HUNTING THREAT ACTORS WITH TLS CERTIFICATES

MARK PARSONS

DEVELOPER/THREAT ANALYST

KING AND UNION

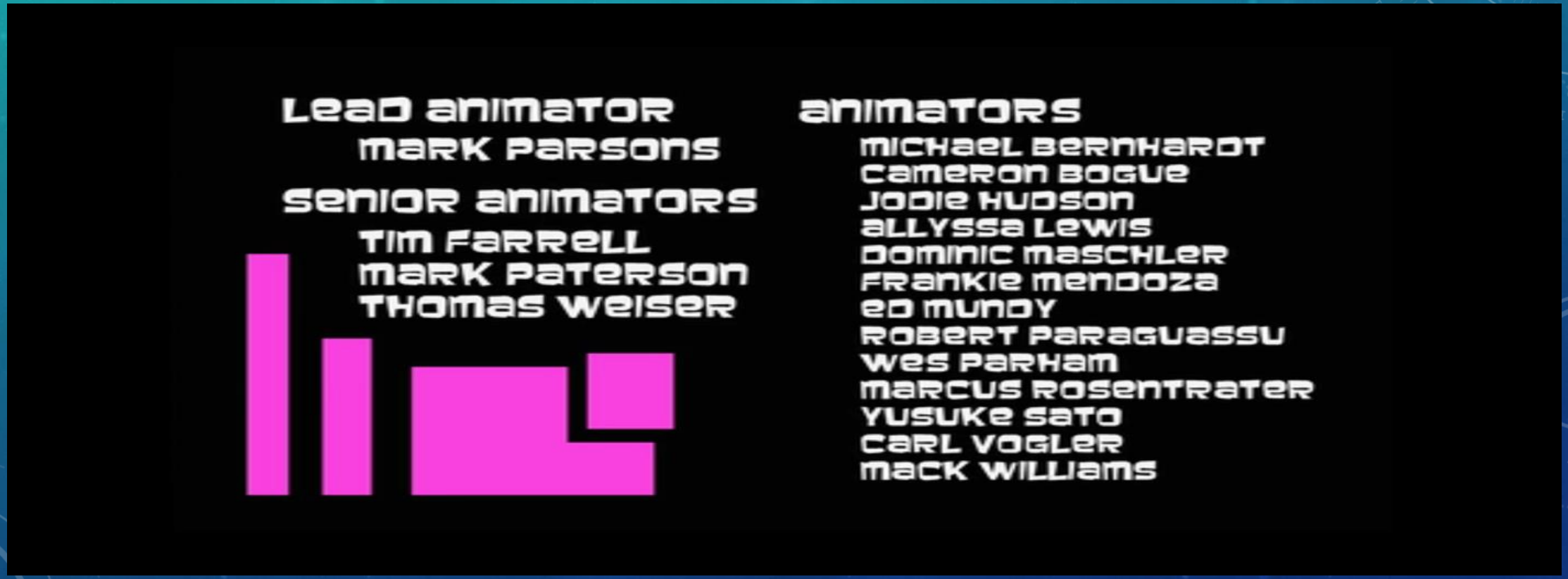
MARK@KINGANDUNION.COM

WHO AM I ?

- Formerly - incident responder / network defender
- Currently – developer / threat analyst

WHO I AM NOT?

Animator - Archer



ONE DIRECTION FAN FICTION?

ANGELA WATERCUTTER CULTURE 05.31.12 4:07 PM

VIRAL VIDEO: *ARCHER* ANIMATOR MAKES BEST ONE DIRECTION FANFIC EVER

QUICK REVIEW

Traditional methods of infrastructure hunting/pivoting using network related resources

PASSIVE DNS (PDNS)

- Historical mappings of domains to IP addresses, and IP addresses to domains
- Some sources of PDNS
  - Farsight
  - Mnemonic
  - RiskIQ/PassiveTotal
  - OpenDNS

WHOIS TRACKING

- Using domain registrant information to look for other potentially related domains
- Sources of trackable WHOIS information
  - DomainTools
  - Whoisology
  - RiskIQ/PassiveTotal
  - DomainIQ
  - Domain Big Data

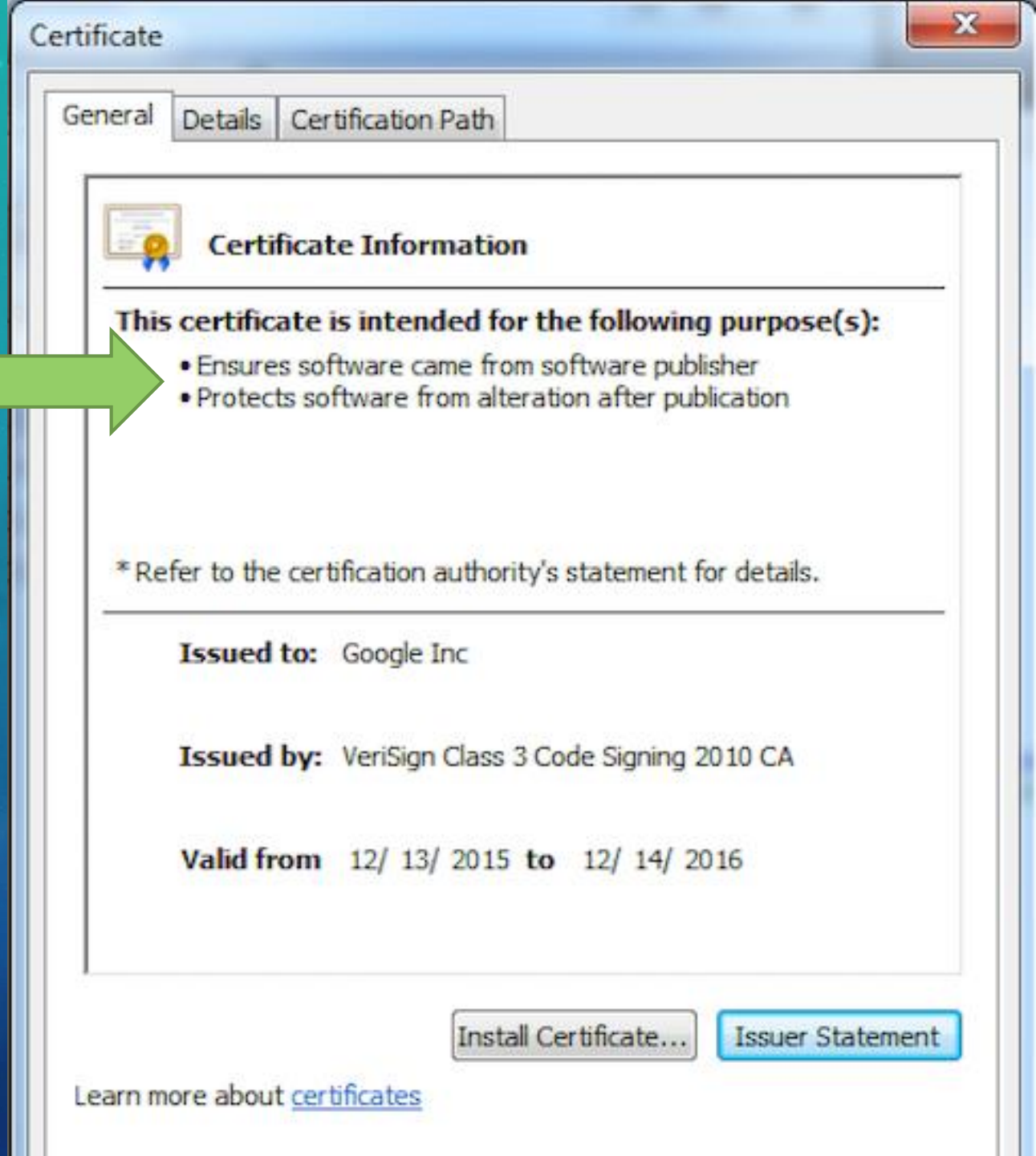
WHAT ELSE MIGHT PROVIDE TRACKABLE DATA THAT HELPS IN INFRASTRUCTURE HUNTING?

THAT IS RIGHT TLS CERTIFICATES!!!

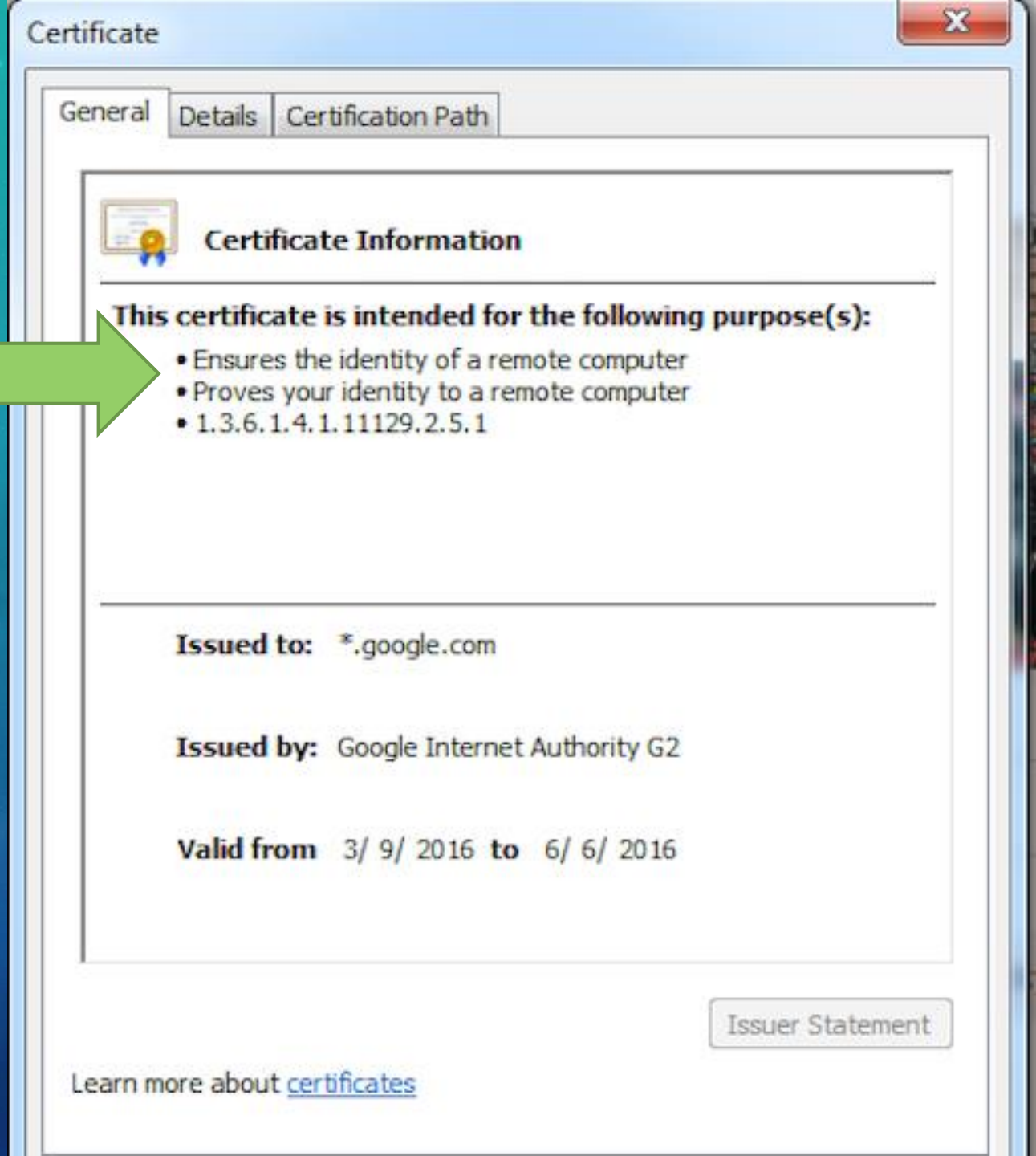
QUICK CAVEAT

Code signing certificate != TLS certificate

CODE SIGNING CERTIFICATE



TLS CERTIFICATE



TLS HUNTING BASICS

Quick tips to help you get started

WHERE TO START

- IP to certificate
- Certificate to IP

IP TO CERTIFICATE

What certificates have been seen on 185.12.44.51?

CERTIFICATE TO IP

What IP addresses has a1833c32d5f61d6ef9d1bb0133585112069d770e been seen on?

BASIC THINGS TO CONSIDER

BEGINNING CONSIDERATIONS

- Do you have malware using this TLS certificate?
- How many other IP addresses are seen using that certificate?

TIME FRAME CONSIDERATIONS

- What time frame was a certificate seen on a suspect IP address
- Expiration dates of the certificate
  - Not Before
  - Not After

CERTIFICATE ISSUER CONSIDERATIONS

- Self Signed
- Free Certificate
- Paid Certificate

NETWORK DEFENSE

IDS MONITORING – TLS FINGERPRINTS

- Suricata
- Bro
- Snort 3 – external package needed

AUTOMATE TRACKING OF TLS CERTIFICATES

- PassiveTotal Monitoring
- Censys.io API script
- Your own local sonar or censys.io datastore
- Combination of all of these
- Create script(s) to put new IP addresses or certificates found into monitoring or blocks as needed for your environment

TLS CERTIFICATES YOU SAY? WHERE DO YOU START?

YOU NEED SOME DATA

IF YOU DON'T WANT TO SCAN ALL THE THINGS

- You could do any of the following:
  - Ingest scans.io sonar SSL scans
  - Use censys.io
  - Use PassiveTotal

SCANS.IO SONAR SSL SCANS

- Only on TCP:443
- Raw data going back to 10/30/2013
- Easily consumable
- Updated weekly
- Incremental in nature
  - certs.gz - Only new sha1s and base64 raw certificate seen that week
  - hosts.gz - SHA1 and host for all hosts seen
- No public search interface
- Is weekly frequent enough ?

CENSYS.IO

- TLS on TCP:25, 110, 143, 443, 993, 995
- Easy to use search interface
- API Access
- Frequent Updates
- All or nothing in nature
  - If there is a delta between scans
  - Old scan data is not in main search interface
  - Old scan data is available in json format
  - Old scan data is available via query interface

PASSIVETOTAL

- Merge traditional hunting with new methods
- Aggregates multiple passive DNS sources
- Provides WHOIS data
- Provides references to OpenSource reporting
- Also has TLS certificates

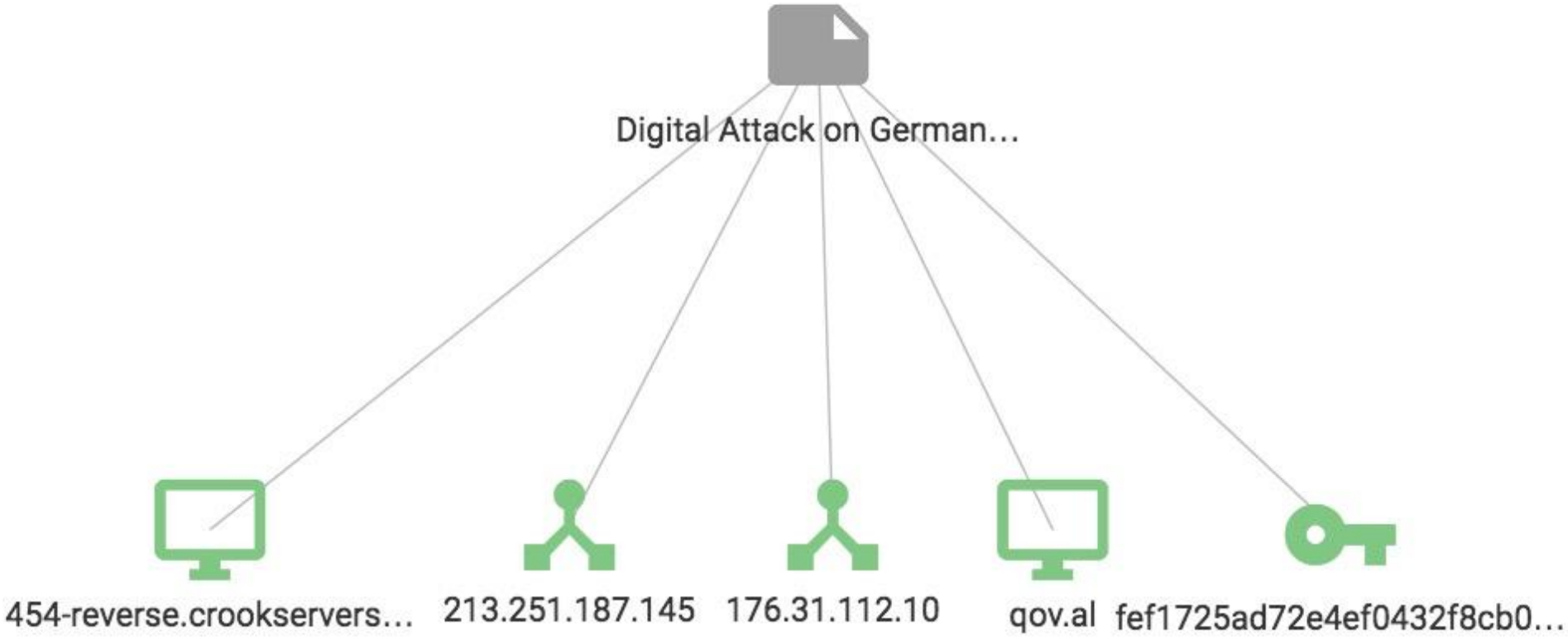
NOW THAT WE HAVE COVERED THE BASICS LETS GO HUNTING


FANCY BEAR
IS SO HOT RIGHT NOW
imgflip.com

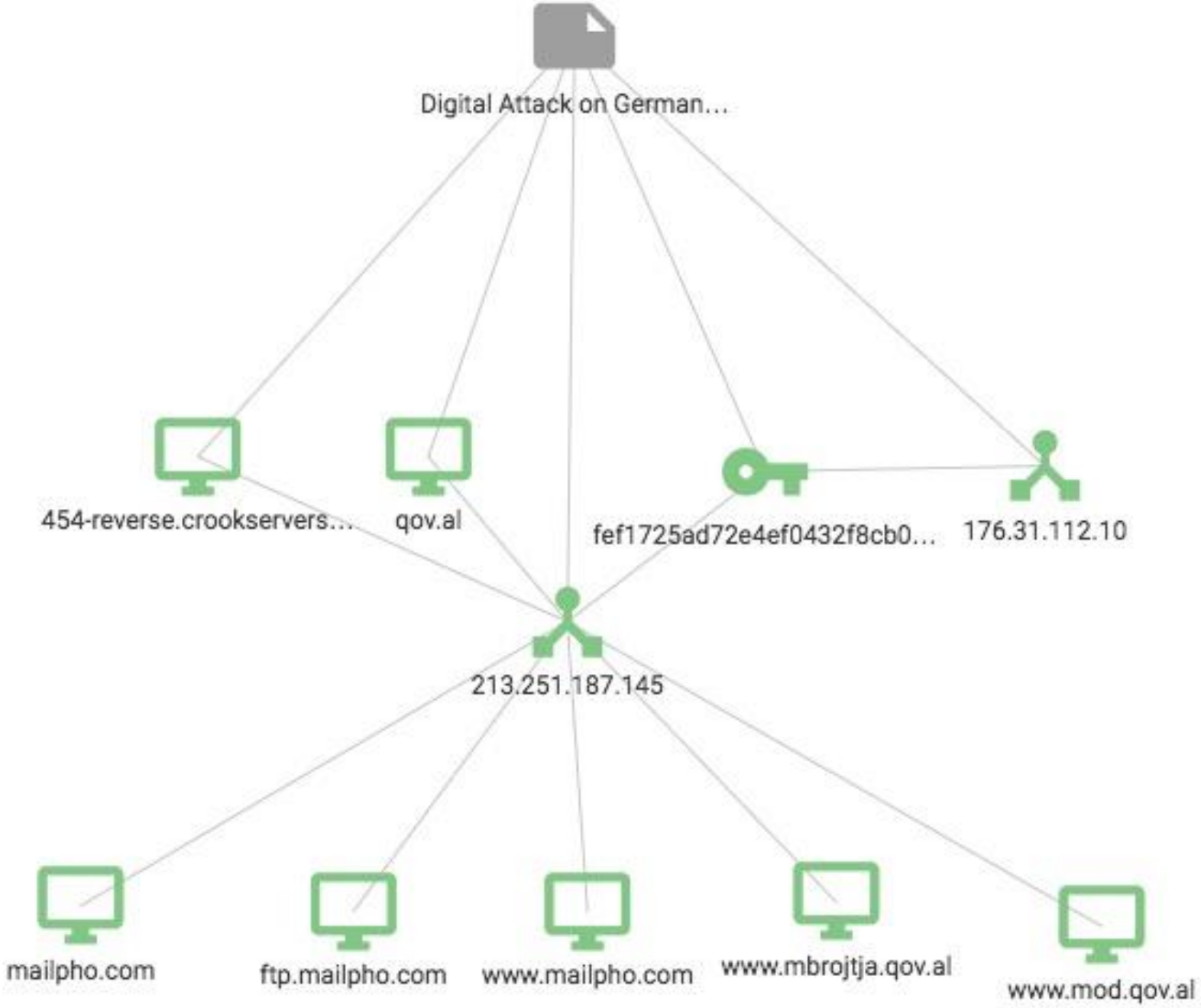
APT 28 / XTUNNEL

- Netzpolotik - Digital Attack on German Parliament
- CrowdStrike – Bears in the Midst
- ESET – Lifting the lid on Sednit

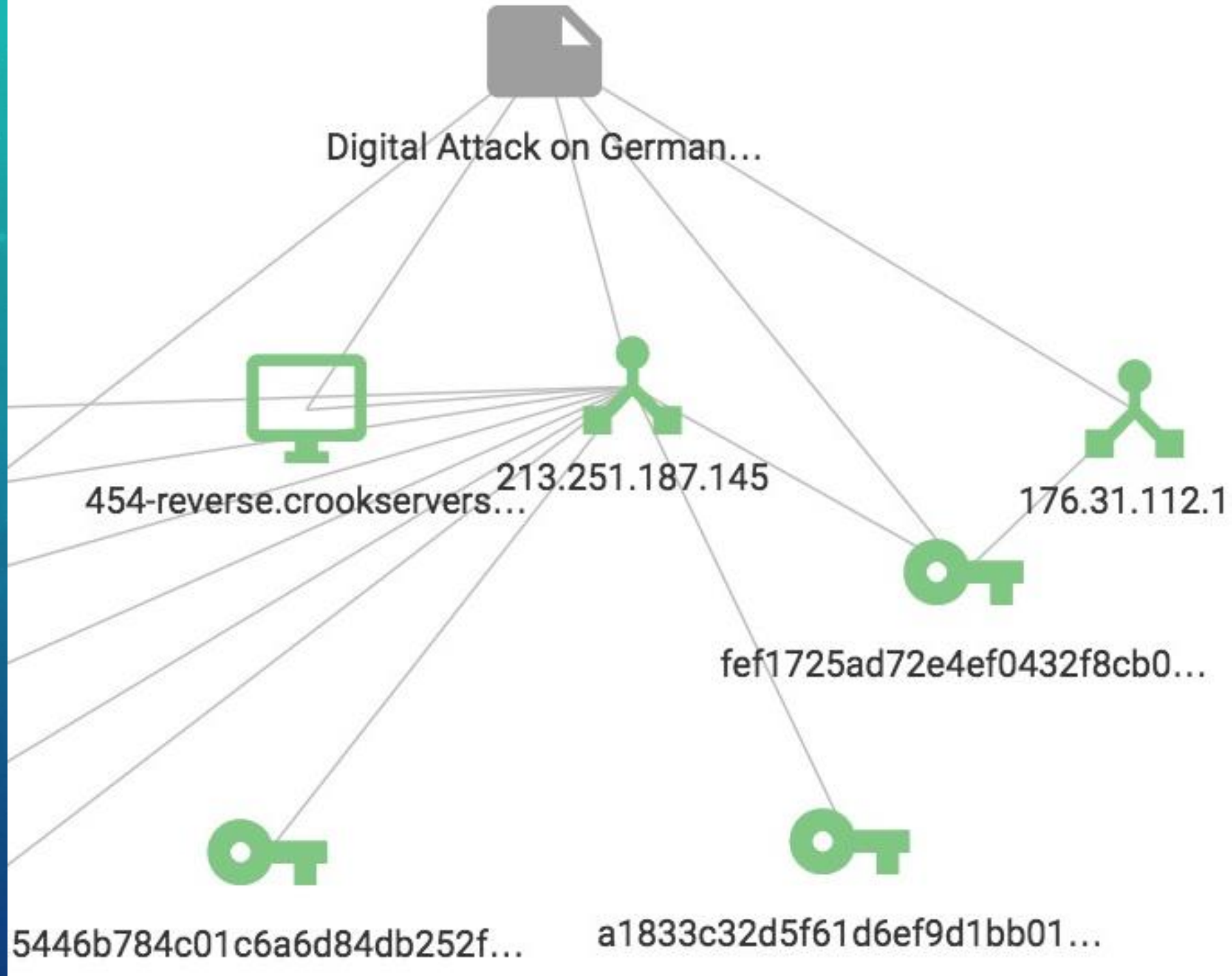
STARTING WITH NETZPOLOTIK REPORT



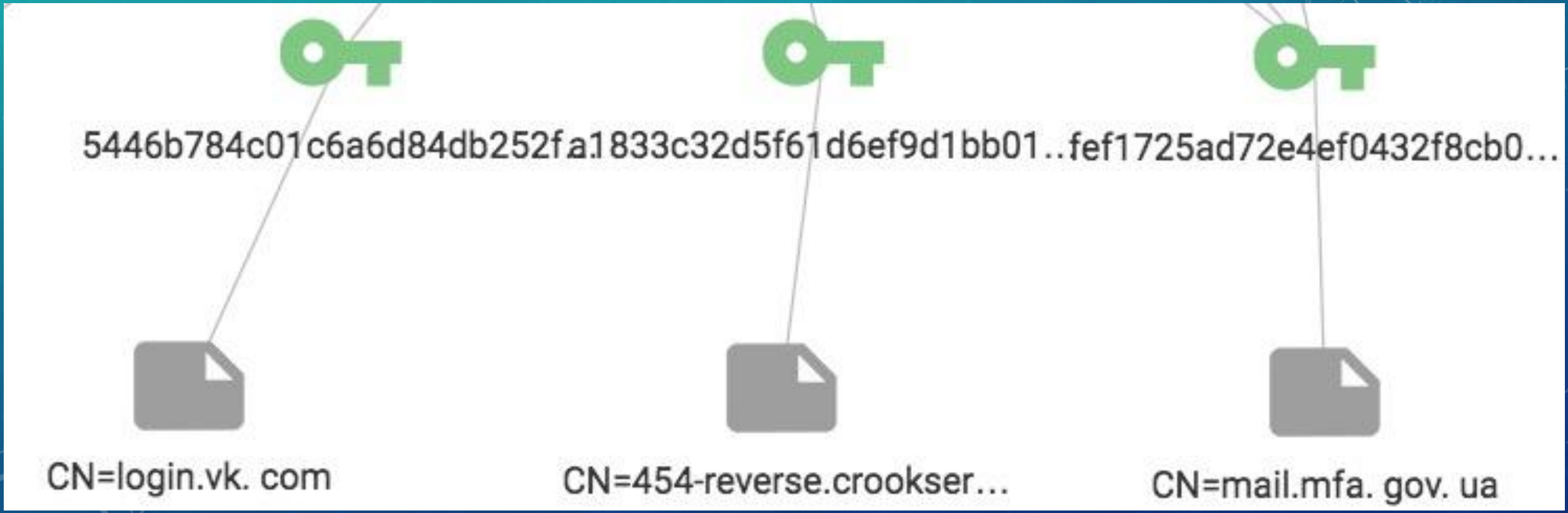
TRADITIONAL PASSIVE DNS PIVOTS



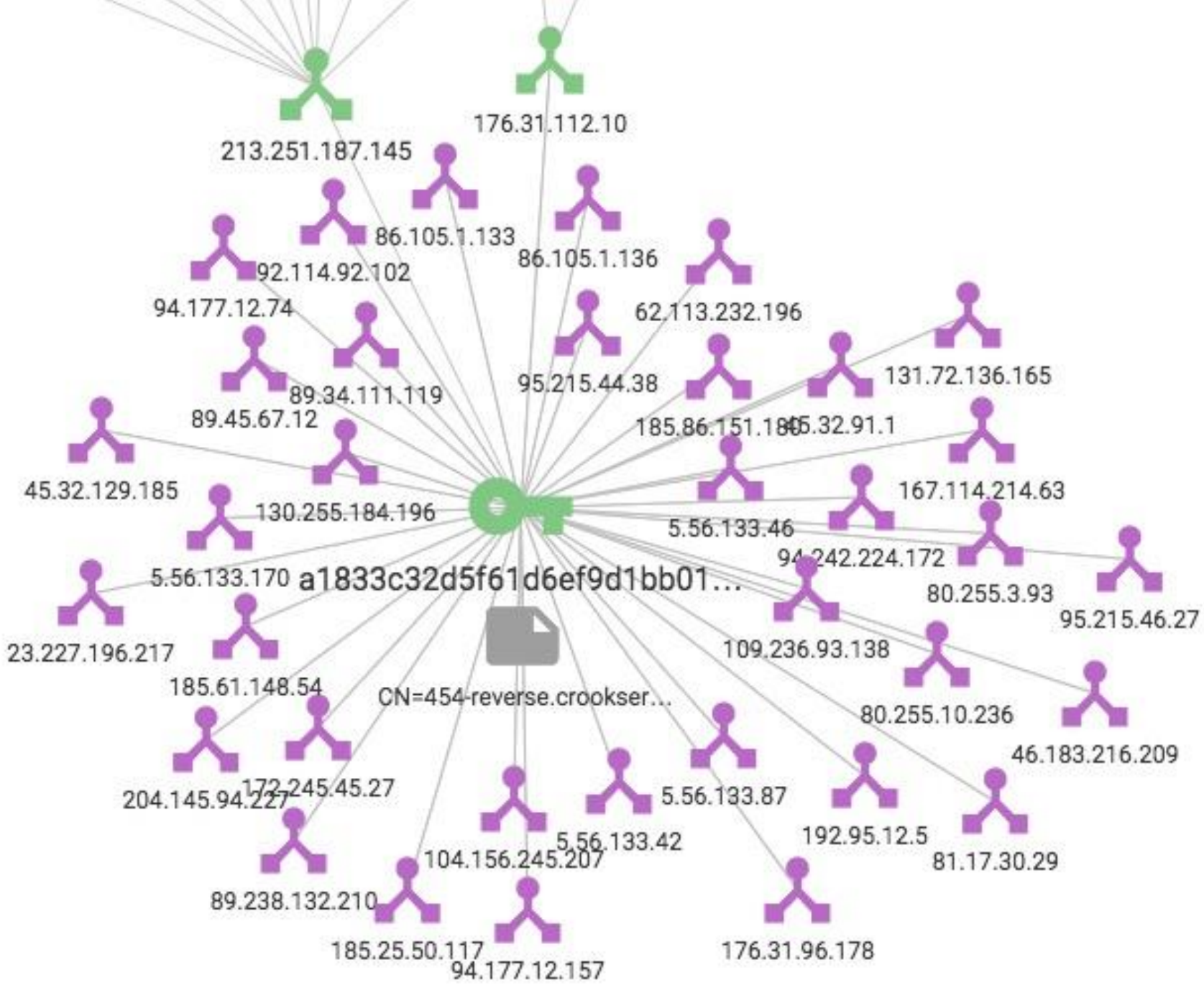
TLS CERTIFICATE PIVOT ON INITIAL IP

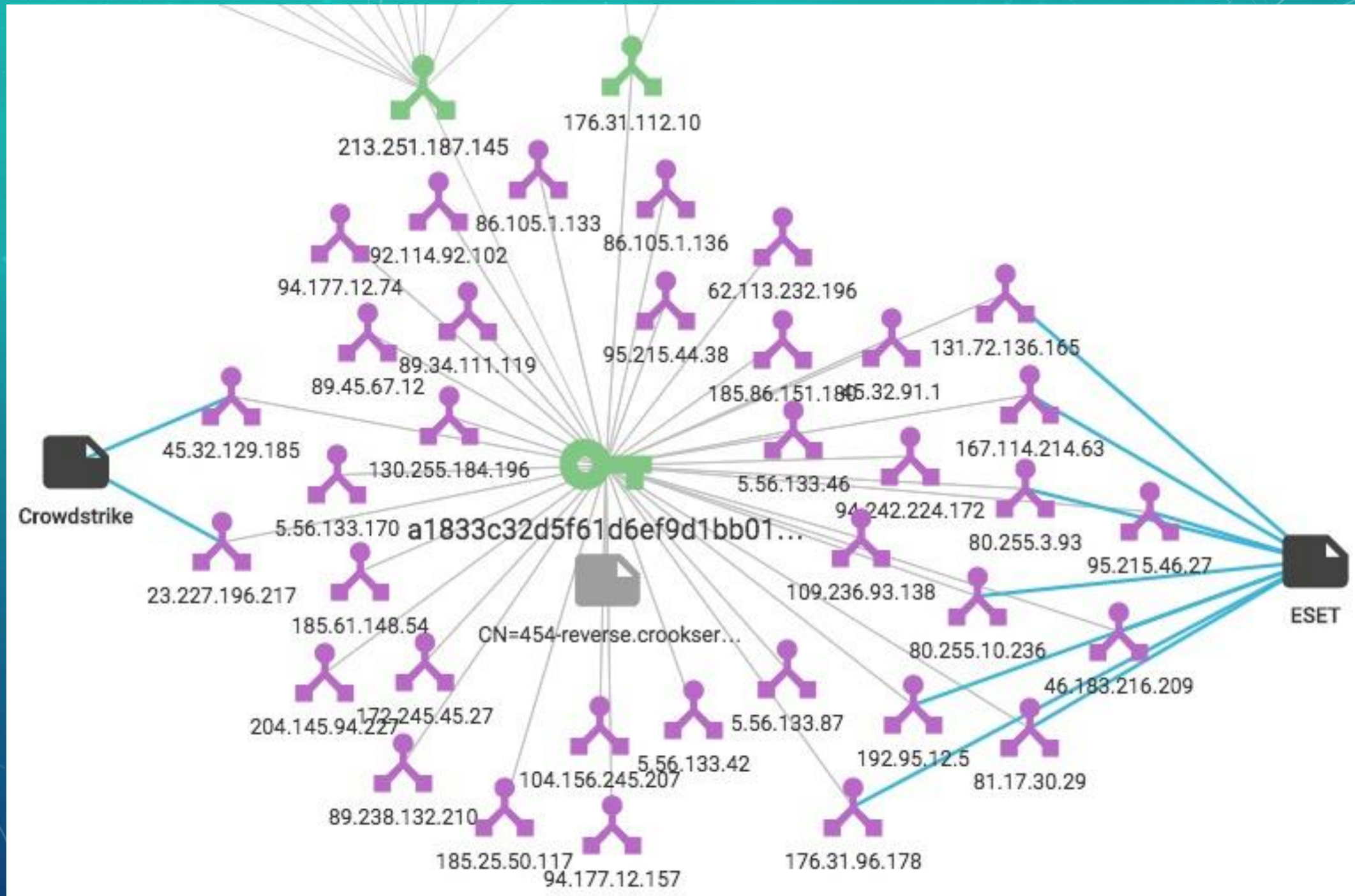


LET'S TAKE A CLOSER LOOK AT THE CERTIFICATES



PIVOT ON 454-CROOKSERVER CERTIFICATE




213.251.187.145
176.31.112.10
86.105.1.133
86.105.1.136
92.114.92.102
94.177.12.74
62.113.232.196
89.34.111.119
95.215.44.38
131.72.136.165
89.45.67.12
185.86.151.180
45.32.91.1
45.32.129.185
167.114.214.63
130.255.184.196
5.56.133.46
Crowdstrike
94.242.224.172
5.56.133.170
a1833c32d5f61d6ef9d1bb01…
80.255.3.93
95.215.46.27
23.227.196.217
109.236.93.138
ESET
185.61.148.54
CN=454-reverse.crookser…
80.255.10.236
46.183.216.209
204.145.94.227
172.245.45.27
5.56.133.87
192.95.12.5
5.56.133.42
81.17.30.29
104.156.245.207
89.238.132.210
185.25.50.117
94.177.12.157
176.31.96.178

TIMELINE

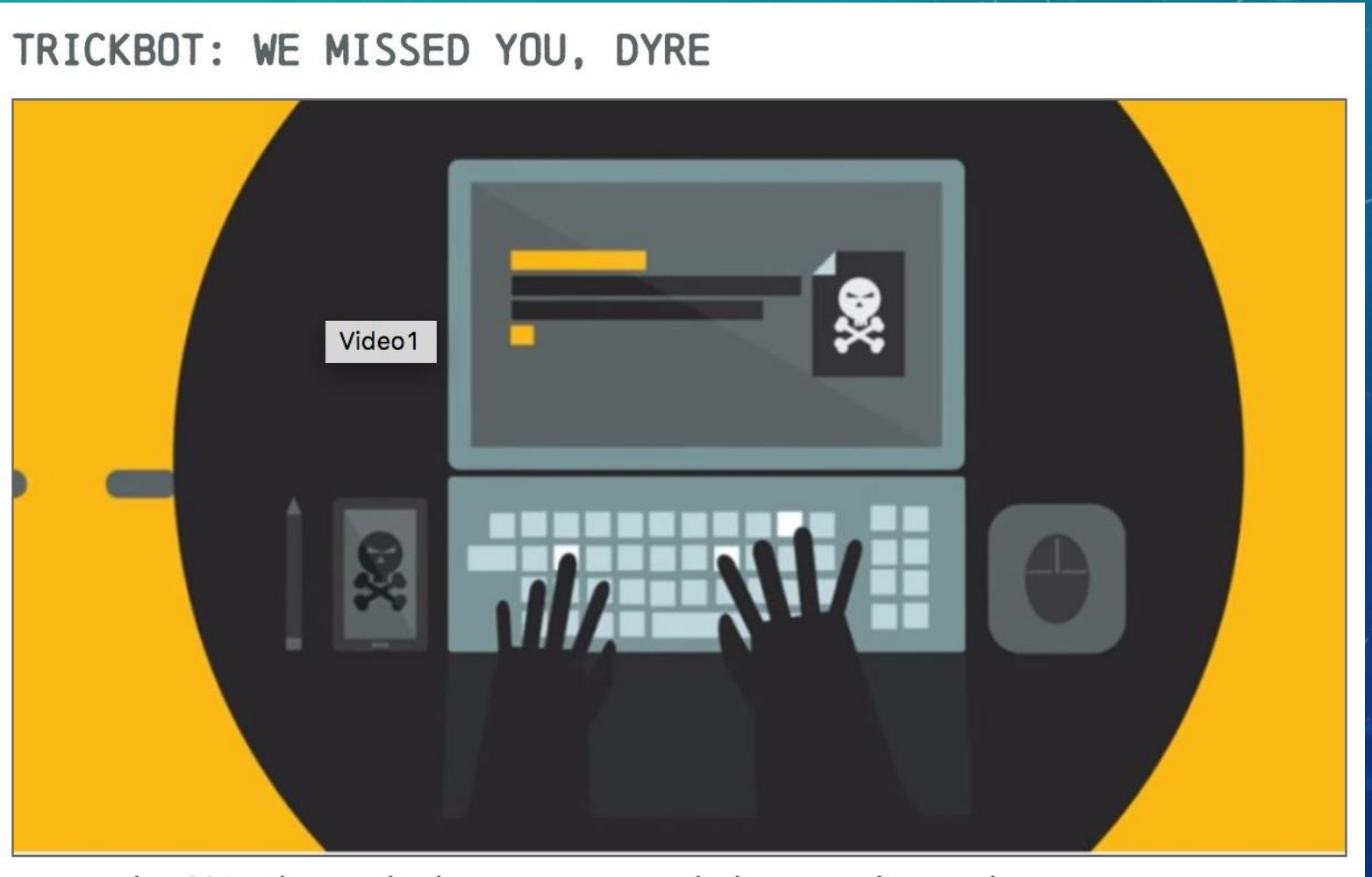

March
April
May
June
July
August
September
October
November
December
January
Februrary
March
April
May
June
July
August
September
October
November
December
January
176.31.112.10
213.251.187.145
5.56.133.170
172.245.45.27
176.31.96.178
95.215.46.27
46.183.216.209
81.17.30.29
94.242.224.172
131.72.136.165
80.255.10.236
167.114.214.63
80.255.3.93
192.95.12.5
204.145.94.227
5.56.133.42
130.255.184.196
45.32.129.185
23.227.196.217
104.156.245.207
45.32.91.1
109.236.93.138
89.45.67.12
5.56.133.46
89.238.132.210
5.56.133.87
185.86.151.180
89.34.111.119
92.114.92.102
62.113.232.196
95.215.44.38
185.25.50.117
86.105.1.133
86.105.1.136
185.61.148.54
94.177.12.74
94.177.12.157
185.86.149.60

APT 28 XTUNNEL SUMMARY

- Initial report 2 domains, 2 IPs, 1 TLS cert
- Traditional pivots reveal 5 interesting domains
- Now have 38 IPs, 7 domains, 3 TLS certs

TRICKBOT

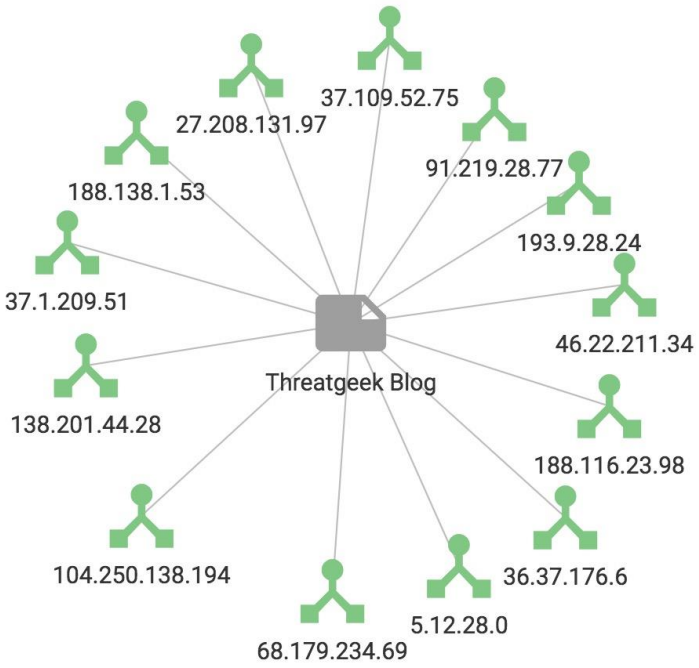
- ThreatGeek – Blog post



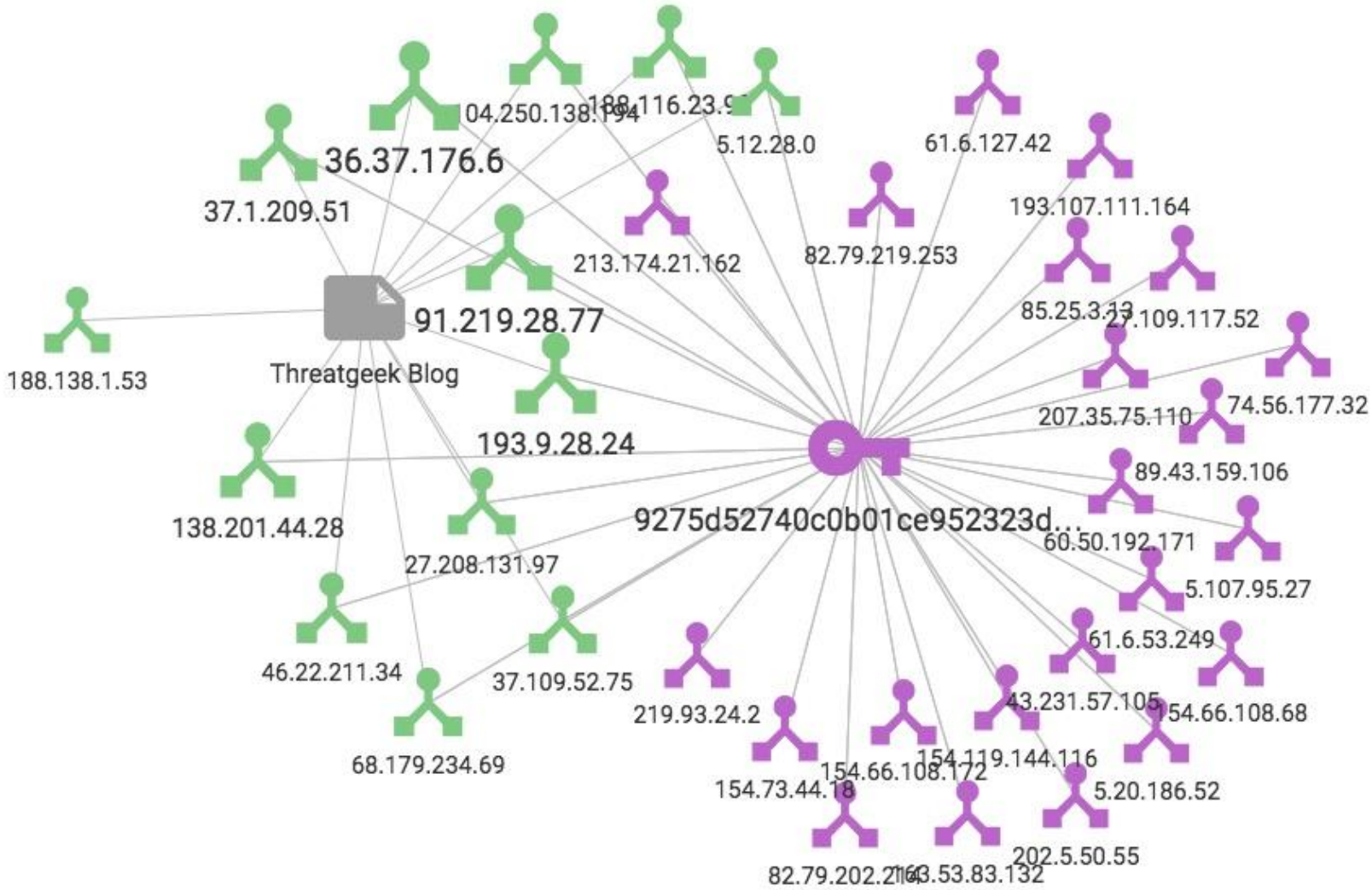
POST HAS SEVERAL ADDRESSES WITH CONNECTIONS TO 443

Trickbot C2s:
188.138.1.53:8082
27.208.131.97:443
37.109.52.75:443
91.219.28.77:443
193.9.28.24:443
37.1.209.51:443
138.201.44.28:443
188.116.23.98:443
104.250.138.194:443
46.22.211.34:443
68.179.234.69:443
5.12.28.0:443
36.37.176.6:443

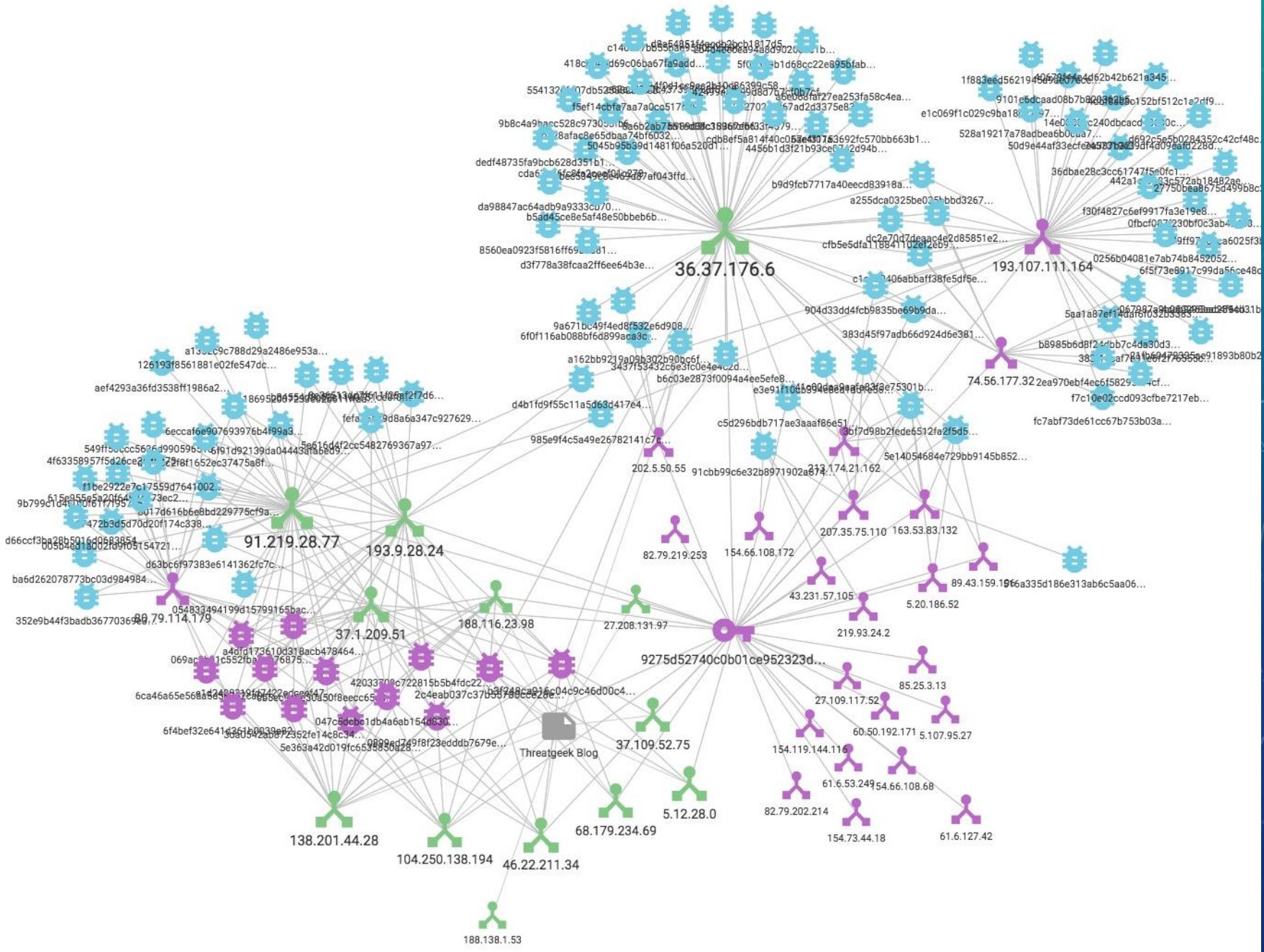
INITIAL INDICATORS



TLS CERTIFICATE PIVOT



MALICIOUS SAMPLES



TRICKBOT SUMMARY

- Initial indicators 13 IP addresses
- All have common TLS certificate
- 22 new IP addresses
- Malware samples show linkages between IP addresses

CONCLUSION

- Continue to look for new ways to monitor and track infrastructure
- Tracking TLS certificates should be added as part of normal infrastructure hunting
- Processing the data can be an initial steep hill but afterwards it is a green pasture

THANKS TO THE FOLLOWING PEOPLE

- Ben Koehl
- James Elliott
- David Westcott

CONTACT INFO

@markpars0ns
github.com/mpars0ns
mark@kingandunion.com

QUESTIONS?