INFORMATION VOM BfV & BKA

004/20, 25.08.2020

Mögliche Cyberspionage mittels der Schadsoftware GOLDENSPY

Hintergrund

Der Cyberabwehr des Bundesamtes für Verfassungsschutz (BfV) sowie dem Bundeskriminalamt (BKA) liegen Erkenntnisse vor, dass deutsche Unternehmen mit Sitz in China möglicherweise mittels der Schadsoftware GOLDENSPY ausgespäht werden. Ziel dieser gemeinsamen Warnmeldung ist es, deutsche Wirtschaftsunternehmen zu sensibilisieren und mit den notwendigen technischen Informationen zu versehen, um eine mögliche Infektion detektieren zu können.

Sachverhalt/ Erkenntnisse

IT-Sicherheitsdienstleister[1] sowie das FBI[2] berichten über folgenden Sachverhalt:
Ausländische Unternehmen, die in China aktiv sind, sind verpflichtet eine Steuersoftware[3] zu installieren, um automatisiert und softwaregestützt Steuerabgaben an das zuständige Finanzamt abzuführen sowie Finanztransaktionen abzuwickeln.[4] Dabei soll es sich um die legitime chinesische Steuersoftware INTELLIGENT TAX (auch GOLDENTAX genannt) handeln. Durch die Installation dieser legitimen Software soll jedoch eine Spionagesoftware mit dem Namen GOLDENSPY nachgeladen werden, durch die Dritte Zugriff auf die Netzwerke der betroffenen Unternehmen erlangen.

Durch BfV und BKA wurden die bekannten technischen Parameter zusammengetragen und um eigene Erkenntnisse ergänzt. Diese werden mit dieser Warnmeldung zum Schutz deutscher Wirtschaftsunternehmen zur Verfügung gestellt.

---

[1] www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/the-golden-tax-department-and-the-emergenceof-goldenspy-malware/

[2] www.ic3.gov/media/news/2020/200728.pdf

[3] Im Sinne einer Finanzverwaltungssoftware zur Abwicklung der Steuerabfuhr an das zuständige Finanzamt.

[4] Anbieter solcher Software sind derzeit nur die Unternehmen AISINO INFORMATION CO und BAIWANG. Über die BAIWANG Edition wurde mutmaßlich 2018-2019 in ähnlicher Vorgehensweise die Schadsoftware GOLDENHELPER verteilt.

ASW Bundesverband | Allianz für Sicherheit in der Wirtschaft e.V.
Bayerischer Platz 6 | 10779 Berlin
Telefon +49 (0)30 246 37 175 | Telefax +49 (0)30 200 77 056
info@asw-bundesverband.de | www.asw-bundesverband.de

Mutmaßliche Funktionsweisen der Schadsoftware

Gemäß den Erkenntnissen von IT-Dienstleistern kann nach Ausführung der legitimen Steuersoftware die zusätzliche Datei **plugins.exe** ausgeführt und dadurch automatisiert und ohne Mitteilung an den Nutzer nach ca. zwei Stunden die GOLDENSPY-Software im betroffenen System nachgeladen und installiert werden. Dadurch könnten Dritte vollumfängliche Zugriffsmöglichkeiten inklusive Administratorenrechte erhalten. Durch die Installation von GOLDENSPY wird eine weitere Datei mit der Bezeichnung **svminstaller.exe** nachgeladen, die zwei identische .exe-Dateien mit der Bezeichnung **svm.exe** und **svmm.exe** im Opfersystem installiert (dabei handelt es sich um zwei identische Versionen von GOLDENSPY), welche von der Domain **ningzhidata[.]com** übertragen werden. Die beiden Dateien weisen die folgenden Backdoor-Fähigkeiten auf:

- Beide Dateien werden als Autostart Services installiert, die sich - sollte einer der beiden Services beendet werden - gegenseitig neu starten. Wird eine der beiden Dateien gelöscht, wird eine neue Version nachgeladen und ausgeführt, was die Entfernung der Malware von einem infizierten System aufgrund der zusätzlichen Nutzung von Administratorenrechten erschwert.
- Durch die Deinstallationsfunktion der INTELLIGENT TAX-Software wird GOLDENSPY nicht deinstalliert.
- GOLDENSPY wird erst ca. zwei Stunden nach Abschluss der Installation der Steuersoftware heruntergeladen und installiert, ohne Benachrichtigung auf dem System des Opfers. Nach Ausführung nimmt die Software Kontakt mit einem Server auf, der nicht zur offiziellen Steuersoftware gehört.
- Nach den ersten Versuchen, den C2-Server zu kontaktieren, werden die Beacon-Zeiten nach dem Zufallsprinzip gesetzt, was eine Identifikation als typische Beaconing-Malware erschwert.

Uninstall GOLDENSPY

Bereits kurz nach Bekanntwerden der Vorfälle und der Schadsoftware GOLDENSPY wurde ein weiteres Tool an betroffene Unternehmen ausgeliefert, wodurch GOLDENSPY mittels der Datei **AWX.exe** vollständig vom Opfersystem entfernt wird. Zu den Funktionsweisen gehören u. a. das Löschen von Registry-Einträgen sowie LogFiles. Nach erfolgreicher Bereinigung entfernt sich das Tool ebenfalls selbstständig vom betroffenen System. Da bereits mehrere IT-Sicherheitslösungen die **AWX.exe** als maliziös erkennen, wurde hier eine weiterentwickelte Version (**BWXT.exe**) in Umlauf gebracht. Die bereits beschriebenen Funktionsweisen wurden beibehalten.

Handlungsempfehlung

Grundsätzlich Risikoabwägung und Prävention
Zwecks Erreichung eines angemessenen IT-Sicherheitsniveaus wird grundsätzlich eine Orientierung an öffentlich verfügbaren Standards empfohlen, etwa den Richtlinien des BSI-Grundschutzes oder den praxisbewährten CIS Controls des Centers for Internet Security.
Für den Einsatz von Software oder Systemen, welche zur Erfüllung von rechtlichen Vorgaben in anderen Ländern zwingend genutzt werden müssen, wird empfohlen, diese nicht in die Domäne zu integrieren, sondern diese – soweit möglich – von kritischen Unternehmensnetzen getrennt zu betreiben. Auf diesen Systemen sollten nur die für die Erfüllung der rechtlichen Vorgaben benötigten Daten verarbeitet werden. Nicht mehr benötigte Daten sollten regelmäßig von diesen Systemen gelöscht werden. Verwendete Zugangsdaten sollten exklusiv genutzt und nicht an anderer Stelle weiterverwendet werden.

ASW Bundesverband | Allianz für Sicherheit in der Wirtschaft e.V.
Bayerischer Platz 6 | 10779 Berlin
Telefon +49 (0) 30 246 37 175 | Telefax +49 (0)30 200 77 056
info@asw-bundesverband.de | www.asw-bundesverband.de

Detektion
Es wird empfohlen, die eigenen Systeme mit den zur Verfügung gestellten IOCs und Detektionssignaturen zu prüfen. Insbesondere sollte in Logdateien und aktiven Netzwerkverbindungen nach Verbindungen zu den im Bereich IOCs genannten externen Systemen gesucht werden. Außerdem sollte in den Windows-Eventlogs nach der Erstellung von Services mit den Namen svm oder svmm gesucht werden.
Die beigefügte YARA-Regel kann ebenfalls zur Detektion genutzt werden.

Reaktion
Bei Hinweisen auf eine Infektion bzw. verdächtiges Systemverhalten sollten die erprobten Pläne für Incident Response ausgeführt werden, um das Ausmaß einer etwaigen Kompromittierung zu erfassen, einzudämmen und effektiv begegnen zu können. Systeme, auf denen verdächtige Software installiert war, sollten auch ohne Hinweise auf eine aktive Infektion, unter Berücksichtigung der im Bereich Prävention genannten Empfehlungen, neu aufgesetzt werden. Darüber hinaus bieten wir Ihnen zusätzliche Hintergrundinformationen an. Hierzu stehen wir Ihnen unter folgenden Kontaktdaten gerne zur Verfügung:
Bundesamt für Verfassungsschutz – Cyberabwehr
Tel.: 0221-792-2600 oder
E-Mail: cyberabwehr@bfv.bund.de

Bundeskriminalamt
Tel.: 02225-890 oder
E-Mail: st23@bka.bund.de

Detektionsregel
YARA-Regel „GOLDENSPY“ – zur Erkennung verschiedener Varianten der Malware „GOLDENSPY“

```
rule goldenspy
{
meta:
description = "detects variants of GoldenSpy Malware"
strings:
$str01 = {c78510ffffff00000000 c78514ffffff0f000000 c68500ffffff00 c78528ffffff00000000
c7852cffffff0f000000 c68518ffffff00 c78540ffffff00000000 c78544ffffff0f000000 c68530ffffff00
c645fc14 80bd04fefff00}
$str02 = "Ryeol HTTP Client Class" ascii
$str03 = "----RYEOL-FB3B405B7EAE495aB0C0295C54D4E096-" ascii
$str04 = "SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\App Paths\\fwkp.exe" ascii
$str05 = "svmm" ascii
$str06 = "PROTOCOL_" ascii
$str07 = "softList" ascii
$str08 = "excuteExe" asci
condition:
(uint16(0) == 0x5A4D) and 5 of ($str*)
}
```

Indicators of Compromise

GoldenSpy - Samples

SHA-256	SHA-1	MD5
285714ff750fe1b3343593b2efb7fc3e8229e755c128759faedc5654deae879a	21045213f9ed383467ca9596107fe6df96fcc845	42117d18cd9f8597533fee5ad530564f
e41102043cfb9279cf1aafa89de7336a5d94fcfd0217eb590b36d119bbfaaa0f	a88fa1e8854d30fd6ce07ba13ce0cbc727f5bf60	c75b885ac2e07a827c5d962795db1a79
843d996888de1201acb028e45c3a36102ae53a6b97428a79097cd9756f85dd62	02a21954127161abc0ca774974205a3cc3c36fd0	56aa403f0de4fdc9250169ee0e69d3c5
f16c756e3bebd76d0c2ca1e73b4539a36fde97afdbb4591c7fac8f0db1492d45	143f76186977ba4f9b3035b959099bd1f56fc839	5307058b4335f14bf703f832e96b52f2
b6982fe4ab882cfdcba091c6617b9d279a9bcfd3e28a76d5fb2c0cdfc0c23064	eec54b7a3921ed35e4709c6f1fdcaf3bf1ce080f	126599da0c79ce196c960d0ba28aacda
68472c7468b931dbbea1900bdeb4dcf10bdbfe1384e0984f4272f1a036659202	49971c535f462aed0aed6843c9d2d08ff8b1f688	27fc849f5ba788646b2d18ca3c22b36b
6366f009e4c0303d7f5ba0bb6a529039618ff8715972713c3b6645d1aef3d4c1	b6c271e1089df84f7b7e4b180f357b392b6d11b8	665fe1f5536f63244ca805325fdf058d
ce3d64f8ad4dcbbf5324e05c81a716c5d2493e149edafbc5cb73c01836bea5f2	6dc1b20996b36e9dfc1edaaec880b6efd8151012	8497a9301e74d3611c2df3e3c0ea24f4
862115c6d8d6e6addeb408c45ac0a7f8a25126d5ccca6d9356143a7a683c009d	4f34ad31da6bf36e82f4bdcfe512cef415159d82	7bc6b5c6da04a231f5fa011944ce5a31
c9d1ec32df1b134aa809bc8b3ad475b690347294693f6c5b65ab1df94fa4d1fd	f9b3fc5bb99e5096fc90b099350cebdf8734d47a	777571fb7528c1baa00282bcfdcc9dab
7bf45c75dca3362331d5a9a116bf9c7a52e1352905a5dee66f0cf123acc461b2	7ba0231c556961ef9137da69936a371a12c2a01d	eb1c4f73efdedd8cd2ed29203efc3341
67316d574d0e05549bf314b4764842e2b598f2ffae1ac82123b3dd592f605751	525473d5f59925412d2587693bfb9d4647027c48	fb1da3f1747ee138c19ac4d423b87595
d41081969a212dec0ca623d848fb51907d8cdb1cb7bd86e1354e3041052858fb	484d2e4d31a0c0a5ce5a2b2525677baa277c8a2c	cf640636f3d85586607c20813884ff4a
afe2bcd5cb2de6349329c42631bfbbdba46d672f6dc515a5bee63cb4265e49f8	159b73c842e94e5628d5e003dafecb3642b4dea0	d11e8433a7df33b9bf51f926102b5bd6
98b5320e7464fc69b12eb626b6336604efcbf6502adc38c77f6db41666da9dd1	f2c7f4d0c5dd576a421f521671c68ff9aac8288d	77b8787a1bcda6e18c42c1855d2f1fa0
f89e898ea40e10901c0c9f9100f269a227323ace1f7248293bfd57982dea1a67	8d07cbd90527568c90f6cb481a1a21853c8b2524	72c7004537cd158b0d80f07d65e71f6b
853ef8130b50e9fce5f7575afc04374de0232fa5fe6b7b4d97fda7bf17ec58c9	8afb6eed2e9579ffb3d97f2ab2d48d612c4aaaa4	22bcafdae83948dce644884c880d16ee
39b914c8064becf3df1df39b0517bda05371e90b8b5fe15aad275faac634876f	7e4cebc4c1d5423a6d793a1bb5463f33e9801d4b	c2e51a827d684412a97a61ed5d02bcd7
8b0e1be70409238e7577429df3eaa84a6b12f36d9dbb6e47607f7fc354ddb961	105937de2ab6ba43193b9816f9d614bda02bac2c	c05f6510636fb660631aa60f505320fb
a8169c566bf4566c6c4ba98ce7f9ecf143ae6c21dc0d7b15779c936e1ff60269	1aa93b29564cfcdff0f3a29058906b08bf44ea1e	2c5557250cbd3f7ff3f778aa4fc6e479
55429a6085d50782be52bb2150cfabecfdaa4eb843350399c3cf88a9ab9fa4c1	0112f57944a20a60bf7cd7a0e2e655a65898db88	c21307b7bv2889e0318eb25dacfe4fcc
e8118cb2941c0421a2f6942919f8541b5fab348e2334102eab8654d2c4bff8ed	1db49878531a7071724c46cb5088ea7e0780ad0f	4c13e49c63063394250d43df1aeef78d
2878ad6d386bc3fd9f0625195a3a60fc5056ff7ff24e57cf466e54af07d0217e	0d0c3a9369f1be3e4e695177d31f6306dff3c94a	0750e344e12de0b653de4e7d600d00c2
af120f411c2c1f3ec52516006a25c734a5a0e4952c3eb942ad99858420c9135e	6fbf40e6e6f11afc0eced837ee7800e6eb50df46	3e241ee25be15c35e40a9140d2923625

a44e6b87dc1165c4c6839554dd412e98fade0a7e7c6341b9d44c0ee0dd034160	615e9744ea5526bc513a7672dabfedc14b8427ad	cce1df224e63ff1aab5f74e2fb1559e3
561f89c566af35a90ae19285177cedaae3a0cbd7c8d415c57766e7988503c686	539090149f36bdd74696d3e9b062e6555dbfb3a6	3fc537665e2154ce9e80c6f4c784cef9
e0e7b4f6878483bdc8c3e01d4daa11c71e61385e85a6eaa2be8fec04d250b74e	cf250cbb6072e84b2b2b25b04c325a4e75f8bcd4	7cee105b82168a5f9aa34acc47231c08
c12e099fb5e825be513c75cff8b4f064b9d4ea8435bab254d69e126b74959372	ff8ac2ab2c6987e351ebcd5606026b3de0256662	29f3253146cbf74a30d02d0e0b179807
8c756a02e7eb863cf1375e7069a92c49fbc669c5e3ea95fb5ddab764096fa31e	caf52b39215639424ae6293d33832211b9829b6f	e53ad7708ff9db1ff5f0a6f31fc36c2c
b1193c3f6f33686e3dd0429e6a873fb5d6f4662af7d43ed72aa4fbae557af56a	de02d48d68cd08a2a66ab6f87c54a84d18343997	8483f41ce77cdbaacae05d5dbc2bfdf4
6b7c7c0d1d574cbd3f7a7df1ed5a78c2340acad9ed319214c12c212dbb6e8b8d	6641163402b293847885a3ad94b64a9d2da5d26c	f351d1ea309d139f895c332d7226dc65
2f36085961f4569733e90c4eb2612cd3b320b60a9270450d30b1943ffefa78a4	7208d987d8802bd653e14ce2223109120c88b7f6	3579f91e64b509e10186e41c4024d94d
a78162bbb5d2b1e90f6bff13e246b7b6f1407b6fe58ba968764aaf8352920c33	0ac461fe1e5f3974ed597b1cd8f933018d6c4966	1850b9492a963a3f4ba116497f47df1a
3b63900e56a7eccee43d42a77fcb6d7834943f5236adae063abe32111f35152d	ae9d505c9822d5680e8ac59eebbe66ea9de0fe2b	71f7e61c2686b4bc1d67745e859b3ca1
5246fc50cce0b3492939a169082eebfde63c9ebc312267eef6d1bb47b44c44aa	ca57a2f0e0e91da297942191889e5f6d058139b2	392b5b60444fa9e27c1de9d977ec9248
534da7cf722968de28eceff23e2924e180bf2c59f3852fb58a4653f8a54fa69a	f618fb54ce246bb0533a95dc315c5259fd195d41	b6be6581862a4fdcf0ff74c88d85fb45
817887f4e977443cb446579f080ae848a2235b79f8c174e7201cebf62e9ccd94	ddbac1755c6d1f564d54e11f4cb2fb24e9a86dfb	2f47656cafc2c6ed0c5a5d7bcbdc74c0
323d0cf9ac1c750761f66482154dbd3144dae7336c955a4576cb4cce6438a6ba	856956c954442ff1a1b91afcc01a3b5bcb82900c	eec690302795ed155f0b1ccc5b3bb9a9
c4fc73dbfc0d61a0a60239971225321b882af5923babf26c324726b80db612a2	38d4812500f6b21d883687ee1034e76f4cdc1c08	c21062f97b2211859a325dd710a92f25

GoldenSpy_Uninstaller - Samples

SHA-256	SHA-1	MD5
d29f78f020e3e50f6692470ad725cb684aa2644596ea0c1b332145a62a6f6a66	508cc8a33b6a3cf26a2f09b7346bd996a53485f2	ed9ec3aec2e8aac13e5d3971f0d56d89
82fb179572b6c4ce92bb2a9950675a135cb88aa64e1b4ca93288f4058a8886f3	9732086c88b6de2ef6f896512ffc2bac8f8c3557	57af01112f6e277c69150f6d5fba51a9
63163b1358e60631f0baf9d04cd8398ca45228ed43d3df48a8b7749fd4181fdf	4bfd2386e78595961eab2c211a716a77350cc614	1484a597aee4850fcf13faac8f382a5c
a9a6116f7a4f592c6bd75e09d9562fe6e21cc9067f6a60cb5d56704a3b746608	c2039528fd8c81110196bb8aba8a115c4d627d2d	a07ebcc316c49c6bbdf0a8d91bf4c546
dfed03b4d22eb818859fdb5cca94ac90d7a538f6bca9a086c9a86806c07f8fe2	bc5722fd5fed2eb0c96032fa467cc5edcffc361f	cc37004f5a1903523657810edb45272e

a26a8103df2d4fd152def868cfead5e1e2c9b333d0d0110cee02c06a98f1c188
8215972987c85e180e7df1a17bac6575df92fe882d0092bf470d2ce651db2585
7b1578fd81d09729784a8200fe79e9255cdd695ac882ec3db22219277c4f675e
3a184ed46b10e27515f8f8726a91886296f7ab1e9c05552b1189d828f15ccb3f
48dbe64eea55a0e579a2e8e12bfe3eb38416563c70a0c49e9ab2d72ac90254ce
5684427b6cd6752bea95cdde7772b28ba0051be97045eef8224a63b5f3da3398
10e8c9ade8687cfb2badb23c90e8f025c2b2e35d0934d287e19c2b14746395c2
e6466b2761600ac993bb0d46e3707fb059edd9212d671c5736cf25070a076508
7f5ed71f18937ecc6db9520ca9a9d16e3c113609c7a9a99a29ba74687f1349d2
7d48f65ff9e904ac98e0f41b94f04723ce907fc221efffbbf83545ca167fe921
985cc0b818fee90bf0cd3b76b60239b5f4eae55f64280c8cca1a667950fb2e4a
7b014a03f58545736685fbad24d65b6324c0c2ad627fadfdb772e1ddcdd15f6c
953cec896a79dc12eecc8e1e48f3b0e43bc9d95bb19dbd7318bae45027ff1334
ac9253dec9288e1277c4b6e842c75de99d156db5ac4516c0780bc2e87b2410c9
9e7957475fb3d849fb1f5bcce5b110f87a47bac621d4a31989c6f5d154b6e0ee
3f823143e545b627759b644fc2d570b08e418ca7
6f36f07b4e5efbf35b4b1f7916a7047db9b49535
8ce91bba10270deb4df88abba1c0a36e80149a48
6b18e8df396a665808ef362354366befc4ed7aeb
86eaf5f70c162d1b383c3e594fe351f9e255f2c5
4a398f91cce12c8152ae0d3d4bed751c804223e2
9092960ab2c9050a3c1a1dd14aab0fb9f779c232
f1a41a475e43a3d89fe1e4250847bf2b7dc22f82
4755b68996b53ad3f734127fe46723b60681856e
3dff337e2b3e1d3dc995a4b6965ae09c1bf5b137
ba7cce6da078c2825b05ee305773edb6
a4e39f608731d31fbcc17d98a3ec8508
72cd43dc5ad0e55f6d26998ac62645e0
568042d040ed7fbbb802d847ef614a4d
08f803140ee607a12b15dca97df5864f
429a1c5756efaab8af3bcee37cccc31f
573adb1569a08472094f0cfbb6264360
f52cc72959e7ed51c75d0b7f6b8611c0
735ac19b261dc66d5850bea21f3d54fe
f2a7363cf43b5900bb872b0d4c627a48

Domains	**Beschreibung**
www.ningzhidata.com	C2-Adresse von GoldenSpy
help.tax-helper.ltd	Domain die durch das FBI dem Vorfall zugeordnet wird
help.tax-assistant.com	Domain die durch das FBI dem Vorfall zugeordnet wird
help.tax-assistant.info	Domain die durch das FBI dem Vorfall zugeordnet wird
info.tax-assistant.com	Domain die durch das FBI dem Vorfall zugeordnet wird

info.tax-assistant.info	Domain die durch das FBI dem Vorfall zugeordnet wird
info.tax-helper.ltd	Domain die durch das FBI dem Vorfall zugeordnet wird
tip.tax-helper.ltd	Domain die durch das FBI dem Vorfall zugeordnet wird
bbs.tax-helper.info	Domain die durch das FBI dem Vorfall zugeordnet wird
update.tax-helper.ltd	Domain die durch das FBI dem Vorfall zugeordnet wird
download.tax-helper.com	Domain die durch das FBI dem Vorfall zugeordnet wird
tools.tax-helper.info	Domain die durch das FBI dem Vorfall zugeordnet wird
update.tax-helper.com	Domain die durch das FBI dem Vorfall zugeordnet wird

IPs

49.232.156.117	C2-Adresse GOLDENSPY
39.98.110.234	neue Adresse der Domain www.ningzhidata.com
223.112.21.2:8090	Adresse zur Verteilung des Uninstallers für GOLDENSPY