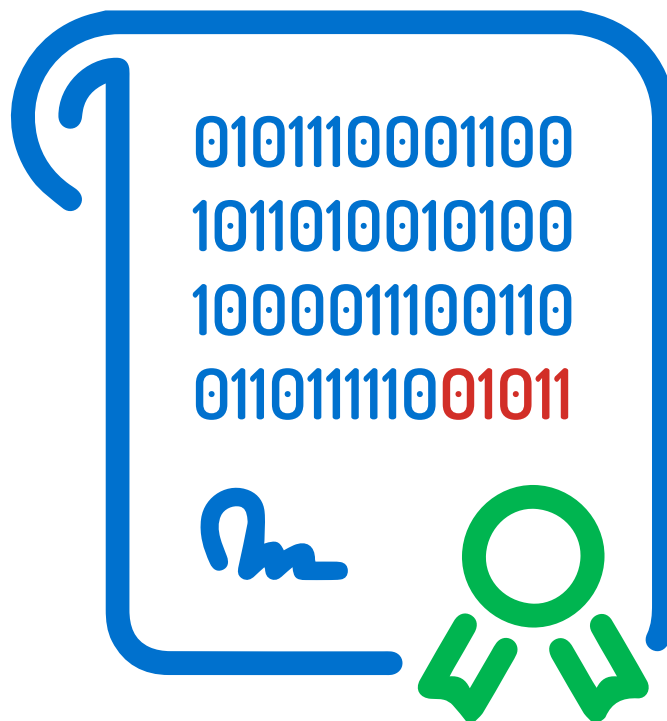



The Use of Counterfeit Code Signing Certificates Is on the Rise

By Andrei Barysevich
Recorded Future



CYBER THREAT ANALYSIS

Appendix A (Screenshots)



8 / 65

8 engines detected this file

SHA-256 337548bc701122b4407137ae7f08bc11a48424e1829c728177a115a48975748b1552

File name @msd402_04_0111.exe

File size 598.5 KB

Last analysis 2018-02-04 21:12:14 UTC

⋮

Detection


Details

Community

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.

CYBER THREAT ANALYSIS



2 / 65


2 engines detected this file

SHA-256 6480220e4b8f1880a3715a2d84088748f9a4747742a2137af2300f74b44675228f

File name 5d9y24d.exe

File size 603.69 KB

Last analysis 2018-02-04 11:21:01 UTC



Detection


Details

Community

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.

CYBER THREAT ANALYSIS



6 / 66


6 engines detected this file

SHA-256 e17714f8b0754386271486c343776c94a4d733d48890885489012a1774d992b147

File name 8fgh76c.exe

File size 592 KB

Last analysis 2018-02-05 17:58:48 UTC



Detection


Details

Community

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.

CYBER THREAT ANALYSIS



1 / 66


One engine detected this file

SHA-256 27f66d7c5e28f527e136348447c115b446222940b1c86897702f73e6d1115164e5

File name Rtgn.exe

File size 597.23 KB

Last analysis 2018-02-05 18:00:38 UTC



Detection

Details

Community

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.