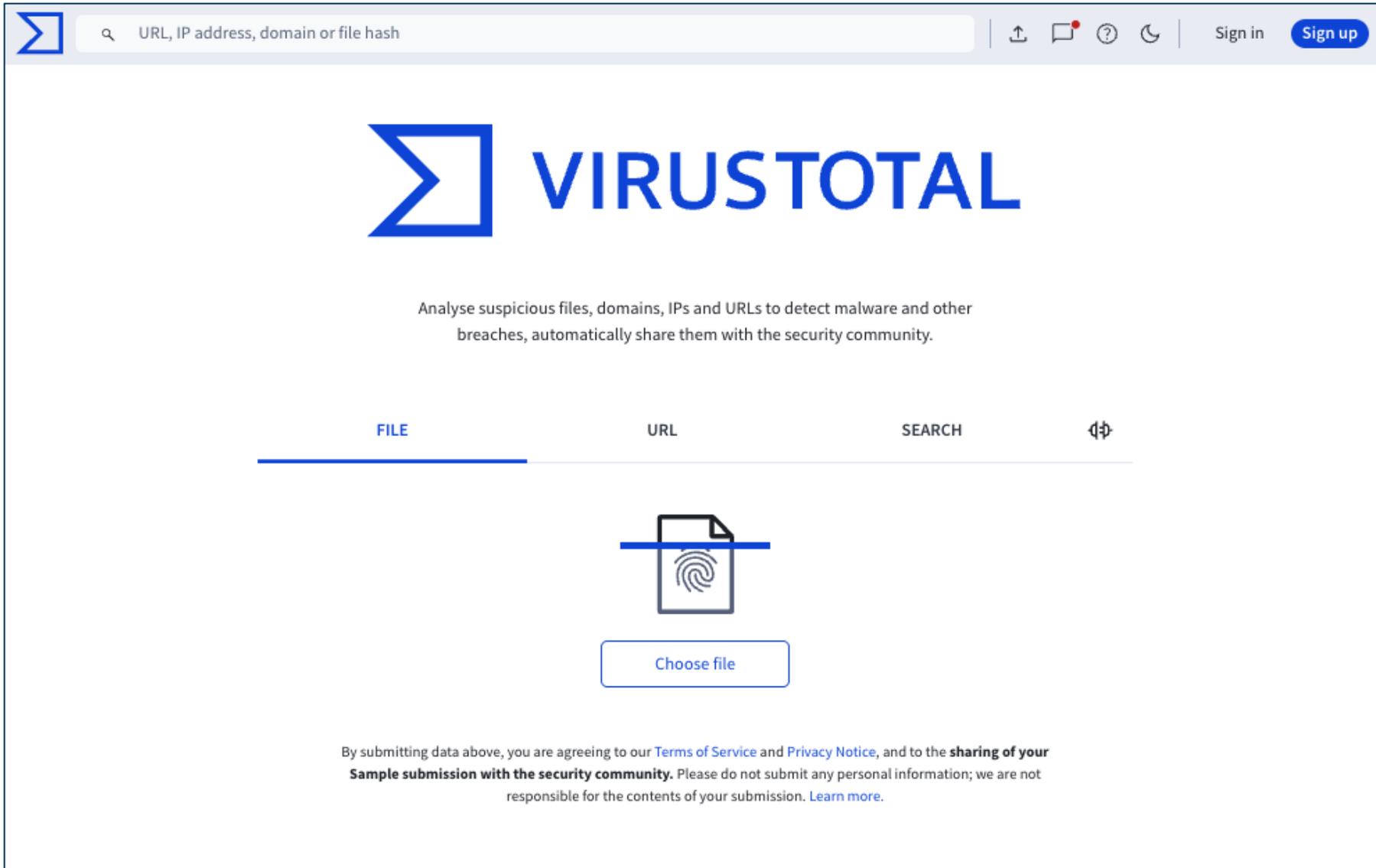


Actively Understanding the Dynamics and Risks of the Threat Intelligence Ecosystem

Tillson Galloway, Allen Chang, Omar Alrawi, Thanos Avgetidis, Manos Antonakakis, Fabian Monroe



The screenshot shows the VirusTotal website interface. At the top, there is a search bar with the placeholder text "URL, IP address, domain or file hash" and a search icon. To the right of the search bar are navigation icons for upload, chat, help, and a "Sign in" button, followed by a "Sign up" button. The main heading is the VirusTotal logo, which consists of a blue square with a white arrow pointing right, followed by the word "VIRUSTOTAL" in blue. Below the logo is the text: "Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community." There are four tabs: "FILE", "URL", "SEARCH", and a shield icon. The "FILE" tab is selected, indicated by a blue underline. Below the tabs is a large icon of a document with a fingerprint, representing a file upload. Below this icon is a button labeled "Choose file". At the bottom, there is a disclaimer: "By submitting data above, you are agreeing to our [Terms of Service](#) and [Privacy Notice](#), and to the **sharing of your Sample submission with the security community**. Please do not submit any personal information; we are not responsible for the contents of your submission. [Learn more](#)."

URL, IP address, domain or file hash

62 / 72
Community Score

62/72 security vendors flagged this file as malicious

000001e41599558a88da7cf4549285f6bab7bc348f4fd780a...
idle.exe

Size: 269.97 KB | Last Analysis Date: 2 months ago

peexe, spreader, persistence, runtime-modules, detect-debug-environment, upx, direct-cpu-clock-access, overlay

EXE

DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY 10+

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label: trojan.genie/scar | Threat categories: trojan | Family labels: genie, scar, poker

Security vendors' analysis

Acronis (Static ML)	Suspicious	AhnLab-V3	Trojan/Win32.Scar.C149469
Alibaba	Trojan:Win32/Scar.2bd4	AliCloud	Worm:Win/Ymacco.ET
ALYac	Gen:Variant.Genie.10	Antiy-AVL	Trojan[PSW]/Win32.Delf
Arcabit	Trojan.Genie.10	Arctic Wolf	Unsafe
Avast	Win32:Evo-gen [Trj]	AVG	Win32:Evo-gen [Trj]
Avira (no cloud)	HEUR/AGEN.1349232	BitDefender	Gen:Variant.Genie.10
Bkav Pro	W32.AIDetectMalware	ClamAV	Win.Trojan.Agent-959440
CrowdStrike Falcon	Win/malicious_confidence_100%_WU	CTY	Evo-trojan-scar

Millions of IoCs are processed by vendors daily

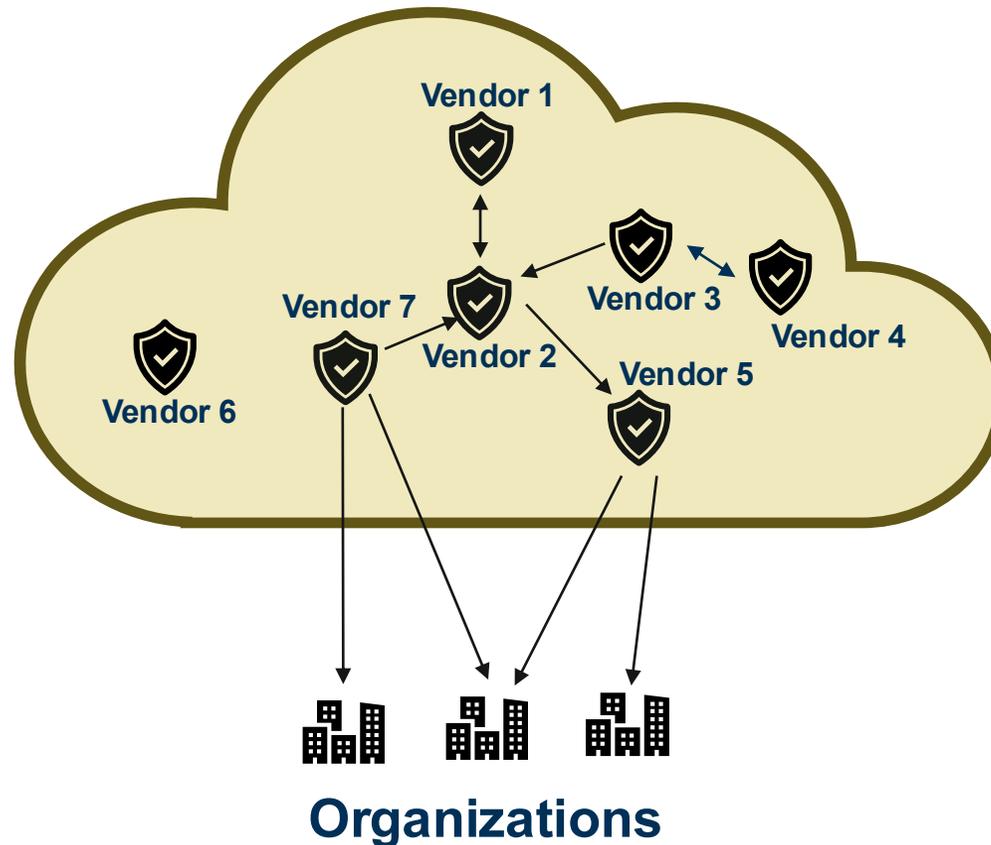


Organizing the TI ecosystem

What are the **threats** facing this ecosystem?

How much **delay** is introduced by each vendor?

How **independent** are observations from crowdsourced TI platforms?



Types of Indicators of Compromise



Files



File
hashes

Endpoint

Types of Indicators of Compromise

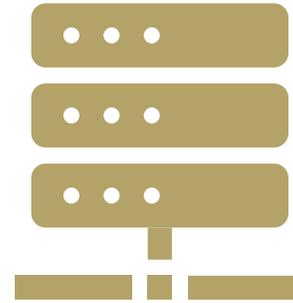


Files

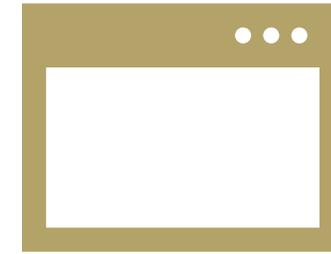


File hashes

Endpoint



IPs



URLs

Network



Domains

Types of Indicators of Compromise

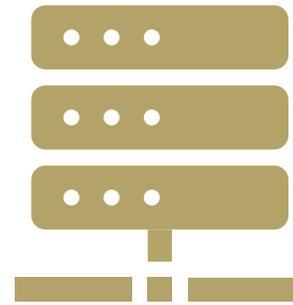


Files

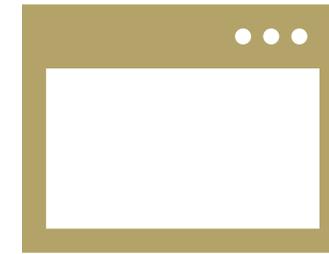


File hashes

Endpoint



IPs



URLs



Domains

Network

Focus of this presentation

Learn more in the paper!

Measurement answers three research questions

 **Relationships** — *how are data sharing relationships leveraged?*



Measurement answers three research questions

 **Relationships** — *how are data sharing relationships leveraged?*

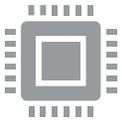
 **Timeliness** — *how quickly do vendors extract, share, and integrate TI with security appliances?*



Measurement answers three research questions

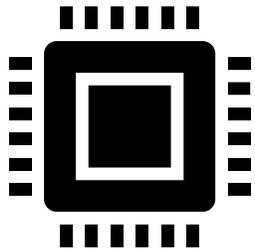
 **Relationships** — *how are data sharing relationships leveraged?*

 **Timeliness** — *how quickly do vendors extract, share, and integrate TI with security appliances?*

 **Extraction** — *how comprehensively do vendors extract TI from binaries?* [Learn more in the paper!](#)



Key idea: map ecosystem supply chains using lightweight active probes to free, public services



Research
profiler binary

Key idea: map ecosystem supply chains using lightweight active probes to free, public services



Uploads to

VIRUSTOTAL

Analyze suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

FILE URL SEARCH

Choose file

Submit Files and URLs for Analysis

Submit Files Submit URLs

DESCRIPTION (TYPE)	TIME SUBMITTED	FILE COMPLETED	STATUS	TLP
NO ENTRIES FOUND				

You do not have any submissions. You can submit files or URLs using the buttons located above.

ANY.RUN INTERACTIVE MALWARE ANALYSIS

Start your analysis

Interact with Windows, Linux, and and immediately see the feedback

Deep interactive investigation in full

Submit File / Email

Detonate an object to observe its malicious activity

+27 more vendors

Key idea: map ecosystem supply chains using lightweight active probes to free, public services



Uploads to

VIRUSTOTAL

Submit Files and URLs for Analysis

ANY.RUN
INTERACTIVE MALWARE ANALYSIS

+27 more vendors

Runs binary



Key idea: map ecosystem supply chains using lightweight active probes to free, public services



Uploads to

+27 more vendors

Runs binary



Dynamic Analysis

Extract IoCs

Key idea: map ecosystem supply chains using lightweight active probes to free, public services



Uploads to

+27 more vendors

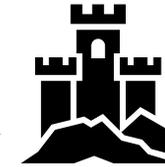
Runs binary

Extract IoCs



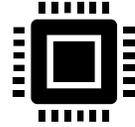
Observer

DNS/HTTP emissions

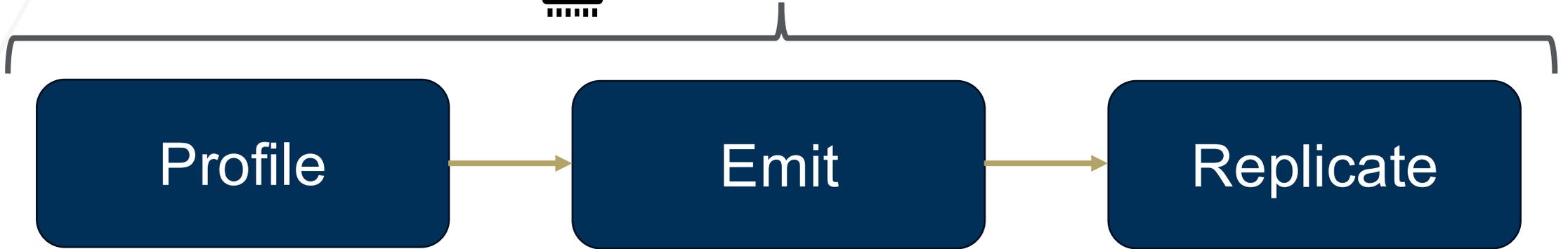


Dynamic Analysis

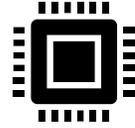
Binary File: Profiling Process



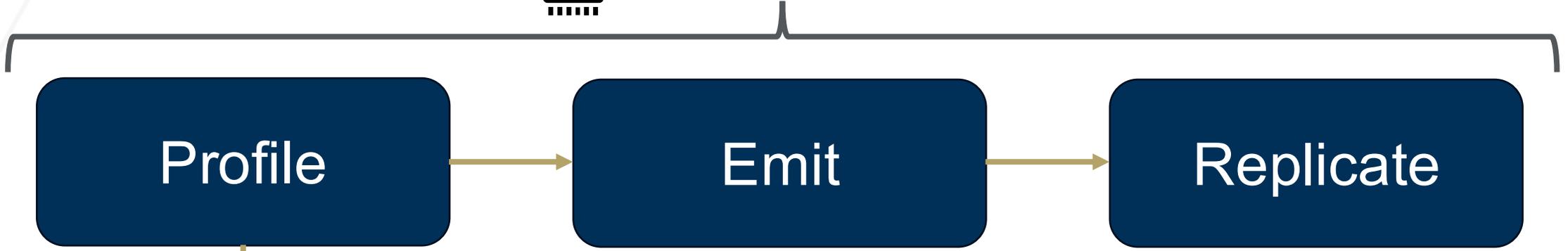
Research profiler binary



Binary File: Profiling Process

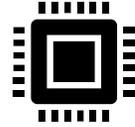


Research profiler binary



Fingerprint	Value	Hashed
RAM	64GB	bf
OS install date	Aug 6, 2025	axzy
Manufacturer	LENOVO	q4

Binary File: Profiling Process



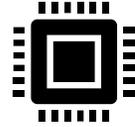
Research profiler binary



Fingerprint	Value	Hashed
RAM	64GB	bf
OS install date	Aug 6, 2025	axy
Manufacturer	LENOVO	q4

DNS bfaxzyq4.1dd.fun
HTTP <http://bfaxzyq4.1dd.fun/>

Binary File: Profiling Process



Research profiler binary

Profile

Emit

Replicate

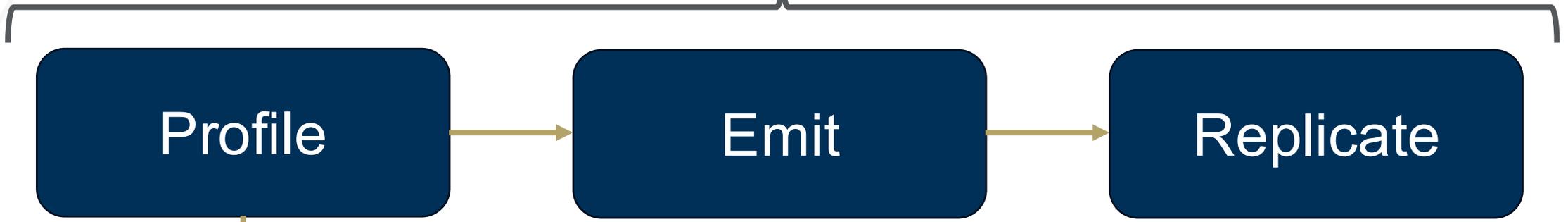
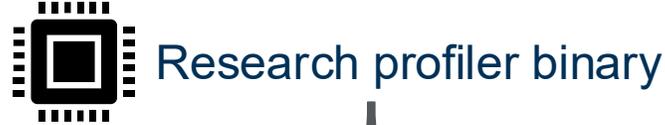
Fingerprint	Value	Hashed
RAM	64GB	bf
OS install date	Aug 6, 2025	axy
Manufacturer	LENOVO	q4

DNS **bfaxyq4.1dd.fun**
HTTP <http://bfaxyq4.1dd.fun/>

Drop binary



Binary File: Profiling Process



Fingerprint	Value	Hashed
RAM	64GB	bf
OS install date	Aug 6, 2025	axyz
Manufacturer	LENOVO	q4

DNS **bfaxzyq4**.1dd.fun
 HTTP <http://bfaxzyq4.1dd.fun/>

Fingerprint	Value	Hashed
RAM	16GB	f4
OS install date	Jan 1, 1970	fa4f
Manufacturer	Dell, Inc.	2f

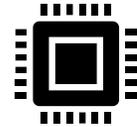
DNS **f4fa4f2fbfaxzyq4**.1dd.fun
 HTTP <http://f4fa4f2fbfaxzyq4.1dd.fun/>

Drop binary



Binary File: Profiling Process

bfaxyq4



Research profiler binary



Fingerprint	Value	Hashed
RAM	64GB	bf
OS install date	Aug 6, 2025	axy
Manufacturer	LENOVO	q4

DNS **bfaxyq4**.1dd.fun
 HTTP <http://bfaxyq4.1dd.fun/>

Fingerprint	Value	Hashed
RAM	16GB	f4
OS install date	Jan 1, 1970	fa4f
Manufacturer	Dell, Inc.	2f

DNS **f4fa4f2f**bfaxyq4.1dd.fun
 HTTP <http://f4fa4f2fbfaxyq4.1dd.fun/>

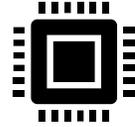
Drop binary



Binary File: Profiling Process

f4fa4f2f

bfaxyq4



Research profiler binary

Profile

Emit

Replicate

Fingerprint	Value	Hashed
RAM	64GB	bf
OS install date	Aug 6, 2025	axy
Manufacturer	LENOVO	q4

DNS **bfaxyq4**.1dd.fun
 HTTP <http://bfaxyq4.1dd.fun/>

Fingerprint	Value	Hashed
RAM	16GB	f4
OS install date	Jan 1, 1970	fa4f
Manufacturer	Dell, Inc.	2f

DNS **f4fa4f2f****bfaxyq4**.1dd.fun
 HTTP <http://f4fa4f2fbfaxyq4.1dd.fun/>

Drop binary

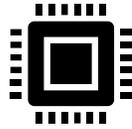


Binary File: Profiling Process

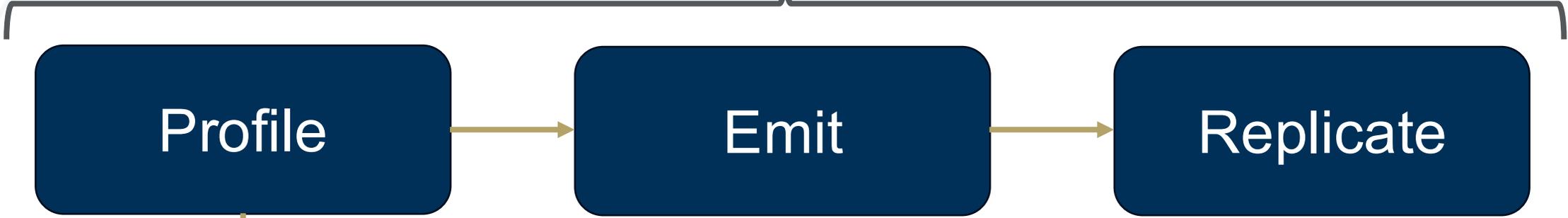
84fofmsd

f4fa4f2f

bfaxyq4



Research profiler binary



Fingerprint	Value	Hashed
RAM	64GB	bf
OS install date	Aug 6, 2025	axy
Manufacturer	LENOVO	q4

DNS **bfaxyq4**.1dd.fun
 HTTP <http://bfaxyq4.1dd.fun/>

Drop binary



Fingerprint	Value	Hashed
RAM	16GB	f4
OS install date	Jan 1, 1970	fa4f
Manufacturer	Dell, Inc.	2f

DNS **f4fa4f2f****bfaxyq4**.1dd.fun
 HTTP <http://f4fa4f2fbfaxyq4.1dd.fun/>

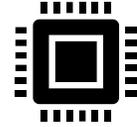
Profiling Process

924fnsk

84fofmsd

f4fa4f2f

bfaxyq4



Research profiler binary

Profile

Emit

Replicate

Fingerprint	Value	Hashed
RAM	64GB	bf
OS install date	Aug 6, 2025	axy
Manufacturer	LENOVO	q4

DNS **bfaxyq4.1dd.fun**
 HTTP <http://bfaxyq4.1dd.fun/>

Drop binary

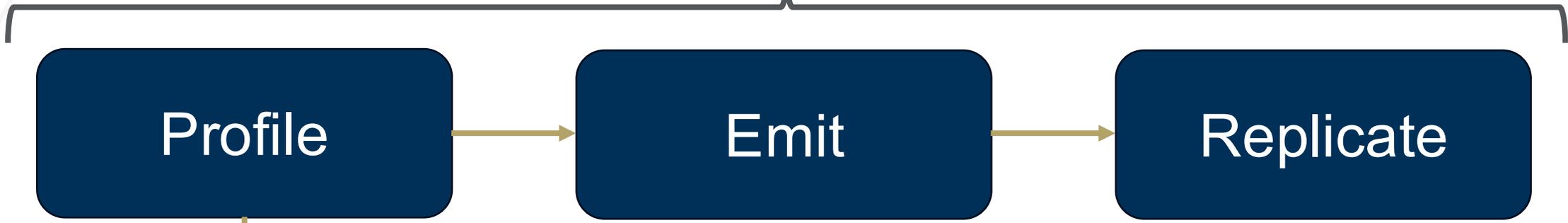
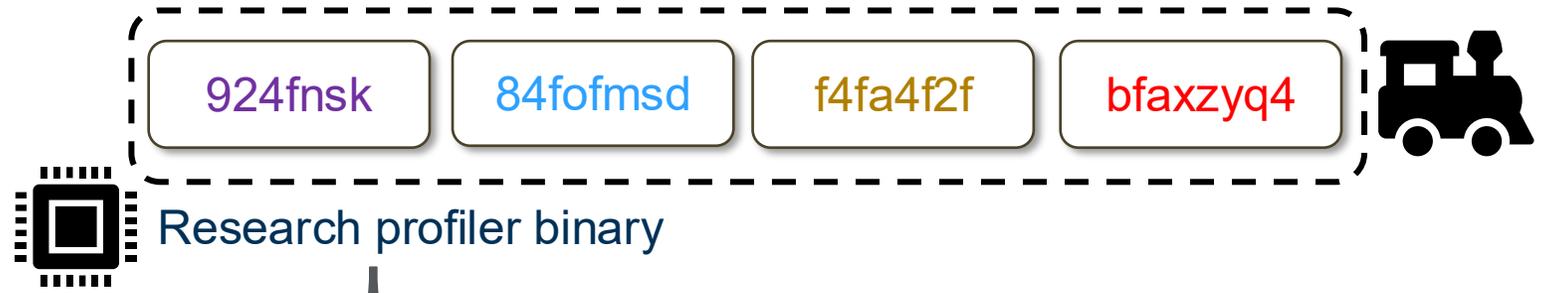


Fingerprint	Value	Hashed
RAM	16GB	f4
OS install date	Jan 1, 1970	fa4f
Manufacturer	Dell, Inc.	2f

DNS **f4fa4f2fbfaxyq4.1dd.fun**
 HTTP <http://f4fa4f2fbfaxyq4.1dd.fun/>

Profiling Process

Provenance Trail



Fingerprint	Value	Hashed
RAM	64GB	bf
OS install date	Aug 6, 2025	axyz
Manufacturer	LENOVO	q4

DNS **bfaxzyq4**.1dd.fun
 HTTP <http://bfaxzyq4.1dd.fun/>

Drop binary

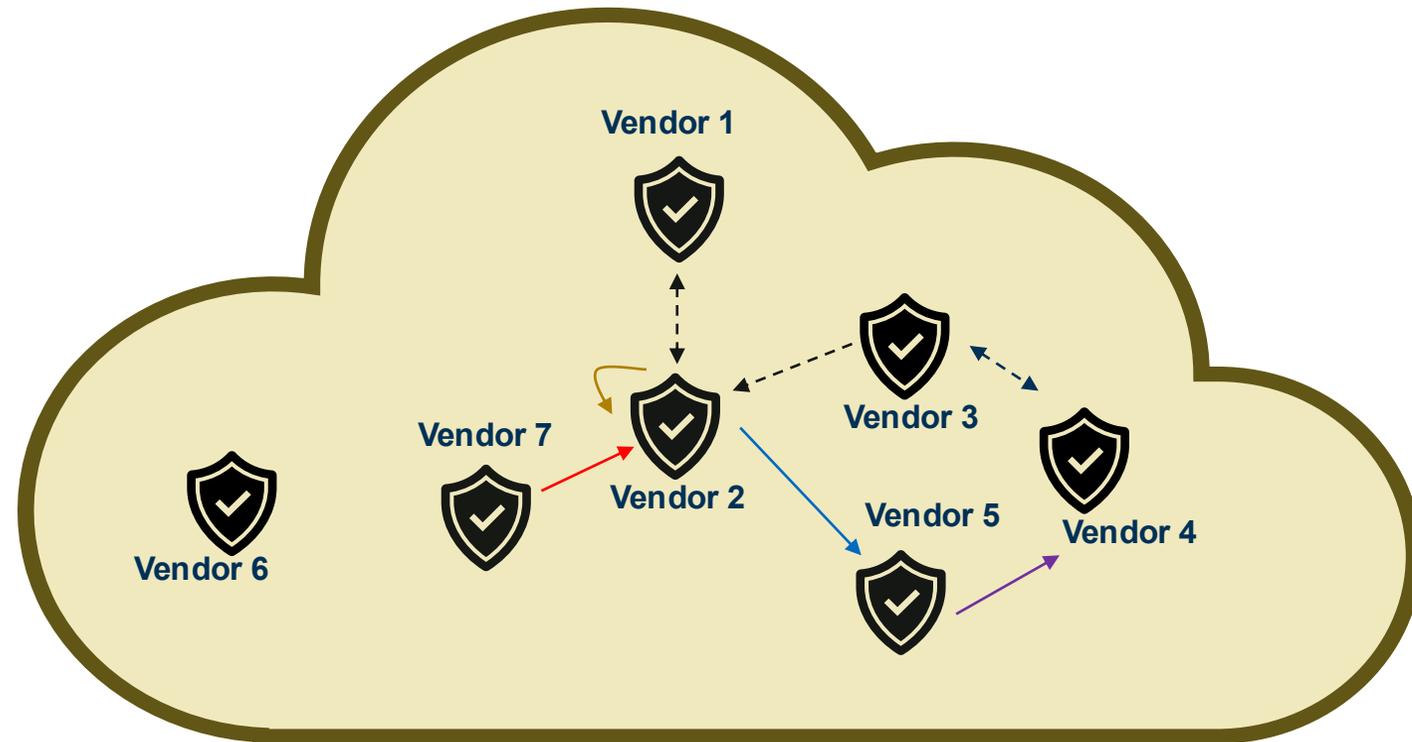


Fingerprint	Value	Hashed
RAM	16GB	f4
OS install date	Jan 1, 1970	fa4f
Manufacturer	Dell, Inc.	2f

DNS **f4fa4f2fbfaxzyq4**.1dd.fun
 HTTP <http://f4fa4f2fbfaxzyq4.1dd.fun/>

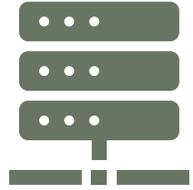
Constructing an ecosystem map

- bfaxyq4
- f4fa4f2f
- 84fofmsd
- 924fnsk



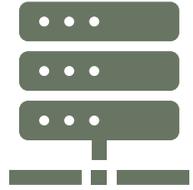
Each execution annotated with vendor name using hand-labeling and clustering

How to minimize potential harm to ecosystem?



One HTTP/DNS query per execution

How to minimize potential harm to ecosystem?

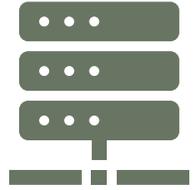


One HTTP/DNS query per execution



Max provenance trail length of five

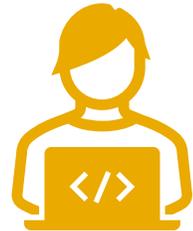
How to minimize potential harm to ecosystem?



One HTTP/DNS query per execution

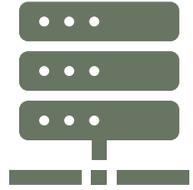


Max provenance trail length of five

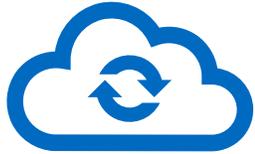


Disclaimer and opt-out are included in both binary and network communications

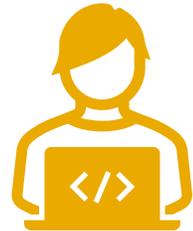
How to minimize potential harm to ecosystem?



One HTTP/DNS query per execution



Max provenance trail length of five



Disclaimer and opt-out are included in both binary and network communications



Responsible disclosure process and anonymization of all vendors

Experiments considered three classes of vendors



+2 anonymous vendors

Sandboxes

Experiments considered three classes of vendors



+2 anonymous vendors

Sandboxes



TI Platforms

Experiments considered three classes of vendors



+2 anonymous vendors

Sandboxes

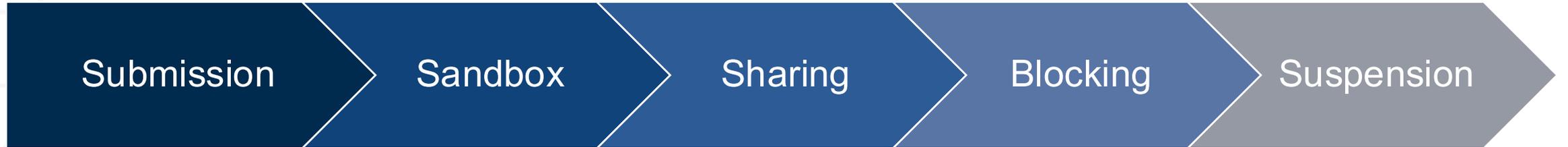


TI Platforms



Antiviruses

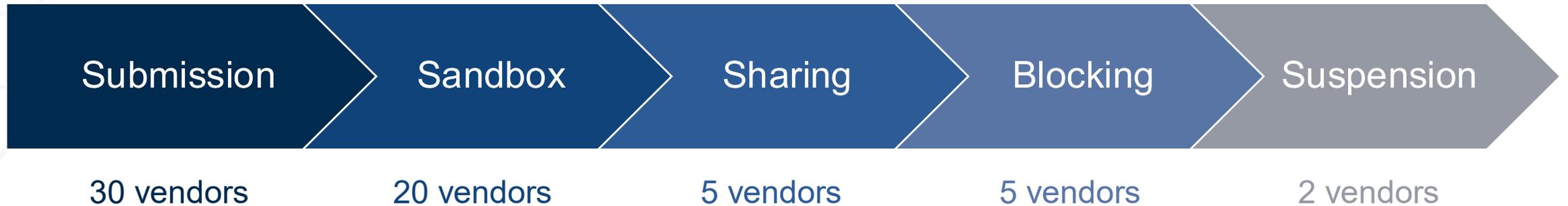
Lifecycle of an IoC



Lifecycle of an IoC



Lifecycle of an IoC



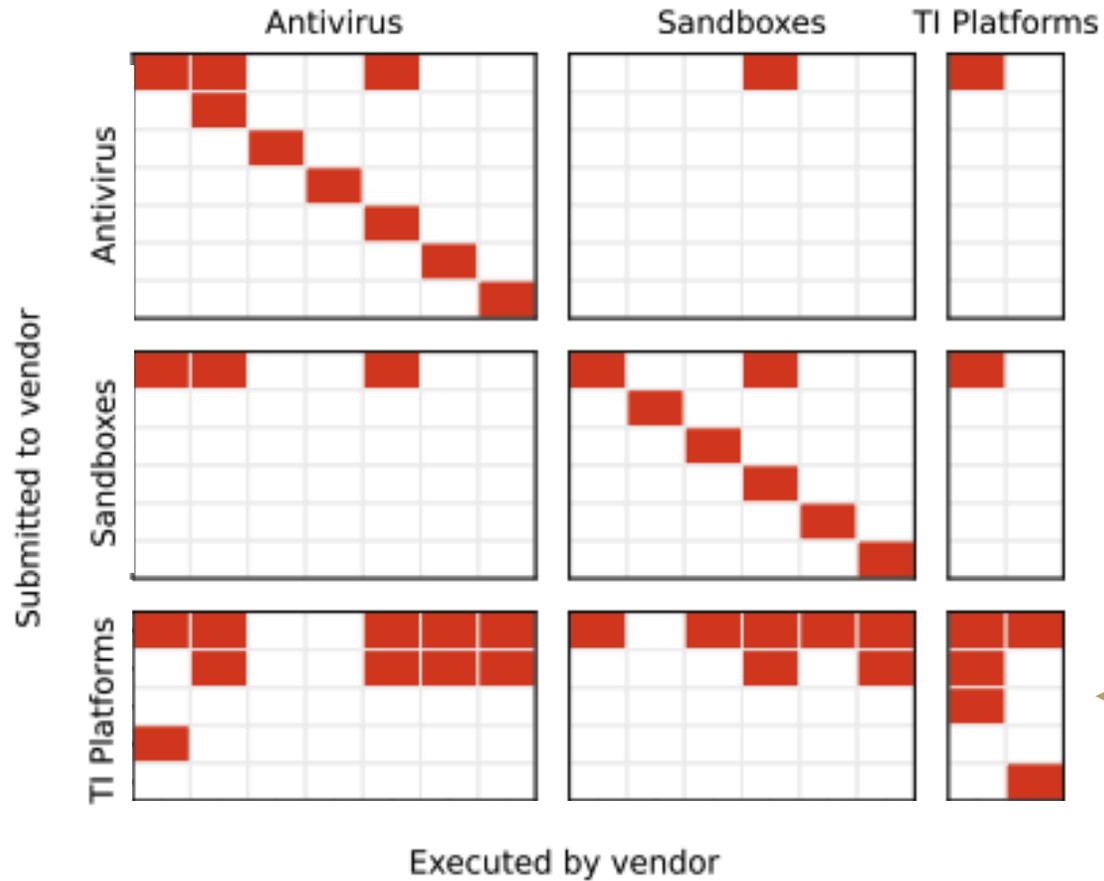
1600
binary
executions

170
unique
fingerprints

20
hand-labeled
vendors

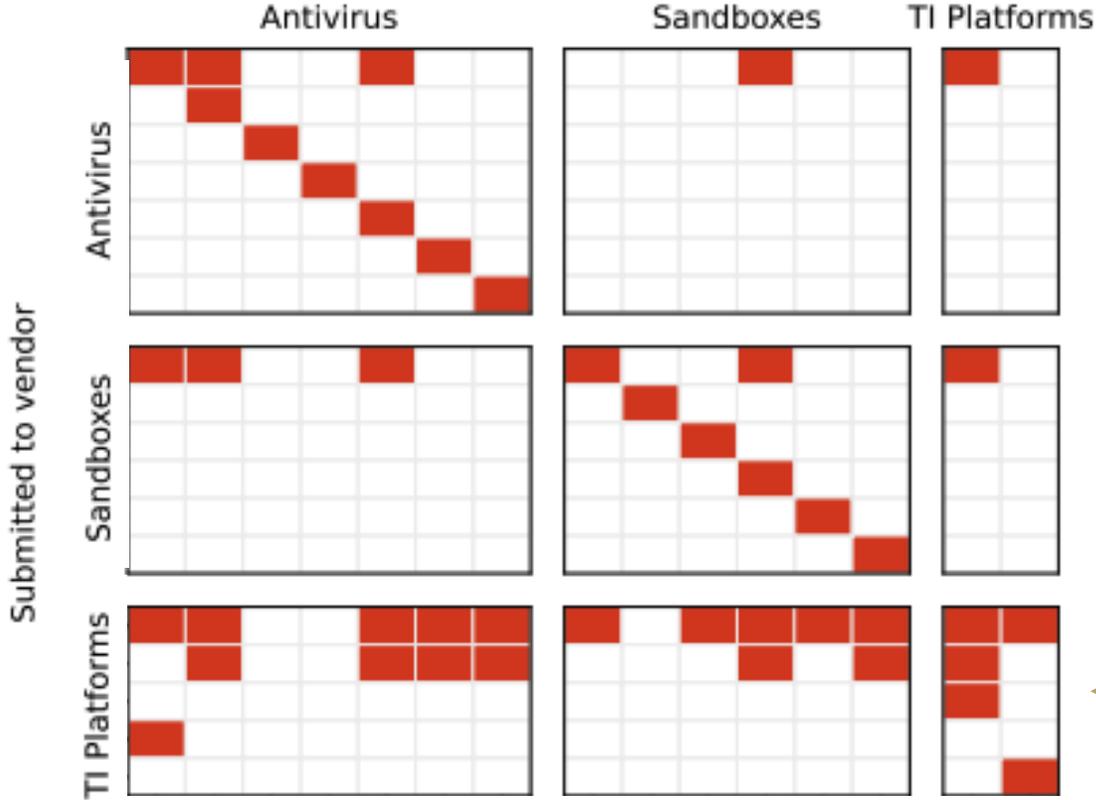
43
unique external
vendors

Adjacency matrix



TI Platforms share the most frequently

Adjacency matrix

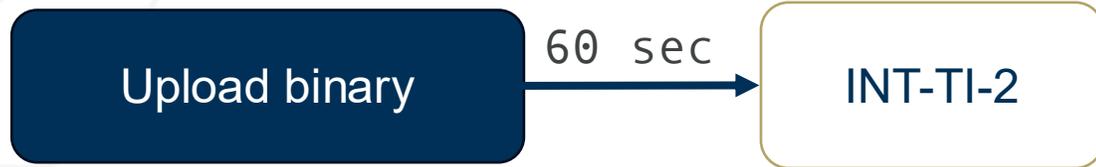


TI Platforms share the most frequently

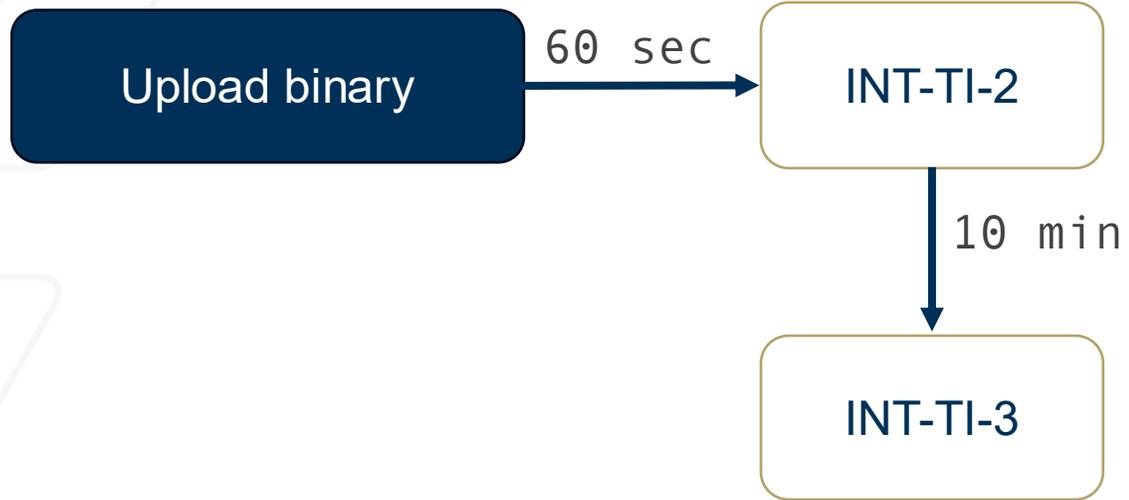
Executed by vendor

5/9 AVs consume from TI Platforms, but only 1/9 share

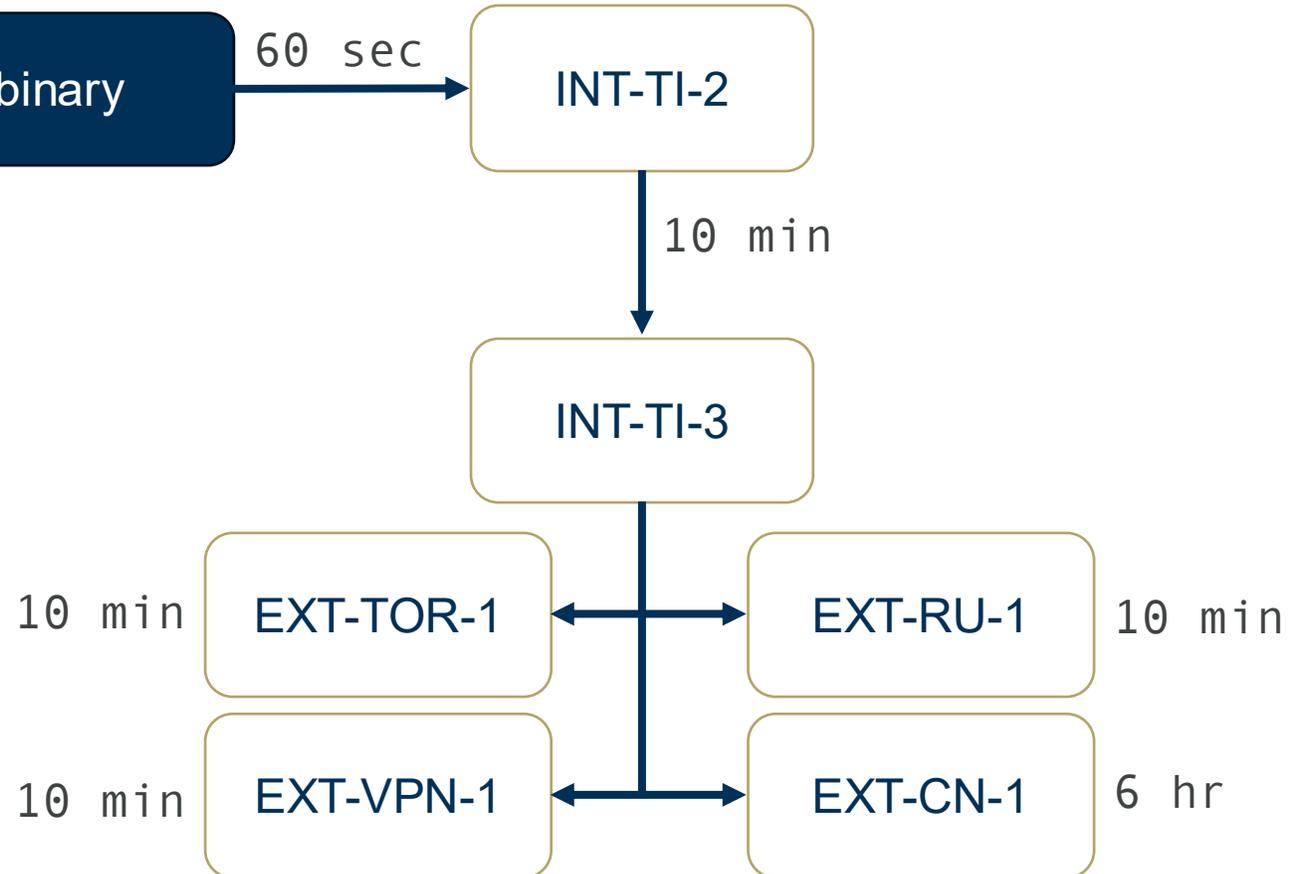
Sharing relationships between vendors



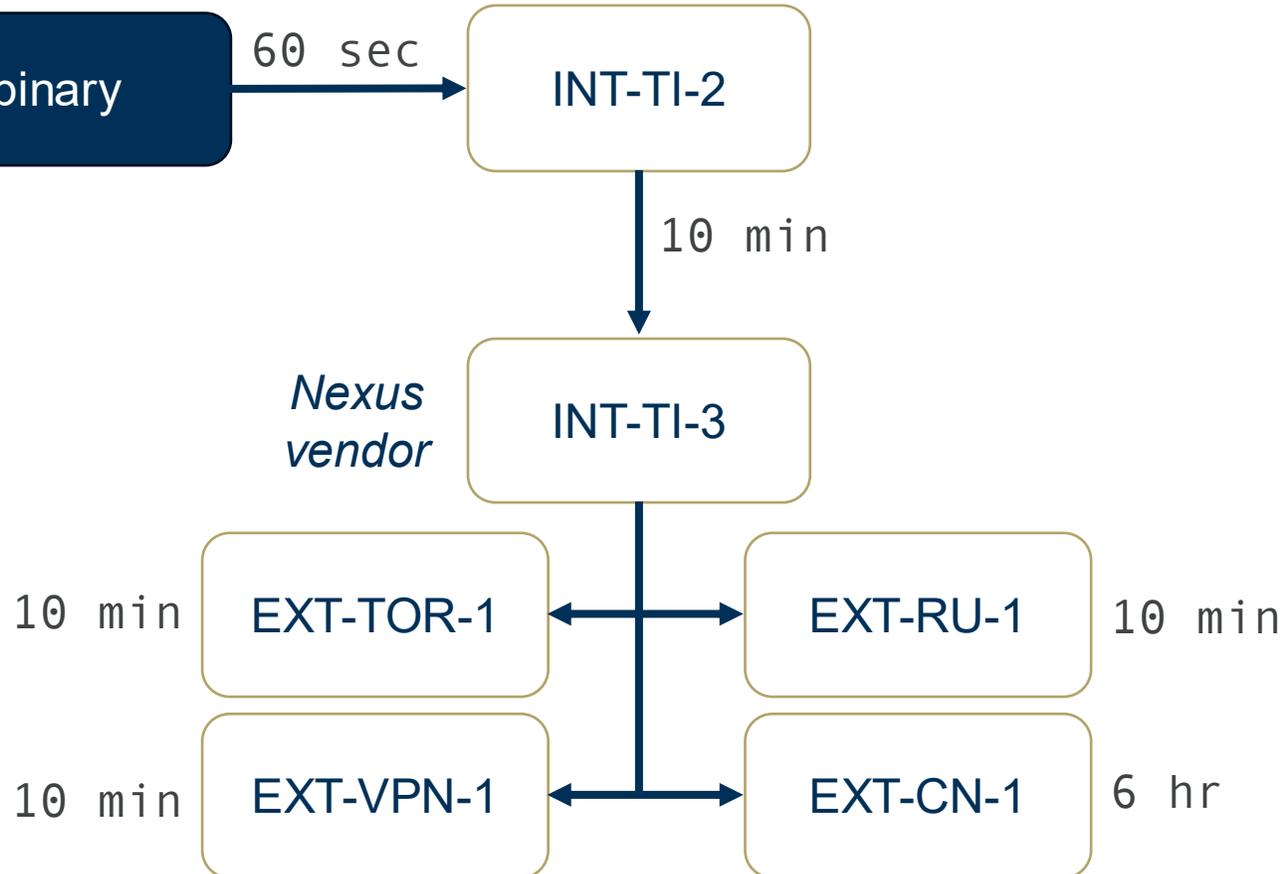
Sharing relationships between vendors



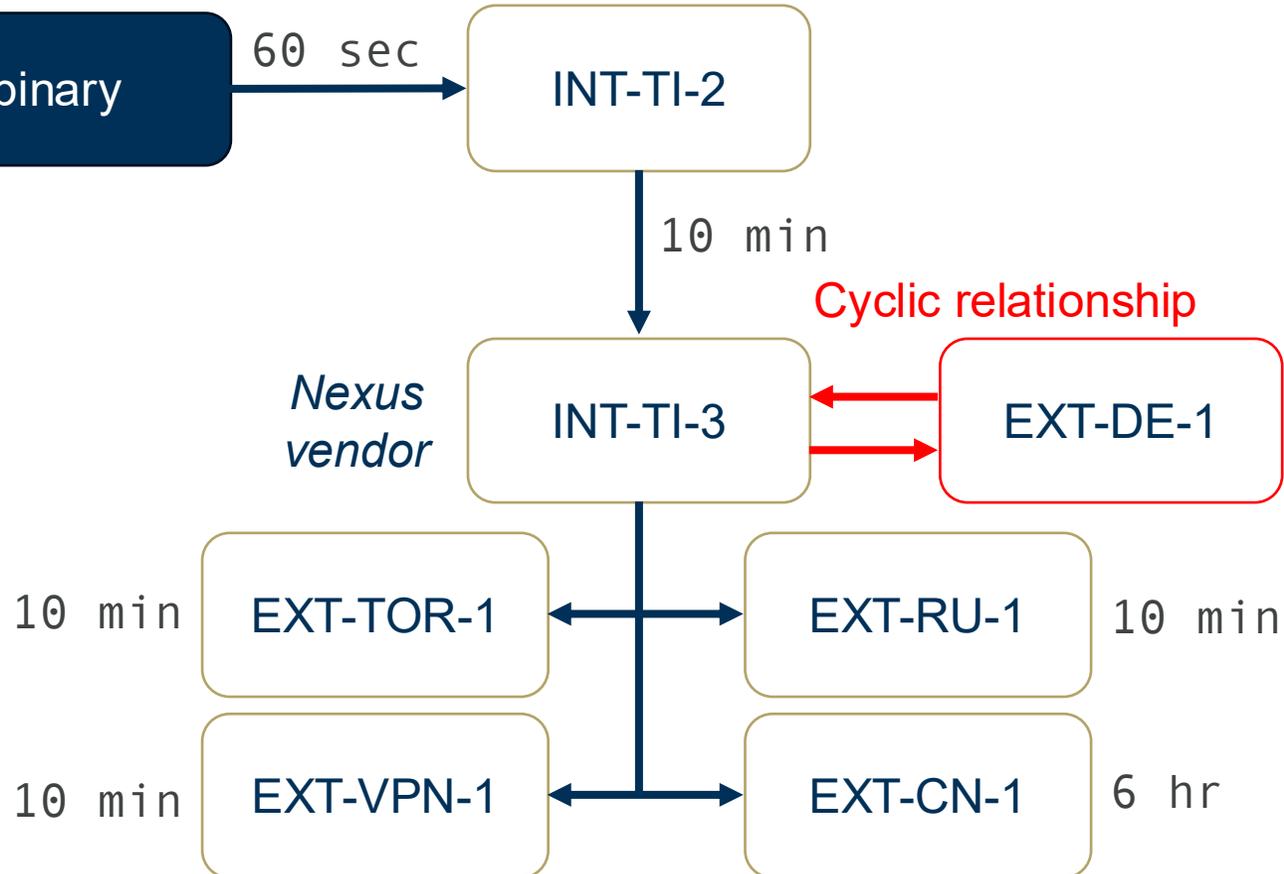
Sharing relationships between vendors



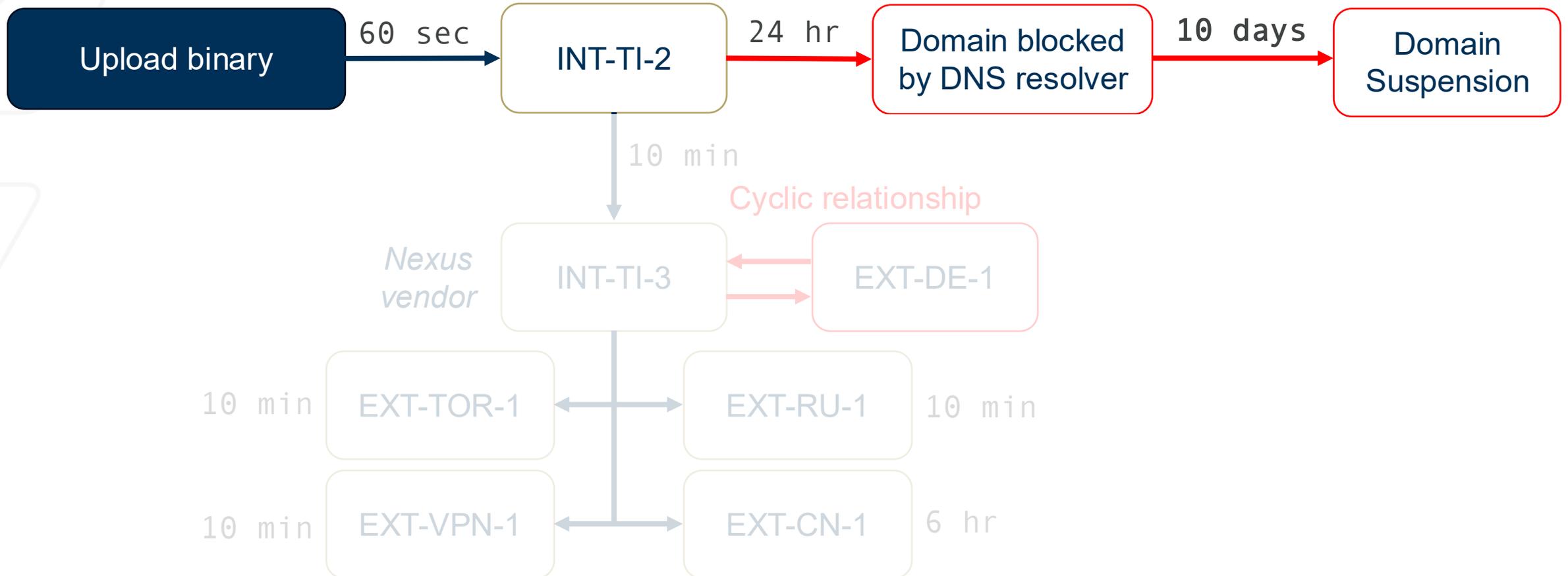
Sharing relationships between vendors



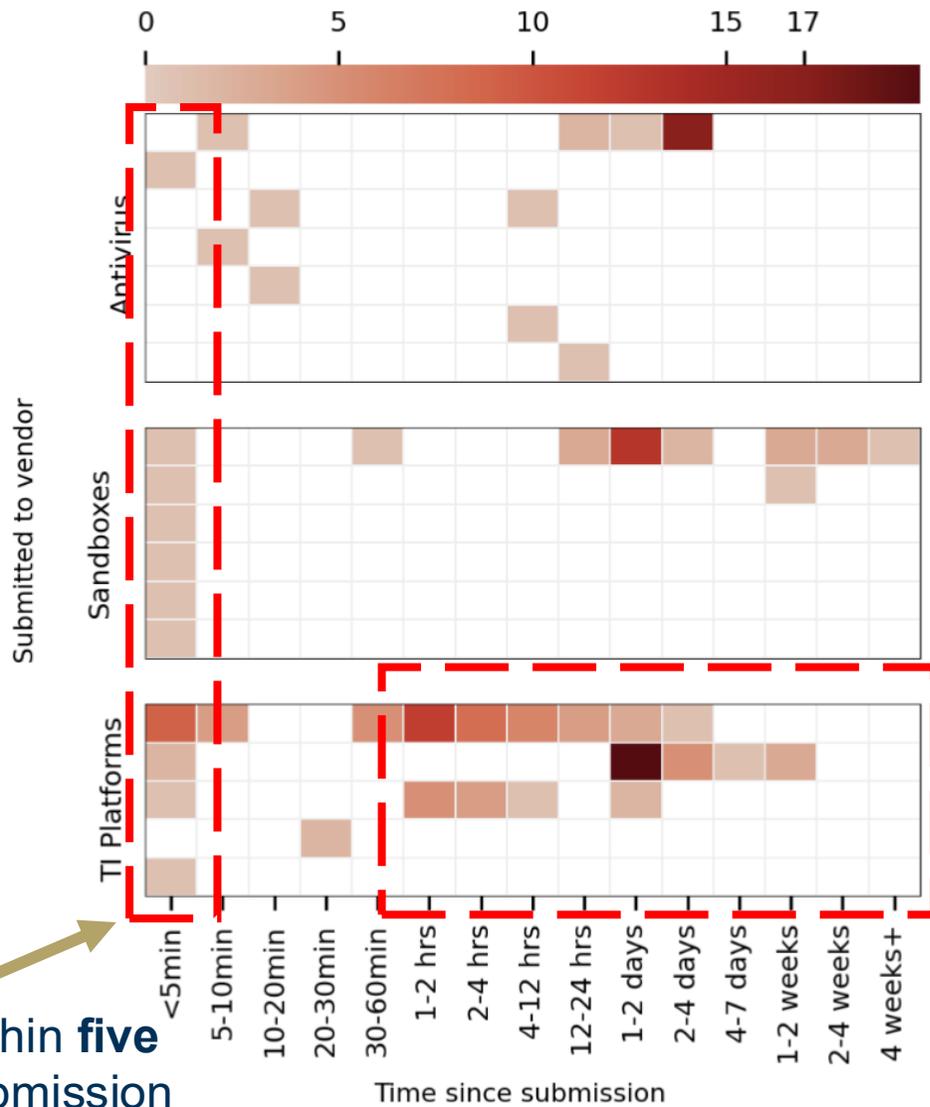
Sharing relationships between vendors



Sharing relationships between vendors

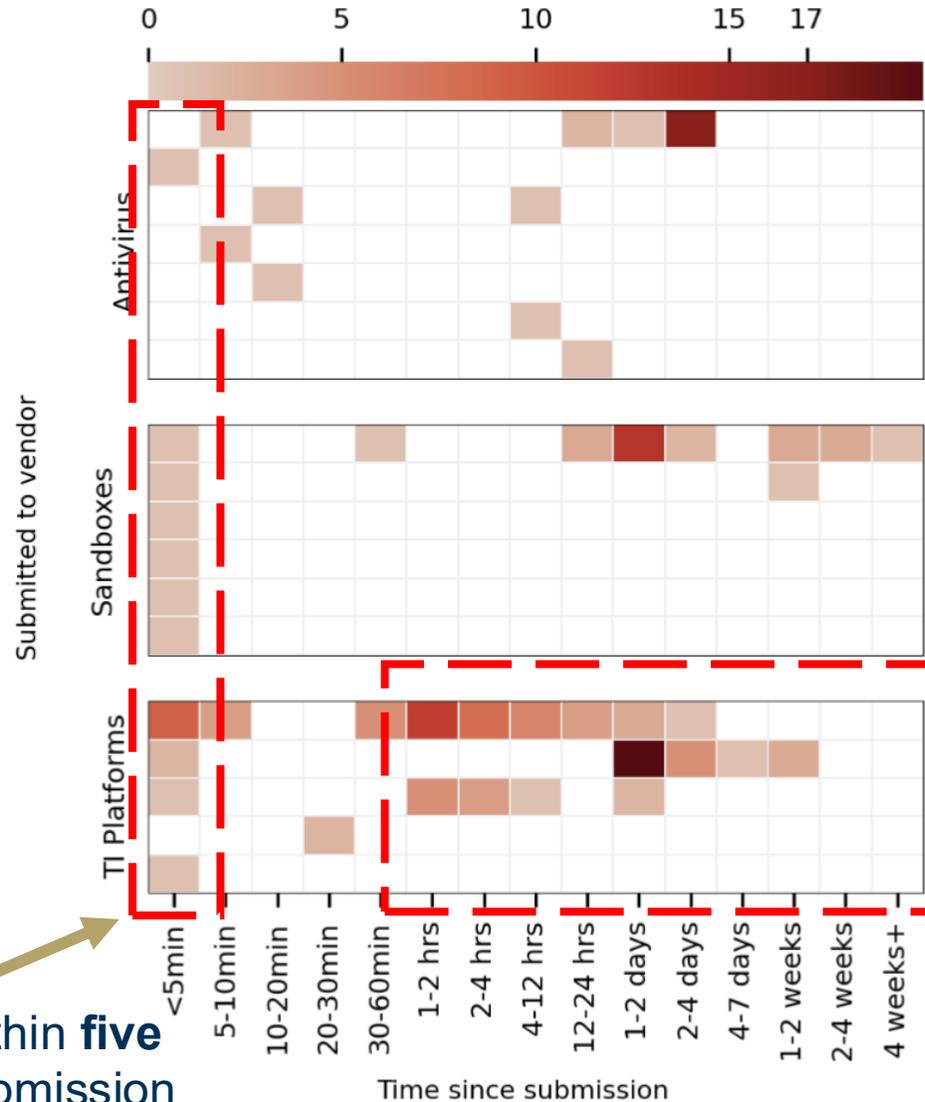


Sharing velocity: a global view



First executions typically occur within **five minutes** after submission

Sharing velocity: a global view



First executions typically occur within **five minutes** after submission

Long tail of newly observed vendors from **one hour to four weeks**

What we learned about the TI Ecosystem



Stratified ecosystem

Blocking can happen within 1 hour of submission, but delays vary by vendor up to 10 days, leaving a wide exploitation window

What we learned about the TI Ecosystem



Stratified ecosystem

Blocking can happen within 1 hour of submission, but delays vary by vendor up to 10 days, leaving a wide exploitation window



Non-independent observations

Presence of data sharing relationships between vendors can compromise independence of observations from crowdsourced TI platforms

What we learned about the TI Ecosystem



Stratified ecosystem

Blocking can happen within 1 hour of submission, but delays vary by vendor up to 10 days, leaving a wide exploitation window



Non-independent observations

Presence of data sharing relationships between vendors can compromise independence of observations from crowdsourced TI platforms



Fingerprinting risk

Adversaries who understand vendor signatures and sharing delays can exploit them to evade detection

What we learned about the TI Ecosystem



Stratified ecosystem

Blocking can happen within 1 hour of submission, but delays vary by vendor up to 10 days, leaving a wide exploitation window



Non-independent observations

Presence of data sharing relationships between vendors can compromise independence of observations from crowdsourced TI platforms



Fingerprinting risk

Adversaries who understand vendor signatures and sharing delays can exploit them to evade detection



Responsible disclosure

Provided vendors with vulnerability write-up and detection rules, responses varied

Actively Understanding the Dynamics and Risks of the Threat Intelligence Ecosystem

Tillson Galloway, Allen Chang, Omar Alrawi, Thanos Avgetidis, Manos Antonakakis, Fabian Monrose

tillson@gatech.edu

Safe travels home!



Read the paper

