Google Cloud

VirusTotal
Threat landscape module

Rich and actionable adversary intelligence

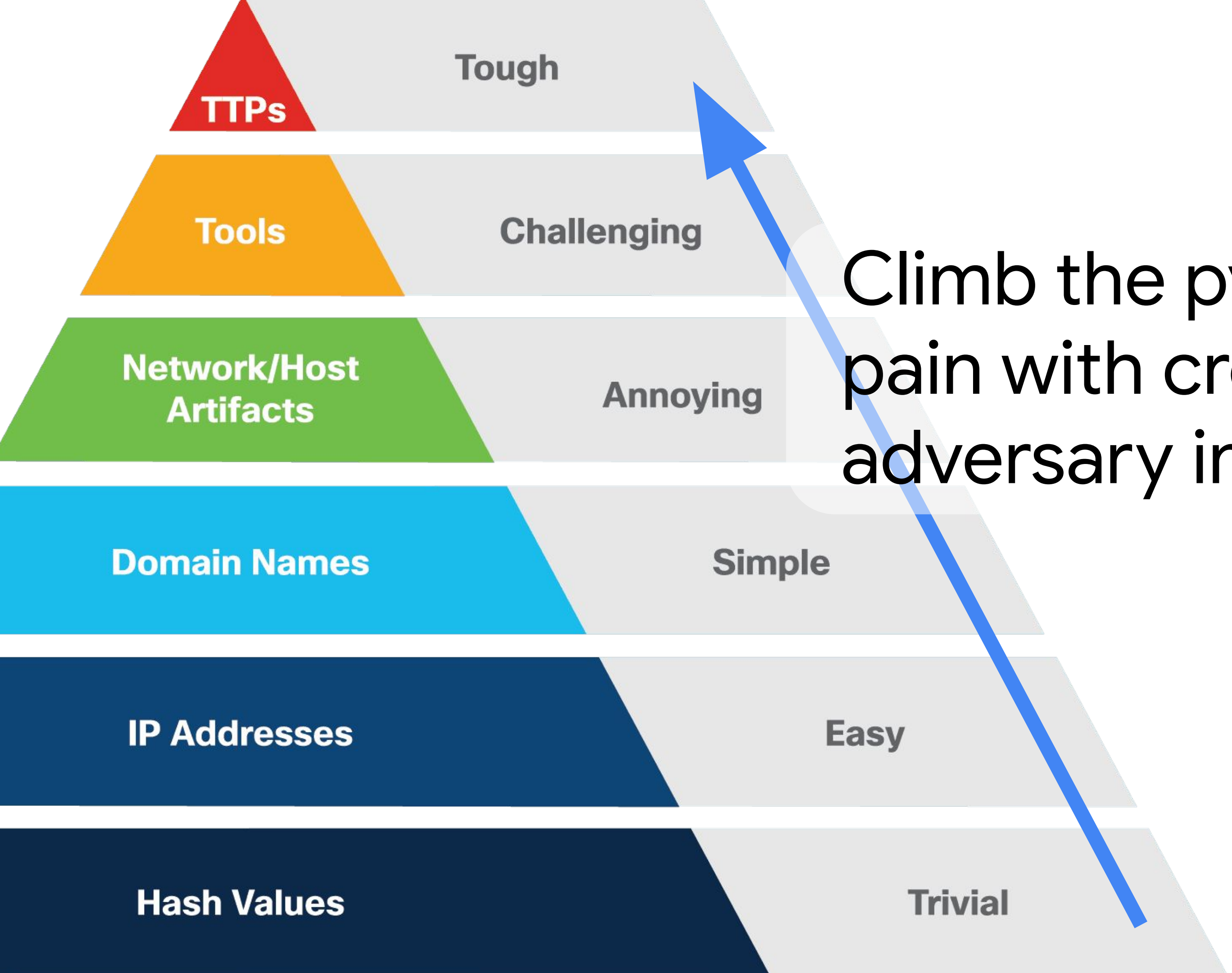
www.virustotal.com/contact

Fighting global adversaries constrained by the narrow visibility of a handful of researchers?

There is a better way.

In a nutshell

Adversary intelligence layer providing superior context across the VT ENTERPRISE threat intelligence suite



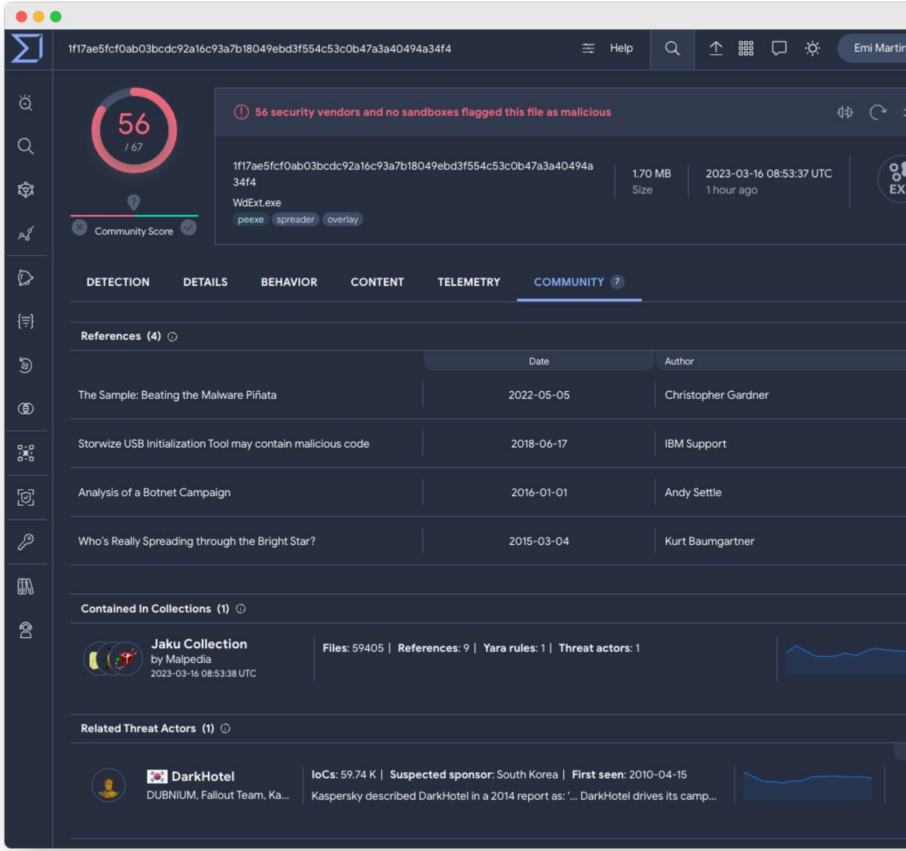
Climb the pyramid of pain with crowdsourced adversary intelligence

Instantly learn who/what is behind an incident

The threat lanscape module adds links and online deep dive research articles to threat {campaign, toolkit, actor} cards in {file, domain, IP, URL} reports.

Understand who is behind a given IoC and how their campaign operates. Linked cards include one-click access to related IoCs, TTPs, hunting artefact, rules, etc. to proactively protect your organization or unearth missed threats.

Extend your knowledge via Finished intelligence reports crowdsourced from online articles. [+]



56 security vendors and no sandboxes flagged this file as malicious

1f17ae5fcf0ab03bcdc92a16c93a7b18049ebd3f554c53c0b47a3a40494a34f4
WdExt.exe
peexe spreader overlay

1.70 MB
Size

2023-03-16 08:53:37 UTC
1 hour ago

References (4)

	Date	Author
The Sample: Beating the Malware Piñata	2022-05-05	Christopher Gardner
Storwize USB Initialization Tool may contain malicious code	2018-06-17	IBM Support
Analysis of a Botnet Campaign	2016-01-01	Andy Settle
Who's Really Spreading through the Bright Star?	2015-03-04	Kurt Baumgartner

Contained In Collections (1)

Jaku Collection
by Malpedia
2023-03-16 08:53:38 UTC
Files: 59405 | **References:** 9 | **Yara rules:** 1 | **Threat actors:** 1

Related Threat Actors (1)

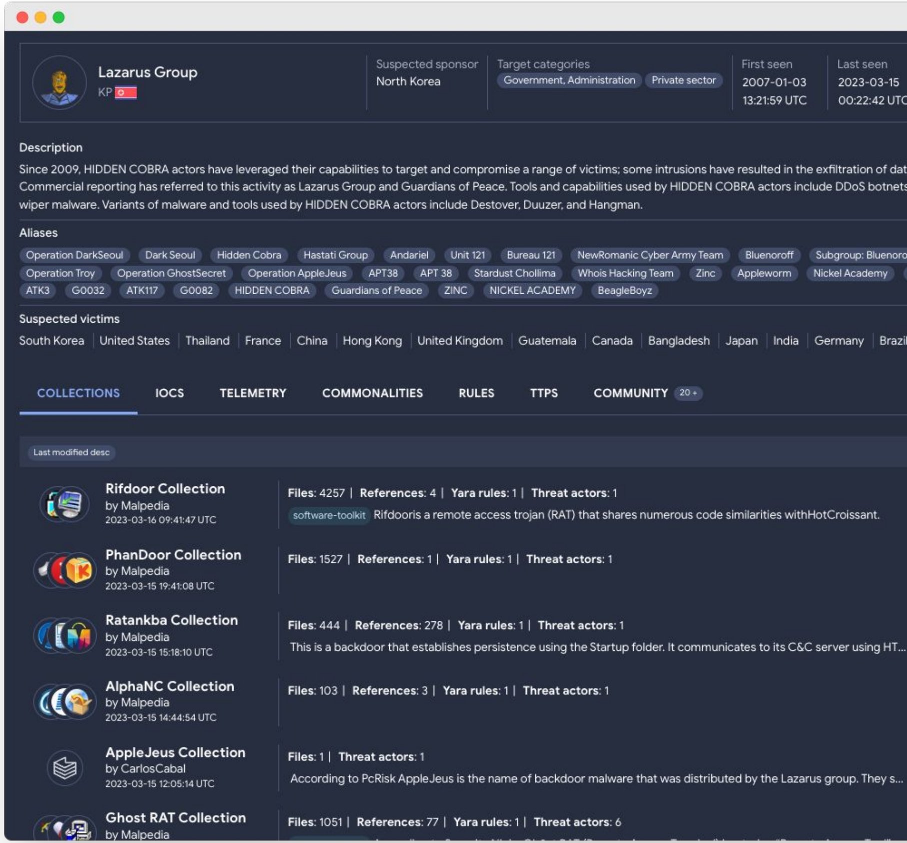
DarkHotel
DUBNIUM, Fallout Team, Ka...
IoCs: 59.74 K | **Suspected sponsor:** South Korea | **First seen:** 2010-04-15
Kaspersky described DarkHotel in a 2014 report as: '... DarkHotel drives its camp...

Outsmart your adversaries via threat actor cards

Essential and actionable information related to a threat actor group, updated real-time.

Summaries include a description, aliases, suspected nation state sponsor, targeted industries, targeted regions, motivations, etc.

Actionable insights in the form of campaigns/toolkit tied to the actor, IoCs, geo+time activity breakdowns, common technical properties for their toolkit, {YARA, Sigma, IDS} detection rules, MITRE ATT&CK TTPs, finished intelligence articles. [+]



Lazarus Group
KP

Suspected sponsor: North Korea

Target categories: Government, Administration | Private sector

First seen: 2007-01-03 13:21:59 UTC

Last seen: 2023-03-15 00:22:42 UTC

Description

Since 2009, HIDDEN COBRA actors have leveraged their capabilities to target and compromise a range of victims; some intrusions have resulted in the exfiltration of dat
Commercial reporting has referred to this activity as Lazarus Group and Guardians of Peace. Tools and capabilities used by HIDDEN COBRA actors include DDoS botnets
wiper malware. Variants of malware and tools used by HIDDEN COBRA actors include Destover, Duuzer, and Hangman.

Aliases

Operation DarkSeoul | Dark Seoul | Hidden Cobra | Hastati Group | Andariel | Unit 121 | Bureau 121 | NewRomanic Cyber Army Team | Bluenoroff | Subgroup: Bluenoro
Operation Troy | Operation GhostSecret | Operation AppleJeus | APT38 | APT 38 | Stardust Chollima | Whois Hacking Team | Zinc | Appleworm | Nickel Academy
ATK3 | G0032 | ATK117 | G0082 | HIDDEN COBRA | Guardians of Peace | ZINC | NICKEL ACADEMY | BeagleBoyz

Suspected victims

South Korea | United States | Thailand | France | China | Hong Kong | United Kingdom | Guatemala | Canada | Bangladesh | Japan | India | Germany | Brazi

Rifdoor Collection
by Malpedia
2023-03-16 09:41:47 UTC
Files: 4257 | **References**: 4 | **Yara rules**: 1 | **Threat actors**: 1
software-toolkit Rifdooris a remote access trojan (RAT) that shares numerous code similarities withHotCroissant.

PhanDoor Collection
by Malpedia
2023-03-15 19:41:08 UTC
Files: 1527 | **References**: 1 | **Yara rules**: 1 | **Threat actors**: 1

Ratankba Collection
by Malpedia
2023-03-15 15:18:10 UTC
Files: 444 | **References**: 278 | **Yara rules**: 1 | **Threat actors**: 1
This is a backdoor that establishes persistence using the Startup folder. It communicates to its C&C server using HT...

AlphaNC Collection
by Malpedia
2023-03-15 14:44:54 UTC
Files: 103 | **References**: 3 | **Yara rules**: 1 | **Threat actors**: 1

AppleJeus Collection
by CarlosCabal
2023-03-15 12:05:14 UTC
Files: 1 | **Threat actors**: 1
According to PcRisk AppleJeus is the name of backdoor malware that was distributed by the Lazarus group. They s...

Ghost RAT Collection
by Malpedia
Files: 1051 | **References**: 77 | **Yara rules**: 1 | **Threat actors**: 6

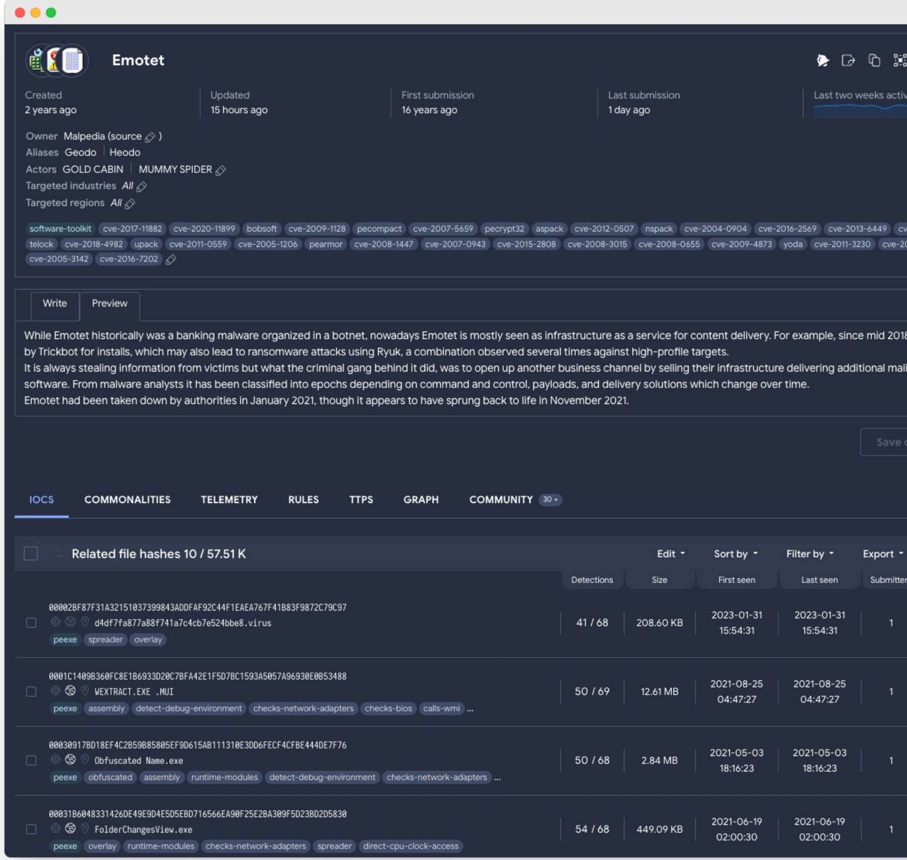
Find breaches with threat campaign/toolkit cards

In-depth analysis of collections of IoCs generating insights to detect missed threats, all the way from hashes to TTPs.

Actionable intelligence for all maturity levels: hashes, IPs, domains, URLs, detection rules, malware toolkit technical commonalities, TTPs, etc.

Search and API lookup activity aggregations to understand targeted countries and operational timeframe.

Finished intelligence in the form of crowdsourced online articles about the campaign/toolkit. [+]



Emotet

Created 2 years ago | Updated 15 hours ago | First submission 16 years ago | Last submission 1 day ago | Last two weeks activi

Owner Malpedia (source)
Aliases Geodo | Heodo
Actors GOLD CABIN | MUMMY SPIDER
Targeted industries *All*
Targeted regions *All*

software-toolkit cve-2017-11882 cve-2020-11899 bobsoft cve-2009-1128 pecompact cve-2007-5659 pecrypt32 aspack cve-2012-0507 nspack cve-2004-0904 cve-2016-2569 cve-2013-6449 cv telock cve-2018-4982 upack cve-2011-0559 cve-2005-1206 pearmor cve-2008-1447 cve-2007-0943 cve-2015-2808 cve-2008-3015 cve-2008-0655 cve-2009-4873 yoda cve-2011-3230 cve-20 cve-2005-3142 cve-2016-7202

While Emotet historically was a banking malware organized in a botnet, nowadays Emotet is mostly seen as infrastructure as a service for content delivery. For example, since mid 2018 by Trickbot for installs, which may also lead to ransomware attacks using Ryuk, a combination observed several times against high-profile targets.
It is always stealing information from victims but what the criminal gang behind it did, was to open up another business channel by selling their infrastructure delivering additional mali software. From malware analysts it has been classified into epochs depending on command and control, payloads, and delivery solutions which change over time.
Emotet had been taken down by authorities in January 2021, though it appears to have sprung back to life in November 2021.

Related file hashes 10 / 57.51 K

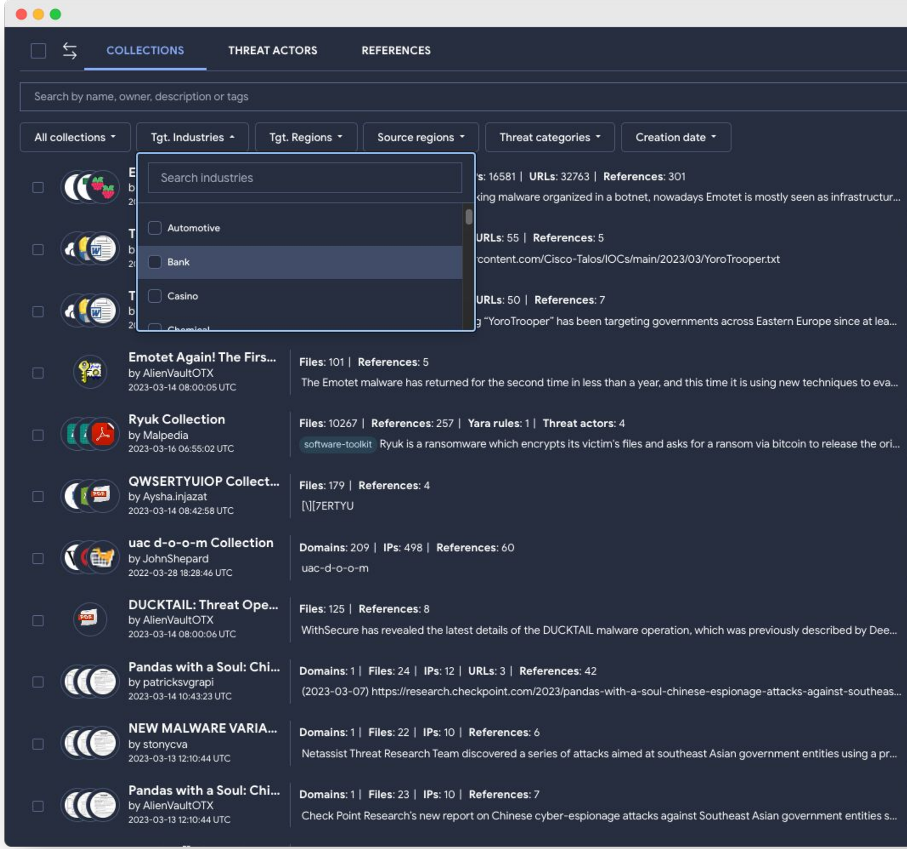
	Detections	Size	First seen	Last seen	Submitte
00002BF87F31A32151037399843ADDFAF92C44F1EAEA767F41B83F9872C79C97 d4df7fa877a88f741a7c4cb7e524bbe8.virus peexe spreader overlay	41 / 68	208.60 KB	2023-01-31 15:54:31	2023-01-31 15:54:31	1
0001C1409B360FC8E1B6933D20C7BFA42E1F5D7BC1593A5057A96930E0B53488 WEXTRACT.EXE .MUI peexe assembly detect-debug-environment checks-network-adapters checks-bios calls-wmi ...	50 / 69	12.61 MB	2021-08-25 04:47:27	2021-08-25 04:47:27	1
00030917BD18EF4C2B59B85805EF9D615AB111310E3DD6FECF4CFBE444DE7F76 Obfuscated Name.exe peexe obfuscated assembly runtime-modules detect-debug-environment checks-network-adapters ...	50 / 68	2.84 MB	2021-05-03 18:16:23	2021-05-03 18:16:23	1
00031B6048331426DE49E9D4E5D5EBD716566EA90F25E2BA309F5D23BD2D5830 FolderChangesView.exe peexe overlay runtime-modules checks-network-adapters spreader direct-cpu-clock-access	54 / 68	449.09 KB	2021-06-19 02:00:30	2021-06-19 02:00:30	1

Trends to achieve faster mean time to detect

Leverage the extended visibility and collective speed of the community, accelerate defensive operations.

The threat landscape module gives you access to all community + partner collections, threat actors and references, in a fully indexed and searchable manner. Focus on what matters to your organization, when it matters, via targeted industry, targeted region, source region, threat category and date filters.

Accelerate beyond the investigations of a handful of researchers staring at a piece of the puzzle. [+]



E
b
2

's: 16581 | **URLs**: 32763 | **References**: 301
king malware organized in a botnet, nowadays Emotet is mostly seen as infrastructur...

T
b
2

URLs: 55 | **References**: 5
content.com/Cisco-Talos/IOCs/main/2023/03/YoroTrooper.txt

T
b
2

URLs: 50 | **References**: 7
g "YoroTrooper" has been targeting governments across Eastern Europe since at lea...

Emotet Again! The Firs...
by AlienVaultOTX
2023-03-14 08:00:05 UTC

Files: 101 | **References**: 5
The Emotet malware has returned for the second time in less than a year, and this time it is using new techniques to eva...

Ryuk Collection
by Malpedia
2023-03-16 06:55:02 UTC

Files: 10267 | **References**: 257 | **Yara rules**: 1 | **Threat actors**: 4
software-toolkit Ryuk is a ransomware which encrypts its victim's files and asks for a ransom via bitcoin to release the ori...

QWSERTYUIOP Collect...
by Aysha.injazat
2023-03-14 08:42:58 UTC

Files: 179 | **References**: 4
[\][7ERTYU

uac d-o-o-m Collection
by JohnShepard
2022-03-28 18:28:46 UTC

Domains: 209 | **IPs**: 498 | **References**: 60
uac-d-o-o-m

DUCKTAIL: Threat Ope...
by AlienVaultOTX
2023-03-14 08:00:06 UTC

Files: 125 | **References**: 8
WithSecure has revealed the latest details of the DUCKTAIL malware operation, which was previously described by Dee...

Pandas with a Soul: Chi...
by patricksvgrapi
2023-03-14 10:43:23 UTC

Domains: 1 | **Files**: 24 | **IPs**: 12 | **URLs**: 3 | **References**: 42
(2023-03-07) https://research.checkpoint.com/2023/pandas-with-a-soul-chinese-espionage-attacks-against-southeas...

NEW MALWARE VARIA...
by stonycva
2023-03-13 12:10:44 UTC

Domains: 1 | **Files**: 22 | **IPs**: 10 | **References**: 6
Netassist Threat Research Team discovered a series of attacks aimed at southeast Asian government entities using a pr...

Pandas with a Soul: Chi...
by AlienVaultOTX
2023-03-13 12:10:44 UTC

Domains: 1 | **Files**: 23 | **IPs**: 10 | **References**: 7
Check Point Research's new report on Chinese cyber-espionage attacks against Southeast Asian government entities s...

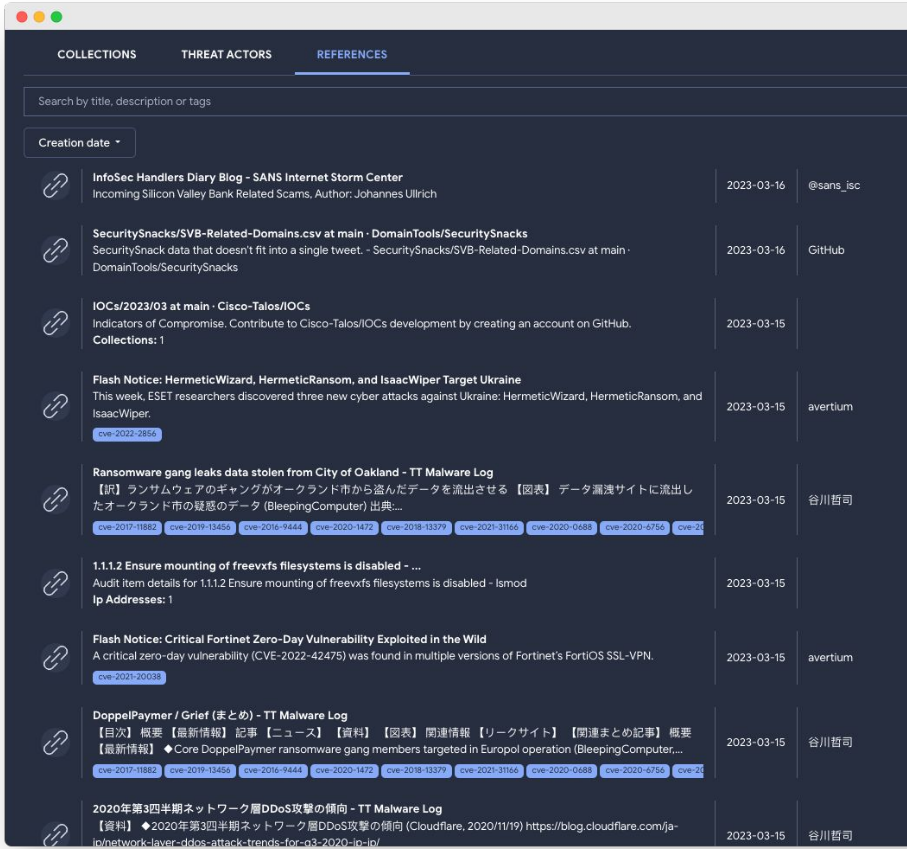
Stay abreast of emerging threats with online reports

Crowdsourced research articles about the latest threats consolidated into a single interface and digested via NLP.

Planet-wide Internet crawls focusing on malware and threat actor articles, acting as a live daily stream of finished intelligence reports.

Automatic extraction and tagging of CVEs, targeted industries, motivations, malware toolkit, affected regions, etc.

Search across the knowledge base and answer your executives' questions. [+]



InfoSec Handlers Diary Blog - SANS Internet Storm Center Incoming Silicon Valley Bank Related Scams, Author: Johannes Ullrich	2023-03-16	@sans_isc
SecuritySnacks/SVB-Related-Domains.csv at main · DomainTools/SecuritySnacks SecuritySnack data that doesn't fit into a single tweet. - SecuritySnacks/SVB-Related-Domains.csv at main · DomainTools/SecuritySnacks	2023-03-16	GitHub
IOCs/2023/03 at main · Cisco-Talos/IOCs Indicators of Compromise. Contribute to Cisco-Talos/IOCs development by creating an account on GitHub. **Collections:** 1	2023-03-15	
Flash Notice: HermeticWizard, HermeticRansom, and IsaacWiper Target Ukraine This week, ESET researchers discovered three new cyber attacks against Ukraine: HermeticWizard, HermeticRansom, and IsaacWiper. cve-2022-2856	2023-03-15	avertium
Ransomware gang leaks data stolen from City of Oakland - TT Malware Log 【訳】ランサムウェアのギャングがオークランド市から盗んだデータを流出させる 【図表】 データ漏洩サイトに流出したオークランド市の疑惑のデータ (BleepingComputer) 出典:... cve-2017-11882 cve-2019-13456 cve-2016-9444 cve-2020-1472 cve-2018-13379 cve-2021-31166 cve-2020-0688 cve-2020-6756 cve-2	2023-03-15	谷川哲司
1.1.1.2 Ensure mounting of freevxfs filesystems is disabled - ... Audit item details for 1.1.1.2 Ensure mounting of freevxfs filesystems is disabled - lsmod **Ip Addresses:** 1	2023-03-15	
Flash Notice: Critical Fortinet Zero-Day Vulnerability Exploited in the Wild A critical zero-day vulnerability (CVE-2022-42475) was found in multiple versions of Fortinet's FortiOS SSL-VPN. cve-2021-20038	2023-03-15	avertium
DoppelPaymer / Grief (まとめ) - TT Malware Log 【目次】 概要 【最新情報】 記事 【ニュース】 【資料】 【図表】 関連情報 【リークサイト】 【関連まとめ記事】 概要 【最新情報】 ◆Core DoppelPaymer ransomware gang members targeted in Europol operation (BleepingComputer,... cve-2017-11882 cve-2019-13456 cve-2016-9444 cve-2020-1472 cve-2018-13379 cve-2021-31166 cve-2020-0688 cve-2020-6756 cve-2	2023-03-15	谷川哲司
2020年第3四半期ネットワーク層DDoS攻撃の傾向 - TT Malware Log 【資料】 ◆2020年第3四半期ネットワーク層DDoS攻撃の傾向 (Cloudflare, 2020/11/19) https://blog.cloudflare.com/ja-jp/network-layer-ddos-attack-trends-for-q3-2020-jp-jp/	2023-03-15	谷川哲司

Actionability first

Go beyond IoCs and PDF reports, focus on patterns and modus operandi, corner your adversaries and unearth unknown threats

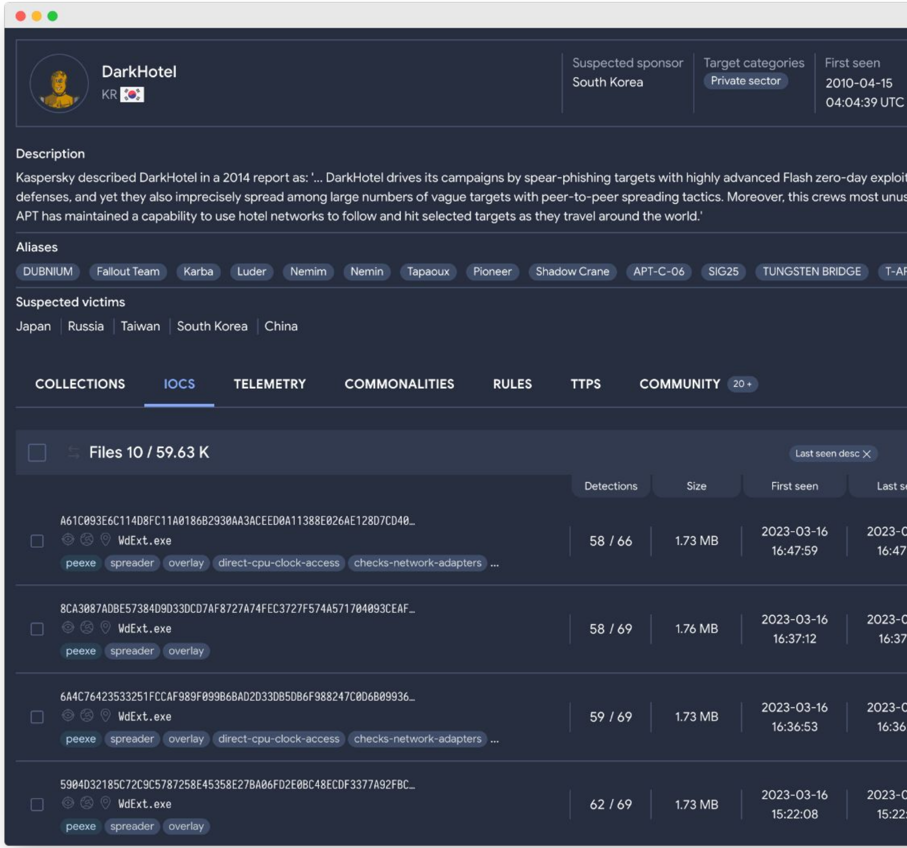
Detect and proactively block high severity IoCs

{file hashes, domains, IPs URLs} tied to threat campaigns and actors, updated real-time.

Flag missed threats via retroactive IoC matching in SIEM logs or proactively block them in defensive technologies such as NGFW, EDRs, etc.

Boost the severity score of these alerts given their direct association with a threat actor.

One-click exports into the most popular ingestion formats and off-the-shelf integrations in security technologies. [+]



DarkHotel
KR

Suspected sponsor
South Korea

Target categories
Private sector

First seen
2010-04-15
04:04:39 UTC

Description

Kaspersky described DarkHotel in a 2014 report as: '... DarkHotel drives its campaigns by spear-phishing targets with highly advanced Flash zero-day exploi
defenses, and yet they also imprecisely spread among large numbers of vague targets with peer-to-peer spreading tactics. Moreover, this crews most unu
APT has maintained a capability to use hotel networks to follow and hit selected targets as they travel around the world.'

Aliases

DUBNIUM | Fallout Team | Karba | Luder | Nemim | Nemin | Tapaoux | Pioneer | Shadow Crane | APT-C-06 | SIG25 | TUNGSTEN BRIDGE | T-AP

Suspected victims

Japan | Russia | Taiwan | South Korea | China

□ Files 10 / 59.63 K

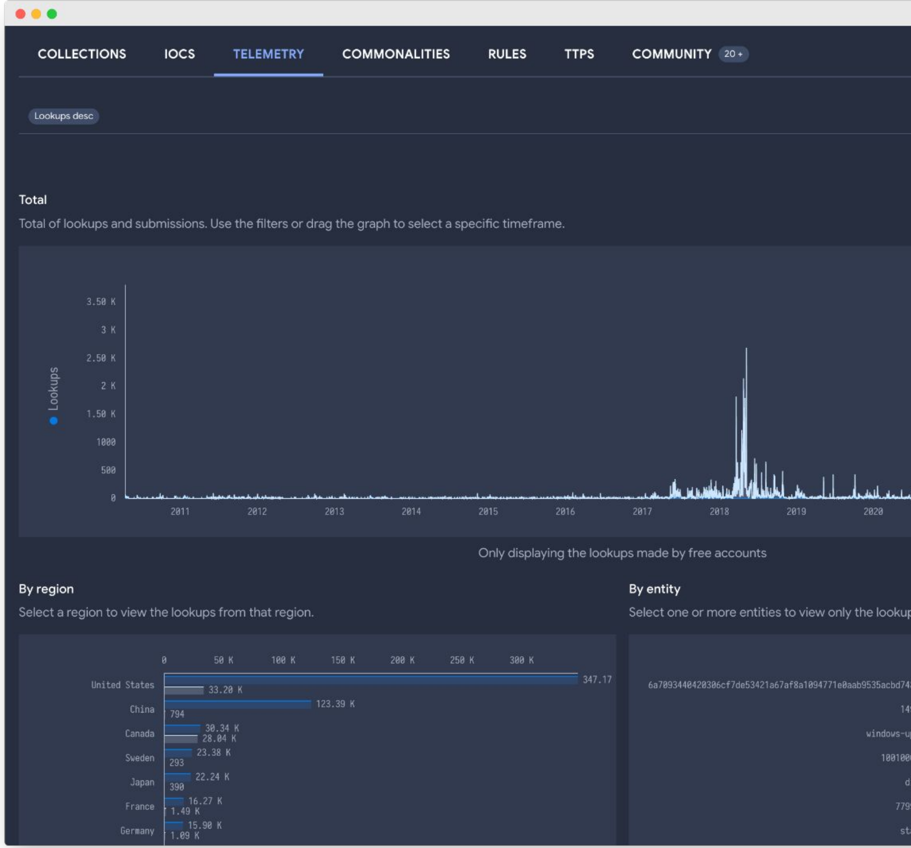
		Detections	Size	First seen	Last s
□	A61C093E6C114D8FC11A0186B2930AA3ACEED0A11388E026AE128D7CD40… WdExt.exe peexe spreader overlay direct-cpu-clock-access checks-network-adapters …	58 / 66	1.73 MB	2023-03-16 16:47:59	2023-0 16:47
□	8CA3087ADBE57384D9D33DCD7AF8727A74FEC3727F574A571704093CEAF… WdExt.exe peexe spreader overlay	58 / 69	1.76 MB	2023-03-16 16:37:12	2023-0 16:37
□	6A4C76423533251FCCAF989F099B6BAD2D33DB5DB6F988247C0D6B09936… WdExt.exe peexe spreader overlay direct-cpu-clock-access checks-network-adapters …	59 / 69	1.73 MB	2023-03-16 16:36:53	2023-0 16:36
□	5904D32185C72C9C5787258E45358E27BA06FD2E0BC48ECDF3377A92FBC… WdExt.exe peexe spreader overlay	62 / 69	1.73 MB	2023-03-16 15:22:08	2023-0 15:22

Answer where, when and what with global telemetry

Web and API lookups by 3.6M+ free users in 230+ countries digested into geographical+time+IoC activity lines.

Focus on specific time ranges and understand targeted regions and IoCs leveraged. Breakdowns and filters across all three dimensions: time, region and IoC.

When was a given actor/campaign active in France? What malware did they use then? During May 2022, which regions did a given actor target? Answer all these questions and more. [+]



Total

Total of lookups and submissions. Use the filters or drag the graph to select a specific timeframe.

Only displaying the lookups made by free accounts

By region

Select a region to view the lookups from that region.

By entity

Select one or more entities to view only the lookup

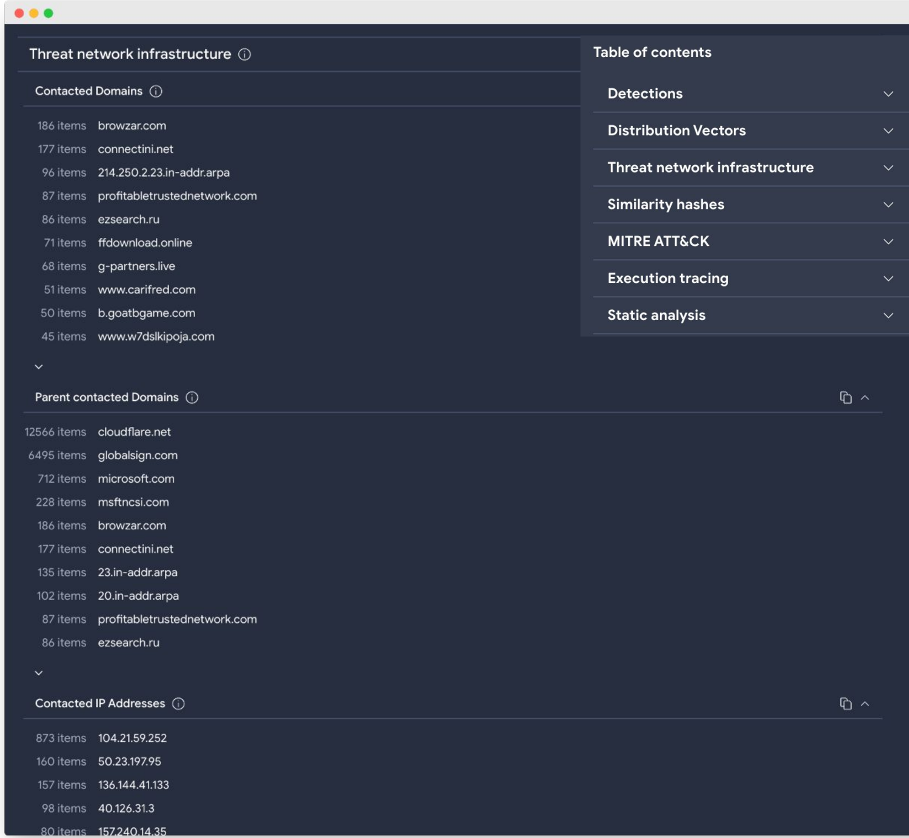
Go beyond IoCs, look for toolkit commonalities

Automatic extraction and ranking of malware toolkit technical properties that can be used for hunting purposes.

Aggregations and ranks across AV/EDR detections, distribution vectors, network infrastructure (CnCs, download URLs...), persistence registry keys, mutexes, dropped files, PDB paths, imphash, etc.

Climb the pyramid of pain and focus on leftovers and repeatable patterns for malware toolkit used by your adversaries.

Includes one-click action to calculate commonalities for custom search / hunt results. [+]



Threat network infrastructure ⓘ

Contacted Domains ⓘ

186 items	browzar.com
177 items	connectini.net
96 items	214.250.2.23.in-addr.arpa
87 items	profitabletrustednetwork.com
86 items	ezsearch.ru
71 items	ffdownload.online
68 items	g-partners.live
51 items	www.carifred.com
50 items	b.goatbgame.com
45 items	www.w7dslkipoja.com

Parent contacted Domains ⓘ

12566 items	cloudflare.net
6495 items	globalsign.com
712 items	microsoft.com
228 items	msftncsi.com
186 items	browzar.com
177 items	connectini.net
135 items	23.in-addr.arpa
102 items	20.in-addr.arpa
87 items	profitabletrustednetwork.com
86 items	ezsearch.ru

Contacted IP Addresses ⓘ

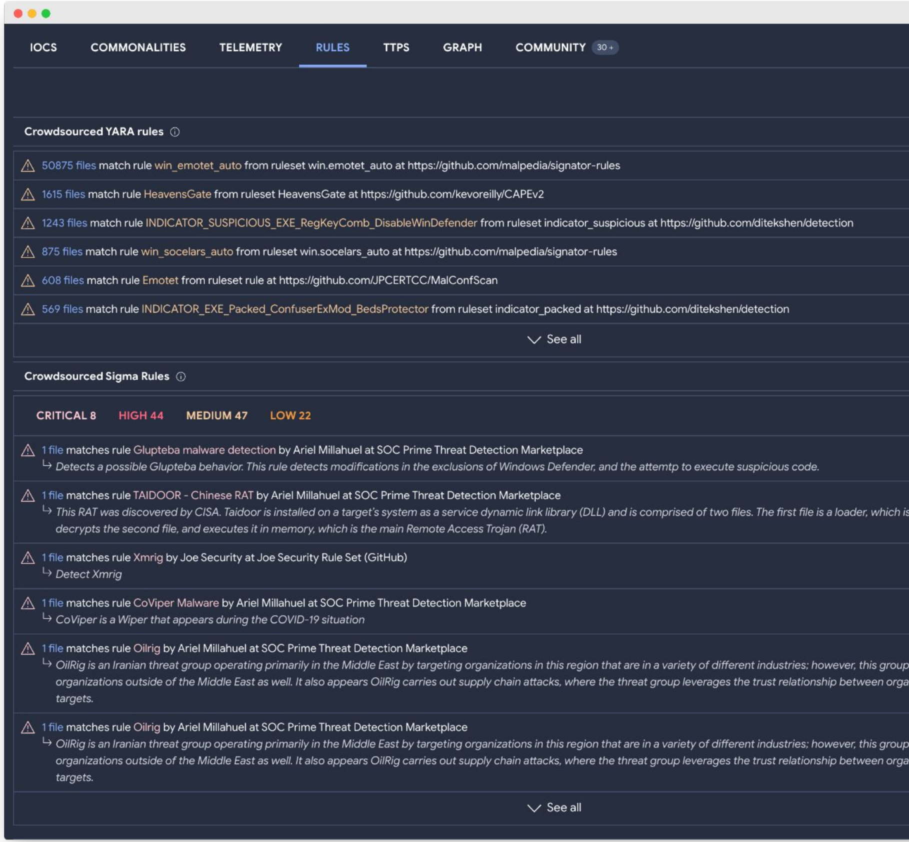
873 items	104.21.59.252
160 items	50.23.197.95
157 items	136.144.41.133
98 items	40.126.31.3
80 items	157.240.14.35

Deploy multi-layered detections

Threat {campaign, toolkit, actor} cards rank crowdsourced {YARA, Sigma, IDS} rules matching against their artifacts.

YARA rules provide an additional static detection layer beyond your AV/EDR. Sigma rules tackle the detonation behaviour angle. IDS rules introduce flags at the network level. Implement a true defense-in-depth security program.

All the rules include detailed descriptions providing further context and pivots to uncover other matching IoCs in the VirusTotal global corpus. [+]



Crowdsourced YARA rules

⚠ 50875 files match rule win_emotet_auto from ruleset win.emotet_auto at https://github.com/malpedia/signator-rules

⚠ 1615 files match rule HeavensGate from ruleset HeavensGate at https://github.com/kevoreilly/CAPEv2

⚠ 1243 files match rule INDICATOR_SUSPICIOUS_EXE_RegKeyComb_DisableWinDefender from ruleset indicator_suspicious at https://github.com/ditekshen/detection

⚠ 875 files match rule win_socelars_auto from ruleset win.socelars_auto at https://github.com/malpedia/signator-rules

⚠ 608 files match rule Emotet from ruleset rule at https://github.com/JPCERTCC/MalConfScan

⚠ 569 files match rule INDICATOR_EXE_Packed_ConfuserExMod_BedsProtector from ruleset indicator_packed at https://github.com/ditekshen/detection

See all

Crowdsourced Sigma Rules

CRITICAL 8 HIGH 44 MEDIUM 47 LOW 22

⚠ 1 file matches rule Glupteba malware detection by Ariel Millahuel at SOC Prime Threat Detection Marketplace
↳ *Detects a possible Glupteba behavior. This rule detects modifications in the exclusions of Windows Defender, and the attemtp to execute suspicious code.*

⚠ 1 file matches rule TAIDOOR - Chinese RAT by Ariel Millahuel at SOC Prime Threat Detection Marketplace
↳ *This RAT was discovered by CISA. Taidoor is installed on a target's system as a service dynamic link library (DLL) and is comprised of two files. The first file is a loader, which is*
decrypts the second file, and executes it in memory, which is the main Remote Access Trojan (RAT).

⚠ 1 file matches rule Xmrig by Joe Security at Joe Security Rule Set (GitHub)
↳ *Detect Xmrig*

⚠ 1 file matches rule CoViper Malware by Ariel Millahuel at SOC Prime Threat Detection Marketplace
↳ *CoViper is a Wiper that appears during the COVID-19 situation*

⚠ 1 file matches rule Oilrig by Ariel Millahuel at SOC Prime Threat Detection Marketplace
↳ *OilRig is an Iranian threat group operating primarily in the Middle East by targeting organizations in this region that are in a variety of different industries; however, this group*
organizations outside of the Middle East as well. It also appears OilRig carries out supply chain attacks, where the threat group leverages the trust relationship between orga
targets.

⚠ 1 file matches rule Oilrig by Ariel Millahuel at SOC Prime Threat Detection Marketplace
↳ *OilRig is an Iranian threat group operating primarily in the Middle East by targeting organizations in this region that are in a variety of different industries; however, this group*
organizations outside of the Middle East as well. It also appears OilRig carries out supply chain attacks, where the threat group leverages the trust relationship between orga
targets.

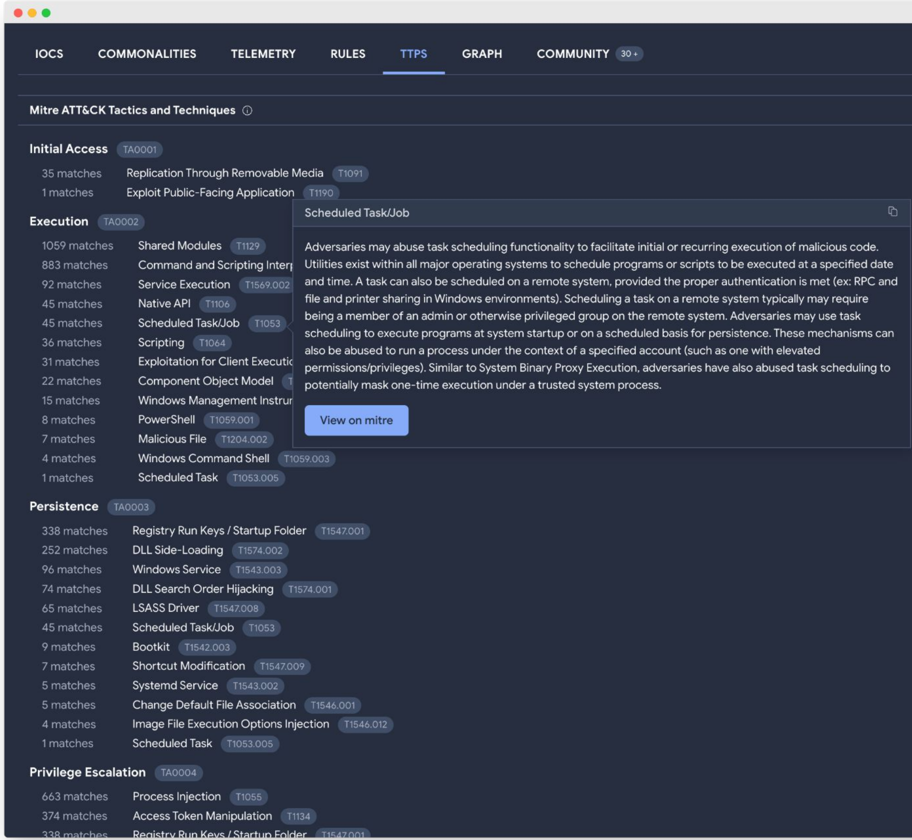
See all

Flag modus operandi with MITRE ATT&CK TTPs

Files processed by VT are detonated in multiple sandboxes and their behavior is mapped to the MITRE ATT&CK matrix.

TTPs do not only characterize single files, they are also aggregated and ranked into commonalities in threat {campaign, toolkit, actor} cards, shedding light into adversary modus operandi. TTP commonalities also for custom groupings of IoCs.

All this data is indexed and searchable in conjunction with other static, dynamic, code and in-the-wild properties. [+]



Mitre ATT&CK Tactics and Techniques ⓘ

Initial Access TA0001

35 matches	Replication Through Removable Media	T1091
1 matches	Exploit Public-Facing Application	T1190

Execution TA0002

1059 matches	Shared Modules	T1129
883 matches	Command and Scripting Interp	
92 matches	Service Execution	T1569.002
45 matches	Native API	T1106
45 matches	Scheduled Task/Job	T1053
36 matches	Scripting	T1064
31 matches	Exploitation for Client Executio	
22 matches	Component Object Model	T
15 matches	Windows Management Instru	
8 matches	PowerShell	T1059.001
7 matches	Malicious File	T1204.002
4 matches	Windows Command Shell	T1059.003
1 matches	Scheduled Task	T1053.005

Scheduled Task/Job

Adversaries may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code. Utilities exist within all major operating systems to schedule programs or scripts to be executed at a specified date and time. A task can also be scheduled on a remote system, provided the proper authentication is met (ex: RPC and file and printer sharing in Windows environments). Scheduling a task on a remote system typically may require being a member of an admin or otherwise privileged group on the remote system. Adversaries may use task scheduling to execute programs at system startup or on a scheduled basis for persistence. These mechanisms can also be abused to run a process under the context of a specified account (such as one with elevated permissions/privileges). Similar to System Binary Proxy Execution, adversaries have also abused task scheduling to potentially mask one-time execution under a trusted system process.

View on mitre

Persistence TA0003

338 matches	Registry Run Keys / Startup Folder	T1547.001
252 matches	DLL Side-Loading	T1574.002
96 matches	Windows Service	T1543.003
74 matches	DLL Search Order Hijacking	T1574.001
65 matches	LSASS Driver	T1547.008
45 matches	Scheduled Task/Job	T1053
9 matches	Bootkit	T1542.003
7 matches	Shortcut Modification	T1547.009
5 matches	Systemd Service	T1543.002
5 matches	Change Default File Association	T1546.001
4 matches	Image File Execution Options Injection	T1546.012
1 matches	Scheduled Task	T1053.005

Privilege Escalation TA0004

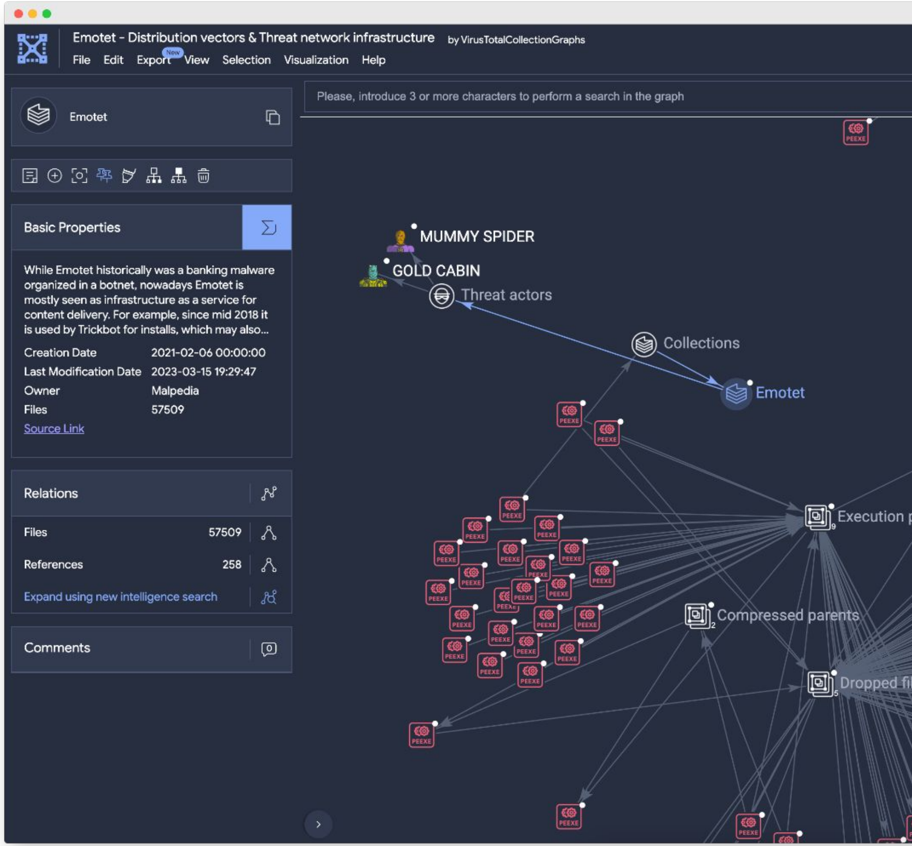
663 matches	Process Injection	T1055
374 matches	Access Token Manipulation	T1134
338 matches	Registry Run Keys / Startup Folder	T1547.001

Collaborate & easily communicate to leadership

Pre-computed VT Graphs for threat campaigns and actors, plus relationships and pivots based on these new notions.

Extend crowdsourced investigations, efficiently collaborate with your team and export visuals for executive presentations.

Leverage VT Graph’s one-click filters to further dissect threats that matter to you. Store subgraphs to focus on activity that is particularly interesting. Create a historical investigative knowledge base for your team. [+]



While Emotet historically was a banking malware organized in a botnet, nowadays Emotet is mostly seen as infrastructure as a service for content delivery. For example, since mid 2018 it is used by Trickbot for installs, which may also...

Creation Date 2021-02-06 00:00:00
Last Modification Date 2023-03-15 19:29:47
Owner Malpedia
Files 57509
Source Link

Relations
Files 57509
References 258
Expand using new intelligence search

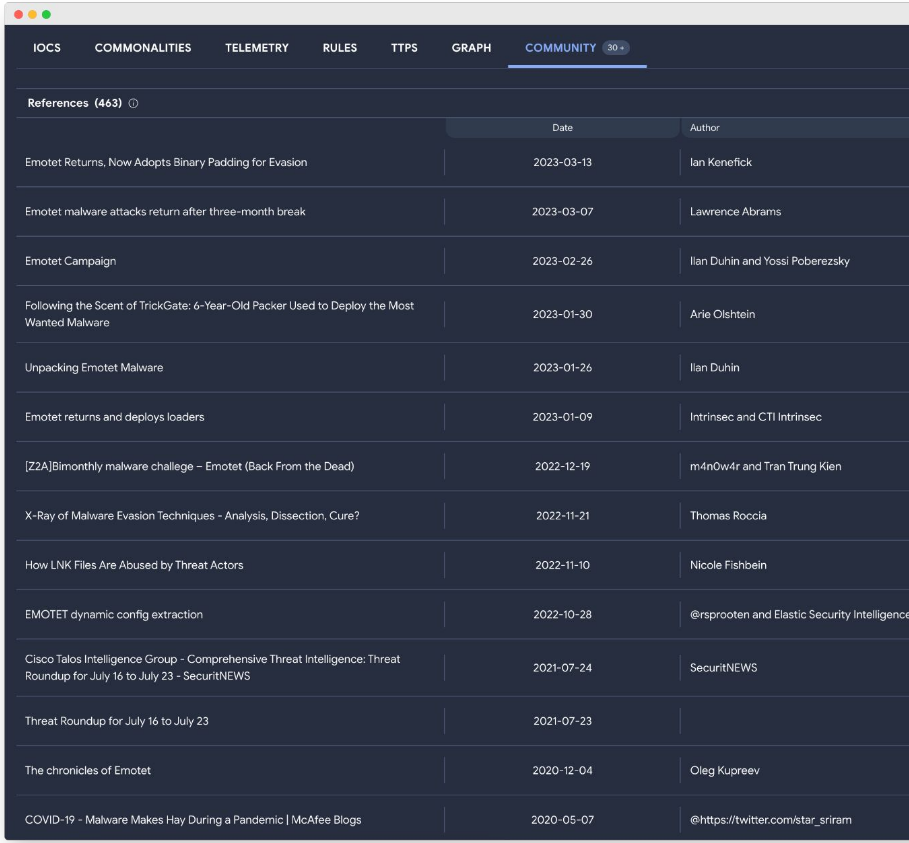
Comments

Fill in the gaps with finished industry articles

All cards include online references speaking about the campaign, actor or IoCs tied to these.

Immediately access conclusions by hundreds of security teams across the industry. Complement automatic static, dynamic, code analysis with human research.

Articles are linked via Internet-wide crawls, learn about a threat as soon as someone speaks about it. Faster and more complete visibility via crowdsourcing. [+]



References (463)

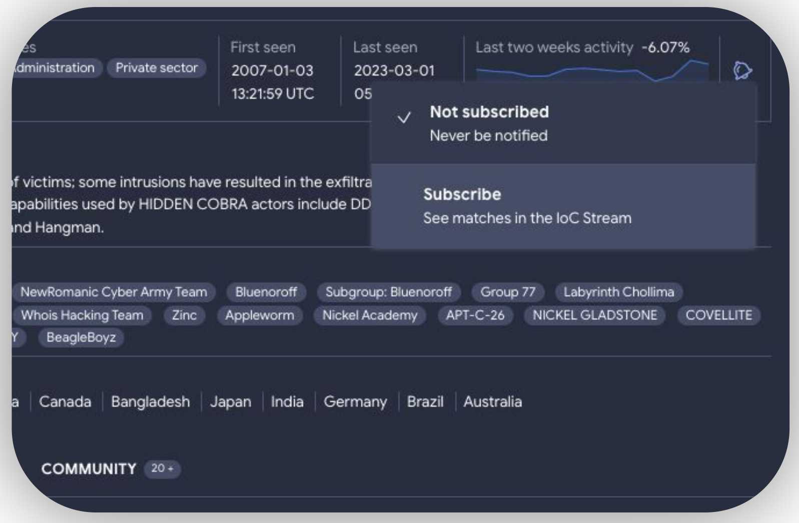
	Date	Author
Emotet Returns, Now Adopts Binary Padding for Evasion	2023-03-13	Ian Kenefick
Emotet malware attacks return after three-month break	2023-03-07	Lawrence Abrams
Emotet Campaign	2023-02-26	Ilan Duhin and Yossi Poberezsky
Following the Scent of TrickGate: 6-Year-Old Packer Used to Deploy the Most Wanted Malware	2023-01-30	Arie Olshtein
Unpacking Emotet Malware	2023-01-26	Ilan Duhin
Emotet returns and deploys loaders	2023-01-09	Intrinsec and CTI Intrinsec
[Z2A]Bimonthly malware challege – Emotet (Back From the Dead)	2022-12-19	m4n0w4r and Tran Trung Kien
X-Ray of Malware Evasion Techniques - Analysis, Dissection, Cure?	2022-11-21	Thomas Roccia
How LNK Files Are Abused by Threat Actors	2022-11-10	Nicole Fishbein
EMOTET dynamic config extraction	2022-10-28	@rsprooten and Elastic Security Intelligence
Cisco Talos Intelligence Group - Comprehensive Threat Intelligence: Threat Roundup for July 16 to July 23 - SecuritNEWS	2021-07-24	SecuritNEWS
Threat Roundup for July 16 to July 23	2021-07-23	
The chronicles of Emotet	2020-12-04	Oleg Kupreev
COVID-19 - Malware Makes Hay During a Pandemic | McAfee Blogs	2020-05-07	@https://twitter.com/star_sriram

Generate relevant intel tailored for your org

Subscribe to threat {campaigns, toolkits, actors}, all new IoCs tied to them will flow into your IoC Stream.

Subscriptions are an effortless vehicle to generate custom threat feeds that can be ingested across your security stack via off-the-shelf integrations or common feed formats (e.g. STIX).

Go beyond pre-packaged and often noisy/irrelevant threat feeds, customize your threat landscape and focus on the threats that truly matter to you. [+]



es
dministration | Private sector

First seen
2007-01-03
13:21:59 UTC

Last seen
2023-03-01
05

Last two weeks activity -6.07%

✓ Not subscribed
Never be notified

Subscribe
See matches in the IoC Stream

f victims; some intrusions have resulted in the exfiltra
apabilities used by HIDDEN COBRA actors include DD
nd Hangman.

NewRomanic Cyber Army Team | Bluenoroff | Subgroup: Bluenoroff | Group 77 | Labyrinth Chollima
Whois Hacking Team | Zinc | Appleworm | Nickel Academy | APT-C-26 | NICKEL GLADSTONE | COVELLITE
Y | BeagleBoyz

a | Canada | Bangladesh | Japan | India | Germany | Brazil | Australia

COMMUNITY 20+

Faster insights & superior visibility

Go beyond the conclusions of a handful of researchers, plug your operations into the collective community's brain

Crowdsourced threat landscape visibility

2K+ campaign cards / month

1K+ active researchers

500+ de-duped threat actors

Telemetry from 3.6M+ users in 230+ countries

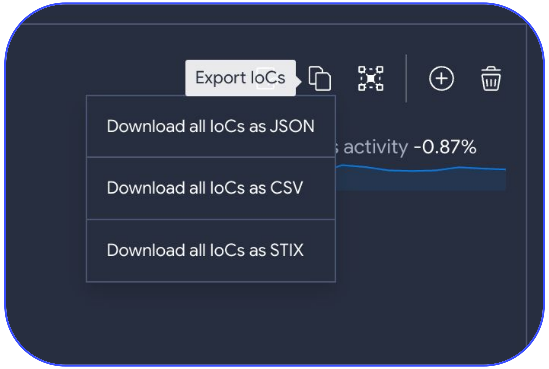
40K+ daily reference sites

7M+ classified IoCs / month

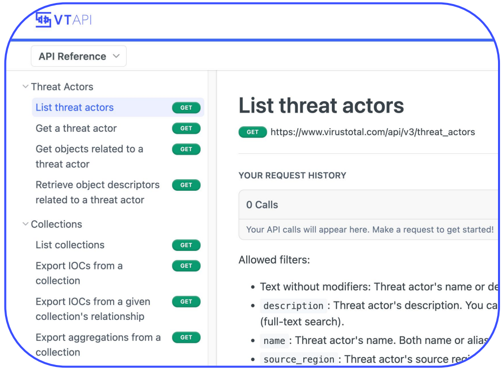
Make your stack smarter, be safer

Effortlessly automate and enrich everything, everywhere

Exportable and user-friendly



One-click exports to common formats for ingestion in your security stack (SIEM, TIP, NGFW...)



Threat Actors
- List threat actors GET
- Get a threat actor GET
- Get objects related to a threat actor GET
- Retrieve object descriptors related to a threat actor GET

Collections
- List collections GET
- Export IOCs from a collection GET
- Export IOCs from a given collection's relationship GET
- Export aggregations from a collection GET

List threat actors

GET https://www.virustotal.com/api/v3/threat_actors

YOUR REQUEST HISTORY

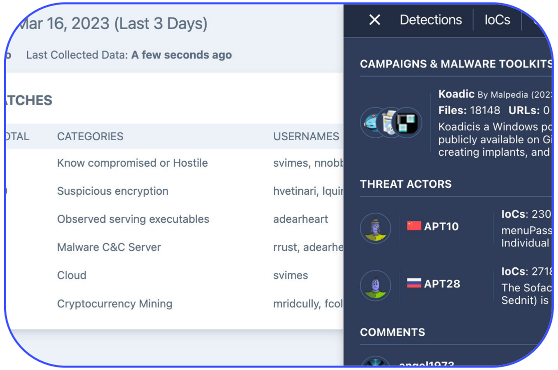
0 Calls

Your API calls will appear here. Make a request to get started!

Allowed filters:

- Text without modifiers: Threat actor's name or de
- `description` : Threat actor's description. You ca (full-text search).
- `name` : Threat actor's name. Both name or alias
- `source_region` : Threat actor's source reg

Automate detection and custom workflows via **API**, focus on higher severity (threat actors) first.



Mar 16, 2023 (Last 3 Days)

Last Collected Data: **A few seconds ago**

TCHES

TAL	CATEGORIES	USERNAMES
	Know compromised or Hostile	svimes, nnobb
	Suspicious encryption	hvetinari, lquir
	Observed serving executables	adearheart
	Malware C&C Server	rrust, adearhe
	Cloud	svimes
	Cryptocurrency Mining	mridcully, fcol

CAMPAIGNS & MALWARE TOOLKITS

Koadic By Malpedia (202
Files: 18148 **URLs:** 0
Koadicis a Windows po publicly available on Gi creating implants, and

THREAT ACTORS

APT10 — **IoCs**: 230 menuPass Individual

APT28 — **IoCs**: 2718 The Sofac Sednit) is

COMMENTS

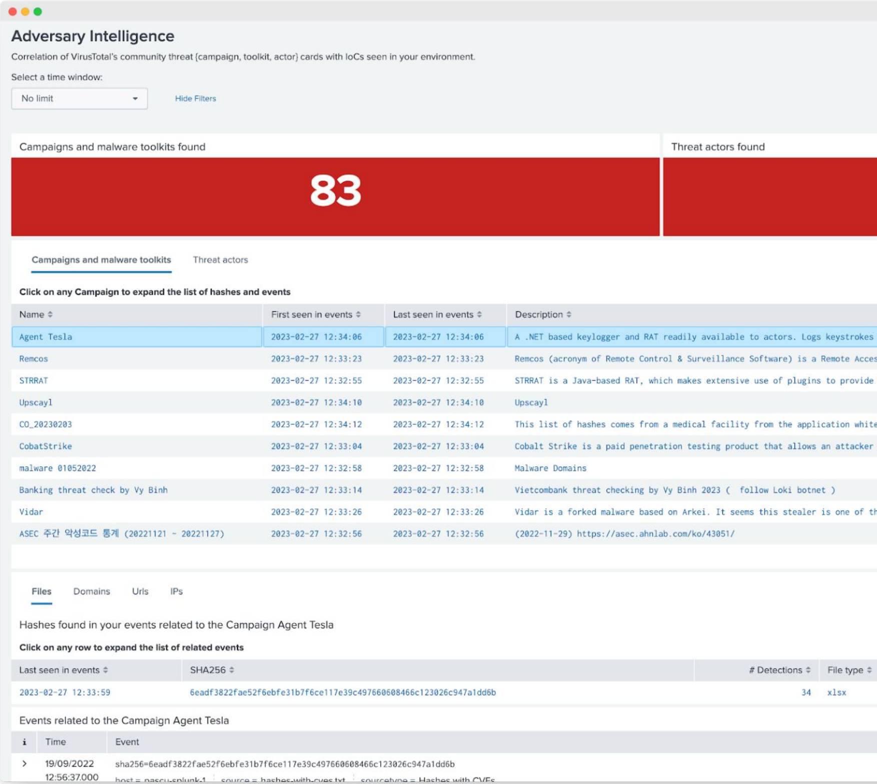
angel1973

Ubiquitously enrich any interface with adversary intelligence via the VirusTotal **browser extension**.

Unearth threats dwelling undetected in your environment

VT’s technology integrations correlate your telemetry with threat actor context to automate triage, expedite investigations and enhance detection.

E.g. VT4Splunk automatically enrich file hashes, domains, IPs and URLs in events with VT reputation and context. Conduct hunt missions on the correlated data. Prioritize indicators based on severity. Dashboards summarizing exploited vulnerabilities and **suspected actors in your environment**, plus their TTPs (MITRE ATT&CK). **Similar integrations for other TOP SIEMs.** [+]



Adversary Intelligence

Correlation of VirusTotal's community threat (campaign, toolkit, actor) cards with IoCs seen in your environment.

Select a time window:

No limit ▾

Hide Filters

Campaigns and malware toolkits found

83

Threat actors found

Campaigns and malware toolkits | Threat actors

Click on any Campaign to expand the list of hashes and events

Name ⇕	First seen in events ⇕	Last seen in events ⇕	Description ⇕
Agent Tesla	2023-02-27 12:34:06	2023-02-27 12:34:06	A .NET based keylogger and RAT readily available to actors. Logs keystrokes
Remcos	2023-02-27 12:33:23	2023-02-27 12:33:23	Remcos (acronym of Remote Control & Surveillance Software) is a Remote Acces
STRRAT	2023-02-27 12:32:55	2023-02-27 12:32:55	STRRAT is a Java-based RAT, which makes extensive use of plugins to provide
Upscayl	2023-02-27 12:34:10	2023-02-27 12:34:10	Upscayl
CO_20230203	2023-02-27 12:34:12	2023-02-27 12:34:12	This list of hashes comes from a medical facility from the application white
CobatStrike	2023-02-27 12:33:04	2023-02-27 12:33:04	Cobalt Strike is a paid penetration testing product that allows an attacker
malware 01052022	2023-02-27 12:32:58	2023-02-27 12:32:58	Malware Domains
Banking threat check by Vy Binh	2023-02-27 12:33:14	2023-02-27 12:33:14	Vietcombank threat checking by Vy Binh 2023 (follow Loki botnet)
Vidar	2023-02-27 12:33:26	2023-02-27 12:33:26	Vidar is a forked malware based on Arkei. It seems this stealer is one of th
ASEC 주간 악성코드 통계 (20221121 ~ 20221127)	2023-02-27 12:32:56	2023-02-27 12:32:56	(2022-11-29) https://asec.ahnlab.com/ko/43051/

Files | Domains | Urls | IPs

Hashes found in your events related to the Campaign Agent Tesla

Click on any row to expand the list of related events

Last seen in events ⇕	SHA256 ⇕	# Detections ⇕	File type ⇕
2023-02-27 12:33:59	6eadf3822fae52f6ebfe31b7f6ce117e39c497660608466c123026c947a1dd6b	34	xlsx

Events related to the Campaign Agent Tesla

i	Time	Event

>	19/09/2022
	12:56:37.000
		sha256=6eadf3822fae52f6ebfe31b7f6ce117e39c497660608466c123026c947a1dd6b
		host = pascu-splunk-1 ⋮ source = hashes-with-cves.txt ⋮ sourcetype = Hashes with CVEs

Outcomes & value proposition

Mature your security program and radically improve your security posture

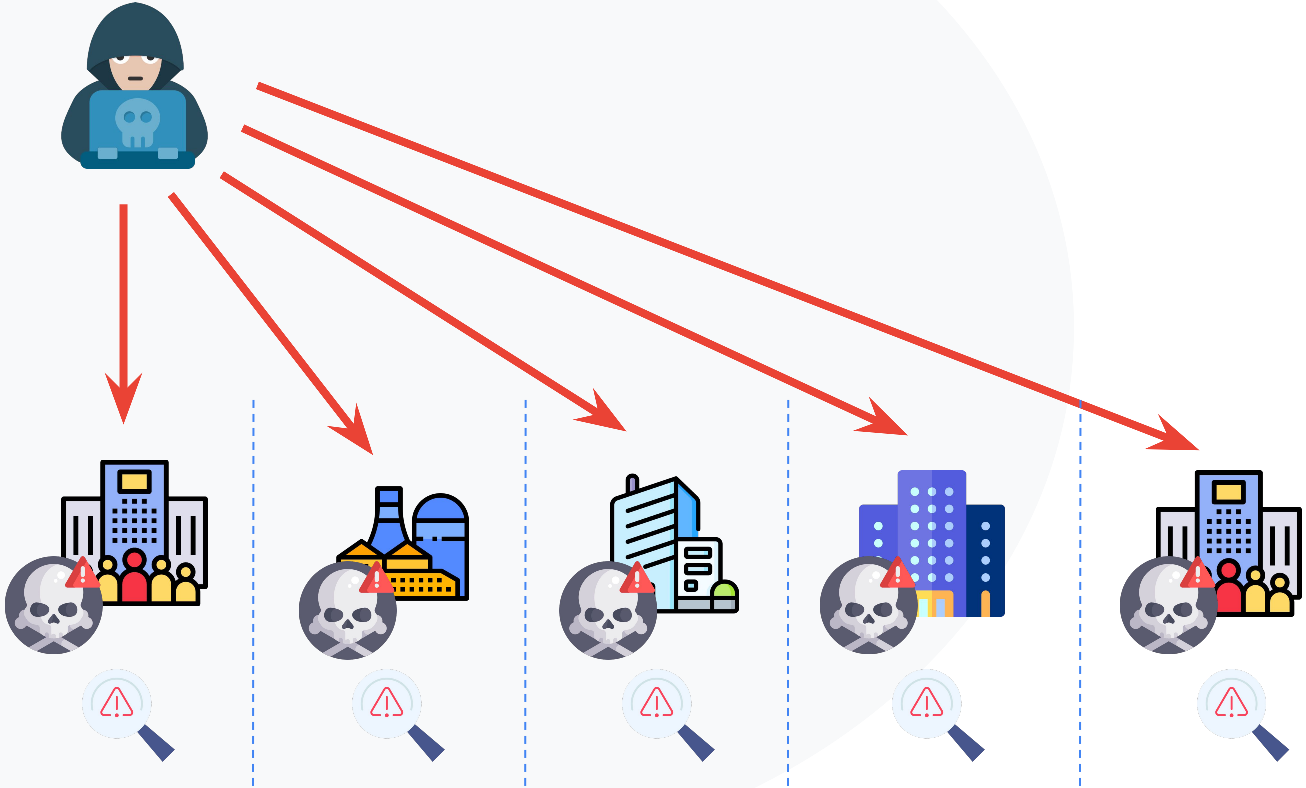
Mature your security program

Security org challenges		Solving with VT Threat Landscape
Alert fatigue and false positives SOCs only able to handle 14% of alerts	❯	**Prioritize alerts based on severity** Address incidents tied to motivated threat actors first
Quality & speed of incident response handling Analyst-intensive and often inaccurate	❯	**IoCs, commonalities and TTPs for 360 response** Supercharge blast radius id, containment and remediation
Missed threats due to lack of context Generic/anomaly/ML detections discarded as low severity	❯	**Attribution to minimize false negatives** Associated threat actors/campaigns on IoC reports
Evolving threat landscape Difficult to keep up with new attack vectors & techniques	❯	**Emerging threat articles and trending campaigns** Filters and rankings to explore latest developments
Many threat intel feeds, few relevant ones Further exacerbate the problem of alert fatigue	❯	**Tailored feeds via {campaign, actor} subscriptions** Focus on specific threats, industries and regions
Security program is too reactive Growing attacker dwell time and no prevention	❯	**Go beyond IoCs, conduct proactive hunt missions** Leverage commonalities, TTPs, rules for hunting
Cybersecurity skills gap CTI analysts and advanced threat hunters are scarce	❯	**Digested intelligence & one-click filters for juniors** Easily filter VT's corpus to depict your threat landscape
Budget constraints & suboptimal spending Expensive generic tools that are threat landscape agnostic	❯	**Situational awareness to invest wisely** Prioritize your $$ to address threats that matter to you

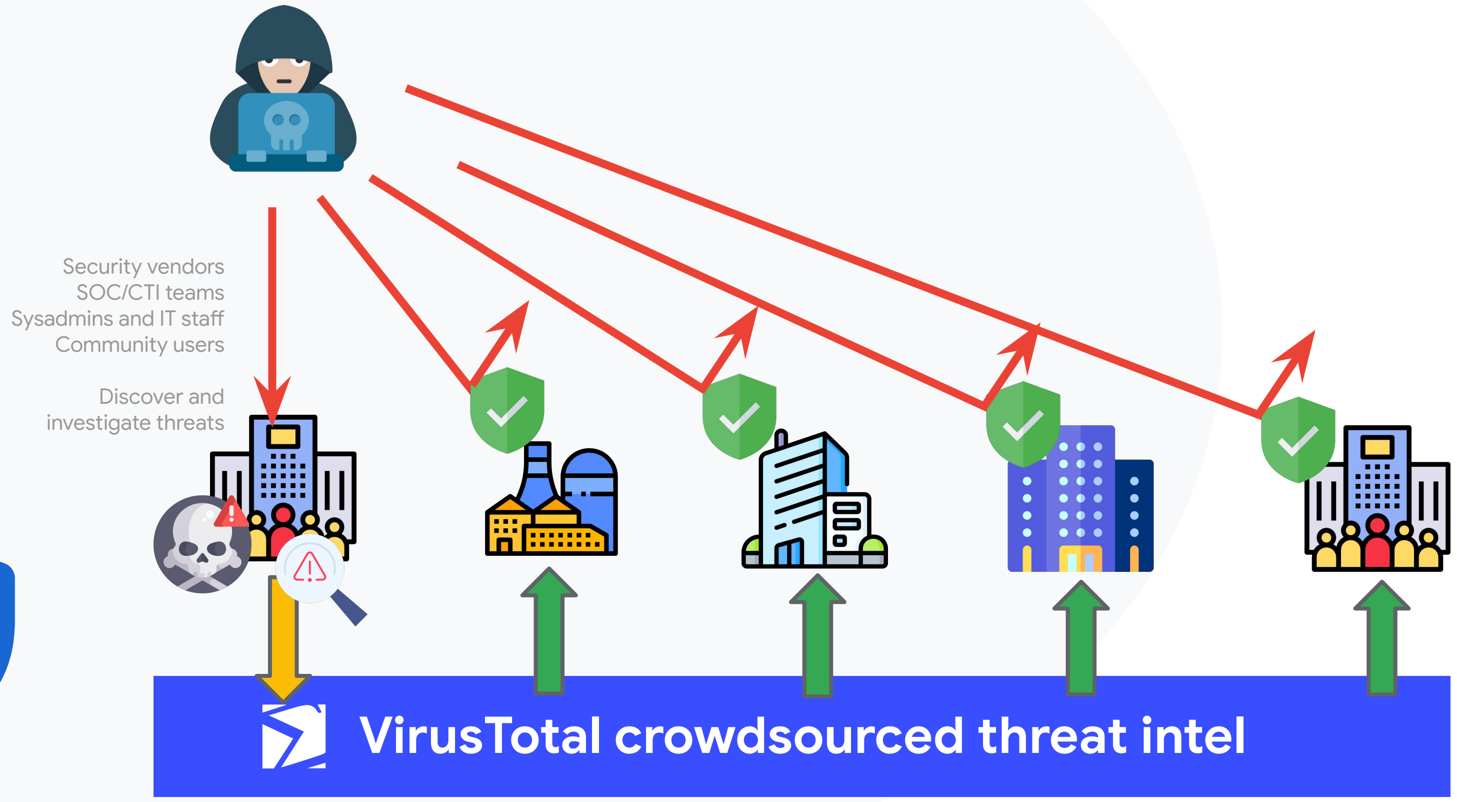
What makes us different?

Timely, more interactive, more actionable

Traditional response to attacks



The power of crowdsourcing



Security vendors
SOC/CTI teams
Sysadmins and IT staff
Community users

Discover and
investigate threats

VirusTotal crowdsourced threat intel

What Makes VT Threat Lanscape Different

Unlike traditional threat intelligence vendors, VirusTotal's adversary intelligence is not the product of a handful of researchers/analysts and a limited set of investigations.

Instead, VirusTotal ensures timeliness and comprehensiveness by leveraging the collective knowledge of the community and Google's planet-scale infrastructure digesting technical toolkit properties into proactive hunting artifacts.

Collective knowledge

1K+ community researchers contributing 2K+ campaign/toolkit collections per month, real-time as emerging threats are spotted.

Community telemetry

Geo+IoC+time web and API lookup activity in campaign / actor cards coming from 3.6M+ users from 230+ countries. Breakdowns and focus filters.

Tailored threat feeds

Generate IoC streams based on subscriptions to relevant threat {actors, campaigns}. Automatic matching in your environment via API and integrations.

Proactive hunting artifacts

Automatic extraction of malware toolkit commonalities for hunting purposes, TTP identification and {YARA, Sigma, IDS} rules.

Filters ensuring relevance

Filter intelligence cards by industry, targeted regions, sponsor, motivations, activity time spans, etc. to focus on threats that matter to your organization.

Interactive TI one-stop-shop

Single provider for technical, tactical, operational and strategic intelligence - peak cost-efficiency. Unrivaled investigative interactivity.

Rich » Timely » Relevant » Actionable » Proactive

Contact us