Chronicle

Google Cloud Whitepaper
May 2019

Abusing code signing for profit

Google Cloud

Abusing code signing for profit

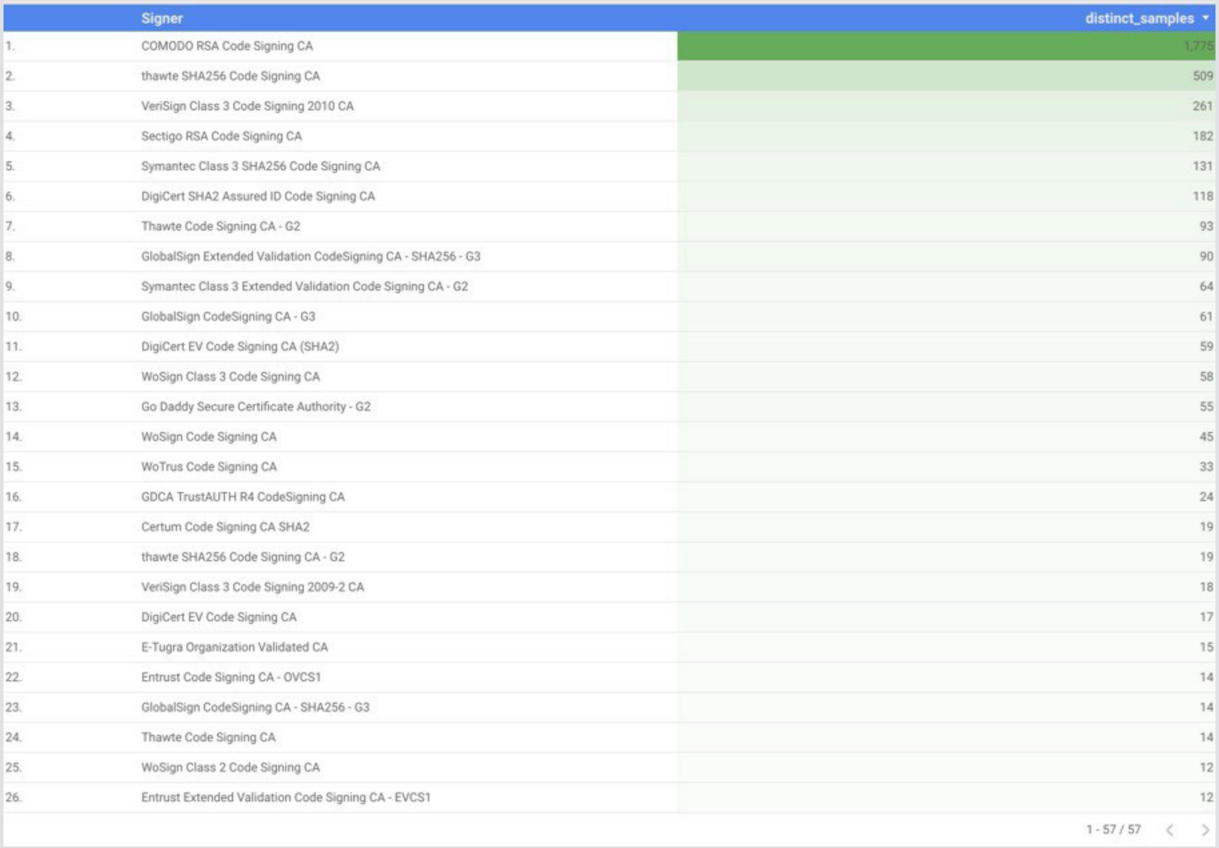
Signing a Windows executable file was originally conceived as a mechanism to guarantee the authenticity and integrity of a file published on the internet. Since its inception, the process of cryptographically signing a piece of code was designed to give the operating system a way to discriminate between legitimate and potentially malicious software. Unfortunately, this system is built on a problematic core tenet: **Trust**.

The chain of trust is relatively straight-forward: certificates are signed (issued) by trusted certificate authorities (CAs), which have the backing of a trusted parent CA. This inherited trust model is taken advantage of by malware authors who purchase certificates directly or via resellers. Whether purchased directly or indirectly, due diligence into customers appears to be lacking. Revoking a certificate, the process by which a CA says the certificate is no longer trustworthy, is unfortunately the only real tool available to combat certificate abuse. This process introduces a delay in which malware with a certificate may be considered “trusted.”

Chronicle researchers hunted within VirusTotal to gain a deeper understanding of this issue. For this investigation researchers only included Windows PE Executable files, filtered out samples with less than 15 aggregate detections, aggressively filtered out grayware files, and calculated the distinct number of samples each signing CA was responsible for (note: the samples may have different certificates, the focus is on the signing CA only). Data was collected within a 365 day span with an initial start date of May 7th, 2019.

Results

In total, 3,815 malware samples met the filtering criteria. Figure 1 shows the top 25 abused CAs as well as the total number of samples signed.



	Signer	distinct_samples ▾
1.	COMODO RSA Code Signing CA	1,775
2.	thawte SHA256 Code Signing CA	509
3.	VeriSign Class 3 Code Signing 2010 CA	261
4.	Sectigo RSA Code Signing CA	182
5.	Symantec Class 3 SHA256 Code Signing CA	131
6.	DigiCert SHA2 Assured ID Code Signing CA	118
7.	Thawte Code Signing CA - G2	93
8.	GlobalSign Extended Validation CodeSigning CA - SHA256 - G3	90
9.	Symantec Class 3 Extended Validation Code Signing CA - G2	64
10.	GlobalSign CodeSigning CA - G3	61
11.	DigiCert EV Code Signing CA (SHA2)	59
12.	WoSign Class 3 Code Signing CA	58
13.	Go Daddy Secure Certificate Authority - G2	55
14.	WoSign Code Signing CA	45
15.	WoTrus Code Signing CA	33
16.	GDCA TrustAUTH R4 CodeSigning CA	24
17.	Certum Code Signing CA SHA2	19
18.	thawte SHA256 Code Signing CA - G2	19
19.	VeriSign Class 3 Code Signing 2009-2 CA	18
20.	DigiCert EV Code Signing CA	17
21.	E-Tugra Organization Validated CA	15
22.	Entrust Code Signing CA - OVCS1	14
23.	GlobalSign CodeSigning CA - SHA256 - G3	14
24.	Thawte Code Signing CA	14
25.	WoSign Class 2 Code Signing CA	12
26.	Entrust Extended Validation Code Signing CA - EVCS1	12

Figure 1: Table showing the top 25 signers by distinct sample count over the past 365 days. Look-back begins on May 7th, 2019.

As indicated in Figure 1, CAs who signed certificates of 100 or more malware samples account for nearly **78%** of signed samples uploaded to VirusTotal. This is broken down further in Figure 2 below.

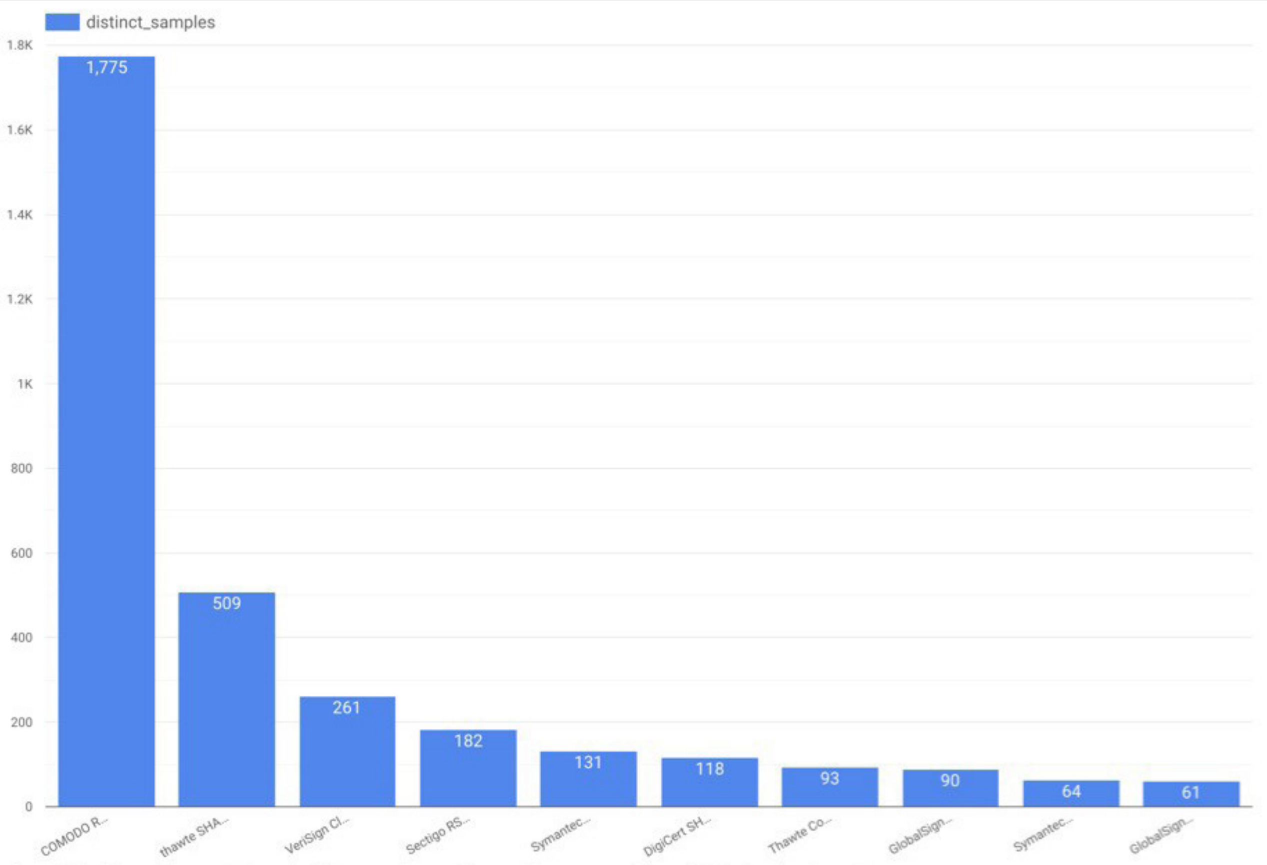
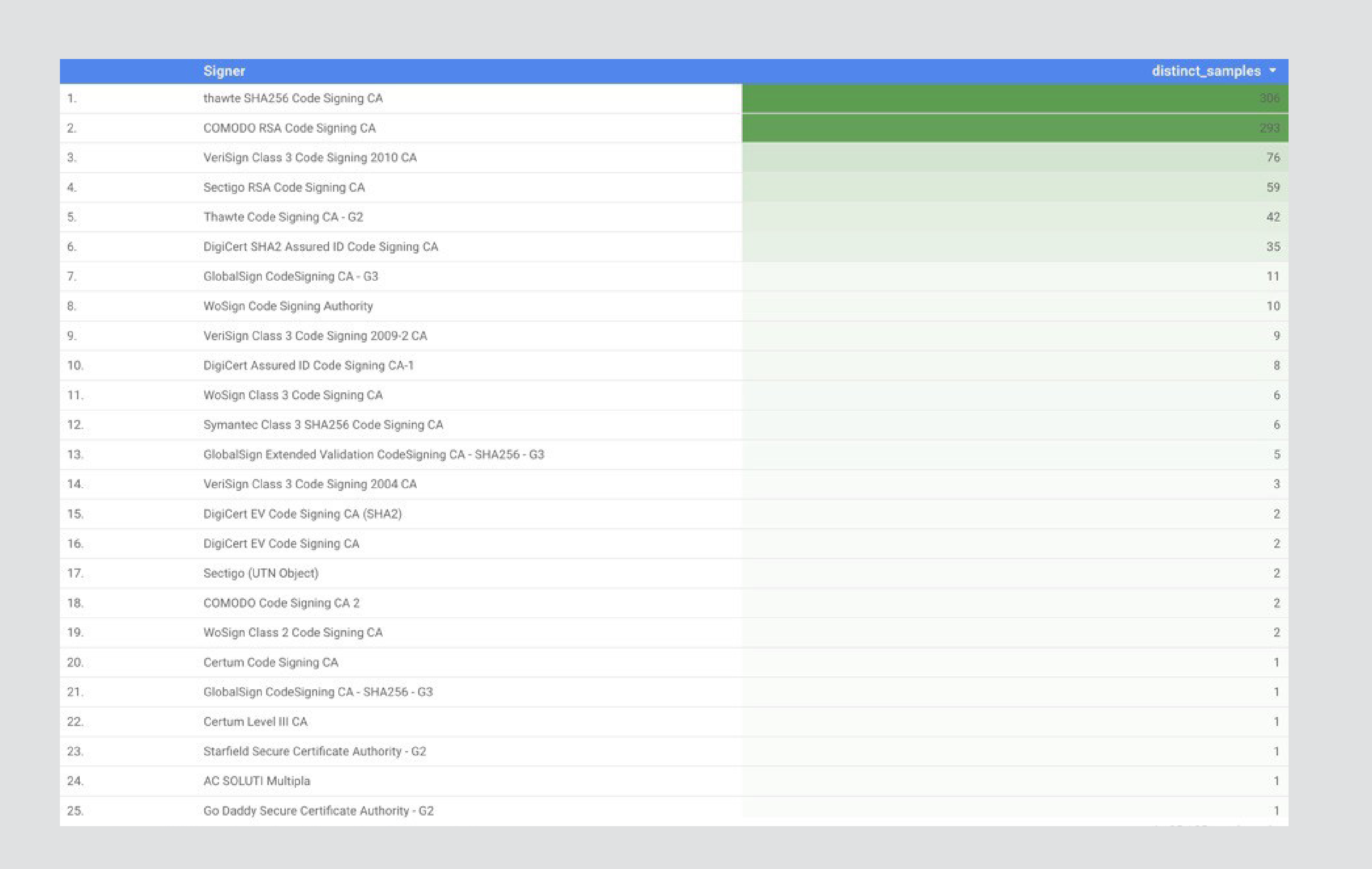


Figure 2: Breakdown of the top 10 signers by distinct sample count. The top 6 signers account for nearly 78% of evaluated samples.

Figure 2 depicts the drop off of malicious samples per signing CA. The CA with the most samples has nearly **3.5x** more samples than the next highest which in turn has almost **2x** more than the next highest. The pattern quickly falls off as we move down the line of the top 10 CAs issuing abused certificates.

There is some hope! When evaluating this data we determined that **21%** of samples had their certificates revoked at the time of writing (May 8th, 2019). This indicates that CAs are taking some action. Note that for the revocation of a certificate to be reflected in the VirusTotal dataset, the sample must be rescanned following the revocation request by the responsible CA.



	Signer	distinct_samples ▾
1.	thawte SHA256 Code Signing CA	306
2.	COMODO RSA Code Signing CA	293
3.	VeriSign Class 3 Code Signing 2010 CA	76
4.	Sectigo RSA Code Signing CA	59
5.	Thawte Code Signing CA - G2	42
6.	DigiCert SHA2 Assured ID Code Signing CA	35
7.	GlobalSign CodeSigning CA - G3	11
8.	WoSign Code Signing Authority	10
9.	VeriSign Class 3 Code Signing 2009-2 CA	9
10.	DigiCert Assured ID Code Signing CA-1	8
11.	WoSign Class 3 Code Signing CA	6
12.	Symantec Class 3 SHA256 Code Signing CA	6
13.	GlobalSign Extended Validation CodeSigning CA - SHA256 - G3	5
14.	VeriSign Class 3 Code Signing 2004 CA	3
15.	DigiCert EV Code Signing CA (SHA2)	2
16.	DigiCert EV Code Signing CA	2
17.	Sectigo (UTN Object)	2
18.	COMODO Code Signing CA 2	2
19.	WoSign Class 2 Code Signing CA	2
20.	Certum Code Signing CA	1
21.	GlobalSign CodeSigning CA - SHA256 - G3	1
22.	Certum Level III CA	1
23.	Starfield Secure Certificate Authority - G2	1
24.	AC SOLUTI Multipla	1
25.	Go Daddy Secure Certificate Authority - G2	1

Figure 3: A total of 805 or 21% of certificates have been revoked.

What does this mean going forward?

While malware abusing trust is not a new phenomenon, the popular trend of financially motivated threat actors buying code signing certificates illuminates the inherent flaws of trust based security. Signed payloads are no longer solely within the domain of nation-state threat actors stealing code signing certificates from victims; they are readily accessible to operators of crime focused malware. The impact is amplified by the scope and scale of typical crimeware campaigns. Expect to see signed malware reported more frequently.

All hope is not lost. Certificate authorities are actively revoking certificates from malware executables that are identified in the wild. This indicates that CAs do take their responsibilities seriously, though more diligence around buyers may help prior to the proverbial cat being out of the bag.

Appendix

All graphics as well as a CSV of the hashes, day last observed, and signer chain of all 3,815 files are provided for analysis here: https://gist.github.com/Blevene/6455fd7a898425d0546206d4be61fc68

Chronicle Researchers would like to thank https://twitter.com/malwrhunterteam for inspiring this study.

[1] Introduction to Code Signing: https://docs.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/platform-apis/ms537361(v=vs.85)

[2] Understanding Code Signing Abuse in Malware Campaigns: https://blog.trendmicro.com/trendlabs-security-intelligence/understanding-code-signing-abuse-in-malware-campaigns/#

[3] 'No questions asked' Windows code cert slingers 'fuel trade' in digitally signed malware: https://www.theregister.co.uk/2018/06/26/digitally_signed_malware/

[4] What You Should Know About Grayware (and What to Do About It): https://www.darkreading.com/vulnerabilities---threats/what-you-should-know-about-grayware-(and-what-to-do-about-it)/d/d-id/1333216