



proofpoint.[®]

Threat Landscape

John Daly - Sr. Sales Engineer SLED West

jdaly@proofpoint.com

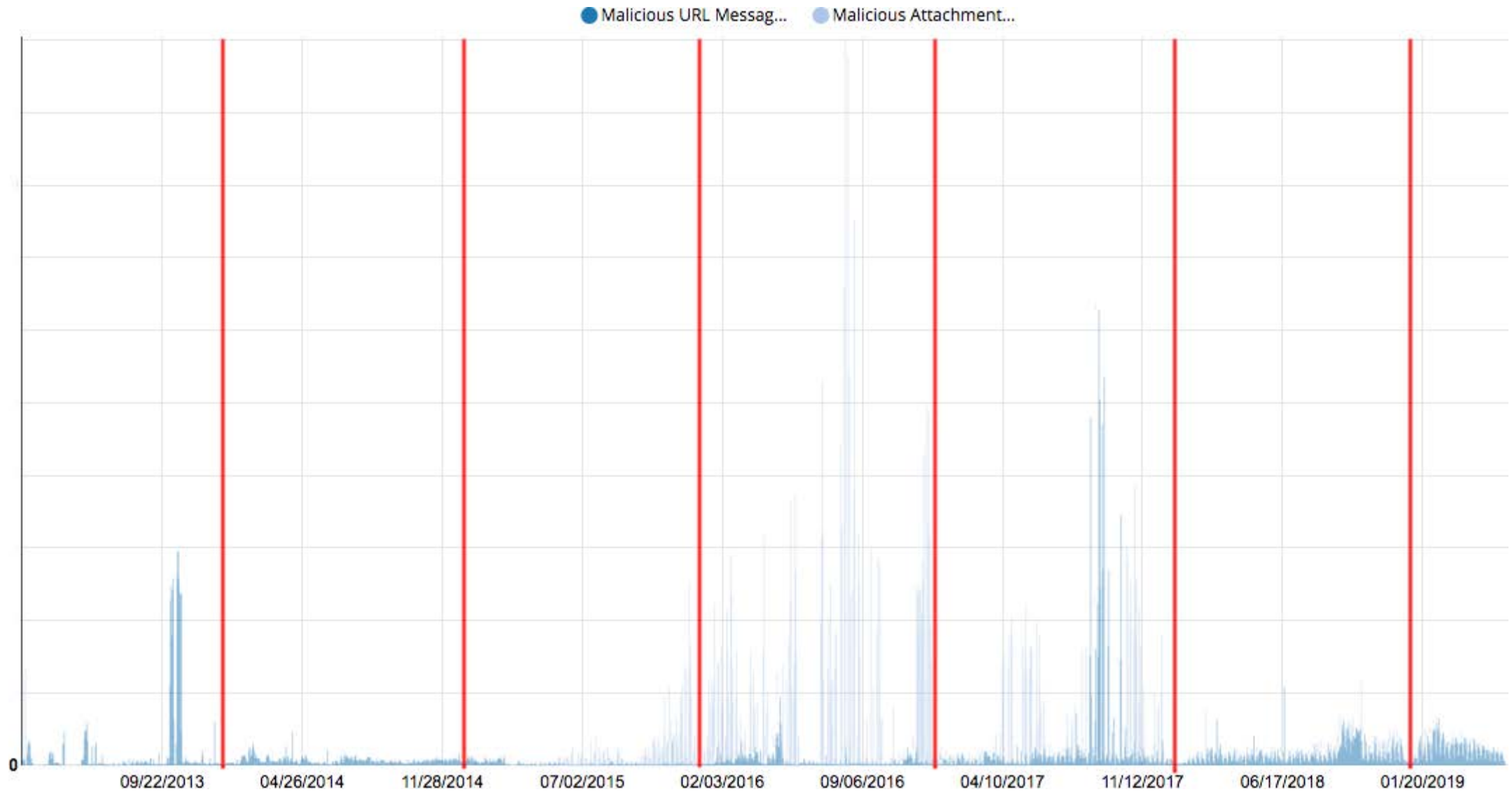
Global Trends



— Volume

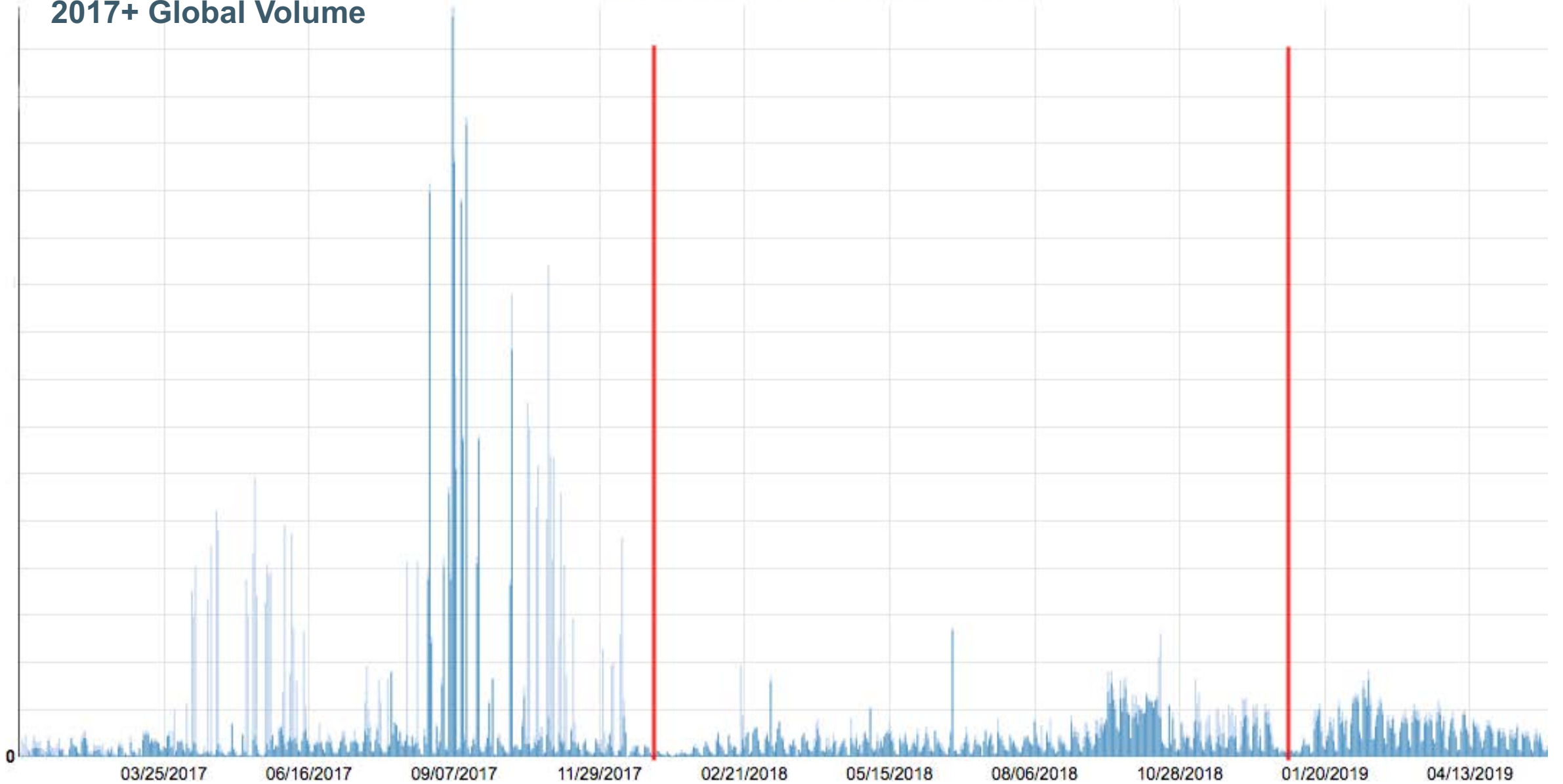
— Variety

2013+ Global Volume



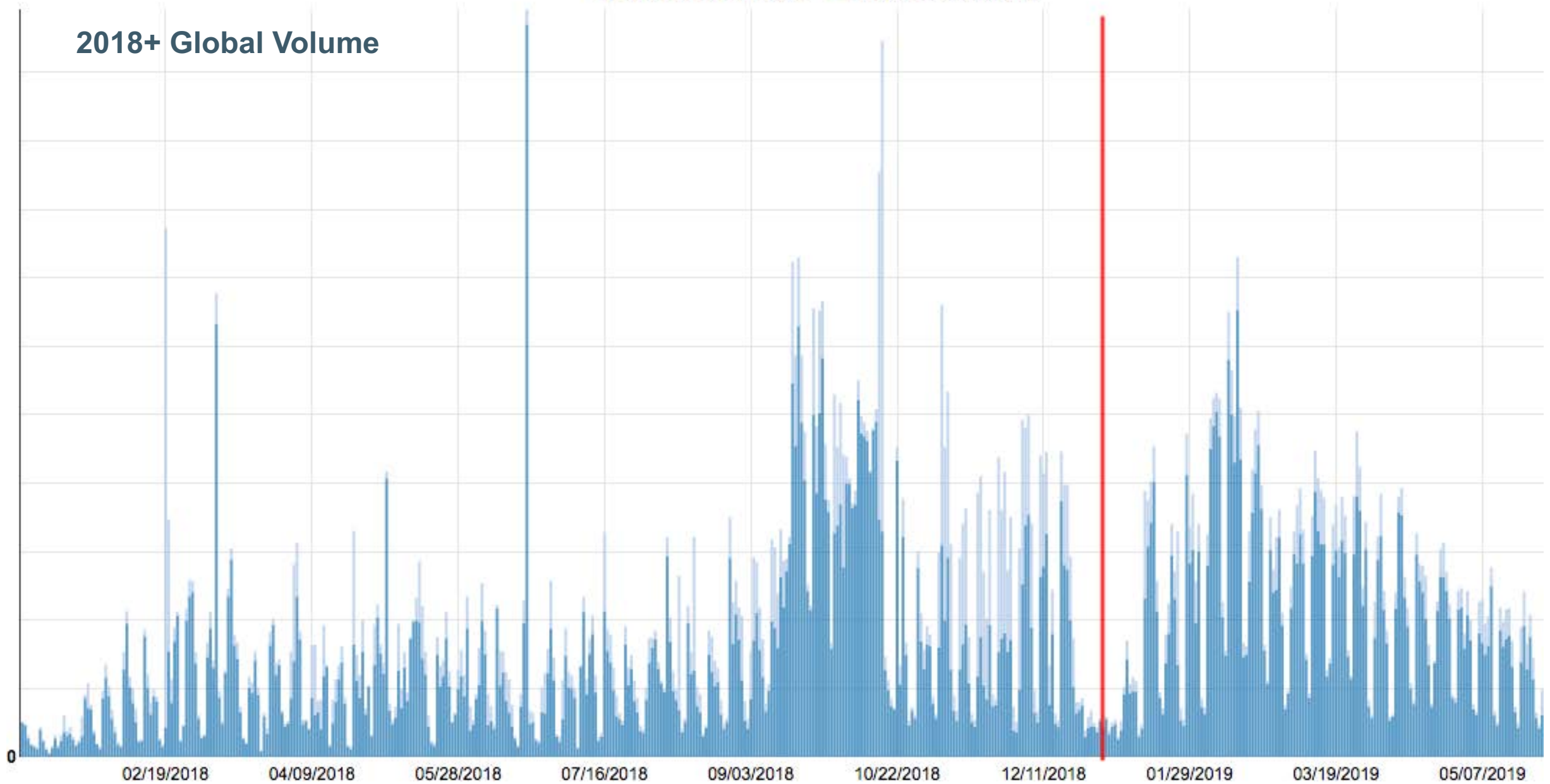
2017+ Global Volume

● Malicious URL Messag... ● Malicious Attachm...



2018+ Global Volume

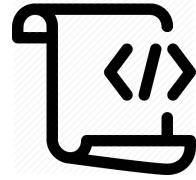
● Malicious URL Messag... ● Malicious Attachment...



Attack Structures







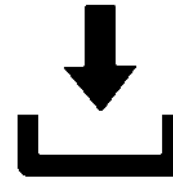
Script



Attachment



Exploit



File Download



Email



Link



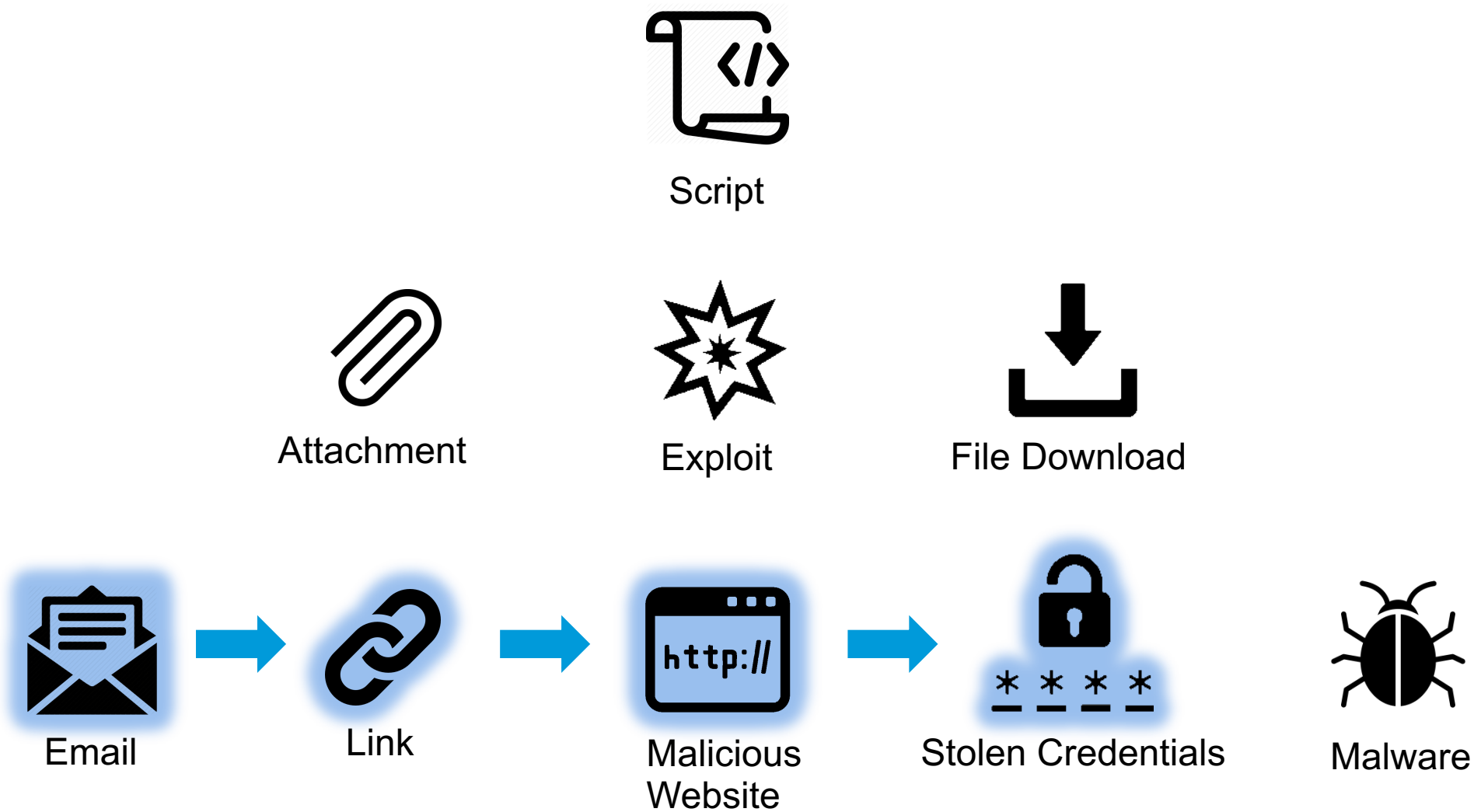
Malicious Website

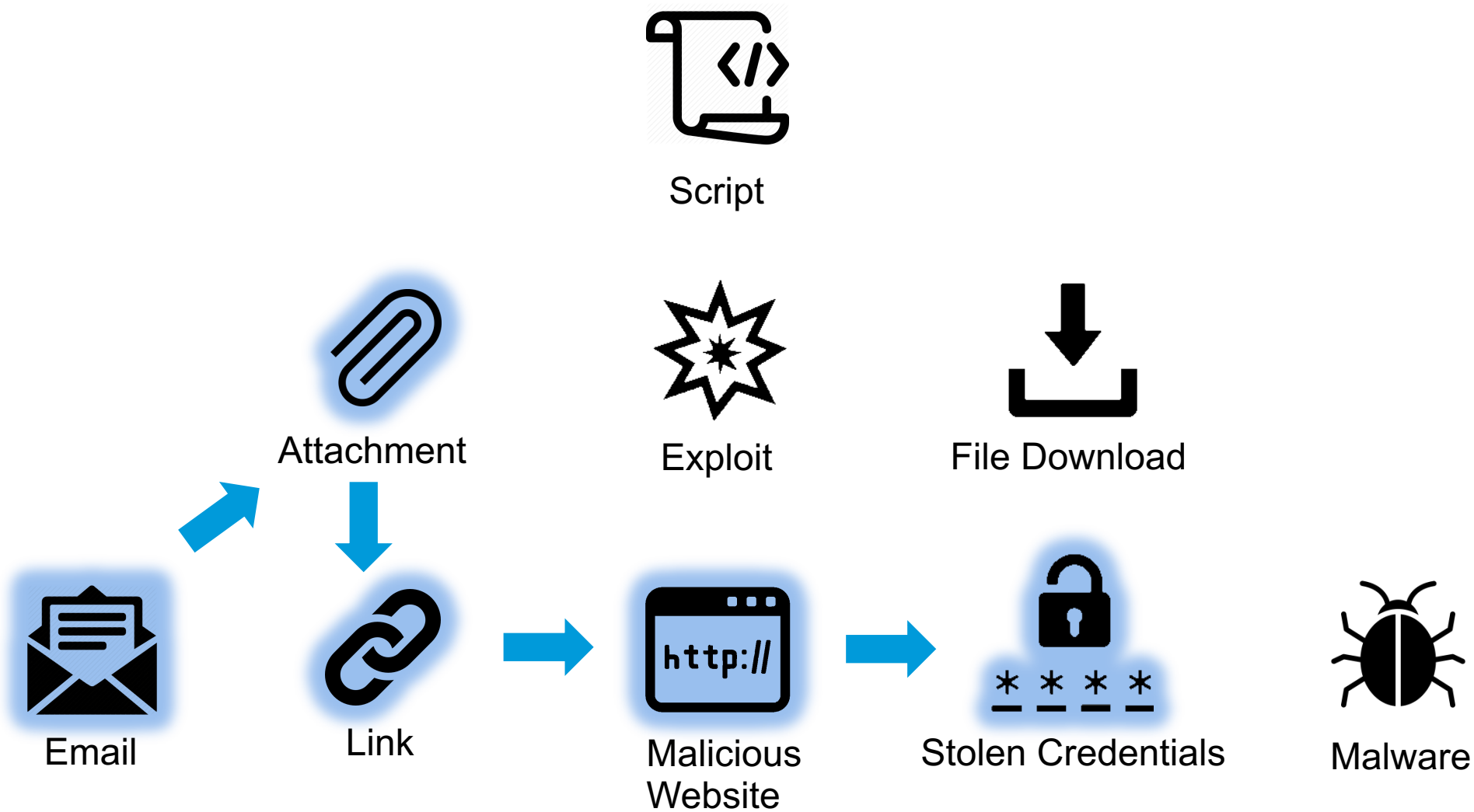


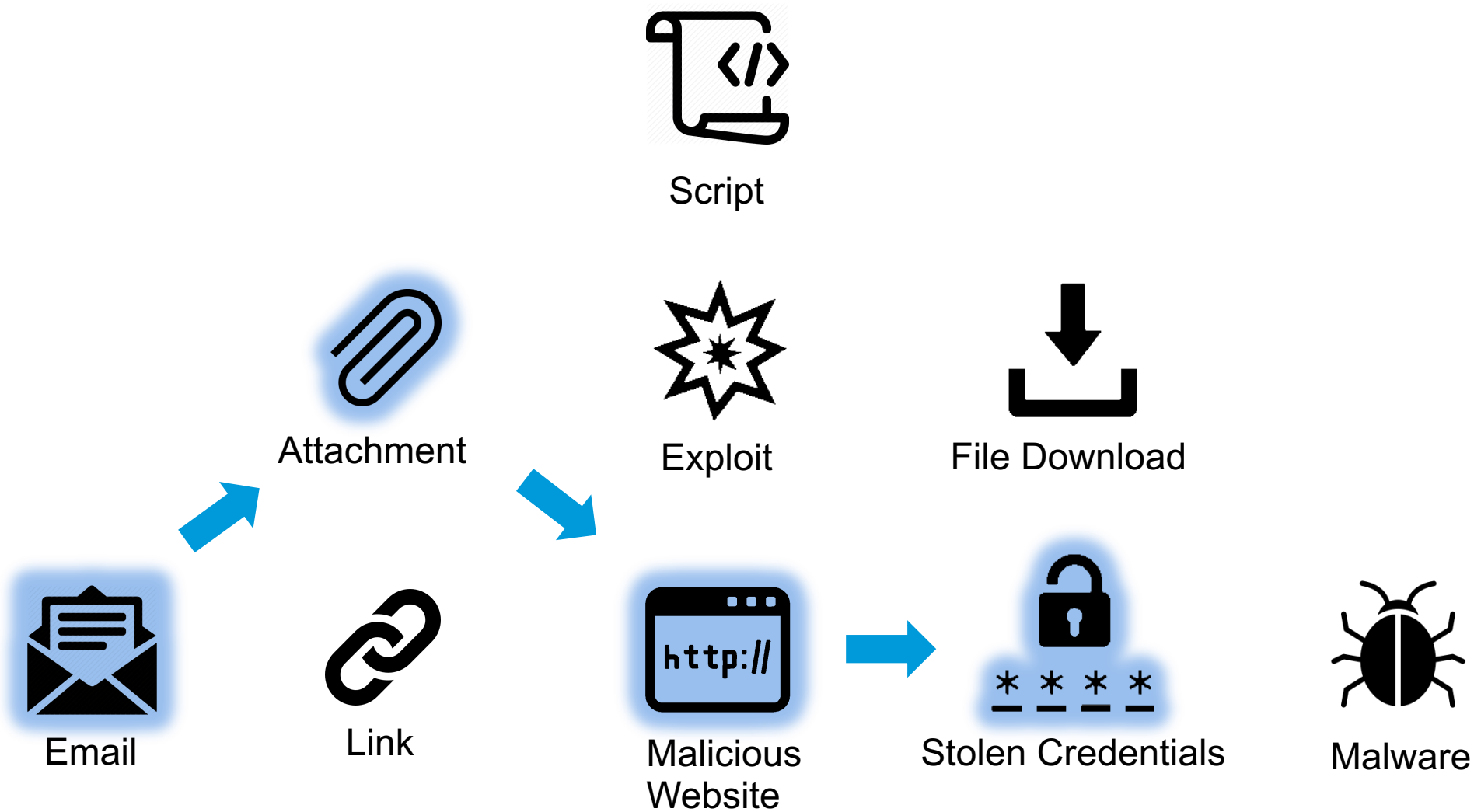
Stolen Credentials

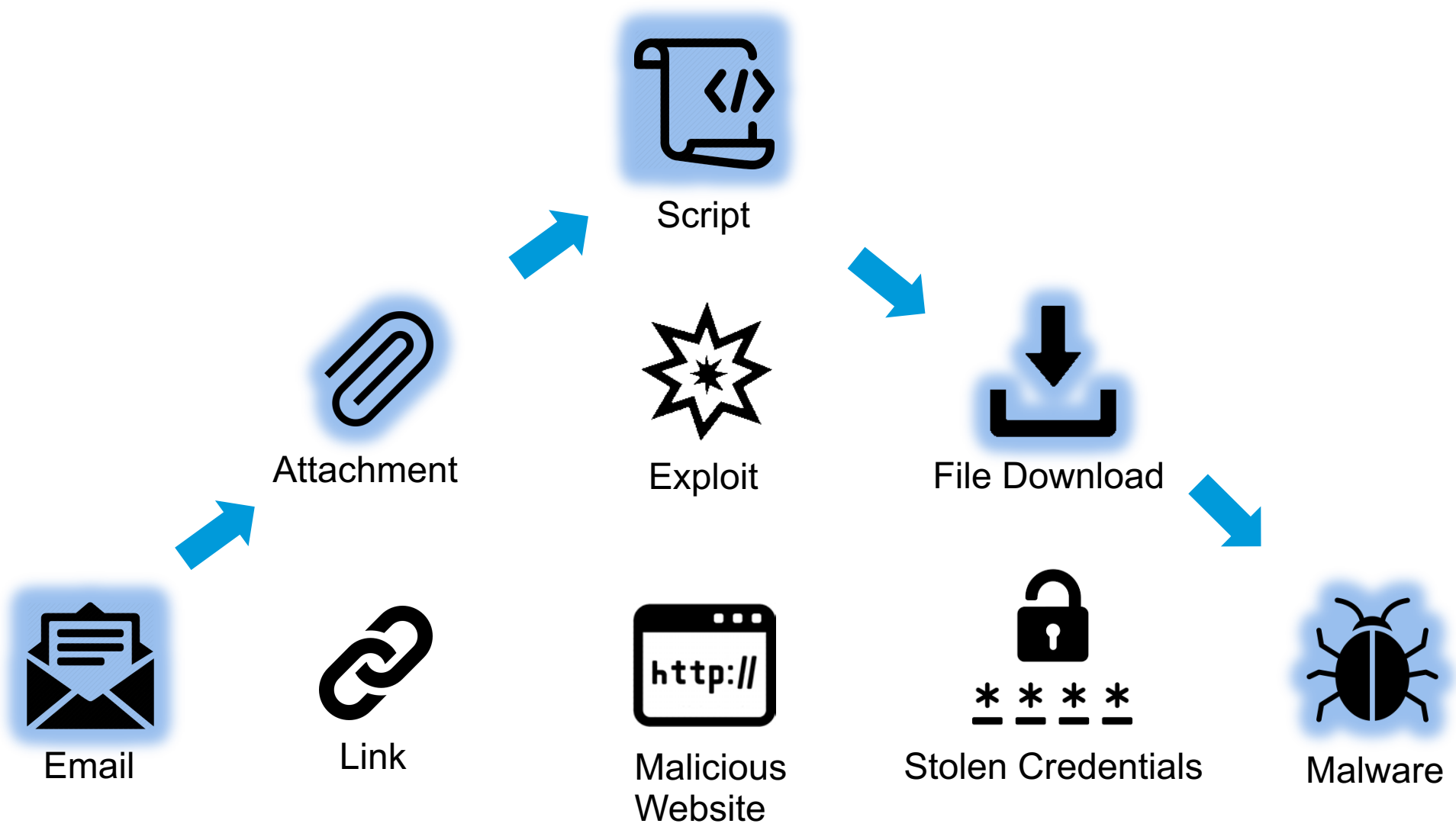


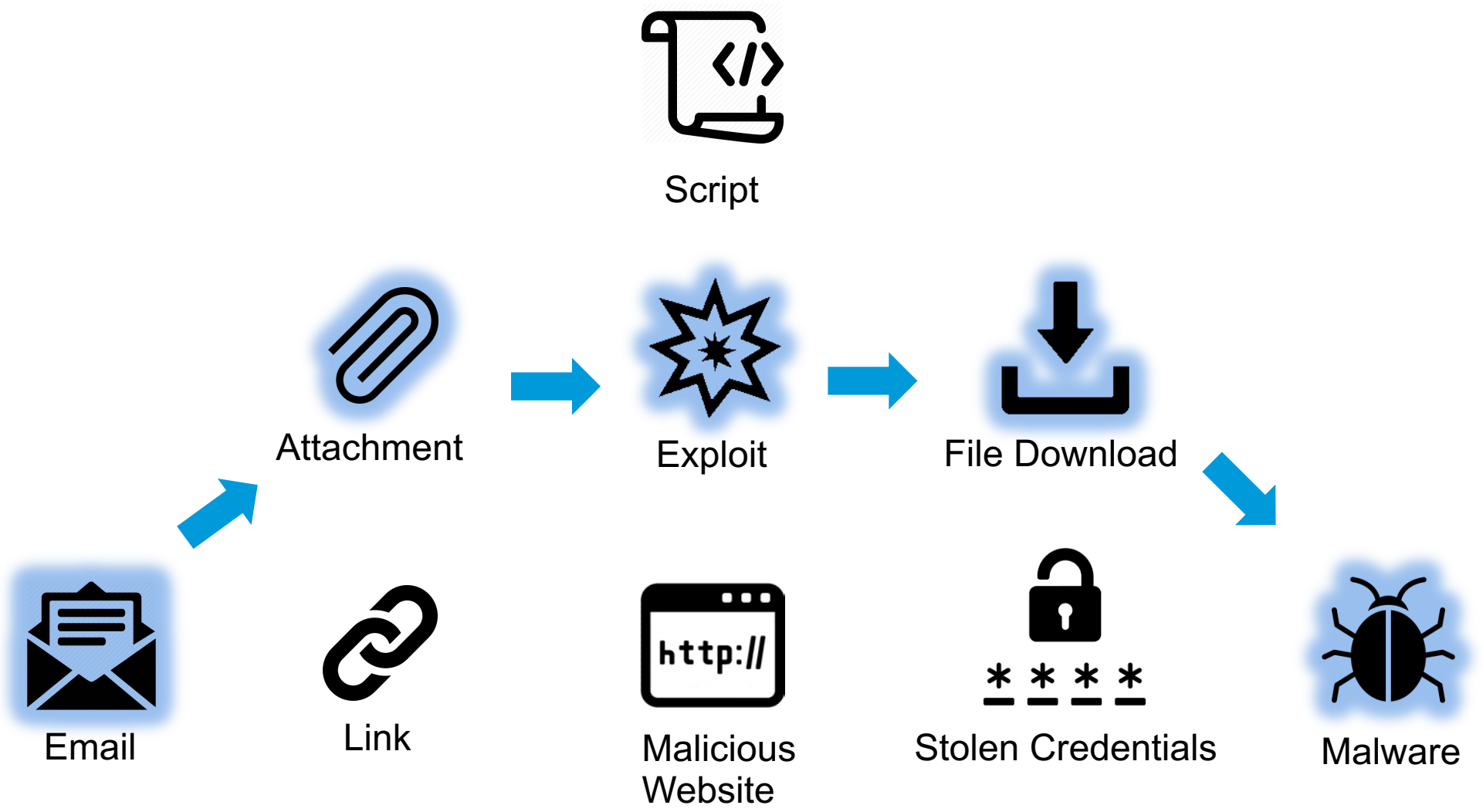
Malware

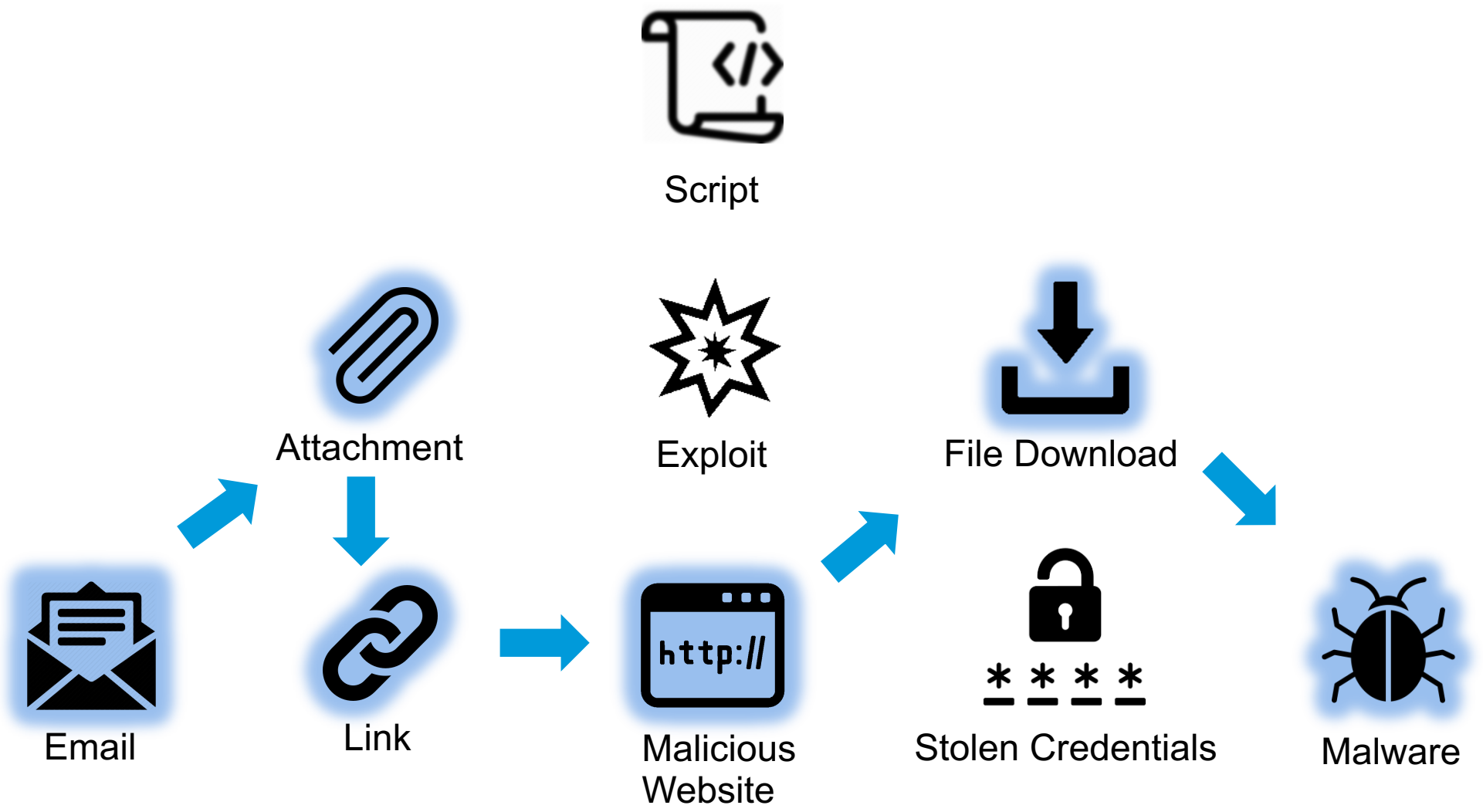


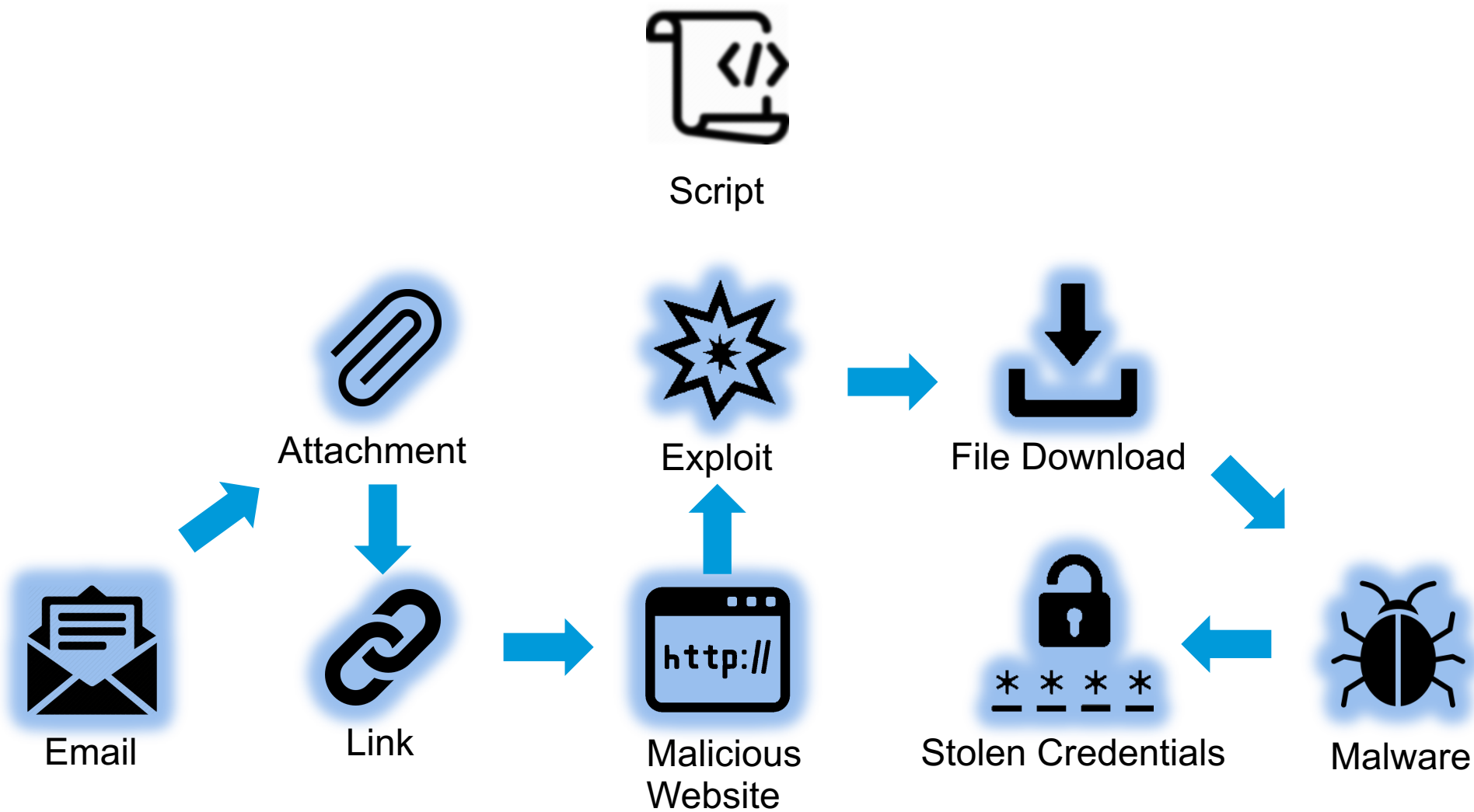










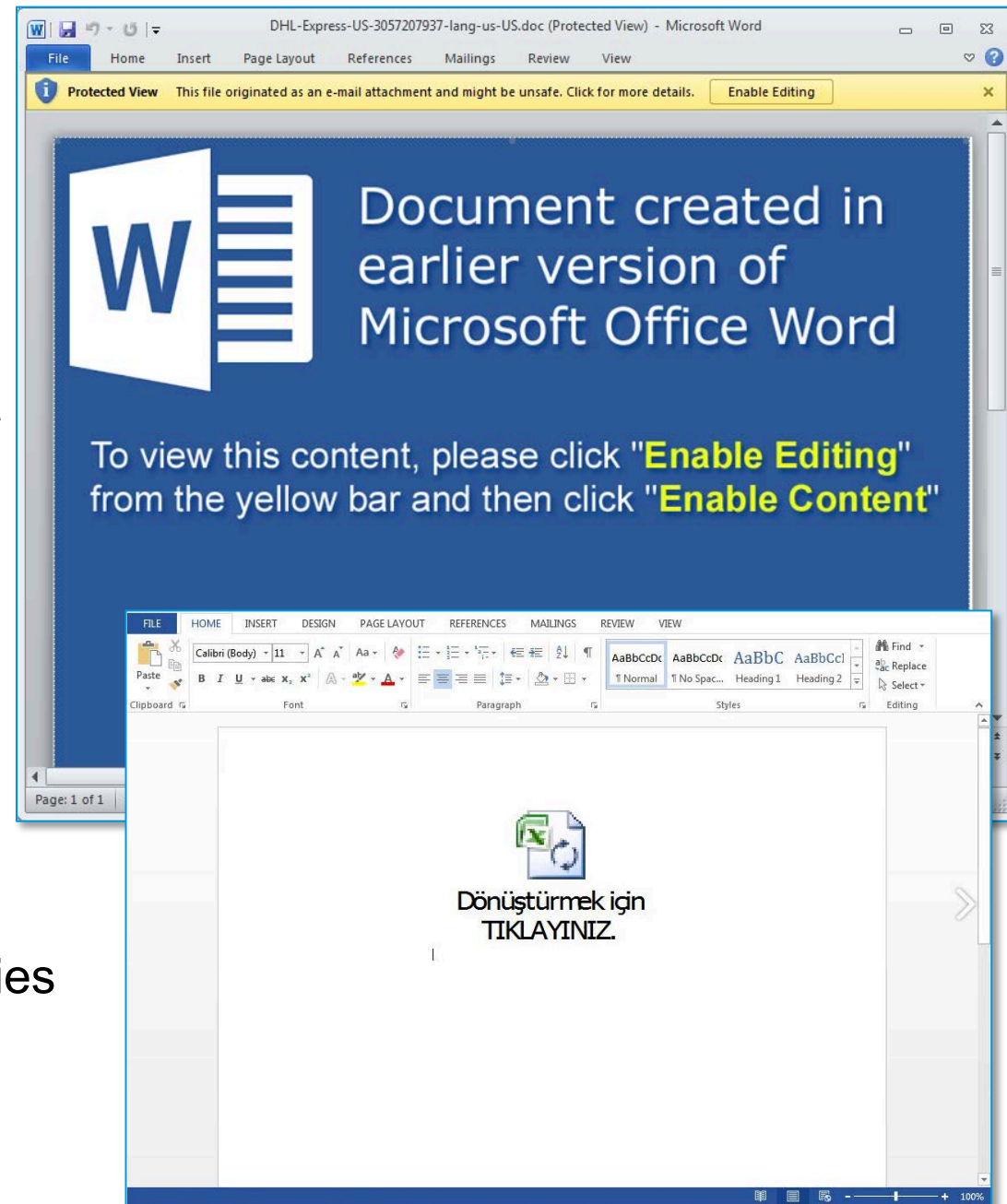




Threat Details

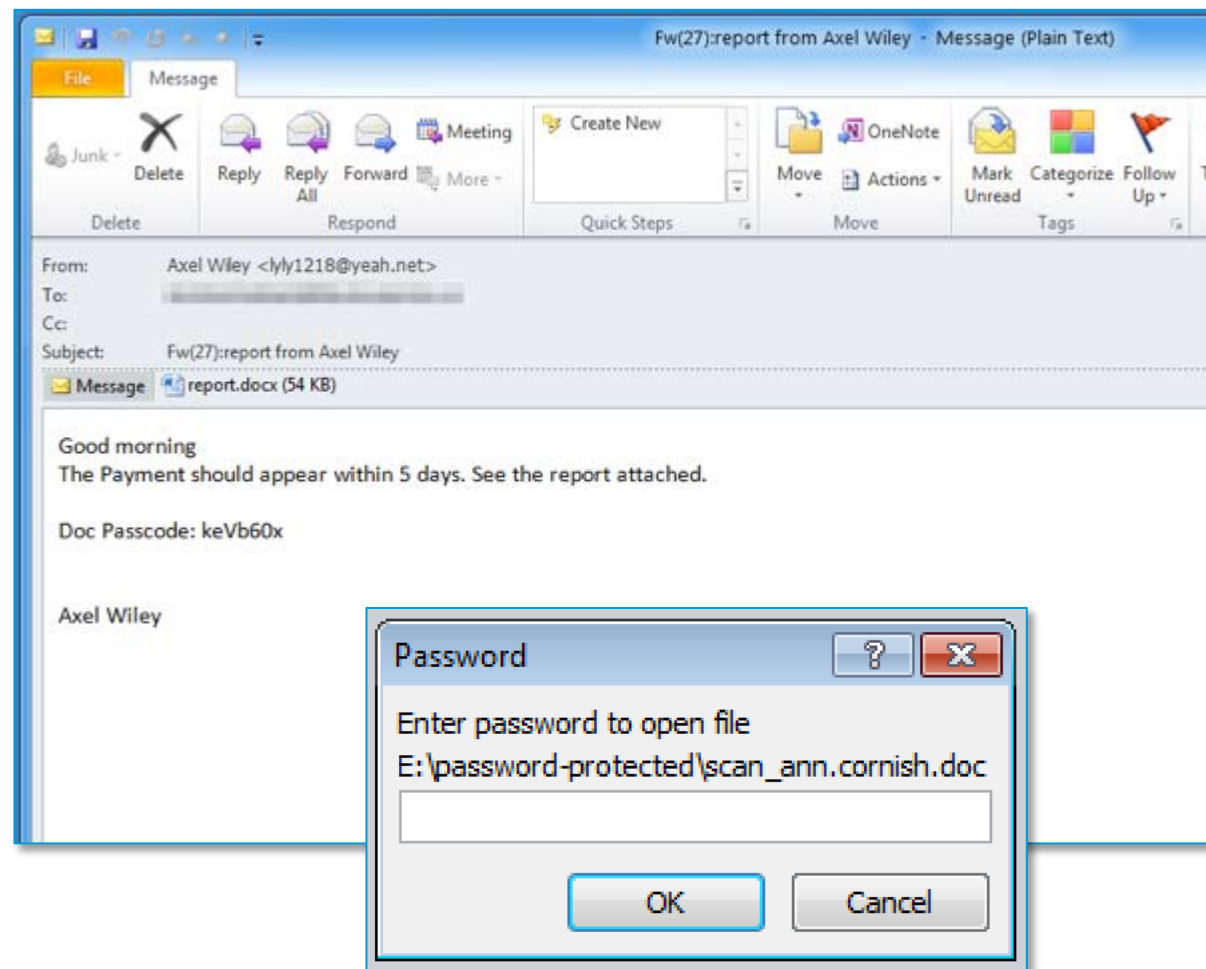
Abused Attachment File Types

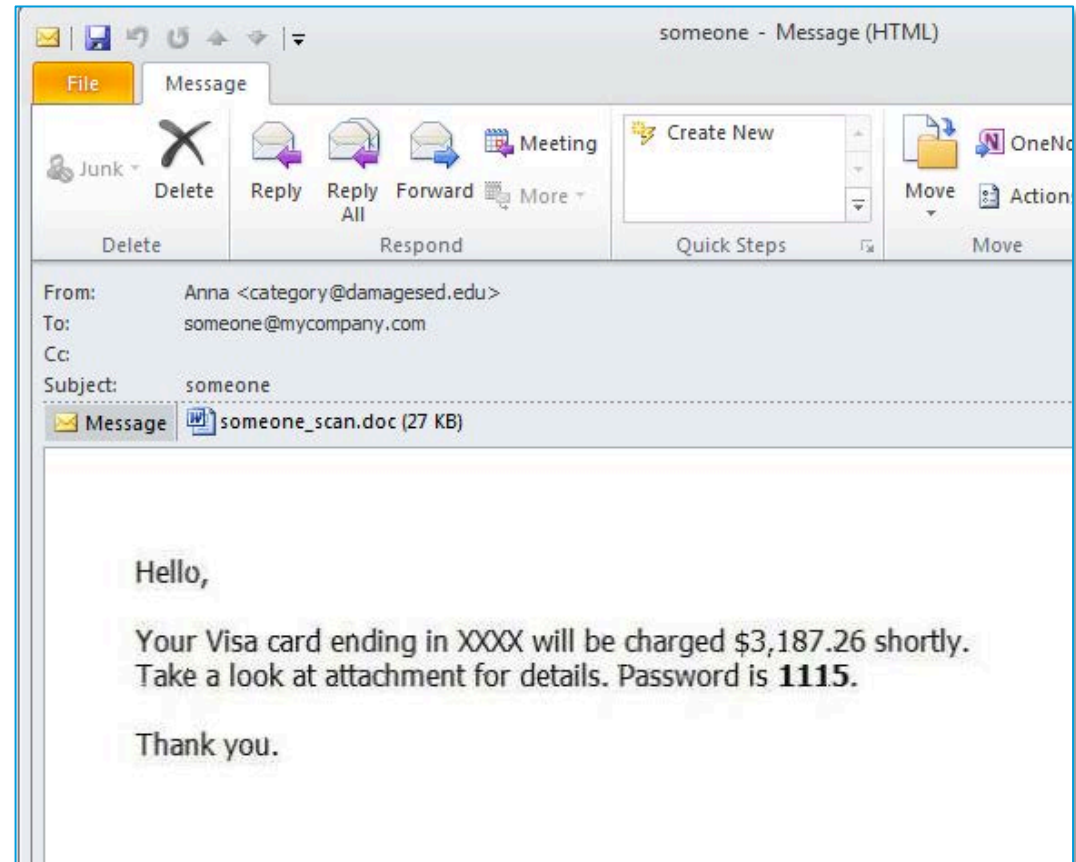
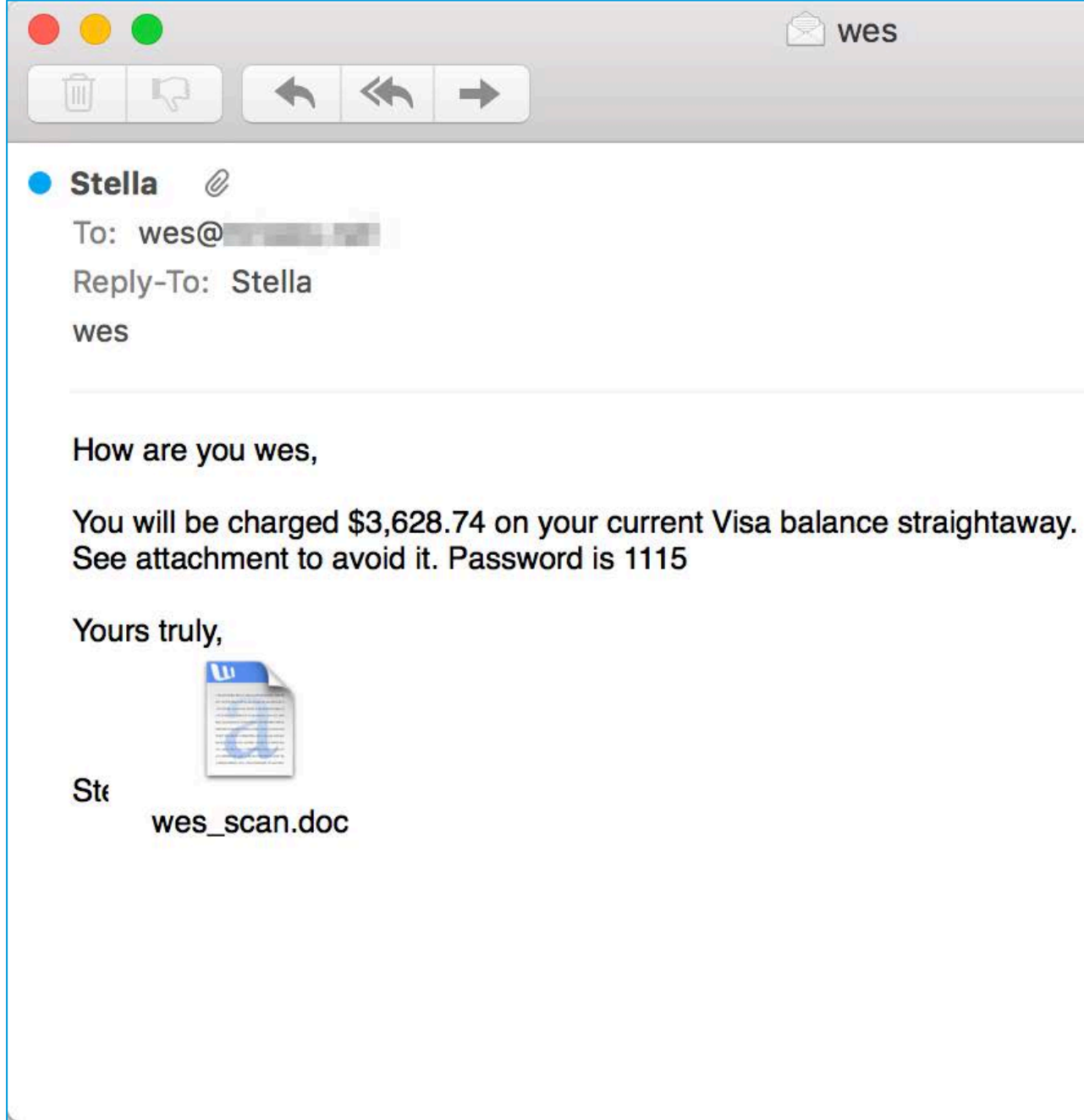
- Most Common
 - Microsoft Office Documents with Macros
 - Microsoft Office Documents with Embedded Object
 - PDF with links
- New
 - XL4 Macro
 - Template Injection
- Other
 - DDE
 - Password protected Microsoft Office Documents
 - Documents that exploit Microsoft Office vulnerabilities
 - Most common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



Password Protected Documents

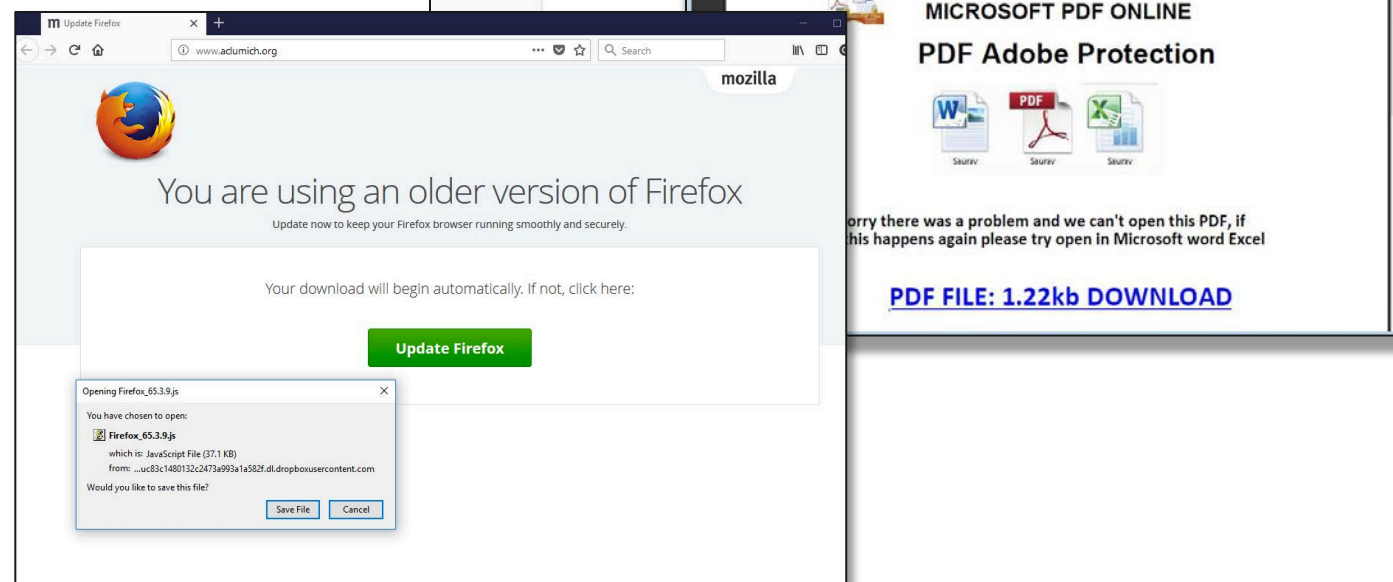
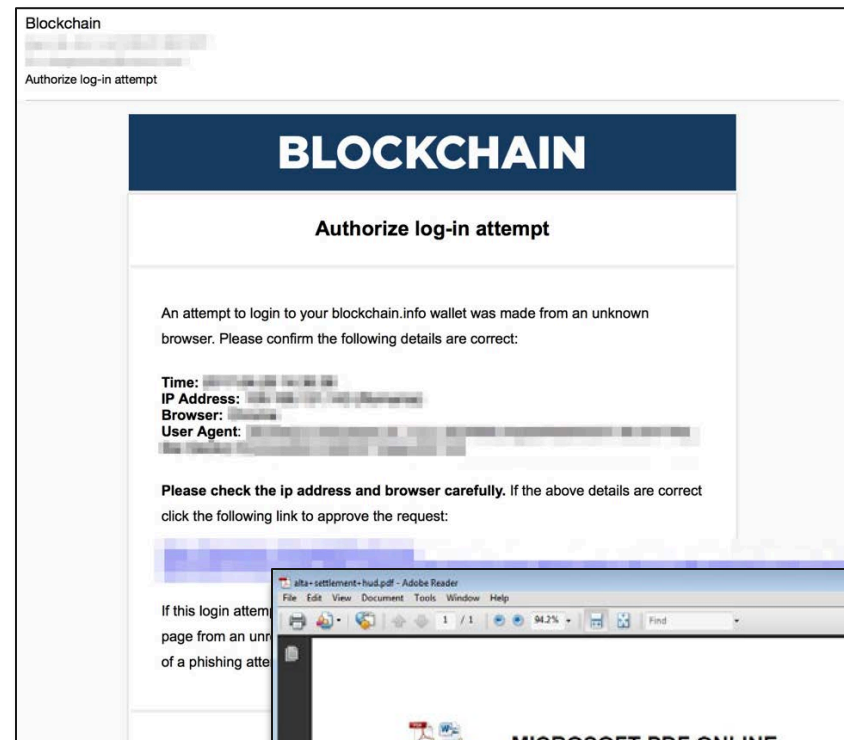
- Office documents where passwords are required to open the document
- Password is presented to the user in the body of the email
- Advantages
 - Appears to the user as privileged information contained within the document
 - Evades automated sandbox analysis
- Campaigns tend to use the same password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



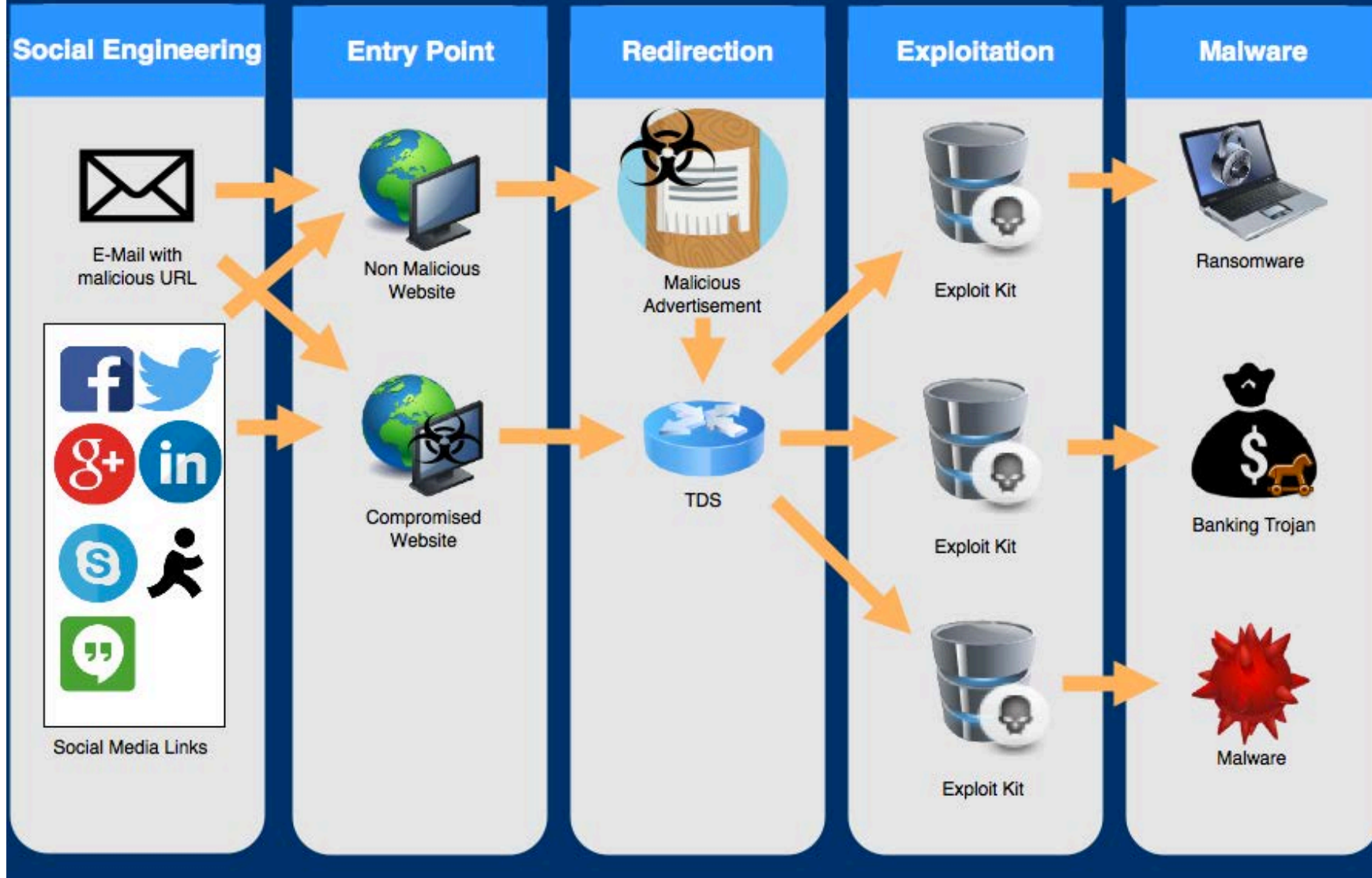


Delivery Methods - URL

- 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
 - SocGhosh
 - SocGoth
- Less common:
 - Links to pages infected by Exploit Kits



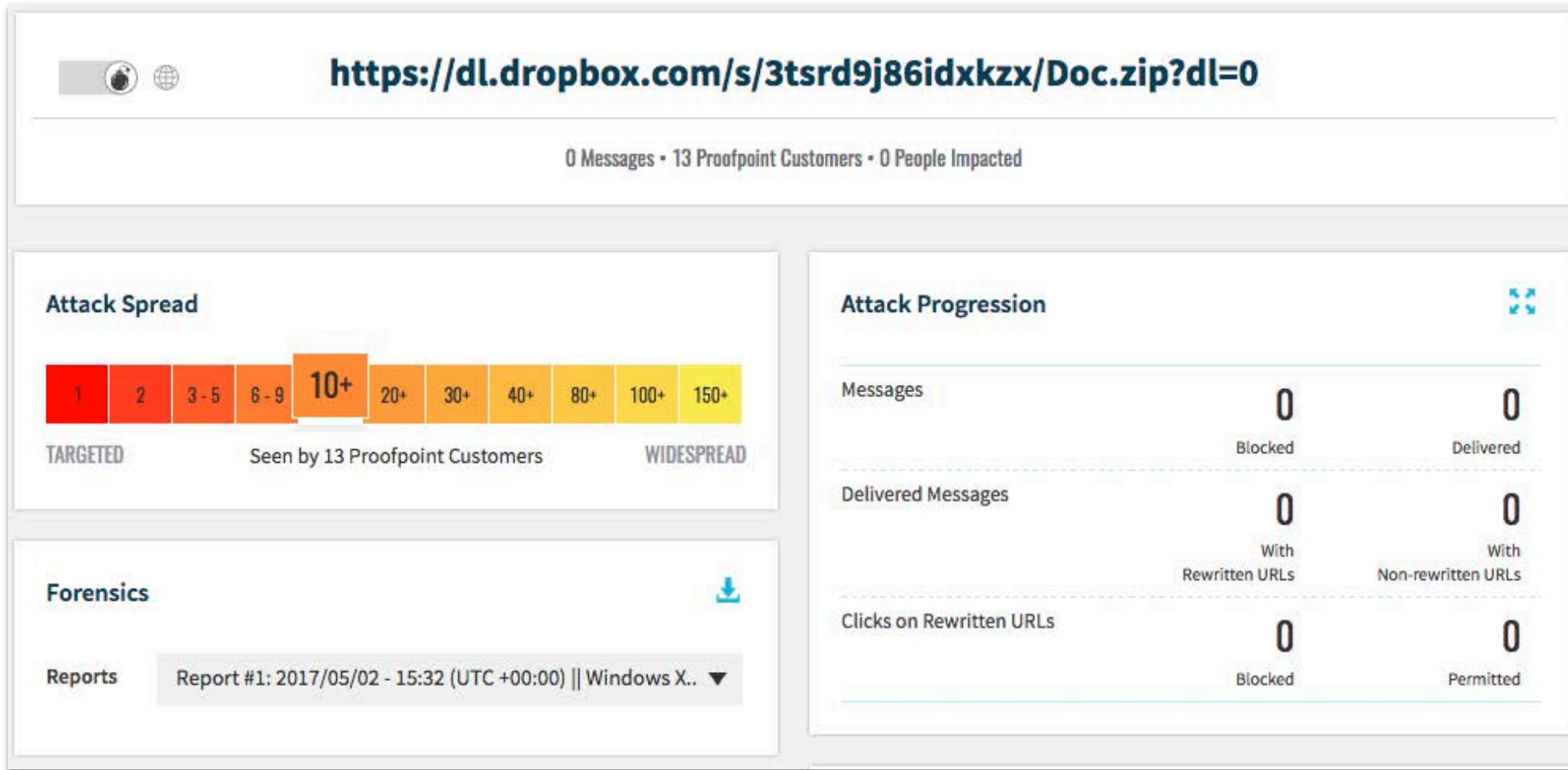
Exploit Kit Kill Chain



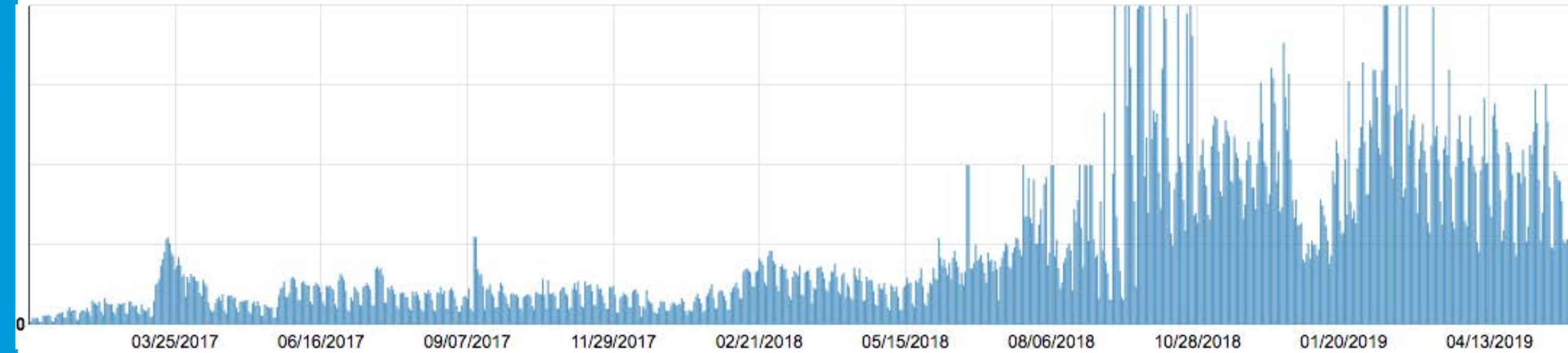
Socgholish

The image is a composite of two screenshots. The left screenshot shows a social media post from 'HONEST SOMOS' on 'http://honestbarcelona.com/'. The post features an Adobe Flash Player advertisement with the text 'Your Ad', 'Adobe Flash Player', and 'Thanks for choosing Adobe Flash Player.' Below this, there is a note about antivirus software and a yellow 'Install now' button. The right screenshot shows a Firefox browser window with the URL 'www.aclumich.org'. A large notification banner reads 'You are using an older version of Firefox' and 'Update now to keep your Firefox browser running smoothly and securely.' Below the banner is a green 'Update Firefox' button. A small dialog box titled 'Opening Firefox_65.3.9.js' is open, displaying the file name 'Firefox_65.3.9.js', its type 'JavaScript File (37.1 KB)', and its source '...uc83c1480132c2473a993a1a582f.dl.dropboxusercontent.com'. The dialog asks 'Would you like to save this file?' and has 'Save File' and 'Cancel' buttons.

Malware at the end of links

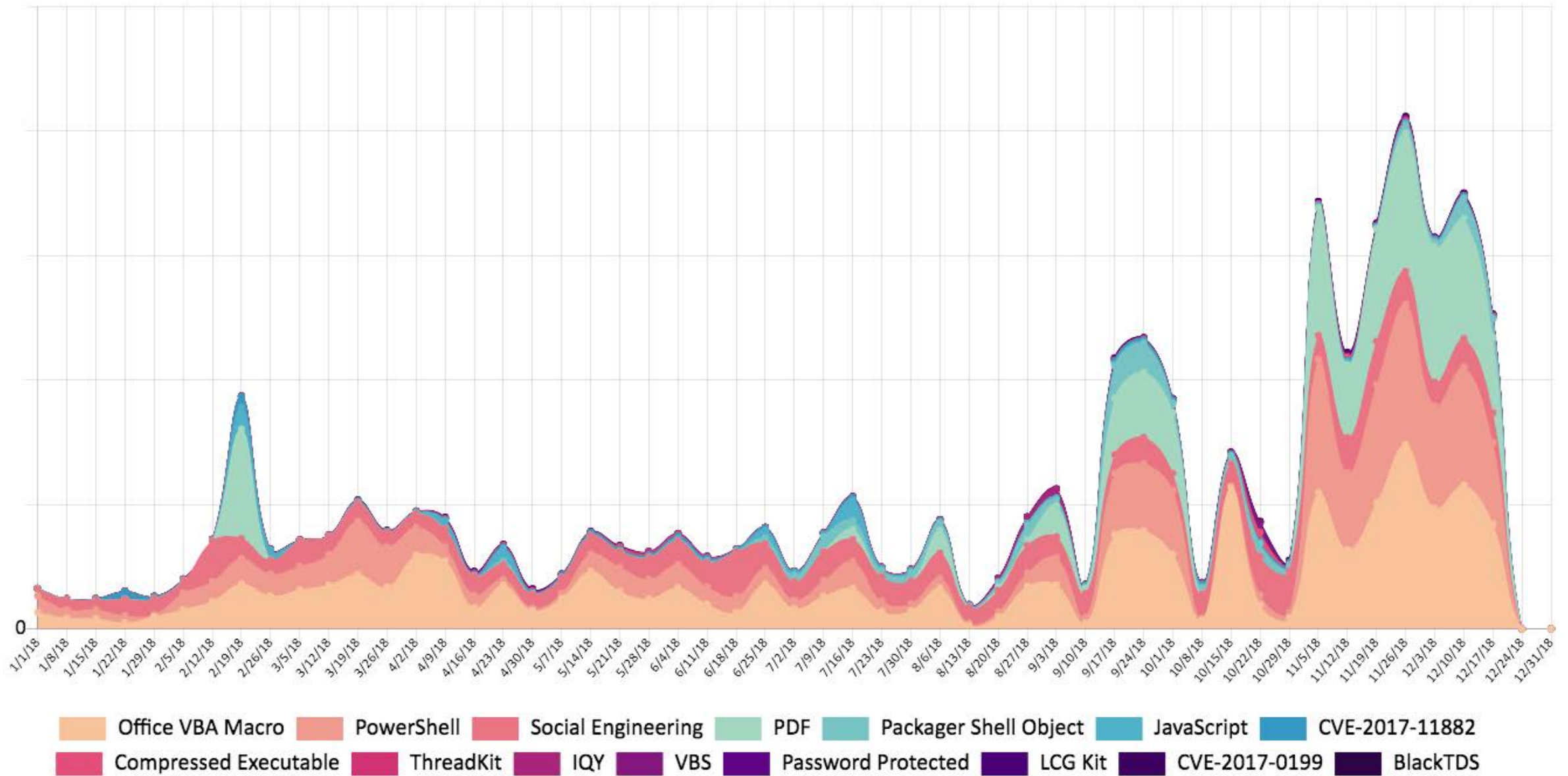


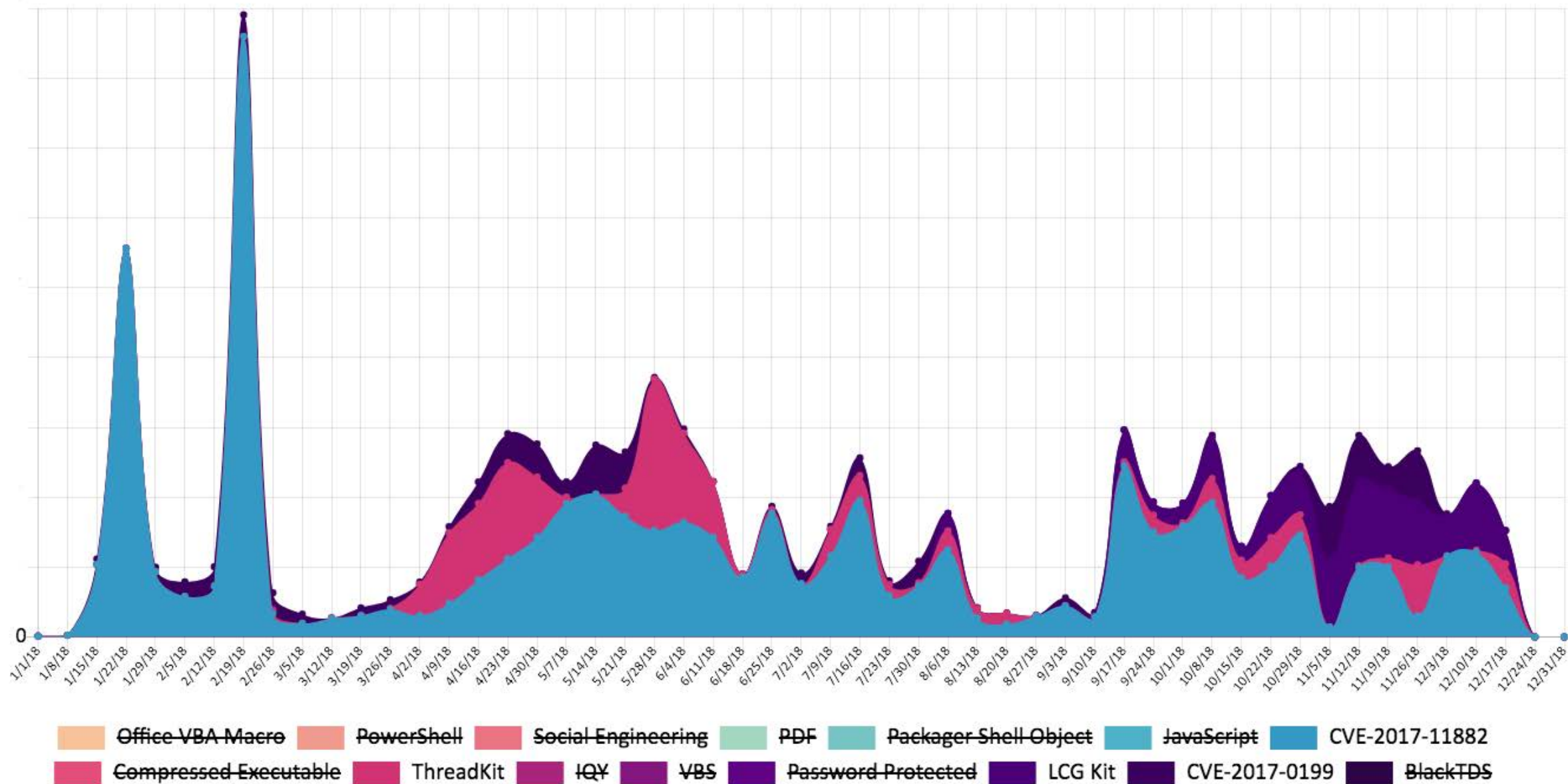
Unique Malicious URLs

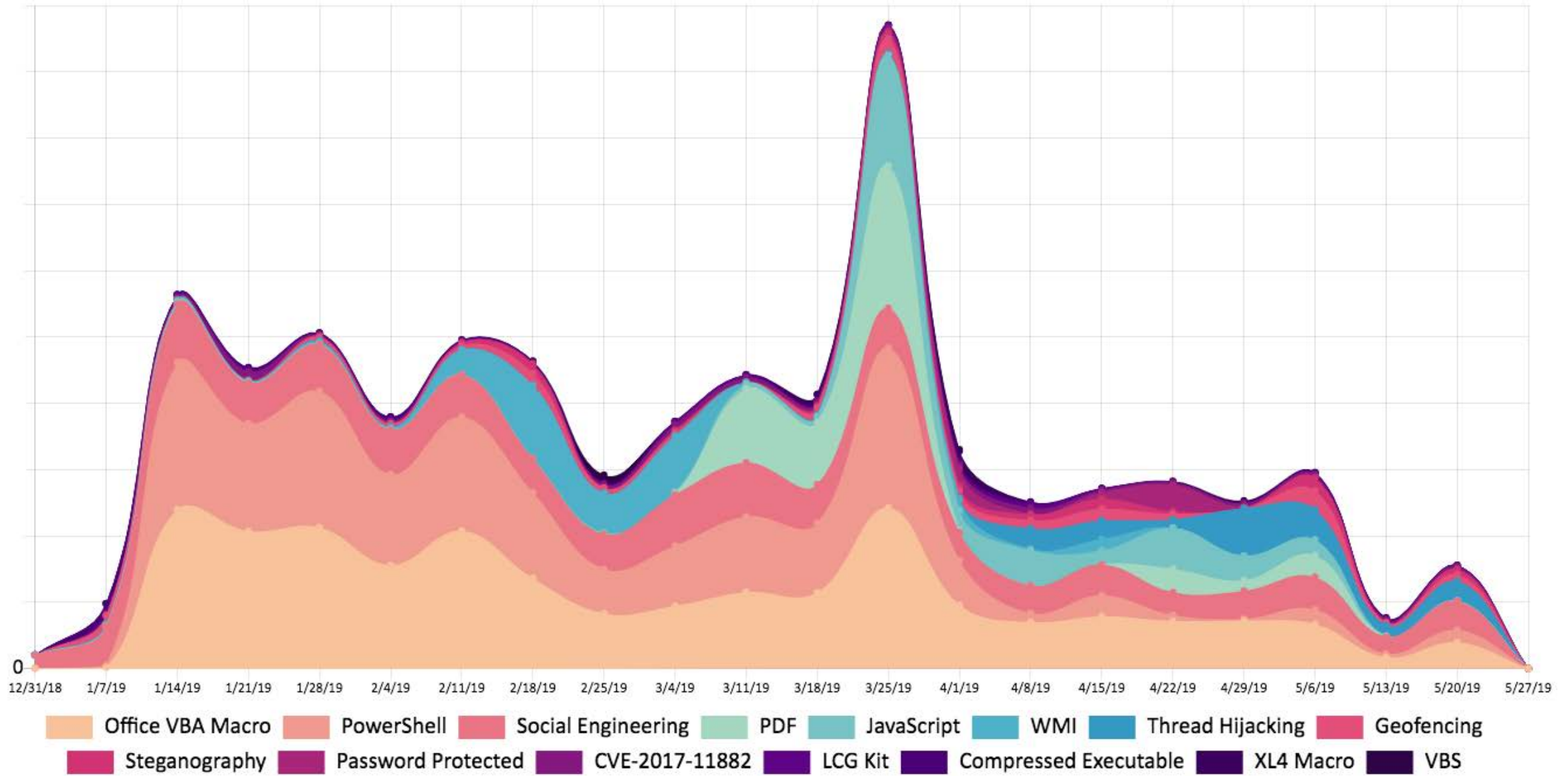


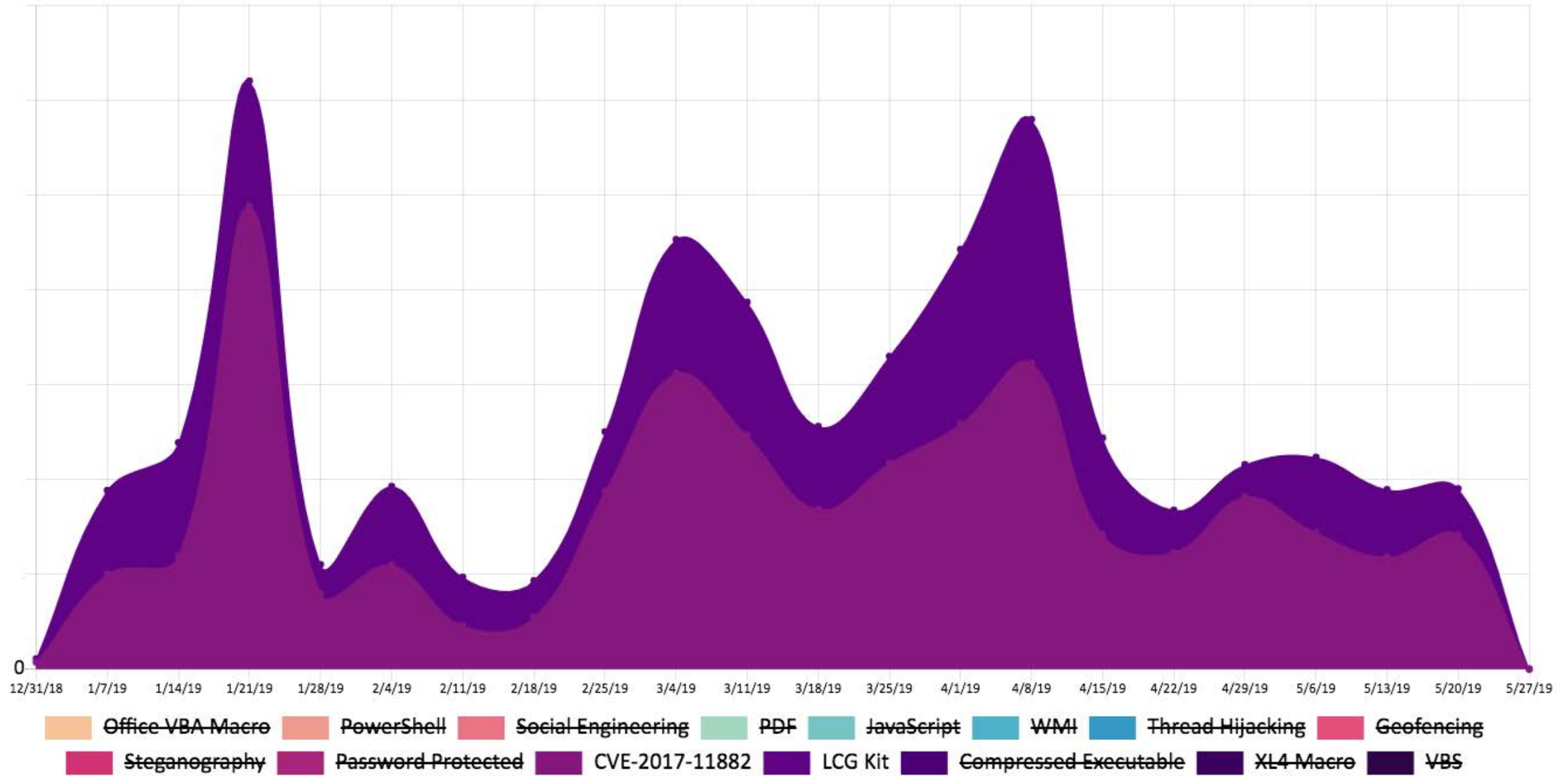
Exploits

- 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



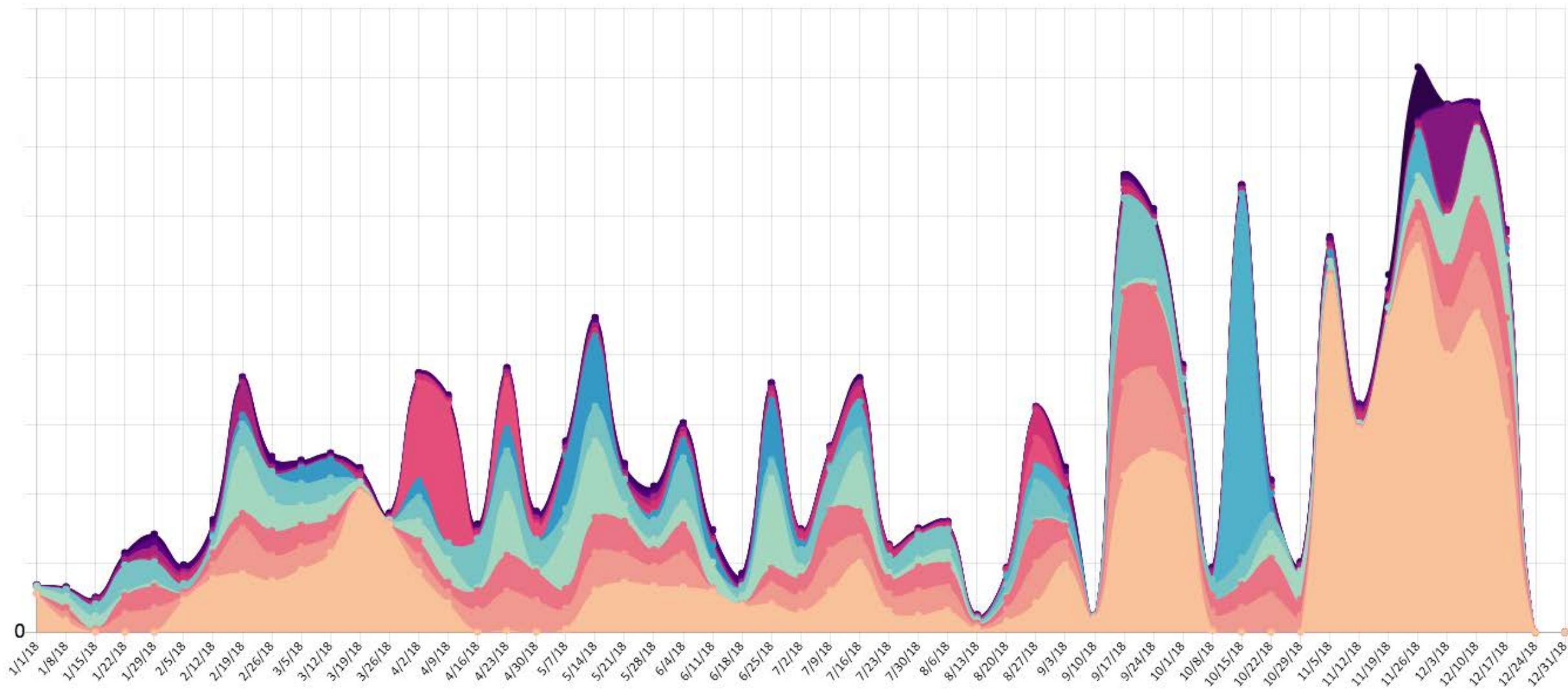




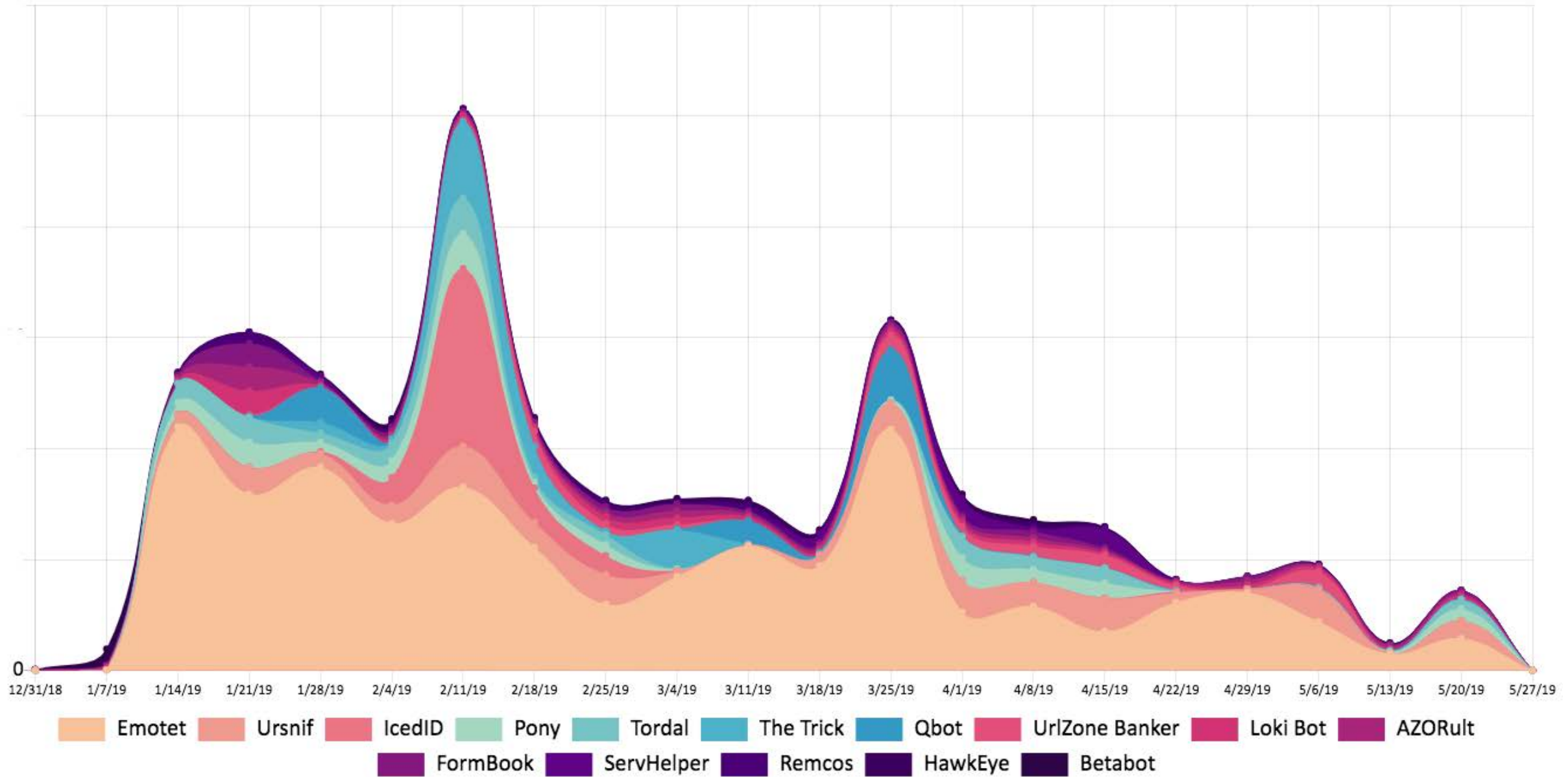


Malware

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



- Emotet
- Pony
- Tordal
- Ursnif
- Panda Banker
- FlawedAmmyy
- UrlZone Banker
- GandCrab
- The Trick
- Loki Bot
- ServHelper
- FormBook
- Nymaim
- AgentTesla
- Remote Manipulator System/RMS



Actors*

*Not the actors pictured in this slide

© 2019 Proofpoint. All rights reserved

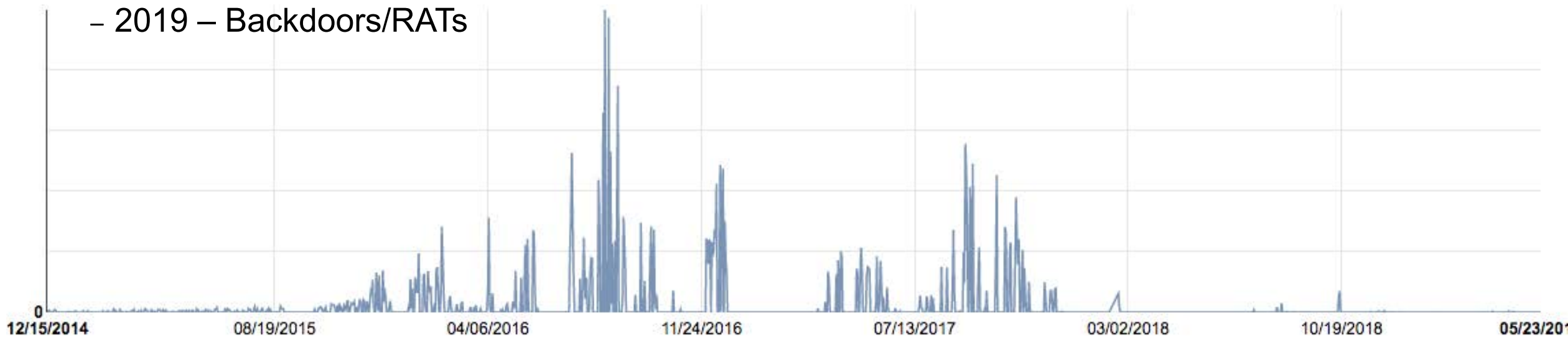
proofpoint.

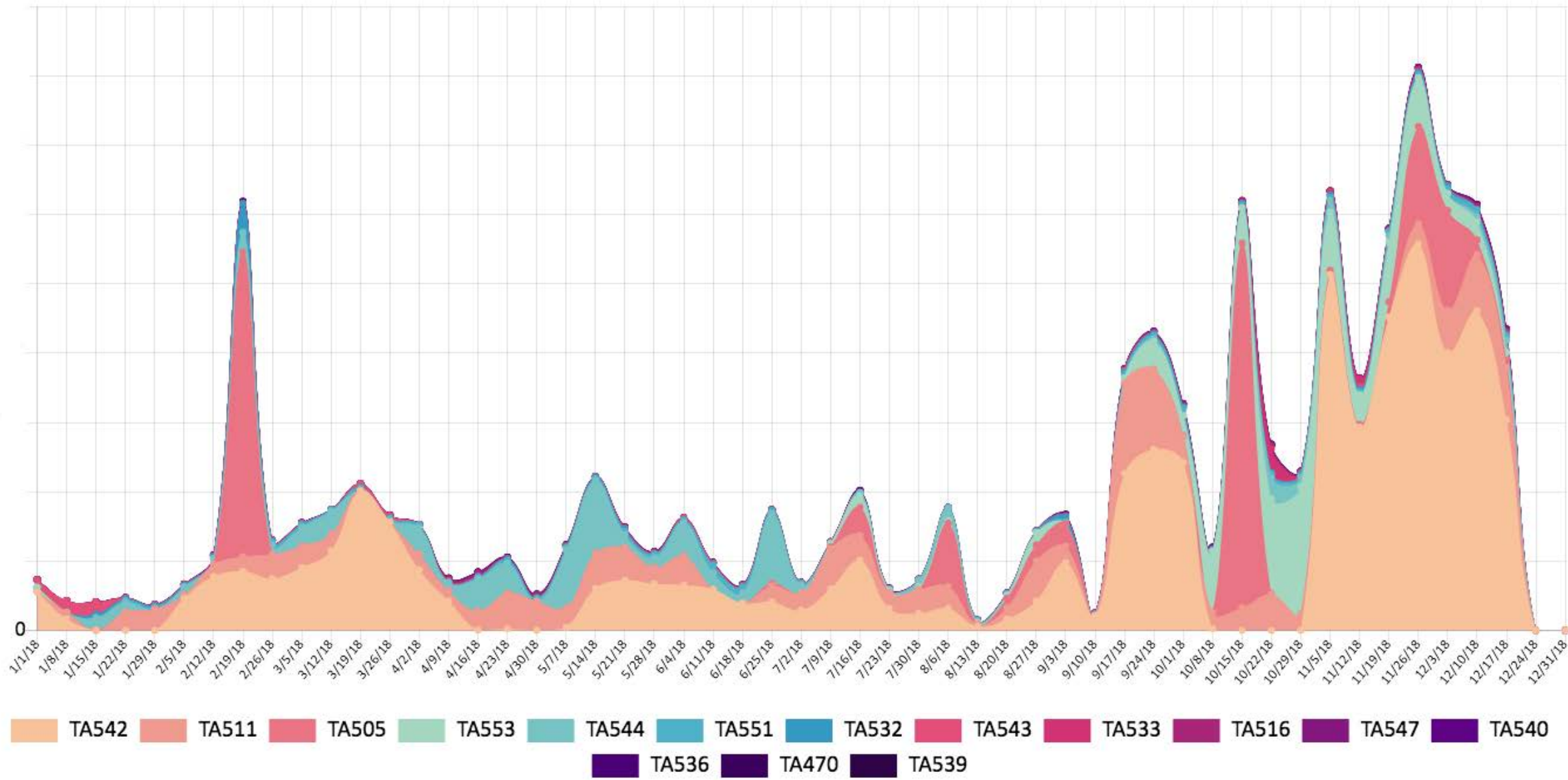
TA Designations

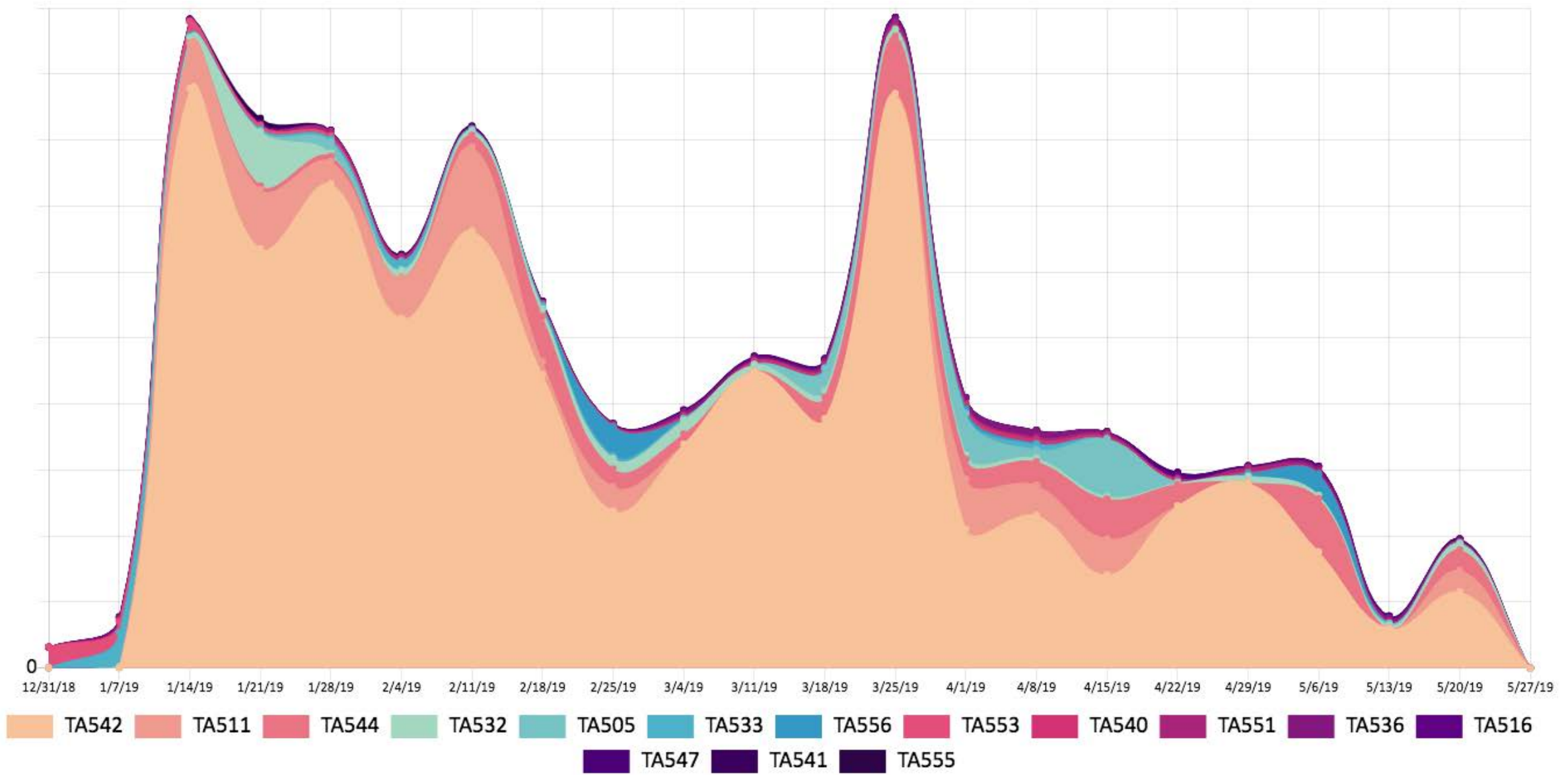
- 000 - 499: APT
- 500 - 1999: Crime large
 - large campaigns like those distributing Locky / Dridex bankers and ransomware
- 2000 - 2999: Crime small
 - more targeted like certain small BEC groups
- 3000 - 3999: Crime sophisticated
 - Cobalt, Fin7
- 4000 - 4999: Unknown/Sophisticated/Specialists
 - 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

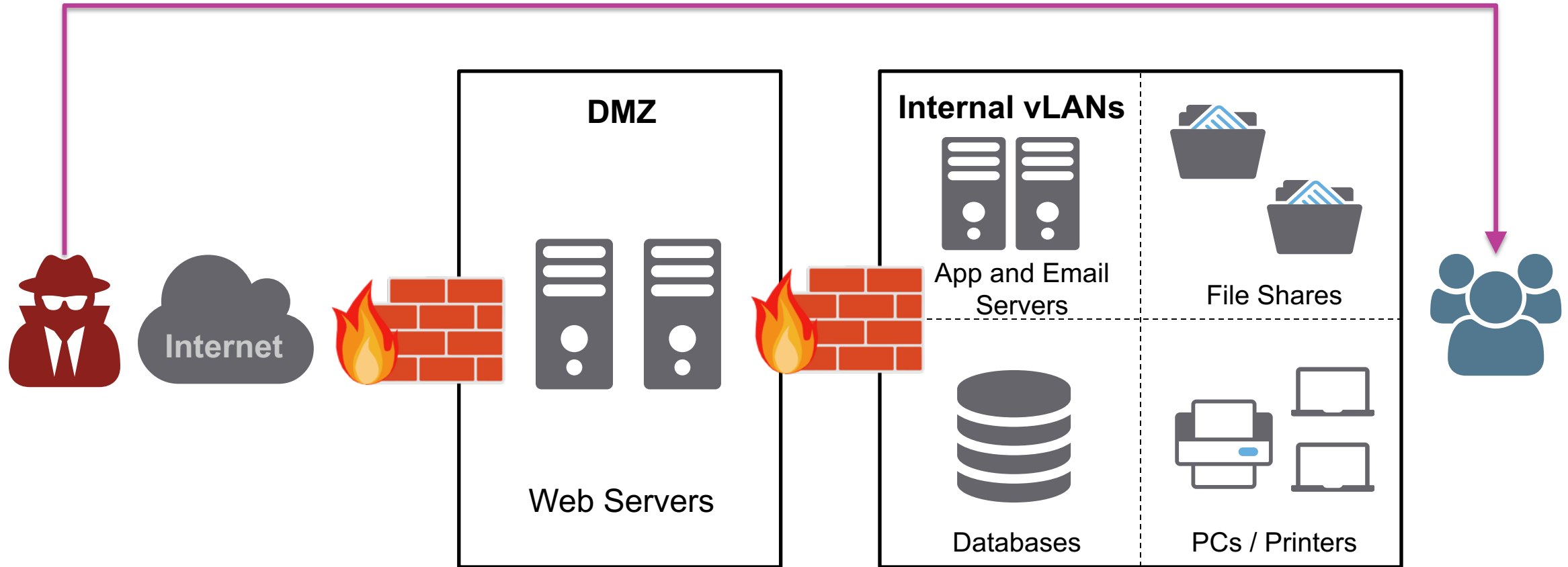






People Centric Security Analytics (PCSA)

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



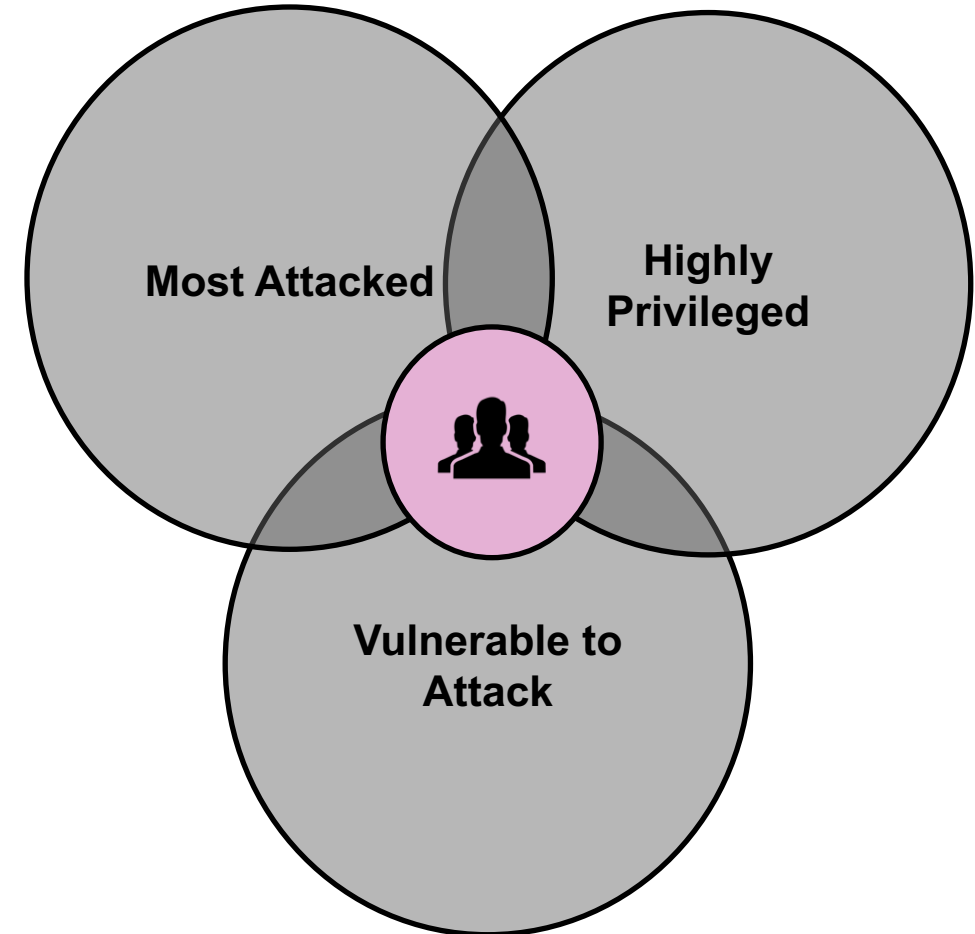
Richard Hendricks • 3rd

Senior Systems Administrator
55 connections
Featured Skills & Endorsements
Microsoft Exchange · 49



People-Centric Security Analytics

Leverage our *unique* data to 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

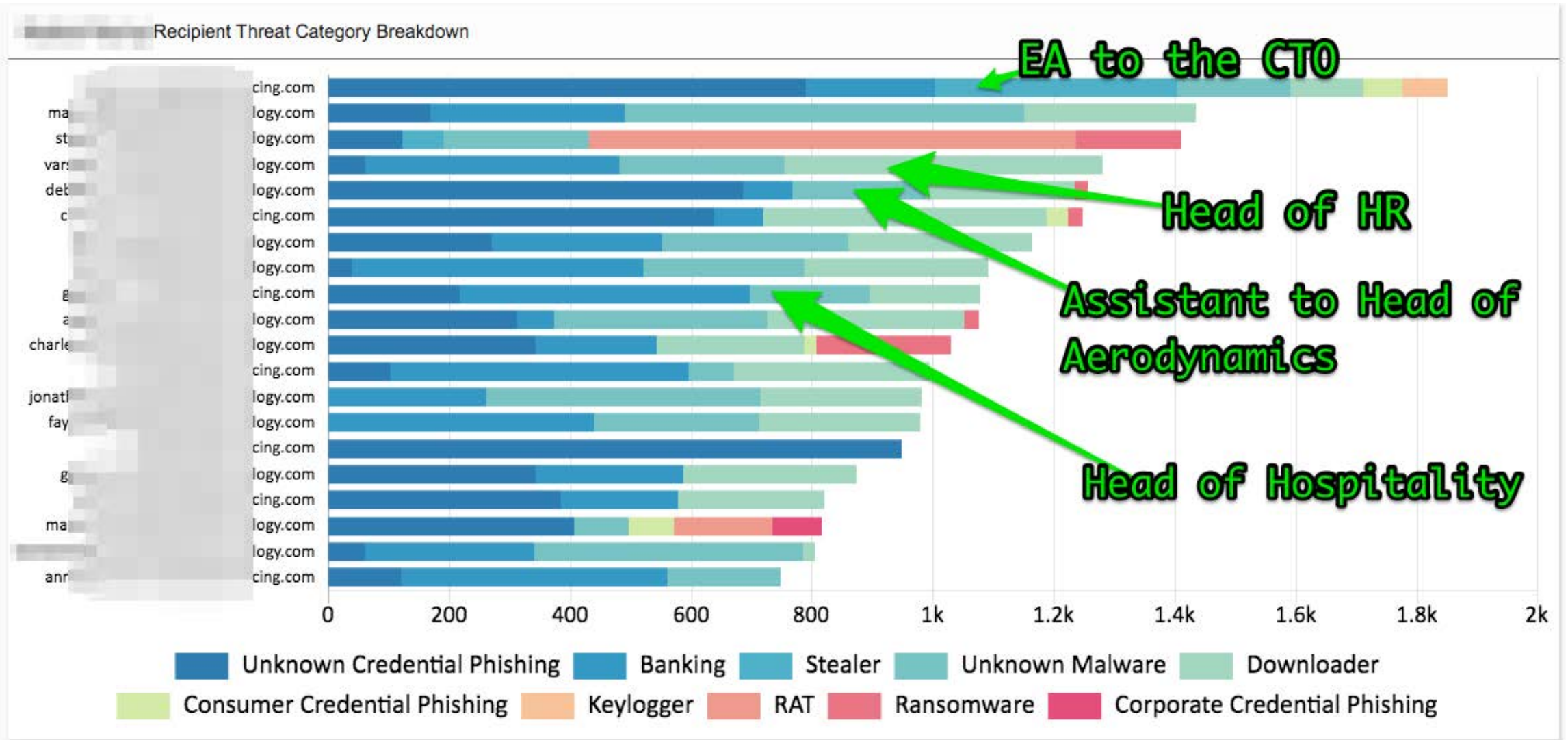


Understand the risk your users face and prioritize the most effective compensating controls



Receive reporting and metrics on the threats your users face

Attack Index Results



Q&A



A man and a woman are in a meeting room. The woman is pointing at a whiteboard covered in sticky notes. The man is holding a tablet. The word "proofpoint" is overlaid in the center.

proofpoint®