BLOGS & STORIES

SpiderLabs Blog

Attracting more than a half-million annual readers, this is the security community's go-to destination for technical breakdowns of the latest threats, critical vulnerability disclosures and cutting-edge research.

GoldenSpy Chapter 5 : Multiple GoldenSpy Uninstaller Variants Discovered

August 17, 2020 Reegun Jayapaul

Summary:

Trustwave identified a significant malicious campaign on mandatory tax invoice software, which is required to conduct business in China. The campaign, we dubbed GoldenSpy, is an embedded backdoor in the software package, which allows full remote command and control of the victim's system via arbitrary code execution.

After GoldenSpy was made public, those behind the backdoor quickly scrambled to push an uninstaller to erase GoldenSpy from infected systems. The uninstaller was dropped from an updater module, cleaned GoldenSpy and finally deleted itself leaving no traces. Another uninstaller was issued right afterwards specifically designed to evade our YARA rules we published to help infected.

Understanding the attackers were watching our every move to help organizations impacted by GoldenSpy, we waited a period-of-time and quietly kept tracking with our threat hunting strategy. What we found is that they are continuing to push new GoldenSpy uninstallers – so far we have discovered five variants totaling 24 uninstaller files.

We observed some of the uninstallers were uploaded to public repositories causing the detection ratios to increase. Some of the uninstallers not found in any public repo's, however, we will report all of them here.

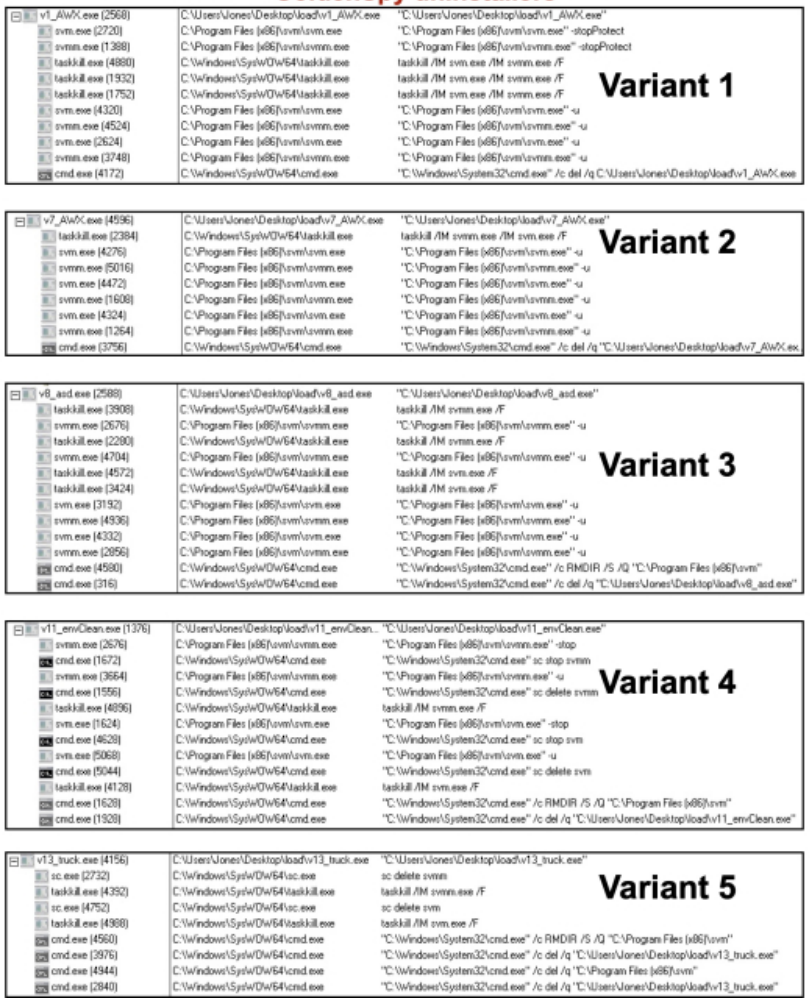
Analysis:

All the variants conducted the exact same behaviour, but utilized different execution flow, string obfuscation, and size to evade detection by security technologies. Detailed analysis of the behaviour is available in GoldenSpy Chapter 2.

- Stop the svm, svmm services
- Stop the svm,svmm process
- Uninstall the svm,svmm modules
- Remove the SVM installed folder including logs
- Remove the uninstaller (Self-delete)
- Specifically checks for process 'ZhuDongFangYu.exe,' which is a China-based antivirus 'Qihoo 360' active defense module

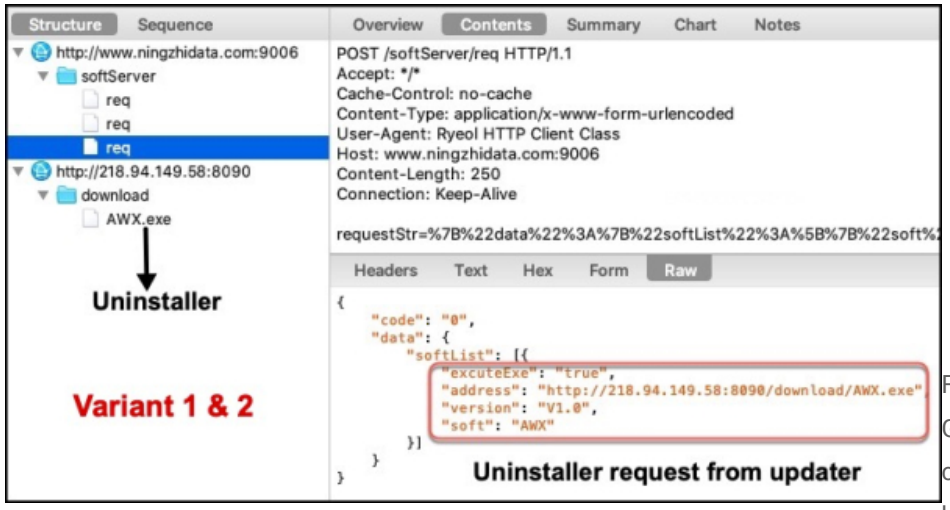
Execution flow :

GoldenSpy uninstallers



Variant 1		
v1_AWX.exe [2568]	C:\Users\Jones\Desktop\load\v1_AWX.exe	"C:\Users\Jones\Desktop\load\v1_AWX.exe"
svm.exe [2720]	C:\Program Files (x86)\svm\svm.exe	"C:\Program Files (x86)\svm\svm.exe" -stopProtect
svmm.exe [1388]	C:\Program Files (x86)\svm\svmm.exe	"C:\Program Files (x86)\svm\svmm.exe" -stopProtect
taskkill.exe [4880]	C:\Windows\SysWOW64\taskkill.exe	taskkill /IM svm.exe /IM svmm.exe /F
taskkill.exe [1932]	C:\Windows\SysWOW64\taskkill.exe	taskkill /IM svm.exe /IM svmm.exe /F
taskkill.exe [1752]	C:\Windows\SysWOW64\taskkill.exe	taskkill /IM svm.exe /IM svmm.exe /F
svm.exe [4320]	C:\Program Files (x86)\svm\svm.exe	"C:\Program Files (x86)\svm\svm.exe" -u
svmm.exe [4524]	C:\Program Files (x86)\svm\svmm.exe	"C:\Program Files (x86)\svm\svmm.exe" -u
svm.exe [2624]	C:\Program Files (x86)\svm\svm.exe	"C:\Program Files (x86)\svm\svm.exe" -u
svmm.exe [3748]	C:\Program Files (x86)\svm\svmm.exe	"C:\Program Files (x86)\svm\svmm.exe" -u
cmd.exe [4172]	C:\Windows\SysWOW64\cmd.exe	"C:\Windows\System32\cmd.exe" /c del /q C:\Users\Jones\Desktop\load\v1_AWX.exe
Variant 2		
v7_AWX.exe [4596]	C:\Users\Jones\Desktop\load\v7_AWX.exe	"C:\Users\Jones\Desktop\load\v7_AWX.exe"
taskkill.exe [2384]	C:\Windows\SysWOW64\taskkill.exe	taskkill /IM svmm.exe /IM svm.exe /F
svm.exe [4276]	C:\Program Files (x86)\svm\svm.exe	"C:\Program Files (x86)\svm\svm.exe" -u
svmm.exe [5016]	C:\Program Files (x86)\svm\svmm.exe	"C:\Program Files (x86)\svm\svmm.exe" -u
svm.exe [4472]	C:\Program Files (x86)\svm\svm.exe	"C:\Program Files (x86)\svm\svm.exe" -u
svmm.exe [1608]	C:\Program Files (x86)\svm\svmm.exe	"C:\Program Files (x86)\svm\svmm.exe" -u
svm.exe [4324]	C:\Program Files (x86)\svm\svm.exe	"C:\Program Files (x86)\svm\svm.exe" -u
svmm.exe [1264]	C:\Program Files (x86)\svm\svmm.exe	"C:\Program Files (x86)\svm\svmm.exe" -u
cmd.exe [3756]	C:\Windows\SysWOW64\cmd.exe	"C:\Windows\System32\cmd.exe" /c del /q "C:\Users\Jones\Desktop\load\v7_AWX.ex
Variant 3		
v8_asd.exe [2588]	C:\Users\Jones\Desktop\load\v8_asd.exe	"C:\Users\Jones\Desktop\load\v8_asd.exe"
taskkill.exe [3908]	C:\Windows\SysWOW64\taskkill.exe	taskkill /IM svmm.exe /F
svmm.exe [2676]	C:\Program Files (x86)\svm\svmm.exe	"C:\Program Files (x86)\svm\svmm.exe" -u
taskkill.exe [2280]	C:\Windows\SysWOW64\taskkill.exe	taskkill /IM svmm.exe /F
svmm.exe [4704]	C:\Program Files (x86)\svm\svmm.exe	"C:\Program Files (x86)\svm\svmm.exe" -u
taskkill.exe [4572]	C:\Windows\SysWOW64\taskkill.exe	taskkill /IM svm.exe /F
taskkill.exe [3424]	C:\Windows\SysWOW64\taskkill.exe	taskkill /IM svm.exe /F
svm.exe [3192]	C:\Program Files (x86)\svm\svm.exe	"C:\Program Files (x86)\svm\svm.exe" -u
svmm.exe [4936]	C:\Program Files (x86)\svm\svmm.exe	"C:\Program Files (x86)\svm\svmm.exe" -u
svm.exe [4332]	C:\Program Files (x86)\svm\svm.exe	"C:\Program Files (x86)\svm\svm.exe" -u
svmm.exe [2856]	C:\Program Files (x86)\svm\svmm.exe	"C:\Program Files (x86)\svm\svmm.exe" -u
cmd.exe [4580]	C:\Windows\SysWOW64\cmd.exe	"C:\Windows\System32\cmd.exe" /c RMDIR /S /Q "C:\Program Files (x86)\svm"
cmd.exe [316]	C:\Windows\SysWOW64\cmd.exe	"C:\Windows\System32\cmd.exe" /c del /q "C:\Users\Jones\Desktop\load\v8_asd.exe"
Variant 4		
v11_envClean.exe [1376]	C:\Users\Jones\Desktop\load\v11_envClean...	"C:\Users\Jones\Desktop\load\v11_envClean.exe"
svmm.exe [2676]	C:\Program Files (x86)\svm\svmm.exe	"C:\Program Files (x86)\svm\svmm.exe" -stop
cmd.exe [1672]	C:\Windows\SysWOW64\cmd.exe	"C:\Windows\System32\cmd.exe" sc stop svmm
svmm.exe [3664]	C:\Program Files (x86)\svm\svmm.exe	"C:\Program Files (x86)\svm\svmm.exe" -u
cmd.exe [1556]	C:\Windows\SysWOW64\cmd.exe	"C:\Windows\System32\cmd.exe" sc delete svmm
taskkill.exe [4896]	C:\Windows\SysWOW64\taskkill.exe	taskkill /IM svmm.exe /F
svm.exe [1624]	C:\Program Files (x86)\svm\svm.exe	"C:\Program Files (x86)\svm\svm.exe" -stop
cmd.exe [4628]	C:\Windows\SysWOW64\cmd.exe	"C:\Windows\System32\cmd.exe" sc stop svm
svm.exe [5068]	C:\Program Files (x86)\svm\svm.exe	"C:\Program Files (x86)\svm\svm.exe" -u
cmd.exe [5044]	C:\Windows\SysWOW64\cmd.exe	"C:\Windows\System32\cmd.exe" sc delete svm
taskkill.exe [4128]	C:\Windows\SysWOW64\taskkill.exe	taskkill /IM svm.exe /F
cmd.exe [1628]	C:\Windows\SysWOW64\cmd.exe	"C:\Windows\System32\cmd.exe" /c RMDIR /S /Q "C:\Program Files (x86)\svm"
cmd.exe [1928]	C:\Windows\SysWOW64\cmd.exe	"C:\Windows\System32\cmd.exe" /c del /q "C:\Users\Jones\Desktop\load\v11_envClean.exe"
Variant 5		
v13_truck.exe [4156]	C:\Users\Jones\Desktop\load\v13_truck.exe	"C:\Users\Jones\Desktop\load\v13_truck.exe"
sc.exe [2732]	C:\Windows\SysWOW64\sc.exe	sc delete svmm
taskkill.exe [4392]	C:\Windows\SysWOW64\taskkill.exe	taskkill /IM svmm.exe /F
sc.exe [4752]	C:\Windows\SysWOW64\sc.exe	sc delete svm
taskkill.exe [4988]	C:\Windows\SysWOW64\taskkill.exe	taskkill /IM svm.exe /F
cmd.exe [4560]	C:\Windows\SysWOW64\cmd.exe	"C:\Windows\System32\cmd.exe" /c RMDIR /S /Q "C:\Program Files (x86)\svm"
cmd.exe [3976]	C:\Windows\SysWOW64\cmd.exe	"C:\Windows\System32\cmd.exe" /c del /q "C:\Users\Jones\Desktop\load\v13_truck.exe"
cmd.exe [4944]	C:\Windows\SysWOW64\cmd.exe	"C:\Windows\System32\cmd.exe" /c del /q "C:\Program Files (x86)\svm"
cmd.exe [2840]	C:\Windows\SysWOW64\cmd.exe	"C:\Windows\System32\cmd.exe" /c del /q "C:\Users\Jones\Desktop\load\v13_truck.exe"

Traffic Flow:



From variant 3, after the GoldenSpy uninstaller clears its traces and before it self-delete, it will send a unique ID to ningzhidata[.]com to track the activity.

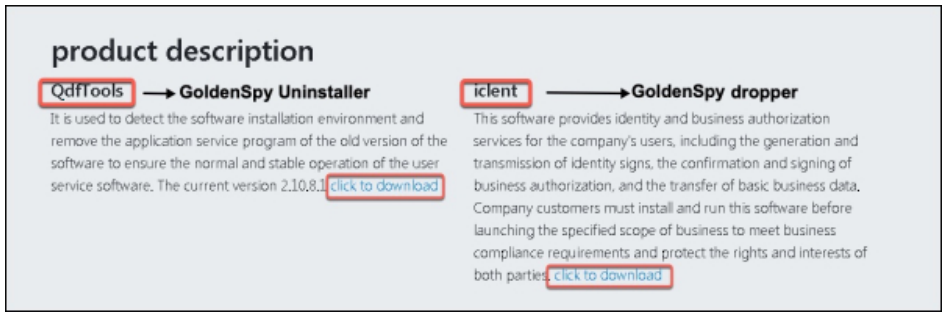
Who is behind the GoldenSpy uninstaller development?

During reverse engineering a file from variant 5, We have observed the IP 39[.]98[.]110[.]234 was used for 3rd stage beacon as mentioned above, and as per the traffic, it does the same.

We checked the above IP, It resolves to 'Ningbo Digital Technology Co., Ltd' hxxp[://]www[.]nbdigit[.]com/

As stated in the description below, they provide professional software solutions and technical support.

From the active website, they are providing two files to download, The ‘QdfTools’ name is not relevant as it is actually the ‘GoldenSpy Uninstaller’ and ‘iclient’ is a ‘GoldenSpy’ dropper, which we identified as svminstaller in the GoldenSpy technical report.



hxxp[://]www[.]nbdigit[.]com/download/QdfTools[.]exe

hxxp[://]www[.]nbdigit [.]com/download/iclient[.]exe

From variant 5, The GoldenSpy uninstaller got downloaded with name 'QdfTools.exe' from 222[.]186[.]130[.]200:9006, They gave the product description for the uninstaller as 'Enterprise service environment detection and cleaning software.'

Based on these findings, we can say that Ningbo Digital Technology Co., Ltd is involved with the development of the 'GoldenSpy Uninstaller' and ningzhidata[.]com serving from CDN servers.

Our GoldenSpy YARA rule successfully detected the 'iclient.exe.'

Traffic comparisons:

Variant	Updater URL	Uninstaller download URL
1	hxxp[://]www[.]ningzhidata[.]com:9006	223[.]112[.]21[.]2:8090
2	hxxp[://]www[.]ningzhidata[.]com:9006	218[.]94[.]149[.]58:8090
3	hxxp[://]www[.]ningzhidata[.]com:9006	120[.]53[.]238[.]96:8090
4	hxxp[://]www[.]ningzhidata[.]com:9006	120[.]53[.]238[.]96:8090
5	hxxp[://]www[.]ningzhidata[.]com:9006	222[.]186[.]130[.]200:9006

GoldenSpy Uninstaller Variant's Indicators of compromise:

Binaries:

FileName	FileSize	TimeStamp GMT	MD5
AWX.exe	20 kB	2020:06:28 16:15:19+00:00	735ac19b261dc66d5850bea21f3d54fe

BWXT.exe	25 kB	2020:06:29 10:38:38+00:00	f2a7363cf43b5900bb872b0d4c627a48
yund.exe	23 kB	2020:06:30 03:47:50+00:00	f52cc72959e7ed51c75d0b7f6b8611c0
yund.exe	25 kB	2020:07:01 12:03:45+00:00	08f803140ee607a12b15dca97df5864f
AWX.exe	26 kB	2020:07:01 15:52:46+00:00	573adb1569a08472094f0cfbb6264360
AWX.exe	26 kB	2020:07:02 01:18:11+00:00	429a1c5756efaab8af3bcee37cccc31f
ac9253	76 kB	2020:07:05 04:34:37+00:00	ddd85c9c8ec325bc2accce4365cb40de
AWX.exe	84 kB	2020:07:05 10:11:57+00:00	eb98b268164e405ba761eee87565d936
dfed	80 kB	2020:07:05 14:09:20+00:00	cc37004f5a1903523657810edb45272e
7b15	76 kB	2020:07:06 17:21:10+00:00	72cd43dc5ad0e55f6d26998ac62645e0
asd.exe	88 kB	2020:07:07 04:21:10+00:00	568042d040ed7fbbb802d847ef614a4d
d29f78	84 kB	2020:07:08 08:10:03+00:00	ed9ec3aec2e8aac13e5d3971f0d56d89
a9a61	84 kB	2020:07:08 10:00:00+00:00	a07ebcc316c49c6bbdf0a8d91bf4c546
953ce	81 kB	2020:07:08 10:37:33+00:00	c8342bbfadc6fb78ea00480e3f8d66e8
asd.exe	84 kB	2020:07:08 10:37:33+00:00	a4e39f608731d31fbcc17d98a3ec8508
iclient.exe	624 kB	2020:07:08 11:01:15+00:00	ab43e4815f1f6cf6d4ef1f7a5334d1ac
asd.exe	88 kB	2020:07:08 14:05:47+00:00	ba7cce6da078c2825b05ee305773edb6
63163	88 kB	2020:07:09 01:19:07+00:00	1484a597aee4850fcf13faac8f382a5c
82fb179	88 kB	2020:07:09 01:46:52+00:00	57af01112f6e277c69150f6d5fba51a9
envClean.exe	80 kB	2020:07:10 01:25:06+00:00	89e0b5e36a384eba8fb269b1da587f09
envClean.exe	80 kB	2020:07:10 01:35:08+00:00	aa3bc5d04e4daaa641dad4a16dba3df9

truck.exe	72 kB	2020:07:13 13:41:44+00:00	7fed28a7623fe421a732d538e87189f4
TrueQdf.exe	80 kB	2020:07:22 11:41:03+00:00	037fa9c57f9f9c62f12927fe44761408
QdfTools.exe	84 kB	2020:07:23 05:45:07+00:00	98818a0b268419a1ea652dd95d9437e1
QdfTools.exe	84 kB	2020:07:25 04:23:05+00:00	3500ee24b14f7c203a360442b680a1d7

Network:

URL's & IP's
hxxp[://]www[.]ningzhidata[.]com:9006
hxxp://222[.]186[.]130[.]200:9006/download/
hxxp://223[.]112[.]21[.]2:8090/download/
hxxp://218[.]94[.]149[.]58:8090/download/
hxxp://120[.]53[.]238[.]96:8090/download/
hxxp://39[.]98[.]110[.]234:8111/download/
223[.]112[.]21[.]2:8090
218[.]94[.]149[.]58:8090
120[.]53[.]238[.]96:8090
222[.]186[.]130[.]200:9006
39[.]98[.]110[.]234:8111
hxxp[://]www[.]nbdigit[.]com/download/QdfTools[.]exe
hxxp[://]www[.]nbdigit[.]com/download/iclient[.]exe

ATT&CK Mappings:

Tactic	Technique
Discovery	File and Directory Discovery [T1083]
	Process Discovery [T1057]
	Query Registry [T1012]
	System Information Discovery [T1082]
Defense Evasion	Virtualization/Sandbox Evasion [T1497]

YARA:

```
rule Goldenspy_Uninstaller

{

meta:

        author = "SpiderLabs"

        malware_family = "GoldenSpy"

        filetype =  "exe_dll"

        version = "4.0"

strings:

        $str1 = "taskkill /IM svm.exe /IM svmm.exe /F" ascii

        $str2 = "\\svm.exe -stopProtect" ascii

        $str3 = "\\svmm.exe -u" ascii

        $str4 = "\\VCProject\\dgs\\Release\\" ascii

        $str5 = "Software\\Microsoft\\Windows\\CurrentVersion\\Uninstall\\svm" ascii
```

```
        $str6 = "\\svmm.exe -stopProtect" ascii

        $str7 = "\\svm.exe -u" ascii

        $str8 = "Software\\Microsoft\\Windows\\CurrentVersion\\App Paths\\svm.exe" ascii

        $str9 = "dGFza2tpbGwgL0lNIHN2bS5leGUgL0lNIHN2bW0uZXhlIC9GIA" ascii

        $str10 = "c3ZtLmV4ZSAtc3RvcFByb3RlY3Q" ascii

        $str11 = "XHN2bW0uZXhlIC11" ascii

        $str12 = "U29mdHdhcmVcTWljcm9zb2Z0XFdpbmRvd3NcQ3VycmVudFZlcnNpb25cVW5pbnN0YWxsXHN2bQ"
ascii

        $str13 =
"U29mdHdhcmVcTWljcm9zb2Z0XFdpbmRvd3NcQ3VycmVudFZlcnNpb25cQXBwIFBhdGhzXHN2bS5leGU" ascii

        $str14 = "XHN2bS5leGUgLXU" ascii

        $str15 = "c3ZtbS5leGUgLXN0b3BQcm90ZWN0" ascii

        $str16 = {4951538BCEE8[0-10]8D4C2424[0-10]8D44243C[0-4]68[0-20]83C4088B5004C644247404}

        $str17 = {535556578D4C2414[0-10]8D44242C68[0-10]50C744247C[0-10]83C4088B7004C64424[0-
50]8BFE83C9FF33C0}

condition:

        (uint16(0) == 0x5A4D) and 4 of ($str*)

}
```

This research depicting regular improvements of the GoldenSpy uninstaller should serve as a wakeup call for organizations because it proves any actions including implanting and extracting malware can be taken covertly and at the will of the attacker with the help of the updater module without impacting the functionality of the Golden Tax software.

Trustwave strongly recommends following best software practices when comes to 3rd party software installations. No matter where an organization operates, extra vigilance needs to be taken when adopting

mandatory software (or any 3rd party software) in order to conduct business. GoldenSpy and what we have seen in terms of its continuous activities is a prime example.

Recent SpiderLabs Blog Posts

SpiderLabs Blog

Aug 24, 2020

RATs and Spam: The Node.JS QRAT

SPIDERLABS BLOG

SpiderLabs Blog

Aug 21, 2020

SpiderLabs Capture the Flag 2020 Results

SPIDERLABS BLOG

SpiderLabs Blog

Aug 20, 2020

IBM Db2 Shared Memory Vulnerability (CVE-2020-4414)

SPIDERLABS BLOG

Trustwave®

SERVICES

Managed Security
Security Testing
Technology
Consulting
Education

CAPABILITIES

By Topic
By Industry
By Mandate

RESOURCES

Blogs & Stories
Resource Library
Security Resources
Events & Webinars

COMPANY

About Trustwave
Careers
Newsroom
Contact
Support

STAY INFORMED

Sign up to receive the latest security news and trends from Trustwave.

email@example.com SUBSCRIBE

No spam, unsubscribe at any time.

LEGAL TERMS OF USE PRIVACY POLICY ENGLISH