Recorded Future

CYBER THREAT ANALYSIS

The Use of Counterfeit Code Signing Certificates Is on the Rise

By Andrei Barysevich
Recorded Future

CTA-2018-0222

Executive Summary

In 2017, security researchers around the world started seeing a sudden increase in code signing certificates being used as a layered obfuscation technique for malicious payload distribution campaigns. Recorded Future's Insikt Group investigated the criminal underground and identified vendors currently offering both code signing certificates and domain name registration with accompanying SSL certificates.

Contrary to a common belief that the security certificates circulating in the criminal underground are stolen from legitimate owners prior to being used in nefarious campaigns, we confirmed with a high degree of certainty that the certificates are created for a specific buyer per request only and are registered using stolen corporate identities, making traditional network security appliances less effective.

Key Judgments

- We observed the earliest use of stolen code certificates in 2011, but it was not until 2015 that code signing certificates became widely available in the criminal underground.

- Insikt Group identified four well-known vendors of such products since 2011; only two vendors are currently soliciting their services to Russian-speaking hackers.

- The most affordable version of a code signing certificate costs $299, but the most comprehensive Extended Validation (EV) certificate with a SmartScreen reputation rating is listed for $1,599. The starting price of a domain name registration with EV SSL certificate is $349.

- All certificates are issued by reputable companies, such as Comodo, Thawte, and Symantec, and have proved to be extremely effective in malware obfuscation. We believe that legitimate business owners are unaware that their data was used in the illicit activities.

- Network security appliances performing deep packet inspection become less effective when legitimate (legitimate certificate) SSL/TLS traffic is initiated by a malicious implant. Netflow (packet headers) analysis is an important control toward reducing risk, as host-based controls may also be rendered ineffective by legitimate code signing certificates.

Background

For a number of years, security researchers have warned the public about cybercriminals using counterfeited code signing certificates in their efforts to obfuscate malicious payloads, but only a handful of times were these underground services researched thoroughly.

As antivirus software detection capabilities improved, the standard tactics such as payload encryption were no longer sufficient. It became more challenging to sustain a file's effectiveness for extended periods of time, sometimes requiring daily "cleaning" of executable files. As a result, cybercriminals needed a more comprehensive security approach and began experimenting with a secondary protection layer, signing payload files with the legitimately issued security certificates.

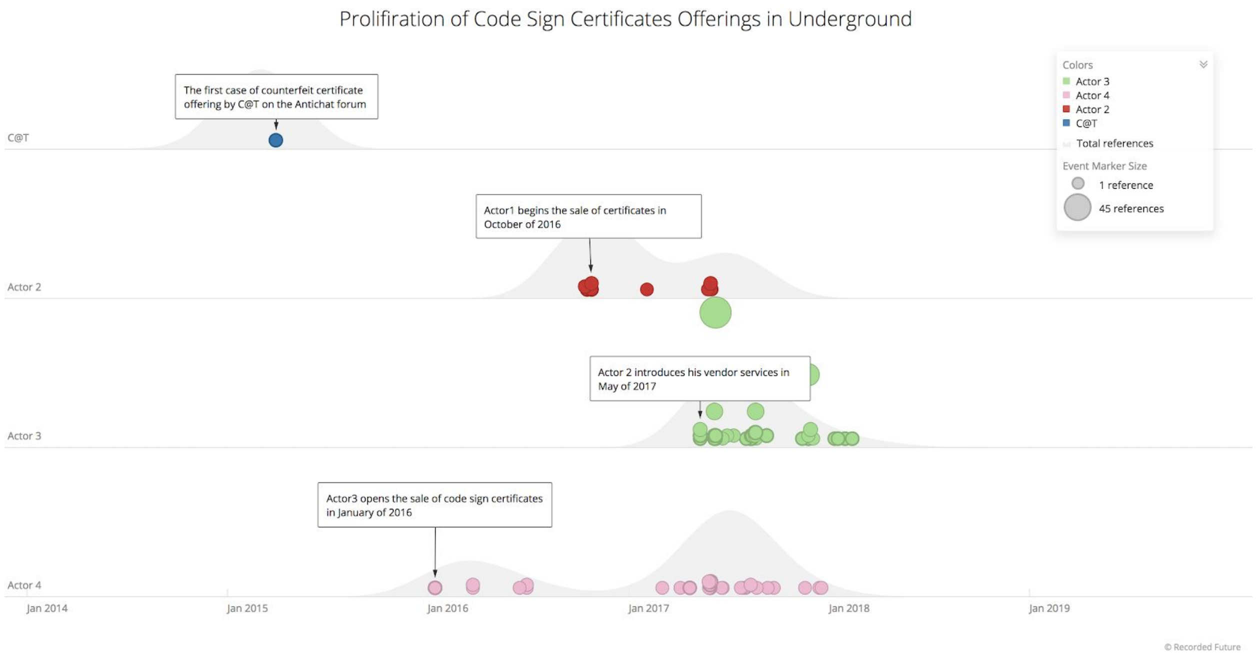
Although it was known that threat actors were using counterfeit certificates as early as 2011, it was not until 2015 that the first offerings surfaced in the underground.

Threat Analysis

One of the first vendors to offer counterfeit code signing certificates was known as C@T, a member of a prolific hacking messaging board. In March 2015, C@T offered for sale a Microsoft Authenticode capable of signing 32/64b versions of various executable files, as well as Microsoft Office, Microsoft VBA, Netscape Object Signing, and Marimba Channel Signing documents, and supported Silverlight 4 applications. Additionally, Apple code signing certificates were also available.

In his advertisement, C@T explained that the certificates are registered under legitimate corporations and issued by Comodo, Thawte, and Symantec — the largest and most respected issuers. The seller indicated that each certificate is unique and will only be assigned to a single buyer, which could be easily verified via HerdProtect.com. According to C@T, the success rate of payload installations from signed files increases by 30 to 50 percent, and he even admitted to selling over 60 certificates in less than six months.

During that time, C@T saw sales dwindle and failed to appeal to a broad client base because of prohibitive costs, in some cases demanding upwards of $1,000 per certificate, when other more affordable and reliable payload obfuscation methods were still available.

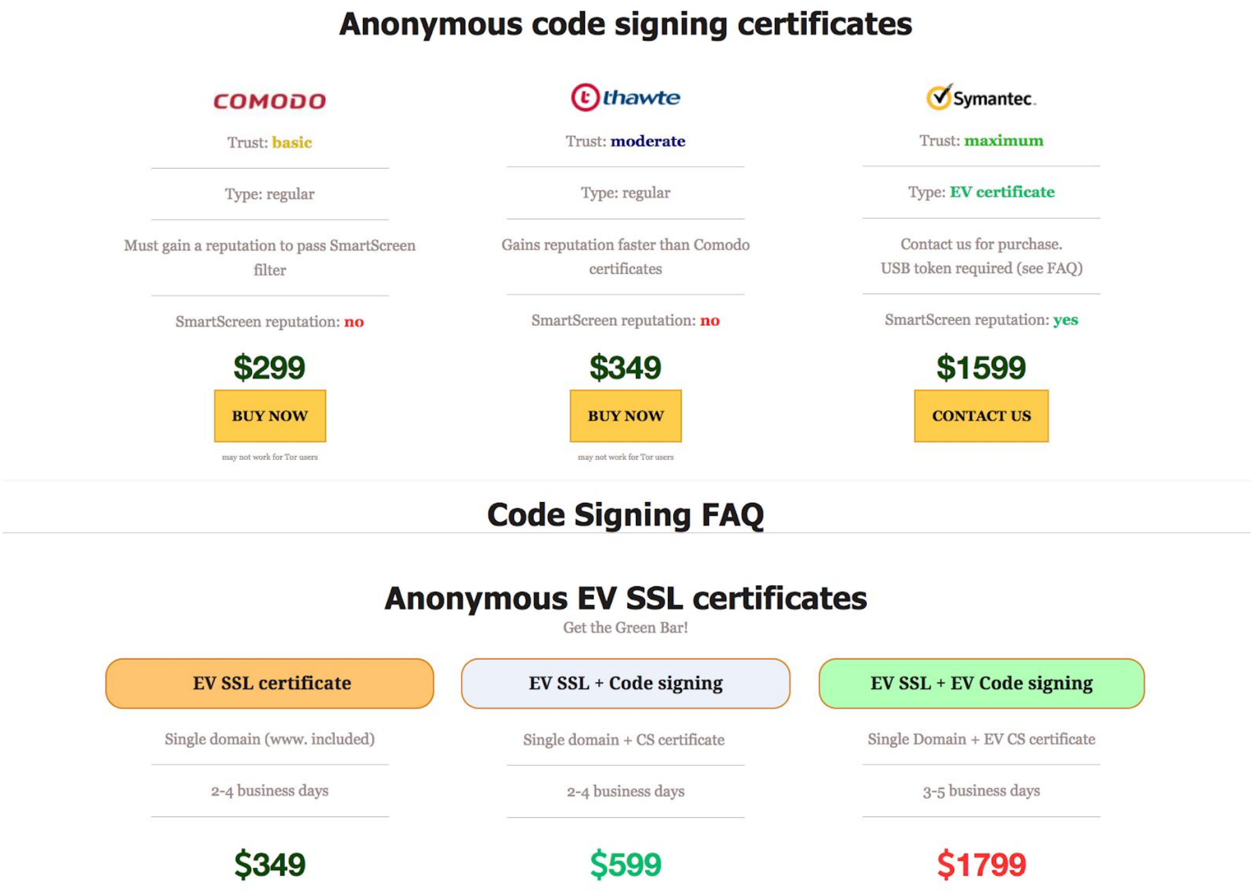


The activity of criminal vendors of counterfeit code signing certificates in the dark web.

Approximately two years later, three new actors began offering their services primarily in the Eastern European underground. While one actor eventually moved on to other illicit operations, the remaining two actors still actively supply counterfeit certificates to Russian-speaking actors.

The second actor specializes in Class 3 certificates, which do not include Extended Validation (EV) assurance and are available for the price of $600, whereas the third actor offers the broadest range of products.

Standard code signing certificates issued by Comodo that do not include SmartScreen reputation rating cost $295. A buyer interested in the most trusted version of an EV certificate issued by Symantec would have to pay $1,599, a 230 percent premium compared to the price of the authentic certificate. For those seeking to purchase in bulk, fully authenticated domains with EV SSL encryption and code signing capabilities could also be arranged for $1,799.



Anonymous code signing certificates

COMODO	thawte	Symantec.
Trust: basic	Trust: moderate	Trust: maximum
Type: regular	Type: regular	Type: EV certificate
Must gain a reputation to pass SmartScreen filter	Gains reputation faster than Comodo certificates	Contact us for purchase. USB token required (see FAQ)
SmartScreen reputation: no	SmartScreen reputation: no	SmartScreen reputation: yes
$299	$349	$1599
BUY NOW	BUY NOW	CONTACT US
may not work for Tor users	may not work for Tor users	

Code Signing FAQ

Anonymous EV SSL certificates

Get the Green Bar!

EV SSL certificate	EV SSL + Code signing	EV SSL + EV Code signing
Single domain (www. included)	Single domain + CS certificate	Single Domain + EV CS certificate
2-4 business days	2-4 business days	3-5 business days
$349	$599	$1799

Product listing advertised by a threat actor.

According to the information provided by both sellers during a private conversation, to guarantee the issuance and lifespan of the products, all certificates are registered using the information of real corporations. With a high degree of confidence, we believe that the legitimate business owners are unaware that their data was used in the illicit activities. It is important to note that all certificates are created for each buyer individually with the average delivery time of two to four days.

Technical Analysis

Both actors have acknowledged that due to the advanced security metrics employed in the Chrome browser — it is considered to be providing excellent security — clients must expect significantly lower levels of success penetrations compared to Firefox, Internet Explorer, and Safari browsers.

Insikt Group successfully convinced a vendor to conduct a trial, signing a provided payload executable of a previously unreported Remote Access Trojan (RAT) with a recently issued Comodo certificate. Despite that test-subject files were encrypted beforehand, the results of the test demonstrated the superior effectiveness of code signed versions.

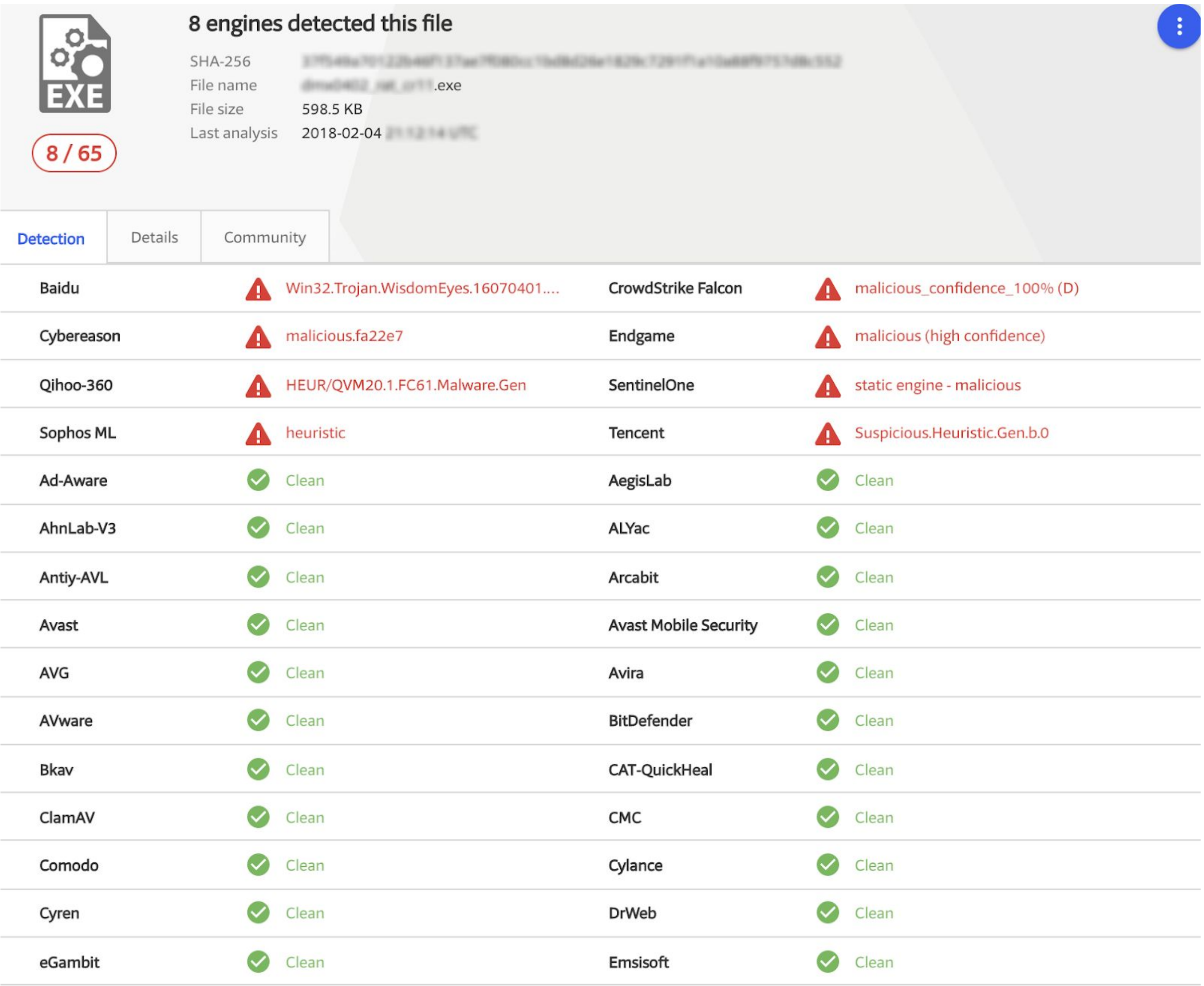
While only eight antivirus providers successfully detected the encrypted version of the payload, only two of them were effective against the code signed version. More disturbing results surfaced after the same test was conducted for a non-resident version of the payload. In that case, only six companies were capable of detecting an encrypted version, and only Endgame protection successfully recognized the file as malicious.

Outlook

Network security appliances performing deep packet inspection become less effective when legitimate (legitimate certificate) SSL/TLS traffic is initiated by a malicious implant. Netflow (packet headers) analysis is an important control toward reducing risk, as host-based controls may also be rendered ineffective by legitimate code signing certificates.

Unlike ordinary crypting services readily available at $10-$30 per each encryption, we do not anticipate counterfeit certificates to become a mainstream staple of cybercrime due to its prohibitive cost. However, undoubtedly, more sophisticated actors and nation-state actors who are engaged in less widespread and more targeted attacks will continue using fake code signing and SSL certificates in their operations.

Appendix A (Screenshots)

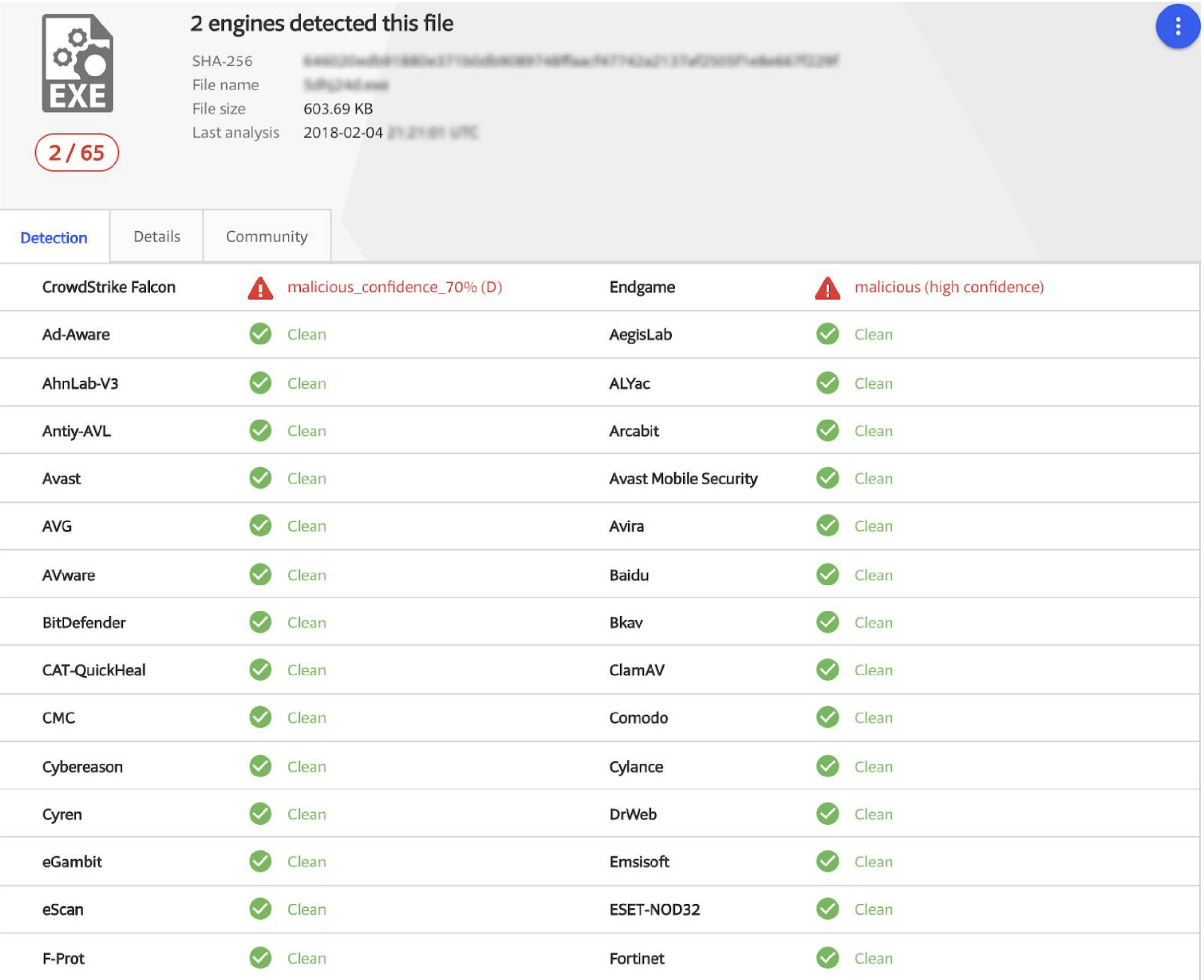


8 engines detected this file

SHA-256 [redacted]
File name [redacted].exe
File size 598.5 KB
Last analysis 2018-02-04 [redacted]

Baidu	⚠ Win32.Trojan.WisdomEyes.16070401....	CrowdStrike Falcon	⚠ malicious_confidence_100% (D)
Cybereason	⚠ malicious.fa22e7	Endgame	⚠ malicious (high confidence)
Qihoo-360	⚠ HEUR/QVM20.1.FC61.Malware.Gen	SentinelOne	⚠ static engine - malicious
Sophos ML	⚠ heuristic	Tencent	⚠ Suspicious.Heuristic.Gen.b.0
Ad-Aware	✓ Clean	AegisLab	✓ Clean
AhnLab-V3	✓ Clean	ALYac	✓ Clean
Antiy-AVL	✓ Clean	Arcabit	✓ Clean
Avast	✓ Clean	Avast Mobile Security	✓ Clean
AVG	✓ Clean	Avira	✓ Clean
AVware	✓ Clean	BitDefender	✓ Clean
Bkav	✓ Clean	CAT-QuickHeal	✓ Clean
ClamAV	✓ Clean	CMC	✓ Clean
Comodo	✓ Clean	Cylance	✓ Clean
Cyren	✓ Clean	DrWeb	✓ Clean
eGambit	✓ Clean	Emsisoft	✓ Clean

VirusTotal scan results of the encrypted payload.



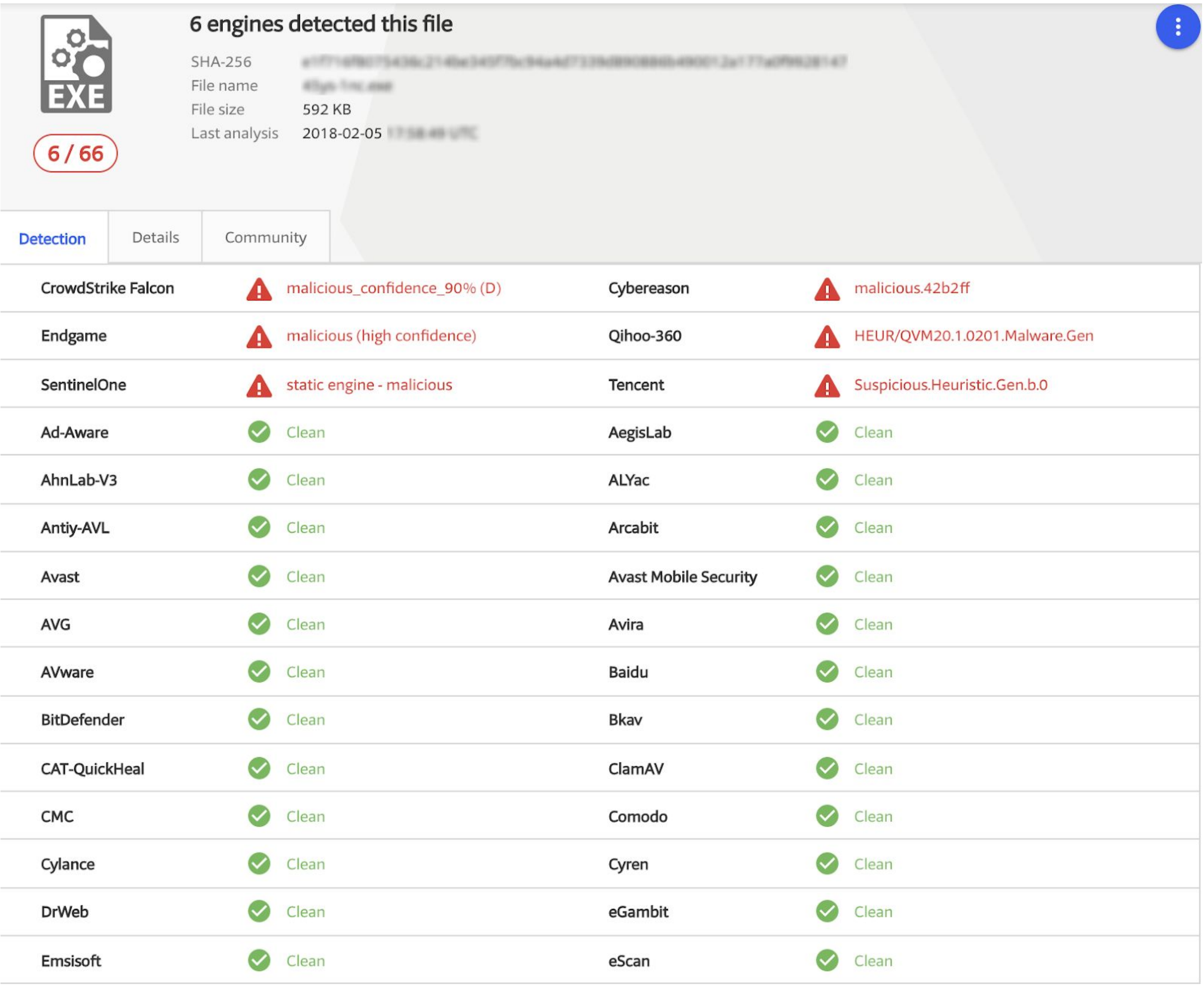
2 / 65

2 engines detected this file

SHA-256 [redacted]
File name [redacted]
File size 603.69 KB
Last analysis 2018-02-04 [redacted]

CrowdStrike Falcon	⚠ malicious_confidence_70% (D)	Endgame	⚠ malicious (high confidence)
Ad-Aware	✓ Clean	AegisLab	✓ Clean
AhnLab-V3	✓ Clean	ALYac	✓ Clean
Antiy-AVL	✓ Clean	Arcabit	✓ Clean
Avast	✓ Clean	Avast Mobile Security	✓ Clean
AVG	✓ Clean	Avira	✓ Clean
AVware	✓ Clean	Baidu	✓ Clean
BitDefender	✓ Clean	Bkav	✓ Clean
CAT-QuickHeal	✓ Clean	ClamAV	✓ Clean
CMC	✓ Clean	Comodo	✓ Clean
Cybereason	✓ Clean	Cylance	✓ Clean
Cyren	✓ Clean	DrWeb	✓ Clean
eGambit	✓ Clean	Emsisoft	✓ Clean
eScan	✓ Clean	ESET-NOD32	✓ Clean
F-Prot	✓ Clean	Fortinet	✓ Clean

VirusTotal scan results of the encrypted and code signed payload.



EXE

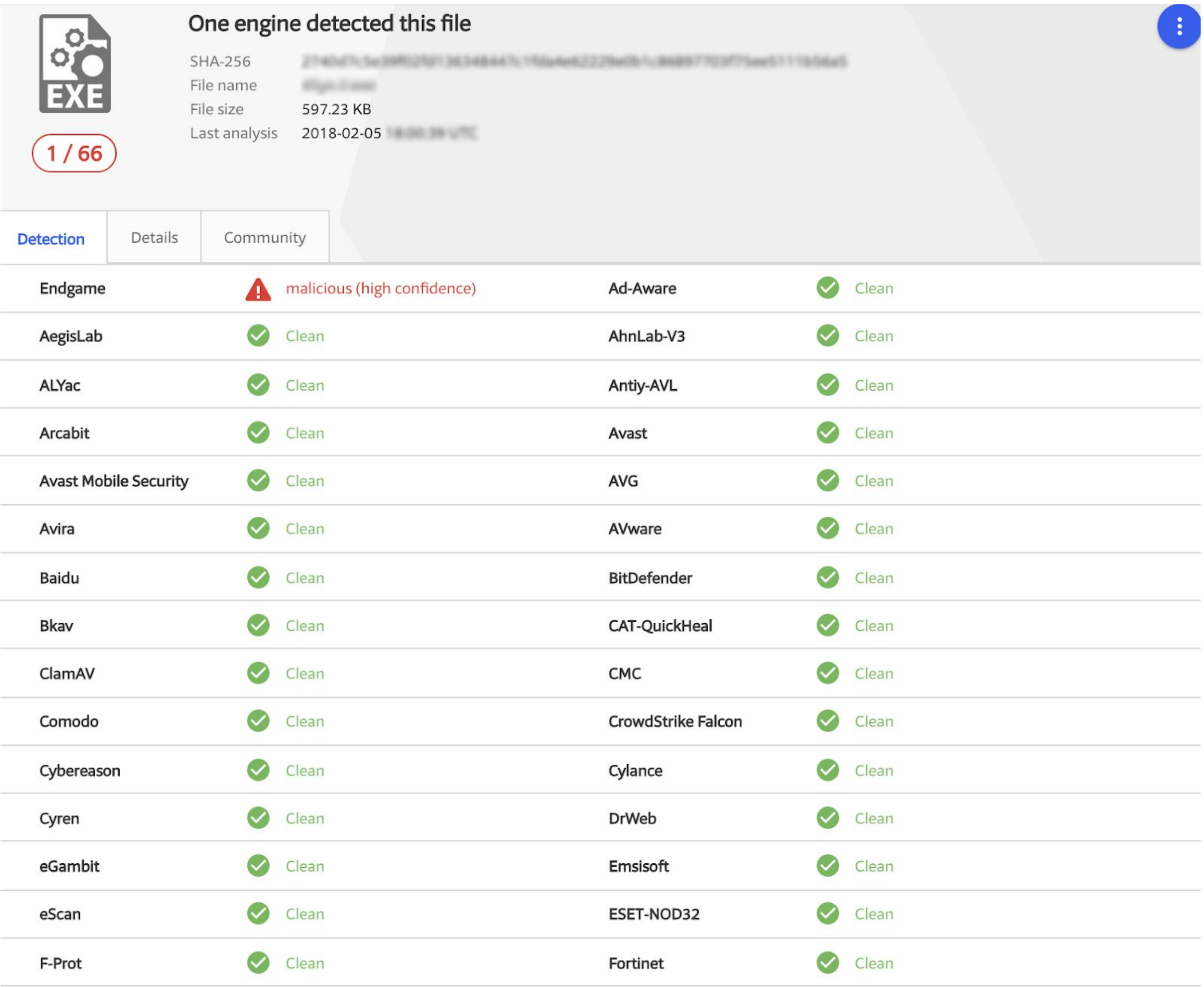
6 / 66

6 engines detected this file

SHA-256	[redacted]
File name	[redacted]
File size	592 KB
Last analysis	2018-02-05 [redacted]

CrowdStrike Falcon	⚠ malicious_confidence_90% (D)	Cybereason	⚠ malicious.42b2ff
Endgame	⚠ malicious (high confidence)	Qihoo-360	⚠ HEUR/QVM20.1.0201.Malware.Gen
SentinelOne	⚠ static engine - malicious	Tencent	⚠ Suspicious.Heuristic.Gen.b.0
Ad-Aware	✓ Clean	AegisLab	✓ Clean
AhnLab-V3	✓ Clean	ALYac	✓ Clean
Antiy-AVL	✓ Clean	Arcabit	✓ Clean
Avast	✓ Clean	Avast Mobile Security	✓ Clean
AVG	✓ Clean	Avira	✓ Clean
AVware	✓ Clean	Baidu	✓ Clean
BitDefender	✓ Clean	Bkav	✓ Clean
CAT-QuickHeal	✓ Clean	ClamAV	✓ Clean
CMC	✓ Clean	Comodo	✓ Clean
Cylance	✓ Clean	Cyren	✓ Clean
DrWeb	✓ Clean	eGambit	✓ Clean
Emsisoft	✓ Clean	eScan	✓ Clean

VirusTotal scan results of the encrypted non-resident payload.



One engine detected this file

1 / 66

SHA-256 [redacted]
File name [redacted]
File size 597.23 KB
Last analysis 2018-02-05 [redacted]

Endgame	⚠ malicious (high confidence)	Ad-Aware	✓ Clean
AegisLab	✓ Clean	AhnLab-V3	✓ Clean
ALYac	✓ Clean	Antiy-AVL	✓ Clean
Arcabit	✓ Clean	Avast	✓ Clean
Avast Mobile Security	✓ Clean	AVG	✓ Clean
Avira	✓ Clean	AVware	✓ Clean
Baidu	✓ Clean	BitDefender	✓ Clean
Bkav	✓ Clean	CAT-QuickHeal	✓ Clean
ClamAV	✓ Clean	CMC	✓ Clean
Comodo	✓ Clean	CrowdStrike Falcon	✓ Clean
Cybereason	✓ Clean	Cylance	✓ Clean
Cyren	✓ Clean	DrWeb	✓ Clean
eGambit	✓ Clean	Emsisoft	✓ Clean
eScan	✓ Clean	ESET-NOD32	✓ Clean
F-Prot	✓ Clean	Fortinet	✓ Clean

VirusTotal scan results of the encrypted and code signed non-resident payload.

About Recorded Future

Recorded Future arms security teams with the only complete threat intelligence solution powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context in real time and packaged for human analysis or integration with security technologies.