proofpoint®

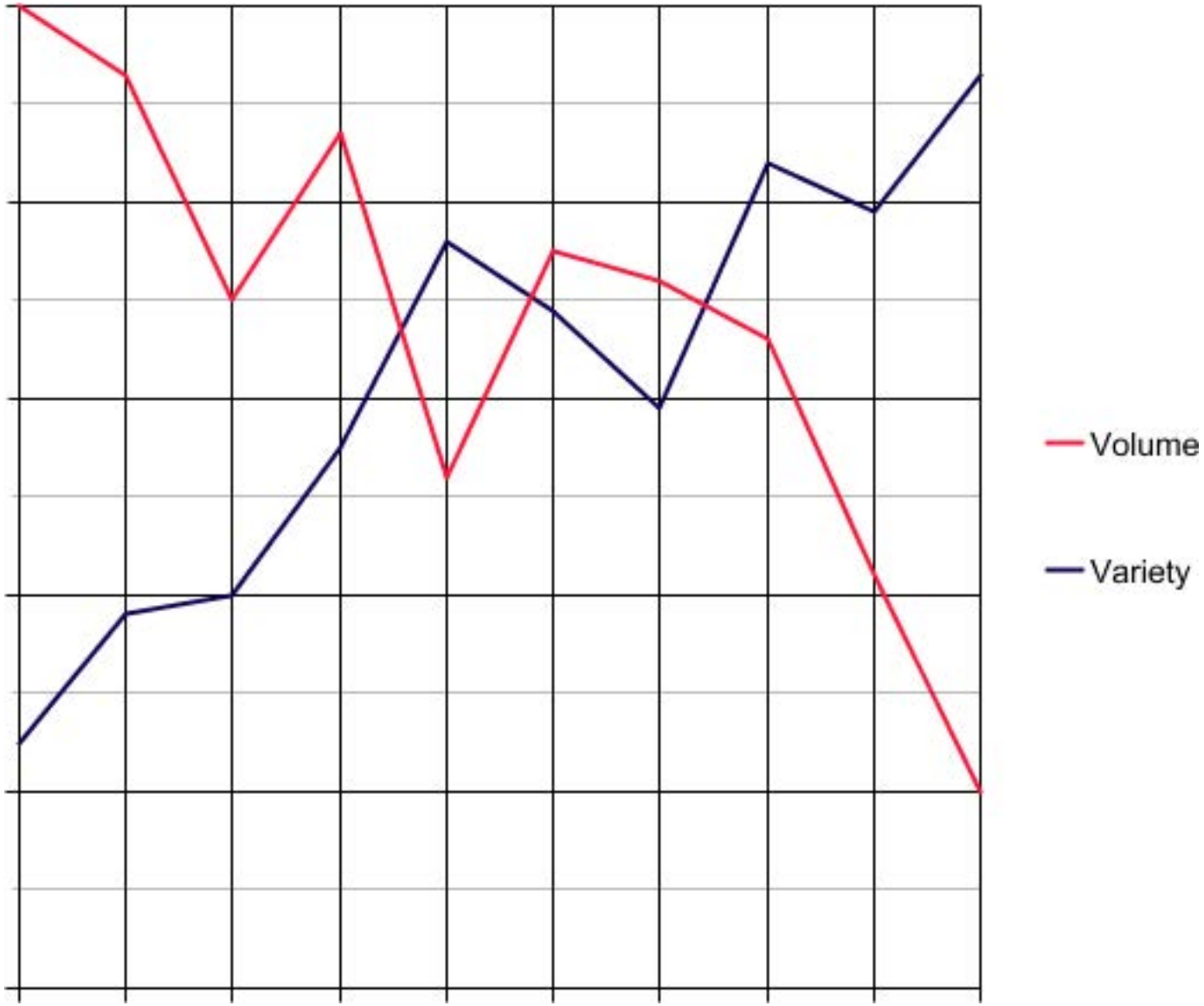
Threat Landscape

John Daly - Sr. Sales Engineer SLED West

jdaly@proofpoint.com

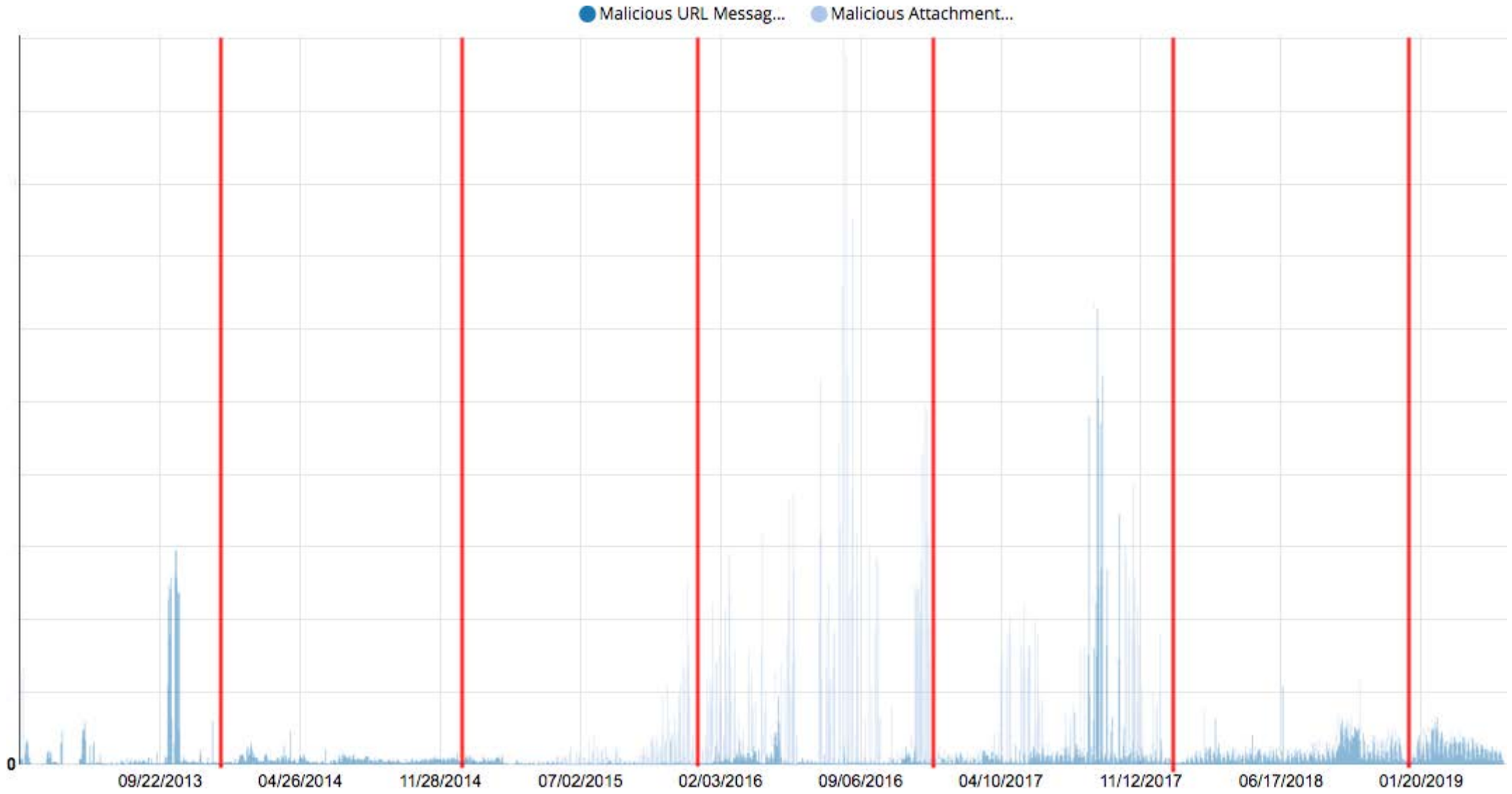
Global Trends

proofpoint®

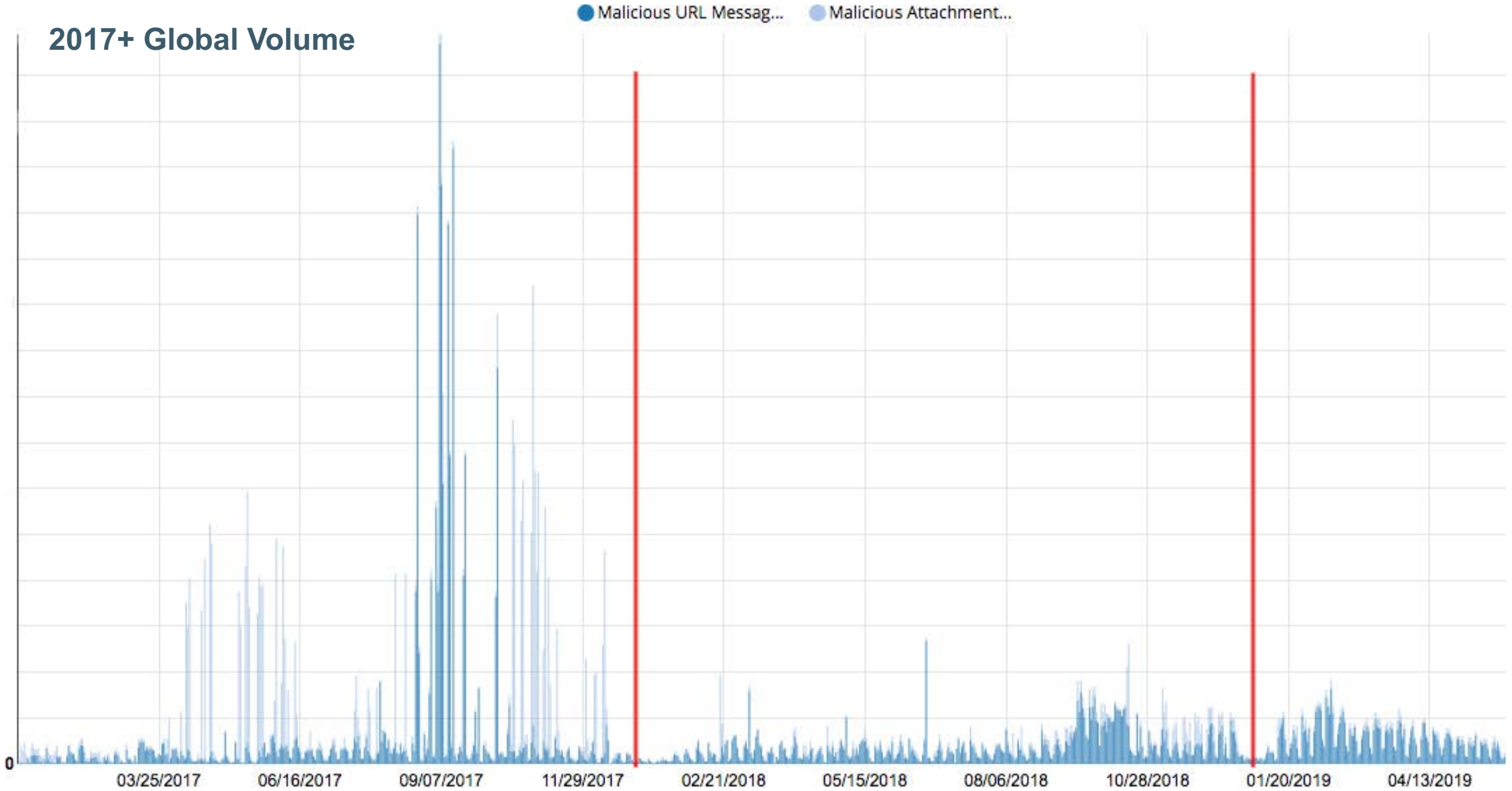


proofpoint.

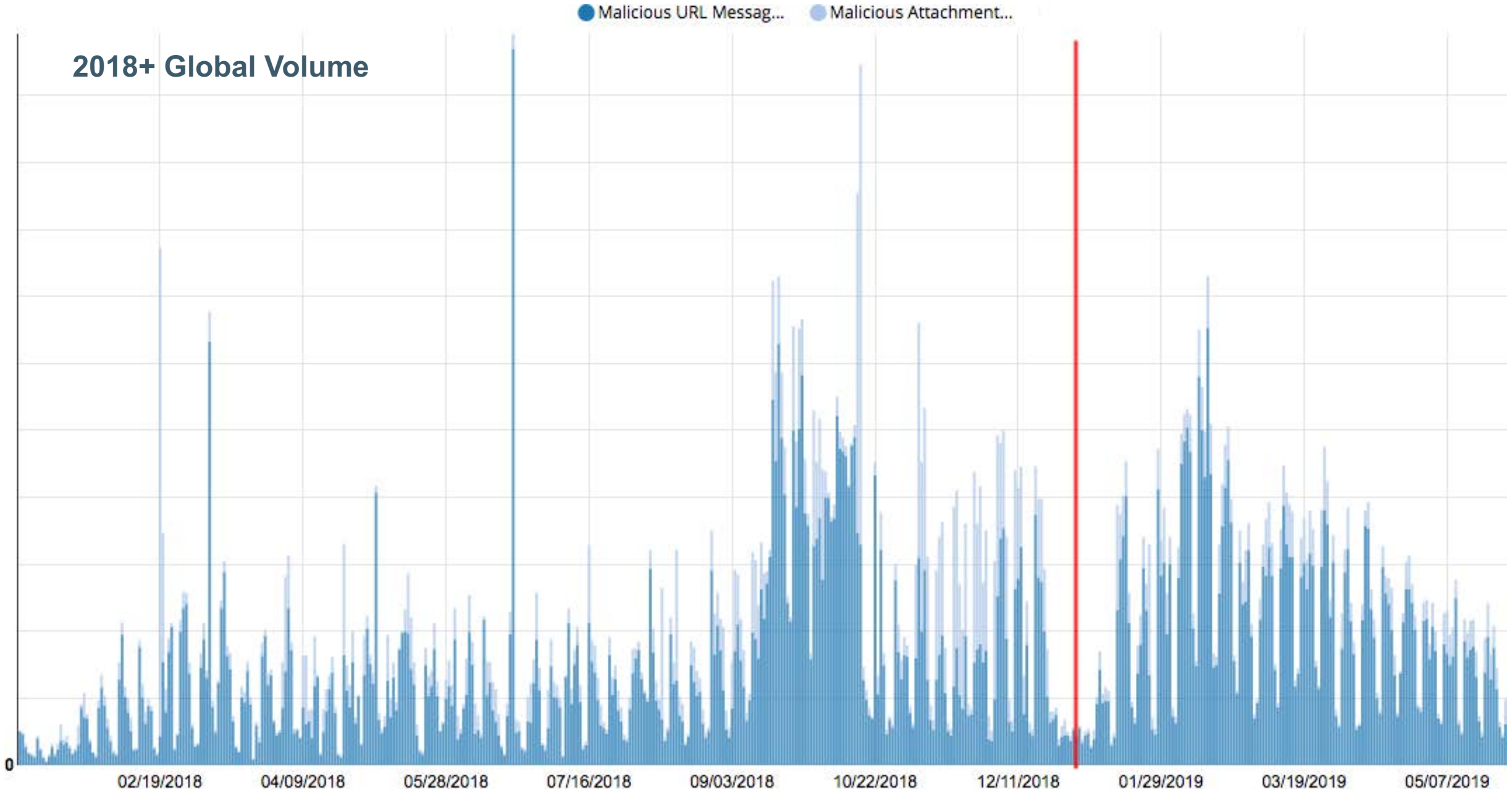
2013+ Global Volume



2017+ Global Volume

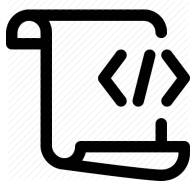


2018+ Global Volume



Attack Structures

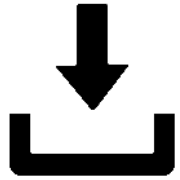
proofpoint®



Script

Attachment

Exploit



File Download

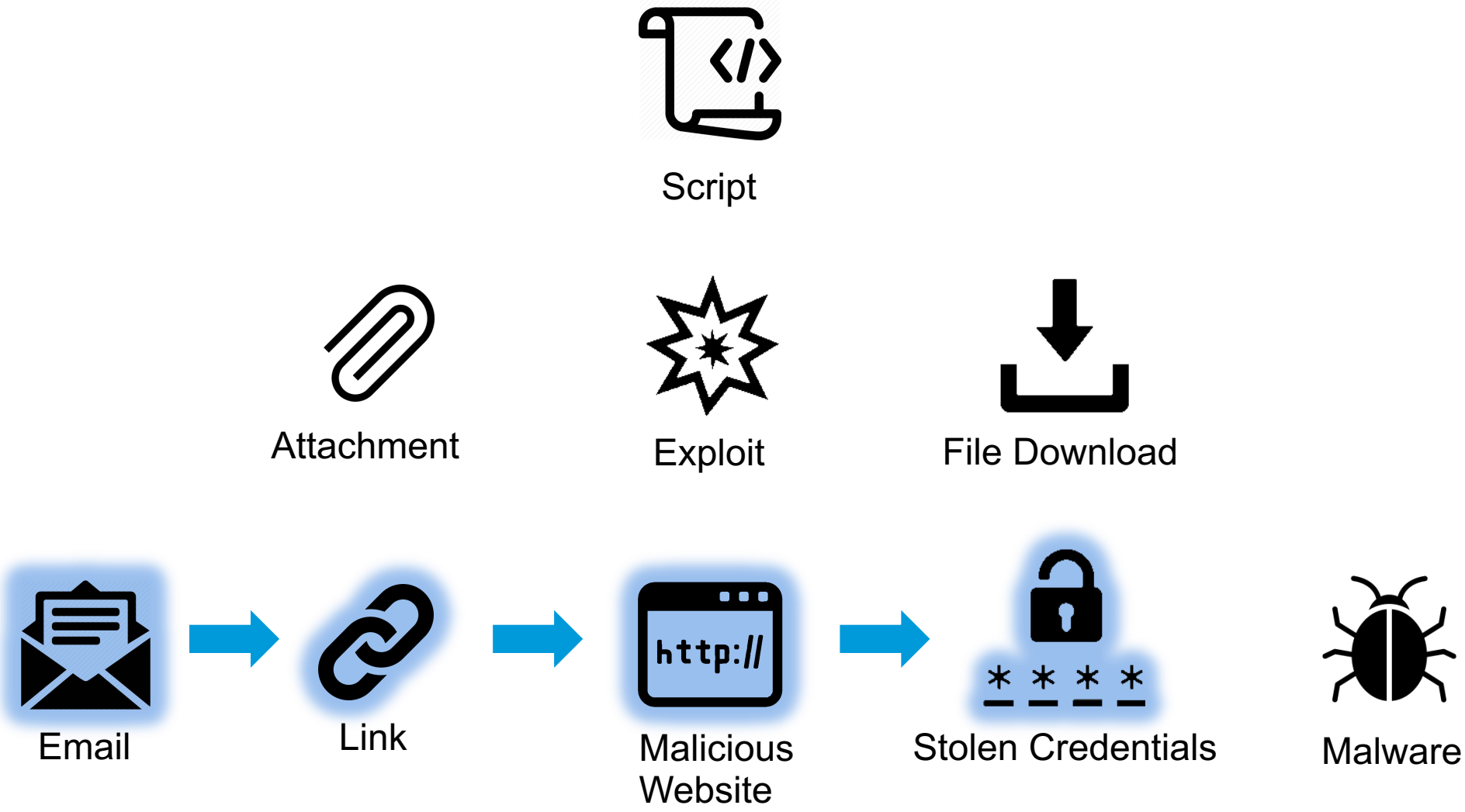
Email

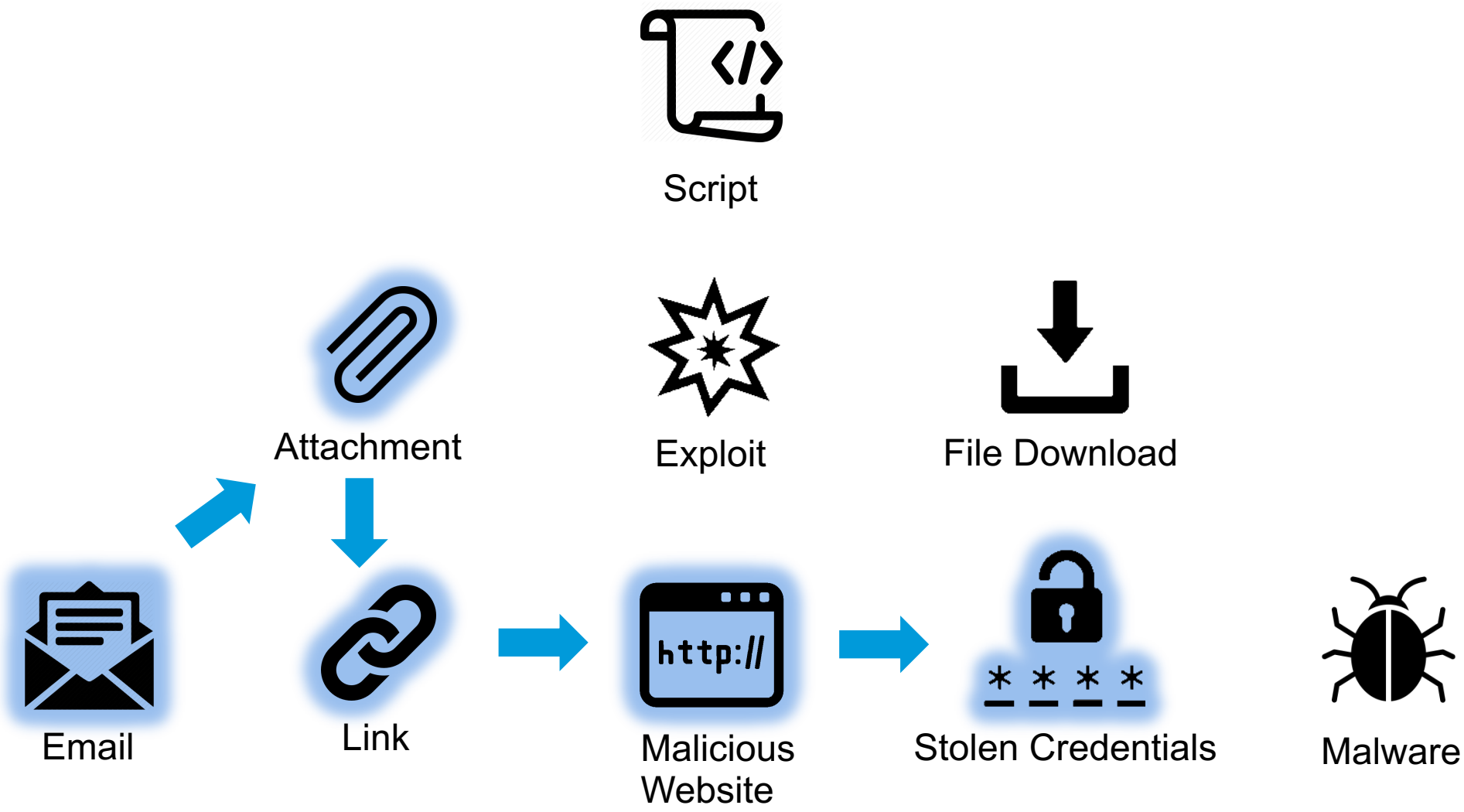
Link

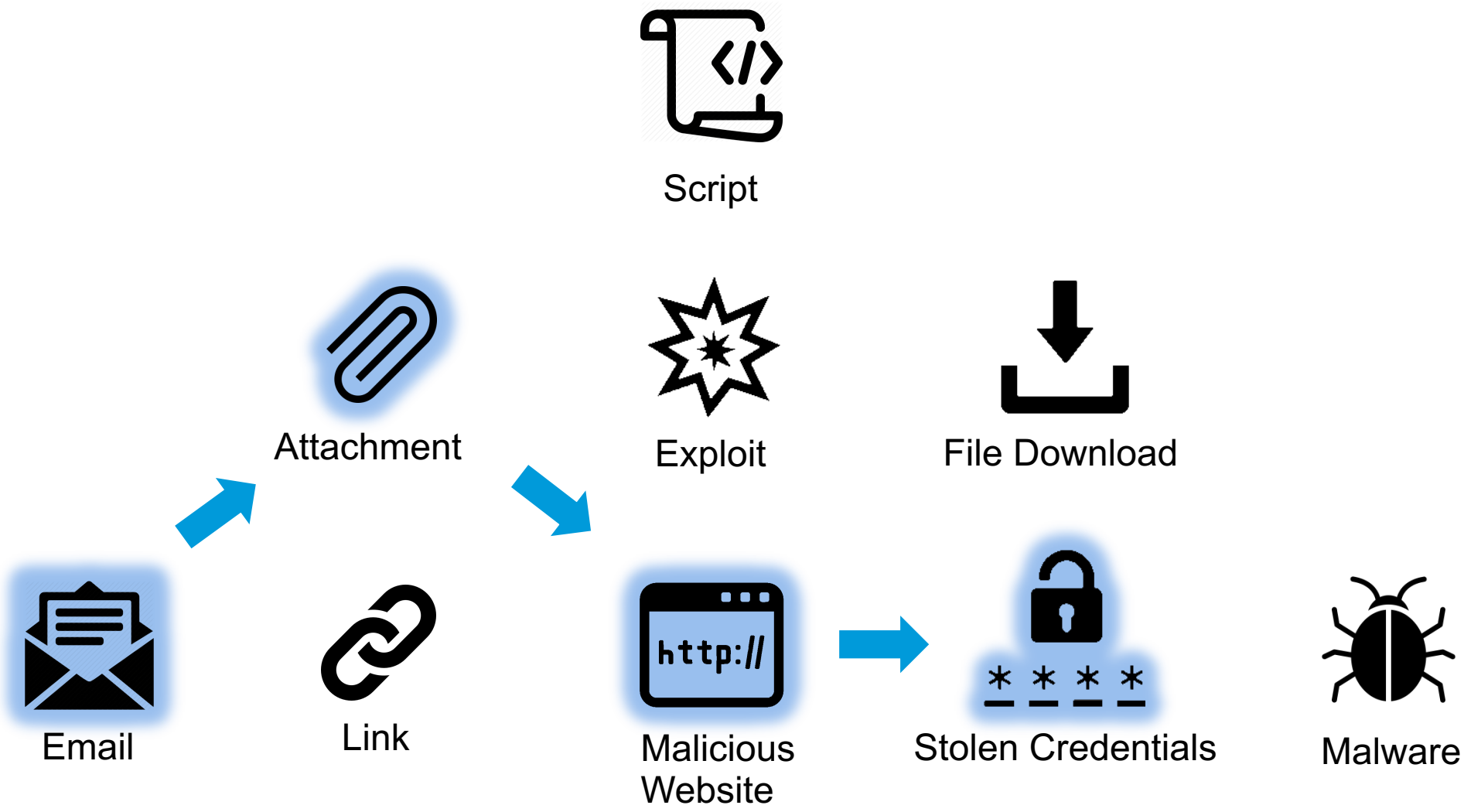
Malicious Website

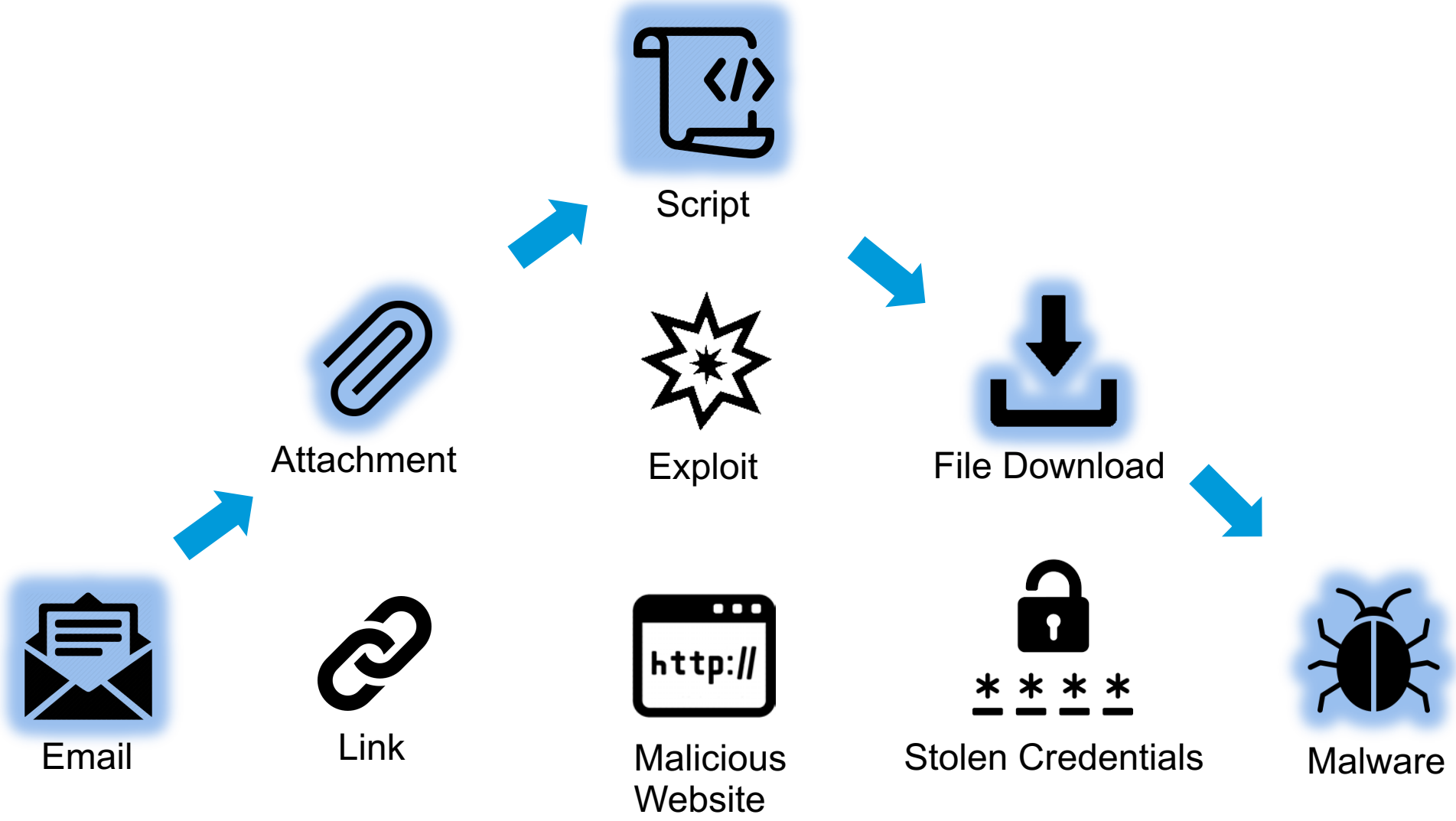
Stolen Credentials

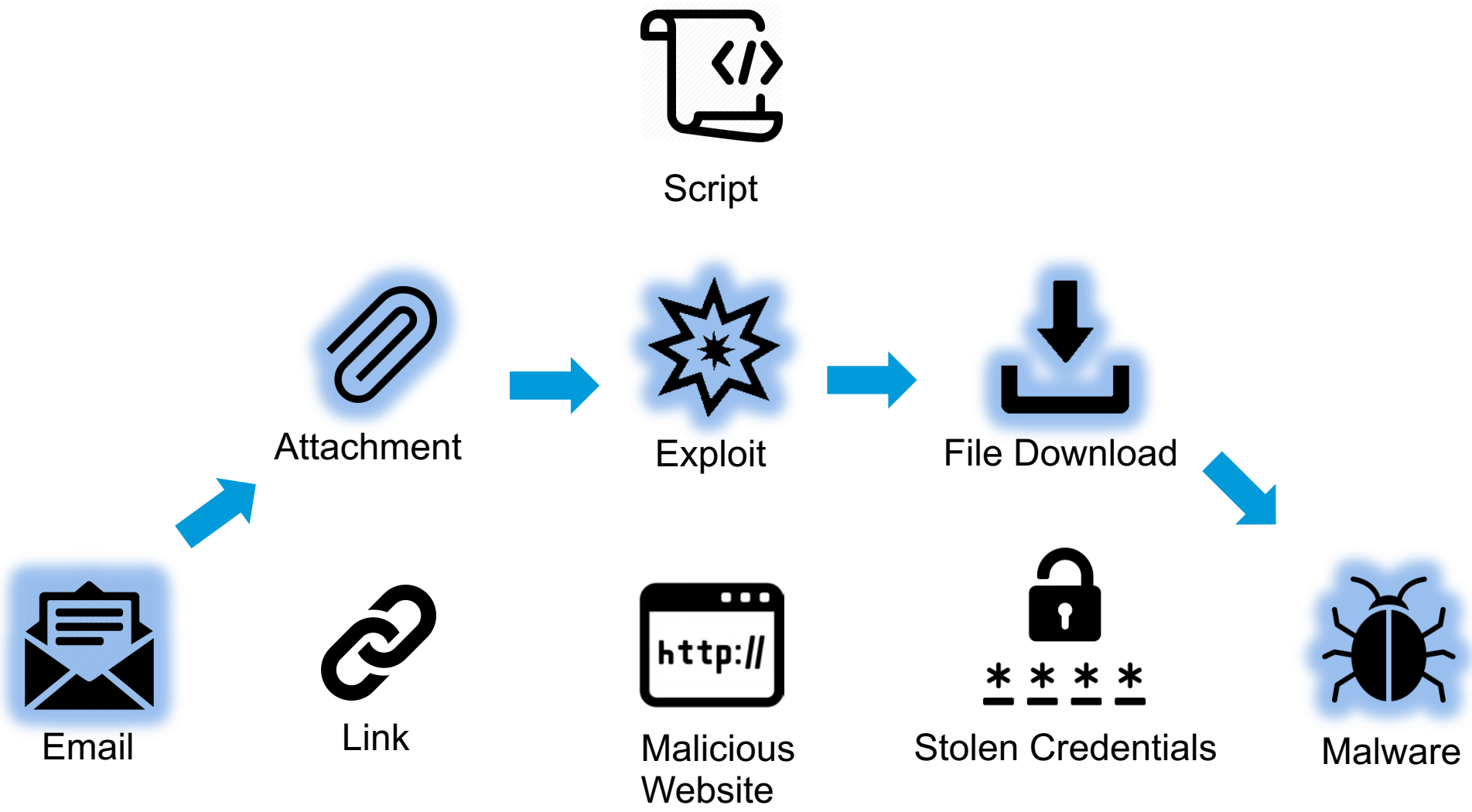
Malware

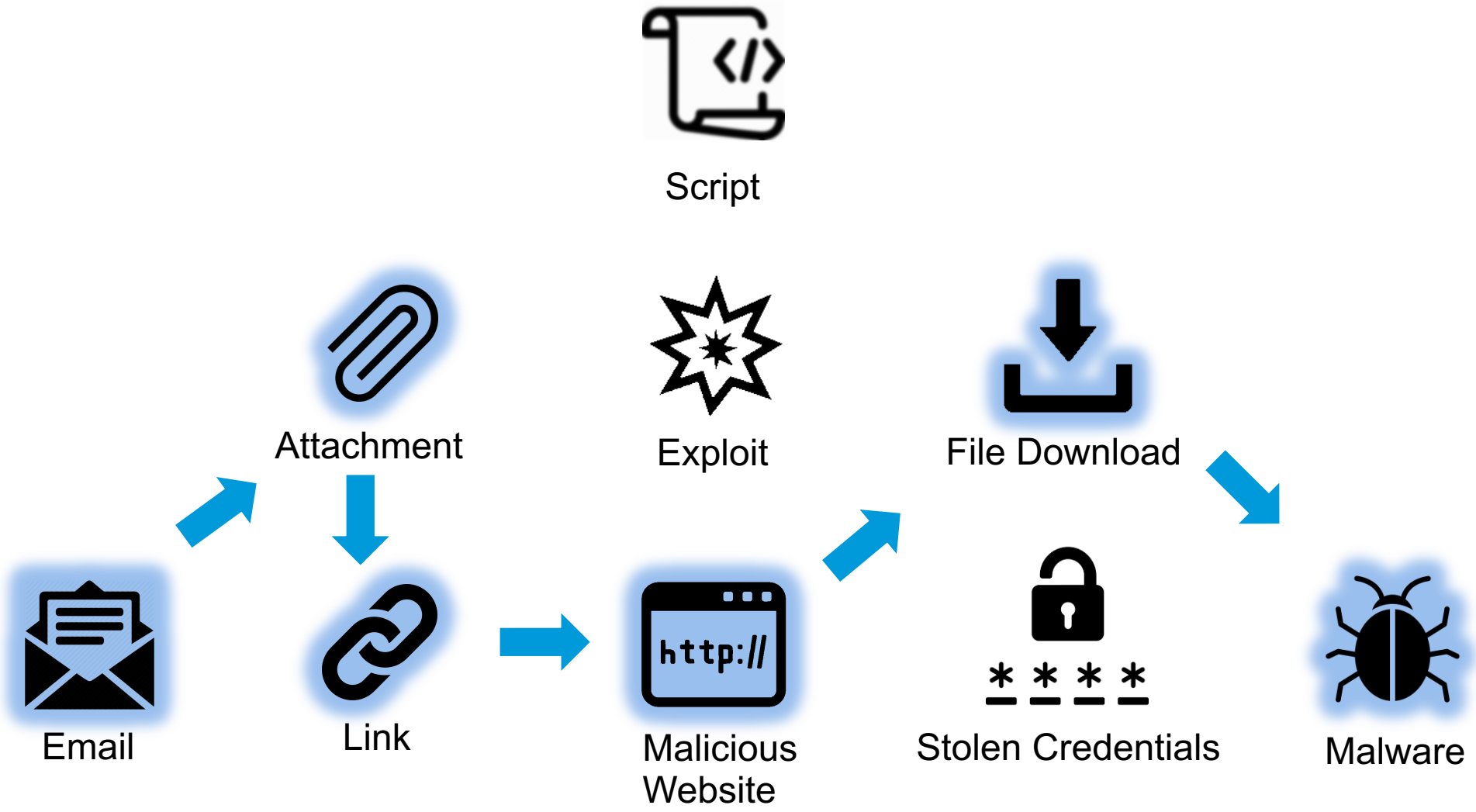


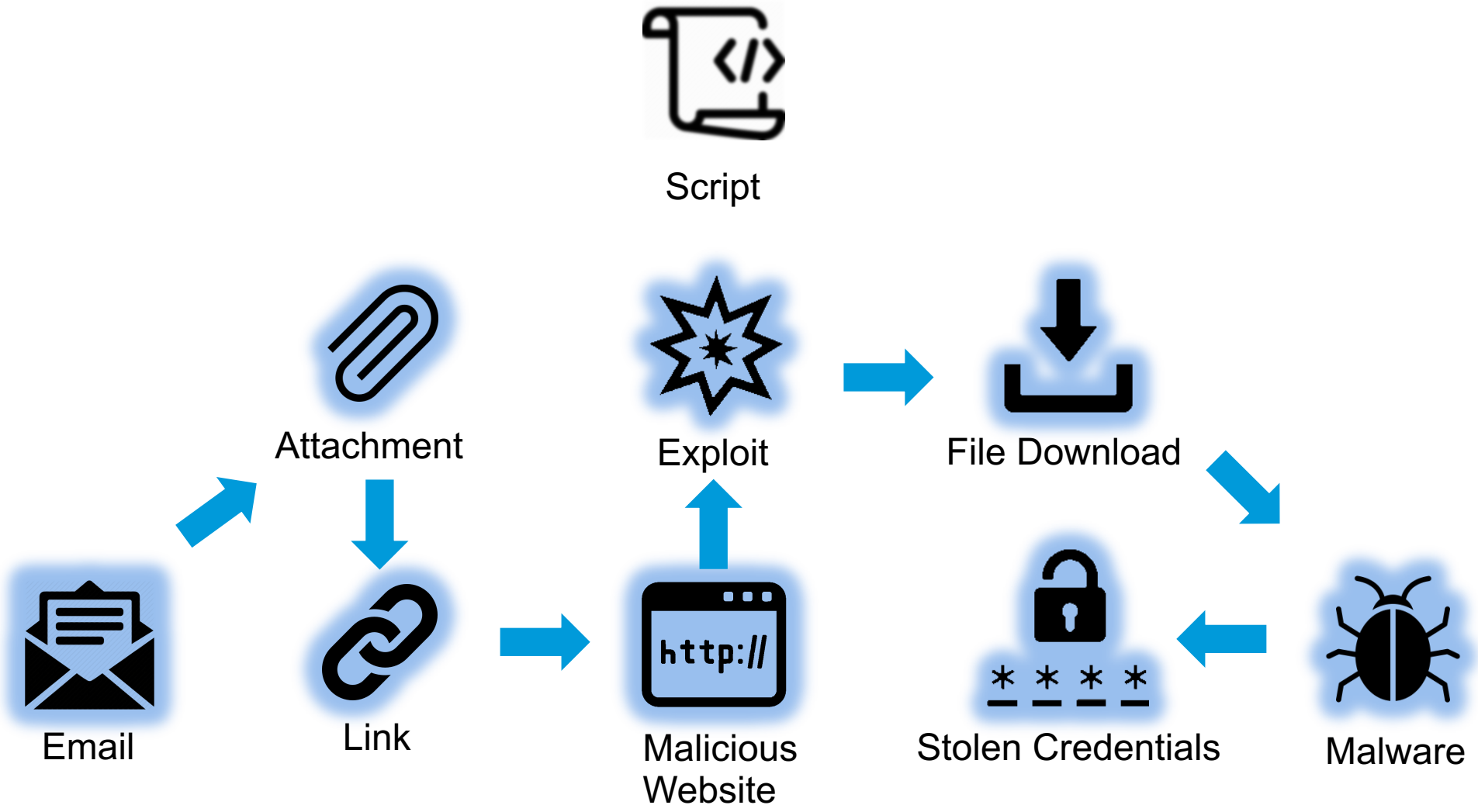








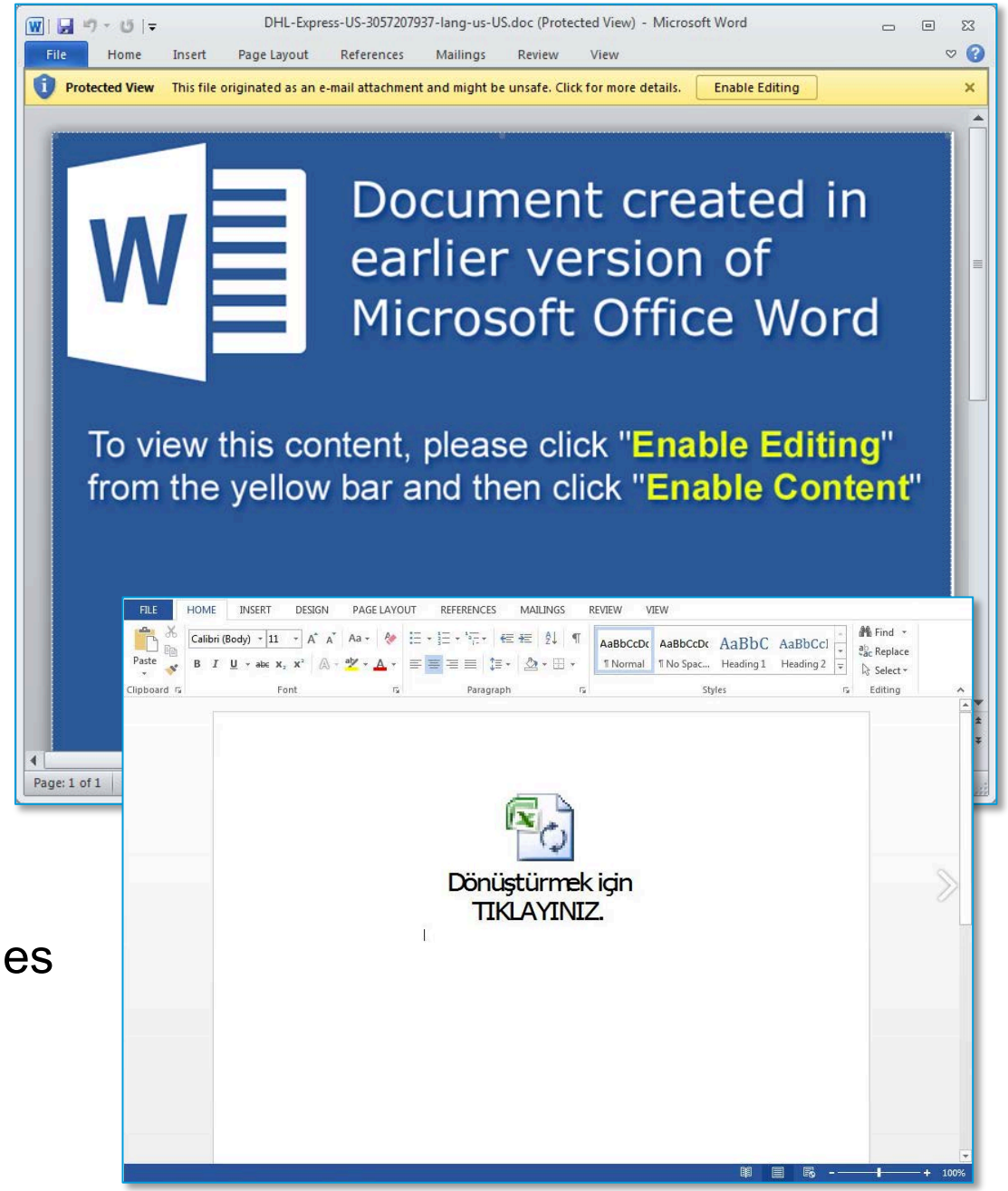




proofpoint

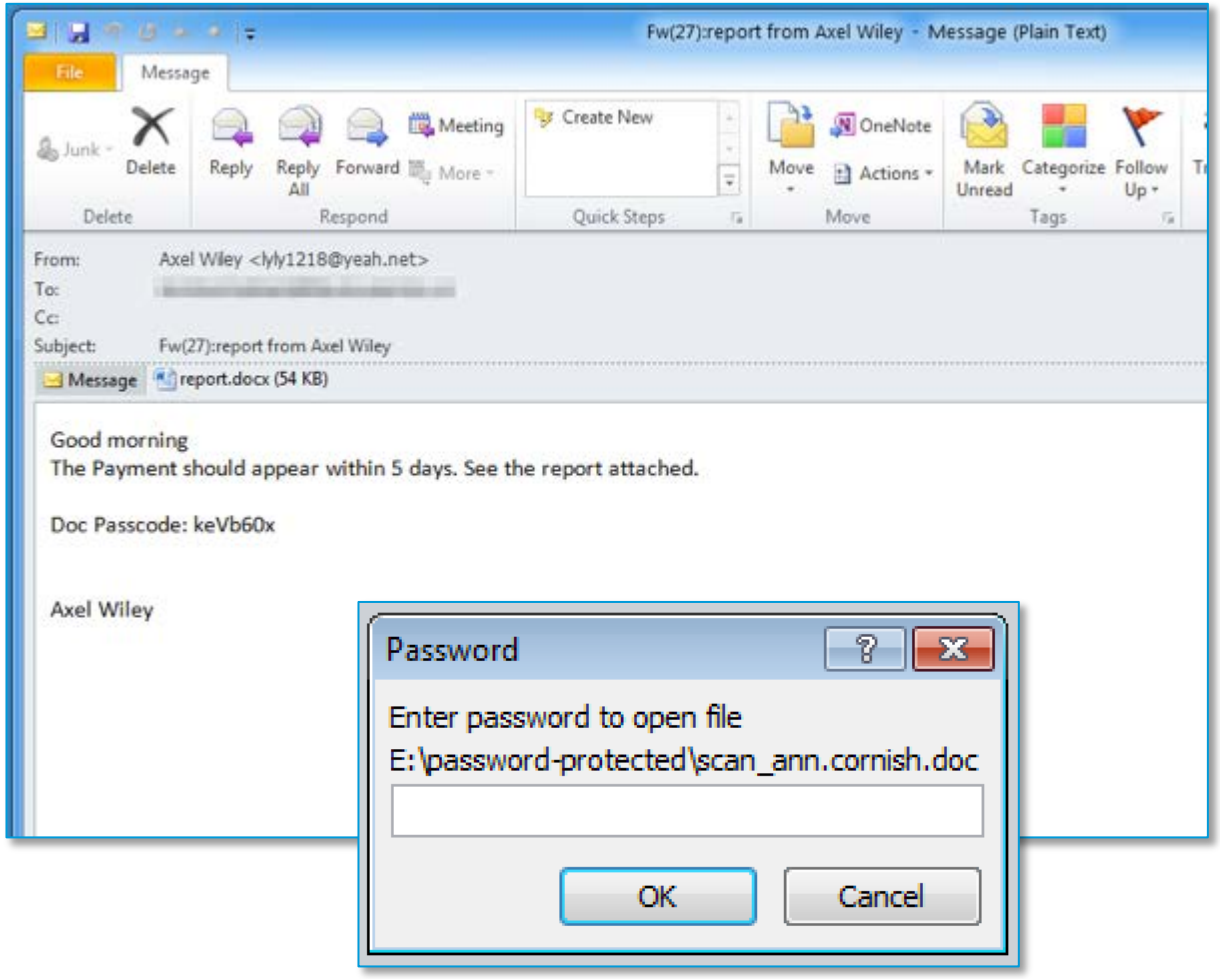
Abused Attachment File Types

- Most Common
  - Microsoft Office Documents with Macros
  - Microsoft Office Documents with Embedded Object
  - PDF with links
- New
  - XL4 Macro
  - Template Injection
- Other
  - DDE
  - Password protected Microsoft Office Documents
  - Documents that exploit Microsoft Office vulnerabilities
    - Most common is CVE-2017-11882
    - All time highest volume is CVE-2017-0199



Password Protected Documents

- Office documents where passwords are required to open the document
- Password is presented to the user in the body of the email
- Advantages
  - Appears to the user as privileged information contained within the document
  - Evades automated sandbox analysis
- Campaigns tend to use the same password for all samples
- Most recently seen in these campaigns
  - IcedID - TA516 [SmokigDro]



wes

Stella

To: wes@[redacted]

Reply-To: Stella

wes

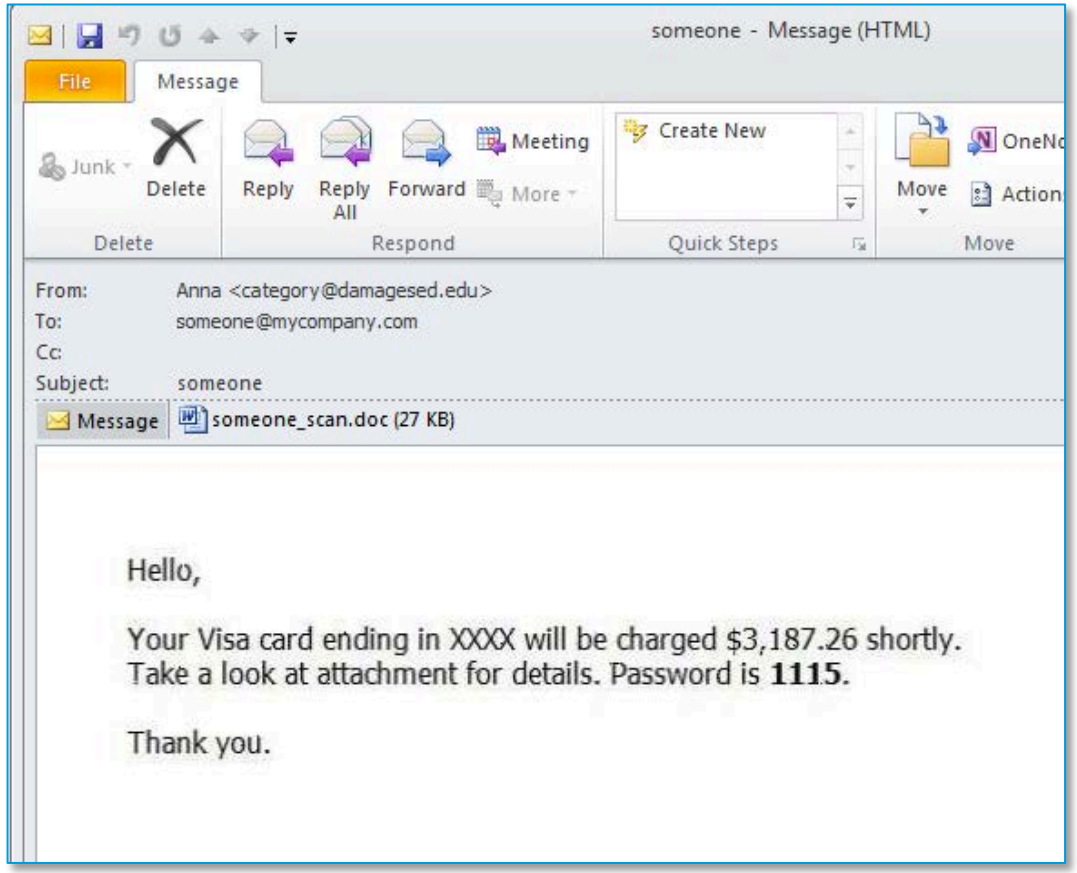
How are you wes,

You will be charged $3,628.74 on your current Visa balance straightaway.
See attachment to avoid it. Password is 1115

Yours truly,

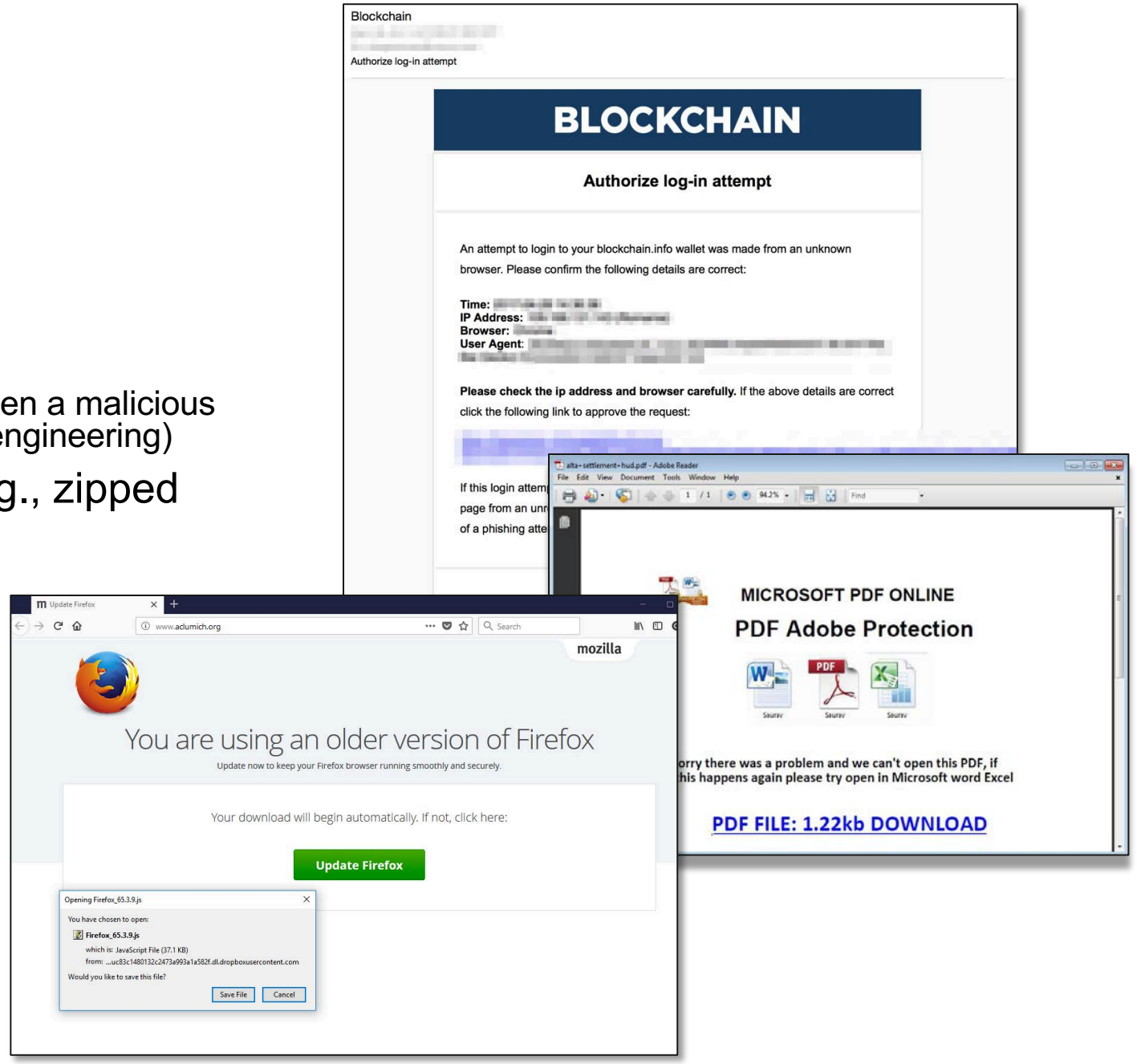
Ste

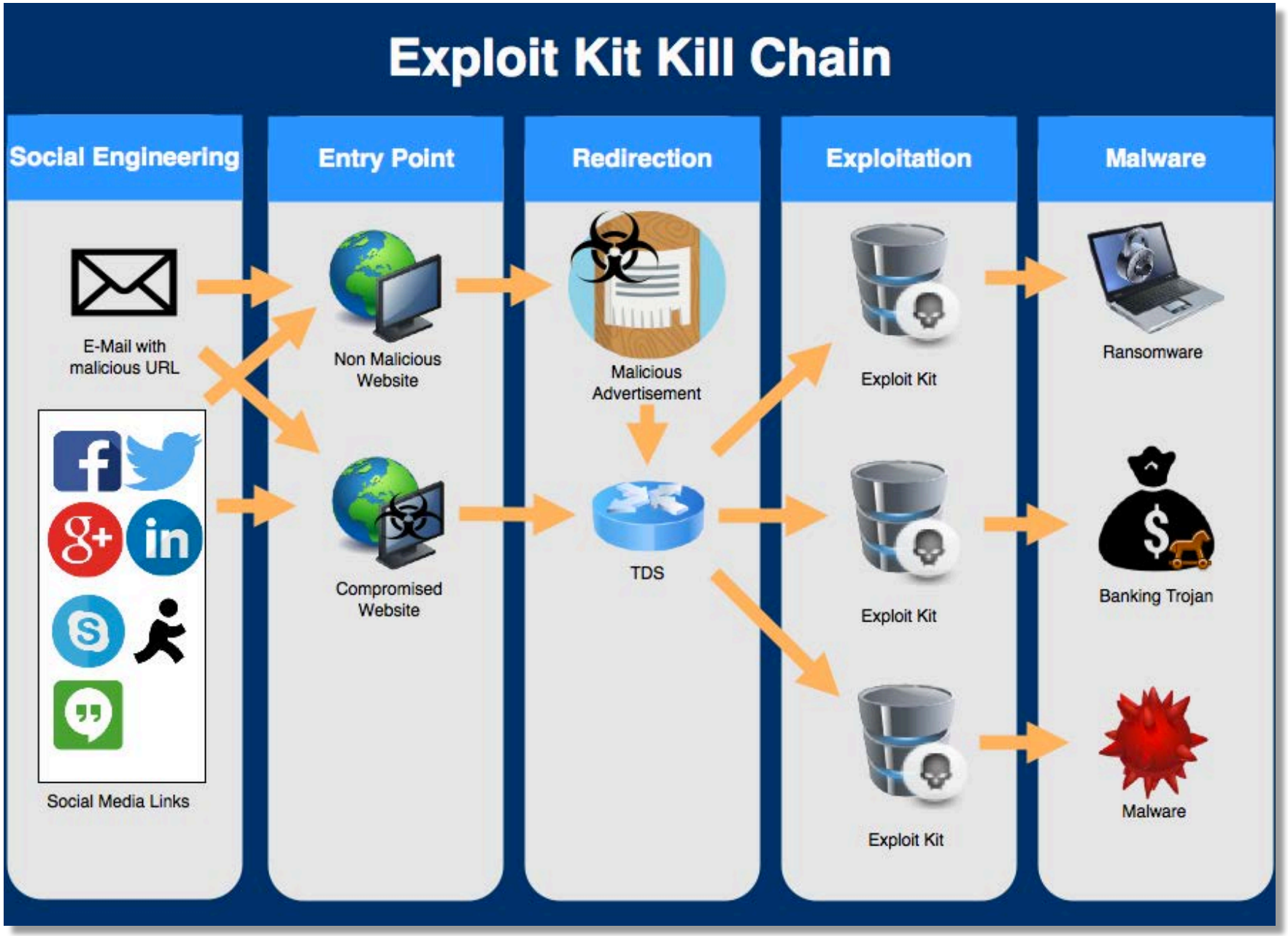
wes_scan.doc



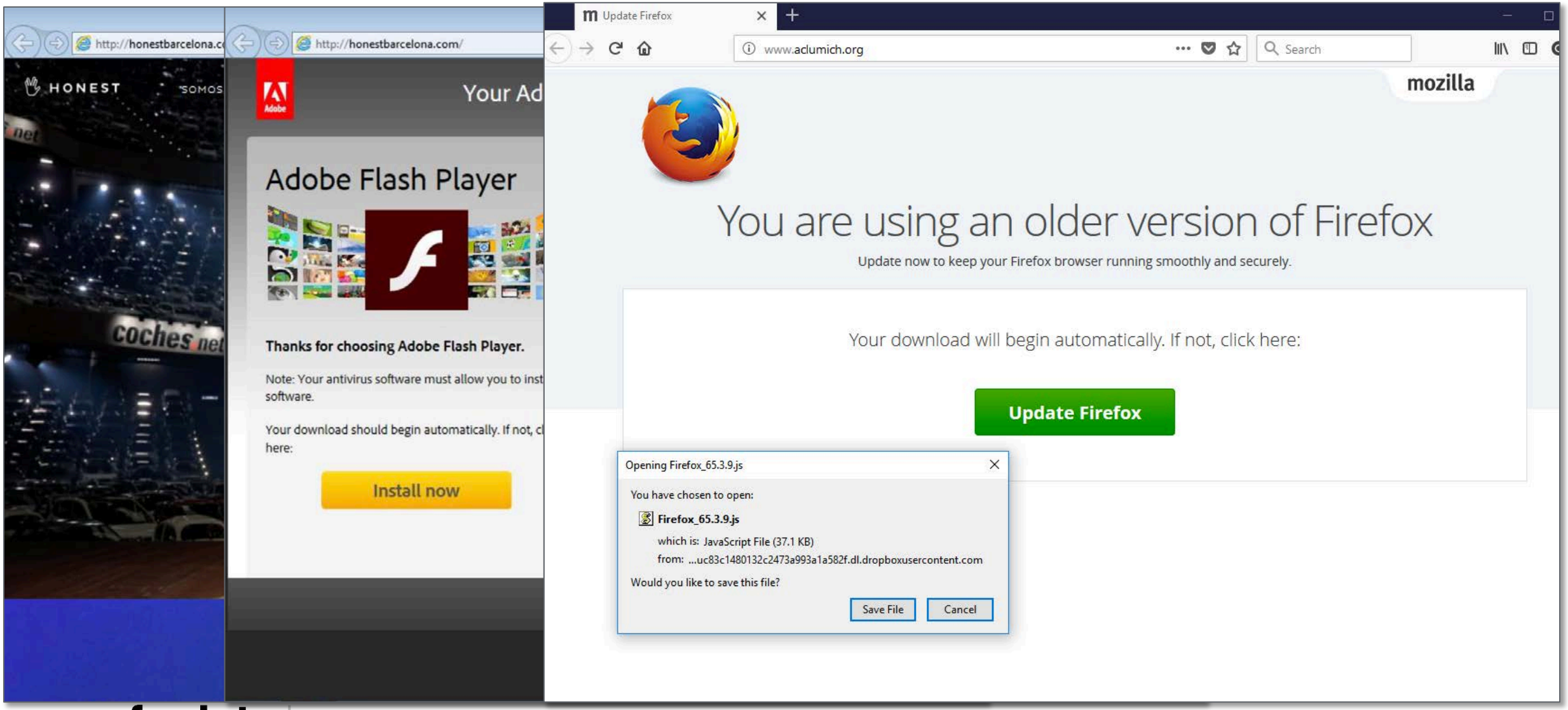
Delivery Methods - URL

- Most Common
  - Links to phishing pages
  - Direct links to malicious docs / exes
    - Typical case: get the victim to download and open a malicious document/executable from the internet (social engineering)
  - Links to zipped downloader scripts (e.g., zipped .js & 7-Zipped .vbs)
- Newer
  - TDS Style
    - BlackTDS
    - SocGholish
    - SocGoth
- Less common:
  - Links to pages infected by Exploit Kits

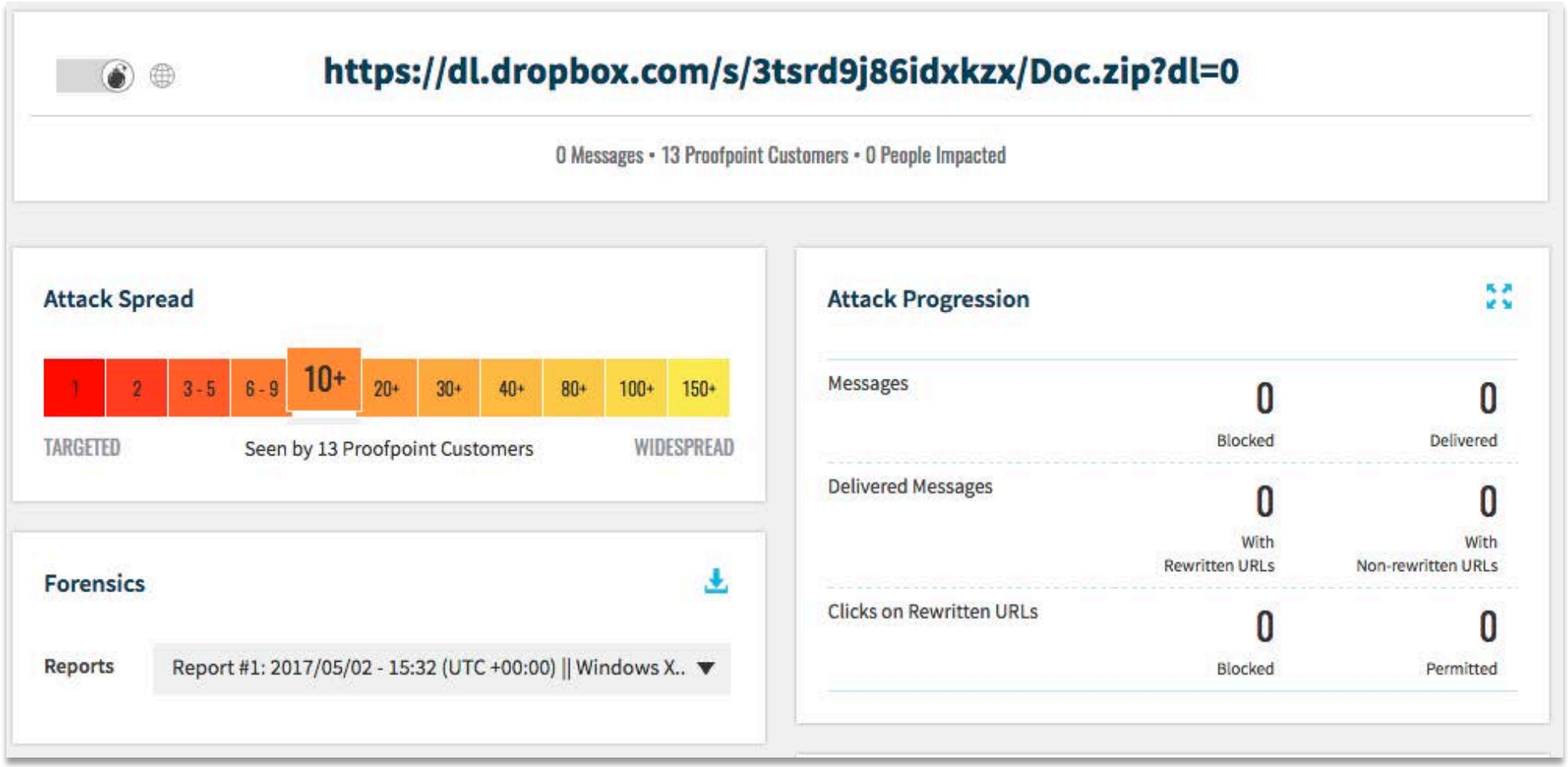




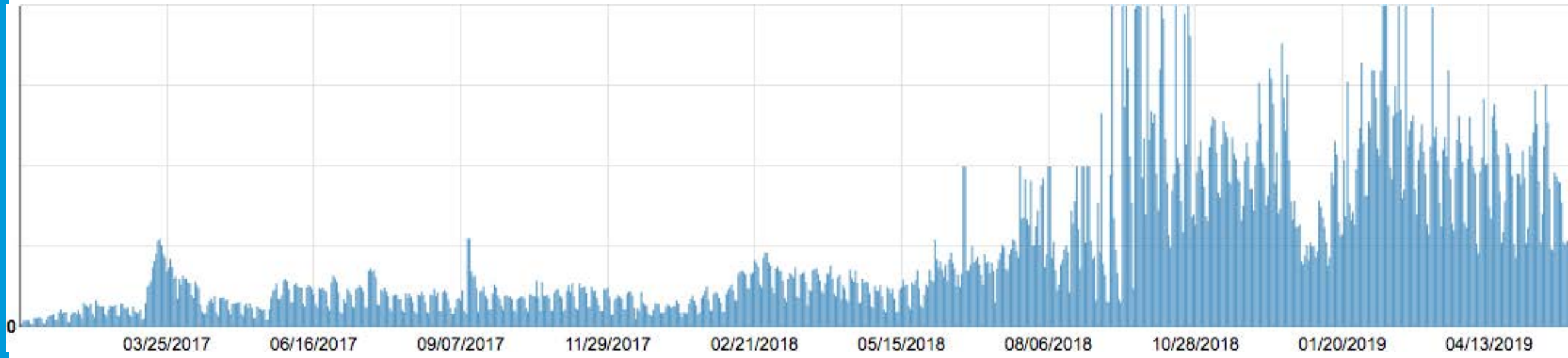
Socgholish



Malware at the end of links



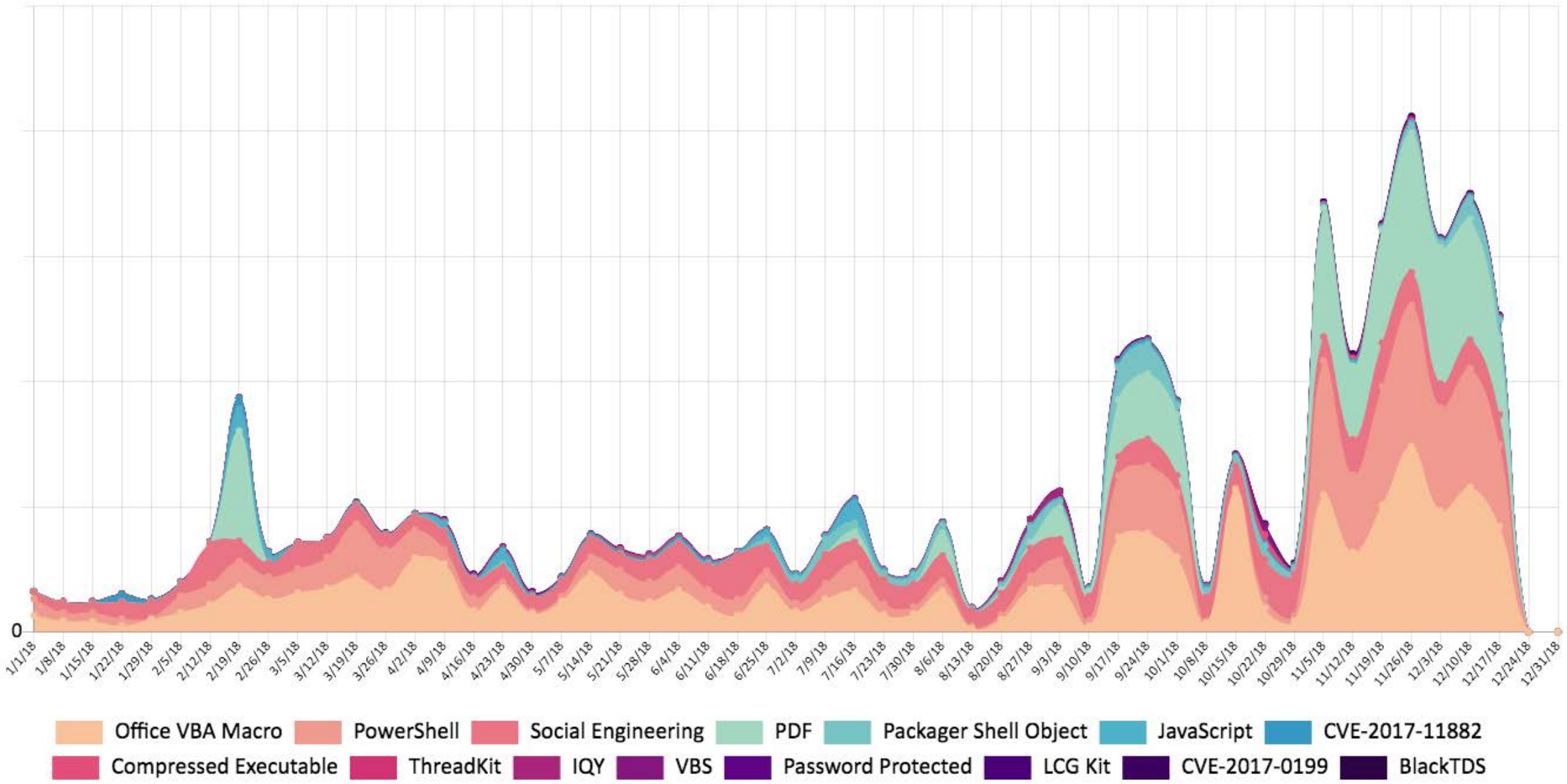
Unique Malicious URLs



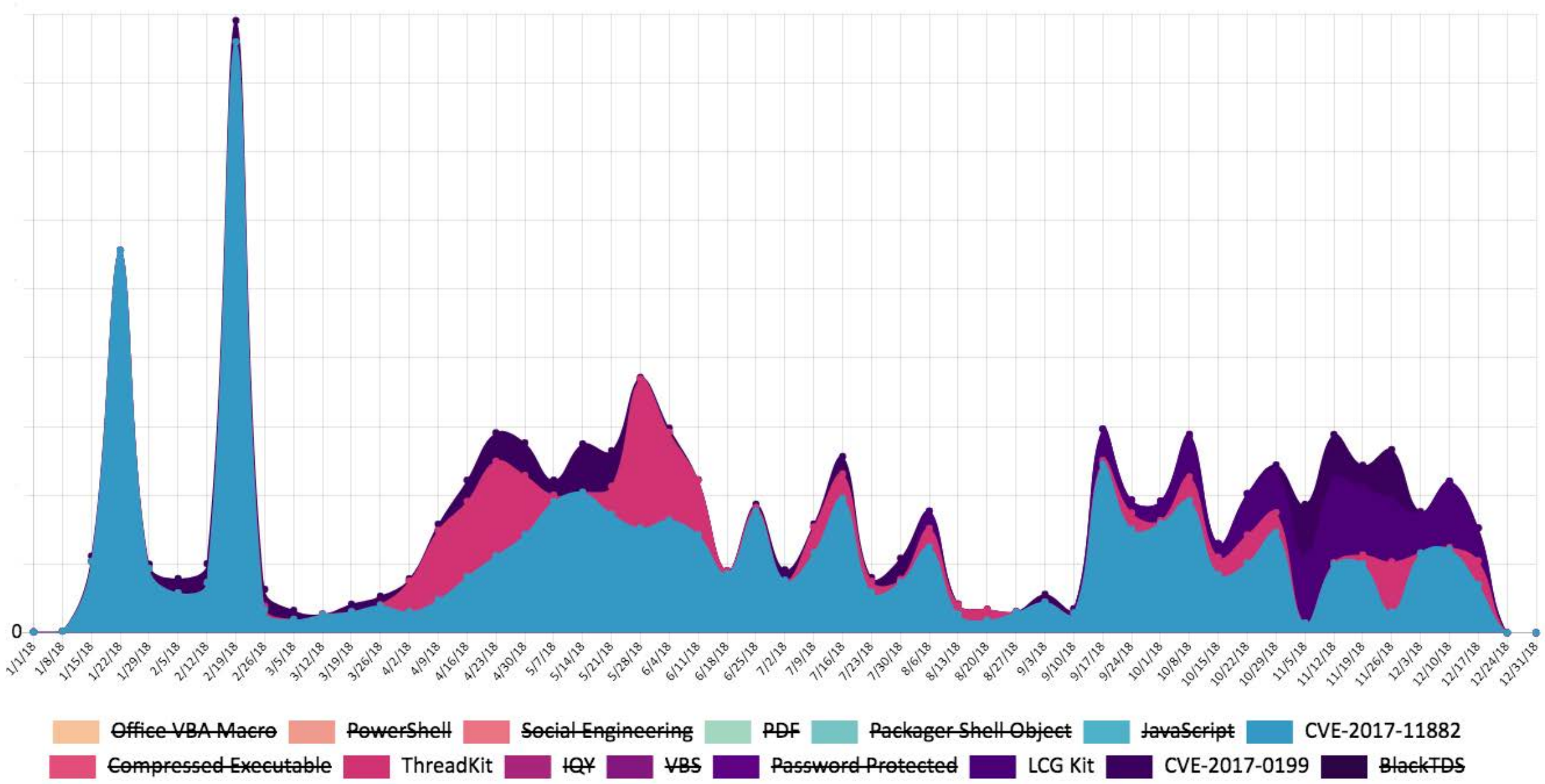
Exploits

- We consider social engineering as an ”exploit”
  - Office Macros are an extension of umbrella “Social Engineering” term
- Almost all exploits we see are Microsoft Office exploits
  - CVE-2017-11882
    - By far the most popular
  - CVE-2017-0199
  - CVE-2017-8570
- Exploit Builder Kits
  - ThreadKit
    - Supports multiple CVE’s.
    - Has been found to be using exploit code from researchers
  - LCG Kit
    - Uses different variations of CVE-2017-11882

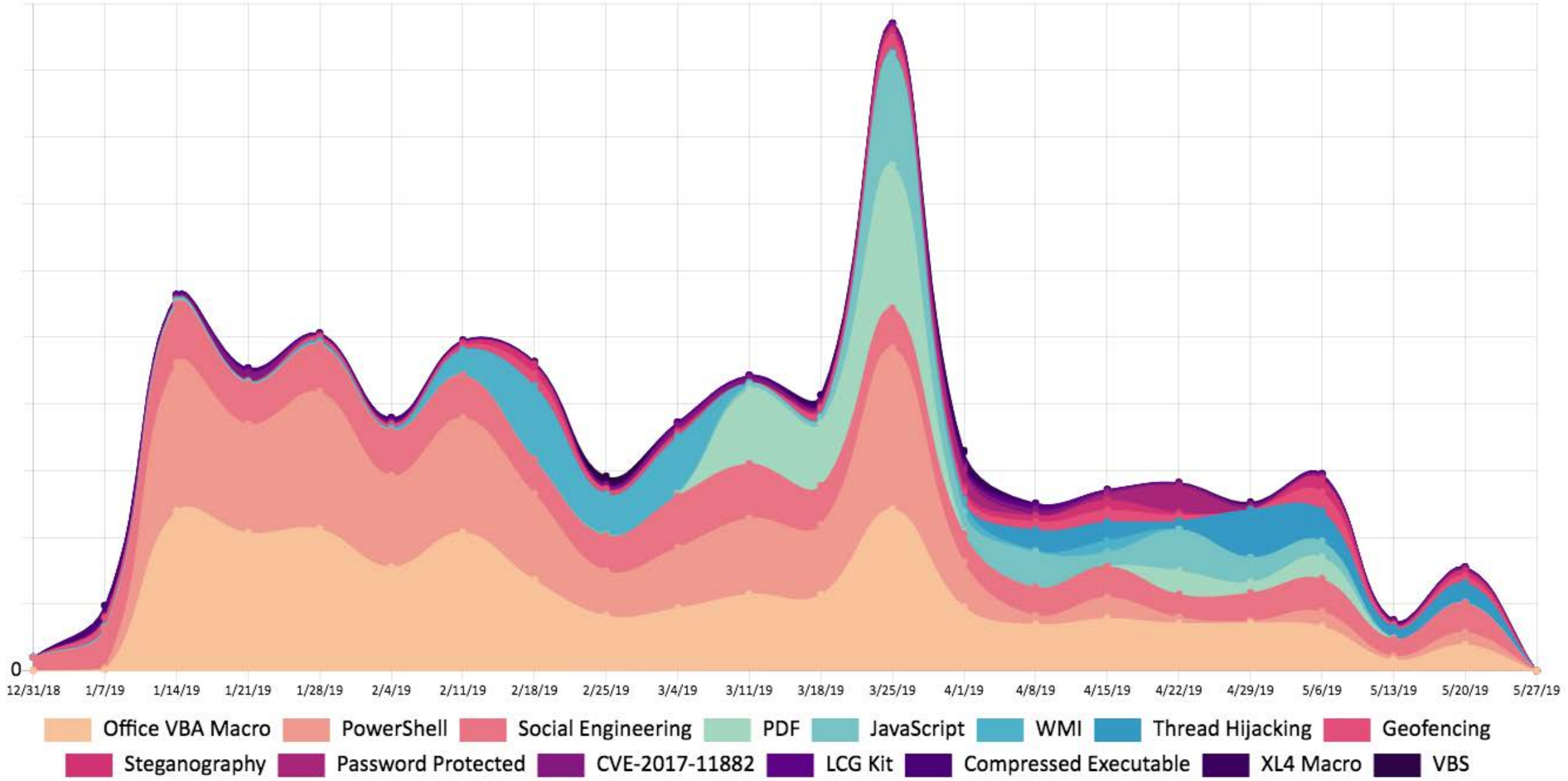
Global Campaign Exploits (Messages)



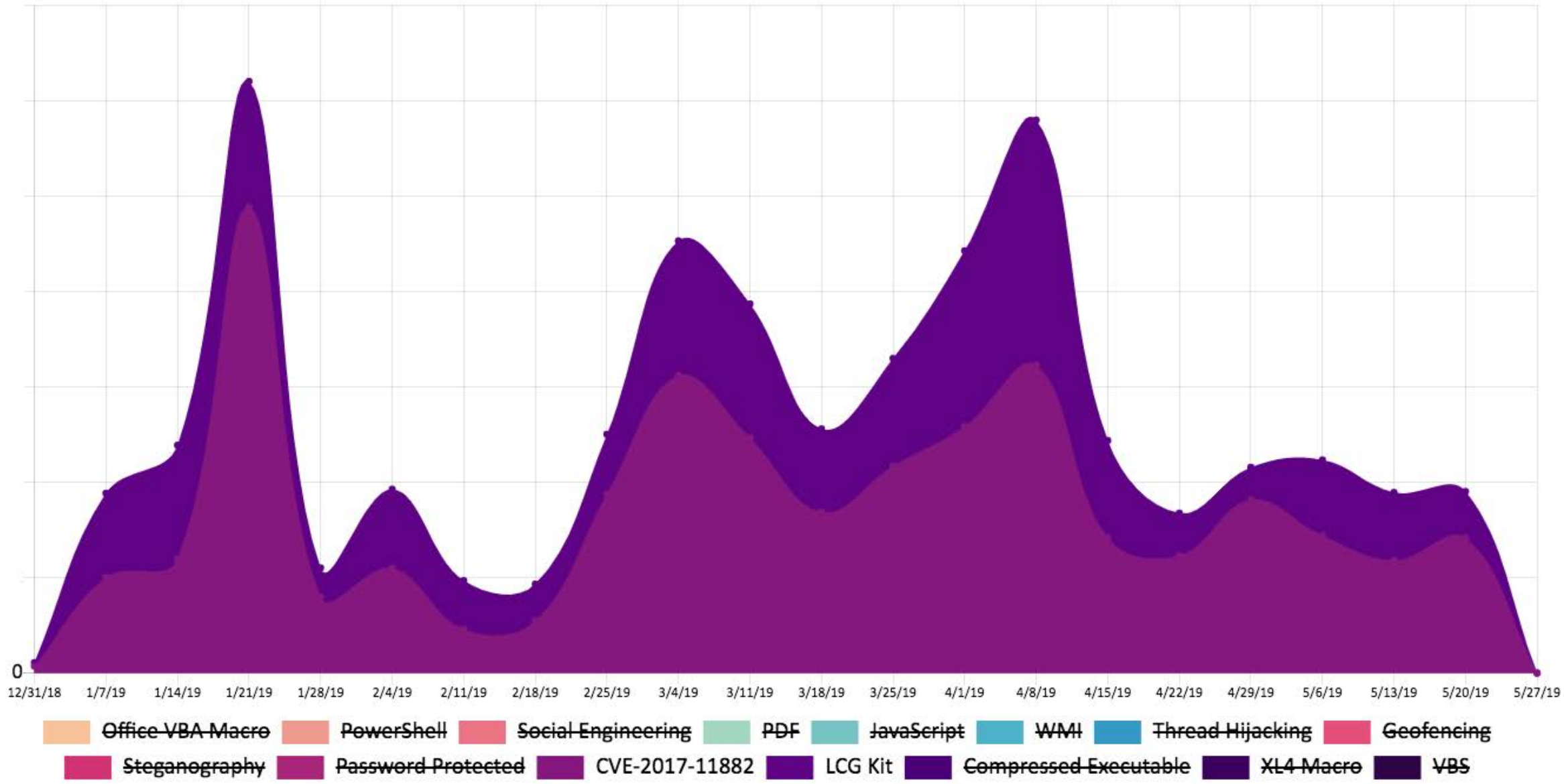
Global Campaign Exploits (Messages)



Global Campaign Exploits (Messages)



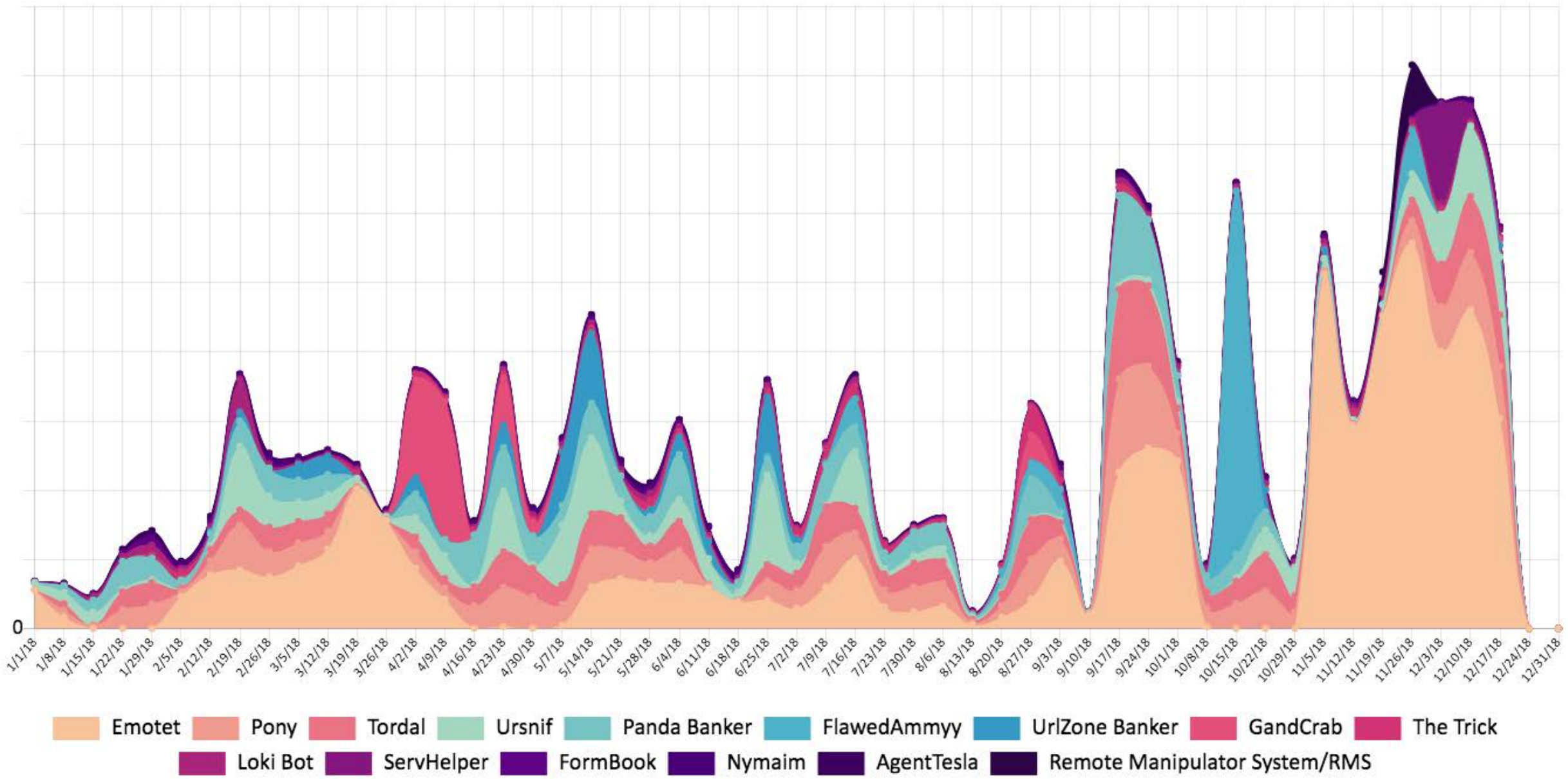
Global Campaign Exploits (Messages)



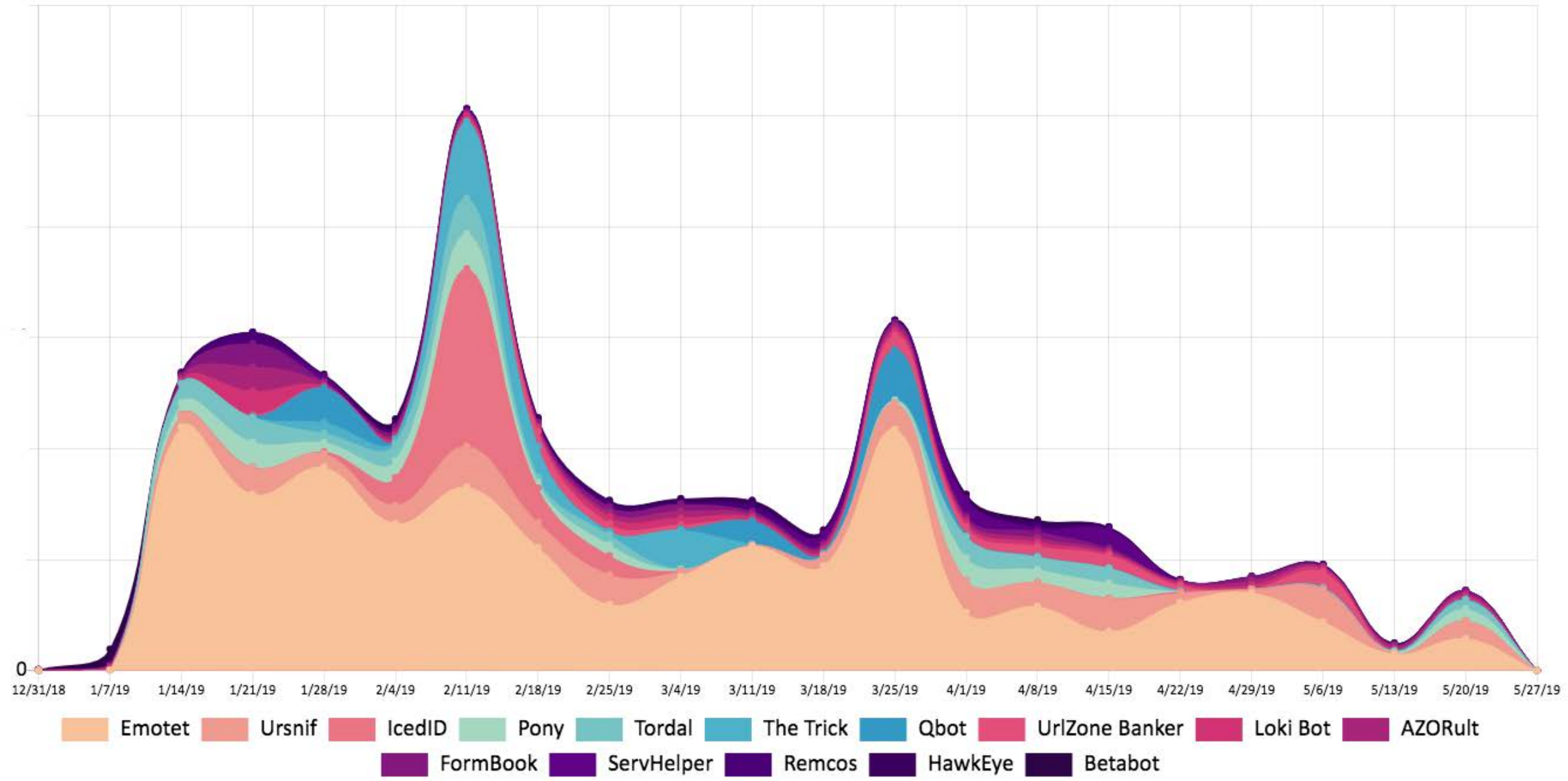
Malware

- Stealers and Downloaders
  - Dominated 2018
  - 2019 not looking any different
- Top malware 2018
  - Emotet
  - Pony
  - Tordal
- Top Malware 2019
  - Emotet
  - Ursnif
  - IcedID

Global Campaign Malware (Messages)



Global Campaign Malware (Messages)



Actors*

*Not the actors pictured in this slide

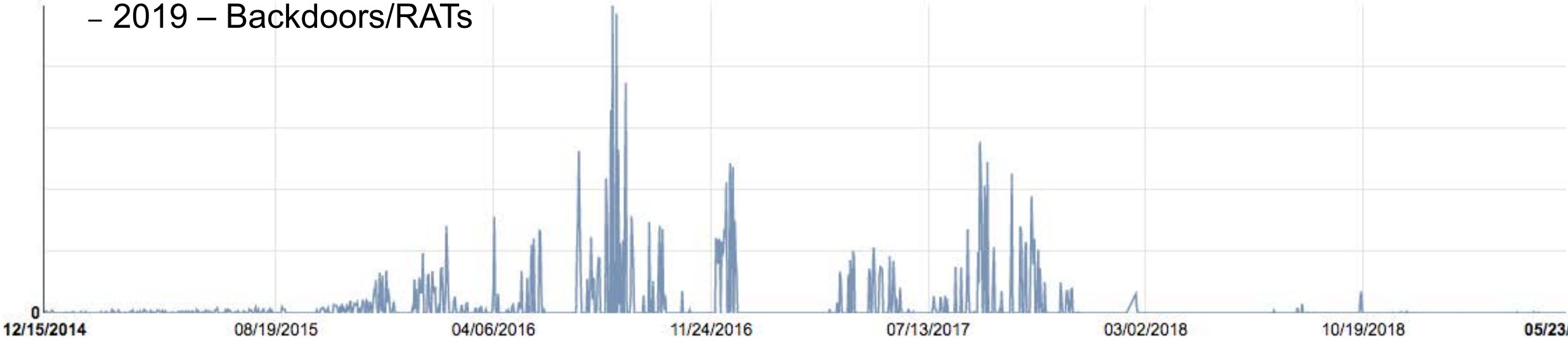
proofpoint®

TA Designations

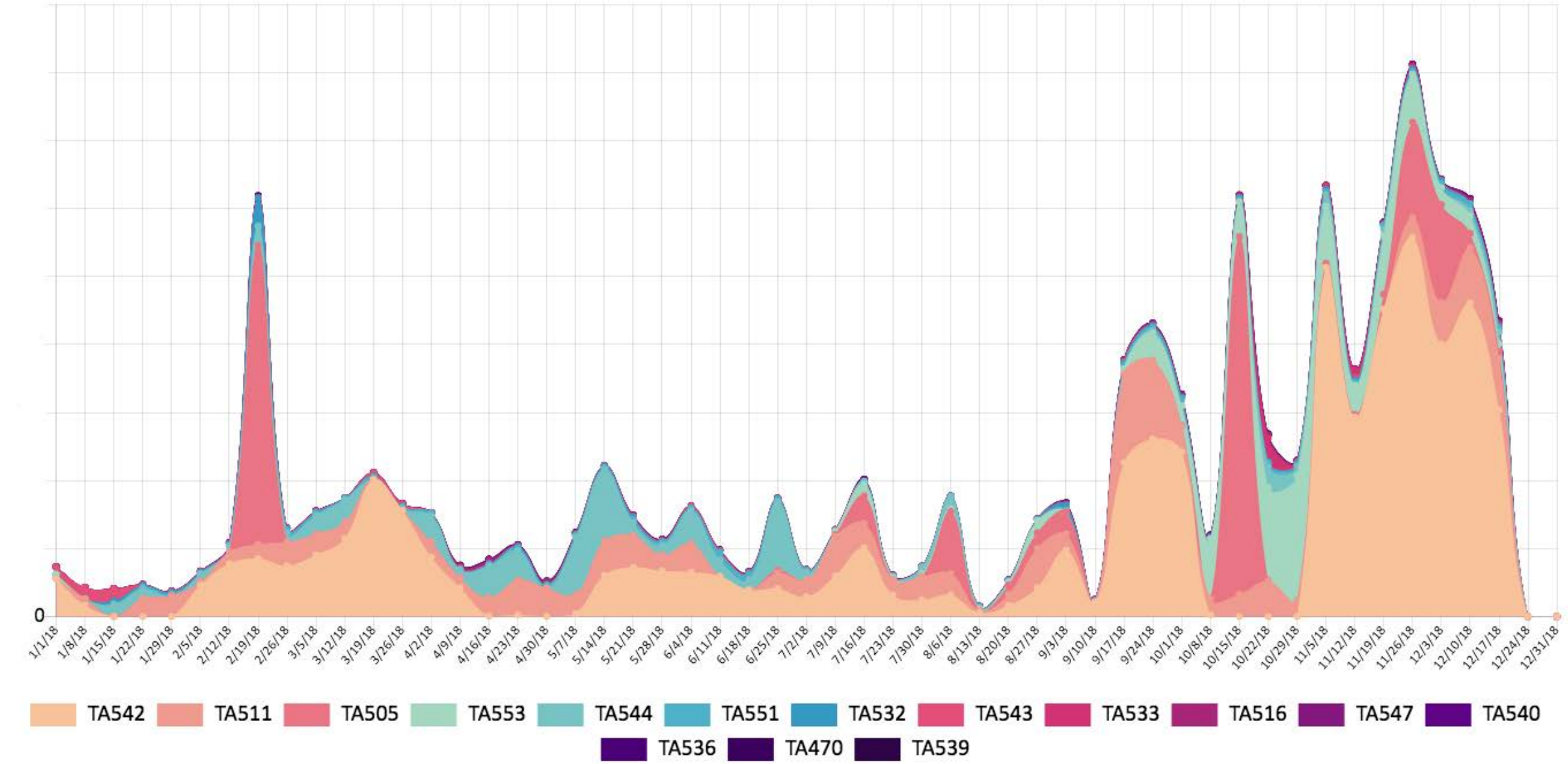
- 000 - 499: APT
- 500 - 1999: Crime large
  - large campaigns like those distributing Locky / Dridex bankers and ransomware
- 2000 - 2999: Crime small
  - more targeted like certain small BEC groups
- 3000 - 3999: Crime sophisticated
  - Cobalt, Fin7
- 4000 - 4999: Unknown/Sophisticated/Specialists
  - interesting groups that we are not sure where else to put

TA505

- TA505 tends to lead trends
  - 2014 – Banking Trojan
  - 2015 – Banking Trojan
  - 2016 – Ransomware
  - 2017 – Ransomware
  - 2018 – RATs
  - 2019 – Backdoors/RATs

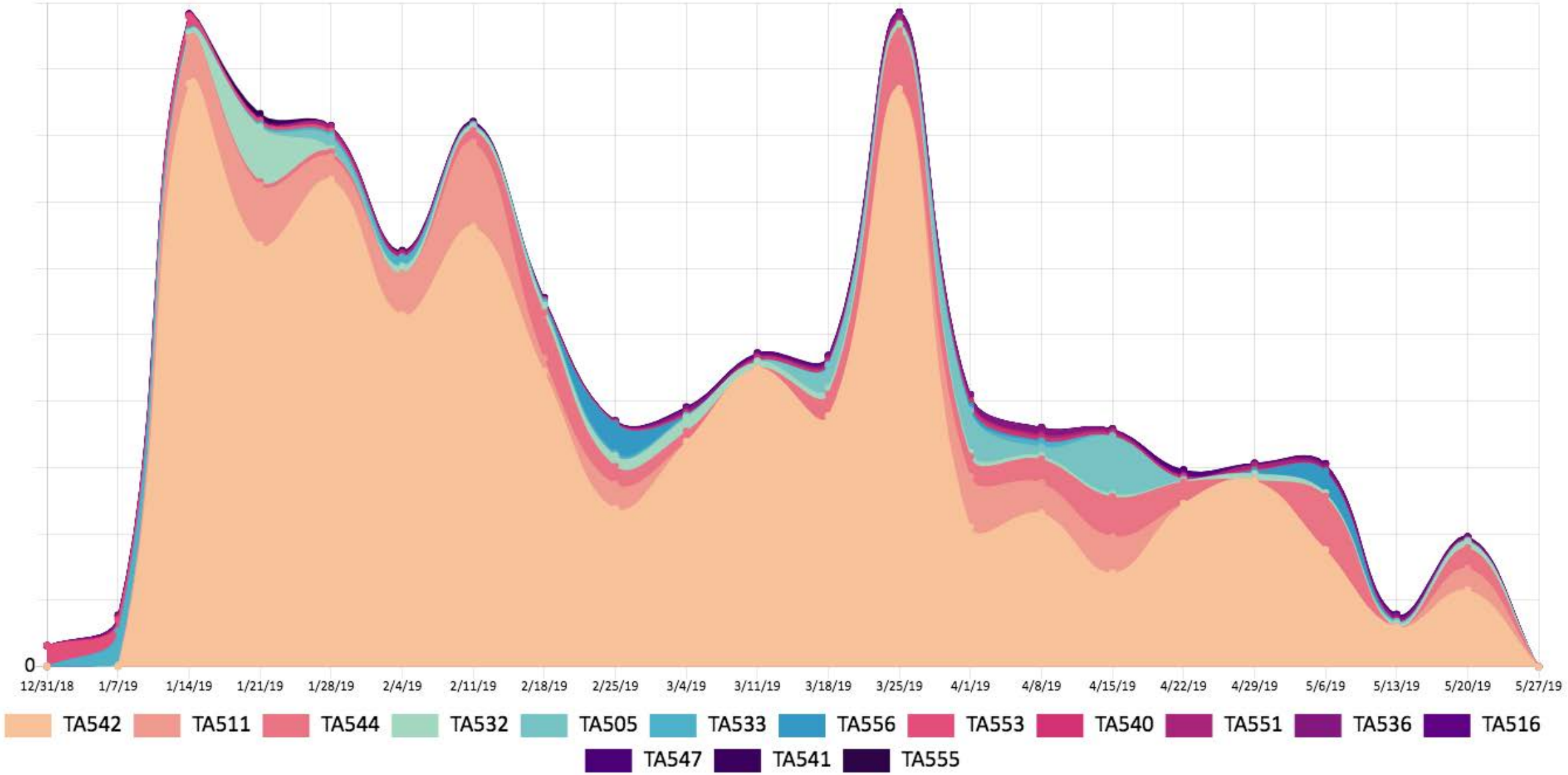


Global Campaign Actors (Messages)



proofpoint.

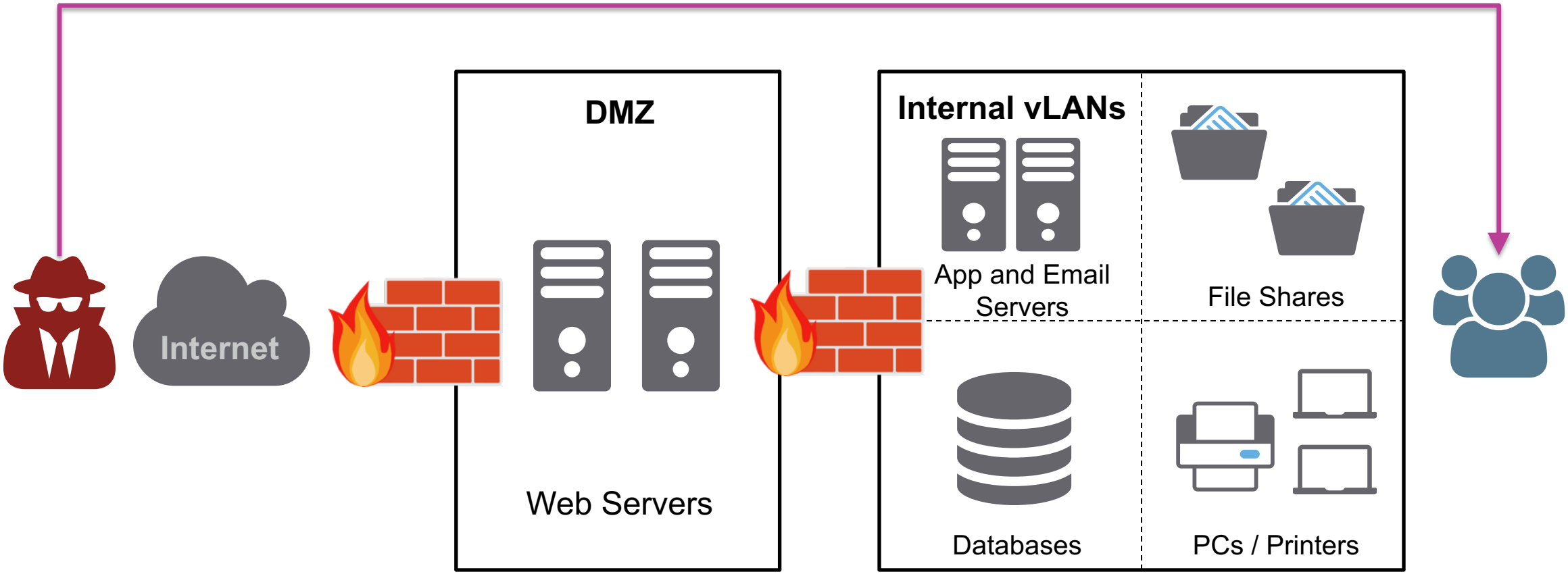
Global Campaign Actors (Messages)



People Centric Security Analytics (PCSA)

proofpoint®

The Defender's POV



O365?

The Attacker's POV

jbarker@bank.co

Jack Barker • 3rd

Executive at Bank Co
500+ connections

lbream@bank.co

Laurie Bream • 2nd

Financial Advisory at Bank Co
500+ connections

rhendricks@bank.co

Richard Hendricks • 3rd

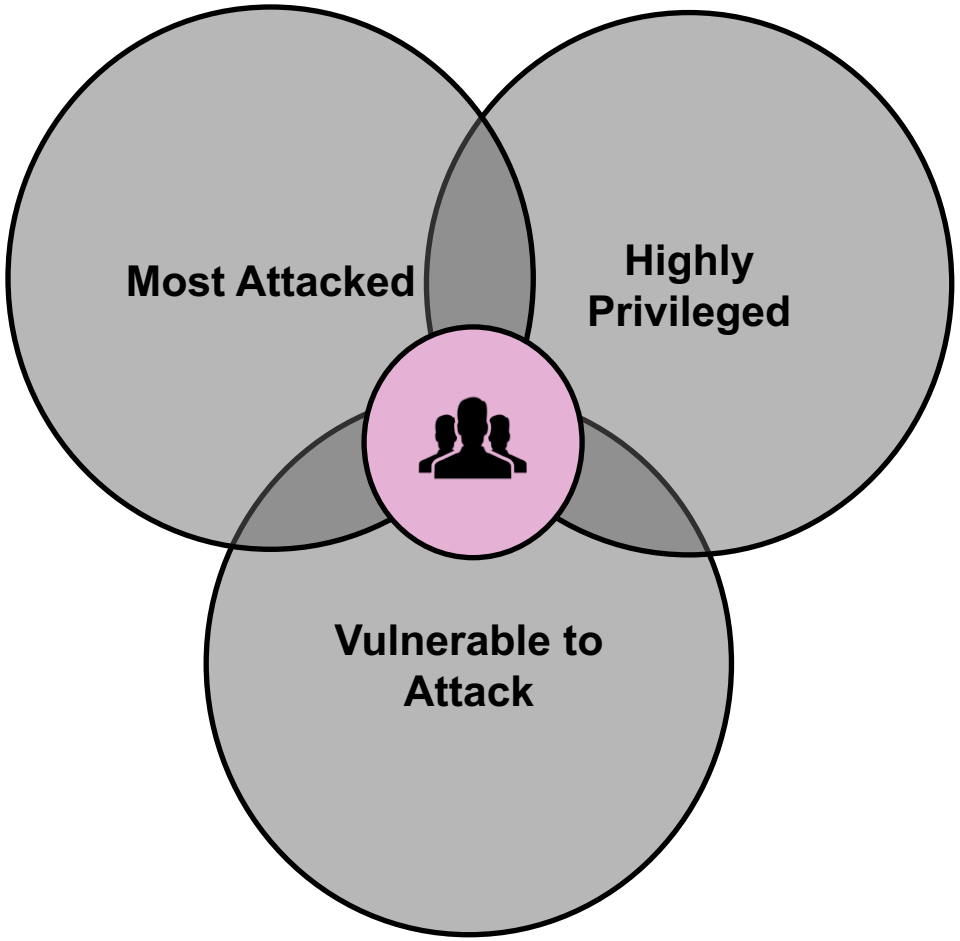
Senior Systems Administrator
55 connections

Featured Skills & Endorsements

Microsoft Exchange · 49

People-Centric Security Analytics

Leverage our *unique* data top identify individuals or groups within an organization that might present a previously unknown security risk.



Proofpoint Attack Index

Actor Sophistication

Attack Targeting

Type of Attack

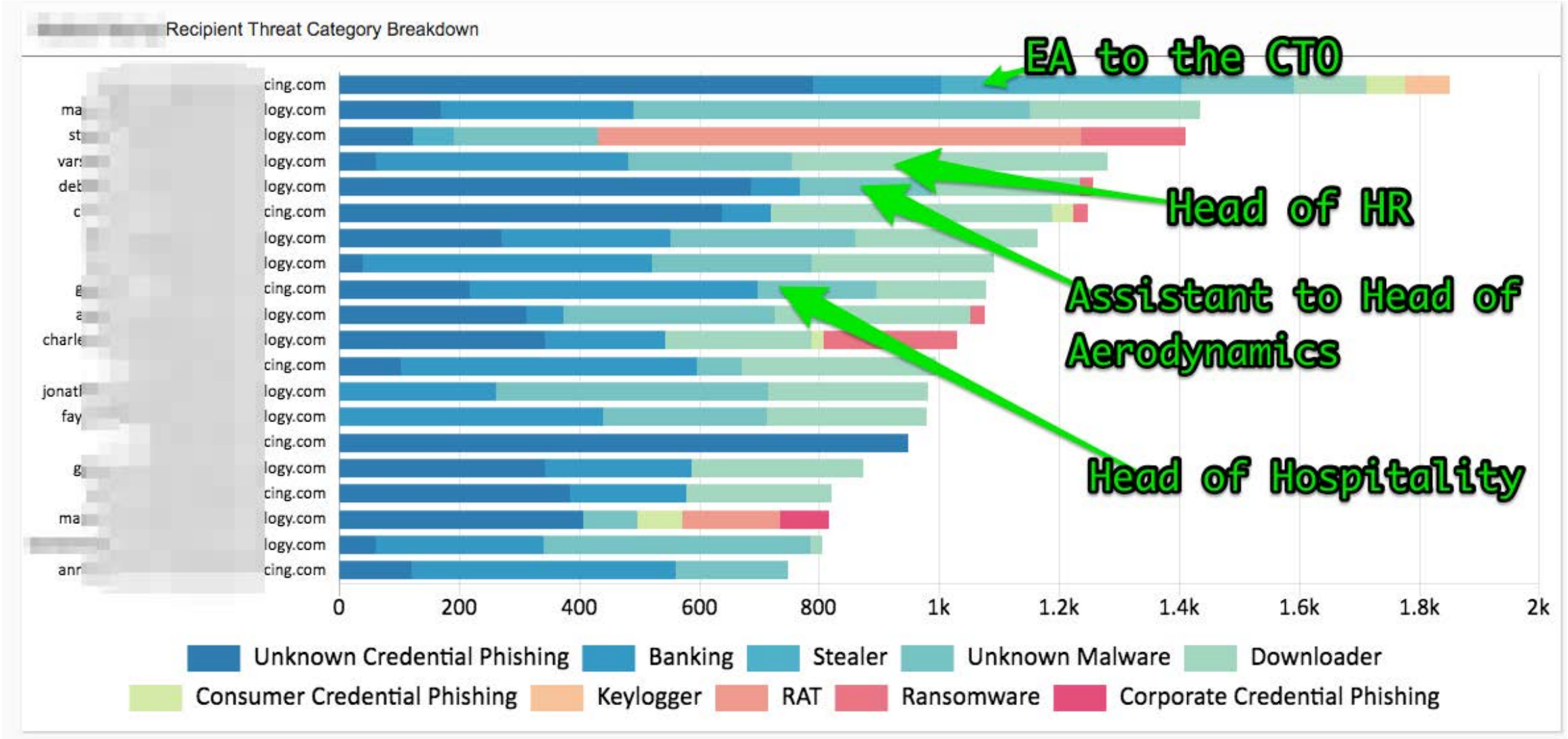
Volume of Attacks

- 0-1000 score per threat **sent**
- Weighted composite score
- Score explanations

Understand the risk your users face and prioritize the most effective compensating controls

Receive reporting and metrics on the threats your users face

Attack Index Results



Q&A

proofpoint®