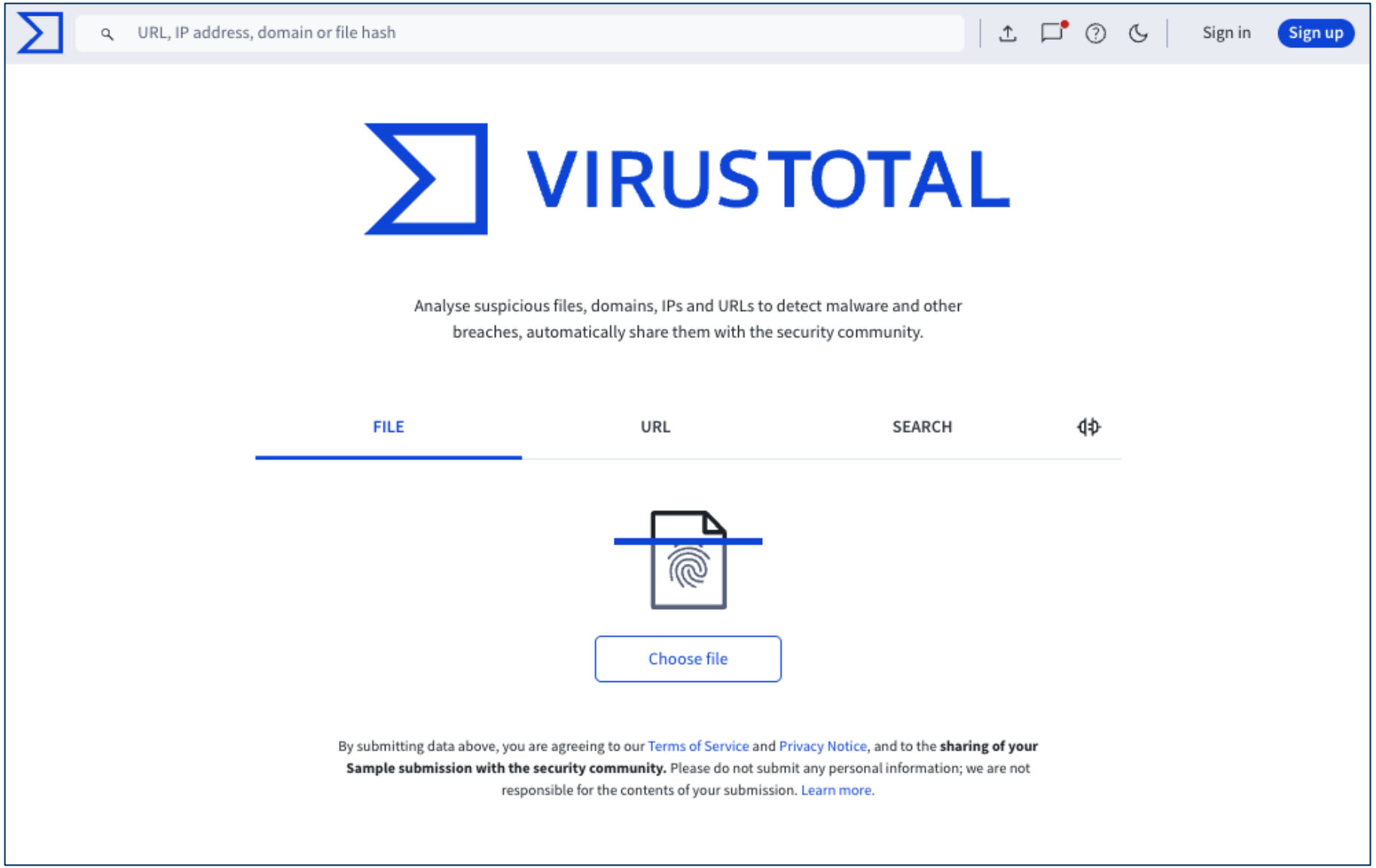
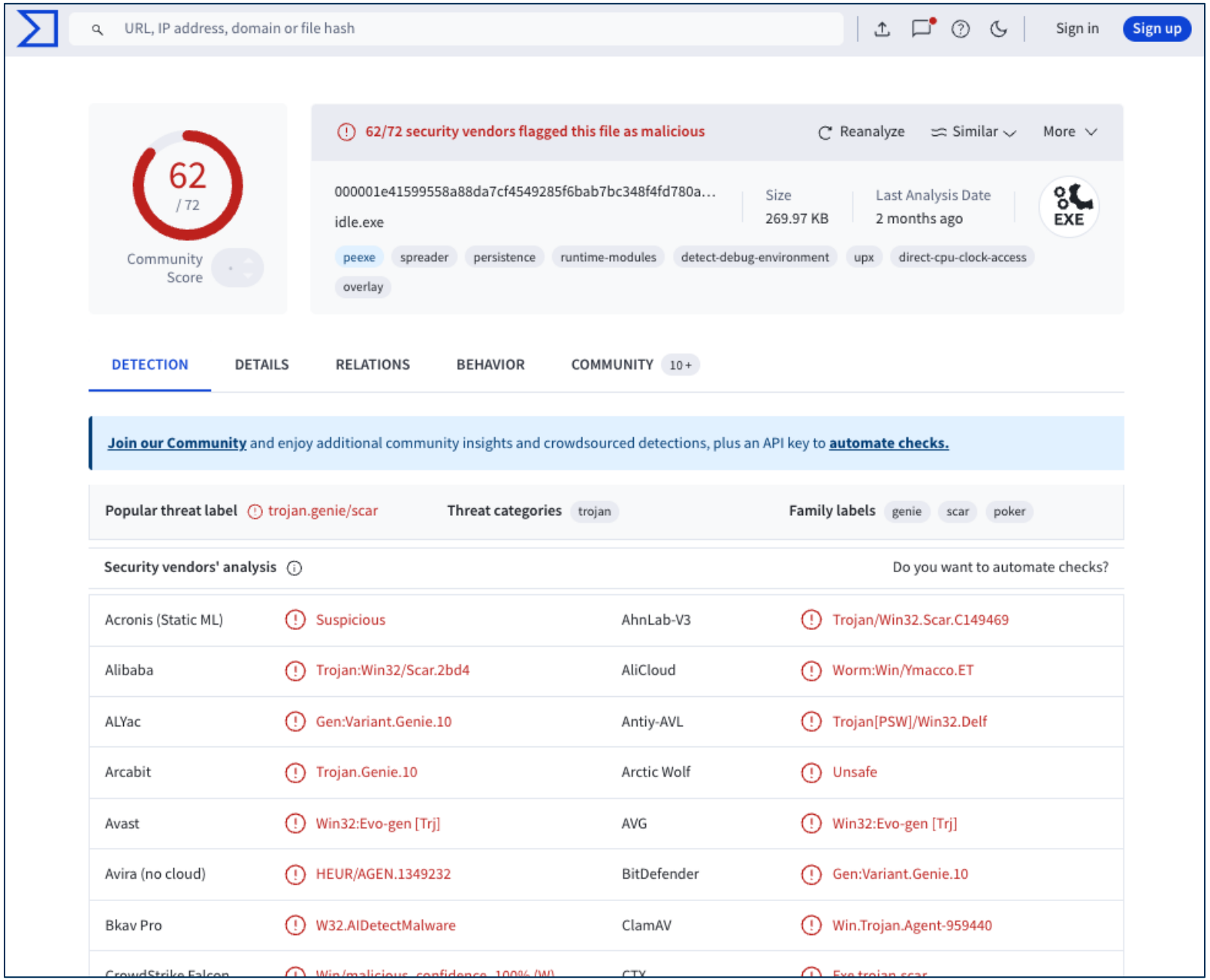
Actively Understanding the Dynamics and Risks of the Threat Intelligence Ecosystem

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

Georgia Tech



Georgia Tech


URL, IP address, domain or file hash
Sign in
Sign up
62
/ 72
Community Score
62/72 security vendors flagged this file as malicious
Reanalyze
Similar
More
000001e41599558a88da7cf4549285f6bab7bc348f4fd780a...
idle.exe
Size
269.97 KB
Last Analysis Date
2 months ago
EXE
peexe
spreader
persistence
runtime-modules
detect-debug-environment
upx
direct-cpu-clock-access
overlay
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
Do you want to automate checks?
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

Millions of IoCs are processed by vendors daily

Microsoft

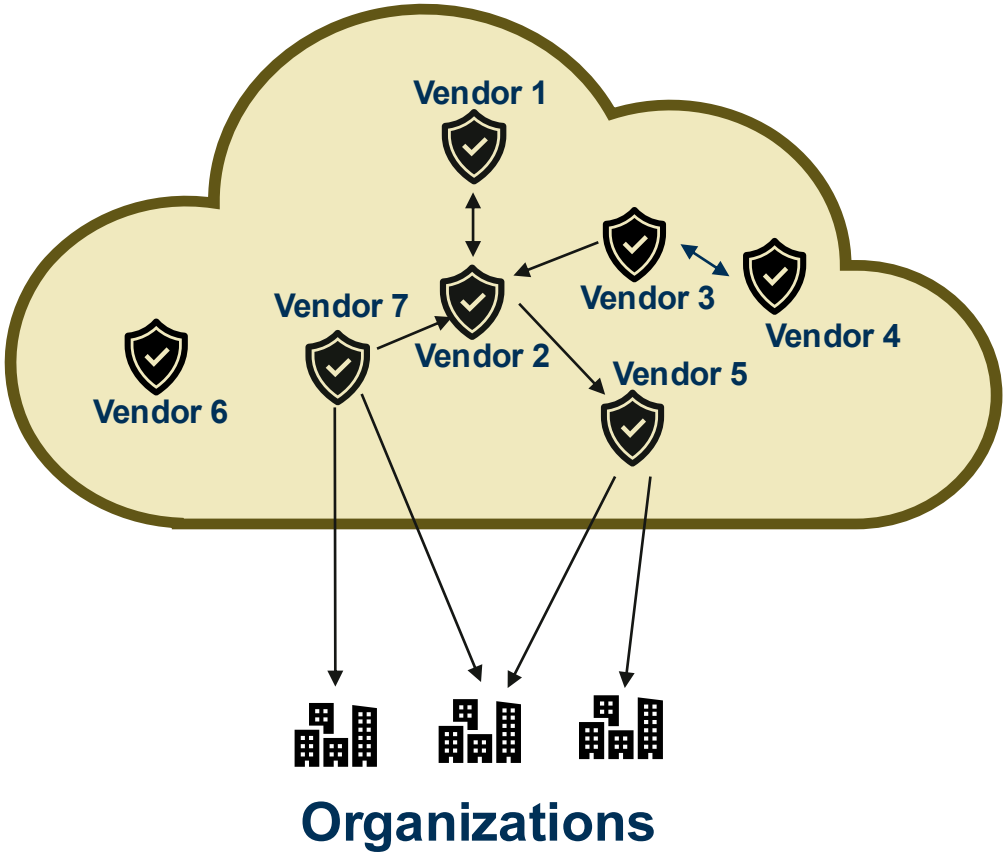
Georgia Tech

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?*



Georgia Tech

Types of Indicators of Compromise

Files

File hashes

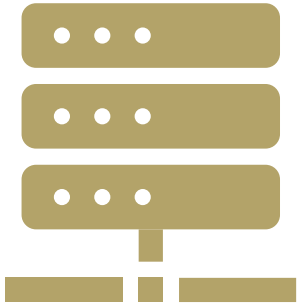
Endpoint

Types of Indicators of Compromise

Files

File hashes

Endpoint



IPs

URLs

Domains

Network

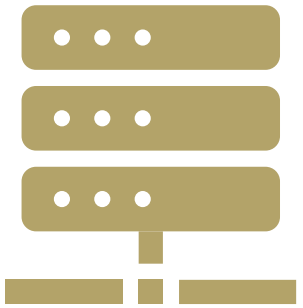
Types of Indicators of Compromise

Files

File hashes

Endpoint

Focus of this presentation



IPs

URLs

Domains

Network

Learn more in the paper!

Measurement answers three research questions

Relationships *— how are data sharing relationships leveraged?*

Georgia Tech

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?*

Georgia Tech

Measurement answers three research questions

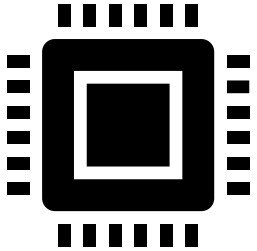
Relationships *— how are data sharing relationships leveraged?*

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!

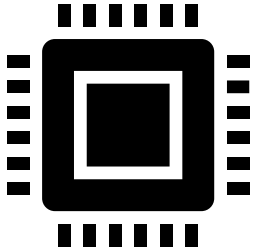
Georgia Tech

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



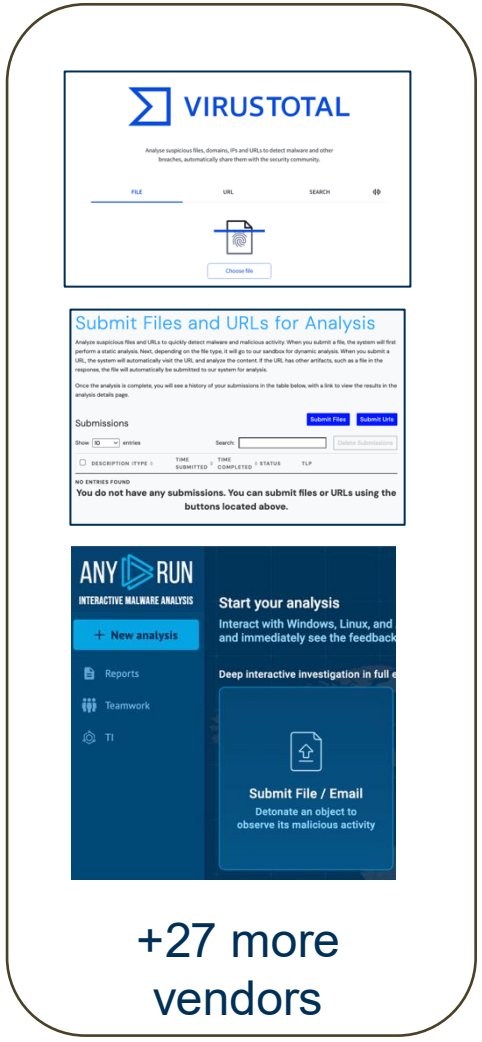
Research profiler binary

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



Research profiler binary

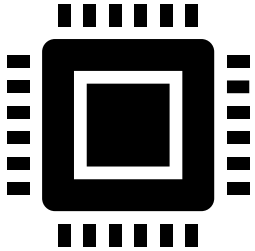
Uploads to



+27 more vendors

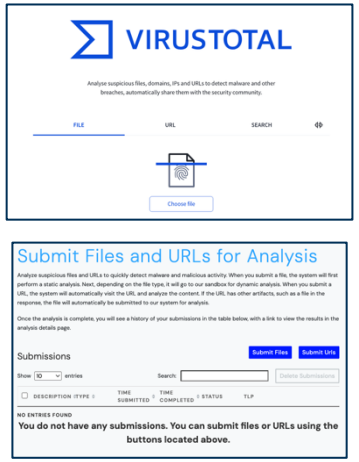
Georgia Tech

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



Research profiler binary

Uploads to



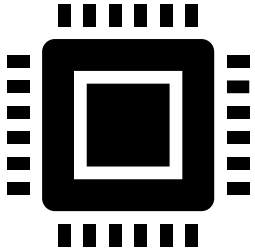
+27 more vendors

Runs binary

Dynamic Analysis

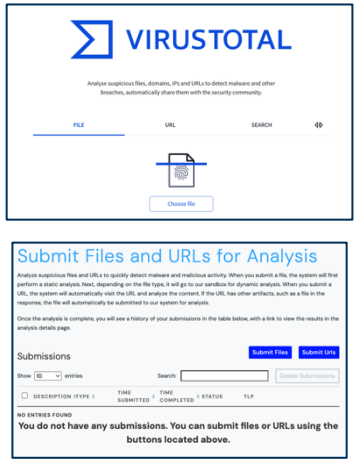
Georgia Tech

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



Research profiler binary

Uploads to



+27 more vendors

Runs binary

Dynamic Analysis

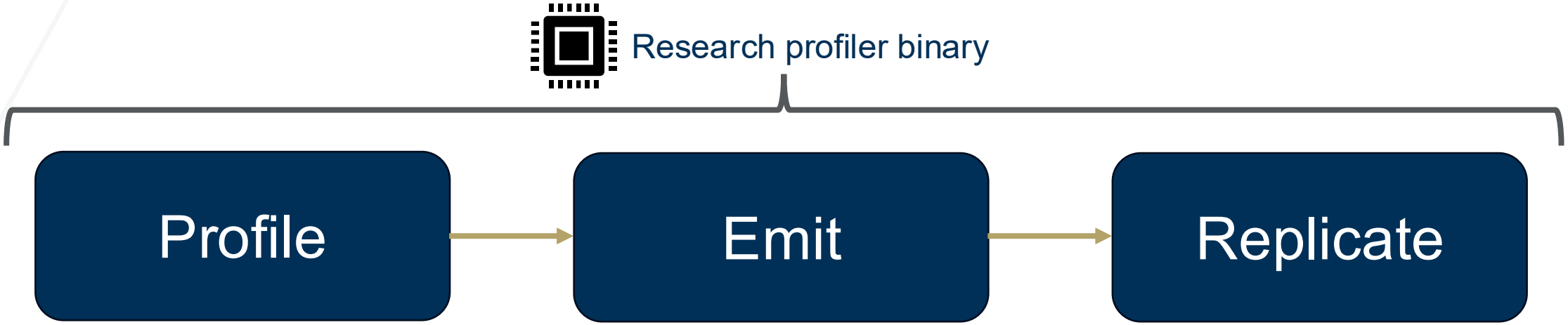
Extract IoCs

Georgia Tech

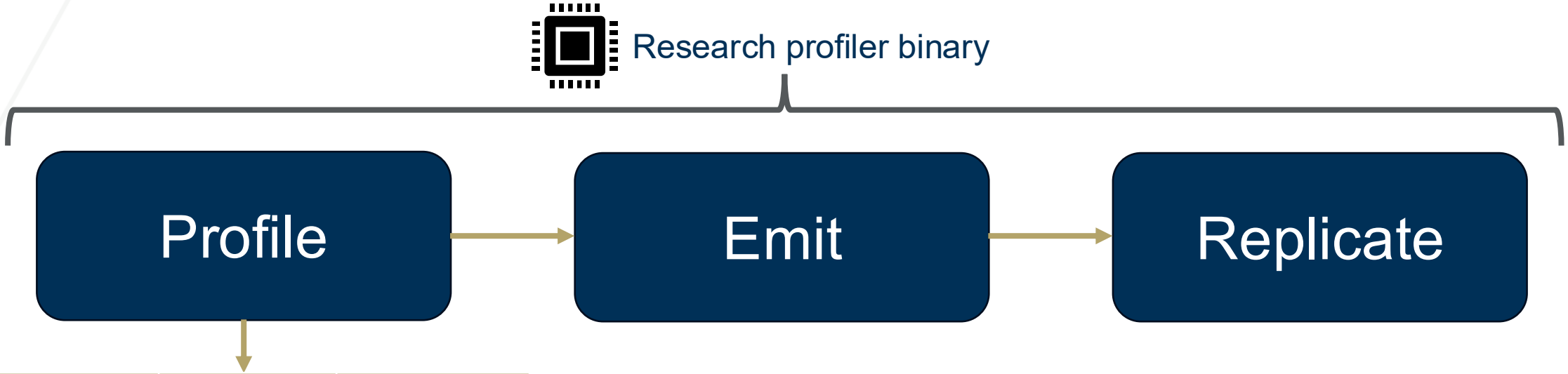
Key idea: map ecosystem supply chains using lightweight active probes to free, public services

Georgia Tech

Binary File: Profiling Process

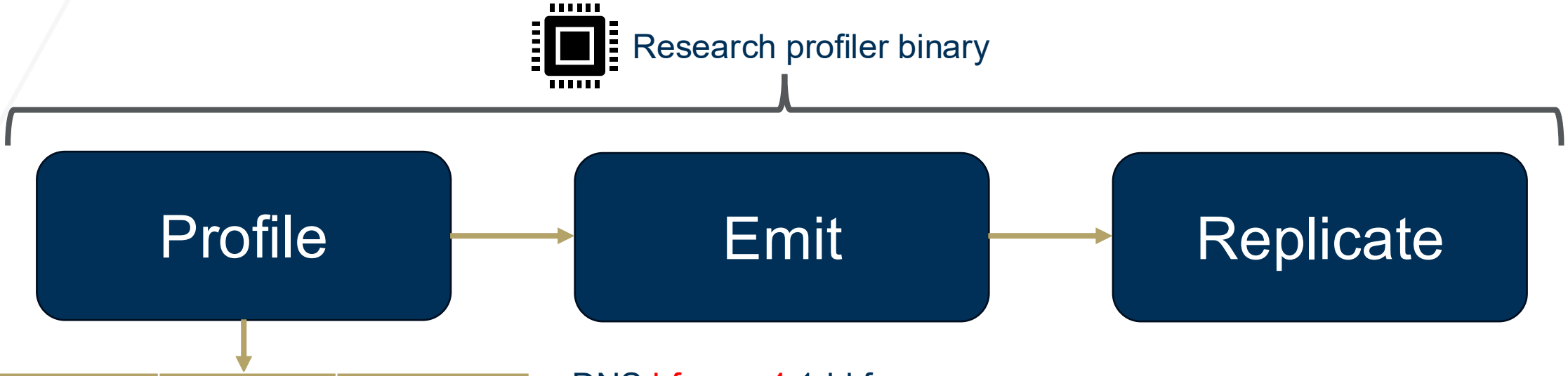


Binary File: Profiling Process



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

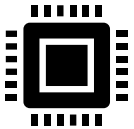
Binary File: Profiling Process



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

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

Binary File: Profiling Process



Research profiler binary

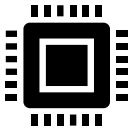
Profile → Emit → Replicate

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

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

Drop binary

Binary File: Profiling Process



Research profiler binary

Profile → **Emit** → **Replicate**

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

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

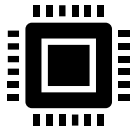
Drop binary

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/

Binary File: Profiling Process

bfaxzyq4



Research profiler binary

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

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

Drop binary

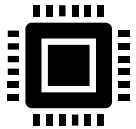
Fingerprint	Value	Hashed
RAM	16GB	f4
OS install date	Jan 1, 1970	fa4f
Manufacturer	Dell, Inc.	2f

DNS f4fa4f2fbfaxzyq4.1dd.fun
HTTP http://f4fa4f2fbfaxzyq4.1dd.fun/

Georgia Tech

Binary File: Profiling Process

f4fa4f2f bfaxzyq4



Research profiler binary

Profile → Emit → Replicate

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

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

Drop binary

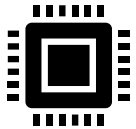
Fingerprint	Value	Hashed
RAM	16GB	f4
OS install date	Jan 1, 1970	fa4f
Manufacturer	Dell, Inc.	2f

DNS f4fa4f2fbfaxzyq4.1dd.fun
HTTP http://f4fa4f2fbfaxzyq4.1dd.fun/

Georgia Tech

Binary File: Profiling Process

84fofmsd f4fa4f2f bfaxzyq4



Research profiler binary

Profile → Emit → Replicate

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

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

Drop binary

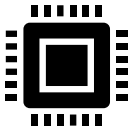
Fingerprint	Value	Hashed
RAM	16GB	f4
OS install date	Jan 1, 1970	fa4f
Manufacturer	Dell, Inc.	2f

DNS f4fa4f2fbfaxzyq4.1dd.fun
HTTP http://f4fa4f2fbfaxzyq4.1dd.fun/

Georgia Tech

Profiling Process

924fnsk | 84fofmsd | f4fa4f2f | bfaxzyq4



Research profiler binary

Profile → **Emit** → **Replicate**

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

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

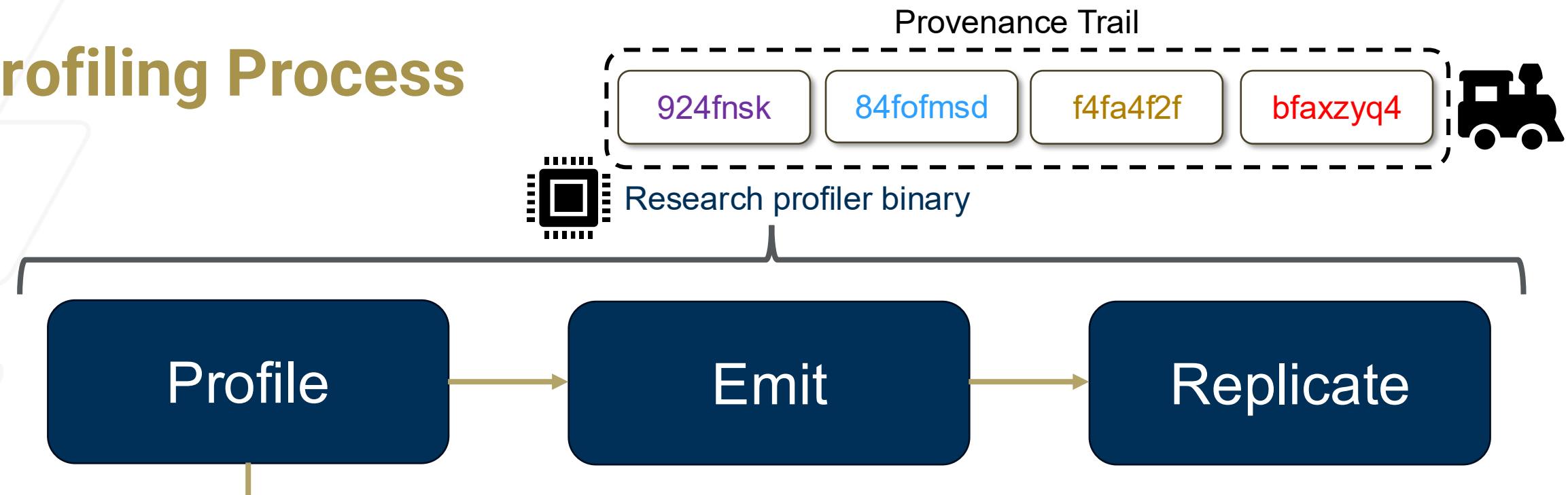
Drop binary

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/

Georgia Tech

Profiling Process



Fingerprint	Value	Hashed
RAM	64GB	bf
OS install date	Aug 6, 2025	axzy
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/

Georgia Tech

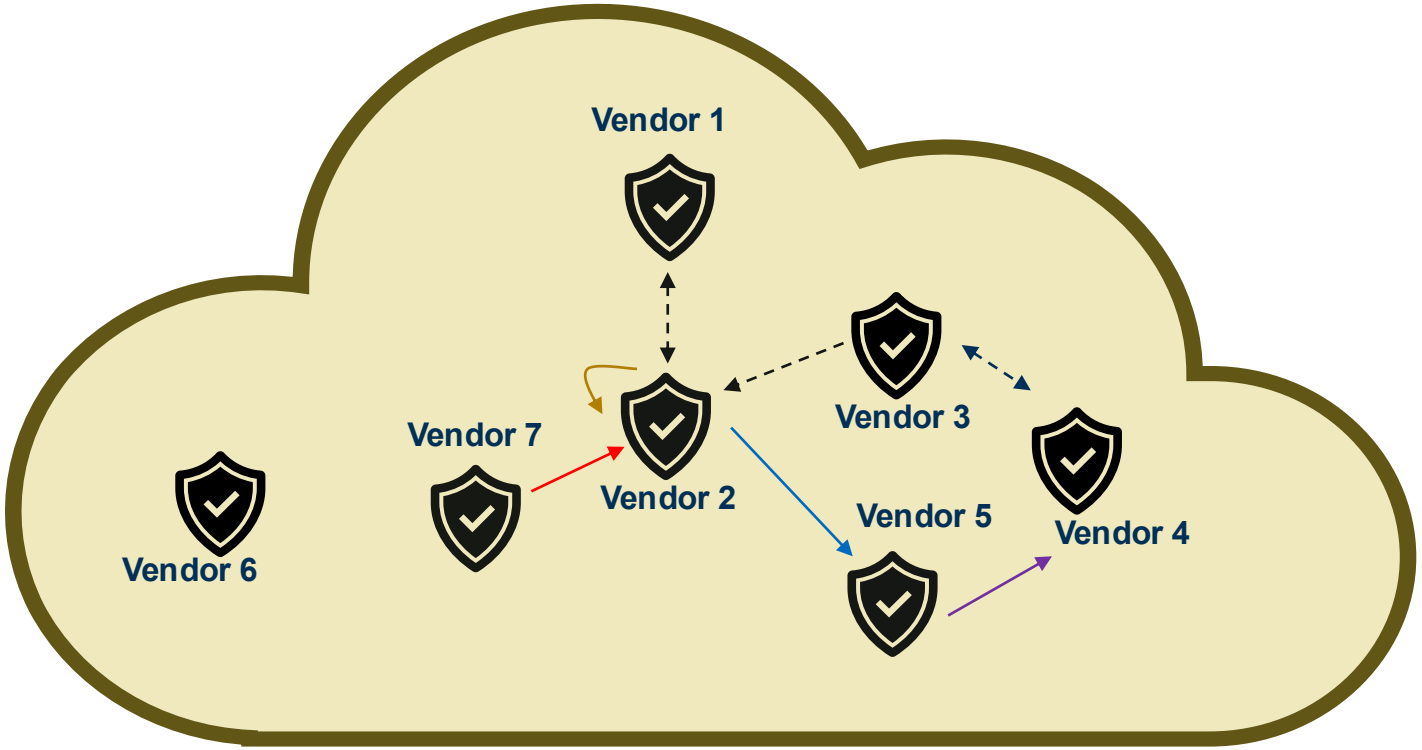
Constructing an ecosystem map

bfaxzyq4

f4fa4f2f

84fofmsd

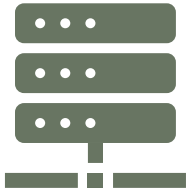
924fnsk



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

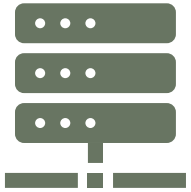
Georgia Tech

How to minimize potential harm to ecosystem?



One HTTP/DNS query per execution

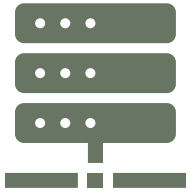
How to minimize potential harm to ecosystem?



One HTTP/DNS query per execution

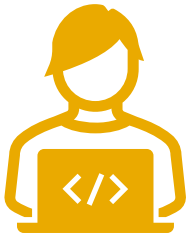
Max provenance trail length of five

How to minimize potential harm to ecosystem?



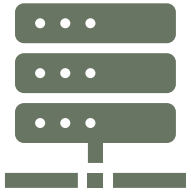
One HTTP/DNS query per execution

Max provenance trail length of five



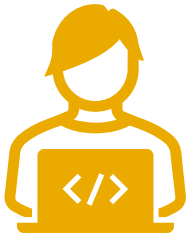
Disclaimer and opt-out are included in both binary and network communications

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

Sandboxes

Experiments considered three classes of vendors

Sandboxes

TI Platforms

Experiments considered three classes of vendors

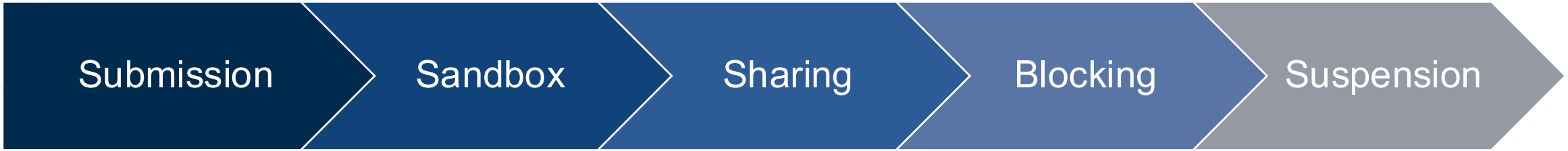
Sandboxes

TI Platforms

Antiviruses

Georgia Tech

Lifecycle of an IoC



Lifecycle of an IoC

Lifecycle of an IoC

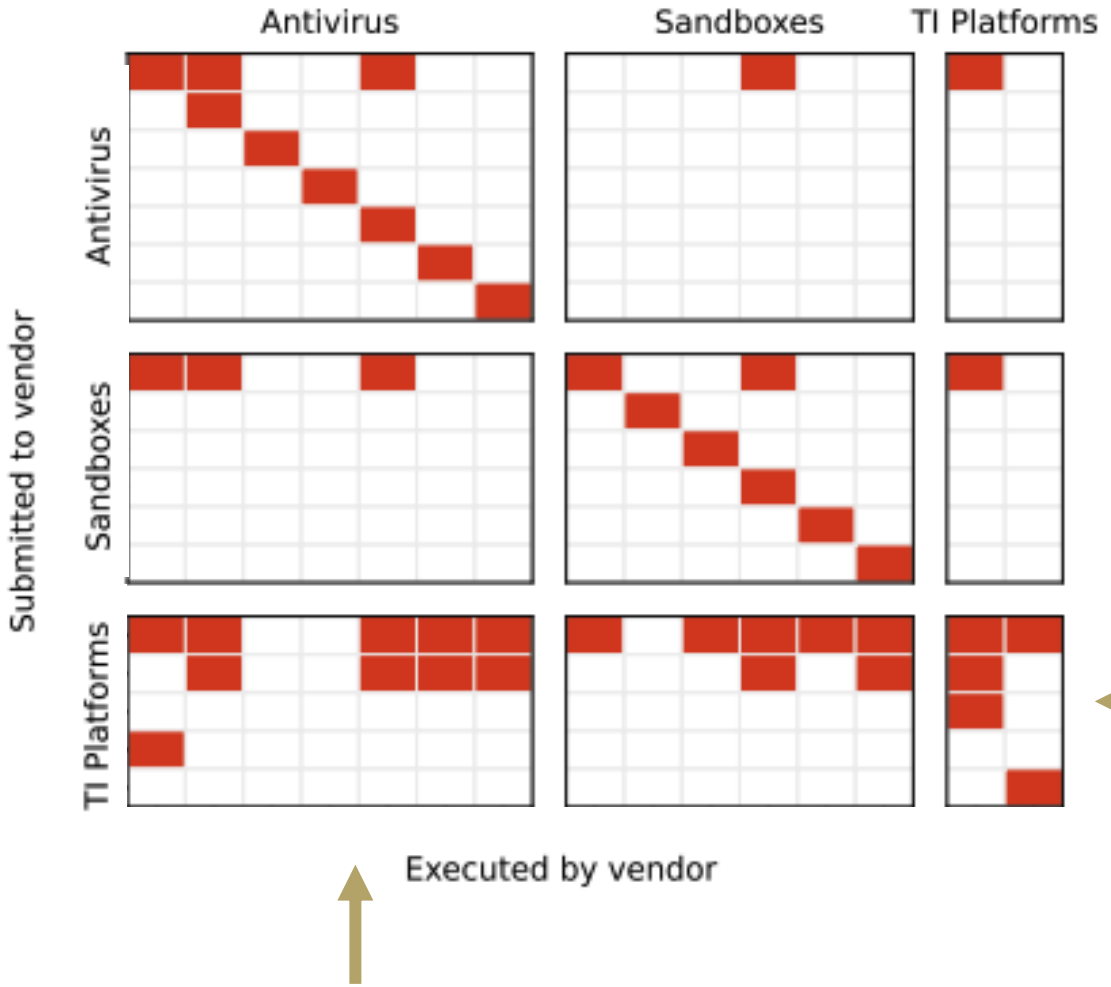
1600	170	20	43
binary executions	unique fingerprints	hand-labeled vendors	unique external vendors

Georgia Tech

Adjacency matrix

TI Platforms share the most frequently

Adjacency matrix

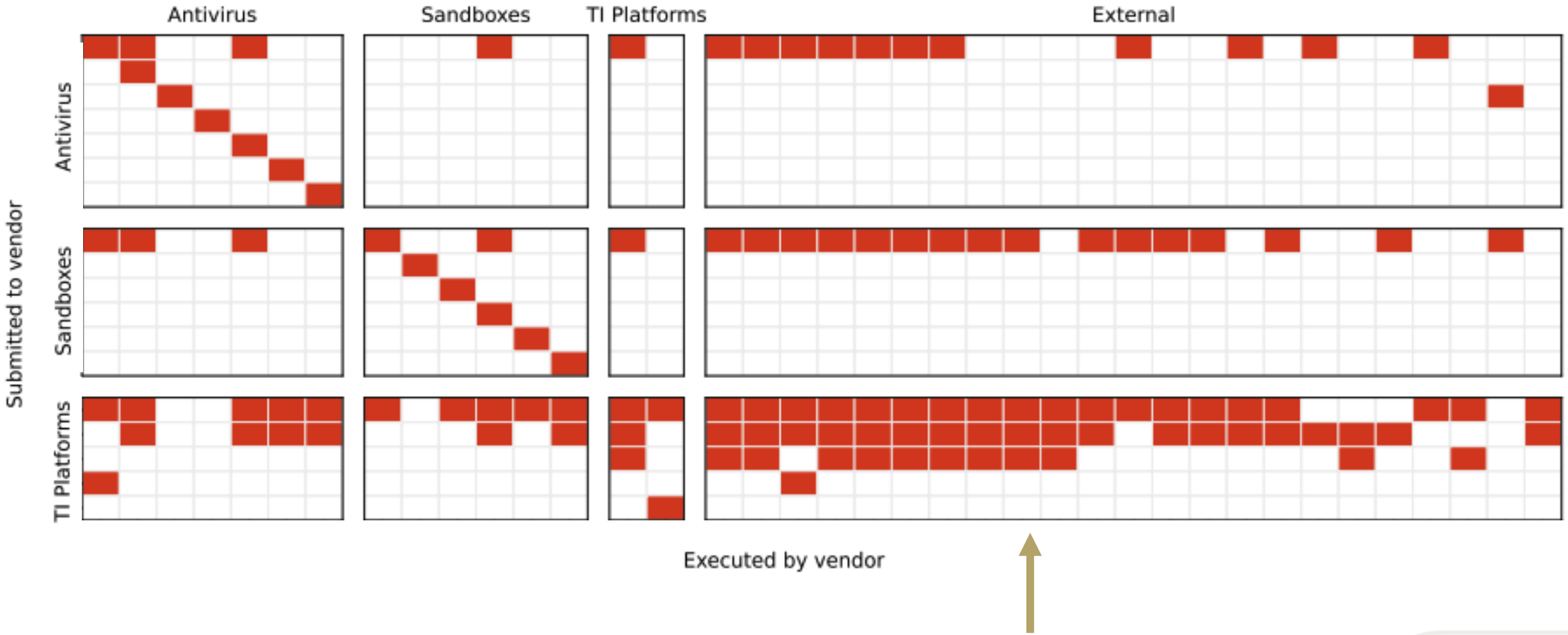


TI Platforms share the most frequently

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

Georgia Tech

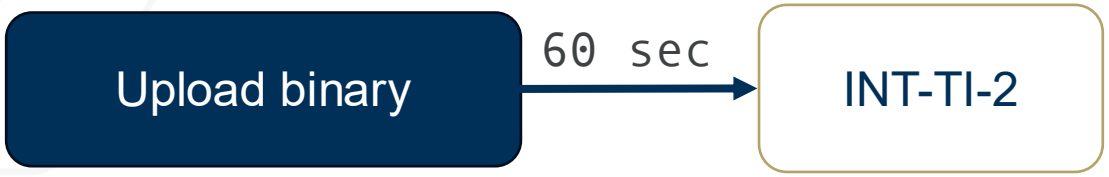
Adjacency matrix



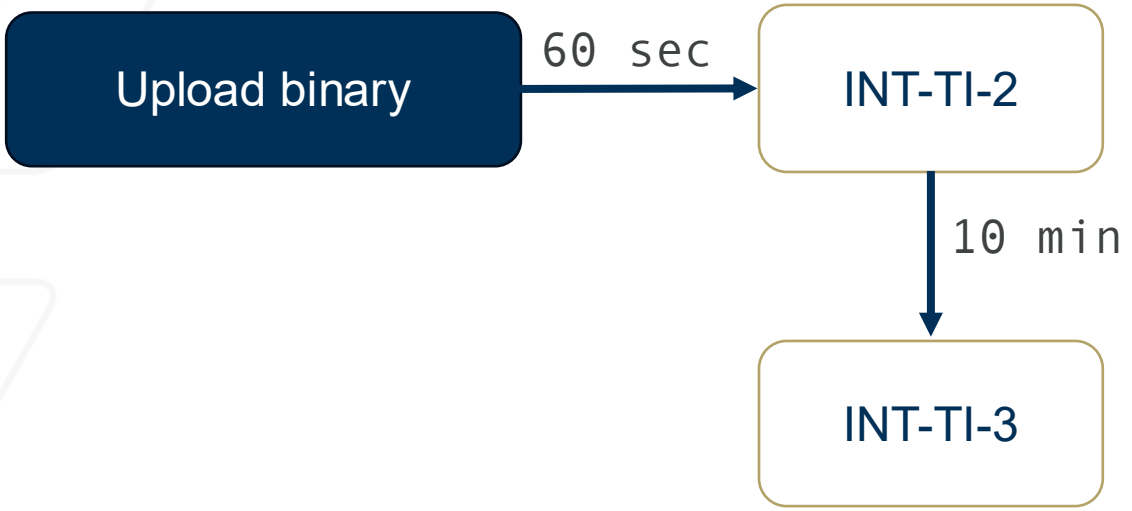
Binaries are often shared to
large number of unknown entities

Georgia Tech

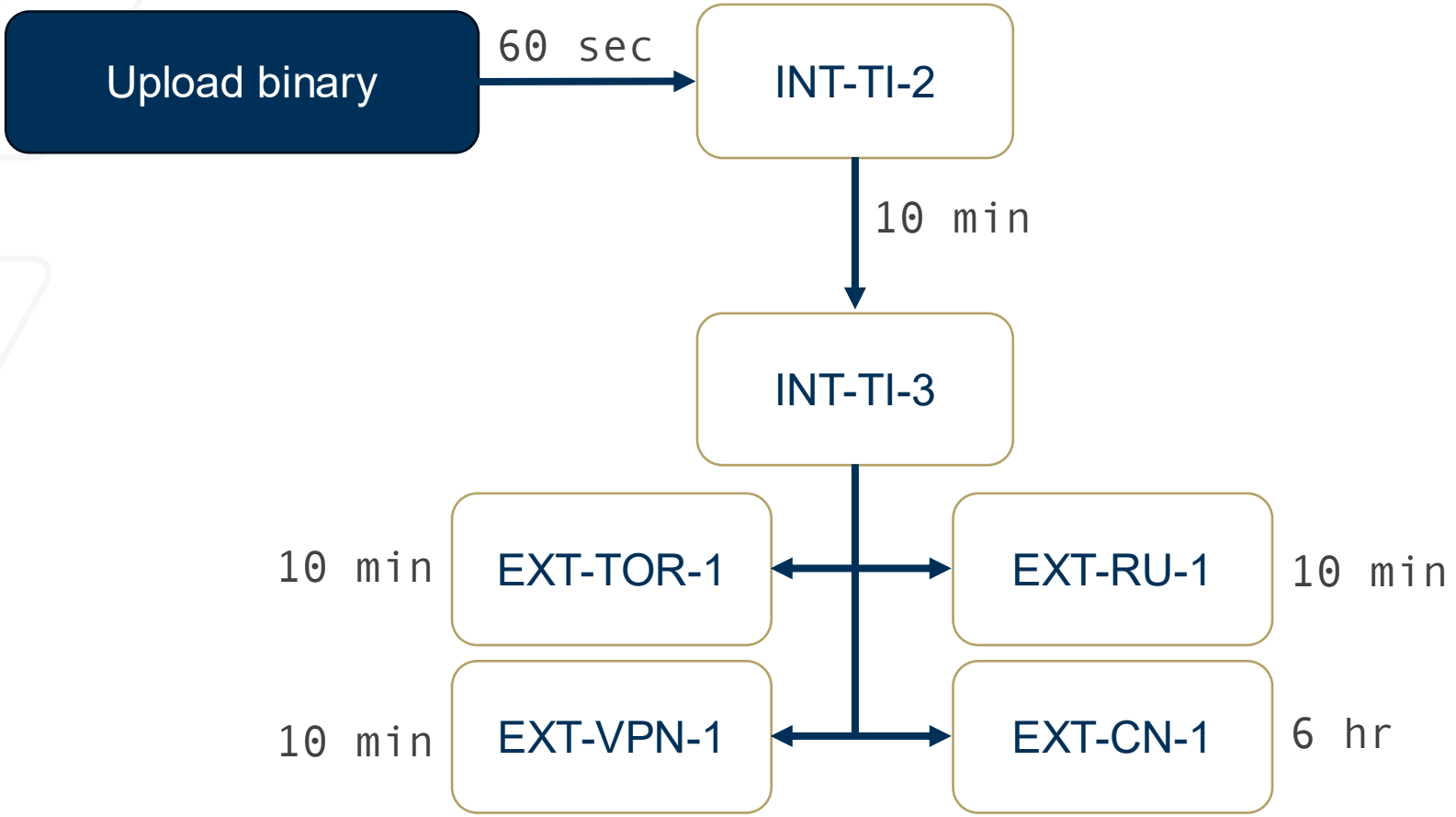
Sharing relationships between vendors



Sharing relationships between vendors

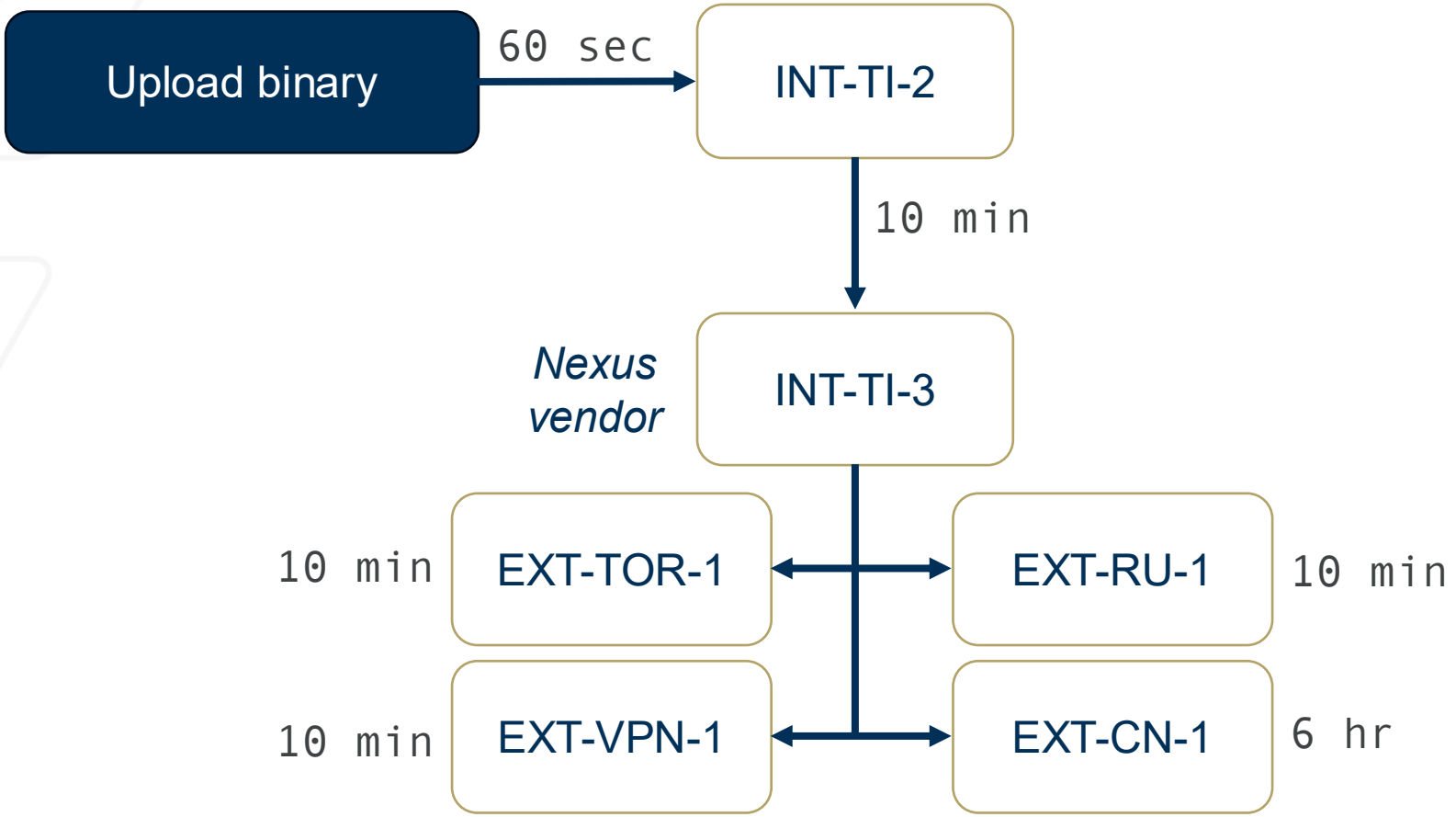


Sharing relationships between vendors



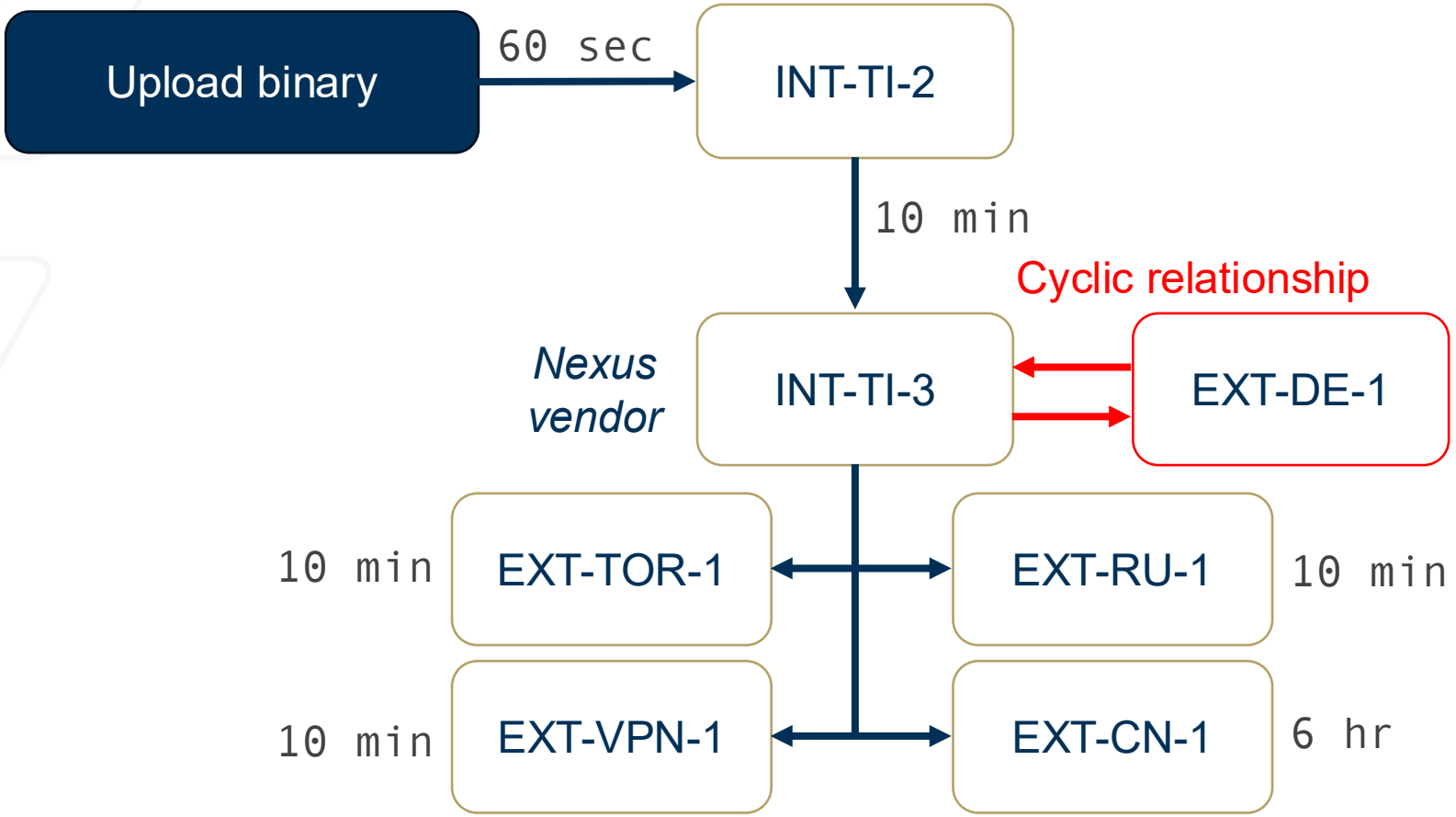
Georgia Tech

Sharing relationships between vendors



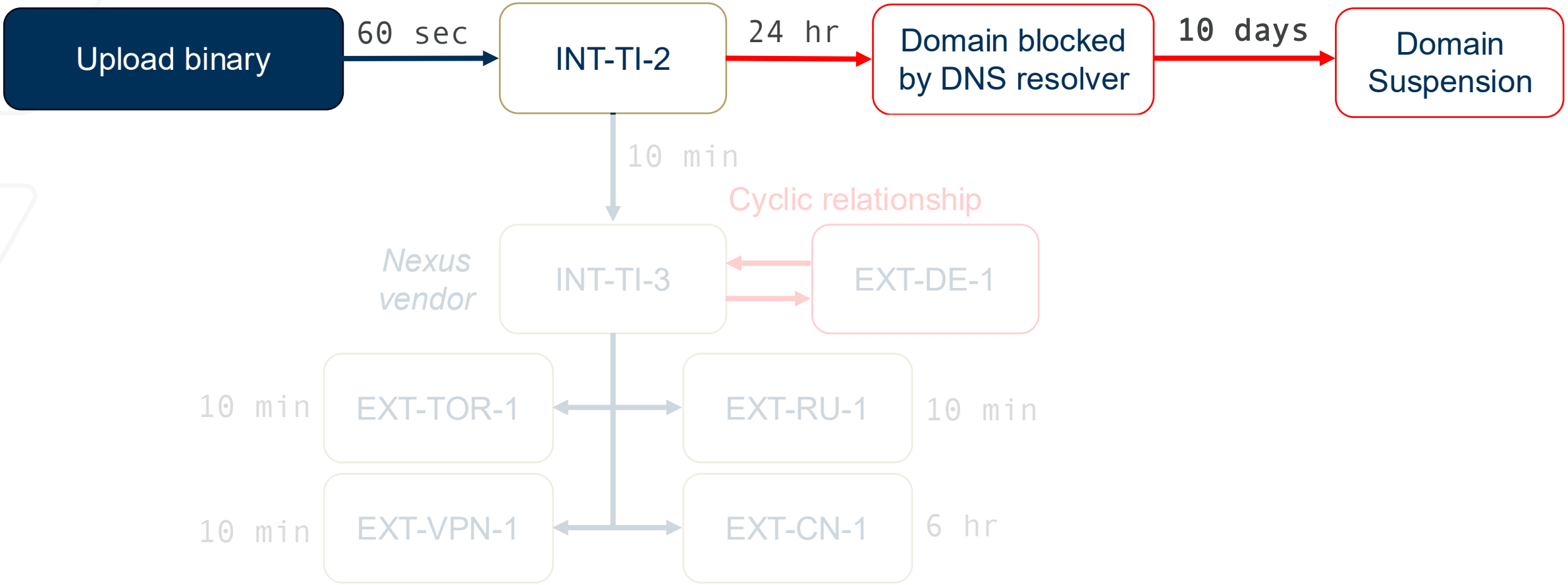
Georgia Tech

Sharing relationships between vendors



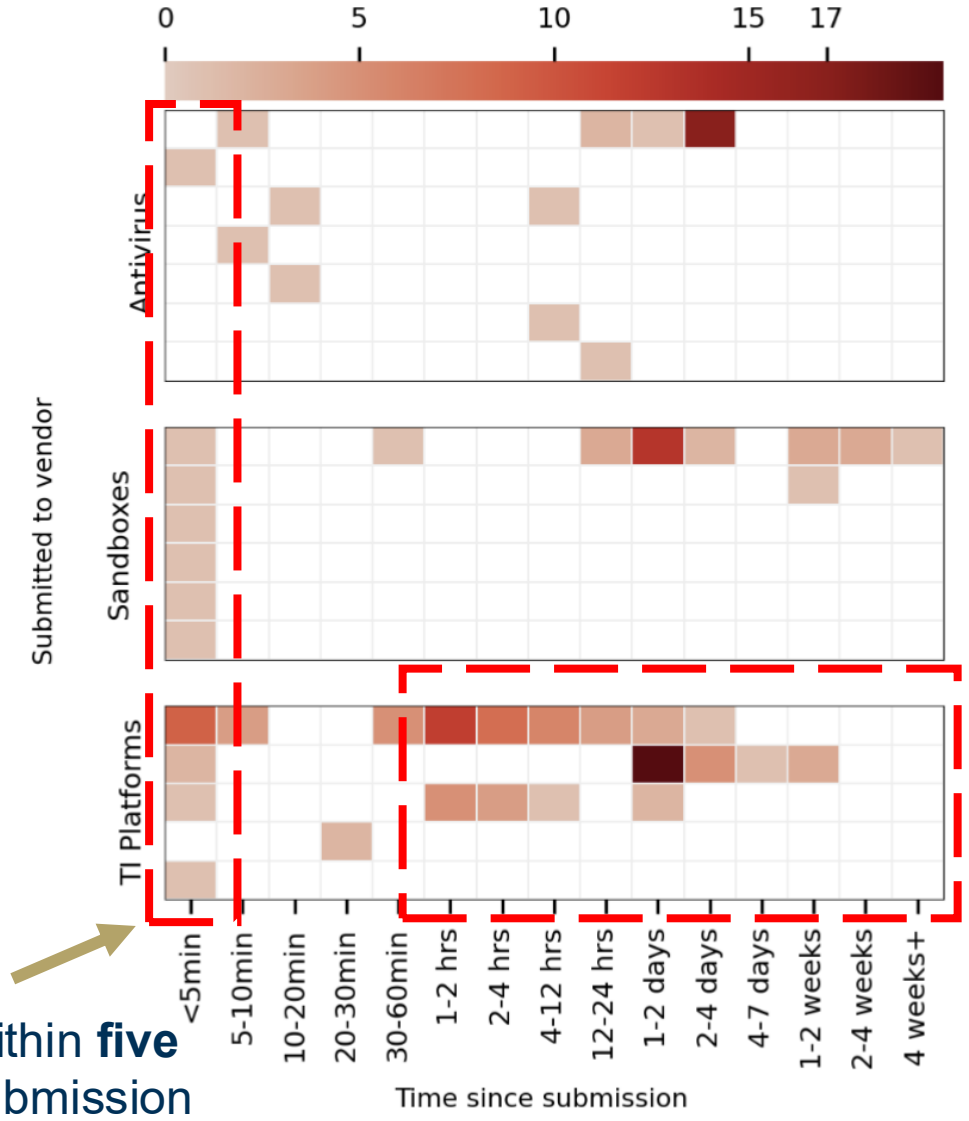
Georgia Tech

Sharing relationships between vendors



Georgia Tech

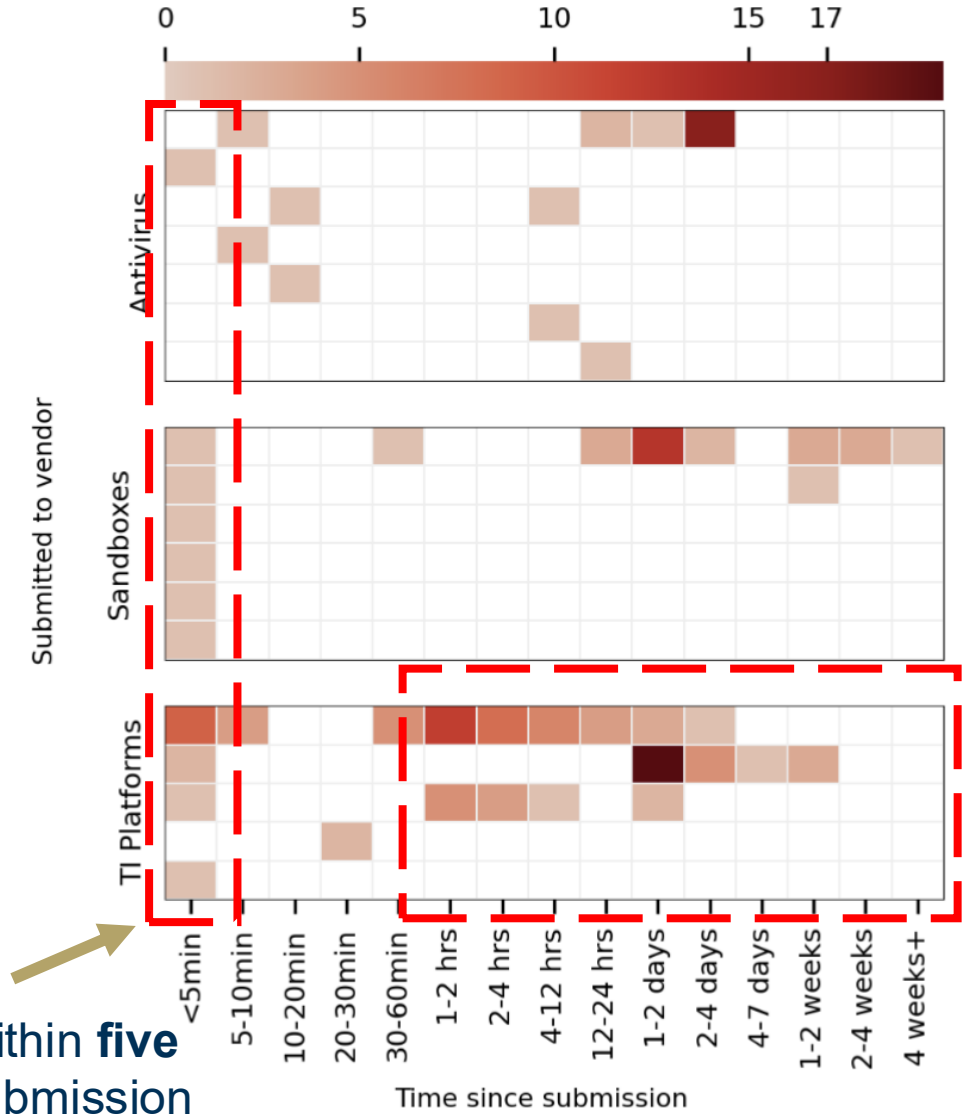
Sharing velocity: a global view



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

Georgia Tech

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**

Georgia Tech

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

Georgia Tech

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

Georgia Tech

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

Georgia Tech