Deloitte Codex Enrichment for Anomali ThreatStream

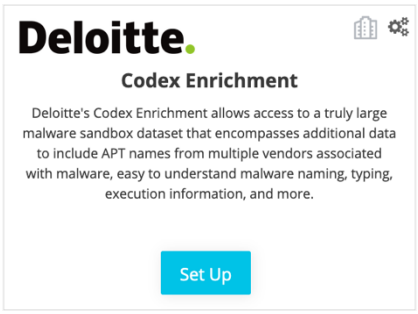
Deloitte's Codex Enrichment allows access to a truly large malware sandbox dataset that encompasses additional data to include APT names from multiple vendors associated with malware, easy to understand malware naming, typing, execution information, and more.

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

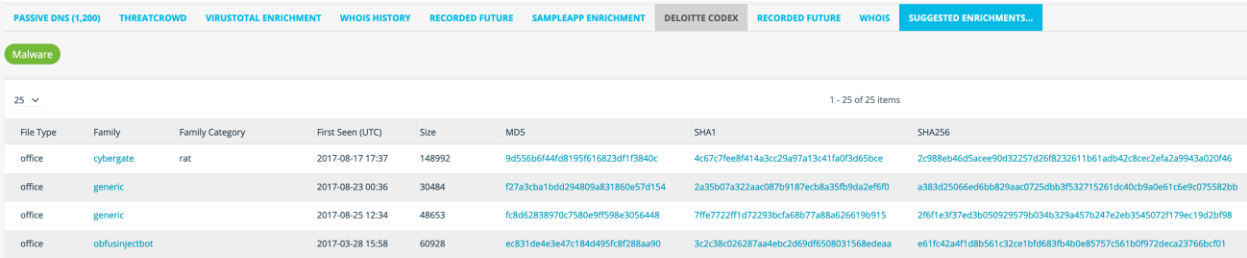
1. Log into the ThreatStream interface
2. In the top navigation bar, click the settings icon, then click “Integrations”
3. Click “Set Up” in the Codex enrichment box
4. Click “I have already registered.”
5. Enter:
    a. Codex username



    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:



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)

THREATCROWD | VIRUSTOTAL ENRICHMENT | RECORDED FUTURE | DELOITTE CODEX | RECORDED FUTURE | SUGGESTED ENRICHMENTS...

Files downloaded in sandbox

25 | 1 - 5 of 5 items

Name
http://covid-19.bufferkart.com/zaekili/785565.jpg
http://mustgrow.com.br/crdbzjyqdg/785565.jpg
http://www.seoberatung.de/xbydzijelg/785565.jpg
http://agnieszkawszolek.com/ismxvv/785565.jpg
http://amateen.slashinnovate.com/akmhlngpwxi/785565.jpg

Files created in sandbox

25 | 1 - 4 of 4 items

Name
c:\users\arrow\appdata\roaming\microsoft\windows\cookies\arrow@agnieszkawszolek[1].txt
c:\users\arrow\appdata\roaming\microsoft\windows\cookies\arrow@covid-19.bufferkart[1].txt
c:\users\arrow\appdata\local\temp\~df733ec012fa0d536f.tmp
c:\users\arrow\appdata\local\microsoft\windows\temporary internet files\content.ie5\66nqwsjar\785565[1].jpg

Files opened in sandbox

25 | 1 - 25 of 35 items

Name
c:\users\arrow\saved games\desktop.ini
c:\users\arrow\biolaters.llos3
c:\
c:\users\arrow\appdata
c:\users\arrow\searches\desktop.ini
c:\users\arrow\videos\desktop.ini
c:\users\arrow\links\desktop.ini
c:\users\arrow\appdata\roaming\microsoft\windows\cookies\arrow@agnieszkawszolek[1].txt
c:\users\
c:\users\arrow\pictures\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\gkexcel.dll
c:\users\arrow\favorites\desktop.ini
c:\program files\microsoft office\office14\msostyle.dll
c:\users\arrow\music\desktop.ini
c:\windows\system32\ui\docvw.dll
c:\users\arrow\appdata\local\temp\95ea4f33d7550f1e6bc7a30503c9c7cca85454ca.xls
c:\users\arrow\contacts\desktop.ini
c:\program files\common files\microsoft shared\office14\msptls.dll
c:\windows\system32\en-us\kernelbase.dll.mui
c:\users\arrow\biolaters.llos1
c:\users\arrow
c:\users\arrow\biolaters.llos2

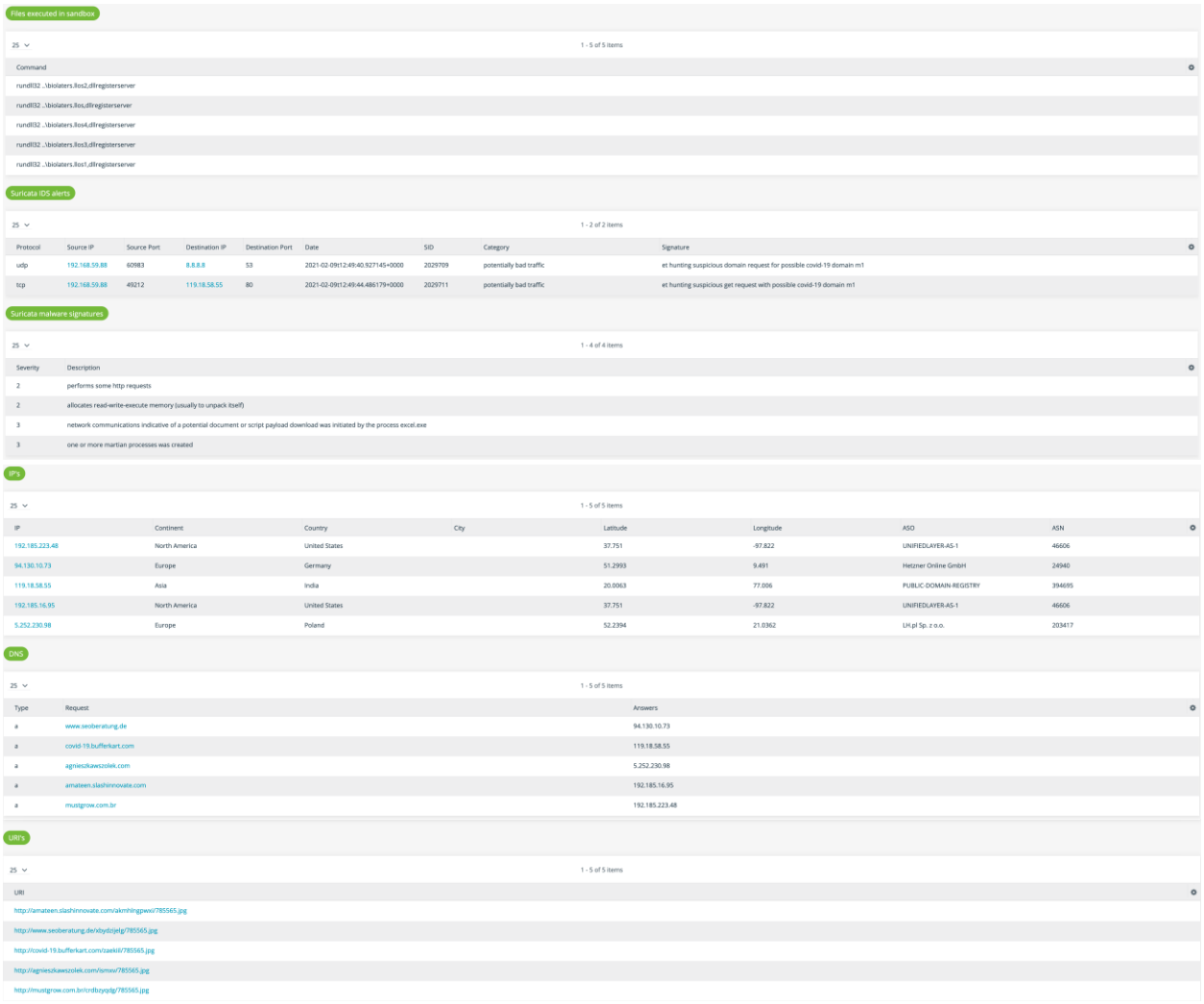
« PREVIOUS 1 | 2 NEXT »

DLL's loaded in sandbox

25 | 1 - 25 of 48 items

Name
c:\windows\system32\mswsock.dll
urlmon.dll
winsta.dll
apphelp.dll
dnsapi.dll
uxtheme.dll
c:\windows\system32\ole32.dll
user32.dll
c:\windows\system32\napinsp.dll
c:\windows\system32\fwpuclnt.dll
msostyle.dll
urlmon.dll
api-ms-win-service-management-l1-1-0.dll
c:\windows\system32\msctf.dll
..\biolaters.llos1
..\biolaters.llos3
..\biolaters.llos2
oleaut32.dll
rasman.dll
iphlpapi.dll
ole32.dll
cryptsp.dll
c:\program files\microsoft office\office14\gkexcel.dll
c:\windows\system32\mswsock.dll
api-ms-win-security-sddl-l1-1-0.dll

« PREVIOUS 1 | 2 NEXT »



Changelog

V1.0.0

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