items

Type	Request	Answers
A	www.secdatabase.org	94.136.10.73
A	covid-19.bufterkart.com	119.18.58.55
A	agneskawiczolek.com	5.252.230.98
A	smatzen.slaahinnovata.com	192.185.16.95
A	muitgrow.com.br	192.185.223.48

URLs

25

1 - 5 of 5 items

URI
http://smatzen.slaahinnovata.com/agneskawiczolek/785565.jpg
http://www.secdatabase.org/de/hydrigp/785565.jpg
http://covid-19.bufterkart.com/covid/785565.jpg
http://agneskawiczolek.com/olmu/785565.jpg
http://muitgrow.com.br/ordbogyip/785565.jpg

Changelog

V1.0.0

- Initial Release
- Supports domain, email, hash, ip and url indicator types