RSAConference™2023
San Francisco | April 24 – 27 | Moscone Center

SESSION ID: HT-R03

Trust Unearned? Evaluating CA Trustworthiness Across 5 Billion Certificates

David J. Bianco
Staff Security Strategist
SURGe by Splunk
@DavidJBianco / @DavidJBianco@infosec.exchange

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™ 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.

The Secret Origins of the CA Trust Project

As a new SURGeon, your first project is an important choice!

I wanted something research-y, but practical. Ideally, something that could benefit from our unlimited Splunk license.

I'd worked with Certificate Transparency before and thought it was neat.

What could I do with ALL THE TLS CERTS ON THE INTERNET?

Source: DALL-E

CA Trust: Is it Truly Earned?

Internet security is built on TLS, which anchors its trust with Root CAs.

OS and browser manufacturers **decide for us** which roots we trust.

- Chrome: 138 trusted roots
- Firefox: 54 trusted roots
- Safari / MacOS: 154 trusted roots

How do we know they are all worthy of our trust? Let's measure!

Splunkvengers, Assemble!

Mikael Bjerkeland
Apps/Sys Engineer

Kelcie Bourne
Security Strategist, SURGe

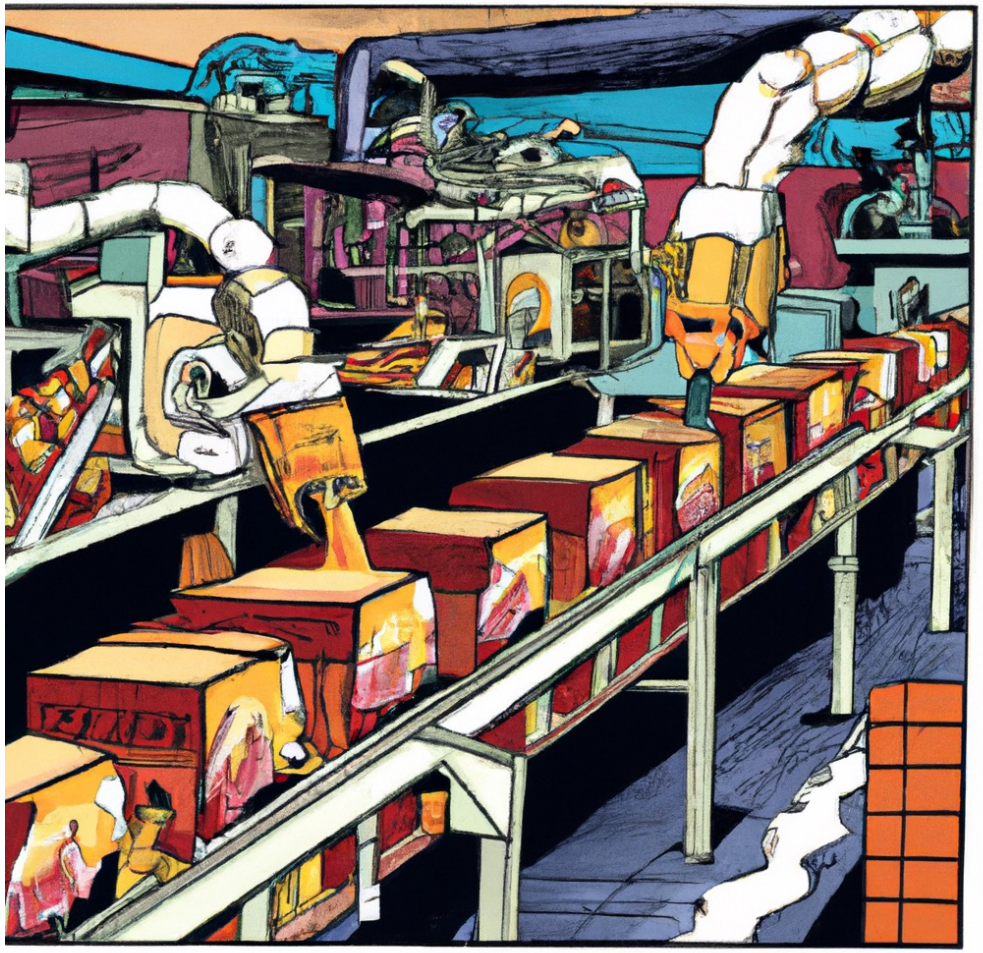
Philipp Drieger
Principal Architect

SURGe by Splunk

Methodology

In theory, this is simple:

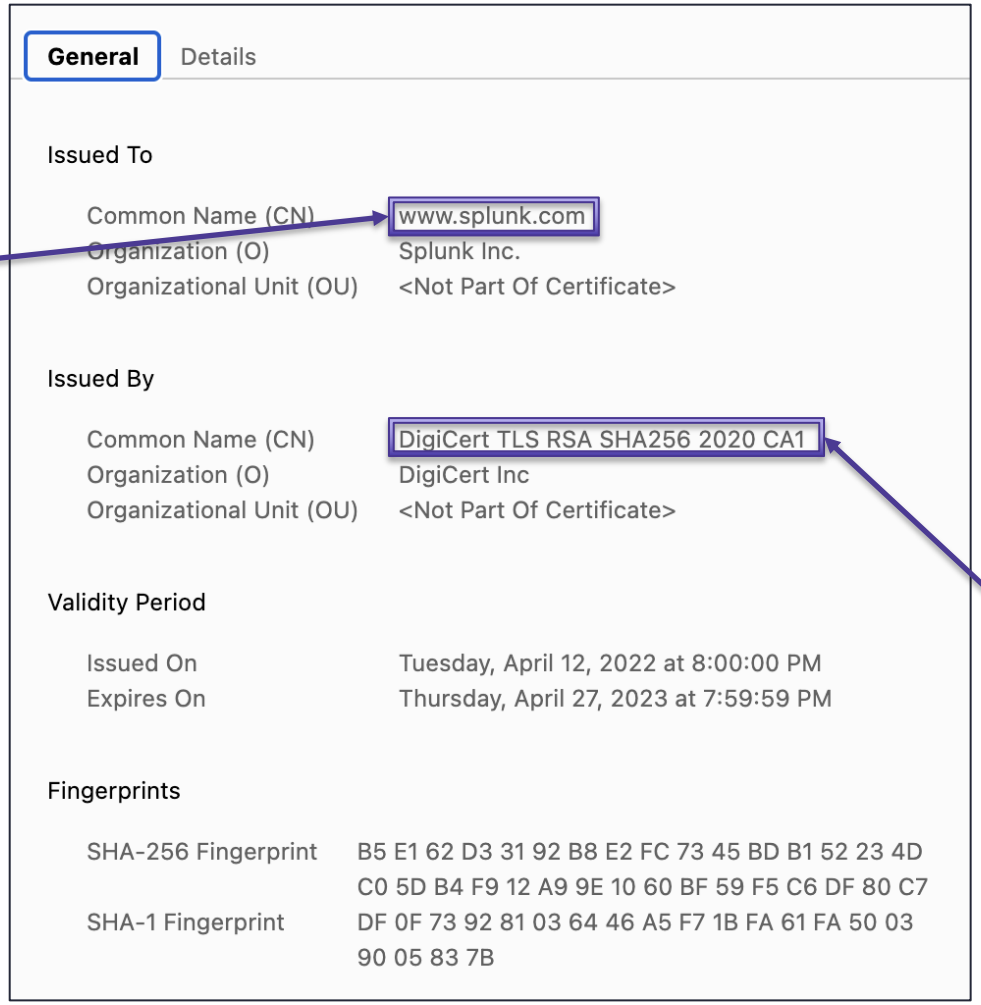
1. Download all TLS certificates on the Internet and load them into Splunk
2. Mark all certificates observed doing Bad Things
3. Calculate the ”worst” and “best” CAs



Source: DALL-E

Certificate Review

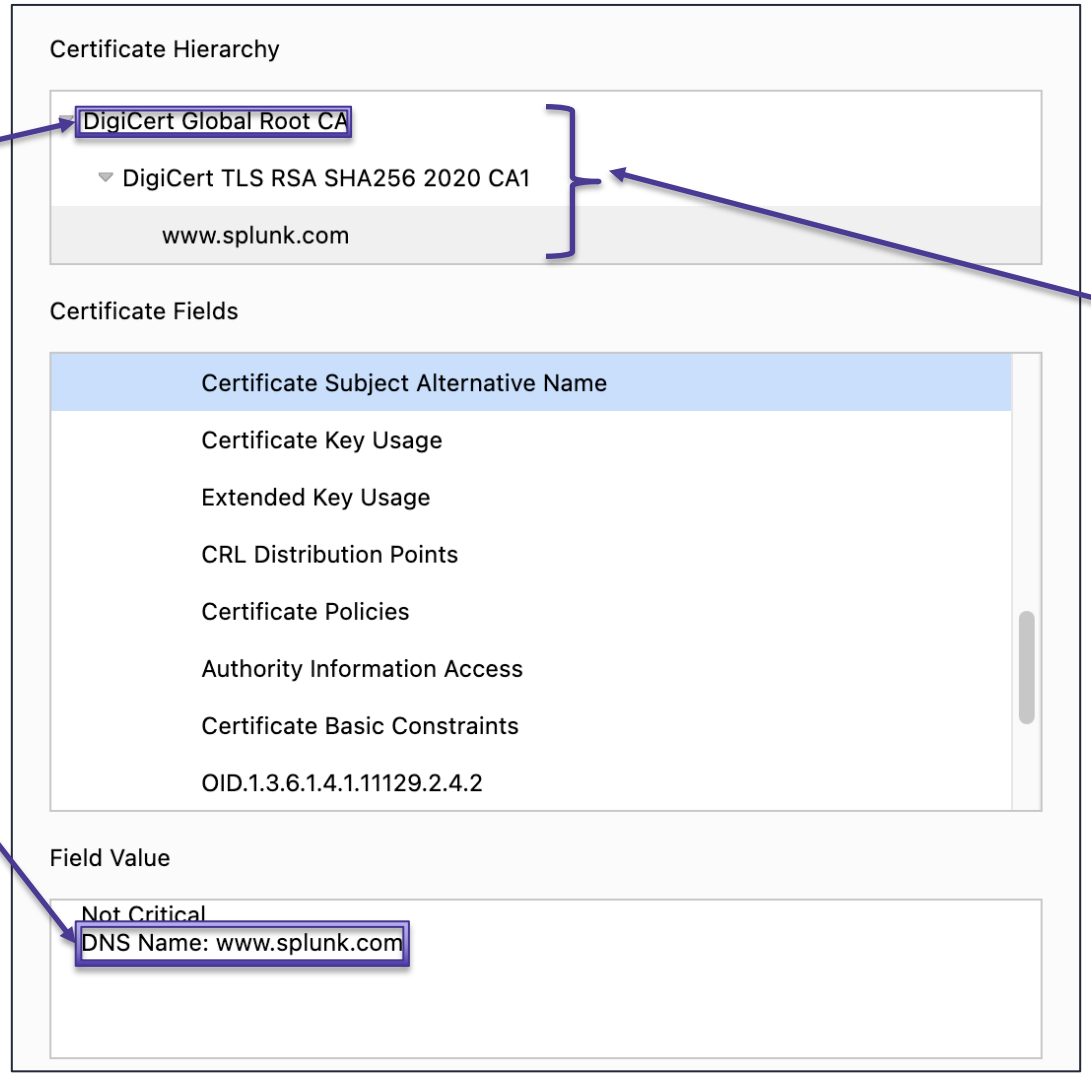
Subject
("Whose cert is this?")



Issuer
("Who created this cert?")

Certificate Review

Root CA
("Who says I can trust it?")



Chain of Trust
("Can I trust this cert?")

SANs
("What other names is this good for?")

Superpower: Certificate Validation

Source: DALL-E

To validate a cert, start by verifying all the signatures in the trust chain.

- If each cert is signed by the cert “above” it, and if you trust the root CA, it’s valid

What if the site owner loses control of their secret key?

- Certificate Revocation Lists (CRLs) or Online Certificate Status Protocol (OCSP)

But what if the CA loses control of its **signing key**?

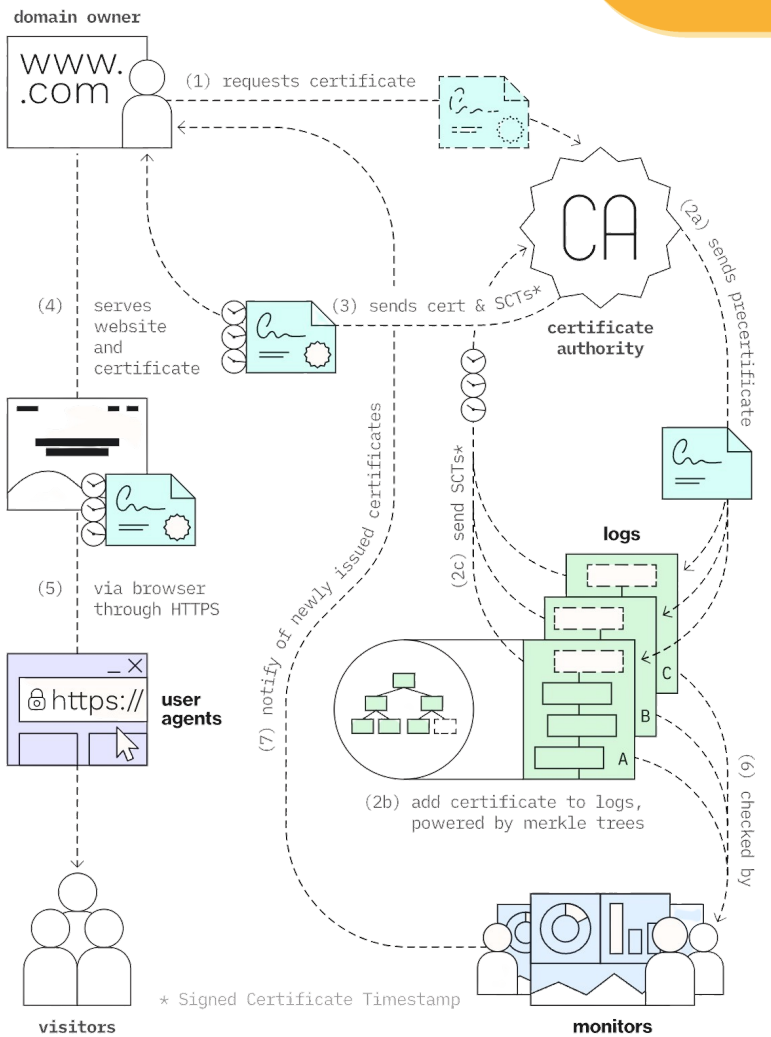
Certificate Transparency Explained Simply

Certificate Transparency (CT) provides public, verifiable records of WebPKI certificate issuance.

Issuers add certificates to Certificate Transparency Logs (CTLs). Anyone can query a CTL for a specific certificate and thus verify the CA issued it.

Chrome began requiring CT for all TLS certificates in April 2018. Most, but not all, major browsers now require CT to validate certificates. Looking at you, Firefox!

CTLs are open to all via a standard API. I used this to download certificates from (mostly) 2021 and 2022.



Source: https://certificate.transparency.dev/howctworks/

Data: Certificates

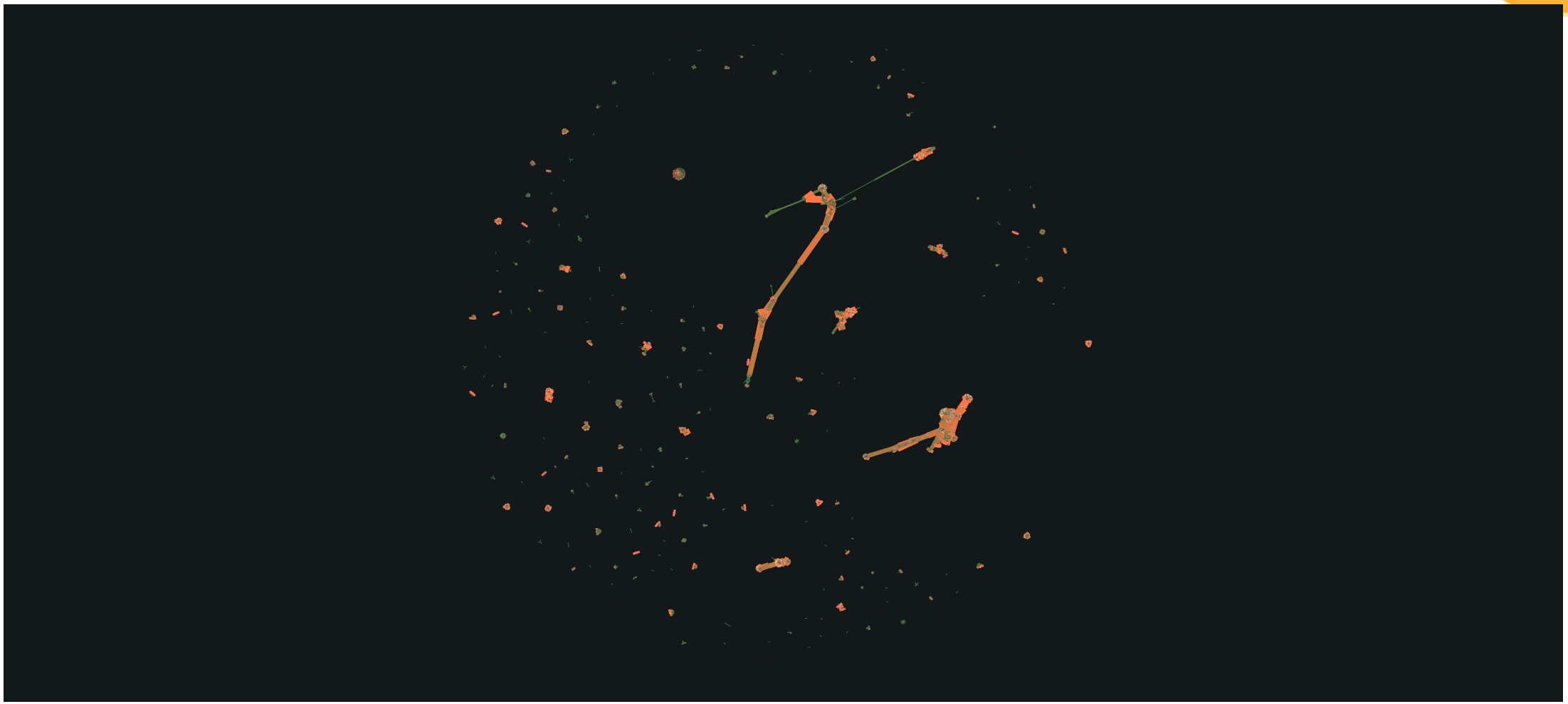
5 Billion
Unique Certificates

497
Root CAs

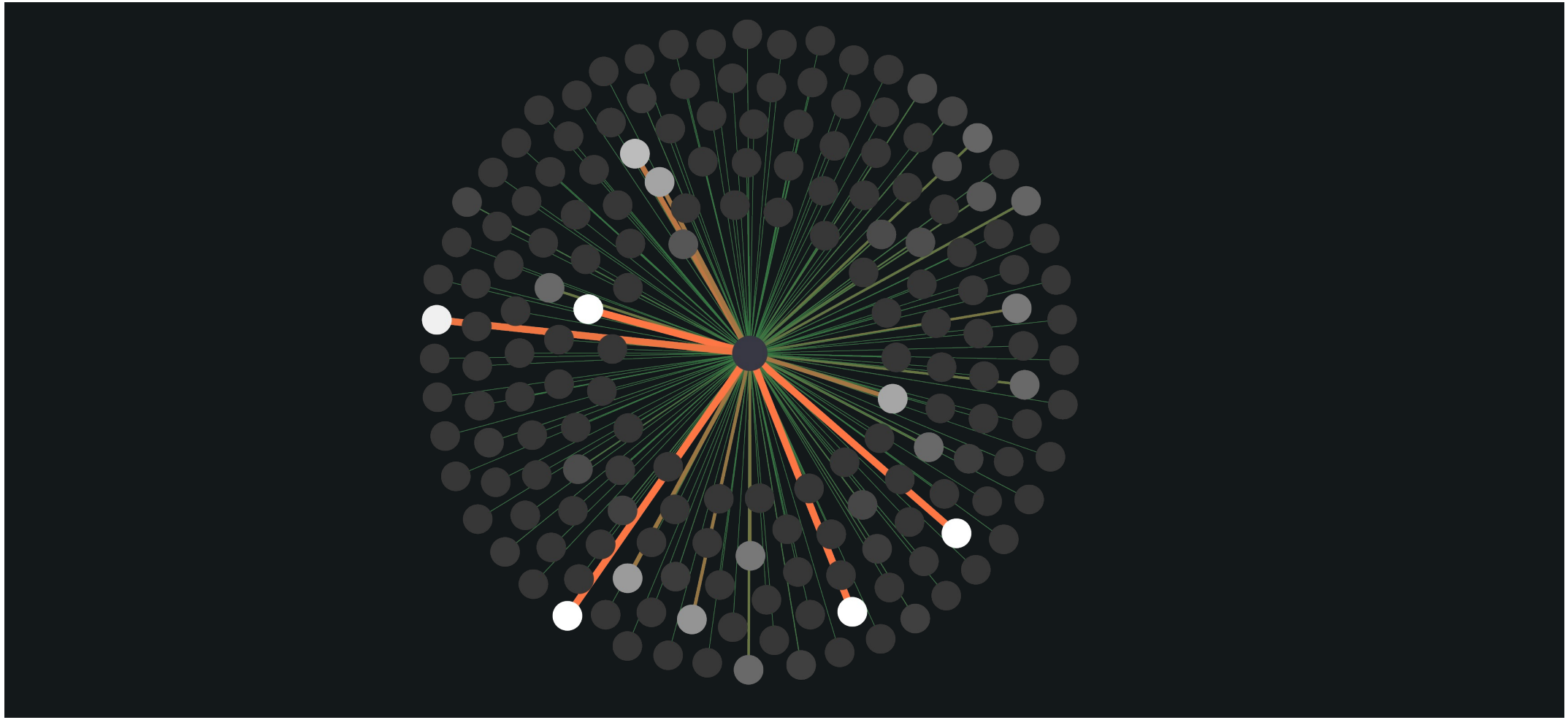
78k
Issuing CAs

15
Certificate Transparency Logs

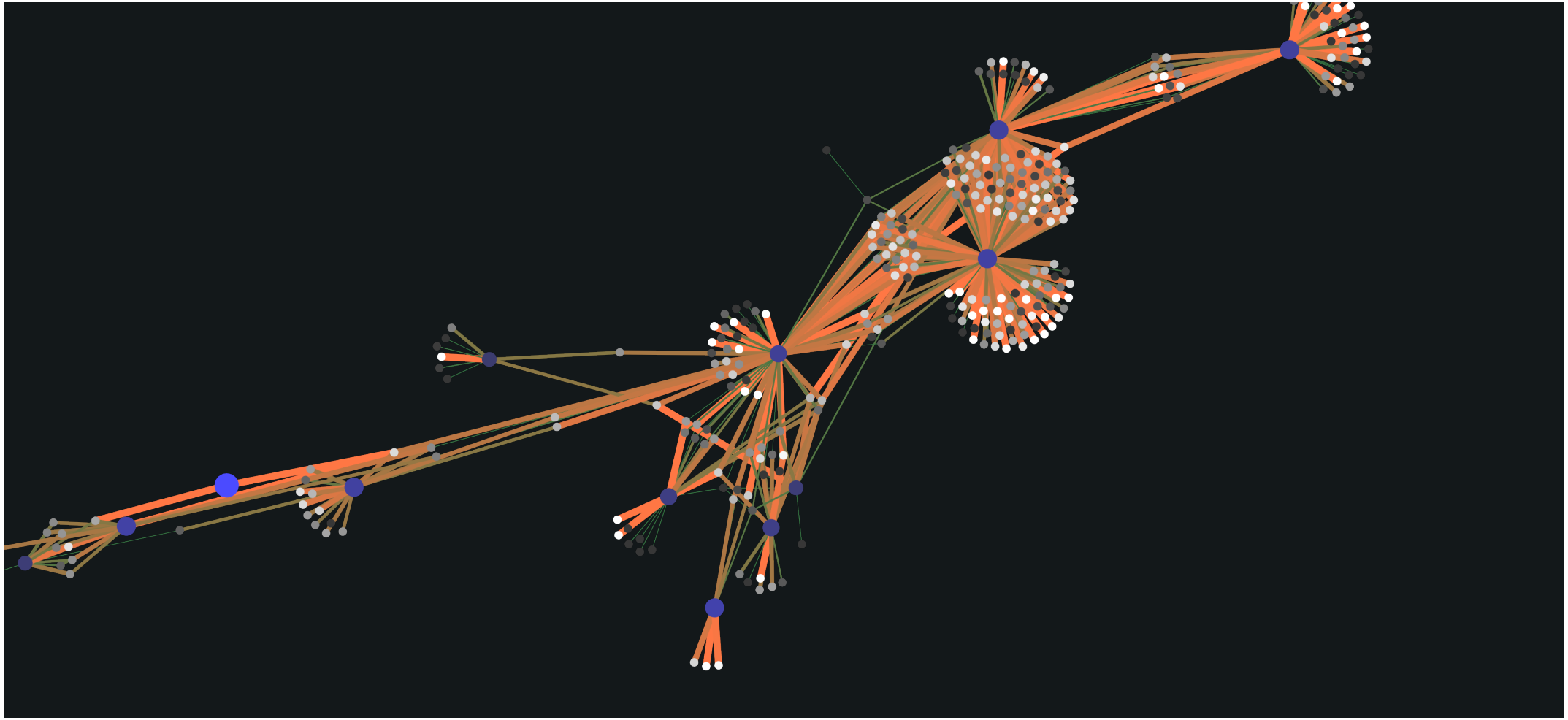
Root CAs and Issuers



Typical Root/Issuer CA Relationships



Highly-Connected Relationships



Data: Intel

185 Million
Malicious Observations

7
Providers

Data: Intel - Big THANK YOUs to the Providers!

DomainTools

GROUP-IB

Paranoids

FIRST™ Improving Security Together

JPCERT CC®

Analysis: Challenges and Limitations

- This was some big “tres commas” data!
  - Needed custom download & parsing tool
  - Ingest was tricky
- Matching intel to certificate subjects isn’t straightforward
- Extreme variation in CA population sizes makes fair comparisons difficult

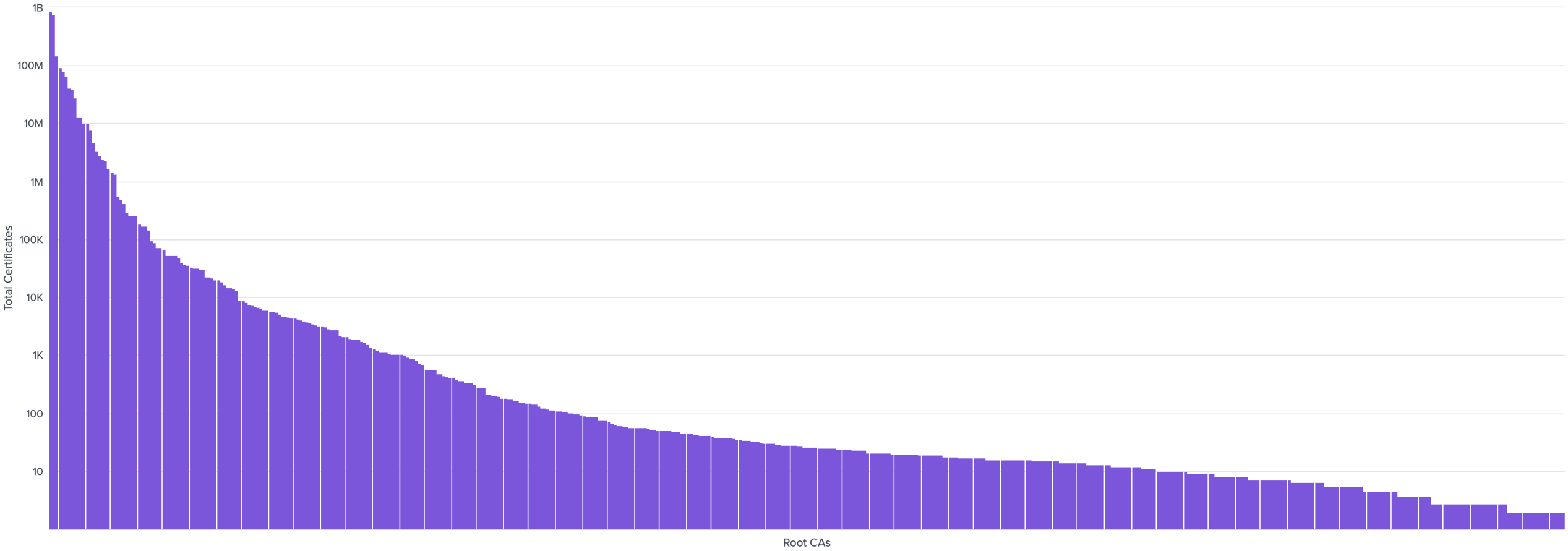
Riskiest Root CAs (Single Pool)

root_ca	total_certs	risky_certs	risk_percent	zscore
/C=US/O=Internet Security Research Group/CN=ISRG Root X2	2	1	50.00	6.310
/C=US/ST=Arizona/L=Scottsdale/O=GoDaddy.com, Inc./CN=Go Daddy Root Certificate Authority - G2	10288790	3495095	33.97	4.132
/C=IN/OU=emSign PKI/O=eMudhra Technologies Limited/CN=emSign Root CA - G1	1932	553	28.62	3.405
/C=US/ST=New Jersey/L=Jersey City/O=The USERTRUST Network/CN=USERTrust RSA Certification Authority	65198821	16528521	25.35	2.961
/C=US/O=Google Trust Services LLC/CN=GTS Root R1	5215	1101	21.11	2.385
/C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate Services	1429856	283522	19.83	2.211
/C=TR/L=Ankara/O=E-Tu\xC4\x9Fra EBG Bili\xC5\x9Fim Teknolojileri ve Hizmetleri A.\xC5\x9E./OU=E-Tugra Sertifikasyon Merkezi/CN=E-Tugra Certification Authority	49565	9596	19.36	2.147
/C=PL/O=Unizeto Technologies S.A./OU=Certum Certification Authority/CN=Certum Trusted Network CA	2423281	382727	15.79	1.662
/C=US/O=Internet Security Research Group/CN=ISRG Root X1	861665191	125180925	14.53	1.490
/C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO RSA Certification Authority	93476404	13359082	14.29	1.458

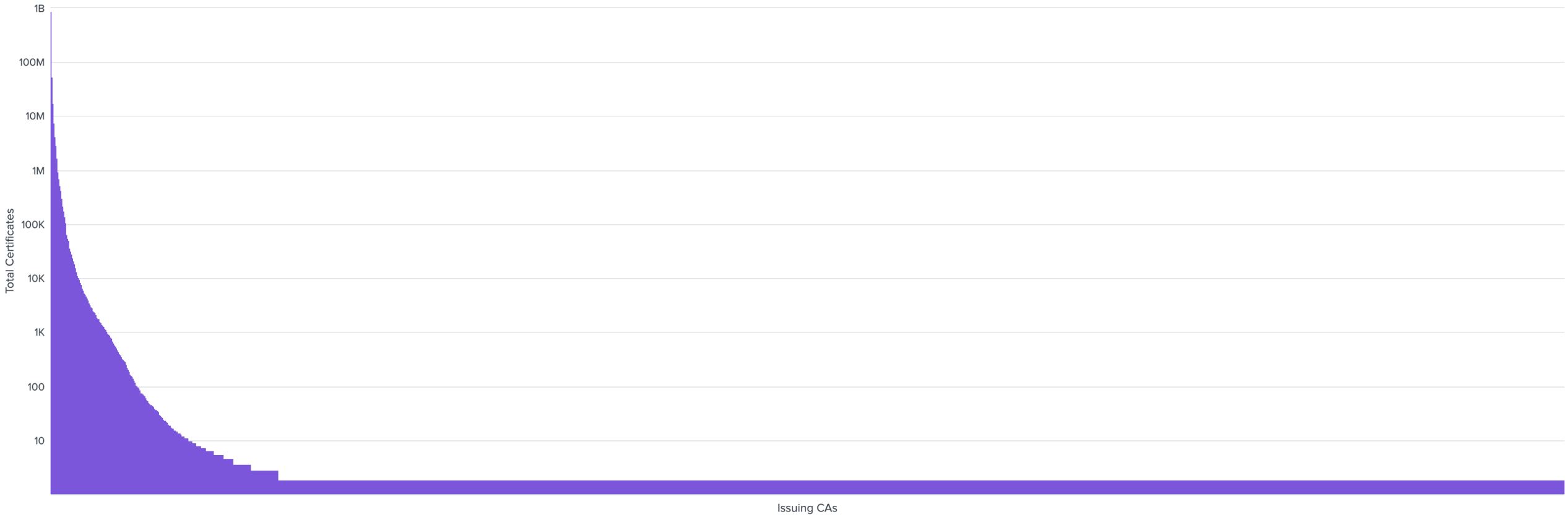
Riskiest Issuing CAs (Single Pool)

issuer	total_certs	risky_certs	risk_percent	zscore
/C=AE/O=Etisalat/OU=Etisalat eBusiness Services/CN=Comtrust Server Certification Authority...	1	1	100.00	8.002
/C=DE/O=EUNETIC GmbH/CN=EuropeanSSL Server CA...	1	1	100.00	8.002
/C=US/O=INTEGRITY Security Services LLC/CN=ISSAuth RSA DV CA...	2	2	100.00	8.002
/C=US/O=TrustOcean Limited/CN=TrustOcean Encryption365 Pro SSL CA...	10611	9756	91.94	7.319
/C=GB/O=Quantum CA Limited/CN=Quantum Secure Site EV TLS RSA R1...	3	2	66.67	5.177
/C=MA/ST=Marrakech/L=Marrakech/O=Genious Communications/CN=GENIOUS ECC Domain Validation Secure Serv...	2	1	50.00	3.764
/C=MA/ST=Marrakech/L=Marrakech/O=Genious Communications/OU=Controlled by Sectigo exclusively for Gen...	4	2	50.00	3.764
/C=SG/ST=Singapore/L=Singapore/O=One Sign Pte. Ltd./CN=OneSignSSL ECC DV Secure Server CA...	2	1	50.00	3.764
/C=US/O=DNEncrypt, Inc/CN=DNEncrypt ECC DV SSL\\/TLS [Run by the Issuer]...	2	1	50.00	3.764
/C=US/O=DigiCert, Inc./CN=DigiCert High Assurance TLS Hybrid ECC SHA256 2020 CA1...	2	1	50.00	3.764

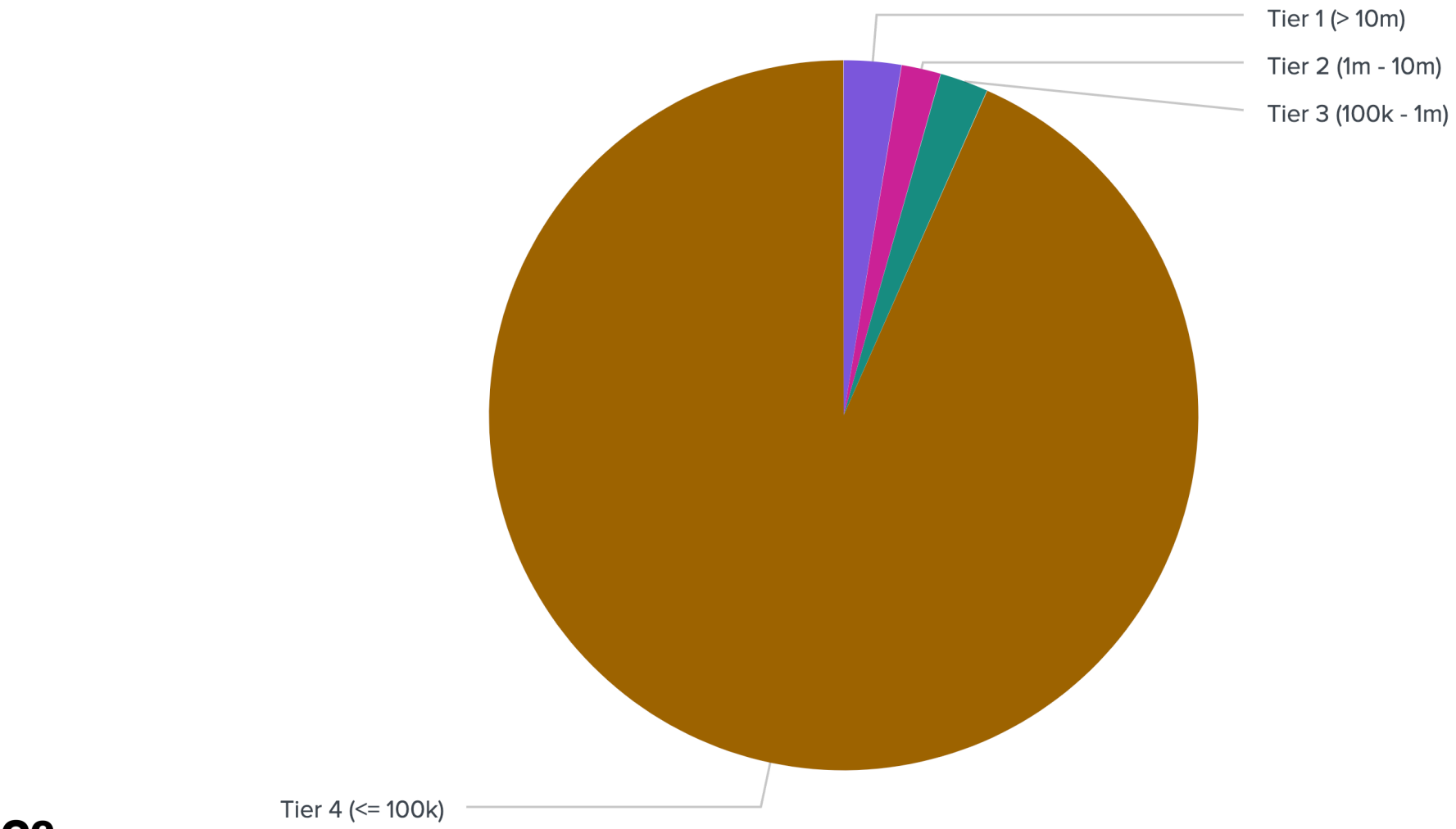
Total Certificates by Root CA



Total Certificates by Issuing CA



Creating Root CA Tiers is Much Fairer!



All Roots – Tier 1

root_ca	total_certs	risky_certs	risk_percent	zscore
/C=US/ST=Arizona/L=Scottsdale/O=GoDaddy.com, Inc./CN=Go Daddy Root Certificate Authority - G2	10288790	3495095	33.97	2.378
/C=US/ST=New Jersey/L=Jersey City/O=The USERTRUST Network/CN=USERTrust RSA Certification Authority	65198821	16528521	25.35	1.536
/C=US/O=Internet Security Research Group/CN=ISRG Root X1	861665191	125180925	14.53	0.478
/C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO RSA Certification Authority	93476404	13359082	14.29	0.454
/C=BE/O=GlobalSign nv-sa/OU=Root CA/CN=GlobalSign Root CA	39008432	3804666	9.75	0.011
/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root CA	80480701	6290176	7.82	-0.178
/C=US/ST=New Jersey/L=Jersey City/O=The USERTRUST Network/CN=USERTrust ECC Certification Authority	12865594	989458	7.69	-0.191
/O=Digital Signature Trust Co./CN=DST Root CA X3	757966004	35051200	4.62	-0.491
/C=US/O=Amazon/CN=Amazon Root CA 1	40908370	1014645	2.48	-0.700
/C=IE/O=Baltimore/OU=CyberTrust/CN=Baltimore CyberTrust Root	149183381	3595497	2.41	-0.707
/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root G2	27664638	507246	1.83	-0.764
/C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO ECC Certification Authority	12940927	60687	0.47	-0.897
/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert High Assurance EV Root CA	10092368	14167	0.14	-0.929

All Roots – Tier 2

root_ca	total_certs	risky_certs	risk_percent	zscore
/C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate Services	1429856	283522	19.83	1.932
/C=PL/O=Unizeto Technologies S.A./OU=Certum Certification Authority/CN=Certum Trusted Network CA	2423281	382727	15.79	1.413
/C=US/ST=Arizona/L=Scottsdale/O=Starfield Technologies, Inc./CN=Starfield Root Certificate Authority - G2	1733430	120647	6.96	0.279
/OU=GlobalSign Root CA - R3/O=GlobalSign/CN=GlobalSign	4665284	12805	0.27	-0.581
/C=US/O=Entrust, Inc./OU=See www.entrust.net\/legal-terms/OU=(c) 2009 Entrust, Inc. - for authorized use only/CN=Entrust Root Certification Authority - G2	2339445	4742	0.20	-0.590
/OU=GlobalSign Root CA - R2/O=GlobalSign/CN=GlobalSign	7688491	3624	0.05	-0.609
/C=BM/O=QuoVadis Limited/CN=QuoVadis Root CA 2	1338331	241	0.02	-0.613
/C=IT/L=Milan/O=Actalis S.p.A.\/03358520967/CN=Actalis Authentication Root CA	2829160	389	0.01	-0.615
/C=US/O=IdenTrust/CN=IdenTrust Commercial Root CA 1	3443366	98	0.00	-0.616

All Roots – Tier 3

root_ca	total_certs	risky_certs	risk_percent	zscore
/C=NO/O=Buypass AS-983163327/CN=Buypass Class 2 Root CA	168955	20584	12.18	2.11
/C=US/ST=Texas/L=Houston/O=SSL Corporation/CN=SSL.com Root Certification Authority RSA	260983	26830	10.28	1.68
/C=JP/O=SECOM Trust Systems CO.,LTD./OU=Security Communication RootCA2	480965	21366	4.44	0.369
/C=US/O=GTE Corporation/OU=GTE CyberTrust Solutions, Inc./CN=GTE CyberTrust Global Root	550676	17631	3.20	0.090
/C=BM/O=QuoVadis Limited/CN=QuoVadis Root CA 2 G3	260288	769	0.30	-0.562
/C=DE/O=T-Systems Enterprise Services GmbH/OU=T-Systems Trust Center/CN=T-TeleSec GlobalRoot Class 2	296824	884	0.30	-0.562
/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Assured ID Root CA	147982	137	0.09	-0.609
/C=US/ST=UT/L=Salt Lake City/O=The USERTRUST Network/OU=http:\/\/www.usertrust.com/CN=UTN - DATACorp SGC	267319	17	0.01	-0.627
/C=US/O=Google Trust Services LLC/CN=GTS Root R4	187987	9	0.00	-0.629
/C=GB/ST=London/O=Google UK Ltd./OU=Certificate Transparency/CN=Merge Delay Monitor Root	417196	0.0	0.0	-0.63
/CN=ct-woodpecker CA51b4a4	173774	0.0	0.0	-0.63

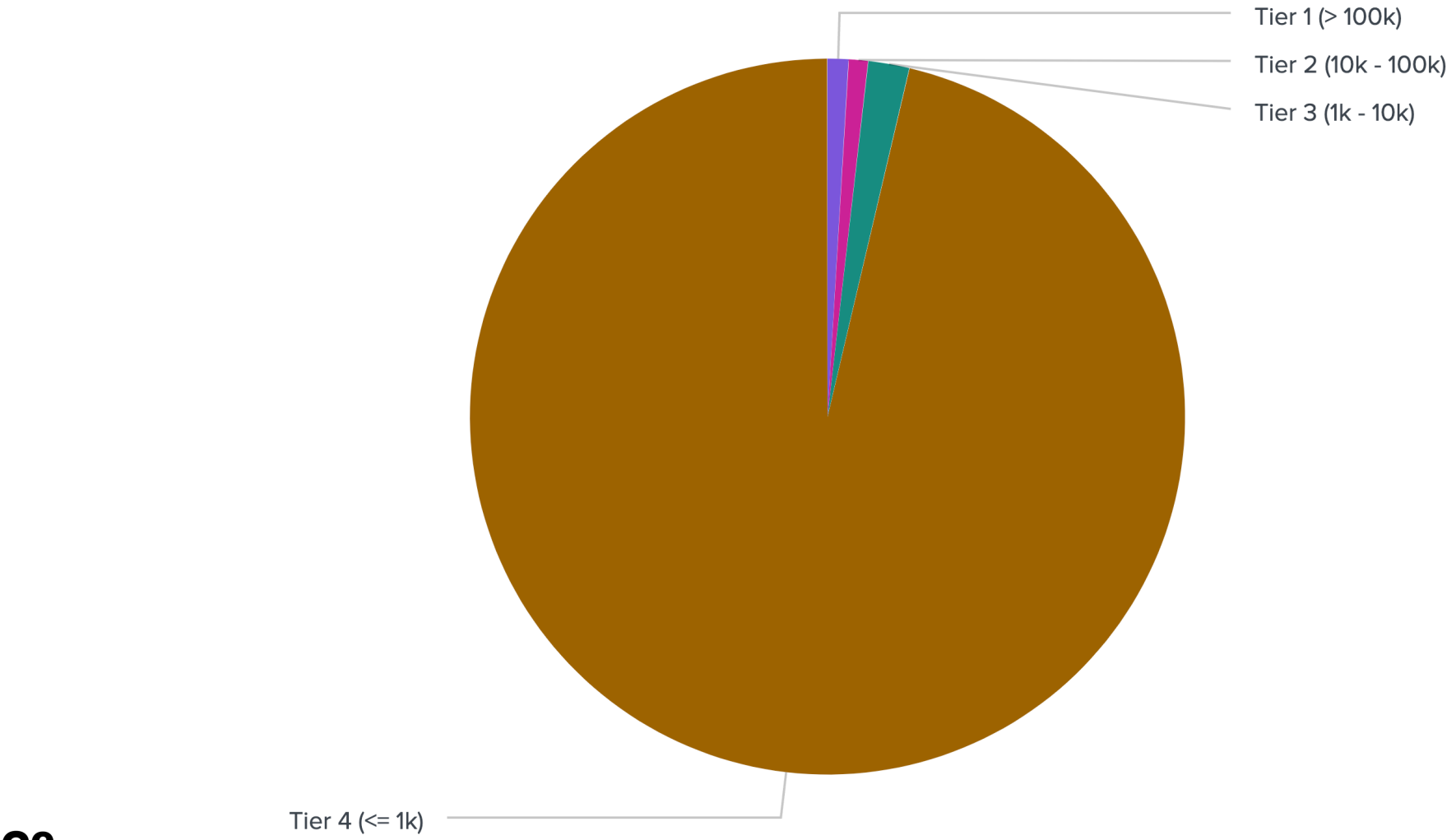
Riskiest Roots – Tier 4

root_ca	total_certs	risky_certs	risk_percent	zscore
/C=US/O=Internet Security Research Group/CN=ISRG Root X2	2	1	50.00	15.69
/C=IN/OU=emSign PKI/O=eMudhra Technologies Limited/CN=emSign Root CA - G1	1932	553	28.62	8.911
/C=US/O=Google Trust Services LLC/CN=GTS Root R1	5215	1101	21.11	6.530
/C=TR/L=Ankara/O=E-Tu\xC4\x9Fra EBG Bili\xC5\x9Fim Teknolojileri ve Hizmetleri A.\xC5\x9E./OU=E-Tugra Sertifikasyon Merkezi/CN=E-Tugra Certification Authority	49565	9596	19.36	5.975
/C=US/ST=Texas/L=Houston/O=SSL Corporation/CN=SSL.com Root Certification Authority ECC	1346	182	13.52	4.124
/C=US/ST=Texas/L=Houston/O=SSL Corporation/CN=SSL.com EV Root Certification Authority RSA R2	125	10	8.00	2.37
/CN=ComSign Secured CA/O=ComSign/C=IL	14	1	7.14	2.10
/C=PA/ST=Panama/L=Panama City/O=TrustCor Systems S. de R.L./OU=TrustCor Certificate Authority/CN=TrustCor RootCert CA-1	20339	1329	6.53	1.91
/C=CN/O=WoSign CA Limited/CN=CA \xE6\xB2\x83\xE9\x80\x9A\xE6\xA0\xB9\xE8\xAF\x81\xE4\xB9\xA6	22697	1472	6.49	1.89
/C=IN/O=India PKI/CN=CCA India 2015 SPL	216	13	6.02	1.75

Trustiest Roots – Tier 4

root_ca	total_certs	risky_certs	risk_percent	zscore
/C=AT/L=Vienna/ST=Austria/O=ARGE DATEN - Austrian Society for Data Protection/OU=GLOBALTRUST Certifi...	61	0.0	0.0	-0.2
/C=AT/O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH/OU=A-Trust-Qual-02/CN=A-Trus...	28	0.0	0.0	-0.2
/C=AT/O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH/OU=A-Trust-Qual-03/CN=A-Trus...	7	0.0	0.0	-0.2
/C=AT/O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH/OU=A-Trust-Root-05/CN=A-Trus...	204	0.0	0.0	-0.2
/C=AT/O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH/OU=A-Trust-Root-07/CN=A-Trus...	95	0.0	0.0	-0.2
/C=AT/O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH/OU=A-Trust-nQual-03/CN=A-Tru...	57	0.0	0.0	-0.2
/C=AT/O=A-Trust/OU=A-Trust-nQual-01/CN=A-Trust-nQual-01...	12	0.0	0.0	-0.2
/C=AT/O=Telekom-Control-Kommission/CN=Telekom-Control-Kommission Top 1...	1	0.0	0.0	-0.2
/C=AT/O=\x00A\x00-\x00T\x00r\x00u\x00s\x00t\x00 \x00G\x00e\x00s\x00.\x00 \x00f\x00\xFC\x00r\x00 \x00...	4	0.0	0.0	-0.2
/C=AT/O=e-commerce monitoring GmbH/CN=GLOBALTRUST 2020...	50	0.0	0.0	-0.2

Issuing CA Tiers



Riskiest Issuers – Tier 1

issuer	total_certs	risky_certs	risk_percent	zscore
/C=US/ST=Arizona/L=Scottsdale/O=GoDaddy.com, Inc./OU=http:\\/\\/certs.godaddy.com\\/repository\\//CN...	10289248	3495113	33.97	3.876
/C=AT/O=ZeroSSL/CN=ZeroSSL RSA Domain Secure Site CA...	8140872	2242672	27.55	3.017
/C=GB/ST=Greater Manchester/L=Salford/O=Sectigo Limited/CN=Sectigo RSA Domain Validation Secure Serv...	54012771	14208272	26.31	2.851
/C=CN/O=TrustAsia Technologies, Inc./CN=TrustAsia RSA DV TLS CA G2...	693647	151705	21.87	2.257
/C=US/O=Google Trust Services LLC/CN=GTS CA 1D4...	17771678	3715428	20.91	2.129
/C=PL/O=home.pl S.A./CN=Certyfikat SSL...	215931	41523	19.23	1.904
/C=LV/L=Riga/O=GoGetSSL/CN=GoGetSSL RSA DV CA...	257721	47659	18.49	1.805
/C=PL/O=Unizeto Technologies S.A./OU=Certum Certification Authority/CN=Certum Domain Validation CA S...	375873	67142	17.86	1.721
/C=CN/O=TrustAsia Technologies, Inc./OU=Domain Validated SSL/CN=TrustAsia TLS RSA CA...	3344714	542667	16.22	1.502
/C=US/ST=TX/L=Houston/O=cPanel, Inc./CN=cPanel, Inc. ECC Certification Authority...	376937	60581	16.07	1.481

Trustiest Issuers – Tier 1

issuer	total_certs	risky_certs	risk_percent	zscore
/C=BE/O=GlobalSign nv-sa/CN=GlobalSign Atlas R3 DV TLS CA 2022 Q4...	270045	0.0	0.0	-0.67
/C=BE/O=GlobalSign nv-sa/CN=GlobalSign CloudSSL CA - SHA256 - G3...	499781	0.0	0.0	-0.67
/C=BE/O=GlobalSign nv-sa/CN=GlobalSign Atlas R3 DV TLS CA 2022 Q3...	1640202	67	0.00	-0.668
/C=IT/ST=Bergamo/L=Ponte San Pietro/O=Actalis S.p.A.\\/03358520967/CN=Actalis Domain Validation Serv...	231821	2	0.00	-0.668
/C=IT/ST=Bergamo/L=Ponte San Pietro/O=Actalis S.p.A.\\/03358520967/CN=Actalis Domain Validation Serv...	731225	3	0.00	-0.668
/C=US/O=Certainly/CN=Certainly Intermediate R1...	501955	10	0.00	-0.668
/C=US/O=DigiCert Inc/CN=DigiCert Basic RSA CN CA G2...	421561	8	0.00	-0.668
/C=US/O=Google Trust Services LLC/CN=GTS CA 2A1...	186878	9	0.00	-0.668
/C=US/O=Google Trust Services/CN=GTS CA 1O1...	7595838	8	0.00	-0.668
/C=US/O=HydrantID (Avalanche Cloud Corporation)/CN=HydrantID SSL CA G3...	841504	19	0.00	-0.668

Riskiest Issuers – Tier 2

issuer	total_certs	risky_certs	risk_percent	zscore
/C=US/O=TrustOcean Limited/CN=TrustOcean Encryption365 Pro SSL CA...	10611	9756	91.94	7.574
/C=PL/O=LH.pl Sp. z o.o./OU=LH.pl/CN=www.lh.pl...	19861	7516	37.84	2.898
/C=SG/O=CertCloud Pte. Ltd./CN=CertCloud RSA TLS CA...	24331	6297	25.88	1.865
/C=US/O=Root Networks, LLC/CN=Root CA - G3...	20268	4589	22.64	1.584
/C=TR/L=Istanbul/O=Isimtescil Bilisim Anonim Sirketi/OU=SSL Department/CN=TrustSafe Domain Validated...	40425	8982	22.22	1.548
/C=CN/O=TrustAsia Technologies, Inc./OU=Domain Validated SSL/CN=TrustAsia TLS ECC CA...	75199	15631	20.79	1.425
/C=US/ST=New Jersey/L=Jersey City/O=The USERTRUST Network/CN=USERTrust RSA Domain Validation Secure ...	91451	16719	18.28	1.208
/C=ES/ST=Illes Balears/L=Manacor/O=Soluciones Corporativas IP, SL/CN=Don Dominio \\/ MrDomain RSA DV...	51551	7714	14.96	0.9207
/C=PL/ST=Ma\\xC5\\x82opolskie/L=Krak\\xC3\\xB3w/O=DOMENY.PL sp. z o.o/CN=DOMENY SSL DV Certification...	17890	2050	11.46	0.618
/C=LU/O=CentralNic Luxembourg S\\xC3\\xA0rl/CN=GlobeSSL DV CA...	11770	945	8.03	0.322

Trustiest Issuers – Tier 2

issuer	total_certs	risky_certs	risk_percent	zscore
/C=PL/O=Dreamcommerce S.A./OU=Dreamcommerce S.A./CN=Shoper\\xC2\\xAE SSL...	52629	1	0.00	-0.372
/C=DE/O=STRATO AG/OU=Domain Validated SSL/CN=STRATO TLS RSA CA...	50238	7	0.01	-0.371
/C=JP/O=SECOM Trust Systems CO.,LTD./CN=NII Open Domain CA - G7 RSA...	42604	3	0.01	-0.371
/C=US/O=HydrantID (Avalanche Cloud Corporation)/CN=HydrantID EV SSL ICA G1...	12971	1	0.01	-0.371
/C=US/O=Aetna Inc/CN=Aetna Inc. Secure CA2...	28258	6	0.02	-0.370
/C=CA/O=AffirmTrust/OU=See www.affirmtrust.com\\/repository/CN=AffirmTrust Certificate Authority - O...	16318	8	0.05	-0.368
/C=US/O=DigiCert Inc/CN=DigiCert Global G3 TLS ECC SHA384 2020 CA1...	16164	8	0.05	-0.368
/C=US/O=DigiCert Inc/CN=DigiCert Baltimore TLS RSA SHA256 2020 CA1...	63492	37	0.06	-0.367
/C=US/ST=MI/L=Ann Arbor/O=Internet2/OU=InCommon/CN=InCommon ECC Server CA...	12326	8	0.06	-0.367
/C=BM/O=QuoVadis Limited/CN=QuoVadis EV SSL ICA G1...	10120	7	0.07	-0.366

Riskiest Issuers – Tier 3

issuer	total_certs	risky_certs	risk_percent	zscore
/C=TR/O=Isimtescil Bilisim A.S./CN=TrustSafe TLS RSA SubCA R1...	5646	2188	38.75	5.301
/C=MA/ST=Marrakech/L=Marrakech/O=Genious Communications/CN=GENIOUS RSA Domain Validation Secure Serv...	2986	1119	37.47	5.112
/C=IN/ST=Karnataka/L=Bengaluru/O=eMudhra Technologies Limited/CN=eMudhra RSA Domain Validation Secur...	4884	1813	37.12	5.060
/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=RapidSSL ECC CA 2018...	2156	671	31.12	4.175
/C=IN/OU=emSign PKI/O=eMudhra Technologies Limited/CN=emSign SSL CA - G1...	1898	553	29.14	3.882
/C=NZ/O=SafeToOpen Ltd/CN=SafeToOpen TLS ICA RSA R1...	1440	347	24.10	3.138
/C=CN/ST=Shanghai/O=TrustAsia Technologies, Inc./CN=TrustAsia RSA DV SSL Server CA...	1155	272	23.55	3.057
/C=GB/O=Quantum CA Limited/CN=Quantum Secure Site DV TLS CN RSA R1...	4040	845	20.92	2.669
/C=CN/O=TrustAsia Technologies, Inc./CN=TrustAsia ECC DV TLS CA G2...	9816	2032	20.70	2.637
/C=CN/O=Baidu, Inc./CN=Baidu, Inc. DV CA...	1112	229	20.59	2.620

Trustiest Issuers – Tier 3

issuer	total_certs	risky_certs	risk_percent	zscore
/C=BE/O=GlobalSign nv-sa/CN=GlobalSign Atlas ECCR5 OV TLS CA 2022 Q1...	2829	0.0	0.0	-0.42
/C=BE/O=GlobalSign nv-sa/CN=GlobalSign Atlas ECCR5 OV TLS CA 2022 Q2...	2494	0.0	0.0	-0.42
/C=BE/O=GlobalSign nv-sa/CN=GlobalSign Atlas ECCR5 OV TLS CA 2022 Q3...	1839	0.0	0.0	-0.42
/C=BE/O=GlobalSign nv-sa/CN=GlobalSign Atlas ECCR5 OV TLS CA H2 2021...	5266	0.0	0.0	-0.42
/C=BE/O=GlobalSign nv-sa/CN=GlobalSign Extended Validation CA - SHA256 - G2...	1666	0.0	0.0	-0.42
/C=BE/O=GlobalSign nv-sa/CN=GlobalSign HV RSA DV SSL CA 2018...	5454	0.0	0.0	-0.42
/C=BE/O=GlobalSign nv-sa/CN=GlobalSign Organization Validated CA - SHA256 - G4...	3144	0.0	0.0	-0.42
/C=BE/O=GlobalSign nv-sa/CN=GlobalSign Organization Validated ECC CA - SHA256 - G4...	2957	0.0	0.0	-0.42
/C=BE/O=GlobalSign nv-sa/CN=GlobalSign PersonalSign 2 CA - G2...	1192	0.0	0.0	-0.42
/C=BR/O=ICP-Brasil/OU=Secretaria da Receita Federal do Brasil - RFB/CN=Autoridade Certificadora do S...	3891	0.0	0.0	-0.42

Riskiest Issuers – Tier 4

issuer	total_certs	risky_certs	risk_percent	zscore
/C=AE/O=Etisalat/OU=Etisalat eBusiness Services/CN=Comtrust Server Certification Authority...	1	1	100.00	36.77
/C=DE/O=EUNETIC GmbH/CN=EuropeanSSL Server CA...	1	1	100.00	36.77
/C=US/O=INTEGRITY Security Services LLC/CN=ISSAuth RSA DV CA...	2	2	100.00	36.77
/C=GB/O=Quantum CA Limited/CN=Quantum Secure Site EV TLS RSA R1...	3	2	66.67	24.49
/C=MA/ST=Marrakech/L=Marrakech/O=Genious Communications/CN=GENIOUS ECC Domain Validation Secure Serv...	2	1	50.00	18.35
/C=MA/ST=Marrakech/L=Marrakech/O=Genious Communications/OU=Controlled by Sectigo exclusively for Gen...	4	2	50.00	18.35
/C=SG/ST=Singapore/L=Singapore/O=One Sign Pte. Ltd./CN=OneSignSSL ECC DV Secure Server CA...	2	1	50.00	18.35
/C=US/O=DNEncrypt, Inc/CN=DNEncrypt ECC DV SSL\\/TLS [Run by the Issuer]...	2	1	50.00	18.35
/C=US/O=DigiCert, Inc./CN=DigiCert High Assurance TLS Hybrid ECC SHA256 2020 CA1...	2	1	50.00	18.35
/C=VN/O=Hao Quang Viet Software Company Limited/CN=MuaSSL.com TLS Issuing ECC CA R1...	10	5	50.00	18.35

Trustiest Issuers – Tier 4

issuer	total_certs	risky_certs	risk_percent	zscore
/C=AD/O=M.I. Govern d'Andorra/serialNumber=D-059888-N/L=Andorra la Vella/CN=Entitat de Certificaci\\...	1	0.0	0.0	-0.08
/C=AE/O=DREAMSCAPE NETWORKS FZ-LLC/OU=Security Dept./CN=Crazy Domains (DV) Certification Authority...	4	0.0	0.0	-0.08
/C=AE/O=DarkMatter LLC/CN=DarkMatter High Assurance CA...	49	0.0	0.0	-0.08
/C=AE/O=Digital Trust L.L.C./CN=DigitalTrust High Assurance CA G4 [Run by the Issuer]...	1	0.0	0.0	-0.08
/C=AE/O=Digital Trust L.L.C./CN=DigitalTrust Secure CA G3 [Run by the Issuer]...	19	0.0	0.0	-0.08
/C=AE/ST=Abu Dhabi/L=Abu Dhabi/O=Crown Prince Court/CN=Crown Prince Court CA...	1	0.0	0.0	-0.08
/C=AR/O=Banco Santander Rio S.A./OU=Symantec Trust Network/OU=Class 2 Managed PKI Individual Subscri...	1	0.0	0.0	-0.08
/C=AT/L=Vienna/O=ARGE DATEN - Austrian Society for Data Protection and Privacy/CN=A-CERT ADVANCED/em...	3	0.0	0.0	-0.08
/C=AT/L=Vienna/ST=Austria/O=ARGE DATEN - Austrian Society for Data Protection/OU=GLOBALTRUST Certifi...	2	0.0	0.0	-0.08
/C=AT/L=Wien/O=Energie-Control GmbH/CN=E-Control Certification Services/emailAddress=cert.services@e...	3	0.0	0.0	-0.08

Apply

- We identified 4 risky outlier root CAs and 10 issuers
  - Tier 4 roots were drowned in noise, so we ignored those
- Blocking specific root CAs is probably not warranted for most orgs
- Blocking specific issuing CAs **might** be beneficial for some orgs, but this is difficult to do
- Logging certificates and issuers enables CAs to be used as observations with Risk-Based Alerting (RBA) or Risk-Based Hunting (RBH).
- Download the full risk rankings: **https://splk.it/CATrust**

Room for Future Work

- Longer certificate history + longer intel history would allow us to track trustworthiness changes over time, which could be interesting
- More precise subject matching
- Why don’t more intel providers track malicious certificates?
- Someone (else) publish CA risk rankings on a regular basis

RSAConference™2023
San Francisco | April 24 – 27 | Moscone Center

SESSION ID: HT-R03

Trust Unearned? Evaluating CA Trustworthiness Across 5 Billion Certificates

David J. Bianco
Staff Security Strategist
SURGe by Splunk
@DavidJBianco / @DavidJBianco@infosec.exchange