RSAConference2022
San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **PART2-W08**

The State of Application Protection 2022

Sander Vinberg

Threat Research Evangelist, F5 Labs

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

Pompous Latin Motto

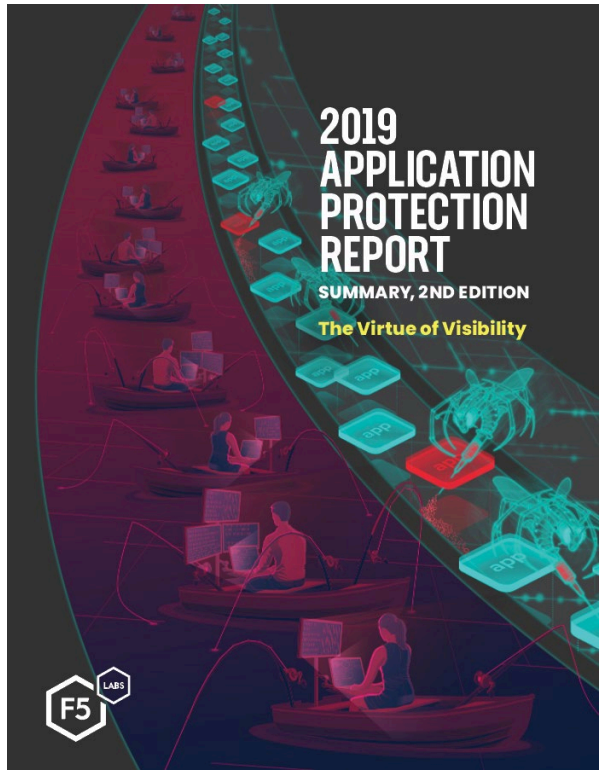
Experientia magistra stultorum

- Erasmus

Experience is the teacher of fools

Application Protection Report

Data-driven strategic security research



so you don't have to learn by "doing"

Agenda

- Methods & Sources
- Data Breach Analysis
  - Breach Attributes
  - Application Tiers Model
  - Attack Chain Analysis
- Notable Attacks & Campaigns
- Recommended Mitigations

State of the State of Security?

It depends on the angle.

Meta-analysis is not possible; multi-source analysis is next best thing.

https://www.f5.com/labs/articles/threat-intelligence/the-state-of-the-state-of-application-exploits-in-security-incidents

Cyentia INSTITUTE

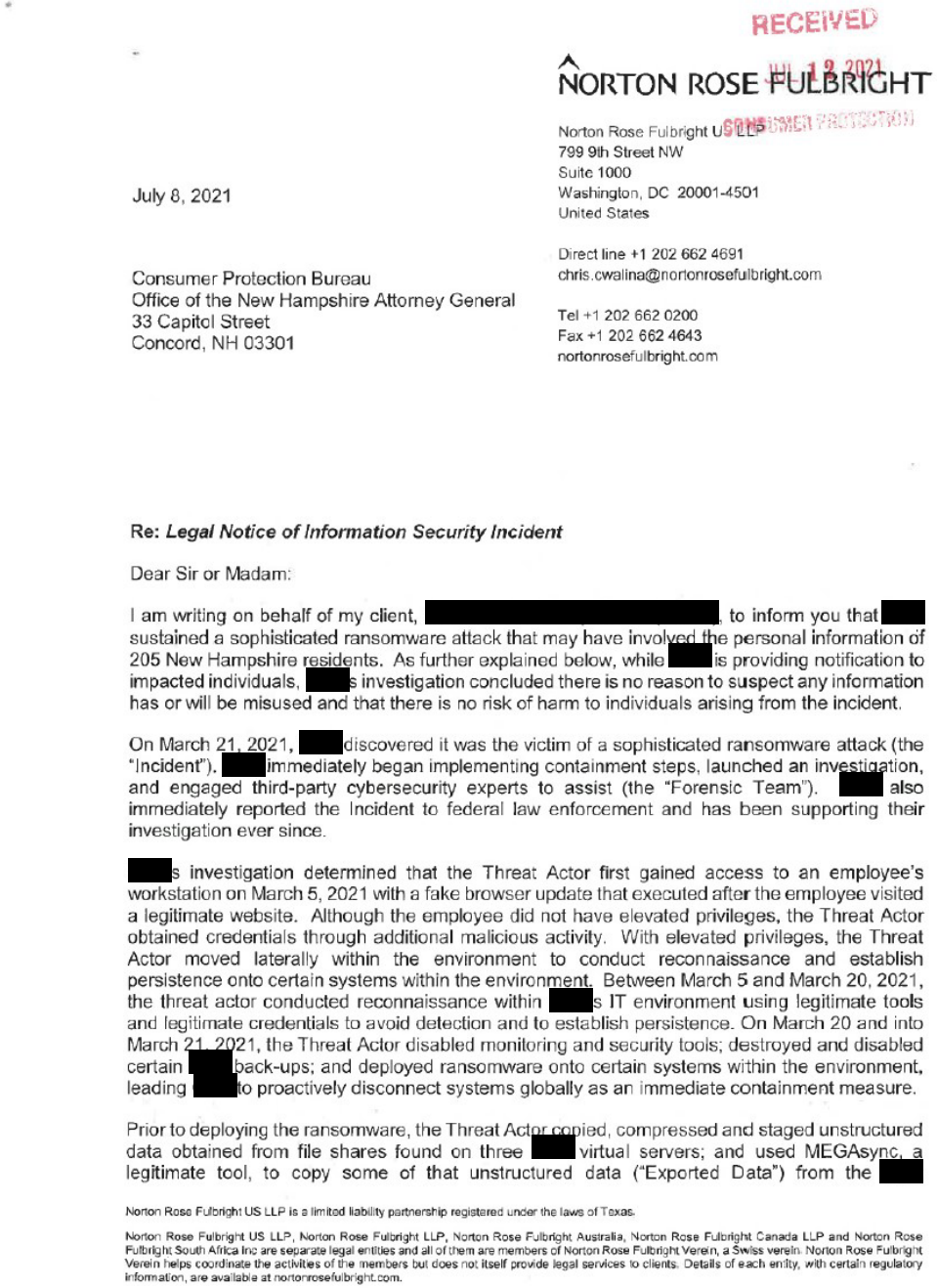
Sponsored by F5 LABS

The State of the State of Application Exploits in Security Incidents

A "SO-SO" MULTI-SOURCE ANALYSIS OF PUBLISHED INDUSTRY RESEARCH

Sources

- Why use breach disclosures?
  - All successful attacks
  - Nothing significant excluded for given time and space
- 2021 *n* = 980



RECEIVED
JUL 12 2021
CONSUMER PROTECTION

NORTON ROSE FULBRIGHT

Norton Rose Fulbright US LLP
799 9th Street NW
Suite 1000
Washington, DC 20001-4501
United States

Direct line +1 202 662 4691
chris.cwalina@nortonrosefulbright.com

Tel +1 202 662 0200
Fax +1 202 662 4643
nortonrosefulbright.com

July 8, 2021

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: *Legal Notice of Information Security Incident*

Dear Sir or Madam:

I am writing on behalf of my client, [redacted], to inform you that [redacted] sustained a sophisticated ransomware attack that may have involved the personal information of 205 New Hampshire residents. As further explained below, while [redacted] is providing notification to impacted individuals, [redacted]'s investigation concluded there is no reason to suspect any information has or will be misused and that there is no risk of harm to individuals arising from the incident.

On March 21, 2021, [redacted] discovered it was the victim of a sophisticated ransomware attack (the "Incident"). [redacted] immediately began implementing containment steps, launched an investigation, and engaged third-party cybersecurity experts to assist (the "Forensic Team"). [redacted] also immediately reported the Incident to federal law enforcement and has been supporting their investigation ever since.

[redacted]'s investigation determined that the Threat Actor first gained access to an employee's workstation on March 5, 2021 with a fake browser update that executed after the employee visited a legitimate website. Although the employee did not have elevated privileges, the Threat Actor obtained credentials through additional malicious activity. With elevated privileges, the Threat Actor moved laterally within the environment to conduct reconnaissance and establish persistence onto certain systems within the environment. Between March 5 and March 20, 2021, the threat actor conducted reconnaissance within [redacted]'s IT environment using legitimate tools and legitimate credentials to avoid detection and to establish persistence. On March 20 and into March 21, 2021, the Threat Actor disabled monitoring and security tools; destroyed and disabled certain [redacted] back-ups; and deployed ransomware onto certain systems within the environment, leading [redacted] to proactively disconnect systems globally as an immediate containment measure.

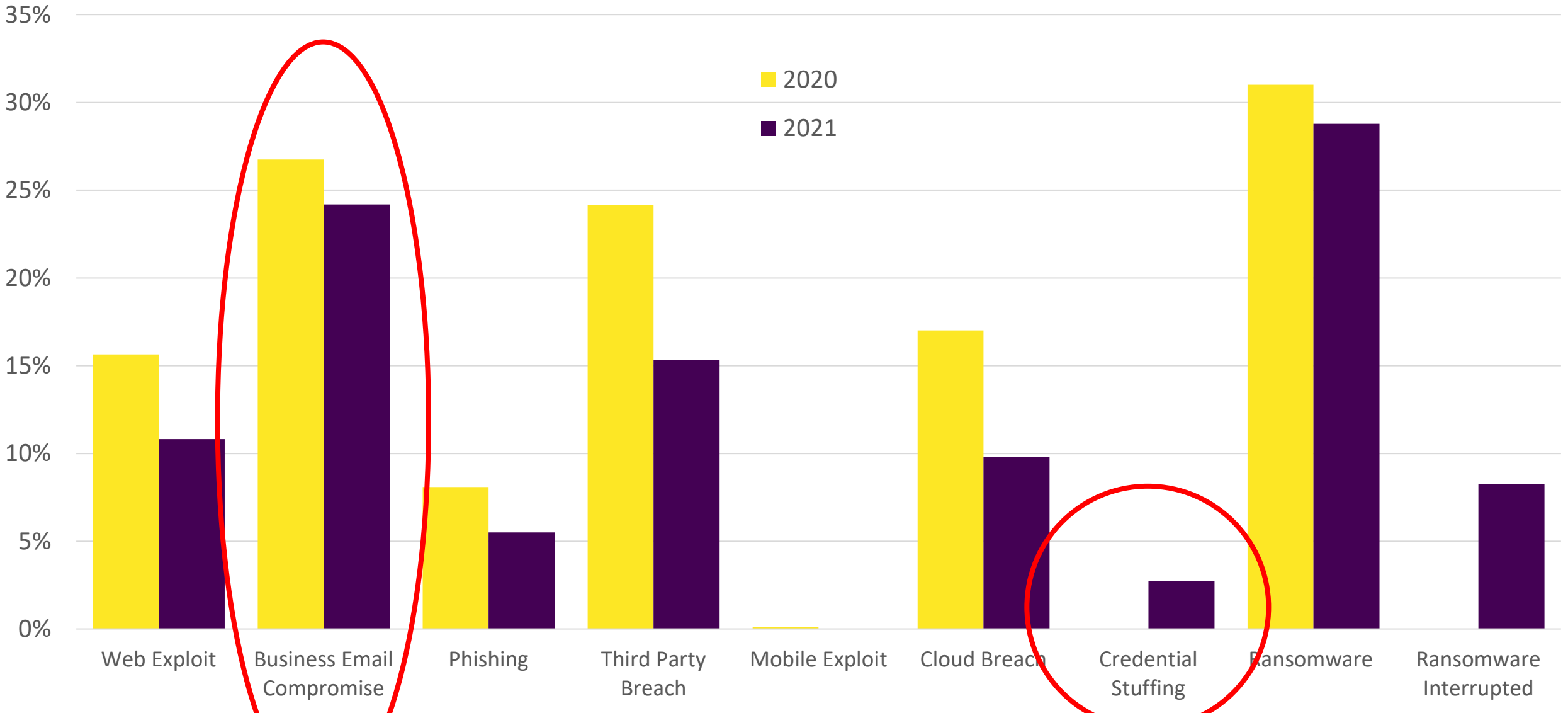
Prior to deploying the ransomware, the Threat Actor copied, compressed and staged unstructured data obtained from file shares found on three [redacted] virtual servers; and used MEGAsync, a legitimate tool, to copy some of that unstructured data ("Exported Data") from the [redacted]

RSAConference2022

Data Breach Analysis

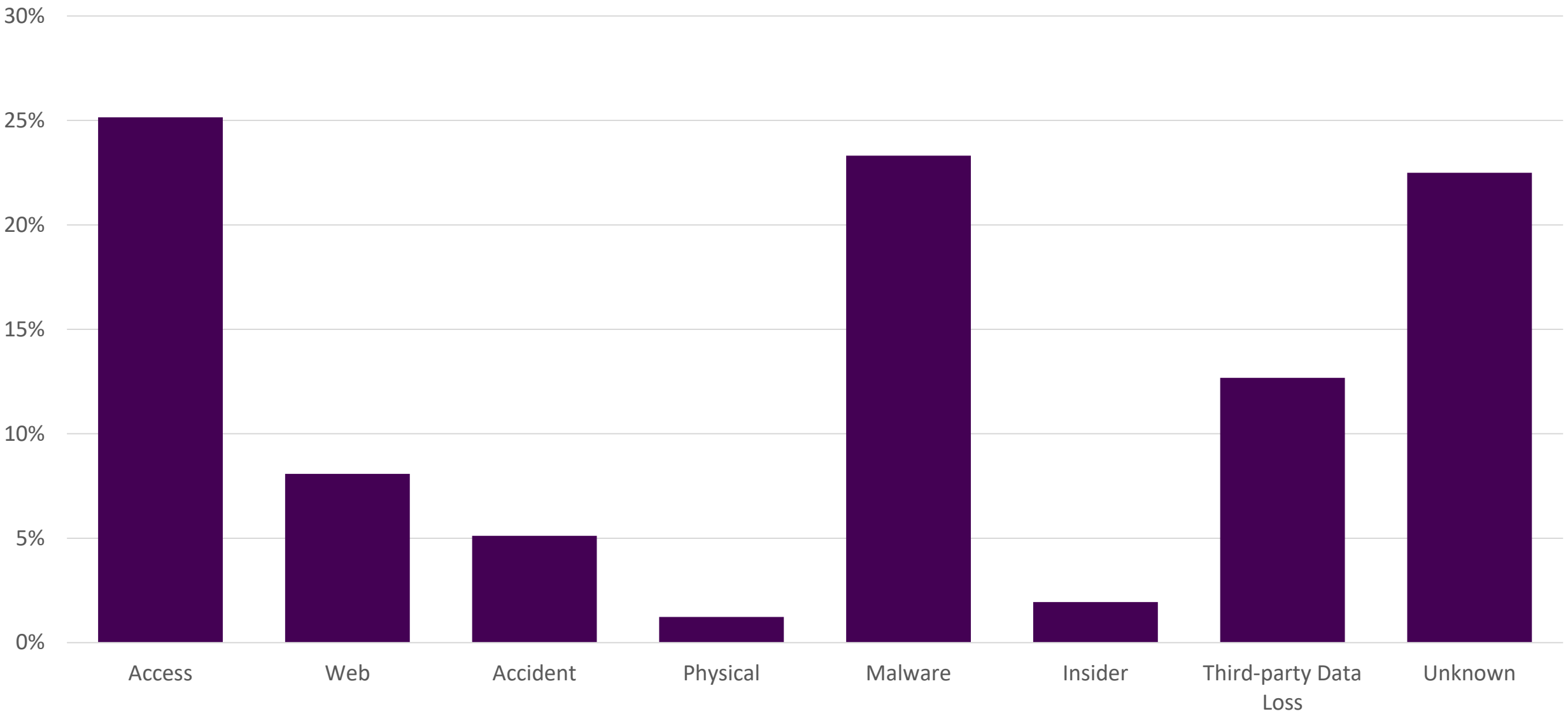
Breach Attributes

(flat, non-exclusive tags)



2021 U.S. Data Breach Distribution

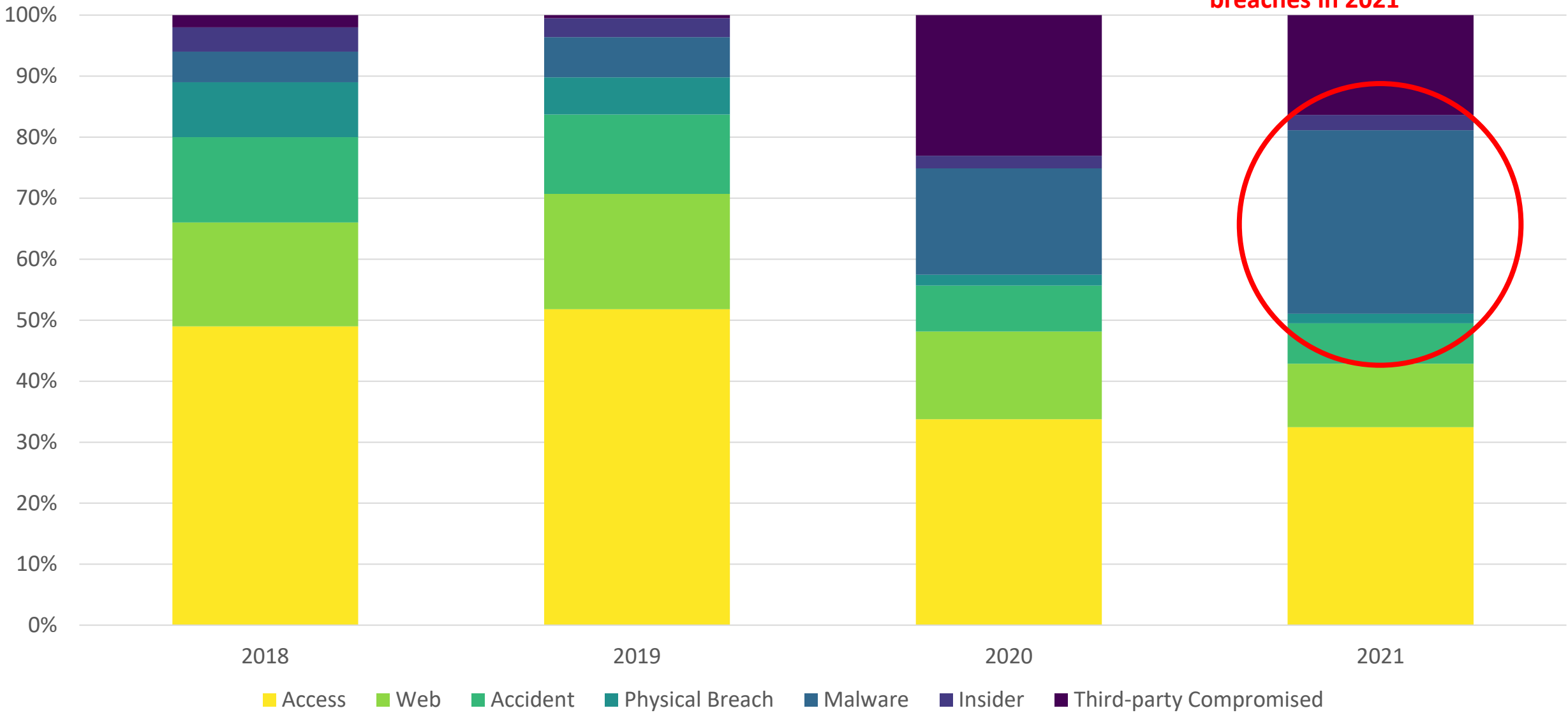
Simple view, Application Tiers Model, *n* = 980



2018-2021 U.S. Data Breach Distribution

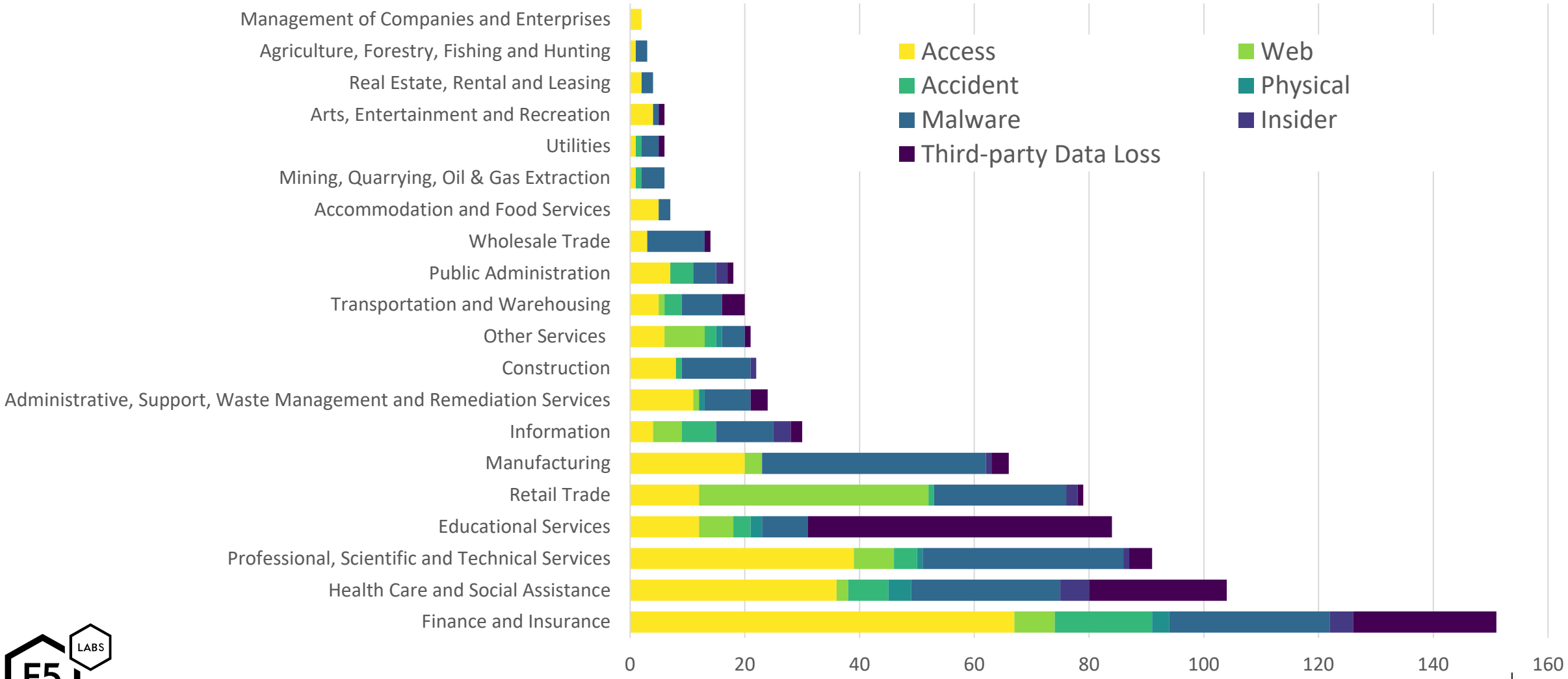
Historical view, Application Tiers Model, unknowns removed

Malware climbed to 30% of breaches in 2021



2021 U.S. Data Breach Causes by Sector

Unknowns removed, n = 758



Data Breach Analysis Summary

- Business email compromise present in at least 24% of attacks
  - Low reporting of credential stuffing and phishing, combined with high rate of BEC, indicates cred stuffing and phishing detection are poor
- Access breaches remain single most common breach cause
  - Includes credential stuffing, phishing, brute force
- Use of malware grew to make up 30% of all known breach causes
- Ransomware grew but nonencrypting malware also grew
- Web exploits less common than past years but still a threat to retail organizations
- Top 3 targeted sectors: Finance and Insurance; Health Care; Professional, Scientific & Technical Services

RSAConference2022

Attack Chain Analysis

(or, more accurately, ATT&CK chain)

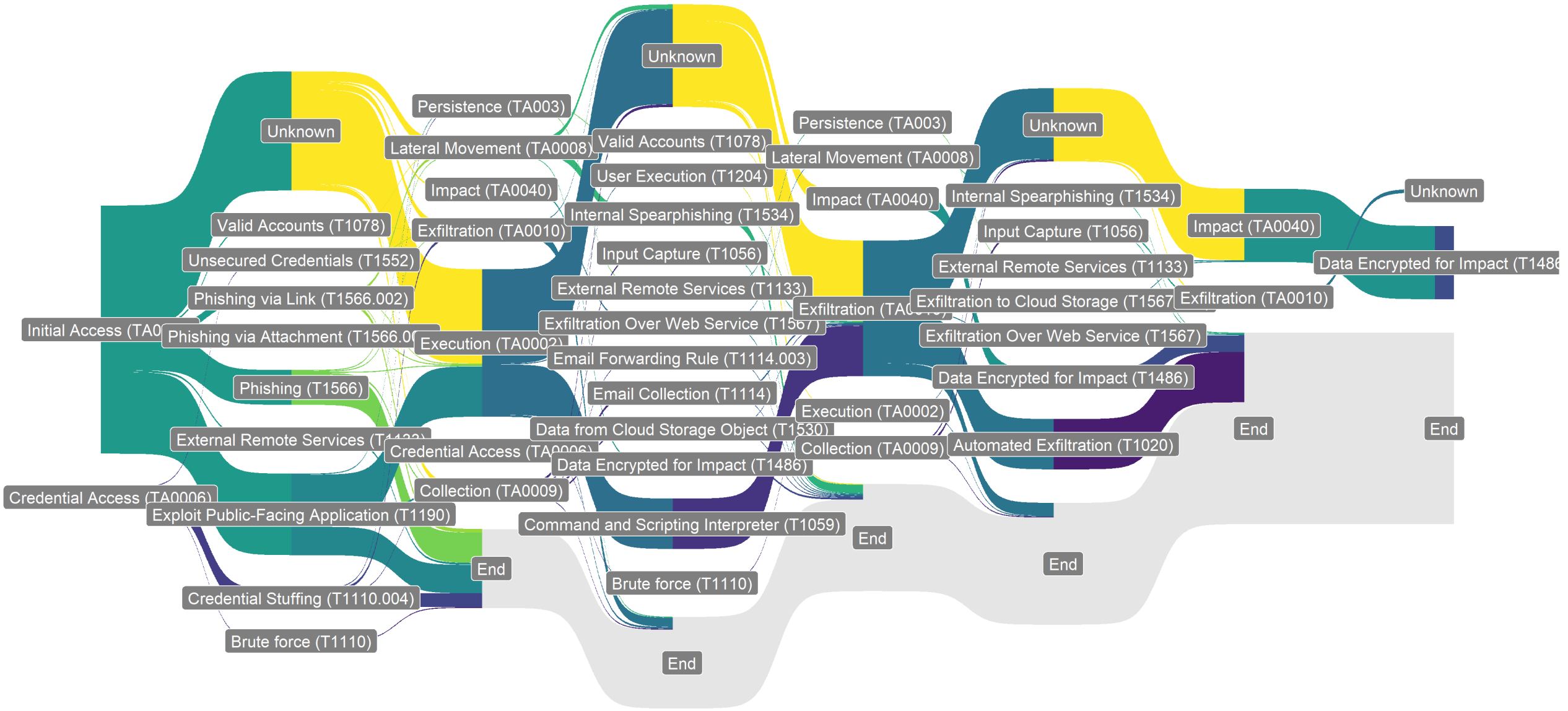
MITRE ATT&CK Framework

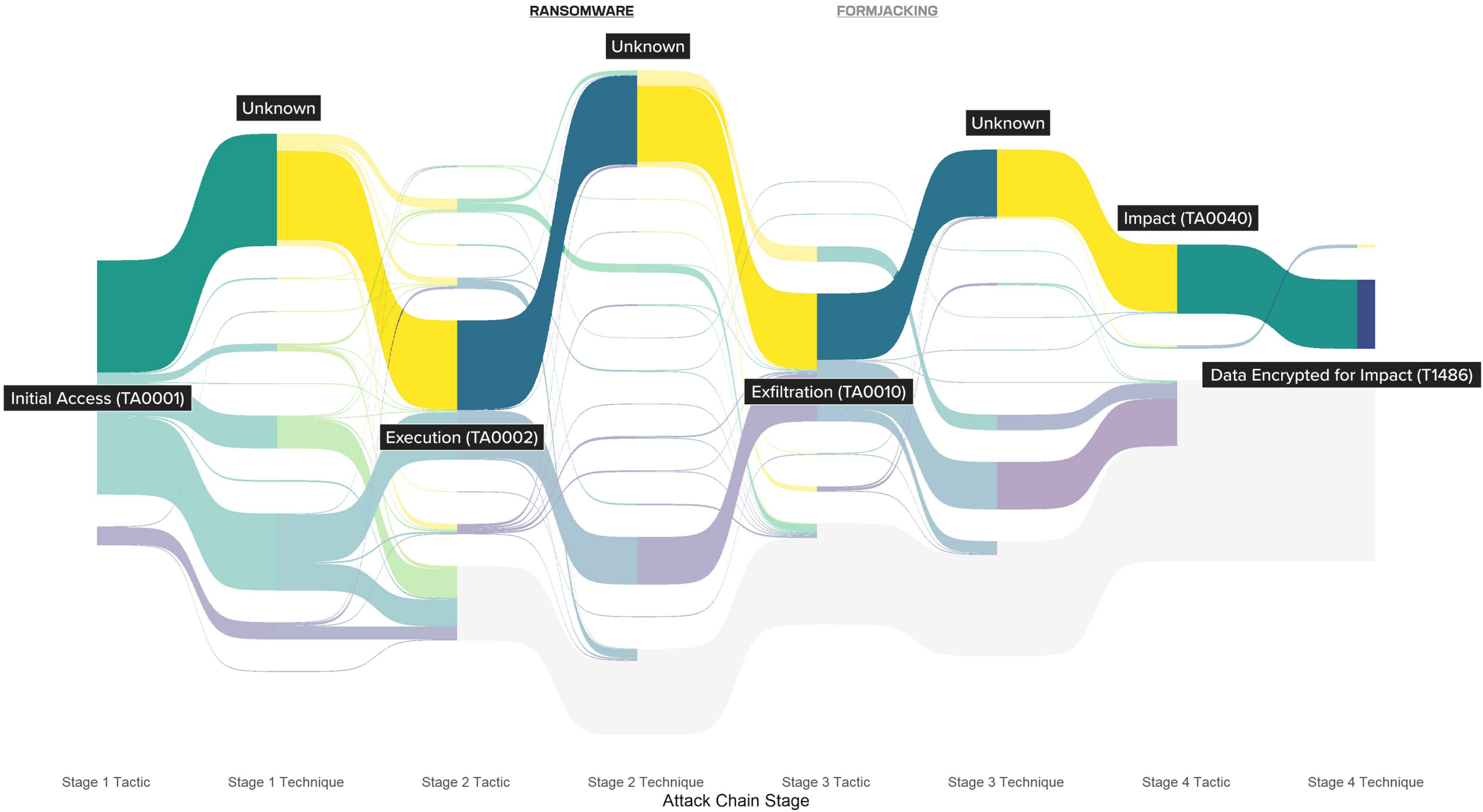
Tactics

Techniques

2020 U.S. Data Breach Attack Chains, Application Attacks Only

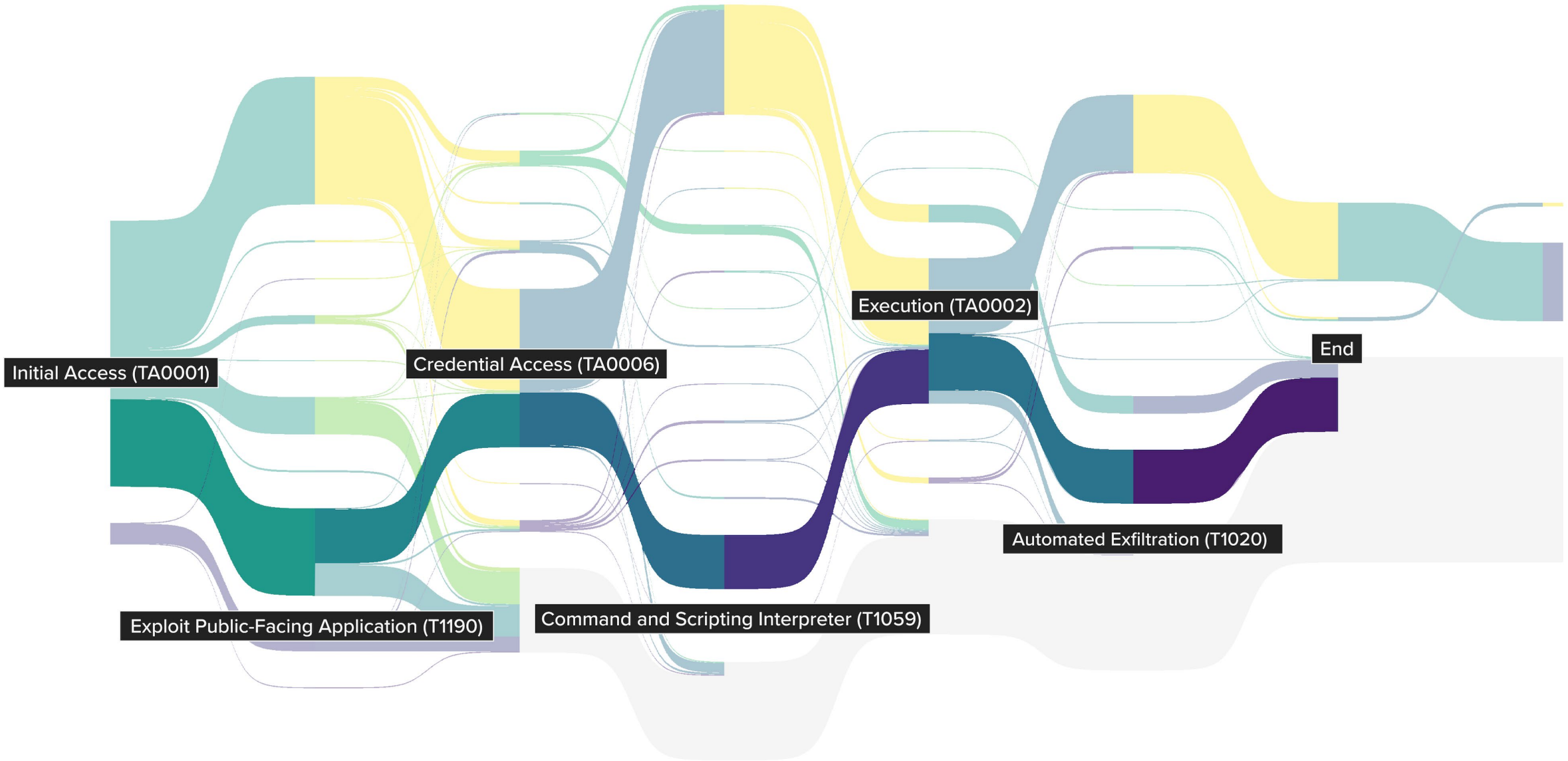
n = 253




RANSOMWARE
FORMJACKING
Unknown
Unknown
Unknown
Impact (TA0040)
Initial Access (TA0001)
Execution (TA0002)
Exfiltration (TA0010)
Data Encrypted for Impact (T1486)
Stage 1 Tactic
Stage 1 Technique
Stage 2 Tactic
Stage 2 Technique
Stage 3 Tactic
Stage 3 Technique
Stage 4 Tactic
Stage 4 Technique
Attack Chain Stage

RANSOMWARE

FORMJACKING

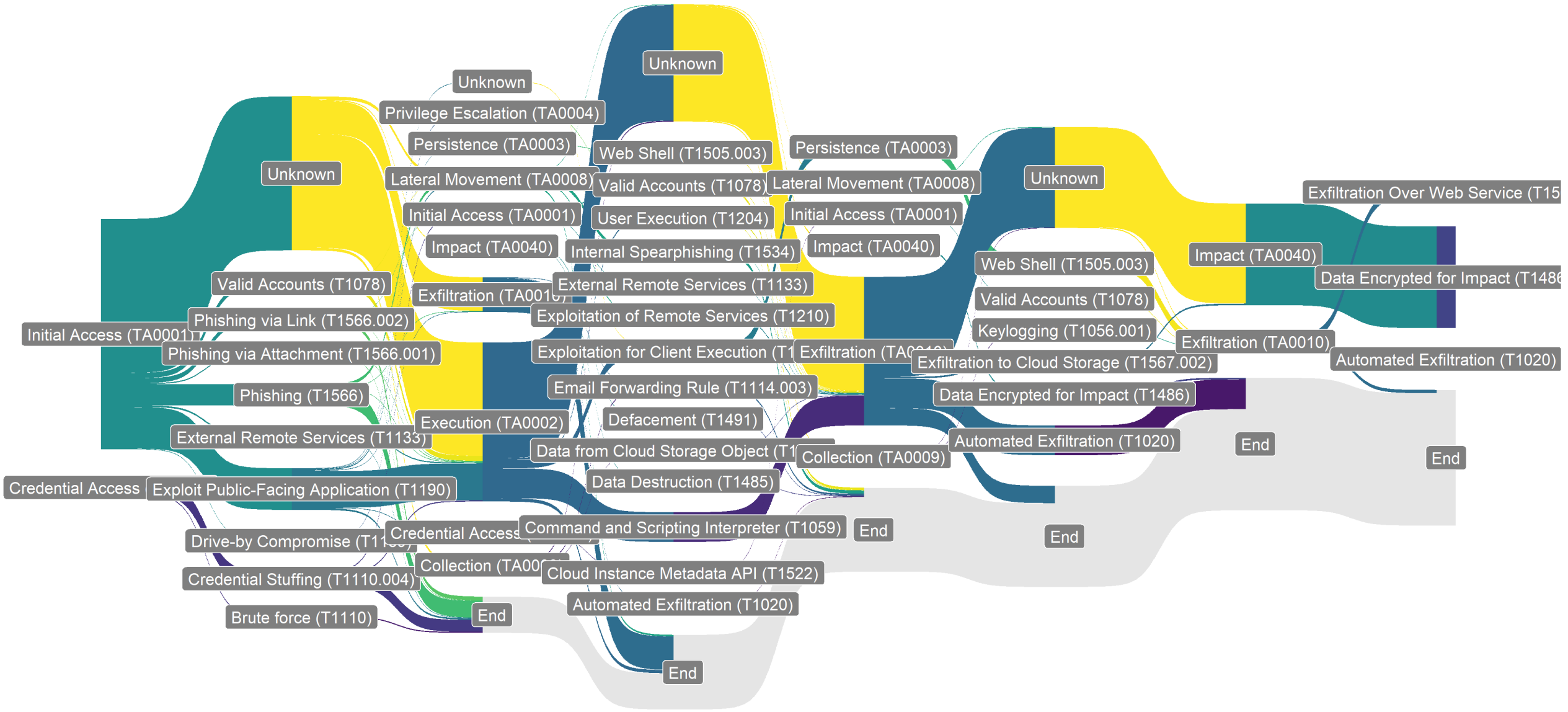


Stage 1 Tactic | Stage 1 Technique | Stage 2 Tactic | Stage 2 Technique | Stage 3 Tactic | Stage 3 Technique | Stage 4 Tactic | Stage 4 Technique

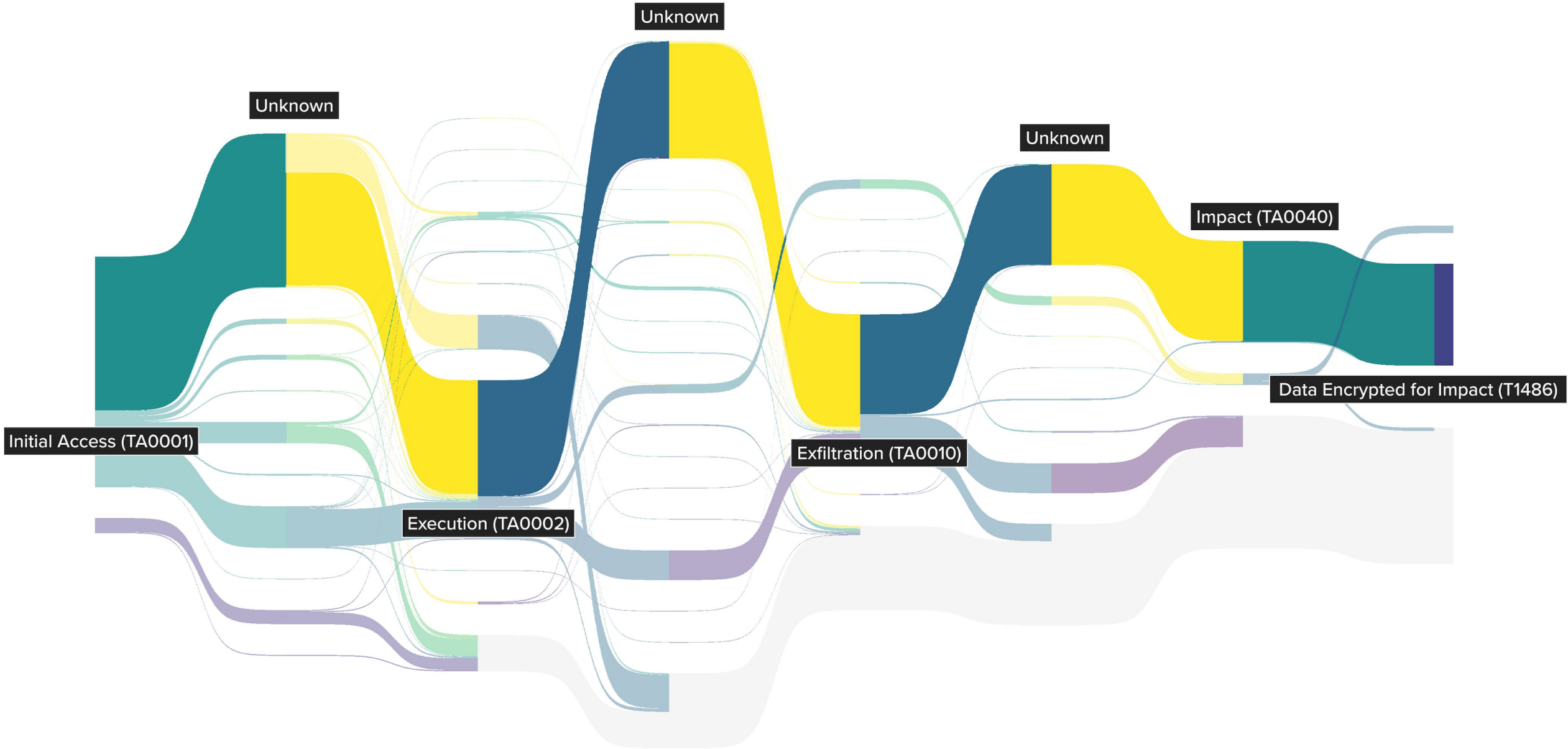
Attack Chain Stage

2021 U.S. Data Breach Attack Chains, Application Attacks Only

n = 454



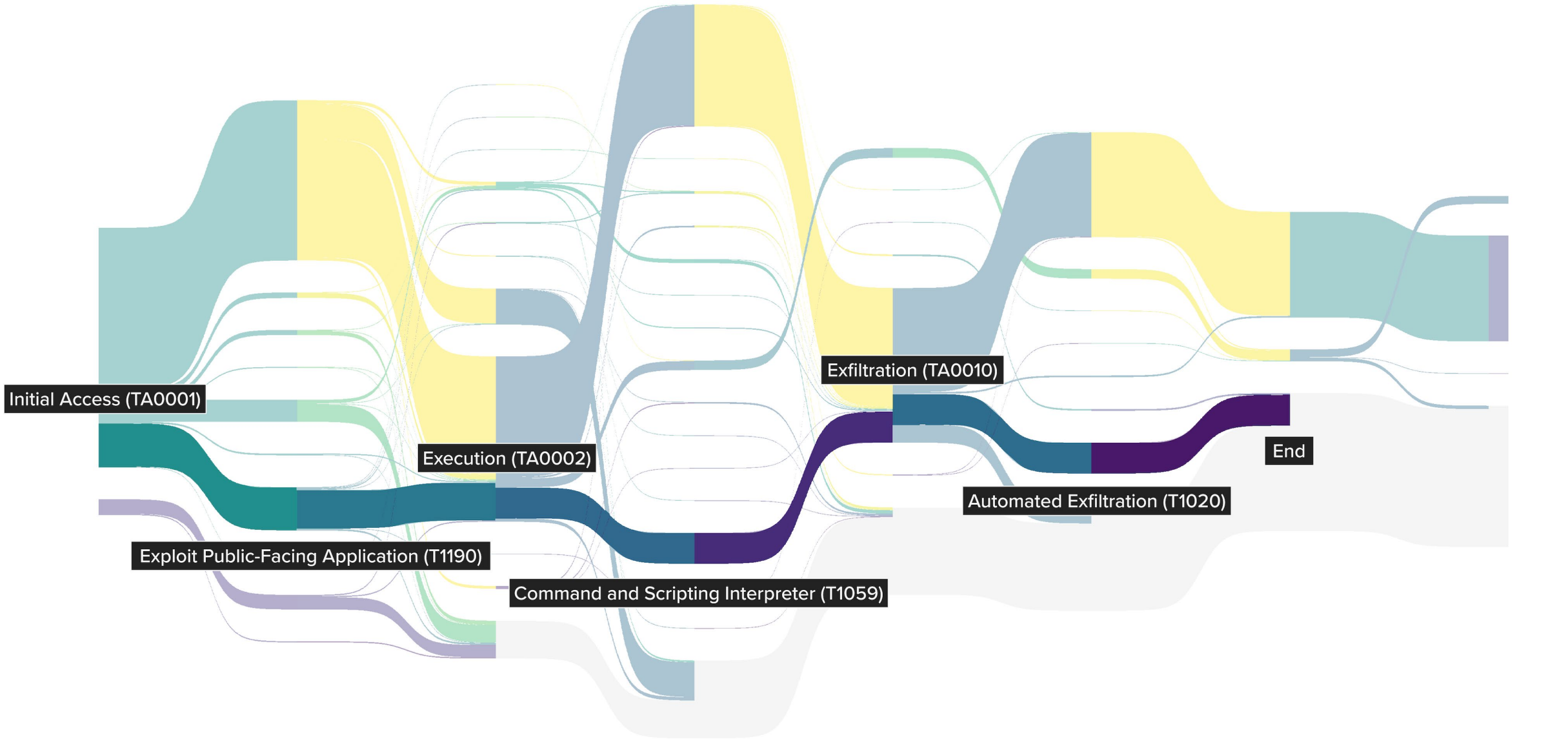
RANSOMWARE FORMJACKING NON-ENCRYPTING MALWARE ACCELLION FTA ATTACKS



Stage 1 Tactic | Stage 1 Technique | Stage 2 Tactic | Stage 2 Technique | Stage 3 Tactic | Stage 3 Technique | Stage 4 Tactic | Stage 4 Technique

Attack Chain Stage

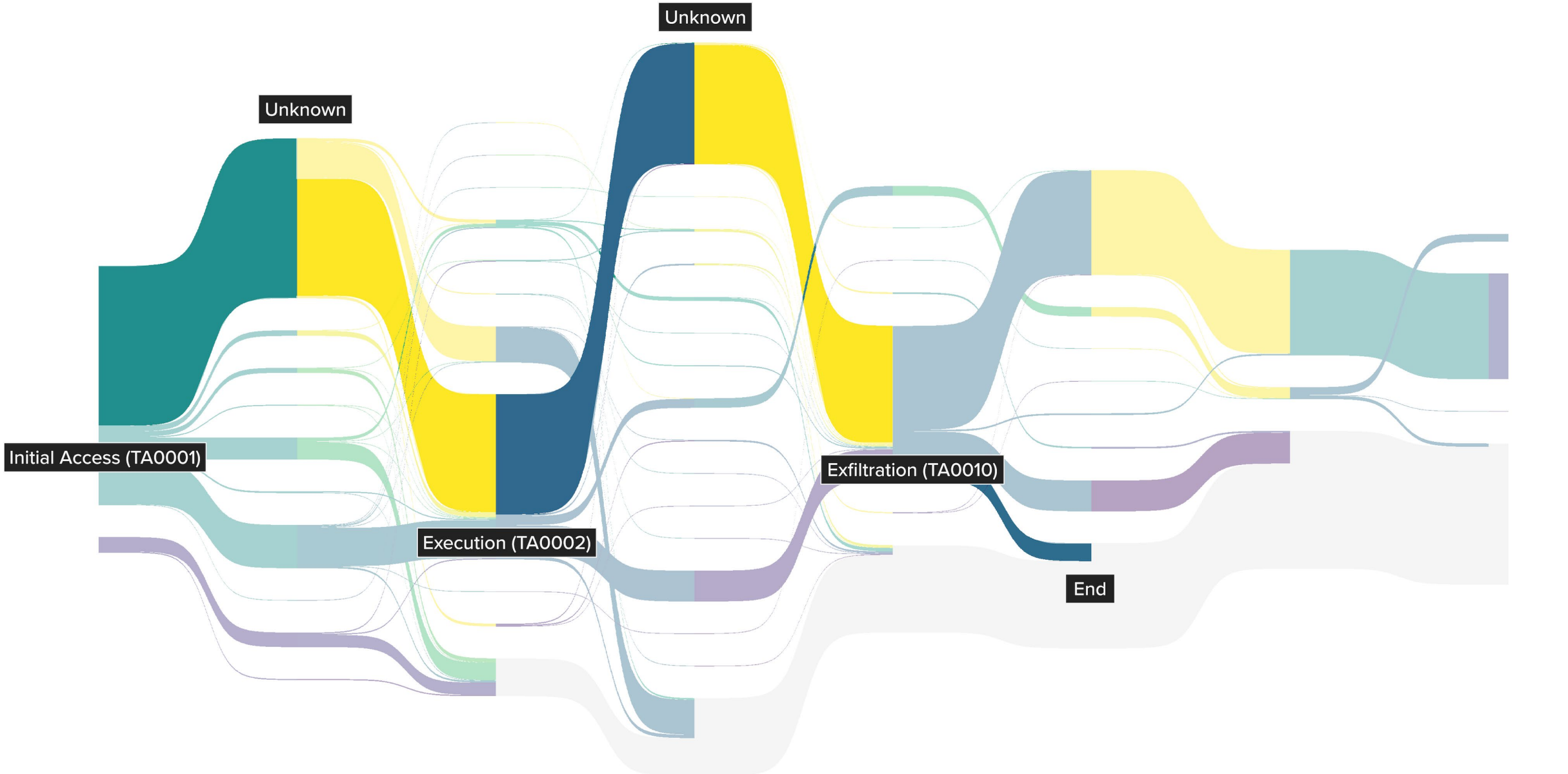
RANSOMWARE **FORMJACKING** NON-ENCRYPTING MALWARE ACCELLION FTA ATTACKS



Stage 1 Tactic | Stage 1 Technique | Stage 2 Tactic | Stage 2 Technique | Stage 3 Tactic | Stage 3 Technique | Stage 4 Tactic | Stage 4 Technique

Attack Chain Stage

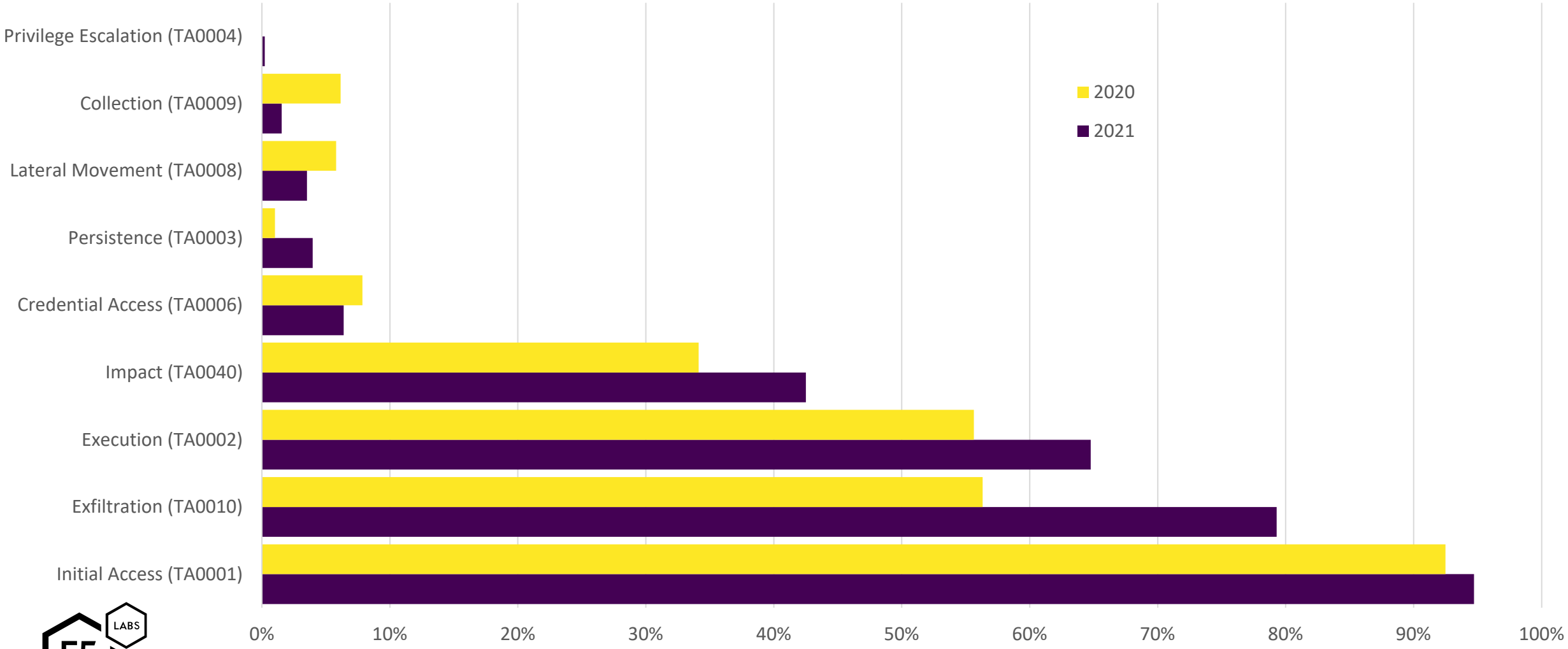
RANSOMWARE FORMJACKING **NON-ENCRYPTING MALWARE** ACCELLION FTA ATTACKS



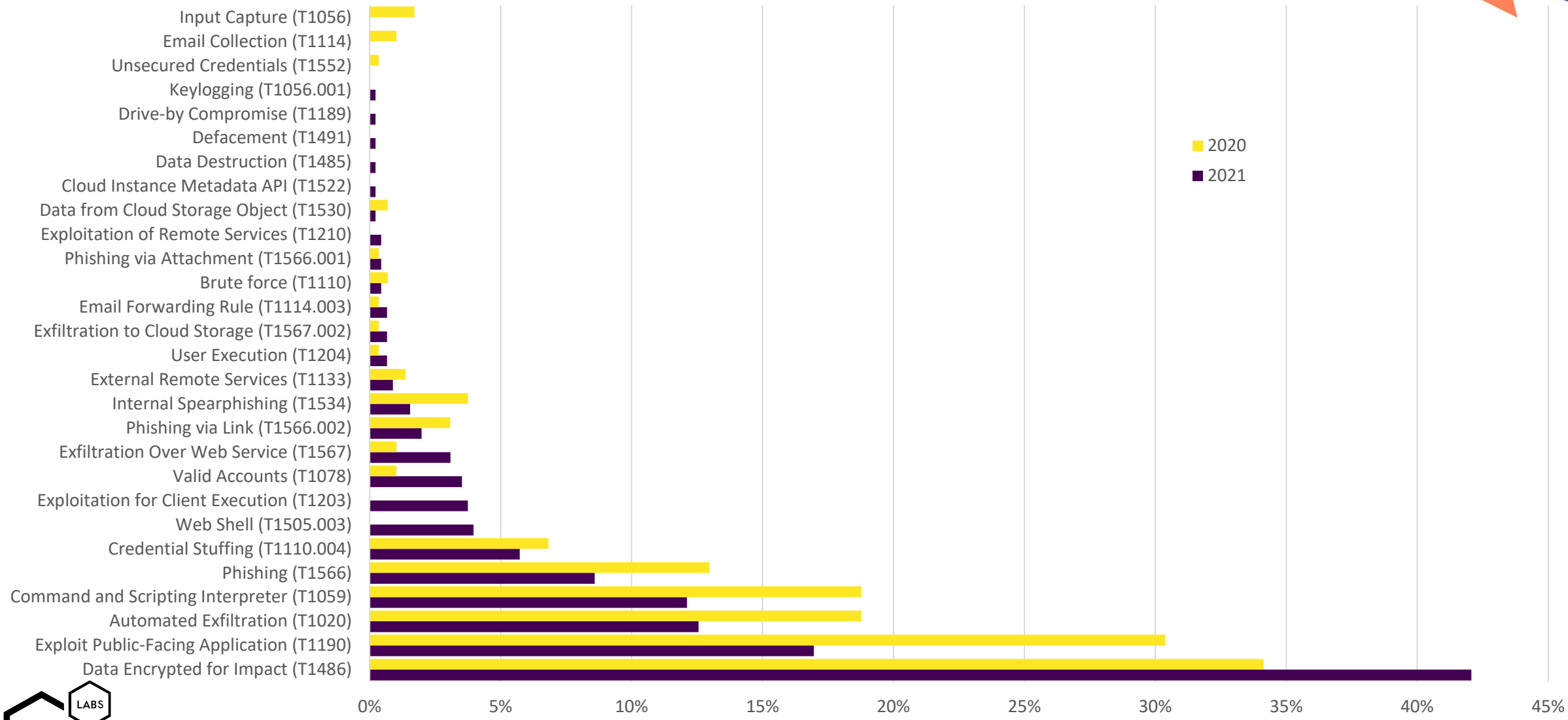
Stage 1 Tactic | Stage 1 Technique | Stage 2 Tactic | Stage 2 Technique | Stage 3 Tactic | Stage 3 Technique | Stage 4 Tactic | Stage 4 Technique

Attack Chain Stage

ATT&CK Tactics in U.S. Data Breaches, 2020-2021



ATT&CK Techniques in U.S. Data Breaches, 2020-2021



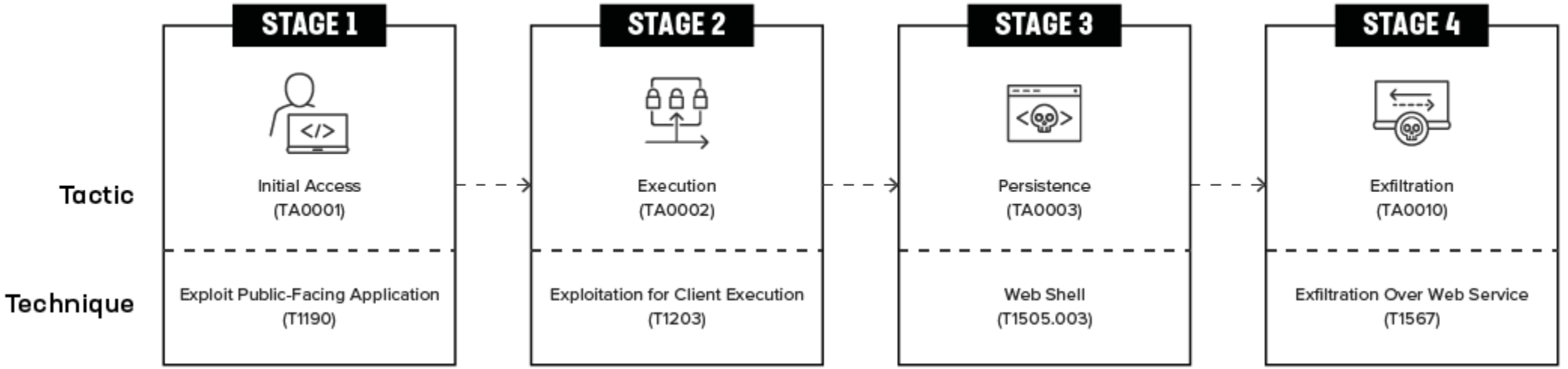
Attack Chain Analysis Summary

- Use of execution increased, reflecting the growing impact of malware
- Exfiltration techniques increased significantly, making up ~80% of application attacks
- Ransomware increased significantly, playing a role in 42% of application attacks
- Web exploits decreased, but became more focused on formjacking
- Attack chains illustrate importance of defense in depth, balancing analysis of tactics with that of techniques

RSAConference2022

Notable Attacks and Campaigns

Accellion FTA Attack Campaign



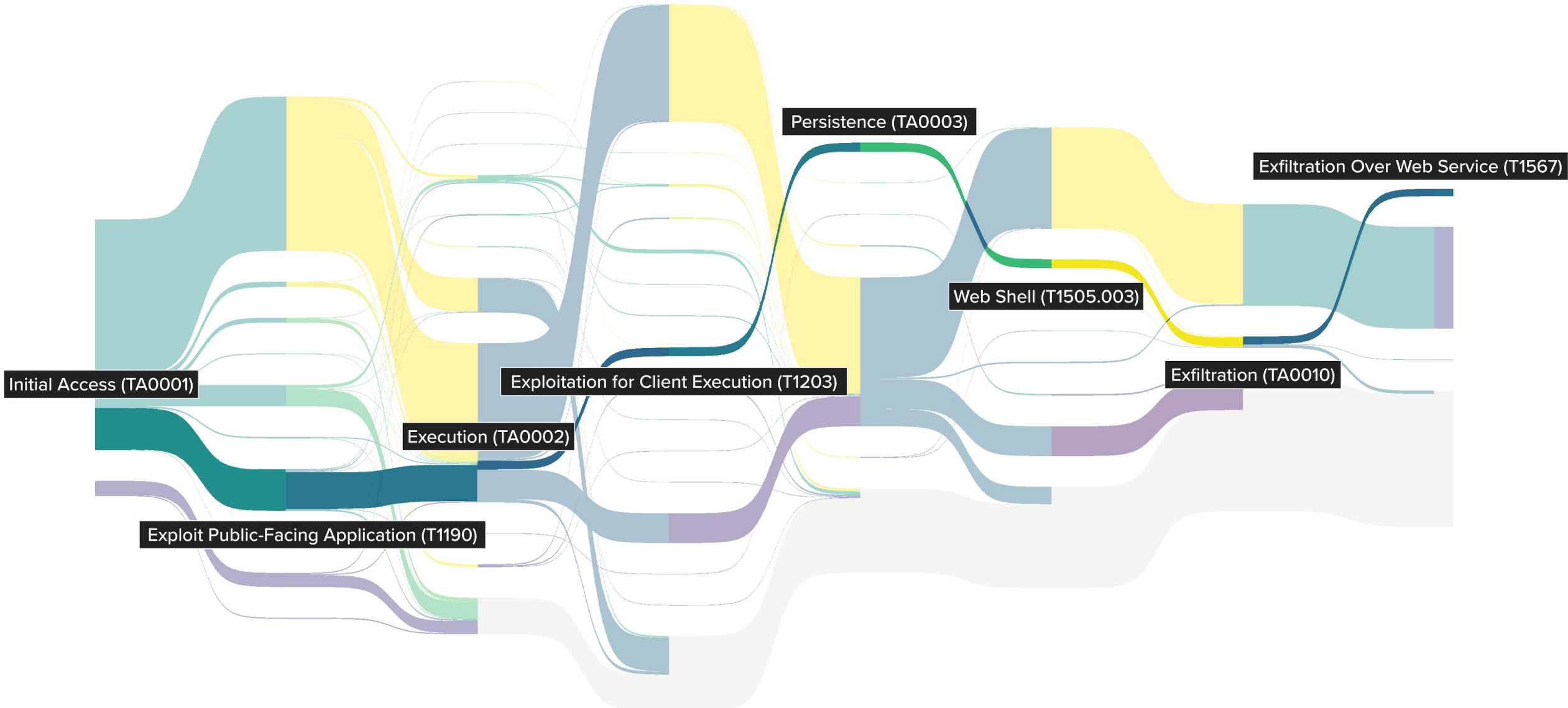
- Attacker exploits a SQL injection vulnerability in the Accellion File Transfer Appliance (FTA) product.
- The injection attack retrieves a key that allows attacker to write an eval-style PHP web shell to the file oauth.api.
- Final payload, the DEWMODE web shell, is delivered by the initial web shell.
- DEWMODE scans the MySQL database within FTA and lists available files and metadata on an HTML page for the attacker.
- The attacker uses DEWMODE to exfiltrate selected files from the database.
- The attacker initiates a cleanup process that uses a shell script to modify a log file, overwrite the incriminating log file with the modified one, remove DEWMODE and the eval web shell, and delete the cleanup script and related temporary files.

RANSOMWARE

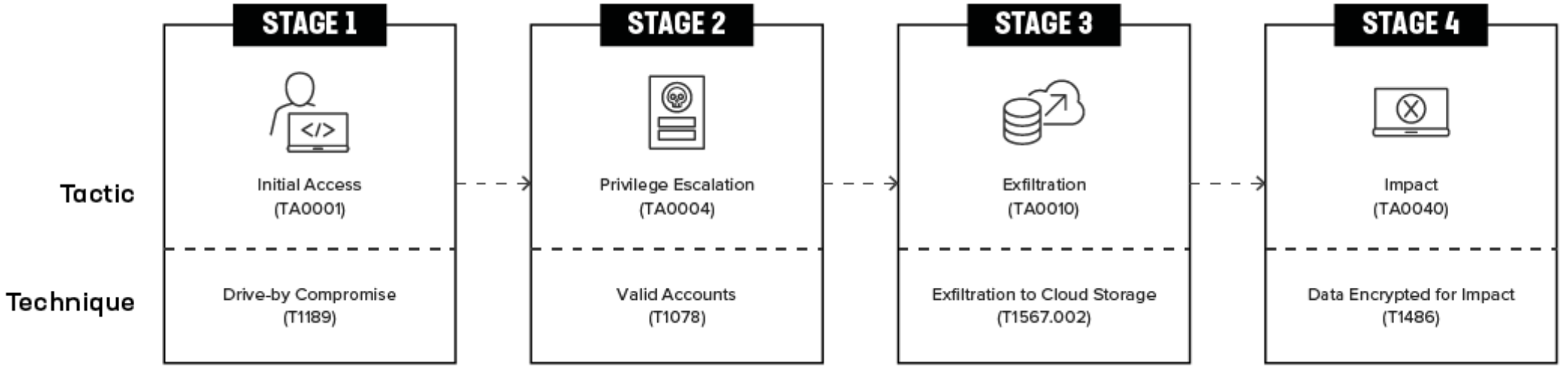
FORMJACKING

NON-ENCRYPTING MALWARE

ACCELLION FTA ATTACKS



Ransomware TTP Details



- Drive-by compromise masquerading as browser update
- Attacker obtained credentials with elevated privileges through unspecified activity
- Lateral movement for reconnaissance and persistence using legitimate tools and credentials
- Disabled monitoring and security tools, destroyed backups.
- Copied, compressed, and staged data from three virtual hosts for exfiltration
- Exfiltration using MEGAsync to cloud storage
- Encrypted data using unspecified ransomware

Additional Notable Campaigns

Auto Insurance Data Scraping Campaign

- Targets include large insurers like GEICO as well as small, local companies
- Automated scraping using seed information found elsewhere
- Third-party data feed provided drivers' license numbers in HTML source, but not displayed on screen
- License numbers used heavily in unemployment fraud
- 13 organizations known to have been breached this way in 2021.

Repeat Formjacking

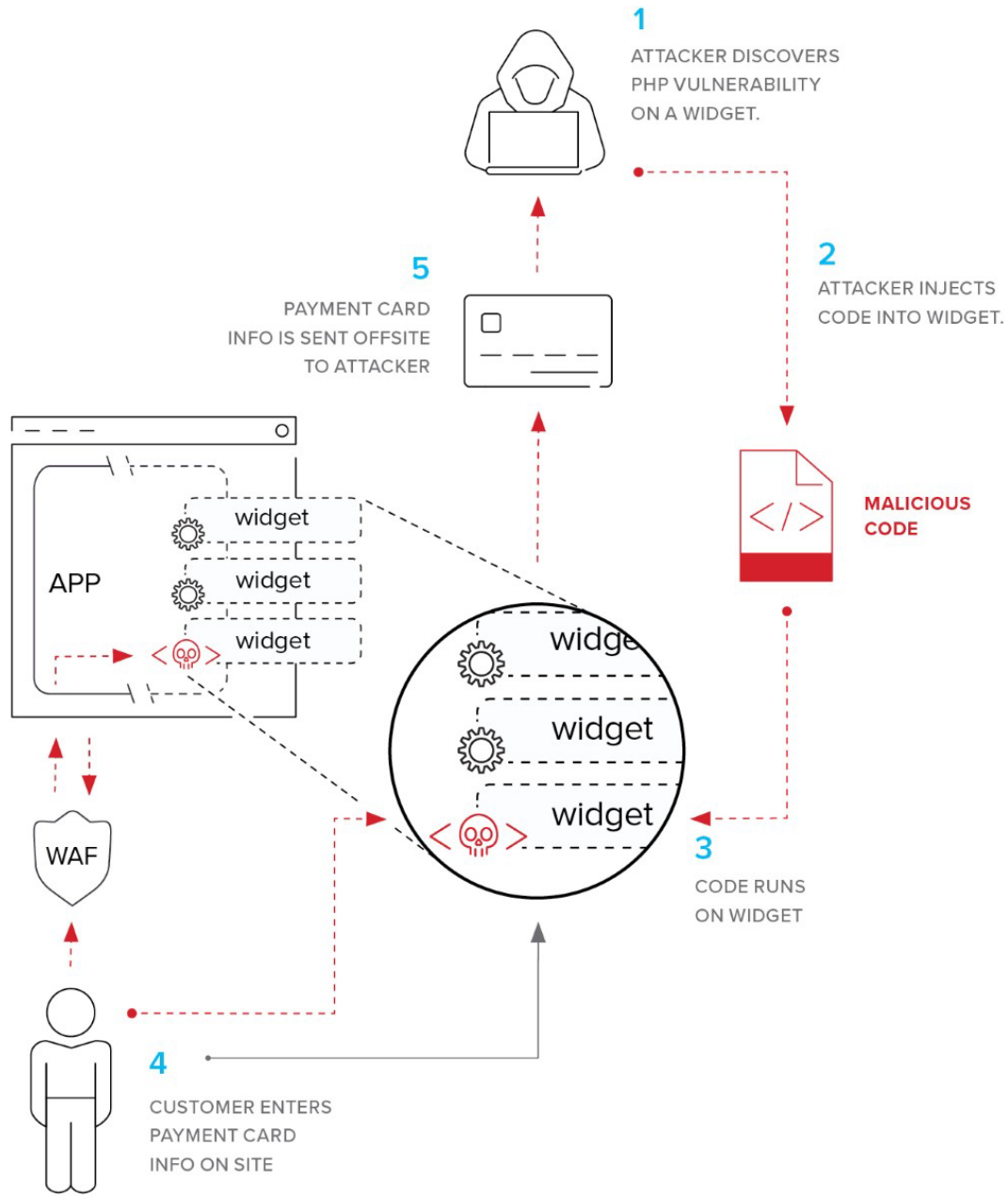
- Multiple instances each year of repeat formjacking attacks
- Organizations compromised by same attack multiple times in succession after ending incident response
- Greatest variation in formjacking attacks lies in initial access and masquerading techniques
- Illustrates dangers of declaring victory too early

Putting Ransomware in Context

- Ransomware tactics have evolved
  - Exfiltration prior to encryption for added leverage
  - Long dwell times
  - Backups often destroyed or encrypted – not a definitive fix
  - Ransomware-as-a-Service and affiliate models increase both likelihood and impact of attack
- Better to view ransomware as an alternative monetization approach to fraud, not as DoS
- Resilience of fraud pipeline in 2021 a surprise, but ransomware still growing

Understanding Formjacking

- Injection attack (usually) to place malicious skimmer script onto retail payment processing functions
- Targets not limited to retail – any application that accepts payment is a target
- Great variety in masquerading, exfiltration techniques
- Diversity of malicious formjacking scripts grew 20x in 2021
  - Onus is on vulnerability management, not signatures
- CSP, SRI potential controls for the right organizations



RSAConference2022

Recommended Mitigations

For more information:
https://attack.mitre.org/mitigations/enterprise/

Recommended Mitigations I

Sorting by Frequency (depth)

Mitigation	Frequency
Data backup	0.42
Application isolation and sandboxing	0.17
Exploit protection	0.17
Network segmentation	0.17
Privileged account management	0.17
Update software	0.17
Vulnerability scanning	0.17
Filter network traffic	0.13
Network intrusion prevention	0.13
Antivirus/antimalware	0.12
Code signing	0.12
Disable or remove feature or program	0.12
Execution prevention	0.12
Restrict web-based content	0.12
User training	0.09
Account use policies	0.06
Multifactor authentication	0.06
Password policies	0.06
User account management	0.06
Application developer guidance	0.04
Limit access to resource over network	0.03
Audit	0.01
Encrypt sensitive information	0.01
Threat intelligence program	0.00
Restrict file and directory permissions	0.00

Recommended Mitigations II

Sorting by Coverage (breadth)

Mitigation	Coverage
Restrict web-based content	7
Disable or remove feature or program	5
Multifactor authentication	5
Network segmentation	5
User training	5
Application isolation and sandboxing	4
Exploit protection	4
Network intrusion prevention	4
Privileged account management	4
User account management	4
Antivirus/antimalware	3
Data backup	3
Filter network traffic	3
Password policies	3
Update software	3
Account use policies	2
Audits	2
Encrypt sensitive information	2
Execution prevention	2
Limit access to resource over network	2
Vulnerability scanning	2
Application developer guidance	1
Code signing	1
Restrict file and directory permissions	1
Threat intelligence program	1

Recommended Mitigations III

Frequency (depth) x Coverage (breadth) = Arbitrary Effectiveness Coefficient

Mitigation	Arbitrary Effectiveness Coefficient
Data backup	1.26
Network segmentation	0.85
Restrict web-based content	0.85
Application isolation and sandboxing	0.68
Exploit protection	0.68
Privileged account management	0.68
Disable or remove feature or program	0.61
Update software	0.51
Network intrusion prevention	0.50
User training	0.43
Filter network traffic	0.38
Antivirus/antimalware	0.36
Vulnerability scanning	0.34
Multifactor authentication	0.29
Execution prevention	0.24
User account management	0.23
Password policies	0.17
Code signing	0.12
Account use policies	0.11
Limit access to resource over network	0.06
Application developer guidance	0.04
Audit	0.01
Encrypt sensitive information	0.01
Threat intelligence program	0.00
Restrict file and directory permissions	0.00

https://attack.mitre.org/mitigations/enterprise/

“Apply” Slide

- Next week, you should:
  - Begin hardening processes by ensuring your inventory is up to date
  - Scope a multifactor authentication initiative (if not in place)
  - Assess backup capabilities; expand if necessary, test recovery
- Within three months, you should:
  - Have begun hardening processes identified in inventory
- Within six months, you should:
  - Have set up monitoring and alerts for pre-ransomware tactics

Thanks for joining me today.
Read more at f5labs.com.
Feedback welcome at f5labs@f5.com